A MITEL
PRODUCT
GUIDE

Unify OpenScape Common Management Platform

Common Management Platform V10

Administration Guide
05/2026

A31003-C22A0-M100-34-76A9

Mitel

Notices

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

Trademarks

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

© Copyright 2026, Mitel Networks Corporation

All rights reserved

Contents

1 About this Manual **12**
1.1 Who should read this Guide? 12
1.2 This Manual's Content 12
1.2.1 What you will NOT find in this manual 12
1.3 Structure of this Manual 13
1.4 Markups used 14
1.5 Other Markups 14
1.6 Specified Default Passwords 15
1.7 Data Protection and Data Security 15

2 Overview **17**
2.1 The functional range of the CMP 17
2.2 Browser Requirements for using the CMP 18
2.2.1 How to Allow Pop-ups Generally 19
2.2.2 How to Allow Pop-ups restrictedly 19
2.2.3 Browser based restrictions for the CMP 20

3 General information **21**
3.1 How to Log On to the CMP 21
3.2 Operating the Common Management Platform (CMP) 22
3.3 CMP System Bar 23
3.3.1 How to Configure the Number of Rows in CMP Lists and Disable confirmation messages 24
3.3.2 How to Change the Administrator Password in the CMP 25
3.3.3 How to Configure the Automatic Logout from the CMP 26
3.3.4 How to Open the CMP Online Help 27
3.3.5 How to Display the Installed Software Versions 27
3.3.6 How to Logout from the CMP 28
3.3.7 The functional range of the CMP 28
3.4 CMP Navigation Bar 30
3.4.1 Alarm Indicator / Preferences 30
3.5 CMP Navigation Tree 32
3.6 CMP Work Area 33
3.6.1 Column Settings 35
3.7 Search and Advanced Search Functionality 36
3.7.1 How to Save an Advanced Filter 37
3.7.2 How to Manage an Advanced Filter 38

4 System Management **39**
4.1 Domain Management 39
4.1.1 How to Add a Domain 40
4.1.2 How to Edit Domain Settings 41
4.1.3 How to Delete a Domain 41
4.2 Management Concept of CMP Administrator User 42
4.2.1 How to Display/Edit a CMP/UM Locality Administrator User 42
4.2.2 How to Create a CMP/UM Locality Administrator User 48
4.2.3 How to Delete a CMP/UM Locality Administrator User 52
4.2.4 Policy for User Passwords 53
4.2.5 How To Change Policy for User Passwords 57
4.2.6 How to Display/Edit Foreign Users 59
4.2.7 How to Add Foreign Users 60
4.2.8 How to Delete Foreign Users 61
4.2.9 How to Display/Terminate Active Sessions 61

4.2.10 How to Configure CMP Alarm Indicator / Preferences.....62
4.2.11 How to Define the System settings.....63
4.2.12 How to Add Proxy Server.....64
4.2.13 How to Display / Edit Proxy Server.....65
4.2.14 How to Delete a Proxy Server.....66
4.2.15 How to Configure the SMTP (Simple Mail Transfer Protocol) server.....66
4.2.16 How to Configure CMP/UM Locality Administrator External Identifiers.....67
4.2.17 How to Configure Unify Phone Servers.....68
4.2.18 How to Configure CMP - CloudLink Daemon connection.....69
4.2.18.1 How to Configure OSV - CloudLink Daemon connection.....71
4.3 Profile Management.....72
4.3.1 Default Profiles.....72
4.3.2 System Profiles.....74
4.3.3 Customer Profiles.....74
4.3.4 Special Handling of CMP Administrator Permission.....74
4.3.5 Default Profiles of the CMP.....75
4.3.6 How to map Symphonia permissions to CMP permissions for Upgrades to V7.....76
4.3.7 Default Profiles of the OpenScape Voice Assistant.....84
4.3.8 How to Display/Edit Profile Settings.....88
4.3.9 How to Add a Profile.....89
4.3.10 How to Copy a Profile.....90
4.3.11 How to Delete a User Profile.....91
4.4 System Management.....91
4.4.1 System Overview.....92
4.4.2 How to Display System Nodes.....93
4.4.3 Node Groups.....94
4.4.3.1 How to Display a Node Group.....94
4.4.3.2 How to Add a Node Group.....94
4.4.3.3 How to Edit a Node Group.....95
4.4.3.4 How to Delete a Node Group.....96
4.4.4 3rd Party Nodes.....96
4.4.4.1 How to Display 3rd Party Node Connections.....96
4.4.4.2 How to Add a 3rd Party Nodes Connection.....97
4.4.4.3 How to Edit the Settings of a 3rd Party Node Connection.....98
4.4.4.4 How to Delete a 3rd Party Nodes Connection.....98
4.4.5 Xpression Node.....99
4.4.5.1 How to Add an OSC Xpressions Node.....99
4.4.5.2 How to Modify an OSC Xpressions Node.....100
4.4.5.3 How to Synchronize the accounts of an OSC Xpressions Node in CMP.....101
4.4.5.4 How to Remove an OSC Xpressions Node.....102
4.4.6 OpenScape 4000 Node.....103
4.4.6.1 How to Add an OpenScape 4000 Node.....107
4.4.6.2 How to Modify a OpenScape 4000 Node.....109
4.4.6.3 How to Remove a OpenScape 4000 Node.....111
4.4.6.4 How to configure routing of an OpenScape 4000 Node.....113
4.4.6.5 How to do a Full Synchronization of an OpenScape 4000 Node.....115
4.4.6.6 How to do a manual Delta Synchronization of an OpenScape 4000 Node.....117
4.4.6.7 How to configure the automated Delta Synchronization of an OpenScape 4000 Node.....118
4.4.7 SNMP Node.....121
4.4.7.1 How to Add an SNMP Node.....121
4.4.7.2 How to Modify an SNMP Node.....122
4.4.7.3 How to display the Processes running on a SNMP Node.....123
4.4.7.4 How to display the Packages Installed on a SNMP Node.....123
4.4.7.5 How to Remove an SNMP Node.....124
4.4.8 System Dashboard overview.....125
4.4.8.1 How to Display the Dashboard of a System Node.....125

4.4.8.2 The Application Dashboard..... 125
4.4.8.3 The Frontend Dashboard.....127
4.4.8.4 The Communication System Dashboard.....128
4.4.8.5 The OpenScape 4000 Dashboard.....129
4.4.8.6 The Media Server Dashboard..... 130
4.4.8.7 The Xpressions Dashboard..... 131
4.4.8.8 The RG8700 Dashboard.....132
4.4.8.9 The SNMP Dashboard.....134
4.4.9 How to Display/Edit Component Settings.....134
4.4.9.1 How to configure the SNMP Service Settings.....136
4.4.9.2 How to configure the Personal Workflow Controls Factory component Settings.....138
4.4.10 How to Start / Stop Components.....140
4.4.11 How to Restart a Component..... 141
4.4.12 How to Restart System Nodes..... 142
4.4.13 How to Move a System Node to a Node Group..... 142
4.4.14 How to Configure the Note for a System Node.....143
4.4.15 Software Package Overview.....143
4.4.15.1 How to Display Software Packages..... 144
4.4.16 How to Activate Backup version.....145
4.4.17 How to Synchronize versions..... 146
4.4.18 How to Display Applications..... 147
4.4.19 How to Execute an Action for an Application..... 148
4.4.20 OpenScape External Applications.....148
4.4.20.1 How to create a Connection with OpenScape Fault Management or OpenScape Performance Management.....149
4.4.20.2 How to configure a Connection with OpenScape Fault Management.....152
4.4.20.3 How to remove a Connection to OpenScape Fault Management.....154
4.4.20.4 How to display the OpenScape Fault Management certificate.....154
4.4.20.5 How to create a Connection with OpenScape Accounting.....155
4.4.20.6 How to configure a Connection with OpenScape Accounting.....157
4.4.20.7 How to remove a OpenScape Accounting Connection..... 159
4.4.20.8 How to display the OpenScape Accounting Certificate..... 159
4.4.20.9 How to create a Connection with Device Management (OpenScape Deployment Service)..... 160
4.4.20.10 How to configure a Connection with Device Management.....162
4.4.20.11 How to remove a Device Management Connection..... 164
4.4.20.12 How to display the Device Management Certificate.....165
4.4.21 OpenScape Enterprice Express Applications..... 165
4.4.21.1 How to create a new or configure an existing Connection with OpenScape Enterprice Express Applications..... 166
4.4.21.2 How to remove an Openscape Enterprice Express Applications Connection..... 166
4.4.22 Software Activation (User Interface Patching).....167
4.4.22.1 How to Update/Hotfix in the CMP..... 167
4.5 Managing Licenses 172
4.5.1 License Management Concept..... 172
4.5.2 License Information.....175
4.5.2.1 How to Display License Information.....176
4.5.2.2 How to Display Bound Licenses.....178
4.5.2.3 How to Display Bound Licenses of a Foreign User..... 178
4.5.3 How to Activate Licenses.....178
4.5.3.1 How to Activate License - Offline..... 180
4.5.3.2 How to Activate License - Online.....181
4.5.4 How to Display License Locking IDs via CMP..... 182
4.5.5 Software Subscription License.....183
4.5.5.1 How to Display Software Subscription License Information.....185
4.5.6 How to Display SIEL IDs via CMP..... 187
4.6 Import and Export of System Data 188

4.6.1 How to Export Data for CMP (Common Management Platform)....191
4.6.2 How to Export Assistant Data....192
4.6.3 How to Export All OpenScape Voice Configuration Data....193
4.6.4 How to Export OpenScape Voice ENUM (Electronic Number Mapping) Data....194
4.6.5 How to Export Data for OpenScape Branch....195
4.6.6 How to Export Data for OpenScape SBC (Session Border Controller)....196
4.6.7 How to Export Data Scheduled....197
4.6.8 How to Import Data....198
4.6.8.1 Import Data Report description....200
4.6.9 How to Configure the IM Address by Import....201
4.6.10 Configuration of Voicemail Numbers....202
4.6.10.1 How to Create a New Voicemail Number by Import....202
4.6.10.2 How to Configure a Voicemail Number for User Accounts....203
4.6.10.3 How to Create User Accounts by Import....204
4.6.11 How to Delete Information by Import....206
4.7 Backup and Restore Concept....206
4.7.1 Archives....208
4.7.1.1 How to Display Archives....208
4.7.1.2 How to Add an Archive....209
4.7.1.3 How to Edit an Archive's Settings....211
4.7.1.4 How to Delete an Archive....212
4.7.1.5 How to Test an Archive....212
4.7.1.6 How to Display/Edit an Archive's Backup Sets....213
4.7.1.7 How to Delete an Archive's Backup Sets....213
4.7.2 Backup Sets....214
4.7.2.1 How to Display/Edit the Settings of a Backup Set....217
4.7.2.2 How to Delete a Backup Set....218
4.7.2.3 How to Restore the Entire System After a Crash....219
4.7.3 Backup Schedules....221
4.7.3.1 How to Display Backup Schedules....221
4.7.3.2 How to Add a Backup Schedule....222
4.7.3.3 How to Edit Backup Schedules....224
4.7.3.4 How to Delete a Backup Schedule....225
4.7.4 Jobs....225
4.7.4.1 How to Display the Job Status....225
4.7.4.2 How to Terminate a Job....226
4.7.5 How to Back Up a Backup Set Manually (Immediate Backup)....227
4.7.5.1 How to Back Up a File System with an External USB hard disk on an LVM based deployment....230
4.7.6 How to Back up manually the File System for Standard Duplex on a Non-LVM based deployment....233
4.7.7 How to Back up manually the File System for Standard Duplex on a LVM based deployment....234
4.7.8 How to Back up manually the Backend File System for on a LVM based deployment with Storage Area Network (SAN) Partitions....236
4.7.9 How to Restore OpenScape Configuration Data....238
4.7.10 How to Restore the OpenScape System for Integrated Simplex....240
4.7.11 How to Restore CMP Application for Standard Duplex....242
4.7.12 How Restore the Backend File System with Storage Area Network (SAN) Partitions....245
4.7.13 How to Restore the Response File from a Backup Set....248
4.7.14 Backup Concept for the OpenScape Web Client....250
4.7.14.1 Settings for the System Backup of the OpenScape Web Client....251
4.7.14.2 How to Restore OpenScape Web Client via System Backup....252
4.8 Download Center....253
4.8.1 How to Provide Software in the Download Center....254
4.8.2 How to Provide Documentation in the Download Center....255
4.8.3 How to Download Software....256
4.8.4 How to Download Documentation....256
4.9 Software Repository....257

4.9.1 How to Display available Upgrade File Packages of the Repository....257
4.9.2 How to Upload an Upgrade File Package to the Repository....258
4.9.3 How to Delete an Upgrade File Package from the Repository....259
4.9.4 How to Increase the Software Repository Size....259
4.10 Concept of the Consistency Check 260
4.10.1 How to perform the Consistency Check....261
4.10.2 How to download the Last Check Report....261
4.11 Further Administrative Tasks....262
4.11.1 Starting/restarting OpenScape UC Application....262
4.11.2 Saving the Security Certificate for the CMP....262
4.11.3 Synchronizing License Assignments anew....264
4.11.4 Changing the IP Address of the Application Computer....265
4.11.5 How to Configure the HTTPS Port for CMP Access....267
4.11.6 Activating HTTP Port for Framework....267
4.11.7 Adjusting the CMP User Interface....268
4.11.7.1 How to Adjust the CMP User Interface....272
4.11.8 Configuring Single Sign-On (SSO) for CMP....273
4.11.8.1 How to Configure Active Directory (AD)....274
4.11.8.2 How to Configure CMP....276
4.11.9 CAC (Common Access Card) Login Method to CMP....278

5 System Monitoring....282
5.1 Concept of Alarms, Fault Messages and SNMP traps....282
5.2 Alarm Reporting....283
5.2.1 Active Alarms....284
5.2.1.1 How to Display Active Alarms....286
5.2.1.2 How to Set a Filter for Active Alarms....286
5.2.1.3 How to Change Filter for Active Alarms....288
5.2.1.4 How to Delete a Filter for Active Alarms....288
5.2.1.5 How to Mask an Alarm....289
5.2.1.6 How to Display Masked Alarms....289
5.2.1.7 How to Confirm Alarms....289
5.2.1.8 How to Cancel an Alarm Acknowledgement....290
5.2.1.9 How to Clear Alarms....290
5.2.1.10 Alarm Severities....291
5.2.2 Alarm Email Notification....292
5.2.2.1 How to Configure E911 Alarm Email Notification....292
5.2.2.2 How to Add/Edit Recipients of E911 Alarm Email Notification....293
5.2.3 Alarm Logs....294
5.2.3.1 How to Display Alarm Log....294
5.2.3.2 How to Set a Filter for Alarm Logs....295
5.2.3.3 How to Change Filter for Active Alarms....296
5.2.3.4 How to Delete a Filter for Alarm Log....297
5.2.4 System Log Concept....297
5.2.4.1 How to Display a System Log....298
5.2.4.2 How to Export a System Log....299
5.2.4.3 How to Load a System Log....299
5.2.4.4 How to Set Filter for a System Log....299
5.2.4.5 How to Clear Filter for System Log....301
5.2.5 Security Log Concept....301
5.2.5.1 How to Display a Security Log....302
5.2.5.2 How to Export a Security Log....302
5.2.5.3 How to Load a Security Log....302
5.2.5.4 How to Set Filter for a Security Log....303
5.2.5.5 How to Clear Filter for Security Log....304
5.2.6 Remote logging for OSV-Trace Manager....305

5.2.6.1 How to Configure Remote logging for OSV Trace Manager....306
5.2.7 Backing up the Log Files....308
5.2.7.1 How to Estimate Backup Interval....309
5.2.8 SysLog....310
5.2.8.1 How to Enable SysLog for the System or/and SecurityLog....310
5.3 Configuration Files....311
5.3.1 How to Display Configuration Files....313
5.3.2 How to Display Metadata of a Configuration File....314
5.3.3 How to Modify Logging Cycle (Appender Configuration)....315
5.3.4 How to Start / Stop Cyclic Overwriting....315
5.3.5 How to Start / Stop an Online Trace....316
5.3.6 How to Activate a Loaded Configuration File....316
5.3.7 How to Upload and Activate a Configuration File....317
5.3.8 How to Backup Configuration Files....318
5.3.9 How to Delete a Configuration File....318
5.3.10 How to Restore the Default Configuration....318
5.4 Diagnostics Data....319
5.4.1 How to Export Diagnostics Data....319
5.4.2 How to Start a new Log File....320
5.5 Online Trace....320
5.5.1 How to Download Trace Files....320
5.5.2 How to Change the Port for an Online Trace....321
5.6 SNMP Notifications....322
5.6.1 SNMP V3 Users....322
5.6.1.1 How to Add an SNMP V3 User....322
5.6.1.2 How to View and Edit an SNMP V3 User....323
5.6.1.3 How to Delete SNMP V3 Users....323
5.6.2 How to Configure SNMP Security....324
5.6.3 Alarm Destination....324
5.6.3.1 How to Add an Alarm Destination....324
5.6.3.2 How to View and Edit an Alarm Destination....325
5.6.3.3 How to Clear Alarm Destinations....326
5.6.4 How to Configure SNMP V3 Settings....326

6 Alarms....328

7 Application server certificates....354
7.1 Customer Environments....358
7.1.1 Customer Environment 1 (ENV 1)– PKI with self-maintained CA....358
7.1.2 Customer Environment 2 (ENV 2)– PKI with self-maintained CA and CSR....359
7.1.3 Customer Environment 3 (ENV 3)– PKI with a commercial CA....359
7.1.4 Customer Environment 4 (ENV 4)– No PKI available....360
7.2 Overview of the Configuration Steps....360
7.3 Preparing the Configuration of the Certificate Strategy....361
7.3.1 Determining the Setup Directory of CMP....361
7.3.2 Defining an X.500 Distinguished Name....362
7.4 Creating a new Certificate Authority....363
7.4.1 Preparation for the Certificate Authority....364
7.4.2 Creating self-signed CA Certificate....366
7.5 Creating the CMP Application Server Certificates....368
7.5.1 Preparation for the Application Server Certificates....368
7.5.2 Creating a key pair for the Application Computer....370
7.5.3 Creating a Certificate Sign Request for the Application Server....370
7.5.4 Signing a Certificate Sign Request....372
7.5.5 Creating a PKSCS#12 keystore....374
7.6 Activating the CMP Application Server keystores....376

7.6.1 Activating the application server keystore for CMP Tomcat Web Server....376
7.6.1.1 Obfuscating the keystore password in the CMP Tomcat's server.xml....378
7.6.2 Activating the application server certificates for CMP Apache Web server....379
7.6.3 Configuring and Rotating Cryptographic Keys for Symphonia....380
7.7 Importing the Root Certificate in the Client Browsers....382
7.7.1 Inspecting the Root Certificate....382
7.7.2 Validating the root certificate....383
7.7.3 Installing the root certificate....384
7.8 Additional Instructions....384
7.8.1 Creating a secure Password....384
7.8.2 Combining multiple certificate files in a certificate chain....385
7.8.3 Converting a certificate chain from DER format to PEM format....386
7.8.4 Converting a certificate chain from PKCS#12 format into PEM format....386

8 OpenScape User Management Overview....388

9 OpenScape User Management License Management....389
9.1 Licensing model for upgrading to OS User Management V10....390
9.2 Licensing model for upgrading to OS User Management V7R2....390
9.2.1 License consumption in OS User Management V7R2....390
9.3 Licensing model for upgrading to OS User Management V7....391
9.3.1 How to Install and Load OS UM V7 GPCF licenses on a System with V6 GPCF....391
9.3.2 How to Install and Load OS UM V7 GPCF licenses on a System with commercial V6 OS UM license file....392
9.3.3 How to Install and Load OS UM V7 commercial licenses....392
9.4 How to check if OS UM User licenses are sufficient....393
9.5 How to grant access to OS UM as soon as sufficient licenses are activated....394

10 OpenScape User Management Administration....395
10.1 Users & Resources....395
10.1.1 How to Display Users....400
10.1.2 How to Display Users' Resources....403
10.1.3 How to Create Users....404
10.1.3.1 How to Create PINs for a User's OpenScape 4000 station....408
10.1.4 How to Create a Resource or Select an existing one....410
10.1.4.1 How to Create an OpenScape Voice Resource or Select an existing one....412
10.1.4.2 How to Create an OpenScape Voice Softphone Resource or Select an existing one....418
10.1.4.3 How to Create an OpenScape Mobile Resource....425
10.1.4.4 How to Create an OpenScape 4000 Resource or Select an existing one....429
10.1.4.5 How to Create an OpenScape Xpressions Resource or Select an existing one....434
10.1.4.6 How to Create a Unified Communications Resource or Edit an existing one....440
10.1.4.7 How to Create an External Resource....445
10.1.4.8 How to Create a Unify Phone Resource....446
10.1.4.9 How to Create a Zoom Resource....447
10.1.5 How to Modify Users....448
10.1.6 How to Modify Users' Resources....451
10.1.6.1 How to Modify Users' Attributes in the bulk mode....454
10.1.7 Moving Resources (OpenScape 4000 Resource)....456
10.1.7.1 How to Move an OpenScape 4000 Resource....457
10.1.7.2 How to Move an OpenScape 4000 Resource using wizard....459
10.1.7.3 How to Change PEN for an OpenScape 4000 Resource....463
10.1.8 How to Delete Users....464
10.1.9 How to Delete or Unassign User's Resources....466
10.1.9.1 How to Delete or Unassign Users' Resources in bulk mode....468
10.1.10 How to perform bulk operations with All UM Users....470
10.1.11 Pickup and Hunt Groups within the User Management....472
10.1.11.1 How to Add Users to a Pickup Group....473

10.1.11.2 How to Add Users to a Hunt Group....474
10.1.11.3 How to Remove Users from a Pickup Group....476
10.1.11.4 How to Remove Users from a Hunt Group....477
10.1.11.5 How to Display Pickup and Hunt Group information in the UM Users list....478
10.1.11.6 How to Add User's Resources to a Pickup Group....480
10.1.11.7 How to Add User's Resources to a Hunt Group....482
10.1.11.8 How to Remove User's Resources from a Pickup Group....483
10.1.11.9 How to Remove User's Resources from a Hunt Group....484
10.1.11.10 How to Display Pickup and Hunt Group information in the UM User's Resources list....486
10.2 Localities....487
10.2.1 How to Display Localities....488
10.2.2 How to Create Localities....489
10.2.3 How to Edit Localities....491
10.2.3.1 How to Define default values for OpenScape Voice Resource....494
10.2.3.2 How to Define default values for OpenScape Voice Softphone Resource....495
10.2.3.3 How to Define default values for OpenScape 4000 Resource....496
10.2.3.4 How to Define default values for Xpressions Resource....497
10.2.3.5 How to Define default values for UC Resource....498
10.2.4 How to Delete Localities....498
10.3 User Templates....500
10.3.1 How to Display User Templates....501
10.3.2 How to Create / Clone User Template....502
10.3.2.1 How to Create User Template with the OpenScape Voice Resource....506
10.3.2.2 How to Create User Template with the OpenScape Voice Softphone Resource....512
10.3.2.3 How to Create User Template with the OpenScape Mobile (OSMO) Resource....516
10.3.2.4 How to Create User Template with the OpenScape 4000 Resource....519
10.3.2.5 How to Create User Template with the OpenScape Xpressions Resource....525
10.3.2.6 How to Create User Template with the Unified Communications Resource....541
10.3.2.7 How to Create User Template with the External Resource....548
10.3.2.8 How to Create User Template with the Xpressions/UC Integration Resource....550
10.3.2.9 How to Create User Template with the Common Management Platform Administrator....552
10.3.2.10 How to Create User Template with the Unify Phone....556
10.3.2.11 How to Create User Template with Zoom....558
10.3.3 How to Edit User Templates....559
10.3.4 How to Delete User Template....564
10.3.5 Modifying Resource Attributes during User Template re-apply....565
10.3.6 Applying the User Template's rules....566
10.3.7 Manage Users associated with a User Template....567
10.3.7.1 How to add Resource for selected Users based on the User Template....567
10.3.7.2 How to Reset the configuration of all User's Resources to default....585
10.3.7.3 How to Manually dissociate a User from an User Template....588
10.4 Extension Ranges....590
10.4.1 How to Define an Extension Range....591
10.4.2 How to Define a Reserved Extension Range....592
10.4.3 How to Display Extension Ranges....593
10.5 Custom User Attributes....593
10.5.1 How to Add a Custom User Attribute....594
10.5.2 How to Edit a Custom User Attribute....594
10.5.3 How to Delete a Custom User Attribute....595
10.6 Organizational Structure Attributes....595
10.6.1 How to Edit an Organizational Structure Attribute....595
10.7 E-Mail Templates....596
10.7.1 How to set up E-mail Templates....596
10.7.2 How to Customize E-mail Templates....597
10.8 Resource Migration....597
10.8.1 How to configure OSV Migration Settings....598

10.8.2 How to Migrate to OSV resource..... 599
10.8.3 How to Migrate to OpenScape 4000 resource..... 603

11 OpenScape User Management Provisioning..... 605
11.1 How to Import Users and Resources with a CSV file..... 605
11.2 How to Import Users from HPUM..... 611
11.3 Synchronization with an LDAP Directory..... 615
11.3.1 How to Setup LDAP Connection..... 615
11.3.1.1 How to configure the LDAP security for CMP..... 621
11.3.2 How to Deactivate LDAP Connection..... 625
11.3.3 How to configure different LDAP synchronization per CMP Domain..... 626
11.3.4 How to retrieve the available LDAP Attributes..... 626
11.3.5 How to perform LDAP Attribute Mappings..... 627
11.3.5.1 How to perform Automatic Resource creation via User Template..... 645
11.3.6 How to perform Advanced Attribute Mapping..... 647
11.3.6.1 How to perform Value Mapping..... 649
11.3.7 Partial LDAP synchronization..... 650
11.3.7.1 How to define a Simple LDAP filter..... 651
11.3.7.2 How to define an Advanced LDAP filter..... 652
11.3.7.3 How to switch from Advanced to Simple LDAP filter..... 653
11.3.8 LDAP Scheduled Synchronization..... 654
11.3.8.1 How to setup LDAP Scheduled Synchronization..... 655
11.3.9 How to perform LDAP Manual Synchronization..... 661
11.3.10 How to delete the LDAP Attribute Mapping..... 667
11.4 How to Create UM Users based on the UC Accounts..... 668
11.4.1 How to create UM Users from the existing UC Accounts on a new CMP installation..... 671
11.5 How to Create UM Users based on the OSV Subscribers..... 671

12 OpenScape User Management Unify Phone..... 677
12.1 Unify Phone Configurations..... 677
12.1.1 How to Create a new SBC configuration for Unify Phone users..... 677
12.1.2 How to Edit a SBC configuration for Unify Phone users..... 678
12.2 Unify Phone Users..... 679
12.2.1 How to Display Unify Phone Users list..... 679
12.2.2 How to Add a Unify Phone User..... 680
12.2.3 How to Edit a Unify Phone User..... 682
12.2.4 How to Delete a Unify Phone User..... 682
12.2.5 How to Reinvite a Unify Phone User..... 683

13 OpenScape User Management for Zoom..... 684
13.1 How to Create a new Zoom configuration..... 684
13.2 How to Edit a Zoom configuration..... 685

14 Zoom Users Configuration..... 687
14.1 How to Add a Zoom User..... 687
14.2 How to Display Zoom Users..... 688
14.3 How to Edit a Zoom User..... 689
14.4 How to Delete a Zoom User..... 690

15 Appendix A: Character Restrictions..... 691

Index..... 692

1 About this Manual

1.1 Who should read this Guide?

This document addresses Service personnel and Administrators who configure and manage the Common Management Platform.

Readers should have the following knowledge for making full use of the information provided in this document:

- Knowledge of the general working method of information technology and voice communication systems
- Knowledge of terms used in the information technology and voice communication systems
- 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 OpenScape Voice system if it is to be configured with CMP

1.2 This Manual’s Content

This manual provides a guideline for configuring a communication solution based on Common Management Platform after you have installed all required system components

Furthermore, this manual presents:

- the available Common Management Platform features and how to operate them.
- guidelines for managing and monitoring the communications solution with the Common Management Platform
- guidelines for backing up and restoring the configuration of your communication solution within the Common Management Portal

1.2.1 What you will NOT find in this manual

This manual does NOT cover the following topics:

- How to install the described system components. This includes the OpenScape applications as well as the external system components (OSV, UC,RG8700, OpenScape Branch).

  You will find information for the above in the setup manuals of the respective system components.
- How to install and configure the client components for using the features described here

  You will find information about the above in the product manuals of the respective client components.

- How to install and configure the network based on the specific network topology.

  You will find information about this in the product manuals of the respective gateway components concerned
- Detailed configuration instructions for system components that are not Common Management Platform components

  This manual contains only guidelines for configuring such system components. Detail description of the system components can be found in the respective configuration manuals.
- How to manage, monitor, back up or restore system components that are not Common Management Platform elements

  You can information about this in the respective product manuals of these system components.

1.3 Structure of this Manual

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 find your way on the following pages and to quickly access important and useful information.

Chapter 2 – Overview

This chapter provides a general overview of the central OpenScape configuration interface – the Common Management Platform.

Chapter 3 –General information

In this chapter you learn how to log on to the Common Management Platform and operate it.

Chapter 4 – System Management

This chapter describes concepts and general tasks for managing an OpenScape system via CMP.

Chapter 5 – System Monitoring

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

Chapter 6– Alarms

This chapter describes alarms that can be displayed in the Common Management Platform.

Chapter 7 – Application server certificates

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

Chapter 8 – OpenScape User Management Overview

This chapter provides an overview of concepts and general tasks for User Management.

Chapter 9 - OpenScape User Management Licence Management

User Management is a licensed product. This chapter describes the UM licensing model, user license management, installation, and other liecnse configurations.

Chapter 10 - OpenScape User Management Administration

This chapter covers the concepts of UM administration and describes administrator configurations in the UM environment.

Chapter 11 - OpenScape User Management Provisioning

This chapter describes the provisioning scenarios supported in the UM system for effiency and ease of use.

Chapter 12 - OpenScape User Management Unify Phone

This chapter enables you to configure Unify Phone resources and other actions required for Unify Phone management.

1.4 Markups used

In this document we use the following markups to highlight selected text passages:

Element	Markup
GUI elements	Click on **Save** to …
Sequence of menu entries	**Users& Resources** > **Resources**
Command line output	`C:> unknown command`
System input	Enter `true` in field ...
Directory and file names	`/var/config.xml`
File contents	`conname=%CONNECTION_NAME%`
Names of keyboard keys	Press `ESC` to …
Specifications with variable content	<user name >
Active cross reference for skipping to the specified passage in the manual	Text Markups Chapter 1, "About Manual"

1.5 Other Markups

In this document we use the following markings to draw your attention to selected content.

IMPORTANT:

This indicates notes that carry information of high priority. You definitely need to act according to such information to rule out malfunctions, damage to devices or possible loss of data.

NOTICE:

This indicates notes that point to information worth knowing or recommendations.

1.6 Specified Default Passwords

In various sections 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 be changed by the administrator for security reasons.

A default password mentioned in the relevant manual section may therefore not be valid any more after the installation /configuration 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.

1.7 Data Protection and Data Security

This system processes and uses personal data for purposes such as display, 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 Software and Solutions 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.

2 Overview

2.1 The functional range of the CMP

The Common Management Platform is the browser-based configuration interface for the OpenScape communications solution.

CMP contains general management features that you can use to administer default components of the OpenScape communications solution. Such general management features are in particular:

- **System management**

  Using the system management you can quickly gain an overview of the available system nodes and their logical grouping (clustering). Furthermore, it provides auxiliary means to configure these system nodes and to log this configuration
- **Domain management**

  With the domain administration you can divide the OpenScape system into different domains. The system can be split into domains, where each domain corresponds to a separate administration area with independent administration rights. All users, resources and profiles in the system are assigned to precisely one domain and are not visible in another domain
- **Profile management**

  The profile management enables you to administer the access privileges for the OpenScape system in a standardized way.
- **User management**

  With the user management you administer the user accounts for the OpenScape system.
- **Resource management**

  With the resource management you administer the OpenScape system resources.
- **Contact list management**

  Using the contact list management you administer the different contact lists of the OpenScape system
- **License management**

  The legal use of the OpenScape system features requires licenses. You can use the license management to activate these licenses and to view activated license information.
- **Alarm and error messages**

  The various OpenScape system components create alarms and error messages when detecting irregularities in the system. The associated alarm and error information is combined in the CMP and be centrally monitored.
- **Logging**

  Important UC and CMP data are recorded in the background and stored in log files.
- **Audit log**

  The audit log logs all important activities performed by the Common Management Platform users.

- **Backup and restore**

  The system configuration and the OpenScape system data can be backed up in regular intervals or when required. You can use the information backed up in this way for restoring the OpenScape system
- **Import and export**

  You can import and export data of the system and domain administration
- **Download center**

  You can use the download center to download different resources from a central place.
- **Software repository**

  In the software repository you can store and manage upgrade files for the different applications of an OpenScape system.

In addition to these general management features the Common Management Platform can integrate further administration interfaces, which belong to other, independent OpenScape components. For example, the OpenScape Voice Assistant, with which you administer and configure the OpenScape Voice communications system

The Common Management Platform provides the described default features however the advanced administration interfaces are only available if you use the associated system component (OSV assistant, UC assistant, OpenScape Branch assistant, RG8700) in your OpenScape communications solution.

Which of the available features are offered to you in the Common Management Platform depends on the access privileges assigned to your user account.

NOTICE:

V9 UC/DVD application server (all deployments) is compatible/ supported on SLES11 SP3/SP4 and also on SLES12 64bit Operating System

---

2.2 Browser Requirements for using the CMP

The Common Management Platform is a browser-based configuration interface. Please note the following for the web browser you use to invoke the Common Management Platform.

The CMP is optimized for:

- Internet Explorer (IE) 7.0, IE 8.0 (compatibility mode), IE 9.0 (compatibility mode), IE 10.0 (compatibility mode), IE 11.0 (compatibility mode)

  NOTICE:

  When using Internet Explorer (IE) browsers, it is recommended to set following option for Temporary Internet Files: Navigate to **Tools#> Internet Options** > **General** > **Settings** > **Temporary Internet Files,** select "**Every time I visit the web page**" and then Press "**OK**"

- Firefox ESR45 (Extended Support Release)

- Google Chrome

NOTICE:

Using different versions of IE or other browsers may lead to rendering errors and/or limited functionality

NOTICE:

When using IE 11 in Windows Server 2008 R2 machines: Navigate to **Internet Options** > **General** > **Tabs** and select "**Always open pop-ups in a new tab**" under the option "**When a pop-up is encountered:**" and then Press "**OK**"

Set the web browser used in a way that it allows pop-ups in general or at least for the internet address under which the Common Management Platform is accessible.

2.2.1 How to Allow Pop-ups Generally

You need to allow pop-ups in the web browser used for deploying the Common Management Platform.

How to generally allow pop-ups in the Internet Explorer:

Step by Step

1) Select **Tools** > **Internet Options …** in the main menu.
2) Switch to the **Privacy** tab.
3) In the **Pop-up Blocker** section deactivate the **Turn on Pop_up Blocker** option.
4) Select **OK**.

2.2.2 How to Allow Pop-ups restrictedly

You need to allow pop-ups in the web browser used for deploying the Common Management Platform.

How to allow pop-ups selectively in the Internet Explorer:

Step by Step

1) Select **Tools** > **Internet Options …** in the main menu.
2) Switch to the **Privacy** tab.
3) In the **Pop-up Blocker** section activate the **Turn on Pop_up Blocker** option.
4) Click on **Settings** in the same section.

5) Specify in the first field the internet address of the server on which the Common Management Platform is installed.
6) Select **Add**.
7) Select **Close**.
8) Select **OK**.

2.2.3 Browser based restrictions for the CMP

You cannot save the user password for logging on to the Common Management Platform in the internet explorer.

3 General information

3.1 How to Log On to the CMP

To administer the OpenScape system with the Common Management Platform, you need to log on to the Common Management Platform under a user account that has been assigned administrator privileges. The default user account for this is administrator@system.

Prerequisites

Before you can deploy the Common Management Platform you need to allow pop-ups in the web browser used.

Step by Step

1) Enter the following internet address in your web browser to invoke the Common Management Platform:

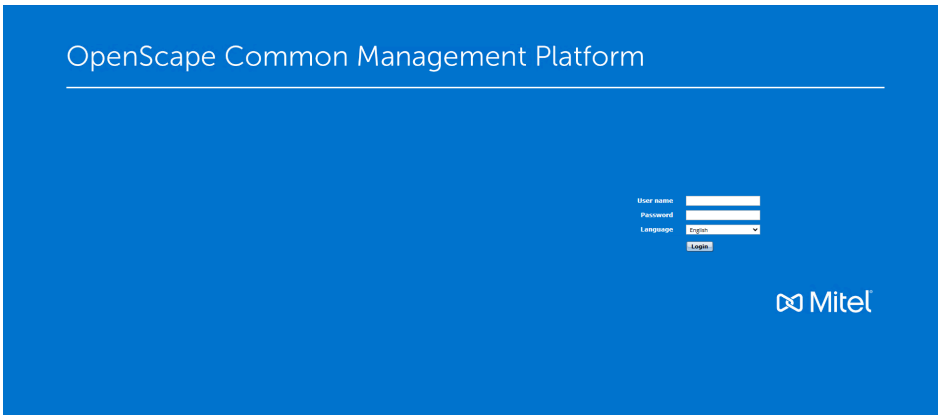
   `https://<server IP address>:<port>/management`

   `<server IP address>` corresponds to the IP address of the server on which the Common Management Platform is installed. `<port>` defines the port number via which communication is to take place.

   `https://10.12.5.100:443/management`

2) If the web browser prompts you to accept or install a security certificate, please follow the respective instructions.

   The Common Management Platform login dialog opens.



3) From the **Language** drop-down list select the language in which the Common Management Platform is to be displayed.

   The login page appears in the selected language.

4) In the **User name** field specify the ID of the user account with which you want to log on, and enter the associated password in the **Password** field.

   You need to deploy a user account that has been assigned administrator privileges.

   When you log on to the Common Management Platform for the first time you need to use the `administrator@system` default user-ID. The password

for this user ID was specified during the Common Management Platform installation.

IMPORTANT: Please change the password for the administrator@system user ID immediately after the initial login for security reasons.

NOTICE: Please heed case sensitivity and check the setting of the `Num` key on your keyboard.

NOTICE: If you do not know your user ID and/ or the associated password, please contact your system administrator.

---

5) Click on **Login**.
If the entries are correct, the Common Management Platform start page appears in the selected language

Next steps

If you are inactive in the Common Management Platform for 10 minutes by default, the system will automatically log you off for security reasons. To continue working in the Common Management Platform you need to log back in again.

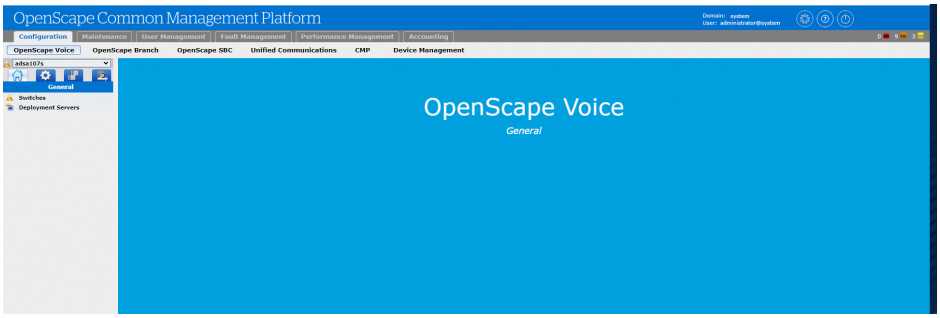
3.2 Operating the Common Management Platform (CMP)

The Common Management Platform is the browser-based configuration interface for the OpenScape communications solution. It provides general management features that you use to administer node-spanning system functions of the OpenScape communications solution, and also special management features that you use to administer system functions of selected system nodes.

The Common Management Platform user interface consists of HTML pages that can be displayed with a web browser. Thus the Common Management Platform works platform-independent under all prevalent operating systems.

The Common Management Platform user interface is divided into the following areas:

1) Navigation bar
2) System bar
3) Work area
4) Navigation tree



You can adjust selected Common Management Platform elements to individual requirements.

The CMP is optimized for:

- Internet Explorer 7.0
- Internet Explorer 8.0 (compatibility mode)
- Internet Explorer 9.0 (compatibility mode)
- Internet Explorer 10.0 (compatibility mode)
- Internet Explorer 11.0 (compatibility mode)
- Firefox ESR45 (Extended Support Release)
- Google Chrome

NOTICE:

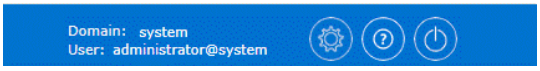
Using different versions of the browsers above may lead to rendering errors and/or limited functionality.

When using the Common Management Platform please note the following.

- Set the web browser used in a way that it allows pop-ups in general or at least for the internet address under which the Common Management Platform is accessible.
- You cannot save the user password for logging on to the Common Management Platform in the internet explorer.

3.3 CMP System Bar

On the Common Management Platform system bar you can see the domain you are logged in and the user ID with which you are logged in at the Common Management Platform.



The system bar contains the following elements.

1) Name of the current user

Displays the user ID with which you are logged in at the Common Management Platform.

2) Menu bar

When you click an option in the menu bar, a list of further menu options appears. The menu options comprise functions which are common to

all applications, as well as further entries which depend on the installed applications and your administrator rights.

For the Common Management Platform the following menu entries can be available:

- **Settings** > **General**

  Defines basic CMP settings for the logged in administrator.
- **Settings** > **Change Password**

  On this tab you can change your user password for the CMP. This is only possible if your user profile is set up accordingly (Symphonia Administrator).
- **Help**

  Click on **Help** to open the online help.

  Click on **About** to display the installed Software Applications.
- **Logout**

  Log-out the logged on administrator from the Common Management Platform.

3.3.1 How to Configure the Number of Rows in CMP Lists and Disable confirmation messages

The Common Management Platform work area displays information in the form of lists. You can customize the number of list rows displayed on a Common Management Platform page. If these rows and thus the entire list cannot be displayed on one page, they are distributed among several pages in the Common Management Platform.

Prerequisites

Adequate administrative permissions

Step by Step

1) Select the **General** menu item from the **Settings** menu in the menu bar.

2) Select the required value in the **Number of rows per list** drop-down list.

The value you enter will be the default value for all lists that you haven't customized. However you may customize a list by specifically changing the number of displayed items.

3) Tick the checkbox **Force it to all lists** if you want to apply the default **Number of Rows per list** value to all the lists, even the customized ones (i.e. Reset all lists to default). The tick will not be saved on the form after click **Save** button, as it works as an one-time action to all lists.

4) Tick on the checkbox if you want to **Disable confirmation messages**

Confirmation messages appear everytime you perform an action within CMP User Interface (add, delete, edit etc)

5) Select **Save** to confirm your entries.

6) Refresh the web browser's display if required (e.g. click on ctrl + F5).

The Common Management Platform lists are from now on displayed with the selected number of rows and no confirmation messages appear.

NOTICE: Every CMP Administrator can define his own timeout setting.

3.3.2 How to Change the Administrator Password in the CMP

How to change the Administrator password for CMP:

Prerequisites

Adequate administrative permissions (Symphonia Administrator)

Step by Step

1) The Change Password prompt is displayed in the following cases:

- A CMP administrator forgot his/her password and requested a new one. A higher level administrator configured a new password for him/her in his/her user profile
- An administrator is logging on for the first time. However, this option must be entered in the CMP Administrator user profile

2) Select the **Change Password** menu item from the **Settings** menu in the menu bar.

3) Enter the old password in the **Old password** field.

4) Enter a new password in the **New Password** and **Confirm Password** field.

NOTICE:

The entries in the **New Password** and **Confirm Password** must be identical. An error message will otherwise appear and the new password not accepted.

NOTICE:

Passwords must comply with the system password policy. All attempts to change the password are logged

---

[1]

[1] Policy Password is described in chapter 4.2.4 "Policy for User Passwords"

5) Select **Save** to confirm your entries.

You need to use the new password for the next login to the Common Management Platform.

NOTICE:

The Password Notification prompt is displayed after login to CMP. The user will get this notification after every login until the day that the password actually expires, when he will be actually forced to change it.

The mechanism checks the timestamp in milliseconds of first login of CMP user, stored on database versus the configurable <MaximumAge>7776000000</MaximumAge> attribute in milliseconds (90 days) in the PassphrasePolicyConfig.xml file.

The default PasswordNotificationTimer value is set to 5 days and it may be set on:

Maintenance > **Inventory** > **Nodes** > **offboard** > **Show Services** and then edit the component "CmpAdmin Service".

For more information on how to create a secure password and password restrictions, please refer to chapter Creating a secure Password on page 384.

3.3.3 How to Configure the Automatic Logout from the CMP

If you are inactive in the **Common Management Platform** for 10 minutes by default, the system will automatically log you off for security reasons. You can customize the time after which you are automatically logged out of the system.

Prerequisites

Adequate administrative permissions

Step by Step

1) Select **Configuration** from the Navigation tab.
2) Select **CMP** from the Navigation menu.
3) Choose the **System Setting** from the Navigation tree.
4) In the **Auto Log Off time out value** field specify the time in minutes after which you are automatically logged out of the system if you remain inactive in the **Common Management Platform**.
5) Select **Save** to confirm your entries.

From now on the system will automatically log you out after the specified time.

NOTICE: Every CMP Administrator can define his own timeout setting.

3.3.4 How to Open the CMP Online Help

The Common Management Platform is set up with an integrated online help. You can generally open this online help via the work area or from an individual dialog.

Procedure

- Select the **Help** button on the menu bar and click on Help

  The online help opens with its title page and all the relevant books of the deployment (e.g Admin manual of SBC, Media Server, CMP, OSV etc).
- Select the help icon in a dialog .

  The online help opens with a page that contains a dialog-relevant description.

3.3.5 How to Display the Installed Software Versions

The Software Version overview displays which software versions are installed on the available system applications. You can open this information via the work area.

Procedure

- Select the **Help** button on the menu bar and click on About.

  A dialog opens that displays a list of **Applications** installed on the system and the **Version/Build** of each application.

NOTICE:

The application **Name**, **Timestamp of Installation or Sync** and the **Software Version** are displayed with the following naming convention:

Vx Ry.p.e-b

Where :

x=Major Release

y=Minor Release

p=Patchset

e=Emergency Patch

b=Build of the solution

For example V7 R1.5.2-141 means Version 7, minor release 1, patchset 5, emergency patch 2, build 141

NOTICE:

The list is displayed according to the **Item/page** value of the window.

3.3.6 How to Logout from the CMP

If you want to shut down the Common Management Platform or log back on with another user ID, you need to log off from the Common Management Platform via Logout first.

Step by Step

1) In the menu bar click on **Logout**.

   The login dialog appears.
2) If you want to exit Common Management Platform, close your browser.
3) If you want to log on to the Common Management Platform with another user ID, enter the appropriate user name and password and click **Login**.

3.3.7 The functional range of the CMP

The Common Management Platform is the browser-based configuration interface for the OpenScape communications solution.

CMP contains general management features that you can use to administer default components of the OpenScape communications solution. Such general management features are in particular:

- **System management**

  Using the system management you can quickly gain an overview of the available system nodes and their logical grouping (clustering). Furthermore, it provides auxiliary means to configure these system nodes and to log this configuration
- **Domain management**

  With the domain administration you can divide the OpenScape system into different domains. The system can be split into domains, where each domain corresponds to a separate administration area with independent administration rights. All users, resources and profiles in the system are assigned to precisely one domain and are not visible in another domain
- **Profile management**

  The profile management enables you to administer the access privileges for the OpenScape system in a standardized way.
- **User management**

  With the user management you administer the user accounts for the OpenScape system.
- **Resource management**

  With the resource management you administer the OpenScape system resources.
- **Contact list management**

  Using the contact list management you administer the different contact lists of the OpenScape system

- **License management**

  The legal use of the OpenScape system features requires licenses. You can use the license management to activate these licenses and to view activated license information.
- **Alarm and error messages**

  The various OpenScape system components create alarms and error messages when detecting irregularities in the system. The associated alarm and error information is combined in the CMP and be centrally monitored.
- **Logging**

  Important UC and CMP data are recorded in the background and stored in log files.
- **Audit log**

  The audit log logs all important activities performed by the Common Management Platform users.
- **Backup and restore**

  The system configuration and the OpenScape system data can be backed up in regular intervals or when required. You can use the information backed up in this way for restoring the OpenScape system
- **Import and export**

  You can import and export data of the system and domain administration
- **Download center**

  You can use the download center to download different resources from a central place.
- **Software repository**

  In the software repository you can store and manage upgrade files for the different applications of an OpenScape system.

In addition to these general management features the Common Management Platform can integrate further administration interfaces, which belong to other, independent OpenScape components. For example, the OpenScape Voice Assistant, with which you administer and configure the OpenScape Voice communications system

The Common Management Platform provides the described default features however the advanced administration interfaces are only available if you use the associated system component (OSV assistant, UC assistant, OpenScape Branch assistant, RG8700) in your OpenScape communications solution.

Which of the available features are offered to you in the Common Management Platform depends on the access privileges assigned to your user account.

NOTICE:

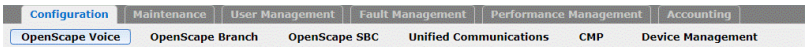
V9 UC/DVD application server (all deployments) is compatible/ supported on SLES11 SP3/SP4 and also on SLES12 64bit Operating System

---

3.4 CMP Navigation Bar

In the Common Management Platform navigation bar you can see the different navigation tabs. Each navigation tab contains a navigation menu with different navigation menu options.

The OpenScape applications installed on your OpenScape system and the access privileges of your user account determine which navigation tabs and navigation menu options you see.



The navigation bar contains the following elements

1) Navigation tab

When you click a navigation tab, the menu items assigned to the tab appear in the navigation menu. The default navigation menu item assigned to the tab is highlighted. The navigation tree belonging to the menu item appears on the left in the browser window, while the work area displays the associated home page.

2) Navigation menu

When you click a navigation menu item, the navigation tree opens and the default entry assigned to the menu item is highlighted. The home page is displayed in the work area.

3) Alarm Preferences

The three most crucial alarms types are depicted. Critical, Major and Minor alarm appear in their respective color.

3.4.1 Alarm Indicator / Preferences

The alarm indicator provides an overview of the most crucial Alarms that are triggered in the system.

You can configure the Alarm indicator if you navigate in the CMP **Configure** > **CMP** > **General** > **Alarm Indicator**.

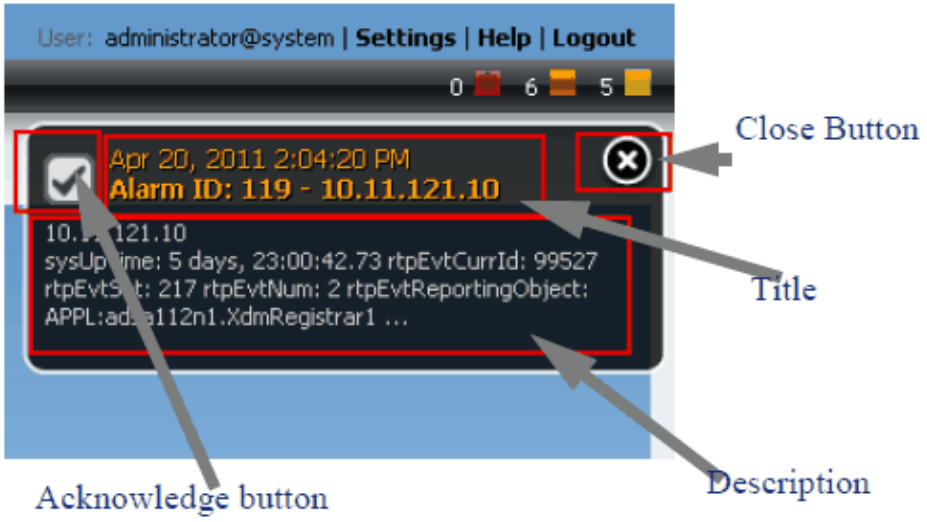
Depending on Administrator settings none, one, two or three Indicators may appear

Next to each alarm type, on the left, there is a number representing the Number of Alarms of the specific type remain at ‘Unacknowledged’ status. If there are no Alarms for a particular Severity, then number zero is displayed.

Each Alarm Indicator has two states (on, off) represented with different shades of the same color, respectively (normal, shaded).

When XXX new alarms (of the above three crucial types) arrive into CMP the following occur:

- The number of alarms next to the corresponding color increases by XXX
- The Corresponding Indicator color starts to Blink. After the 'Blink Period', the color for the Alarm is set to the ON state (normal).
- A Notification pane fades-in prompting the basic details of each alarm and stays in site for 2 seconds. Then it fades-out.



The Notification Pane has the following info:

1) **Acknowledge button**

   If this button is clicked the Alarm is marked as “Acknowledged” and changes its color to green.

   The Notification Pane is closed immediately

2) **Close Button**

   If this button is clicked the Notification Pane is immediately closed and the next notification appears (if there is any)

3) **Title**

   Title is composed from the **Time stamp, Alarm ID, Origin (IP address)**

   The Title is in the Color of the corresponding Severity

4) Description

Description is composed from the following Alarm attributes:

- Source Name (takes up to 2 lines),
- Description (takes up to 5 lines).

When text does not fit the space, three dots appear next to the end of the last line

---

NOTICE:

A bold line separates the Title from the Description. The Color of the Line corresponds to the Severity of the Alarm.

NOTICE:

When Hovering over the Description in the Notification Pane, the whole description text is marked as a link to the alarm details of the Active Alarm page

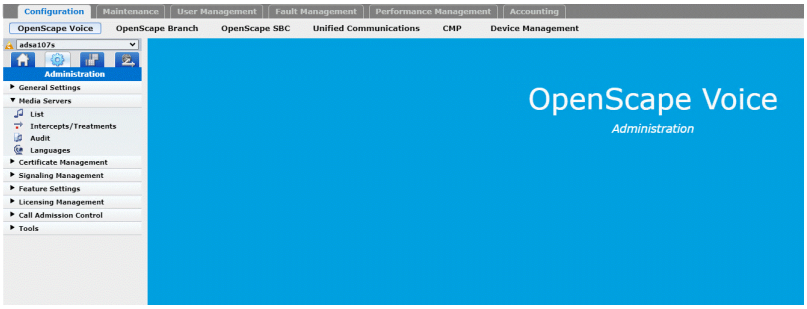
---

When you click one of the three numbers you will be directed to the Active Alarm page and a filter is applied to the Active Alarm List so you can see the unacknowledged Alarms of the severity you have clicked.

3.5 CMP Navigation Tree

For each navigation menu option the associated navigation tree opens next to the work area in the Common Management Platform. The tree contains all topics that belong to the selected navigation menu option.

If you click a navigation menu item, a navigation tree unfolds in the navigation area to the left; in the workspace, the home page for the selected navigation menu item is displayed. The navigation tree contains all entries associated with the current navigation menu item. Some individual entries are grouped and you can display or hide these groupings. The name of the navigation menu item is repeated once more at the top of the navigation tree. To hide the entries, click the "down arrow" icon in the group name. The entries disappear and a "right arrow" icon is displayed. Click the right arrow icon to display the entries again. When you click one of the displayed sub items, the associated page is displayed in the workspace .



3.6 CMP Work Area

The Common Management Platform work area lists comprehensive information and displays different activity options. The number and selection of information and activity items depends on the entry you have chosen in the navigation tree. The information area above each list displays a description of the information and actions.

The name of mandatory system settings are marked in bold text.

The work area contains the following general elements:

- Lists

  The work area displays the actual information about the entry selected in the navigation tree in the form of lists.

  You can sort the list elements in ascending or descending order.

  If a list cannot be completely displayed in the work area due to its length, it will extend over several pages.

  On pages that display a numerus amount of items you can customize the list according to your preference with the following options:

  1) “Sel”: the amount of items ticked in the checkbox. This option appears only if a checkbox is available in the list

  2) Items/Page: you can choose from the pull down menu the amount of (10,20,50,100,200) items displayed per page

  At the beginning of you Administrator user session all lists are initialized with the default value.

  Whenever you change the default items (rows) / page value (you have “customize” it) of a list in CMP this value is saved per Administrator User id, which means whenever you logoff and login CMP applies the value you have set for this list.

  You can preset the number of rows (items) /page for all the non “customized” lists and you can also force it to all lists, including “customized” lists as it is described in Section 3.2.2.1, “Settings”

  3) All: total amount of items in the list

  4) If the total amount of items exceeds the items/page value then you can use the page navigator. Use << and >> to page forward and back in the

list. Use |< and >| to jump to the beginning or end of the list. You can use the Page drop-down list to select a specific page

You have the option to sort the list entries by clicking the title in the column headings. For this to be done the column headings must be highlighted in blue.

If you click the column heading a second time, the sort sequence changes from ascending to descending or from descending to ascending.

If you wish to mark all list elements, click in the gray list header row on the checkbox at the start of the row.

NOTICE:

The sorting is for the entire list not just the page you are currently on

---

- General Icons / Buttons

  The general icons and buttons shown in the work area are dependent on the selection of the entry in the navigation tree. The icons/buttons shown below are possible and have the following meanings:

Elemen	Function
	Information icon Displays information about the topic represented in the work area in the information bar. A note also appears here when you enter the wrong value.
	Help icon Invokes the help for the topic concerned.
	Refresh icon Updates the page shown (forexample, when displaying list entries).

- Information bar

  The information bar describes which information is currently displayed in the work area. If you enter an invalid value in an entry field, the information bar will also indicate the type of input error. The relevant entry field appears in a red frame.

- Action Menu

  You can use the action menu to initiate specific functions for a list entry in a list (e. g. edit a user). The action menu appears always on the right-hand margin of a list entry. Whether an action menu is provided in a list or not depends on the list selected. Most of the functions in the action menu can also be reached with the buttons displayed in the work area. In instances where there are two ways of initiating a function, this manual describes the button procedure.

Elemen	Function
	Action Menu icon Opens the action menu for the associated list entry

- Filter

  You can use the filter function in the work area to filter displayed lists according to a specific search item. Setting a filter reduces the total number of items displayed and makes it easier to identify those desired.

  Within the search text only the wildcard * is allowed. It can be used instead of several arbitrary characters. Logical operators are not supported.

  Besides filtering by a specific search term, it is also possible to select certain items with a check mark. These marked items can then be displayed with **Show Selected ()**. If this selective display is no longer desired, all items can be displayed again with **Show All**.

  The filter function also supports the * wildcard search.

  An advanced filter in which additional criteria can be selected for filtering the lists is available for alarms, error messages and audit logs. The criteria for the advanced filter are described in the associated sections.
- Dialogs

  There are many work area elements that open additional dialogs in which you can set component-depending values. In these dialogs the names of the fields where entries are mandatory are bold.

3.6.1 Column Settings

This feature (available for OpenScape User Management) allows to customize the columns of the list according to the preferences.

Column Setting provides the following options:

- To set which columns will be visible/invisible in the list:

  1) check the box in front of the column(s) you want to appear/not appear in the list

  2) click **Show/Hide** button to confirm your selection.

  INFO:

  It is recommended to set maximum six (6) columns in the main list. More than six (6) might affect the displayed list.

- To set the order of the columns in the list

  1) check the box in front of the column you want to move

  2) in the row of a respective column, click on ‣ to open the application's action menu and then select **Move Up** / **Move Down**.
- To save the current setting

  1) click the **Save** button.
- To decline the current setting

  1) click the **Cancel** button.

The main list will contain only the columns that have been set as visible and in the order of your preference.

3.7 Search and Advanced Search Functionality

The Common Management Platform provides a powerful and flexible configurable Search and Advanced search functionality for quick, focused search and retrieval of specific information.

Search

Search functional helps reducing the search by specifying the search criteria. After applying this functionary, only those elements that match specified search category are displayed as the search result.

Advanced search

The **Advanced...** allows to refine the search even more, by specifying additional criteria in order to retrieve only those elements that match specified search conditions.

NOTICE: Simple and Advanced Search support the use of wildcards. By typing the "*" symbol in the <**Search for**> field and selecting an attribute from <**Attributes list**> you can filter out results that have empty values in the selected fields.

Usage of Common Management Platform Search and Advanced Search Functionality

The search and advanced search functionality offers the following options:

- **Search** (drop-down list)

  The **Search** drop-down list displays search categories matching the area in which you are currently located. Choose the search category to be used as selection criterion in the search process. After applying this search, only those elements that match the specified search category are displayed.
- **Search** (button)

  Click **Search** after selecting a search category from the drop-down list to apply the search.
- **Advanced...** (link)

  Click the **Advanced...** link to define your own advanced search by specifying additional criteria in order to retrieve only those elements that match the specified criteria.

  The **Advanced Search** dialog opens, displaying the search categories that match the area in which you are currently located.

  Navigate to Filter's Rules area and configure the criteria for the **Advanced Search**:

  – For fields that accept dates or numbers it is possible to specify a range.
  – For fields that accept specific values, a drop-down list lets you select the available ones.
  – For fields that accept arbitrary text you can use wildcards (e.g. "a*" for listing all the ones that begin with an "a").

- **Advanced Search** / **Add** (button)

  Navigate to Filter's Rules area and click **Add** button to store the search criteria in the list.
- **Advanced Search** / **Delete** (button)

  Navigate to Filter's Rules area and click **Delete** to discard the search criteria settings.
- **Advanced Search** / **Search** (button)

  Click **Search** button to perform the search and show the result on the main screen.
- **Advanced Search** / **Close** (button)

  Clicking the **Close** button will close the **Advanced Search** dialog without saving the data entered.
- **Advanced Search** / **Load** (button)

  Navigate to Stored Filters area and click **Load** to manage the already stored filters.
- **Advanced Search** / **Save as** (button)

  Navigate to Stored Filters area and click **Save as** to save a new filter.
- **Advanced Search** / **Save** (button)

  Navigate to Stored Filters area and click **Save** to update an already stored filter which is loaded.

3.7.1 How to Save an Advanced Filter

How to save an advanced filter:

Prerequisites

Adequate administrative permissions

Step by Step

1) After selecting the desired criteria in the **Advanced Search** menu click on **Save as** button.

A pop-up window **Save Advanced Filter As** is displayed.

2) Enter the name of the filter in the **Filter Name** field and a short description in the **Description** field.

NOTICE:

The **Filter Name** field is mandatory and an already existing filter name cannot be given.

---

3) Select **Save** to confirm your entries.

3.7.2 How to Manage an Advanced Filter

How to manage a stored advanced filter:

Prerequisites

Adequate administrative permissions

Step by Step

1) At the **Advanced Search** menu click on **Load** button.

A pop-up window **Select Advanced Filter** is displayed with all the saved filters.

2) Click on **Show All** to see all the available stored filters or **click on Search** to perform search operation using the following rule:

`Search for:` <**User input**> `in` <**Attributes list**>.

a) <**Attribute list**> contains the following items:

Filter Name, Filter Owner and Description.

A list of the available advanced filters is displayed.

3) Select the desired filter(s) and click on **Load** to add it on the **Advanced Search** menu or on **Delete** to delete them.

NOTICE:

Only one filter can be loaded per time.

NOTICE: A filter currently loaded cannot be deleted.

---

4 System Management

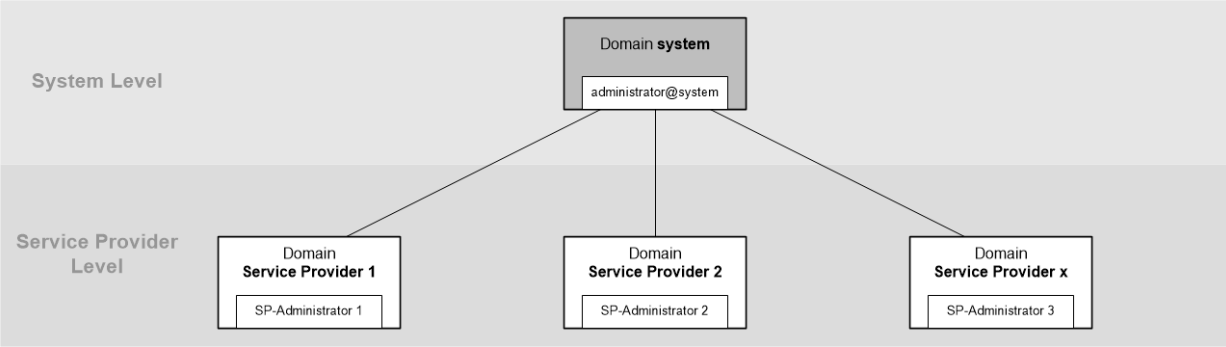
4.1 Domain Management

With the domain management you can divide the OpenScape system into different domains. The system can be split into domains, where each domain corresponds to a separate administration area with independent administration rights.

NOTICE:

OpenScape Voice can currently only be operated with one domain– the predefined system domain **system**. To organize the access rights of OpenScape Voice subscribers you can use access control lists.

The following figure describes the domain concept.



The domain concept divides into the following levels.

- System level

  On the system level exists the defaulted domain **system** with the default administrator **administrator@system**. This defaulted administrator can configure service provider domains and define further administrators and service provider administrators. You cannot delete the **system** domain.
- Service Provider Level

  On the service provider level exist service provider domains that can be created by the administrators of the system level. When an administrator creates a new service provider domain, he/she also becomes service provider administrator of the new service provider domain by default and is thus a foreign user for this domain. If an individual administrator is configured for the new service provider domain, he/she can withdraw the administrator privileges for the relevant service provider domain from the foreign user.

  A service provider administrator can define further administrators on the service provider level.

Domains can only be added, edited and deleted by administrators who have the **Domain Management** privilege.

4.1.1 How to Add a Domain

How to add a domain:

Prerequisites

Adequate administrative permissions

IMPORTANT:

OpenScape Voice can currently be operated with only one domain– the predefined system domain **system**.

NOTICE:

If an administrator creates a new domain, other logged-in administrators do not see this modification until they log off and back on again in the Common Management Platform.

Step by Step

1) On the **Configuration** navigation tab, click on the **CMP** navigation menu item.

2) Click on **Domains** from the Navigation Tree.
A list of domains appears in the work area, showing the domains for which you have the **Domain Management** privilege.

3) Click on **Add** to add a new service provider domain.
The dialog for adding a new domain opens.

4) Under **Parent domain** select the domain under which you want to hierarchically add the new domain.

5) Under **Domain name**, enter a short, unique name for the new domain.
Under this name the domain will later be administered in the Common Management Platform.

6) Under **Domain description** enter a description for the new domain.

7) Enter the value for the **Default Ring-No-Answer (RNA) timeout (sec)**
This is the RNA value that is applied to all devices of the domain.
Valid range is between 0 and 60 (seconds).
Default value is 12 seconds.

8) Enter the value for the **Default Workgroup purge time (days)**
Workgroups that are not longer being used can be periodically deleted by the system after the amount of days defined in this field.
Valid range is between 0 and 60 (days).
Default value is 0 indicating that no criteria is applied for purging workgroups.

9) Select the **Create administrator account for the domain** option if you would like to create an individual administrator account for this domain. Administrator of the new domain will otherwise be the administrator who has created the domain by default.

10) If you have activated the **Create administrator account for the domain** option, the **Administrator Login Name**, **Administrator password** and **Administrator password (confirm)** settings become active. Then enter the values for these settings.
11) Click on **Save** to copy the entries to the system's database.

NOTICE:

The following special characters must not be used for the **Domain name** and **Administrator Login Name**:

" > " (Greater-than sign)

" < " (Less-than sign)

" / " (Backslash).

The new domain is saved and displayed in the domain list.

4.1.2 How to Edit Domain Settings

How to edit domain settings:

Prerequisites

Adequate administrative permissions

Step by Step

1) On the **Configuration** navigation tab, click on the **CMP** navigation menu item.
2) Click on **Domains** from the Navigation Tree.
   A list of domains appears in the work area, showing the domains for which you have the **Domain Management** privilege.
3) Click on the path of the domain the settings of which you want to modify.
   The dialog with the settings of the relevant domain opens.
4) Edit the desired settings of the selected domain.
5) Click on **Save** to copy the entries to the system's database.

4.1.3 How to Delete a Domain

How to delete a domain:

Prerequisites

Adequate administrative permissions

IMPORTANT:

When you delete a domain, you also delete all users, resources and profiles associated to the relevant domain.

NOTICE:

If an administrator deletes a domain, other logged-in administrators do not see this modification until they log off and back on again in the Common Management Platform.

Step by Step

1) On the **Configuration** navigation tab, click on the **CMP** navigation menu item.
2) Click on **Domains** from the Navigation Tree.
   A list of domains appears in the work area, showing the domains for which you have the **Domain Management** privilege.
3) Select the checkboxes of the schedules that you want to delete.

NOTICE:

You cannot delete the defaulted **System** domain.

4) Click on **Delete**.
5) Click on **OK** to confirm the deletion of the selected domains.

The selected domains are removed from the system's database and from the list of all domains.

4.2 Management Concept of CMP Administrator User

The administrator accounts are managed in the Common Management Platform with the help of the domain management, user profile management.

Besides the CMP Administrator users of the selected domain, it is also possible to create foreign users. These foreign users are external users or administrators from another domain who are to receive specific rights in the selected domain. You can assign profiles from the selected domain to them for this purpose. Profiles from other domains cannot be assigned. It is not possible to assign resources to foreign users.

4.2.1 How to Display/Edit a CMP/UM Locality Administrator User

How to display or edit CMP/UM Locality administrator User:

Prerequisites

1) The Admin User has successfully logged-in CMP.
2) The Admin User's 's permission level allows the creation of CMP/UM Locality Admin Users.
3) The account “administrator@system” exists, allowing the initial configuration of the CMP/UM Locality Admin Users.
4) Default Profile “CMP Login” has been defined. This profile allows a CMP Admin User to login to CMP.
5) The Admin User has an "Symphonia Administrator" permission Profile

Step by Step

1) On the **Configuration** navigation tab, click on the **CMP** navigation menu item.
2) In the navigation tree, click on **General / Administrators** > **List**.

   A list of all CMP/UM Locality Administrator Users within selected domain appears in the work area.

   The following attributes of the CMP/UM Locality Admin Users are listed:

Attribute	Sort	Comments
Login Name	supported	
Display Name	supported	
Last Login	not supported	Last successful login date
Failed Attempts	not supported	Number of unsuccessful login attempts since the last login
Locked	yes	An indicator of the status of the CMP Admin User account

   The list is initially sorted ascending using the first column.

   You can sort the list by any displayed column that supports sorting.

3) The list can be filtered according to specific terms (patterns).

a) Enter the desired filter term in the field **Search for:**. You can either enter the complete term or the initial letters followed by *.

b) From the list displayed, select whether the filtering is to be applied to the **Login Name** or **Display Name** column.

c) Select whether the filtering according to Status is to be applied for **Any Status, Locked**, **Unlocked** or **Inactive**.

NOTICE:

Inactive administrators shown in this list, will be locked upon their next login attempt.

NOTICE:

The CMP "administrator@system" or/and any custom created CMP user may be locked due to inactivity after 90 days.

If CMP "administrator@system" user goes to “inactive” / "locked" state, please follow steps described at section "Special Handling of CMP Administrator Permission"

If any custom CMP user goes to "inactive" / "locked"state ,then login as "administrator@system" and go to **Configuration>CMP>Administrators>List**

Edit the custom CMP user and check/uncheck the option "User locked".

The custom CMP user wil be set to "active" / "unlocked" state again and one will be able to login with its credentials.

If needed, one may reset to him also a new password from the same form.

---

d) Click on **Search** to activate the filter. Only the list elements which correspond to the pattern entered are displayed.

e) Click on **Show all** to deactivate the filter. Filter conditions are deleted. All the list elements are displayed again.

4) Select the CMP/UM Locality Administrator User by clicking the check box and click on **Edit**

- If the chosen CMP/UM Locality Administrator User Account is disabled after too many unsuccessful login attempts then following message appears above the Login information area:
  "This CMP Admin User cannot currently login due to too many unsuccessful login attempts. In order

to re-enable this account please re-set the user’s password."

The list contains, for the Selected CMP/UM Locality Administrator User, the following atributes:

- **Login Name (read only)**

  Login Name can’t be edited.
- **Domain (read only)**

  Domain can’t be edited.
- **User Locked**

  Locks the Admin User for the CMP.

  NOTICE:

  CAC

  This attribute is used in order to provide CMP the possibility to know which users are setup to login with CAC login method or not and to provide a specific behavior for CAC login users. When enabled, the user will be able to login to CMP only via the "CAC Login" button using the CAC login method to CMP and will not be able to login to CMP via its credentials. This specific behavior provides an emergency account that must be available during CAC login method to CMP. Please see related info for CAC login method to CMP section "CAC (Common Access Card) Login Method to CMP".

- **Domain (Single Sign on)**

  this attribute can take the following values: **Disabled**, **<external Systems that have been configured in krb.conf>** or **LDAP Attribute**.
- **Username (Single Sign on)**

  Mandatory field when a domain is selected.

  NOTICE:

  If SPNEGO/SOAP SSO is not configured the SSO section is not displayed.

- **Last Name (mandatory)**

  Last Name of the Admin User

  NOTICE:

  After an upgrade the CMP/UM Locality Administrator account that comes from a previous version might

have the last name field empty. System fills in the field "Lastname" with the contents of the field "Login Name"

- **First Name**

  First Name of the Admin User
- **Display Name**

  If no value is entered in this field the System fills it in using the form "LastName FirstName".
- **Set new password**

  If you set this checkbox new password must be entered
- **Login Password (mandatory)**

  Filed is "read only" unless new password field is set
- **Login Password (confirm)**

  Filed is "read only" unless new password field is set
- **Comments**
- **Login password never expires**

  Field is "read only" unless new password field is set

  Activate this checkbox if the password is not to expire after a certain interval. If you activate this option, the system-spanning password policy MaximumAge is suspended for an unlimited period for the relevant user.
- **User has to change password at next login**

  Field is "read only" unless new password field is set

  Activate this checkbox if the user is to change the password at the next login.This option is only valid until the next password-based login of the relevant user. After this user login this option is deactivated again for the relevant user.
-

  NOTICE: If the Login password never expires and User has to change login password at next login options are active at the same time, the user needs to change his/her password at the next login. The changed password is then infinitely valid
- **e-mail address**
- **Home time zone** (**mandatory**)

  Home time zone of the Admin User.
- **Default locale** (**mandatory**)

  Language of the Admin User

5) Click on the **Profiles** tab in case of CMP Administrator User or on the **Localities** tab in case of UM Locality Administrator User.

- For CMP Administrator User:
  - A list of all Administrator Profiles assigned to this Admin User is displayed.
  - **NOTICE:** Profile “CMP Login” cannot be removed.
  - The **Assign** button allows you to Select Administrator profile(s) to be assigned to CMP administrator user.
  - To remove Profiles from the CMP Admin User, choose them from the Profile list and click the **Unassign** tab.
  - You can check the licenses assigned to the administrator user by clicking on the **Show bound licenses** button

    Administrator users obtain licenses when they are assigned a profile containing the relevant features. If no licenses are available the list is empty.
  - **NOTICE:**

    Detailed information on profiles can be found in relevant chapter “Managing Profiles” of this document.
- For UM Locality Administrator User:
  - A list of all Administrator Localities assigned to this Admin User is displayed.
  - The **Assign** button allows you to Select Administrator localities to be assigned to UM Locality administrator user. Click on the drop down menu to see the available localities which can be assigned.
  - To remove Localities from the UM Locality Admin User, choose them from the Locality list and click the **Unassign** tab.
  - **NOTICE:**

    Detailed information on localities can be found in relevant chapter “Localities” of this document.

6) Click on the **External IDs** tab to list all the External Identifiers of the CMP/ UM Locality administrator, 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 CMP/UM Locality Administrator External Identifiers* " chapter.

7) Click on **Save** to copy the entries to the system's database.

a)

b)

NOTICE:

If an error occurs during the creation of the CMP/UM Locality Admin User related information is displayed.

System assigns the specified Profiles to the new CMP Admin User or the specified Localities to the new UM Locality Admin User.

NOTICE:

If no localities have been assigned to an UM Locality Administrator system displays a warning message.

c)

The CMP/UM Locality Admin User has been edited successfully and has been assigned the specified Profiles/Localities.

4.2.2 How to Create a CMP/UM Locality Administrator User

Prerequisites

1) The Admin User has successfully logged-in CMP.
2) The Admin User's 's permission level allows the creation of CMP/UM Locality Admin Users.
3) The account "administrator@system" exists, allowing the initial configuration of the CMP/UM Locality Admin Users.
4) Default Profile “CMP Login” has been defined. This profile allows a CMP Admin User to login to CMP.
5) The Admin User has an "Symphonia Administrator" permission Profile

Step by Step

1) On the **Configuration** navigation tab, click on the **CMP** navigation menu item.
2) In the navigation tree, click on **General / Administrators** > **List**.

   A list of all Administrator Users within selected domain appears in the work area.
3) Select from the drop down menu if you want to create a CMP or a UM Locality Administrator user.
4) Click **Add** to add a new administrator User.

   The Admin User settings dialog opens.

5) On the **General** tab, you can enter the following data:

- **Login Name (mandatory)**

  User ID of the user. This name is used for logging on to the system.The following special characters must not be used for the login name:

  – " @ " (At sign)
  – " < " (Less-than sign)
  – " > " (Greater-than sign)
  – " / " (Backslash)
  – " ; " (Semicolon)
  – Blank at the beginning or end of a login name.

  NOTICE: If the "Login name" is already used by another CMP/UM Locality Admin User the System prompts you to enter a different Login name.

  If the "Login Name" is already used by another, non administrative account (e.g. UM, UC User) then the System prompts you to choose between the following actions:

  a) If you proceed and create this CMP/UM Locality Administrator User then the attributes you filled in for the CMP/UM Locality Administrator will overwrite the corresponding attributes of the existing account. If you have left an attribute of the CMP/UM Locality Administrator

empty, the corresponding attribute of the existing account will not be overwritten.

The specified CMP/UM Locality Administrator password will overwrite the UC or UM resource password of the existing account (where applicable).

b) If you don't wish to proceed, please select another "Login name" for the CMP/UM Locality Administrator.

- **Domain (read only)**
- **User Locked**

  Locks the Admin User for the CMP.
- **Domain (Single Sign on)**

  this attribute can take the following values: **Disabled**, **<external Systems that have been configured in krb.conf>** or **LDAP Attribute**.
- **Username (Single Sign on)**

  Mandatory field when a domain is selected.

  NOTICE:

  If SPNEGO/SOAP SSO is not configured the SSO section is not displayed:

- **Last Name (mandatory)**

  Last Name of the Admin User
- **First Name**

  First Name of the Admin User
- **Display Name**

  If no value is entered in this field the System fills it in using the form "LastName FirstName".
- **Comments**
- **Login Password (mandatory)**
- **Login Password (confirm)**
- **Login password never expires**

  Activate this checkbox if the password is not to expire after a certaininterval.If you activate this option, the system-spanning password policyMaximumAge is suspended for an unlimited period for the relevant user.
- **User has to change password at next login**

  Activate this checkbox if the user is to change the password at the next login.This option is only valid until the next password-based login of the relevant user. After this user login this option is deactivated again for the relevant user.
-

  NOTICE: If the Login password never expires and User has to change login password at next login options are active at the same time, the user needs to change his/her

password at the next login. The changed password is then infinitely valid

- **e-mail address**
- **Home time zone**

  Home time zone of the user.
- **Default Language**

  Language of the Admin User

6) Click on the **Profiles** tab in case of CMP Administrator User or on the **Localities** tab in case of UM Locality Administrator User.

- For CMP Administrator User:
  - A list of all Administrator Profiles assigned to this Admin User is displayed.
  - **NOTICE:** System automatically assigns the Profile “CMP Login” to every CMP Admin User. This Profile cannot be removed
  - The **Assign** tab allows you to Select Administrator profile(s) to be assigned to CMP administrator user.
  - To remove Profiles from the CMP Admin User, choose them form the Profile list and click the **Unassign** tab.
- For UM Locality Administrator User:
  - A list of all Administrator Localities assigned to this Admin User is displayed.
  - The **Assign** tab allows you to Select Administrator localities to be assigned to UM Locality administrator user. Click on the drop down menu to see the available localities which can be assigned.
  - To remove Localities from the UM Locality Admin User, choose them form the Profile list and click the **Unassign** tab.
  - **NOTICE:**

    System automatically assigns to the account two new CMP profiles in order to group the subset of the CMP/

OSV permission that are needed to allow them to perform the following operations:

– The set of CMP permissions:

  -) manage Users & Resources

  -) view Localities

  -) view User Templates

  -) In addition, it shall be allowed to access to EM specific resource configuration screens from the User's resources list:

  4K Manager/Assistant edit 4K station

  Xpressions edit resource

  UC edit resource

– The set of the OSV Assistant permission shall allow the administrator to:

  -) create/modify/delete subscribers

---

7) **External IDs** tab can be edited only after the new administrator User is saved.

8) Click on **Save** to copy the entries to the system's database.

a)

b)

c) System creates the new CMP/UM Locality Admin User with all required attributes.

d)

NOTICE:

If an error occurs during the creation of the CMP/UM Locality Admin User related information is displayed.

The specified Profiles are assigned to the new CMP Admin User.

The specified Localities are assigned to the new UM Locality Admin User.

NOTICE:

If no localities have been assigned to the UM Locality Administrator system creates the UM Locality Admin User but displays a warning message.

---

e) The new CMP/UM Locality Admin User has been created successfully.

4.2.3 How to Delete a CMP/UM Locality Administrator User

How to delete a CMP/UM Locality Administrator User:

Prerequisites

1) The Admin User has successfully logged-in in CMP.

2) The Admin User's 's permission level allows the deletion of CMP/UM Locality Admin Users.

3) The account "administrator@system" exists, allowing the initial configuration of the CMP/UM Locality Admin Users.
4) Default Profile “CMP Login” has been defined. This profile allows a CMP Admin User to login to CMP.
5) The Admin User has an "Symphonia Administrator" permission Profile

Step by Step

1) On the **Configuration** navigation tab, click on the **CMP** navigation menu item.
2) In the navigation tree, click on **General / Administrators** > **List**.

   A list of all Administrator Users within selected domain appears in the work area.
3) Select the checkboxes of the Administrator Users that you want to **Delete**
4) Click **Delete** to delete the selected Administrator User/s.
5) Click **OK** to confirm the deletion of the selected users.

NOTICE:

If a selected CMP Administrator User is assigned additional non-Administrator Profiles (e.g. UM or UC Profiles) only the Administrator Profiles are removed from the CMP Admin User.

NOTICE:

If an error occurs during the deletion of the CMP/UM Locality Admin User related information is displayed.

The selected CMP/UM Locality Administrator Users are successfully deleted.

4.2.4 Policy for User Passwords

You can define system-spanning requirements, CMP administrator and/or UC user passwords have to satisfy.

IMPORTANT:

The password policy is applied per Server, so if the UC application and CMP are located on the same server they will have the same password policy

---

To comply with the default requirements a CMP administrator and/or UC 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. It is possible to disable this feature if needed by setting the "PeriodOfInactivity" parameter to value 0.

  NOTICE: This system-spanning setting can be disabled for the respective UC user. If this is desired, activate the **Telephony PIN never expires** option on the **Password / PIN** tab of the relevant UC user settings.

- A CMP administrator and/or UC 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 UC user via telephone.
- The last five passwords of a CMP administrator and/or UC user are stored in a password history. An CMP administrator and/or UC 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 CMP server:

For Standard Duplex under: `/opt/siemens/common/conf/` For Integrated Simplex `/enterprise/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>7776000000</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>
    <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**

  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 **Telephony PIN 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.

- **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.
- **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 a threshold value for considering a user inactive in number of days. Default value is 90 days. If you set value 0 this policy is not used.
- **MinimumChangedCharacters**

  Specifies the number of characters a new user password must at least change compared to the previous one.

4.2.5 How To Change Policy for User Passwords

How to change Password policy for User Passwords:

Prerequisites

Adequate administrative permissions

Step by Step

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 CMP.

`/opt/siemens/common/conf/` (Standard Duplex Small)

`/enterprise/common/conf/` (Integrated Simplex)

IMPORTANT:

The password policy is applied per Server, so if the UC application and CMP are located on the same server they will have the same password policy

---

2) Adjust the desired settings in the following file section.

```
<PassphrasePolicy>
   <Type>pwd</Type>
   <MinimumAge>86400000</MinimumAge>
   <MaximumAge>7776000000</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>
   <LockoutTime>1800000</LockoutTime>
</PassphrasePolicy>
```

3) On the **Maintenance** navigation tab, click on the **Inventory** navigation menu item.

4) In the navigation tree, click on **Nodes&Applications** > **Nodes**.

A list of all system nodes and 3rd party node connections available in the entire system is displayed in the workspace.

5) Save the changes in the configuration file.

6) Click on the name of the system node on which CMP is installed.
A dialog box 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 checkbox of the component.

NOTICE:

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**.

The changed password policy is now effective.

4.2.6 How to Display/Edit Foreign Users

How to display or edit a foreign user:

Prerequisites

1) The Admin User has successfully logged-in in CMP.
2) The Admin User's 's permission level allows the creation of the Foreign User.

Step by Step

1) On the Configuration navigation tab, click on the CMP navigation menu item.
2) In the navigation tree, click on **General** > **Administrators** > **Foreign**

   A list of all Administrator Users within selected domain appears in the work area.A list of all foreign users in the selected domain appears in the workspace. This list contains for each entry the following information:

   Login name User ID of the user. This name is used for logging on to the system.
   Name of the user.
3) Click on the login name of the desired user.

   The dialog with the settings of the relevant user opens.
4) On the **General** tab, you can change the following data:
   - **Login name** User ID of the user. This name is used for logging on to the system.
   - **Domain** The domain in which the user is created.
5) Click OK to confirm the deletion of the selected users.
6) On the Profiles tab you can assign profiles to the user and display the licenses assigned to the profiles. In the Assigned to user column, select the checkboxes of the profiles that you would like to assign to the user
7) You can check the licenses assigned to the user with Show bound licenses. Users obtain licenses when they are assigned a profile containing the relevant features. If no licenses are available the button is inactive.

   Licenses from other domains cannot be checked.
8) Click on Save to copy the settings

Example

NOTICE:

CMP can currently only be operated with one domain– the predefined system domain system. Therefore, no foreign users are currently supported.

4.2.7 How to Add Foreign Users

How to add a foreign user to a domain:

Prerequisites

1) The Admin User has successfully logged-in in **CMP**.
2) The Admin User's 's permission level allows the creation of the Foreign User.
3) Before you can add a foreign user to a domain, this user must have been created in his/her home domain.

Step by Step

1) On the Configuration navigation tab, click on the **CMP** navigation menu item.
2) In the navigation tree, click on **General** > **Administrators** > **Foreign**

.A list of all Administrator Users within selected domain appears in the work area.A list of all foreign users in the selected domain appears in the workspace. This list contains for each entry the following information:

Login name User ID of the user. This name is used for logging on to the system.
Name of the user.

3) Click on **Add**.

The user settings dialog opens.

4) On the **General** tab, you can enter the following data:

- **Login name** User ID of the user. This name is used for logging on to the system.
- **Domain** The domain in which the user is created.

5) Click **OK** to confirm the deletion of the selected users.
6) On the **Profiles** tab you can assign profiles to the user and display the licenses assigned to the profiles. In the Assigned to user column, select the checkboxes of the profiles that you would like to assign to the user
7) You can check the licenses assigned to the user with **Show bound licenses**. Users obtain licenses when they are assigned a profile containing the relevant features. If no licenses are available the button is inactive.

Licenses from other domains cannot be checked.

8) Click on **Save** to copy the settings

NOTICE:

NOTICE:

CMP can currently only be operated with one domain– the predefined system domain **system**. Therefore, no foreign users are currently supported.

4.2.8 How to Delete Foreign Users

When you delete a foreign user in a domain, this user will be removed from the selected domain only. In his/her home domain the user will still be present.How to remove a foreign user from a domain:

Prerequisites

1) The Admin User has successfully logged-in in **CMP**.
2) The Admin User's 's permission level allows the creation of the Foreign User.
3) Before you can add a foreign user to a domain, this user must have been created in his/her home domain.

Step by Step

1) On the Configuration navigation tab, click on the **CMP** navigation menu item.
2) In the navigation tree, click on **General** > **Administrators** > **Foreign**

   .A list of all foreign users in the selected domain appears in the workspace.
3) Select the checkboxes of the foreign users that you want to delete.

   The user settings dialog opens.
4) Click on **Delete**.
5) Click **OK** to confirm the deletion of the selected users.

   The selected foreign users will be removed from the selected domain

4.2.9 How to Display/Terminate Active Sessions

How to display and terminate the Administrator Active Sessinons:

Prerequisites

1) The Admin User has successfully logged-in in CMP.
2) The Admin User's 's permission level allows the termination of an Active Session.

Step by Step

1) On the **Configuration** navigation tab, click on the **CMP** navigation menu item.

2) In the navigation tree, click on **General** > **Administrators** > **Active Sessions**.

   A list of all Active Sessions is displayed with the following attributes:.

   - **Login Name**
   - **Data**

     Data and Time the session started
   - **IP Address**

     IP Address of Administrator who activated the session

3) Click on the action menu button and **Terminate** the chosen session. .

   a)

4.2.10 How to Configure CMP Alarm Indicator / Preferences

The three critical Alarm Indicators that appear on the CMP Navigation Bar are configured in the following way:

Prerequisites

1) The Admin User has successfully logged-in in CMP.
2) Default Profile “CMP Login” has been defined. This profile allows a CMP Admin User to login to CMP.
3) The Admin User has an "Symphonia Administrator" permission Profile.
4) The Admin User has a CMP permission Profile to access the Alarm Indicator page.

Step by Step

1) On the **Configuration** navigation tab, click on the **CMP** navigation menu item.
2) In the navigation tree, click on **General** > **Alarm Indicator**.

   A pop -up Window allows you to configure the Alarm Preferences
3) For each Alarm Severity you can choose one of the three options in the drop-down menu

   - Hide alarm indicator
   - Show alarm indicator
   - Show alarm indicator and pop-up notifications

   NOTICE: The default selection is "Show alarm indicator and pop-up notifications"

4) The field **Browser updates alarm indicator every:** expects a value in seconds

   NOTICE: The default value for this filed is 5 seconds and the maximum value is 999 seconds"

5) The chek box field **Blink with new incoming alarm for:** expects a value in seconds

> **NOTICE:** The default state is checked and the default value for this field is 4 seconds and the maximum value is 99 seconds"

6) Click on **Save** to enter the configuration in the system's database.

4.2.11 How to Define the System settings

You can set the time for the automatic logoff, disable check for unassigned Unified Communications accounts at startup and Use Domain to Business Group Mapping:

Prerequisites

1) The Admin User has successfully logged-in in CMP.
2) The Admin User's 's permission level allows the definition of the System settings

Step by Step

1) On the **Configuration** navigation tab, click on the **CMP** navigation menu item.
2) In the navigation tree, click on **General** > **System Settings**.
   The dialog with the administrator settings opens.
3) In the **Auto Log Off time out value** field specify the time in minutes after which you are automatically logged out of the system if you remain inactive in the Common Management Platform

> **NOTICE:** If you are inactive in the Common Management Platform for the time set, the system will automatically log you off for security reasons. To continue working in the Common Management Platform you need to log back in again.

4) When User Management is deployed in your system you can tick the box “Disable check for unassigned Unified Communications accounts at startup” if you want to disable this check when you login.

> **NOTICE:**
>
> If User Management is deployed in your system then at login Common Management Platform detects if any Unified Communications accounts have pending assignment to Users. In order to take advantage of the advanced User Management features of CMP, it is required to have each UC resources assigned to a User and this check is performed

upon login and the Administrator User is prompted with a pop up window.

You can trigger manually the automatic creation of Users from Unified Communications accounts by navigating to **User Management** > **Provisioning** > **Users from UC Accounts**.

5) Tick the box “Use Domain to Business Group Mapping” if you want to allow this mapping

NOTICE:

When the option above is enabled, system will restrict each CMP domain to access the data of the mapped Business Group only. The Domain to Business Group mapping is defined in the Openscape Voice Business Group page.

You may navigate **Configuration** > **OpenScape Voice** > **Business Group** > **Business Group List** > **Add or Edit** the BG you want to map.

Click on the **General** tab and choose in the Domain field the domain you want to asign to this Business Group

6) Click on **Save** to confirm your entries.

NOTICE: Every CMP Administrator can define his own timeout setting.

4.2.12 How to Add Proxy Server

The proxy server is required only if CMP is configured to exchange data over external networks.

Prerequisites

1) The Admin User has successfully logged-in in CMP.
2) The Admin User's 's permission level allows the creation of Proxy Server.

Step by Step

1) On the **Configuration** navigation tab, click on the **CMP** navigation menu item.
2) In the navigation tree, click on **General / Proxy Servers**.
   A list of proxies already configured is displayed.
3) Click **Add** to configure a new Proxy Server.

4) The following parameters for a proxy server can be configured:

- **Name (mandatory)**

  Name of the proxy serverUser ID of the user. :
- **Type**

  Select betweeen HTTP or SOCKS
- **Host (mandatory)**

  Specify the IP address of your proxy server.
- **Port (mandatory)**

  Specify the used port (e.g. port 80 for HTTP)
- **Use authentication**

  If the proxy needs authentication, mark this checkbox and specify the appropriate User name and Password.

5) Click on **Save**.

   a) The proxy is saved successfully .

4.2.13 How to Display / Edit Proxy Server

The proxy server is required only if CMP is configured to exchange data over external networks.

Prerequisites

1) The Admin User has successfully logged-in in CMP.
2) The Admin User's 's permission level allows the editing of Proxy Server.

Step by Step

1) On the **Configuration** navigation tab, click on the **CMP** navigation menu item.
2) In the navigation tree, click on **General / Proxy Servers**.
   A list of proxies already configured is displayed.
3) Select a proxy from list and click **Edit**
4) The following parameters for a proxy server can be configured:

- **Name (mandatory)**

  Name of the proxy serverUser ID of the user. :
- **Type**

  Select betweeen HTTP or SOCKS
- **Host (mandatory)**

  Specify the IP address of your proxy server.
- **Port (mandatory)**

  Specify the used port (e.g. port 80 for HTTP)
- **Use authentication**

  If the proxy needs authentication, mark this checkbox and specify the appropriate User name and Password.

5) Click on **Save**.

   a) The proxy is saved successfully .

4.2.14 How to Delete a Proxy Server

How to delete a Proxy server:

Prerequisites

1) The Admin User has successfully logged-in in CMP.
2) The Admin User's 's permission level allows the removal of a Proxy Server.

Step by Step

1) On the **Configuration** navigation tab, click on the **CMP** navigation menu item.
2) In the navigation tree, click on **General / Proxy Servers**.
   A list of proxies already configured is displayed.
3) Select a proxy from list and click **Delete** to remove the Proxy Server.

   The Proxy is removed succesfully.

4.2.15 How to Configure the SMTP (Simple Mail Transfer Protocol) server

You can configure an SMTP server that will be used by CMP whenever it is required to send e-mail (e.g. notification e-mails):

Prerequisites

1) The Admin User has successfully logged-in in CMP.
2) You have the Host or IP Address of the SMTP server to be used
3) The Admin User's 's permission level allows the configuration of **SMTP Server**

Step by Step

1) On the **Configuration** navigation tab, click on the **CMP** navigation menu item.
2) In the navigation tree, click on **General** > **SMTP Server**.
   The dialog with the **SMTP server** opens.
3) Tick the box **Enable** to activate the SMTP functionality.

NOTICE:

Whenever CMP is requested to send e-mails the System informs the Administrator User if the functionality of the *SMTP server* is enabled or disabled.

---

4) Configure the **SMTP Server** and enter values in the following fields:

   Host Address: Entrer the IP Addressor the Host Name of the SMTP server

   Port Number: Enter the Port Number of the SMTP Server (default value is 25)

5) Tick the **Authentication Required** box if you wanrt activate the **User Name, Password** fields and the SSL box.
   a) Enter a **User Name** for the SMTP server
   b) Enter a **Password** for the SMTP Server
   c) Tick the box if you want to activate the **SSL** option

6) Click on **Save** to confirm your entries.

4.2.16 How to Configure CMP/UM Locality Administrator External Identifiers

Prerequisites

Adequate administrative permissions

The CMP/UM Locality administrator account must already exist

Step by Step

1) On the **Configuration** navigation tab, click on the **CMP** navigation menu item.
2) In the navigation tree, click on **General / Administrators** > **List**.

   A list of all Administrator Users within selected domain appears in the work area.
3) Select the CMP/UM Locality Administrator User by clicking the check box and click on **Edit**.
4) Click on the **External IDs** tab.
5) A Database View with a list of all the CMP 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**

6) Click on the **Add** or **Edit** button to add a new or edit an existing External ID

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.

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 on **Save** to copy the entries to the system's database.

4.2.17 How to Configure Unify Phone Servers

Unify Phone Servers configuration allows you to use an API Key for the provisioning of Unify Phone users. This is a required action prior to creating a Unify Phone resource for UM users.

Prerequisites

Adequate administrative permissions

For an overview of the Unify Phone app, refer to Unify Phone V3 Administration.

Step by Step

1) On the **Configuration** navigation tab, click on the **CMP** navigation menu item.
2) In the navigation tree, click on **General** > **Unify Phone servers**.

   A list of all Unify Phone tenants appears in the work area.

   For each tenant, the following information is displayed:

   - **Tenant name**
   - **Url**
   - **Proxy**

3) Click **Add**.

   A **Unify Phone server** window pops up.
4) In the **Tenant name** text field, enter the tenant's name.
5) (Optional) In the **URL** text field, enter the URL of the page from which you retrieve the API key.

   The default value is `https://phoneapp.unify.com`

6) Click **Retrieve API key...** to navigate to the Unify Phone Administration environment where you can retrieve the API key.

   NOTICE: If you entered a custom URL in the **URL** field, the **Retrieve API Key...** directs you to that URL. Otherwise, it directs you to the default Unify Phone Server site.

   a) Log in to the Unify Phone Administration environment.
   b) In the navigation panel, click on **Telephony connector**.

      A new page appears containing **Telephony status** information and an **API key** field.
   c) Click on **Copy to Clipboard** under the **API key** area.
7) Navigate back to the **Unify Phone server** window and paste the API key into the **API key** field.
8) From the **Proxy** drop-down menu, select a proxy that is configured for Unify Phone.

   You can see more information on how to add a proxy server in CMP in How to Add Proxy Server on page 64.
9) Click **Save** to save the settings.

4.2.18 How to Configure CMP - CloudLink Daemon connection

CloudLink is a cloud-based development and integration platform. As an administrator, you can configure CloudLink to integrate CMP with CloudLink tenants. This integration enables the management of Zoom users associated with those tenants, ensuring a secure connection through a proxy server.

Prerequisites

Adequate administrative permissions

Install the `cld-oscmp` CloudLink Daemon RPM package from the CMP server.

For more information, refer to the "Searching for RPMs" section, included in the **Using osc-setup for handling Repositories** chapter of the OpenScape UC Application V10 Installation Guide.

For an overview of the CloudLink Daemon and information on its user interface, refer to the CloudLink Daemon Solution Guide.

For an overview of the Zoom with OpenScape OSV and OpenScape SBC phone system integration solution, refer to **OpenScape Solution Set V11 Zoom Phone with OpenScape SBC and OpenScape Voice (Phone System Integration)**.

IMPORTANT: CloudLink is supported only in Standard Duplex deployments. It must **not** be enabled in OSV simplex deployments, as this configuration is unsupported.

Step by Step

To set up a connection with CloudLink Daemon:

1) Log in to the OpenScape Common Management Platform.
2) To install the CloudLink Daemon package, execute the following command in cmd: `osc-setup in cld-oscmp`.
3) Optional: To check the CloudLink Daemon status, execute the following command in cmd: `systemctl status cld`.

   By default, the CloudLink is deactivated.
4) To activate CloudLink Daemon, on the **Configuration** navigation tab, click on the **CMP** navigation menu item.
5) In the navigation tree, under the **General** area, click **CloudLink Settings**.

   NOTICE: The CloudLink settings option is visible only if the CloudLink Daemon package installation is successfully completed.

   A **CloudLink Settings** window pops up.
6) From the **Proxy** drop-down menu, select a proxy that is configured for CloudLink.

   The **Selected Proxy** field (read-only) displays the values that are already stored in CloudLink Daemon.

   NOTICE:

   CloudLink requires an internet connection. Set up a proxy for CloudLink only if necessary. For instructions on adding a proxy, refer to How to Add Proxy Server on page 64.
7) Click **Activate** to enable CloudLink daemon. To deactivate it, click **Deactivate**.

   IMPORTANT: If you change the proxy selection after clicking the **Activate** button, you will need to click on it again.
8) Click **Tenant Connection** to set up a connection with a tenant.

   NOTICE: The **Tenant Connection** button becomes active when the CloudLink daemon is enabled. Please note that it might take a few seconds for the button to activate after enabling it.

   Upon clicking, you will be redirected to the CloudLink window within the CMP.

   If your CloudLink account is not linked, you will be prompted to log in with your admin credentials to establish the connection. If the account is already linked, details of the connected account will be displayed.
9) To link to CloudLink, click **Link to CloudLink**.
10) Enter your credentials in the sign-in pop-up window and click **Next**.
    The CloudLink Daemon window refreshes to display the connection details.

11) Click **Close** to save the settings.

Next steps

Connect OSV to CloudLink:

- Configure OSV - CloudLink connection
- How to Create a new Zoom configuration on page 684

4.2.18.1 How to Configure OSV - CloudLink Daemon connection

As an administrator, you can configure OSV connection to CloudLink Daemon via the Common Management Platform.

Prerequisites

Adequate administrative permissions.

The CloudLink Daemon RPM is installed and CMP is connected to CloudLink Daemon.

You have enabled OSV- CloudLink to access the Internet via a proxy. For more information, refer to OpenScape Voice V10, Installation and Ugrades, Installation Guide, or to **OpenScape Solution Set V11 Zoom Phone with OpenScape SBC and OpenScape Voice (Phone System Integration)**.

To connect OpenScape OSV to CloudLink Daemon:

Step by Step

1) Log in to the OpenScape Common Management Platform.

2) Navigate to the **Configuration** > **OpenScape Voice** tab and lick on the **General** icon.

3) Select **Switches**.

The **Switches** dialog opens listing the switches accessible on the system.

4) Optional: Select a switch from the list of available switches. If no switch is selected, all listed switches will be included in the OSV-to-CloudLink connection.

5) Click **Connect to OSV/Cloudlink**.

CMP connects to Cloudlink Daemon on OSV nodes.
The **CloudLink connectivity** column displays the status of each system. There possible statuses are:

- **Disconnected**
- **Connected and deactivated**
- **Connected and activated**

NOTICE: The **Connected and activated** status indicates that the CloudLink is successfully connected, and that you have also enabled CloudLink Features for Zoom on that switch (see step 7).

If any node encounters an issue, a warning message is displayed.

6) To enable CloudLink features for Zoom on a switch, select the switch of your choice and click **Edit**.
The **Edit switch** pop-up window appears.
7) Locate the the **CloudLink Configuration** area and click **Enable container**.

NOTICE: The **Enable container** button is active only when the OSV status is **Connected** or **Connected and deactivated**, but NOT **Connected and activated**.

---

8) Click **Save** to save the settings.
Upon a successful connection, you can open the CloudLink Daemon GUI and configure the allocated tunnels.

Next steps

Create a new Zoom configuration and provision Zoom users:

- Zoom configurations
- Zoom Users configuration

4.3 Profile Management

The profile management enables you to administer the access privileges for the OpenScape system in a standardized way.

A profile consists of a collection of access privileges. By assigning such a profile to an administrator, you grant this person all access privileges of the relevant profile.

Each user-profile is assigned to exactly one domain.

Furthermore, each profile is assigned to a specific application. This application determines which type of access privileges the profile contains. If a profile is e.g. assigned to the Symphonia application, it controls the access privileges for the features of the CMP – for example for the domain administration. For which applications user-profiles are available depends on the OpenScape components installed with the system.

To use the user-profile management for limiting the configuration scope of the Common Management Platform, the access privileges control the display of the menu options an administrator can see on the navigation bar or in the navigation tree. If, for example, an administrator has not been assigned the **Domain** privilege, he/she cannot see the **Domains** navigation menu on the **CMP** navigation tab.

We can generally distinguish three types of profiles.

- Default profiles
- System profiles
- Customer profiles

4.3.1 Default Profiles

Default user-profiles are automatically created upon the system setup. Default profiles are indicated with the icon in the Common Management Platform

profile list and can neither be deleted nor modified. Which default profiles are altogether available in the Common Management Platform depends on the OpenScape components installed with the system.

Each default profile is assigned to a specific application. This application determines which type of access privileges the default profile contains. If a default profile is e.g. assigned to the Symphonia application, it controls the access privileges for the features of the Common Management Platform – for example for the profile or domain administration. For which applications default profiles are available depends on the OpenScape components installed with the system.

In the Common Management Platform, default profiles may be available for the following applications.

- CMP

  Provides the default user profiles for CMP.
- Device Management

  Provides the default user profiles for Device Management i.e external application Deployment Service (DLS).
- E / A Cockpit

  Provides the default user profiles for E / A Cockpit.
- OpenScape Voice

  Provides the default user-profiles for the access privileges of the OpenScape Voice Assistant.
- OpenScape SBC Assistant

  Provides the default user profiles for the access privileges OpenScape SBC Assistant.
- OpenScape Accounting

  Provides the default user profiles for external application OpenScape Accounting.
- OpenScape FM

  Provides the default user profiles for external application OpenScape Fault Management.
- OpenScape UC App

  Provides the default user-profiles for the access privileges of the OpenScape UC Application.

  NOTICE:

  TheOpenScape UC App is only available when you also use OpenScape UC Application with your communications solution.

- RGAssistant

  Provides the default user-profiles for the access privileges of the RG Assistant.
- Symphonia

  Provides the default user-profiles for the access privileges of the Common Management Platform.

4.3.2 System Profiles

The following Symphonia Application profiles are the System profiles and can only be modified not deleted.

- **CMP Login**
- **Administrator**
- **Customer Administrator**
- **Service Technician**

Which system profiles are altogether available in the CMP depends on the - OpenScapecomponents installed with the system.

4.3.3 Customer Profiles

In addition to the default and system profiles, you can also create individual profiles– so-called customer profiles.

Customer profiles are indicated in the Common Management Platform profile list with the icon. You can use them to provide user groups with standardized privilege levels, which are adjusted to the requirements and the level of knowledge of the relevant users.

We recommend to exclusively use customer profiles as far as possible.

Every feature of CMP has a corresponding permission defined in order to allow/ restrict the access to this feature

Profiles containing sets of these permissions can be created in order to model the different Roles that the CMP Admin Users may have.The assignment of these profiles to CMP Admin Users is essentially equivalent with granting the permissions described by the Role to the CMP Admin User. In order for a feature to work properly, additional non-CMP permission may be required to be granted to a User (e.g. Symphonia permissions) reference.

- The CMP permissions are used primarily to restrict access to various CMP screens in the User Interface level
- CMP permission do not restrict the access to Assistant screens
- CMP permission do not restrict access to Symphonia services Export of configuration data

4.3.4 Special Handling of CMP Administrator Permission

Special handling of CMP Administrator Permission is required in order to prevent the Admin Users from locking themselves out of the system and allowing them to regain access in case they are locked out of the system.

Following restrictions are applied to the CMP Admin User Permission:

- It is not allowed to remove this permission from the last, unlocked CMP admin User.

  This special handling is required in order to prevent the Users from locking themselves out of the system.

- **NOTICE:** An unlocked CMP Admin User account is neither explicitly locked nor locked due to too many unsuccessful logins

- It is not allowed to remove this permission from a CMP application Profile ONLY IF there is at least one other CMP application profile that contains this feature AND there is at least one, unlocked CMP Admin User that has this profile assigned.

  This special handling is required in order to prevent the Users from locking themselves out of the system when modifying Profiles.
- It is possible for an administrator to login to the CMP server using ssh and as root user execute the following script :

  ```
  #./opt/siemens/servicetools/security/resetUserAccount.sh

  resetUserAccount.sh <userURI> <new passphrase> [<path to
  installation directory>]
  ```

  This script will create the Super Administrator Profile with the default configuration and assign it to a specific symphonia user.

  This special handling is required in order to allow the administrator to regain access to CMP Admin Users Management in case s/he is locked out of the system by an operation that is not covered by the above two rules.
- It is possible for an administrator to explicitly lock an administrator. In this case, the system does not make any effort to protect the User from locking themselves out of the system. The administrator has to login to the CMP server using ssh and as root user execute a script that will unlock the locked user in order to regain access to CMP.

  The same applies when the administrator is locked out of the system due to too many unsuccessful login.

  The CMP "administrator@system" may be locked due to inactivity after 90 days. If CMP user goes to “inactive” state, he cannot longer login to CMP login page. The administrator may access the server using ssh and as root user execute the following:

  – On the application server execute the following (offboard server):

    ```
    /opt/siemens/servicetools/security/resetUserAccount.sh
    administartor@system 'Asd123!.'
    ```
  – On the integrated Simplex application server execute the following (onboard server):

    ```
    /enterprise/servicetools/security/resetUserAccount.sh
    administartor@system 'Asd123!.'
    ```

  The above commands will reset the user “administrator@system” to the default password "Asd123!." and will set its account in “active” state again so re-login to CMP can take place.

4.3.5 Default Profiles of the CMP

Common Managment Protal application contains all the necessary permission to control the access to the various CMP features.The default profiles for the

CMP are automatically created during the CMP setup and can neither be deleted nor modified.

Following profiles are installed automatically with CMP:

- A profile named **Super Administrator** is created by default and contains all the CMP permissions execpt the ones that are linked with licenses
- A profile named **Service Technician**is created by default and contains all the CMP permissions execpt the ones that are linked with licenses
- A profile named **Customer Administrator** is created by default and contains all the CMP permissions execpt the ones that are linked with licenses, Profile and Domain Managment, Software and Documentation Downloads, Importing and Exporting files.
- A profile named **OS User Management Feature Package LDAP** is created by default and contains all the CMP permissions that are linked to the OS_UM_FP1 License
- A profile named **OS User Management Feature Package OS ILA** is created by default and contains all the CMP permissions that are linked to the OS_UM_FP2 License

---

NOTICE:

No other profiles will be automatically installed with CMP.

NOTICE:

The default CMP profiles can’t be edited.

Following profile handling is performed :

- For fresh/new installations the administrator accoun that is created automatically is assigned with the Super Administrator profile.
- For upgrades, the assigned profiles of the default administrator account are not modified.
- For upgrades, the assigned profiles of the default administrator account are not modified.

  1) The administrator that created the subdomain automatically becomes a foreign user in that subdomain

  2) This foreign user is automatically assigned the Symphonia/ Administratorprofile in the subdomai

  3) CMP assigns to this foreign user the profile CMP/Super Administrator in the subdomain

4.3.6 How to map Symphonia permissions to CMP permissions for Upgrades to V7

In order for an administrator to use a feature in CMP it is required to have assigned both a Symphonia Application profile and a CMP Application profile

When you upgrade from versions prior to V6, the administrator accounts in the system already have a Symphonia profile assigned but no CMP profile. In order

for them to be able to access CMP screens, a proper CMP profile must also be assigned.

Below you can choose the “proper” CMP profile depending on the existing Symphonia profiles you had assigned to the administrator in the previous version:

- If the administrators have assigned the **default** Symphonia profiles only, you can use the following table to select the appropriate CMP profile that needs to be assigned to them in order to allow access to the same functionality they had in the previous version:

Symphonia Application profile (default)	CMP Application Profile (default)
Administrator	Super Administrator
Service Technical	CMP Service Technician
Customer Administrator	CMP Customer Administrator

IMPORTANT:

When upgrading to V7 the CMP Application **Super Administrator** profile is automatically assigned to the default administrator account (administrator@system) regardless of the Symphonia profile assigned to him.

If the default administrator account had full access to CMP, after the upgrade this account will still have full access to CMP

If the default administrator account had restricted access to CMP, after the upgrade the CMP Application **Super Administrator** profile must be un-assigned from this account and a different CMP Application profile must be assigned that will be aligned with the Symphonia permissions the default administrator account (administrator@system) has.

IMPORTANT:

When upgrading to V7, if the account that had full access to CMP is different from the administrator@system account, the CMP Application Super Administrator profile must be assigned to this account manually so that it will have full access to CMP V6 and be able to configure the other administrator accounts.

In order to Re-assign the CMP Super Administrator Profile back to the preferred user perform the following steps:

1) `login ssh`

2) `cd SYMPHONIA@HOME/servicetools/install/bin ./installlib.sh profileAssignmentHandling –DuserName <username@domain>`

Example: `sh installlib.sh profileAssignmentHandling -DuserName=administrator@system`

- In case you have created custom Symphonia profiles, you must also create custom CMP Application profiles to allow the access to the specific functionality the custom Symphonia profiles allowed.

  In order to select the necessary CMP Application permissions for your custom profiles, you can use the mapping table below to determine which CMP Application permissions are necessary in order to allow an administrator to use the functionality provided by a specific Symphonia permission:

For example if you want to grant the “AuditConfiguration” Symphonia permission the new custom CMP profile should include the permissions

CMP > **Configuration** > **CMP** > **Download Center** > **Documentation**

and **CMP** > **Configuration** > **CMP** > **Download Center** > **Software**

Symphonia Permission	CMP Permission(s)
AlarmManagement	**CMP** > **Maintenance** > **Monitoring** > **Alarms** > **Destinations**
	CMP > **Configuration** > **CMP** > **General** > **Alarm Indicator**
AuditAccess	
AuditConfiguration	**CMP** > **Configuration** > **CMP** > **Download Center** > **Documentation**
	CMP > **Configuration** > **CMP** > **Download Center** > **Software**
BackupRestore	**CMP** > **Maintenance** > **Monitoring** > **Tools & Utilities** > **Diagnostics Data Download**
	CMP > **Maintenance** > **Recovery** > **Backup & Restore** > **Backup**
	CMP > **Maintenance** > **Recovery** > **Backup & Restore** > **Restore**
	CMP > **Maintenance** > **Recovery** > **General** > **Archives**
	CMP > **Maintenance** > **Recovery** > **General** > **Backup Sets**
	CMP > **Maintenance** > **Recovery** > **General** > **Latest Job**
BasicManagement	
DeploymentSupport	
DomainLevelManagement	**CMP** > **Configuration** > **CMP** > **Download Center** > **Documentation**
	CMP > **Configuration** > **CMP** > **Download Center** > **Software**
DomainManagement	**CMP** > **Configuration** > **CMP** > **General** > **Domains**
	CMP > **Maintenance** > **Recovery** > **Import & Export** > **Export**

Symphonia Permission	CMP Permission(s)
	CMP > Maintenance > Recovery > Import & Export > Import
JMX_Monitoring	
LicenseManagement_Admin	CMP > Maintenance > Licenses > Management > Information
	CMP > Maintenance > Licenses > Management > Locking IDs
LicenseManagement_Extend	CMP > Maintenance > Licenses > Management > Information
	CMP > Maintenance > Licenses > Management > Locking IDs
LicenseManagement_Install	CMP > Maintenance > Licenses > Management > Information
	CMP > Maintenance > Licenses > Management > Locking IDs
ProfileManagement	CMP > Configuration > CMP > Download Center > Documentation
	CMP > Configuration > CMP > General > Profiles
	CMP > Configuration > CMP > Download Center > Software
Provisioning	
ResourceManagement	CMP > Configuration > Unified Communications > Accounts > Contact Settings > Private List
	CMP > Configuration > Unified Communications > Accounts > Contacts
	CMP > Configuration > Unified Communications > Configuration > Address Translation St.Routing
	CMP > Configuration > Unified Communications > Configuration > Address Translator Contexts
	CMP > Configuration > Unified Communications > Configuration > Conferences
	CMP > Configuration > Unified Communications > Configuration > Connections > Groupware
	CMP > Configuration > Unified Communications > Configuration > Connections > OpenScape 4000 Connection
	CMP > Configuration > Unified Communications > Configuration > Connections > Media Server Connections
	CMP > Configuration > Unified Communications > Configuration > Connections > OpenScape Voice Connection

Symphonia Permission	CMP Permission(s)
	CMP > Configuration > Unified Communications > Configuration > Presence & IM
	CMP > Configuration > Unified Communications > Devices > Media Server Resources > Conference Devices
	CMP > Configuration > Unified Communications > Devices > Media Server Resources > Prefixes
	CMP > Configuration > Unified Communications > Devices > Office Codes
	CMP > Configuration > Unified Communications > Devices > Prefixes
	CMP > Configuration > Unified Communications > Devices > Voice Subscribers
	CMP > User Management > Administration > OSV Migration Settings
	CMP > User Managment > Unified Communications > Devices > Media Server Resources > Office Codes
Scheduling	CMP > Maintenance > Recovery > Backup & Restore > Schedules
	CMP > Maintenance > Recovery > Import & Export > Schedules
SystemManagement_App	CMP > Configuration > CMP > General > Administrators > Active Sessions
	CMP > Configuration > CMP > General > Proxy Servers
	CMP > Configuration > CMP > General > System Settings
	CMP > Configuration > CMP > Smart Services Delivery Platform > Customer Information
	CMP > Configuration > CMP > Smart Services Delivery Platform > Enterprise Server
	CMP > Configuration > CMP > Smart Services Delivery Platform > Policy Server
	CMP > Configuration > CMP > Smart Services Delivery Platform > SNMP Profiles
	CMP > Configuration > Unified Communications > Configuration > Connections > LDAP Connectivity
	CMP > Maintenance > Inventory > Nodes & Applications > Applications
	CMP > Maintenance > Inventory > Nodes & Applications > Nodes

Symphonia Permission	CMP Permission(s)
	CMP > Maintenance > Inventory > Nodes & Applications > Repository
	CMP > Maintenance > Monitoring > Alarms > Active
	CMP > Maintenance > Monitoring > Logs > Alarm
	CMP > Maintenance > Monitoring > Logs > Fault
	CMP > Maintenance > Monitoring > Logs > Security
	CMP > Maintenance > Monitoring > Logs > System
	CMP > Maintenance > Monitoring > Tools & Utilities > Configuration Files
	CMP > Maintenance > Monitoring > Tools & Utilities > Consistency Checker
	CMP > Maintenance > Monitoring > Tools & Utilities > Trace File
SystemManagement_Service	CMP > Configuration > CMP > General > Administrators > Active Sessions
	CMP > Configuration > CMP > General > Proxy Servers
	CMP > Configuration > CMP > General > System Settings
	CMP > Configuration > CMP > Smart Services Delivery Platform > Customer Information
	CMP > Configuration > CMP > Smart Services Delivery Platform > Enterprise Server
	CMP > Configuration > CMP > Smart Services Delivery Platform > Policy Server
	CMP > Configuration > CMP > Smart Services Delivery Platform > SNMP Profiles
	CMP > Configuration > Unified Communications > Configuration > Connections > LDAP Connectivity
	CMP > Maintenance > Inventory > Nodes & Applications > Applications
	CMP > Maintenance > Inventory > Nodes & Applications > Nodes
	CMP > Maintenance > Inventory > Nodes & Applications > Repository
	CMP > Maintenance > Monitoring > Alarms > Active
	CMP > Maintenance > Monitoring > Logs > Alarm

Symphonia Permission	CMP Permission(s)
	CMP > Maintenance > Monitoring > Logs > Fault
	CMP > Maintenance > Monitoring > Logs > Security
	CMP > Maintenance > Monitoring > Logs > System
	CMP > Maintenance > Monitoring > Tools & Utilities > Call Trace
	CMP > Maintenance > Monitoring > Tools & Utilities > Configuration Files
	CMP > Maintenance > Monitoring > Tools & Utilities > Consistency Checker
	CMP > Maintenance > Monitoring > Tools & Utilities > Trace File
SystemManagement_System	CMP > Configuration > CMP > General > Administrators > Active Sessions
	CMP > Configuration > CMP > General > Proxy Servers
	CMP > Configuration > CMP > General > System Settings
	CMP > Configuration > CMP > Smart Services Delivery Platform > Customer Information
	CMP > Configuration > CMP > Smart Services Delivery Platform > Enterprise Server
	CMP > Configuration > CMP > Smart Services Delivery Platform > Policy Server
	CMP > Configuration > CMP > Smart Services Delivery Platform > SNMP Profiles
	CMP > Configuration > Unified Communications > Configuration > Connections > LDAP Connectivity
	CMP > Maintenance > Inventory > Nodes & Applications > Applications
	CMP > Maintenance > Inventory > Nodes & Applications > Nodes
	CMP > Maintenance > Inventory > Nodes & Applications > Repository
	CMP > Maintenance > Monitoring > Alarms > Active
	CMP > Maintenance > Monitoring > Logs > Alarm
	CMP > Maintenance > Monitoring > Logs > Fault
	CMP > Maintenance > Monitoring > Logs > Security

Symphonia Permission	CMP Permission(s)
	CMP > Maintenance > Monitoring > Logs > System
	CMP > Maintenance > Monitoring > Tools & Utilities > Call Trace
	CMP > Maintenance > Monitoring > Tools & Utilities > Configuration Files
	CMP > Maintenance > Monitoring > Tools & Utilities > Consistency Checker
	CMP > Maintenance > Monitoring > Tools & Utilities > Trace File
UserAuthenticationManagement	
UserManagement	CMP > Configuration > CMP > General > Administrators > Foreign
	CMP > Configuration > CMP > General > Administrators > List
	CMP > Configuration > Unified Communications > Accounts > Contact Settings > Global List
	CMP > Configuration > Unified Communications > Accounts > List
	CMP > User Management > Administration > Localities
	CMP > User Management > Administration > User Templates
	CMP > User Management > Administration > Users & Resources
	CMP > User Management > Provisioning > CSV Import
	CMP > User Management > Provisioning > Users from HPUM
	CMP > User Management > Provisioning > Users from OSV Subscribers
	CMP > User Management > Provisioning > Users from UC Accounts
UserPreferencesAccess	
UserPreferencesDeleteScope	

4.3.7 Default Profiles of the OpenScape Voice Assistant

The default user-profiles for the OpenScape Voice Assistant are automatically created during the OpenScape Voice Assistant setup.

In the Common Management Platform profile list they are indicated with the OpenScape Voice application and the icon and can neither be deleted nor modified.

With the OpenScape Voice Assistant the following default user-profiles are installed. These profiles are administrator profiles that control access to the OpenScape Voice Assistant features.

- Customer Administrator
- Basic Administrator
- Security Administrator
- Super Administrator

An OpenScape Voice administrator must be able to access the Common Management Platform features also. This requires the assignment of a Common Management Platform user-profile that has sufficient access privileges to the administrator's user account.

The following table describes which Common Management Platform default user-profile must be assigned to the respective administrators for OpenScape Voice.

Default user-profile for OpenScape Voice Assistant	Minimum required default user-profile for Symphonia Application
Customer Administrator	CMP login
Basic Administrator	CMP login
Security Administrator	CMP login
Super Administrator	CMP login

Overview of the Access Privilege Assignment

The OpenScape Voice Assistant access privileges are available in the Common Management Platform profile management under the OpenScape Voice application.

The below table shows in detail how these access privileges are assigned to the OpenScape Voice Assistant default user-profiles by default.

Name and short description of the Common Management Platform privilege	Basic Administ	Custome Administ	Securtiy Administ	Super Administrator
Basic Management Allows access to the **OpenScape Voice** tab in the Common Management Platform.	✓	✓	✓	✓

Name and short description of the Common Management Platform privilege	Basic Administ	Custome Administ	Securtiy Administ	Super Administrator
Communication System Access List Allows viewing all systems in the communication system list and administering the list entries. The administrator need not be a member of the access lists for communication systems.			✓	✓
Communication System Management Adds the administrator to the communication systems access list.	✓	✓	✓	✓
Communication System Settings Allows editing the settings of the displayed communication systems.		✓		✓
Call Admission Control Allows administering the call admission control of the communications systems.				✓
Number Display Allows administering the display number modification.				✓
Global Numbering Plan Allows administering the following settings: • Translation • Destinations and routes • Endpoint management				✓
Business Group Access List Allows viewing all business groups and creating or deleting new business groups for all displayed communication systems. The administrator need not be a member of the business group access lists.				✓
Business Group Management Adds the administrator to the business group access list for all displayed communication systems.		✓		✓

Name and short description of the Common Management Platform privilege	Basic Administ	Custome Administ	Securtiy Administ	Super Administrator
Business Group Settings Allows administering all displayed business groups. Within this scope you can also edit special business group settings – e. g. feature profiles, endpoint profiles, hunt and pickup groups.		✓		✓
Directory Numbers Allows administering office codes and home directory numbers.		✓		✓
Number Display		✓		✓
Main Office Subscribers Allows administering main office subscribers.		✓		✓
Main Office Endpoints Allows administering main office endpoints.		✓		✓
Branch Offices Access List Allows viewing all Branch Offices and creating or deleting new ones. The administrator need not be a member of the Branch Office access list.		✓		✓
Branch Office Management Allows administering OpenScape Branch		✓		✓
Branch Office Settings Allows administering the general settings of OpenScape Branch		✓		✓
Branch Office Subscribers Allows administering the subscriber settings of OpenScape Branch		✓		✓
Branch Office Endpoints Allows administering the endpoint settings of OpenScape Branch		✓		✓
OpenBranch Allows access to the **OpenScape Branch** tab in the Common Management Platform		✓		✓

Name and short description of the Common Management Platform privilege	Basic Administ	Custome Administ	Securtiy Administ	Super Administrator
Private Numbering Plan Access List Allows viewing all numbering plans and creating or deleting new ones. The administrator need not be a member of the access list for the numbering plan.		✓		✓
Private Numbering Plan Management Adds the administrator of all displayed communication systems or business groups to the numbering plan access list.		✓		✓
Private Numbering Plan Settings Allows administering numbering plans. This comprises the administration of the following elements of private numbering plans: • Translation • Destinations and routes		✓		✓
Business Group Reports Allows using statistics for business groups and MLHGs.		✓		✓
Directory Numbers Allows administering office codes and home directory numbers.				✓
ENUM Allows administering ENUM settings.				✓
Feature Management Allows administering the OpenScape Voice Feature Settings.				✓
Global Settings Allows administering the general OpenScape Voice settings and the signaling management.			✓	✓
Database Password			✓	✓
Other Global Settings				✓

Name and short description of the Common Management Platform privilege	Basic Administ	Custome Administ	Securtiy Administ	Super Administrator
Licensing Allows administering statistics intervals for dynamic and trunking licenses. Furthermore, the created statistics can be displayed.				✓
MediaServer Allows administering the OpenScape Voice settings for Media Server.				✓
Signaling Management Allows administering the OpenScape Voice settings for Signaling Management: SIP, SIP-Q, Digest Authendication, TLS, CSTA.				✓
Basic Configuration Allows administering settings in the OpenScape Voice Assistant.	✓			✓

4.3.8 How to Display/Edit Profile Settings

How to display and if necessary edit a Profile:

Prerequisites

Adequate administrative permissions

Step by Step

1) On the **Configuration** navigation tab, click on the **CMP** navigation menu item.
2) In the navigation tree, click on **General** > **Profiles**.

   A list of all profiles in the selected domain appears in the work area.

   This list contains for each entry the following information:

   Profile

   Name of the profile. Under this name the profile is administered in the Common Management Platform.

   Application

   Name of the application the access privileges of which are specified by the profile.

   Number of Users Assigned

   Number of users assigned to the profile.

3) Click on the name of the profile the settings of which you want to edit.

   The profile-settings dialog opens.

4) Select the checkbox of the privileges you want to assign to the selected profile.

   NOTICE:

   The privileges of default profiles cannot be modified.

   The product names and licenses required for the activated rights are displayed in the **Licenses** area.

5) Click on **Save** to copy the entries to the system's database.

4.3.9 How to Add a Profile

How to add a Profile:

Prerequisites

Adequate administrative permissions

Step by Step

1) On the **Configuration** navigation tab, click on the **CMP** navigation menu item.
2) In the navigation tree, click on **General** > **Profiles**.

   A list of all profiles in the selected domain appears in the work area.

3) Click on **Add**.

   The profile settings dialog opens.

4) Under **Name** enter a short, unique name for the new profile.

   Under this name the profile is administered in the Common Management Platform.

5) Select under **Application** which privilege group the profile is to determine.

   Which privilege groups are offered here for selection depends on the components installed with the OpenScape system.

   - Select **CMP** to define privileges for CMP.
   - Select **Device Management** to define privileges for external application Deployment Service (DLS).
   - Select **E/A Cockpit** to define privileges for E/A Cockpit.
   - Select **OpenScape Voice** to define the privileges for the OpenScape Voice Assistant.
   - Select **OpenScape SBC Assistant** to define the privileges for the OpenScape SBC Assistant.
   - Select **OpenScape Accounting** to define the privileges for the OpenScape Accounting.
   - Select **OpenScape FM** to define the privileges for the OpenScape Fault Management.
   - Select **OpenScape UC App** to define privileges for OpenScape UC Application.
   - Select **RGAssistant** to define privileges for the RG Assistant.
   - Select **Symphonia** to define privileges for the Common Management Platform.

6) Select the checkbox of the privileges you want to assign to the profile.

   Which privileges are offered for selection depends on the privilege group you have selected under **Application**.

   NOTICE:

   Saving a Profile without any privileges/permissions assigned may lead to issues affecting the functionality of users who are assigned to this Profile.

   ---

7) Click on the Profile and navigate to the **Licenses** area to see the product names and licenses required for the activated privileges.
8) Click on **Save** to copy the entries to the system's database.

The new user profile is saved and displayed in the profiles list.

4.3.10 How to Copy a Profile

You can create a new profile based on an already existing one. Copy the existing profile and adjust the privileges of the profile copy to your requirements.

Prerequisites

Adequate administrative permissions

Step by Step

1) On the **Configuration** navigation tab, click on the **CMP** navigation menu item.
2) In the navigation tree, click on **General** > **Profiles**.

   A list of all profiles in the selected domain appears in the work area.

3) Select the checkbox of the profile you want to copy.
4) Click on **Copy**.
   The dialog with the settings of the profile copy opens.
5) Under **Name** enter a short, unique name for the new profile.
   Under this name the profile is administered in the Common Management Platform.
6) Select the checkbox of the privileges you want to assign to the profile.
   The product names and licenses required for the activated privileges are displayed in the **Licenses** area.
7) Click on **Save** to copy the entries to the system's database.

The new user profile is saved and displayed in the profiles list.

NOTICE: Profile Symphonia:Administrator must not be copied. An administrator that needs to have the permissions of Symphonia:Administrator must have this specific profile.

4.3.11 How to Delete a User Profile

How to Delete a profile:

Prerequisites

Adequate administrative permissions

Step by Step

1) On the **Configuration** navigation tab, click on the **CMP** navigation menu item.
2) In the navigation tree, click on **General** > **Profiles**.
   A list of all profiles in the selected domain appears in the work area.
3) Click on the name of the profile the settings of which you want to edit.
   The profile-settings dialog opens.
4) Select the checkboxes of the profiles that you want to delete.

   NOTICE: Default and System profiles cannot be deleted.

   ---

5) Click **Delete**.
6) Click on **OK** to confirm the deletion of the selected profiles.

The selected profile (s) will be deleted

4.4 System Management

Using the system management you can quickly gain an overview of the available system nodes and their logical grouping (clustering). Furthermore,

it provides auxiliary means to configure these system nodes and to log this configuration.

The system management is devided into the following areas:

- System Status
  - Nodes
  - Applications
- Node Groups
- 3rd Party Nodes
- Xpression Node
- OpenScape 4000 Node
- SNMP Node

The system management is domain-spanning. It cannot be used by service provider administrators, since these administrators should not be in a position to display the installed components.

4.4.1 System Overview

The system overview provides information about the structure of the OpenScape system and the status of the associated system nodes. Furthermore, you can arrange the various system nodes in a logic order and configure associated applications.

The System overview is divided into the following areas:

- Nodes
- Applications

The system overview is domain-spanning. It cannot be used by service provider administrators, since these administrators should not be in a position to display the installed components.

Nodes

Under Nodes you are provided with an overview of the available system nodes, the connections to 3rd party systems and their groups (nodes cluster).

For each node you can display a so-called dashboard. Depending on the system node type this dashboard can comprise detailed information about the following topics:

- Individually configurable note for the system node
- Alarms for the system node
- System information about the hardware of the system node
- Applications installed on the system node and their software versions
- Actions executable for the system node. E. g:
  - Show status information about the nodes system health by means of OSV Rapidstat and UC Rapidstat.
  - Show related log files.
  - Show information of related services and components.
  - Configure settings of related services and components.
  - Show the version of installed software packages.

- Operational status information

You find details about the displayed node type dependent information in the chapters about the corresponding node type.

Applications

Under Applications you are provided with an overview of all internal and external applications

For internal applications that are installed on the system nodes you can see in which software version the application is installed and on which system node.

For external applications that can be accessed via CMP you can see the applications IP or Hostname.

The action menu (‣) of an application entry lets you configure application individual settings. You find details about the application individual settings in the chapters about the corresponding application.

4.4.2 How to Display System Nodes

The Nodes section provides an overview of the existing system nodes and their groupings. Furthermore, the Nodes section allows you to administer the connections to 3rd party nodes. To display node overview proceed as indicated:

Prerequisites

Adequate administrative permissions

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.

This list contains for each system node the following information:

- **Node Icon**

  Icon for the system node
- **Name**

  System node name
- **Group**

  To which system node is grouped in
- **IP Address/Hostname**

  IP address or Hostanme of the system node
- **Type**

  System node type

4.4.3 Node Groups

The system nodes of an OpenScape system can be combined in node groups. This lets you manage the different system nodes in logic groups.

If a system node is not assigned to an individual node group, it belongs to the node group Root. The node group Root is automatically configured after the installation of the OpenScape system and cannot be deleted.

4.4.3.1 How to Display a Node Group

How to show all configured node groups:

Prerequisites

Adequate administrative permissions

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**.
3) Click on **Group**.

A dialog opens that displays a list of all configured node groups.

4.4.3.2 How to Add a Node Group

How to add a node group:

Prerequisites

Adequate administrative permissions

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 **Group**.

   A dialog opens that displays a list of all configured node groups.
4) Click on **Add**.

   The dialog for adding a new node group opens.
5) Enter a short, unique name for the new node group under **Group Name** .

   Under this name the node group is administered in the Common Management Platform.

6) Specify under **Description** a short descriptive text for the new node group.
7) Switch to the **Nodes in Group** tab.
8) Click on **Add**.

   A dialog that lists all available system nodes opens.
9) Select the checkbox of the system nodes you want to assign to the new node group.
10) Click on **Add**.

    The selected system nodes are displayed as part of the new node group.
11) Click on **Save**.

    The selected system nodes are displayed as part of the new node group.

The new node group is displayed in the list of all node groups.

4.4.3.3 How to Edit a Node Group

How to edit a configured node group:

Prerequisites

Adequate administrative permissions

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**.
3) Click on **Group**.

   A dialog opens that displays a list of all configured node groups.
4) Click on the name of the node group that you want to edit.

   The dialog with the settings of the relevant node group opens.
5) Change the desired settings.
6) Click on **Save** to copy the entries to the system's database.

NOTICE:

If a system node is not assigned to an individual node group, it belongs to the node group Root. The node group Root is automatically configured after the installation of the OpenScape system and cannot be deleted or modified.

Node group Root Contains all Nodes that have not been added to any already created Group.

4.4.3.4 How to Delete a Node Group

How to delete a node group:

Prerequisites

Adequate administrative permissions

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**.
3) Click on **Group**.

   A dialog opens that displays a list of all configured node groups.
4) Select the checkboxes of the node groups that you want to delete.
5) Click on **Delete**.
6) Click on **OK** to confirm the deletion of the selected node groups.

NOTICE:

If a system node is assigned to an individual node group and the node group is deleted then this system node is moved to the node group “Root”. The node group “Root” is automatically configured after the installation of the OpenScape system and cannot be deleted or modified.

The selected node groups are removed from the system's database and from the list of all node groups.

4.4.4 3rd Party Nodes

An OpenScape system can be connected to 3rd party nodes to provide OpenScape users with additional web applications. 3rd party nodes can be connected via Telnet, HTTP, HTTPS, or SSH to the OpenScape system.

4.4.4.1 How to Display 3rd Party Node Connections

How to display and if necessary edit the configuration of a 3rd party nodes connection:

Prerequisites

Adequate administrative permissions

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**.
3) Click on **3rd party nodes**.

A dialog opens that displays a list of all configured 3rd party node connections.

4.4.4.2 How to Add a 3rd Party Nodes Connection

How to add a new connection for a 3rd party node:

Prerequisites

Adequate administrative permissions

NOTICE:

Communicating with a 3rd party node via SSH requires the SSH Secure Shell client (PuTTY). Before you can add a new 3rd party nodes connection, you must therefore install the SSH Secure Shell client if it has not been set up yet.

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**.
3) Click on **3rd party nodes**.

   A dialog opens that displays a list of all 3rd party node connections configured in the entire system.
4) Click on **Add**.

   The dialog with the link settings opens.
5) Select under **Ext. Link Type** the protocol to be used for communicating with the 3rd party node.
6) Under **Name** enter a short, unique name for the new 3rd party nodes connection.

   Under this name the 3rd party nodes connection is administered in the Common Management Platform.
7) Specify under **Ext. Link** the address under which the external system can be reached.
8) If you have selected the SSH protocol under **Ext. Link Type**, enter under **Username** the name of the user to be deployed for the connection setup.
9) Specify under **Description** a short descriptive text for the new 3rd party node connection.
10) Click on **Test** to test the settings.
11) Click on **Save** to copy the entries to the system's database.

The new 3rd party nodes connection is displayed in the list of 3rd party nodes connections.

4.4.4.3 How to Edit the Settings of a 3rd Party Node Connection

How to edit the settings of a 3rd party node connection:

Prerequisites

Adequate administrative permissions

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**.
3) Click on **3rd party nodes**.

   A dialog opens that displays a list of all 3rd party node connections configured in the entire system.
4) Click on the name of the desired 3rd party nodes connection.

   The dialog with the settings of the relevant 3rd party nodes connection opens.
5) Change the desired settings.
6) Click on **Save** to copy the entries to the system's database.

4.4.4.4 How to Delete a 3rd Party Nodes Connection

How to delete a connection to a 3rd party node:

Prerequisites

Adequate administrative permissions

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**.
3) Click on **3rd party nodes**.

   A dialog opens that displays a list of all 3rd party node connections configured in the entire system.
4) Select the checkboxes of the 3rd party nodes connections that you want to delete.
5) Click on **Delete**.
6) Click on **OK** to confirm the deletion of the selected 3rd party nodes connection.

The selected 3rd party nodes connections are removed from the system's database and from the list of all 3rd party nodes connections.

4.4.5 Xpression Node

When the Xpression is deployed in the Open Scape System you can configure the Xpression nodes by entering IP address, SNMP Community String and support for Software Subscription License (SSL) and log this configuration.

You can also edit an already Configured Xpression Node that appears in the Node list by using the actions menu ‣ .

NOTICE:

The “add” button for Xpressions is available only if the component is deployed in the System

4.4.5.1 How to Add an OSC Xpressions Node

How to add an Xpressions node:

Prerequisites

Adequate administrative permissions

Install the top-level rpm OpenScapeUC_xpraddons

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 node connections available in the entire system is displayed in the workspace.
3) Click on **Add OSC Xpressions**.

   The dialog with the link settings opens.
4) Following attributes are required to configure the node:

   - **Name**
   - **Node IP**
   - **SNMP Com. String**

     IMPORTANT:

     SNMP Com. String field is case sensitive (e.g. value *“Public”* is different from value *“public”*).
   - **Port** (default value is 161)
   - **EM SDK Port** (default value is 4444)

   If Xpressions Node supports Software Subscription License (SSL) then following attributes are also mandatory

   a) **SSL SNMP Community String**

   a) **SSL Port** (default value is 161)

5) Click on **Save** to copy the entries to the system's database.

   Xpression node is added to the Nodes list.

Next steps

As soon as the Xpressions node is added to the Nodes list an “Xpressions resource synchronization” is initiated.

The Synchronization is done in two (2) steps:

1) In the fIrst step the system retrieves the Xpressions accounts.

   During this process following message is displayed:

   “Fetching Xpressions accounts...”

   The progress bar is not active and the step can’t be canceled.
2) In the second step Synchronization of the accounts is performed.

   During this process following message is displayed:

   “Synchronizing Xpression account x/y.” (x is the current account and y is the total amount of accounts to be synchronized)

   The progress bar is active during this step and you can cancel it at any time by clicking on the **Cancel** button. Cancelation triggers the following:

   The operation is cancelled after the synchronization of the current Xpressions account is completed.
   The modifications made up to the point when the operation was Cancelled are committed. There is no roll-back functionality.
   Following message is displayed:

“The Xpressions node was added in the nodes list. The synchronization of the Xpressions node was cancelled. YY new Xpressions accounts were synchronized in CMP”

If the synchronization process is completed following message is displayed:

“The Xpressions node was added in the nodes list. Synchronization of the Xpressions node completed successfully. YY new Xpressions accounts were synchronized in CMP”

IMPORTANT:

If the connection to the Xpressions node is lost during the synchronization then no Xpressions accounts are synchronized in CMP.

4.4.5.2 How to Modify an OSC Xpressions Node

How to modify an Xpressions node:

Prerequisites

Adequate administrative permissions

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 node connections available in the entire system is displayed in the workspace.
3) Click on the actions menu of the Xpressions node you wish to **Edit**.
4) Click on **Edit**

   The dialog with the node settings opens.
5) Following attributes of the Xpressions node can be modified:

   - **Name**
   - **Node IP**
   - **SNMP Com. String**

   IMPORTANT:

   SNMP Com. String field is case sensitive (e.g. value *“Public”* is different from value *“public”*).

   - **Port** (default value is 161)
   - **EM SDK Port** (default value is 4444)

   If Xpressions Node supports Software Subscription License (SSL) then following attributes are also mandatory:

   a) **SSL SNMP Community String**

   a) **SSL Port** (default value is 161)
6) Click on **Save** to copy the entries to the system's database.

4.4.5.3 How to Synchronize the accounts of an OSC Xpressions Node in CMP

You can trigger the synchronization of the accounts of an Xpressions node in CMP so you can then have these accounts available when selecting to assign an existing resource to a UM User.

Prerequisites

Adequate administrative permissions

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 node connections available in the entire system is displayed in the workspace.
3) Click on the action menu of the node you wish to Synchronize.

4) Click on **Synchronize**

Synchronization is initiated and is done in two (2) steps:

- In the flrst step the system retrieves the Xpressions accounts.

  During this process following message is displayed:

  "`Fetching Xpressions accounts...`"

  The progress bar is not active and the step can't be canceled.
- In the second step Synchronization of the accounts is performed.

  During this process following message is displayed:

  "`Synchronizing Xpression account x/y.`" (x is the current account and y is the total amount of accounts to be synchronized)

  The progress bar is active during this step and you can cancel the step at any time by clicking on the **Cancel** button.

  Cancelation triggers the following:

  1. The operation is cancelled after the synchronization of the current Xpressions account is completed.

  2. The modifications made up to the point when the operation was Cancelled are committed. There is no roll-back functionality.

  3. Following message is displayed:

  "`The synchronization of the Xpressions was cancelled. YY new Xpressions accounts were synchronized in CMP.`"

  If the synchronization process is completed following message is displayed:

  "`Synchronization of the Xpressions node completed successfully. YY new Xpressions accounts were synchronized in CMP`"

NOTICE: If another Administrator has initiated the synchronization of an Xpressions node and you also attempt to Synchronize it during this time then an error message is displayed and your synchronization is not performed.

IMPORTANT:

If the connection to the Xpressions node is lost during the synchronization then no Xpressions accounts are synchronized in CMP.

4.4.5.4 How to Remove an OSC Xpressions Node

How to remove an Xpressions node from Node List:

Prerequisites

Adequate administrative permissions

There are no Xpressions resources of the selected to “be removed” Xpressions Node that are assigned to Users

The selected “be removed” node doesn't have an active Software Subscription License (SSL) connection

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 node connections available in the entire system is displayed in the workspace.
3) Click on the actions menu of the Xpressions node you wish to remove.
4) Click on **Remove Node**

   You are requested to confirm the following by clicking **OK**:

   “ Any Xpressions resources associated with the selected Xpressions Node will be removed from the system”

   or if the node is supporting SSL

   “Any Xpressions resources associated with the selected Xpressions Node will be removed from the system. This node also supports SSL. The collection of SSL data will stop. Any SSL related information will not be removed from the system”

   IMPORTANT:

   If you attempt to delete an Xpressions Node that has Xpressions resources assigned to Users then the removal of the Node is not possible. You should first unassign the Xpressions resources from the Users and then remove the node.
5) Xpressions node is now removed

4.4.6 OpenScape 4000 Node

When the OpenScape 4000 is deployed in the Open Scape System you can configure the self-managed or manager OpenScape 4000 node and log this configuration.

You can also edit, remove or synchronize an already Configured OpenScape 4000 Node that appear in the Node list by using the actions menu ‣.

NOTICE:

The “add” button for OpenScape 4000 is available only if the component is deployed in the System.

The OpenScape 4000 Nodes (OS4K) are depicted in the list with the following icons:

Node Type	Icon
OS4K Manager	
OS4K Managed	
OS4K Managed - Incomplete	
OS4K Self Managed	

OpenScape 4000 Node Full Synchronization

The Full Synchronization of an OpenScape 4000 Node may synchronize managed Nodes but also synchronizes Phone data, Office Codes (Numbering Plans) and the Prefixes (Dial Plans). Full Synchronization is triggered manually.

NOTICE:

Full Synchronization is performed once a OpenScape 4000 node is added and all OS4K entities that interest UC are copied to the UC Database. After the initial synchronization the delta synchronization mechanism of CMP keeps the UC database up to date with all DN changes instituted on OS4K.

In case of a Virtual OpenScape 4000 Numbering Plan (VNR) CMP synchronizes the virtual numbering plan along with the OS4K subscribers and stores their extensions in the Device Model.

The table below illustrates all the types of numbering plans the CMP's synchronization process supports, along with a typical example:

#	Description	CC (country Code)	AC (Area Code	LC (Local Code)	Skip Digits	VNAC	VNAC Skip Digits	Prefix Digits	Extension OS4K	Extensi to create by CMP	Extensio recalcula by Device Model	Ove	Normalized Number
1	Plain	30	210	8189	4	NA	NA	NA	100	100	100	0	302108189100
2	Plain with overlap	30	210	8189	3	NA	NA	NA	9100	100	9100	1	302108189100
3	Prefix Digit	30	210	8189	4	NA	NA	73	73100	73100	73100	0	302108189100
4	Prefix Digit with overlap	30	210	8189	3	NA	NA	73	739100	739100	739100	1	302108189100
5	VNR	30	210	8189	4	25	2	NA	25100	100	100	0	302108189100
6	VNR with overlap (simple)	30	210	8189	3	29	1	NA	29100	100	9100	1	302108189100
7	VNR with overlap (1/2)	30	210	81891	4	251	2	NA	25110	100	110	1	302108189110

#	Description	CC (country Code)	AC (Area Code	LC (Local Code)	Skip Digits	VNAC	VNAC Skip Digits	Prefix Digits	Extension OS4K	Extensi to create by CMP	Extensio recalcula by Device Model	Ove	Normalized Number
8	VNR with overlap (2/2)	30	210	81892	4	252	2	NA	25210	100	210	1	302108189210

The following points elaborate on the table above:

1) "Skip Digits" (SD) is the number of digits in the LC that are considered as "valid" (starting from the left). E.g. LC=8189, SD=3 means only "818" is valid - ignore the rest (obviously because it is part of the extension).

2) Same as "1." holds for Skip Digits in VNAC (Virtual Number Access Code) . E.g. in rows 4 and 5, only "25" is the valid part of the VNAC.

3) VNAC is a prefix that needs to be removed from the extension. But because of "2.", only its "valid" part needs to be removed from the extension,e.g. only "25" needs to be "removed" from the extension in rows 5 and 6.

4) As it becomes obvious by the examples above, VNACs and overlaps do not have any influence on the normalized number. However, they are important to know when originating from the OS4K data, because they need to be "removed" from the extension.

5) When there is a VNAC or overlap defined, then they must be part of the extension configured in the OS4K. Otherwise the configuration is considered as invalid

6) Prefix Digit (PD) is used for an alternative to VNR Numbering Plan and is not implemented in a VNR configuration, hence the NA in relevant VNR columns.

NOTICE:

Countries like Italy or Belgium could have empty either ISDN_AreaCode or ISDN_LocalCode in their OpenScape 4000 numbering plan schemes. This was causing synchronization issues between CMP and OpenScape 4000 in the past which are now resolved. As a result 4000 ONS UC accounts can be set with such Italian or Belgium OpenScape 4000 numbers.

OpenScape 4000 Synchronization Exceptions

The following OpenScape 4000 configurations can’t be synchronized correctly by CMP:

- Every OS4K Phone (Station) must have a corresponding Numbering Plan (KNDEF) and Dial Plan (KNPRE) configured. OS4K Phones that do not meet this requirement will not be synchronized to CMP/UC.
- CMP's synchronization process does not support OS4K Dial Plans that have one or more of the following characters: *#, *, A, B, C, and D.*

  Any attempt to synchronize these Dial Plans will be treated by Device Management with an exception message.

- Non-VNR Numbering Plans where there is still a shortcut-prefix to access a OS4K Node (=Office Code), the so-called "site code".
- Any other plain numbering plans with overlap, where the extensions do not start with the overlap.

OpenScape 4000 Node Delta Synchronization

The Full Synchronization is either triggered automatically when a OpenScape 4000 (OS4K) is added to CMP or manually by the Administrator and recreates the UC Database with all OpenScape 4000 (OS4K) entities.

The Delta Synchronization is automated and CMP is informed in administrable time periods about any add/delete/moves that are performed using the OS4K Manager / Assistant (Self Managed).

IMPORTANT:

When you attempt to move one station (phone) from one OS4K switch to another using the OS4K Manager / Assistant (Self Managed) you must make sure the E.164 number stays the same in order to avoid any problems. If you don't keep the same E.164 numbers for a station that is moved the journal entries for this station will not be displayed in the OpenScape Web Client.

The Administrator can provide a solution[2] but a UC restart is required for the updates to take effect.

UC database is automatically updated to reflect these changes.

The Administrator has also the option to initiate manually a Delta Synch.

---

[2] Navigate to CMP -> Configuration -> Unified Communications -> Address Translation Station Routing -> Update the Address Translation Station Routing by adding a single Address Translation Station Routing for the station that has been moved.

Example:

The Address Translation Station Routing for a range of stations is

20000-29999 => 4930423-2xxxx.

So for station 20101 in this range the above “Address Translation Station Routing” translates it to

20101 => 493042320101

If the numbering plan of station 20101 is modified by OS4K Manager/Assistant and Normalized Number is changed from

493042320101 to 493043320101 due to the Address Translation Station Routing the Station is mistakenly translated to 493042320101.

A quick solution after the Delta Sync mechanism is performed to create additional “Address Translation Station Routing” entries, as shown below:

20000-20100 => 4930423-2xxxx20101-20101 => 4930433-2xxxx (single station number)20102-29999 => 4930423-2xxxx

A UC restart is required for the Address Translation Station Routing changes to take effect.

4.4.6.1 How to Add an OpenScape 4000 Node

How to add an OpenScape 4000 (OS4K) node:

Prerequisites

Adequate administrative permissions

Install the top-level rpm OpenScapeUC_OS4Kaddons

When adding an OS4K Node V7 or higher, you need to ensure that the OS4K Node's SNMP Agent is properly configured either from the OS4K Assistant[3] or from the OS4K Manager.[4]

NOTICE:

For further information refer to chapter "Assistant GUI SNMP" in "OpenScape 4000 Manager V7, Installation and Service Manual, Service Documentation".

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 node connections available in the entire system is displayed in the workspace.
3) Click on **Add OpenScape 4000**.

   The dialog with the link settings opens.
4) Choose the Node Type (Manager, self managed) and node version (lower than version 7, node version 7 or higher) from the pull down menu:
   - self managed - lower than version 7
   - manager - lower than version 7
   - self managed - version 7 or higher
   - manager - version 7 or higher

[3] **Diagnostics** > **Fault Management** > **SNMP Configurator** > **Protocol SNMPv1** > **Community** > **Add Community**

[4] **Fault Management** > **SNMP Configurator**

5) The attributes used to configure the node are listed below and the relative fields that are editable depend on the Node Type and version chosen in the previous step:

- **Name**
- **IP address/Hostname**

  You are not permitted to use an IP that is already used by another node of any type in the Node List
- **Administration Port** (Communication system SOAP Port, default value 443)
- **User Name** (for SOAP/CORBA access)
- **Password** (for SOAP/CORBA access)
- **SNMP Read Community** (is requested only for nodes lower than v7, “public” is the default value)
-

  IMPORTANT:

  SNMP Read Community field is case sensitive (e.g. value *“Public”* is different from value *“public”*).
- **CSTA IP** (for self-managed node only)
- **CSTA Port (default value is 1040)**
- **App ID** (for self-managed node only)
- **Sub App ID** (for self-managed node only)

6) Click on **Save** to copy the entries to the system's database.

NOTICE:

You can add up to 120 OpenScape 4000 nodes to one UC System

Next steps

- If the Node Type is manager and Node version is “lower than version 7” then after **Saving** the Node, the System has also added to the Node List all the Nodes that are managed by this “Manager -type” Node

  These newly added **Nodes** are initially marked as “Incomplete” in the Node List so you have to **Edit** (“How to Modify an OpenScape 4000 Node”) these Nodes and fill in the same fields as in step 5 leaving out the **Name.**

  Name in this case is a read only field and is already specified by the “Manager” of the Node.
- If the Node Type is manager and Node version is “version 7 or higher” after **Saving** the Node the System has also added to the Node List all the Nodes that are managed by this “Manager -type” Node.

  If we add an OS4K Manager (“of version 7 or higher”), who manages several OS4K Switches, the **CSTA IP** address of each OS4K Switch will be populated only for the V7 or higher OS4K Switches. For managed switches “lower than version 7” (< V7), the switches will be set as incomplete in the Node list, and the **CSTA IP** address, the IP or Hostname and the password will have to be provided manually by the user.

4.4.6.2 How to Modify a OpenScape 4000 Node

How to modify a OpenScape 4000 node:

Prerequisites

Adequate administrative permissions

In case you want to modify an IP address/Hostname of a “Manager Node” "lower than version 7" you should first update the connections (Operation UPLOAD[5] via OpenScape 4000 Configuration Management) of all the OpenScape 4000 switches managed by this OpenScape 4000 manager

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 node connections available in the entire system is displayed in the workspace.
3) Click on the actions menu of the OpenScape 4000 node you wish to edit.
4) Click on **Edit**

   The dialog with the node setting opens.

[5] Following navigation directs you to Operation Upload:

a.Log on to the OS4K assistant

b.Navigate to Configuration Management-->Netwrok-->System

c. Press the search button to find the data for your OS4K system

d. Go to action menu and then press upload

5) If you choose to edit a OpenScape 4000 “Node” you are allowed to edit the following attributes of the Node:

- **Node Version** (“lower than version 7”, “version 7 or higher”)

  IMPORTANT:

  You can change the OS4K node version from “lower than version 7” to “version 7 or higher” in edit mode but you can’t change the node type.

- **IP address/Hostname**

  You are not permitted to use an IP that is already used by another node of any type in the Node List

  If you want to modify the IP address/Hostname of a “Manager Node” lower than version 7 you are only allowed to enter a Node IP that corresponds to the same “OpenScape 4000 Manager Node”

  IMPORTANT:

  In order for CMP to support the IP address/Hostname modification of a “Manager Node” lower than version 7 you must update first the connections (Operation UPLOAD via OpenScape 4000 Configuration Management) of all the OpenScape 4000 switches managed by this OpenScape 4000 manager.

  All Nodes that are managed by the “Manager -type” Node lower than version 7 are added to the Node List and are marked as “Incomplete”

  IMPORTANT:

  If you are changing IPs in an installation with multiple OpenScape 4000 Managers you must take in to account that you are not allowed to change a Manager’s Node IP to an IP of a different Manager Node. The modification

of the Manager's Node IP within CMP is **supported only** when the "same" Manager runs on the new IP

- **Administration Port** (Communication system SOAP Port and only for versions 7 or higher, default value 443)
- **User Name** (for SOAP/CORBA access)
- **Password** (for SOAP/CORBA access)
- **SNMP Read Community** (is requested only for nodes lower than v7, “public” is the default value)
-

  IMPORTANT:

  SNMP Read Community field is case sensitive (e.g. value *“Public”* is different from value *“public”*).

  NOTICE:

  It is possible to edit **SNMP Read Community** field for a manager - version 7 or higher node.

- **CSTA IP** (for self-managed node only)
- **CSTA Port (default value is 1040)**
- **App ID** (for self-managed node only)
- **Sub App ID** (for self-managed node only)

6) Click on **Save** to add the Node to the Node list.

NOTICE:

You can add maximum 120 OpenScape 4000 nodes to one UC System.

4.4.6.3 How to Remove a OpenScape 4000 Node

How to remove a OpenScape 4000 node:

Prerequisites

Adequate administrative permissions

If you are going to remove a OpenScape 4000 “Managed Node” / OpenScape 4000 “Self-Managed Node” there should be no resources of this node assigned to Users.

If you are going to remove a OpenScape 4000 “Managed Node” / OpenScape 4000 “Self-Managed Node” there should be no **Address Translation Contexts** associated with this node.

If you are going to remove a OpenScape 4000 “Manager Node” then all OpenScape 4000 switches managed by this OpenScape 4000 manager should not have Users assigned to their (OpenScape 4000 switches) resources.

If you are going to remove a OpenScape 4000 “Manager Node” then all OpenScape 4000 switches managed by this OpenScape 4000 manager should have no **Address Translation Contexts** associated with these switches.

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 node connections available in the entire system is displayed in the workspace.
3) Click on the actions menu of the OpenScape 4000 node you wish to remove.
4) Click on **Remove Node**

   You are requested to confirm the following by clicking **OK**:

   "*You have requested to remove the HiPath OS4K Node "Node_Name". Any subscribers associated with the selected node will be removed from the system. Do you want to continue?*"

   or if you want to remove a "Manager Node"

   "*You have requested to remove the HiPath OS4K Manager Node "Node_Name". Any managed node ascociated with the selected manager node will be removed from the system. Do you want to continue?*"

   If any of the Prerequisites for removing a OpenScape 4000 Node is not fulfilled, a relative message will appear mentioning the reason for which the removal failed.

   So if you attempt to:

   - - Remove a OpenScape 4000 "Managed Node" or OpenScape 4000 "Self-Managed Node" with resources of this node assigned to Users. You are prompt with the following message:

     "*You have requested to remove the HiPath OS4K Node "Node_Name". There are XYZ HiPath OS4K resources associated with the selected node that are assigned to Users. The removal of the node is not possible. Please unassign the HiPath OS4K resources from the Users first*"
   - -Remove a OpenScape 4000 "Managed Node" / OpenScape 4000 "Self-Managed Node" and there is an **Address Translation Context** associated with this node. You are prompt with the following message:

     "*You have requested to remove the HiPath OS4K Node "Node_Name". There are Address Translation Contexts associated with the selected node. The removal of the node is not possible. Please remove the associated Address Translation Contexts first*"
   - -Remove a OpenScape 4000 "Manager Node" with OpenScape 4000 switches managed by this OpenScape 4000 manager that have Users assigned to their (OpenScape 4000 switches) resources.

     "*You have requested to remove the HiPath OS4K Manager Node "Node_Name". The following OS4K Nodes with the respective associated subscribers assigned to Users are managed by this manager: (list_of_managed_nodes-subscribers_assigned_to_users). There are HiPath OS4K resources associated with the managed nodes of the selected OS4K Manager that are assigned to Users. The removal of the*

OS4K Manager node is not possible. Please unassign the HiPath OS4K resources from the Users first."

IMPORTANT:

When a OpenScape 4000 “Manager Node” is removed then all the associated OpenScape 4000 “Managed Node” are also removed from the system.

IMPORTANT:

When a OpenScape 4000 switch (node) is removed then all of its subscribers, Office Codes (Numbering Plans), Prefixes (Dial Plans) and BCFederations are deleted.

5) The OpenScape 4000 node is now removed.

4.4.6.4 How to configure routing of an OpenScape 4000 Node

How to configure routing of an OpenScape 4000 node:

Prerequisites

Adequate administrative permissions

User Management is installed to CMP

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 node connections available in the entire system is displayed in the workspace.

3) Click on the actions menu of the OpenScape 4000 node you wish to configure.

4) Click on **Configure Routing**

The dialog with the routing configuration view of the node opens.

5) Navigate to **Enable/Disable Routing Notifications** section and check or uncheck the checkbox in order to enable or disable the routing notifications for the node.

6) Navigate to **Mappings** section and select one **OpenScape 4000 External System ID**, one **OpenScape Voice Switch** and one of the **OpenScape Voice Office Codes** from the drop down menus.

NOTICE:

In case ’Pattern’ is selected in OpenScape Voice Office Codes then a new field where the administrator can put a free text matching pattern of wildcards :e.g. 30210818*. Wildcards supported are * and . while CMP validates the input that contains only digits and the . and * characters

7) Click on **Add** to add the mapping to the mappings list.

NOTICE:

If an OpenScape 4000 External System ID or an OpenScape Voice Switch is already used to a mapping the new one will not be added to mappings list.

8) Select the checkboxes of the mappings you want to delete and click on **Delete**.

The mappings are removed from the mappings list.

9) Click on the action menu of the mappings you want to move and click on **Move Up** or Move Down.

The mappings are moved to the new potisitions into the mappings list.

10) Click on **Synchronize**.

The following actions are performed:

- System fetches configured routes for the OpenScape 4000 Manager
- System fetches all OSV Phones from UC DB and cross checks the tow lists, synchronizing OpenScape 4000 Manager routing tables
- System provides progress bar for the procedure
- When the process completes system presents a Result Screen and offers a detailed result log for download.

NOTICE:

In order not to disturb custom made routes created by the administrator, the synchronization process only creates new routes and does not delete existing routes that do not match OSV Phones.

NOTICE:

Synchronization creates new entries when the routes for one OSV phone are not present in ALL OpenScape 4000 switches included in an external system configuration.

11) Click on **Save** to confirm the routing configuration.

NOTICE:

In case an external system correlation is changed, the system prompts to re-synchronize the routing entries. If yes is selected, system saves the configuration, triggers the synchronization and provides the progress bar for the procedure.

4.4.6.5 How to do a Full Synchronization of an OpenScape 4000 Node

You are able to trigger manually the Full synchronization of a OpenScape 4000 Node (“Manager / Managed / Self Managed”) from the Node list in CMP:

Prerequisites

Adequate administrative permissions

Synchronize the OpenScape 4000 Manager with the managed OpenScape 4000 nodes (Operation UPLOAD[6] via OpenScape 4000 Configuration Management)

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 node connections available in the entire system is displayed in the workspace.
3) Click on the actions menu of the OpenScape 4000 node you wish to synchronize.

[6] Following navigation directs you to Operation Upload:

a.Log on to the OS4K assistant

b.Navigate to Configuration Management-->Netwrok-->System

c. Press the search button to find the data for your OS4K system

d. Go to action menu and then press upload

4) Click on **Synchronize**

IMPORTANT:

If the Manager Node of a particular managed node supports Delta-sync, it shall not be possible to trigger full sync for this Node.

If you Synchronize a “Self Managed” or “Managed” OpenScape 4000 node then the Phone data, the Office Codes (Numbering Plans) and the Prefixes (Dial Plans) of the specific Node will be updated.

If you Synchronize a OpenScape 4000 “Manager” node then the following actions are performed:

- All OpenScape 4000 nodes managed by the OpenScape 4000 Manager are retrieved, synchronized and appear in the Node List.

  Phone data, the Office Codes (Numbering Plans) and the Prefixes (Dial Plans) of all specific Node are updated.
- If a new Managed Node is added then it appears as incomplete and additional Editing of this node is required as if it is been added manually.
- If an OpenScape 4000 Node is no longer managed by this Manager then it is removed and doesn’t appear on the Node List.

IMPORTANT:

All conditions for removing manually a Managed node are also applied when a OpenScape 4000 Managed node is removed during synchronization. These conditions are described in the relative chapter for Removing a OpenScape 4000 node.

IMPORTANT:

If the removal of a OpenScape 4000 Managed Node fails then the synchronization of its OpenScape 4000 Manager Node fails. When the removal fails because OpenScape 4000 resources of the Node are assigned to Users then the failure message displays the amount of these resources.

INFO:

You are advised to synchronize the OpenScape 4000 Manager to updated the Node List and the Node

resources unless you need to synchronize just a specific OpenScape 4000 “Managed” or a “Self Managed” Node.

When the synchronization is initiated, a progress window opens and a progress bar is displayed with the following information:

a) The current operation (i.e. synchronizing Nodes, synchronizing Phone data, synchronizing Office Codes (Numbering Plans) synchronizing the Prefixes (Dial Plans) etc.)
b) The current/remaining operations (i.e. 23/123)

NOTICE:

For each node, the synchronization can be initiated only once and each time only one Administrator User can initiate the synchronization of a specific node.

IMPORTANT:

If the progress window is closed and the user that initiated the synchronization returns to this node, the system displays the current progress.

5) When the Progress window is closed the Synchronization is completed

4.4.6.6 How to do a manual Delta Synchronization of an OpenScape 4000 Node

You are able to trigger manually a Delta synchronization of an OpenScape 4000 (OS4K) Node (“Manager / Self Managed”) from the Node list in CMP:

Prerequisites

Adequate administrative permissions

The OpenScape 4000 managing Node supports the Delta Synchronization (OS4K Manager/ (Enabled) OS4K Assistant v7.0 onward)

In order to have an up to date status of OS4K synchronize the OpenScape 4000 Manager with the managed OpenScape 4000 nodes (Operation UPLOAD[7] via OpenScape 4000 Configuration Management)

Step by Step

1) On the **Maintenance** navigation tab, click on the **Inventory**navigation menu item.

[7] Following navigation directs you to Operation Upload:

a.Log on to the OS4K assistant

b.Navigate to Configuration Management-->Netwrok-->System

c. Press the search button to find the data for your OS4K system

d. Go to action menu and then press upload

2) In the navigation tree, click on **Nodes & Applications** > **Nodes**.

   A list of all system nodes and 3rd party node connections available in the entire system is displayed in the workspace.

3) Click on the actions menu of the OpenScape 4000 node you wish to synchronize.

4) Click on **Synchronize Delta**

INFO:

The **Synchronize Delta** option is available only if the OS4K node supports it.

When the delta synchronization is initiated, a progress window opens and a progress bar is displayed with the current/remaining operations (i.e. 23/123)

NOTICE:

For each node, the synchronization can be initiated only once and each time only one Administrator User can initiate the synchronization of a specific node.

IMPORTANT:

If the progress window is closed and the user that initiated the synchronization returns to this node, the system displays the current progress.

---

5) When the Progress window is closed the Synchronization is completed and the Delta Synch timestamp is updated and stored by CMP so the automated Delta Synch will start after the configured time elapses.

IMPORTANT:

If the Delta Synch cannot be reported a major CMP alarm is raised and the delta synch is canceled. In this case the Administrator must trigger a Full Synchronization for the relevant OS4K Manager or Self Managed switch before the system initiates again the automated Delta Sync process.

4.4.6.7 How to configure the automated Delta Synchronization of an OpenScape 4000 Node

You are able to configure a Delta synchronization of a OpenScape 4000 (OS4K) Node (“Manager / Self Managed”) from the Node list in CMP:

Prerequisites

Adequate administrative permissions

The OpenScape 4000 managing Node supports the Delta Synchronization (OS4K Manager/ (Enabled) OS4K Assistant v7.0 onward)

The clocks of CMP & OS4K Manager/Assistant MUST be in sync

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 node connections available in the entire system is displayed in the workspace.
3) Click on the **Name** of the *Application* node

   The **Dashboard** type **Application** (in case of Standard Duplex, computer named is offboard) opens.
4) Click on **Show services status: – Show**.

   A dialog opens that displays a list of all components that are available for the selected system node:

   - **Component**

     The name of the component is displayed
   - **Critical** to **Normal**

     Shows the quantity and severity of alarms signaled on the system unit
   - **State**

     Displays whether the component is currently started ( ) or stopped ( )
   - **Version**

     The version of the component is displayed.
5) Select the checkbox of the **Hipath4kNodeManager Service**.

INFO:

You can search for OpenScape 4000 related instance files by entering *h4k“*” in the search field and click on **Go**

---

6) Click on **Edit**.

The dialog with the settings of the **Hipath4kNodeManager Service** opens.

Only the following value can be configured:

- **DeltaSyncInterval**

  This is the period of time (in minutes) that CMP requests a DELTA of the changes that have happened on the OS4K Manager/Assistant after a given time(stamp). Default value is 10 (minutes)

  The automated Delta Synch mechanism is based on the established SOAP interface and the timestamp comparison between CMP and OS4K Manager/Assistant:

  -CMP stores the local timestamp of the last delta sync and provides it to the OS4K Manager/Assistant

  - OS4K Manager /Assistant compares its local time with the delivered timestamp to determine the period in which changes are requested.

  - Subsequent delta sync is triggered after the DeltaSyncInterval time is elapsed from the last Sync.

IMPORTANT:

It is necessary to have both CMP and OS4K Manager clocks synchronized so it is recommended that the administrator configures both CMP and OS4K Manager to use a NTP server for the synchronization of the clocks.

NOTICE:

If a delta sync is running and a full sync is requested, the delta sync is canceled. Timestamp is reset to the time the full sync was initiated.

NOTICE:

If a delta sync is running and a manual delta sync is requested then the manual delta sync is not permitted.

---

7) Click on **Save** to copy the entries to the system's database.

IMPORTANT:

If the Delta Synch cannot be reported a major CMP alarm is raised and the delta synch is canceled. In this case the Administrator must trigger a Full Synchronization for the relevant OS4K Manager or Self Managed switch before the system initiates again the automated Delta Sync process.

4.4.7 SNMP Node

An OpenScape system can add an SNMP node by entering IP address, SNMP Community String and support for Software Subscription License (SSL).

You can also edit an already Configured SNMP Node that apperas in the Node list by using the actions menu ‣

NOTICE:

SNMP nodes are not available in case of JTIC (Joint Interoperability Test Command) deployment.

4.4.7.1 How to Add an SNMP Node

How to add an SNMP node:

Prerequisites

Adequate administrative permissions

The system is not a JITC 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 node connections available in the entire system is displayed in the workspace.
3) Click on **Add SNMP node**.

   The dialog with the link settings opens.
4) Following atributes are required to configure the node:
   - **Name**
   - **Node IP**
   - **SNMP Com. String**

     IMPORTANT:

     SNMP Com. String field is case sensitive (e.g. value *“Public”* is different from value *“public”*).
   - **Port (default value is 161)**

   If the SNMP Node will support Software Subscription License (SSL) then following attributes are also mandatory

   a) **SSL SNMP Community String**

   a) **SSL Port (default value is 161)**
5) Click on **Save** to copy the entries to the system's database.

IMPORTANT:

Two or more SNMP agents may exist on the same server but should listen to different ports. This port restriction holds both for the SNMP and the SSL port.

4.4.7.2 How to Modify an SNMP Node

How to modify an SNMP node:

Prerequisites

Adequate administrative permissions

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 node connections available in the entire system is displayed in the workspace.
3) Click on the actions menu of the SNMP node you wish to Edit.
4) Click on **Edit**

   The dialog with the node settings opens.
5) Following atributes of the Xpressions node can be modified:
   - **Name**
   - **Node IP**
   - **SNMP Com. String**

     IMPORTANT:

     SNMP Com. String field is case sensitive (e.g. value *“Public”* is different from value *“public”*).
   - **Port** (default value is 161)

   If SNMP Node supports Software Subscription License (SSL) then following attributes are also mandatory:

   a) **SSL SNMP Community String**

   a) **SSL Port** (default value is 161)
6) Click on **Save** to copy the entries to the system's database.

IMPORTANT:

Two or more SNMP agents may exist on the same server but should listen to different ports. This port restriction holds both for the SNMP and the SSL port.

4.4.7.3 How to display the Processes running on a SNMP Node

You can display the list of all processes running on a SNMP node:

Prerequisites

Adequate administrative permissions to manage Nodes in CMP

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 node connections available in the entire system is displayed in the workspace.
3) Click on the Name of the SNMP node you want to display the list of processes running.

   The SNMP dashboard opens.
4) Click on the **Running Services** button in the **Actions** area

   A list of the processes running on this SNMP node is displayed with following info:

   - **ID**

     Name

     Parameters

     Path

     Status

     Type

NOTICE:

The list is displayed according to the **Item/page** value of the window.

4.4.7.4 How to display the Packages Installed on a SNMP Node

You can display the list of all packages installed on a SNMP node:

Prerequisites

Adequate administrative permissions to manage Nodes in CMP

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 node connections available in the entire system is displayed in the workspace.

3) Click on the Name of the SNMP node you want to display the list of installed packages.

   The SNMP dashboard opens.

4) Click on the **Installed Packages** button in the **Actions** area

   A list of the packages installed on this SNMP node is displayed with following info:

   - **Installation Date**

     ID

     Name

     Type

NOTICE:

The list is displayed according to the **Item/page** value of the window.

4.4.7.5 How to Remove an SNMP Node

How to remove an SNMP node from Node List :

Prerequisites

Adequate administrative permissions to manage Nodes in CMP

The selected “be removed” node dosen’t have an active Software Subscription License (SSL) connection

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 node connections available in the entire system is displayed in the workspace.
3) Click on the actions menu of the SNMP node you wish to remove.
4) Click on **Remove Node**

   You are requested to confirm the following by clicking **OK**:

   “You have requested to remove the Generic SNMP Node "Node_Name”

   or if the SNMP node is supporting SSL:

   “You have requested to remove the Generic SNMP Node "Node_Name. This node supports SSL. The collection of SSL data will stop. Any SSL related information will not be removed from the system”
5) SNMP node is now removed.

4.4.8 System Dashboard overview

The dashboard contains detailed information on a selected system node. This detailed information includes for example hardware information, alarm information, installed applications and their software level.

System Dashboards are divided into the following types:

4.4.8.1 How to Display the Dashboard of a System Node

The dashboard view suits for the administrator as well as for the service technician to get a quick and global overview of the selected sytem node.

Prerequisites

Adequate administrative permissions

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 dialog with the dashboard of the selected system node opens.

IMPORTANT:

In case a version Upgrade is in progress for an OpenScape Voice node then its dashboard is greyed out until the Upgrade is completed.

4.4.8.2 The Application Dashboard

The **Dashboard** type **Application** (in case of Standard Duplex, computer named is offboard), provides a variety of performance and system information.

The **Application** dashboard consists of the following areas:

Dashboard <name>

Contains the **Note** for the specific Node.

Alarm summary:

The following information is provided:

- Number of **Critical** alarms (red).
- Number of **Major** alarms (orange).
- Number of **Minor** alarms (yellow).

- Number of **Warning** alarms (cyan).

System Info

The system info presents the following information:

- If the "***Node runs on a Virtual Machine***" it is stated in the info field.
- **CPU** (Central Processing Unit):

  This is the percentage of CPU usage. This is snapshot information for a small period. Depending on the system load it will indicate from 0% to 100% of usage.
- **Memory**:

  This is the percentage of RAM memory use - a snapshot information for a small period. Depending on the system load it will indicate from 0% to 100% of usage.
- **Date/Time**

  Shows the time at the system.
- **Last Reboot**

  It shows date and time of latest system reboot.

Applications

The application **Name**, **Timestamp of Installation or Sync** and the **Software Version** are displayed with the following naming convention:

Vx Ry.p.e

Where :

x=Major Release

y=Minor Release

p=Patchset

e=Emergency Patch

For example V7 R1.5.2 means Version 7, minor release 1, patchset 5, emergency patch 2

Actions

The **Actions** section provides various buttons to display advanced information. The following options are available:

- UC Rapidstat.
- Show services status.
- Show software packages.
- Backup version
- Synchronize versions

SIEL-IDs

The **SIEL-IDs** section contains the SIEL-IDs values which are retrieved via license service from the imported license files to CMP server. OpenScape Branch, OpenScape UC Application and OpenScape Common Management Platform can be included.

4.4.8.3 The Frontend Dashboard

The **Dashboard** for **Frontend** provides different system information. Several subwindows provide advanced information.

The **Frontend** dashboard consists of the following areas:

Dashboard <name>

Contains the **Note** for the specific Node.

Alarm summary:

The following information is provided:

- Number of **Critical** alarms (red).
- Number of **Major** alarms (orange).
- Number of **Minor** alarms (yellow).
- Number of **Warning** alarms (cyan).

System Info

The system info presents the following information:

- If the "***Node runs on a Virtual Machine***" it is stated in the info field.
- **CPU** (Central Processing Unit):

  This is the percentage of CPU usage. This is snapshot information for a small period. Depending on the system load it will indicate from 0% to 100% of usage.
- **Memory**:

  This is the percentage of RAM memory use - a snapshot information for a small period. Depending on the system load it will indicate from 0% to 100% of usage.
- **Date/Time**

  Shows the time at the system.
- **Last Reboot**

  It shows date and time of latest system reboot.

Applications

The application **Name** and the **Software Version** are displayed with the following naming convention:

Vx Ry.p.e

Where :

x=Major Release

y=Minor Release

p=Patchset

e=Emergency Patch

For example V7 R1.5.2 means Version 7, minor release 1, patchset 5, emergency patch 2

Actions

The **Actions** section provides various buttons to display advanced information. The following options are available:

- Show services status.
- Show software packages.

4.4.8.4 The Communication System Dashboard

The **Dashboard** type **Communication System** (OpenScape Voice), provides a variety of performance and system information.

This dashboard consists of the following areas:

Dashboard <name>

Contains the **Note** for the specific Node.

Alarm summary:

The following information is provided:

- Number of **Critical** alarms (red).
- Number of **Major** alarms (orange).
- Number of **Minor** alarms (yellow).
- Number of **Warning** alarms (cyan).

System Info

The system info presents the following information:

- If the "***Node runs on a Virtual Machine***" it is stated in the info field.
- **CPU** (Central Processing Unit):

  This is the percentage of CPU usage. This is snapshot information for a small period. Depending on the system load it will indicate from 0% to 100% of usage.
- **Memory**:

  This is the percentage of RAM memory use - a snapshot information for a small period. Depending on the system load it will indicate from 0% to 100% of usage.
- **Date/Time**

  Shows the time at the system.
- **Last Reboot**

  It shows date and time of latest system reboot.

Applications

The application **Name** and the **Software Version** are displayed with the following naming convention:

Vx Ry.p.e

Where :

x=Major Release

y=Minor Release

p=Patchset

e=Emergency Patch

For example V7 R1.5.2 means Version 7, minor release 1, patchset 5, emergency patch 2

Actions

The **Actions** section provides various buttons to display advanced information. The options (buttons) that are shown on the dashboard depend on the deployment and include:

- OSV Rapidstat.
- Core Network Interface
- Show/Change Node status
- Show services status
- Show software package
- UC Rapidstat
- Backup version
- Synchronize versions
- Configure hardware.

NOTICE:

You may find additional info on these buttons at the relevant OSV Administration Manual under chapter *System Dashboard overview*.

SIEL-IDs

The **SIEL-IDs** section contains the SIEL-ID value which is retrieved via SNMP from the OpenScape Voice imported license file to OpenScape Voice node.

4.4.8.5 The OpenScape 4000 Dashboard

The **Dashboard** type **OpenScape 4000** contains a variety of performance and system information.

The **OpenScape 4000** dashboard consists of the following areas:

Dashboard <name>

Contains the **Note** for the specific Node.

System Info

The system presents the following information:

- **CPU** (Central Processing Unit):

  This is the percentage of CPU usage. This is snapshot information for a small period. Depending on the system load it will indicate from 0% to 100% of usage.

- **Memory**:

  This is the percentage of RAM memory use - a snapshot information for a small period. Depending on the system load it will indicate from 0% to 100% of usage.
- **Software Version**

  Shows the software version for this node.
- **Last Update on**
- **Last Reboot**

NOTICE:

The dashboard is not real time and the update frequency is controlled by the 4K system.

Alarm summary:

The following information is provided:

- Number of **Critical** alarms (red).
- Number of **Major** alarms (orange).
- Number of **Minor** alarms (yellow).
- Number of **Warning** alarms (cyan).

Status

The system presents the following status information:

- **Backup**
- **DB sync**
- **APE**
- **License**

4.4.8.6 The Media Server Dashboard

The **Media Server Dashboard** type provides a variety of performance and system information.

The **Media Server** dashboard consists of the following areas:

Dashboard <name>

Contains the **Note** for the specific Node.

Alarm summary:

The following information is provided:

- Number of **Critical** alarms (red).
- Number of **Major** alarms (orange).
- Number of **Minor** alarms (yellow).
- Number of **Warning** alarms (cyan).

System Info

The system info presents the following information:

- If the "***Node runs on a Virtual Machine***" it is stated in the info field.
- **CPU** (Central Processing Unit):

  This is the percentage of CPU usage. This is snapshot information for a small period. Depending on the system load it will indicate from 0% to 100% of usage.
- **Memory**:

  This is the percentage of RAM memory use - a snapshot information for a small period. Depending on the system load it will indicate from 0% to 100% of usage.
- **Date/Time**

  Shows the time at the system.
- **Last Reboot**

  It shows date and time of latest system reboot.

Applications

The application **Name** and the **Software Version** are displayed with the following naming convention:

Vx Ry.p.e

Where :

x=Major Release

y=Minor Release

p=Patchset

e=Emergency Patch

For example V7 R1.5.2 means Version 7, minor release 1, patchset 5, emergency patch 2

Actions

The **Actions** section provides various buttons to display advanced information. The following options are available:

- Show services status.
- Show software packages.

4.4.8.7 The Xpressions Dashboard

The **Xpressions Dashboard** provides the basic system information.

The **Xpressions** dashboard consists of the following areas:

Dashboard <name>

Contains the **Note** for the specific Node.

System Info

System info includes the following information:

- **Memory**:

  This is the percentage of RAM memory use - a snapshot information for a small period. Depending on the system load it will indicate from 0% to 100% of usage.
- **OS. Version**

  Displays the Operating System version of the Xpression server.
- **Type**.

  Shows the Xpression system type: **Voice** or **UMS** (Unified Messaging Server). This value is set via Xpressions Web Assistant, **Special Server Settings** > **System Type** (for more information see the Chapter “System Type” in OpenScape Xpressions V7 Web Assistant, User Guide.)

4.4.8.8 The RG8700 Dashboard

The **Dashboard** type **Gateway** provides a variety of performance and system information.

The **Gateway** dashboard consists of the following areas:

Dashboard <name> <IP address>

Contains the **Note** for the specific Node.

Alarm summary:

The following information is provided:

- Number of **Critical** alarms (red).
- Number of **Major** alarms (orange).
- Number of **Minor** alarms (yellow).
- Number of **Warning** alarms (cyan).

System Info

The system info presents the following information:

- **Blade 1 - CPU 1** (Central Processing Unit):

  This is the percentage of CPU 1 usage. This is snapshot information for a small period. Depending on the system load it will indicate from 0% to 100% of usage.
- **Blade 1 - CPU 2**(Central Processing Unit):

  This is the percentage of CPU 2usage. This is snapshot information for a small period. Depending on the system load it will indicate from 0% to 100% of usage.
- **Blade 1 - Memory 1**:

  This is the percentage of RAM memory use - a snapshot information for a small period. Depending on the system load it will indicate from 0% to 100% of usage.
- **Blade 1 - Memory 2**:

  This is the percentage of RAM memory use - a snapshot information for a small period. Depending on the system load it will indicate from 0% to 100% of usage.

- **Blade 1 - Uptime**:

  This field displays the date and time of the last reboot of the RG 8700.
- **Facilities**

  Amount of ethernet ports the RG8700 has. Possible values are 2, 8 or 16
- **Date/Time**

  Shows the date and time at the system.

Status

The system presents the following status information of RG8700:

- **Redundancy Configuration**

  This field displays the Redundancy Configuration status. Possible Redundancy Configuration statuses are:

  – **Standalone**
  – **Redundant**
- **Gateway Operational Status**

  This field displays the current Gateway Operational status of RG 8700. Possible Gateway operational statuses are:

  – **booting**
  – **provisioning**
  – **outOfService**
  – **inServiceNonRedundant**
  – **inServiceRedundant**
- **Operational Status Blade 1**

  This field displays the current operational status of this RG 8700's module. Possible operational statuses are:

  In Service - The blade is completely operational, and all resources are available for use

  Standby - (Only for the secondary RG 8700s) The secondary (backup) RG 8700 is ready to back up the corresponding primary RG 8700.

  Synching - The database on the secondary (backup) RG 8700 is being synchronized with the database on the active (primary) RG 8700.

  Out Of Service - The blade is not operational, and no resources are available for use.

  Reset - The blade is going through initialization. The blade will automatically transition to the "**Out of Service**" state on completion of its initialization sequence.

  Failed - The blade has encountered a catastrophic failure. The blade will remain in this state until operator intervention has cleared the problem.

  Empty - The blade does not currently have a physical existence. The blade is actually empty, or the blade is so badly damaged that it cannot be recognized. The blade is available for configuration, but will not transition from this state until the RG 8700 is populated.

Applications

The application **Name** and the **Software Version** are displayed.

4.4.8.9 The SNMP Dashboard

The **Dashboard** for SNMP provides a variety of performance and system information.

The SNMP dashboard consists of the following areas:

Dashboard <name>

Contains the **Note** for the specific Node.

System Info

The system info presents the following information:

- **Node Name**
- **Node Description**

  This is the percentage of RAM memory use - a snapshot information for a small period. Depending on the system load it will indicate from 0% to 100% of usage.
- **Date/Time**

  Shows the time at the system.
- **System Uptime**:

  This is the time of system usage (how long the system has been in operation). If the system uptime is more than one day, it shows days, hours and minutes: "d days hh:mm". If the system uptime is less than one day, only hours and minutes are displayed: "hh:mm".
- **Total Memory**

Actions

The **Actions** section provides various buttons to display advanced information. The following options are available:

- **Running Services**.
- **Installed Packages**.

4.4.9 How to Display/Edit Component Settings

You can display general information and the properties for each component of a system node. Some information and properties can also be changed. This depends on the component concerned. How to display and if necessary edit a component:

Prerequisites

Adequate administrative permissions

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.

4) Click on the name of the system node for which you want to edit component settings.

   A dialog with the dashboard of the selected system node opens.

5) Click on **Show services status: – Show** under **Actions** .

   NOTICE:

   Components are not available for all nodes.

   A dialog opens that displays a list of all components that are available for the selected system node:

   - **Component**

     The name of the component is displayed
   - **Critical** to **Normal**

     Shows the quantity and severity of alarms signaled on the system unit
   - **State**

     Displays whether the component is currently started ( ) or stopped ( )
   - **Version**

     The version of the component is displayed.

   NOTICE:

   The status reported along with every service relates to whether the service is up-running/stopped/disabled. This status is not necessarily impacted by the existence of alarms that may be associated with this service.

6) Select the checkbox of the component the settings of which you want to edit.

7) Click on **Edit**.

   The dialog with the settings of the component opens.

8) Change the desired settings,

   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.

   NOTICE:

   Some component settings may not be changeable.

9) Click on **Save** to copy the entries to the system's database.

4.4.9.1 How to configure the SNMP Service Settings

You can configure specific settings of the SNMP Service instance file running on the Application Server in order to customize the community string based authentication, the receiving port, the reloading frequency of data and the option to send a heartbeat trap to the alarm destinations at predefined intervals:

Prerequisites

Adequate administrative permissions

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 Application Server node for which you want to edit SNMP Agent settings.

   A dialog with the Application Server dashboard opens.
4) Click on **Show services status: – Show**.

   A dialog opens that displays a list of all components that are available for the selected system node:

   - **Component**

     The name of the component is displayed
   - **Critical** to **Normal**

     Shows the quantity and severity of alarms signaled on the system unit
   - **State**

     Displays whether the component is currently started ( ) or stopped ( )
   - **Version**

     The version of the component is displayed.
5) Select the checkbox of the **SNMP Service**.

INFO:

You can search for all SNMP related instance files by entering “snmp*” in the search field and click on **Go**

---

6) Click on **Edit**.

The dialog with the settings of the SNMP-Agent opens.

Following values can be configured:

- **CleanupSnmpTrapsTime**

  Enter the value of the SNMP traps messages that are stored on the Application Server.

  Default value is “336 hours”

  IMPORTANT:

  Community string fields are case sensitive (e.g. value *“Public”* is different from value *“public”*).

- **CommunityName**

  Enter the community string value for the SNMP Agent off the Application Server.

  Default value is “public”

  IMPORTANT:

  Community string fields are case sensitive (e.g. value *“Public”* is different from value *“public”*).

- **NodeSupervisorInterval**

  Enter the value about how often the UC to poll/check the status of the Nodes, as well as the Services. This check is taking place through SNMP.

  Minimum value is “300” (seconds)

  Maximum value is “3600” (seconds)

  Default value is “600” (seconds)

- **ReloadSysDataAutomatically**

  Enter the frequency value for SNMP Service reloading its data (in seconds)

  Default value is “3600” (seconds)

- **RequestReceivingPort**

  Enter the value of the SNMP Agents receiving port.

  Default value is “8167”

  IMPORTANT:

  If you change the **RequestReceivingPort** value a restart is necessary for the change to take effect.

- **SendHeartBeatTrapInterval**

  Enter the frequency value for Heart Beat Trap to be sent (in seconds).

  Default value is “600” seconds

  IMPORTANT:

Minimum value you should enter for field **SendHeartBeatTrapInterval** is 30 seconds. If you enter less than 30 seconds the system will override your entry and use the 30 second value even if the displayed value is less.

- **StartHeartBeatTrap**

  You can enable the Heart Beat Trap[8]function SNMP agent to optionally send a heartbeat trap to the alarm destinations at predefined intervals.

  Default value is “false”. To start it value must be set to “true”

7) Click on **Save** to copy the entries to the system's database.

NOTICE:

All changes take effect when you save them.

Restart is necessary only if you change the value **RequestReceivingPort**

4.4.9.2 How to configure the Personal Workflow Controls Factory component Settings

You can configure specific settings of the Personal Workflow Controls Factory component instance file running on the Application Server.

Prerequisites

Adequate administrative permissions

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 Application Server node for which you want to edit Personal Workflow Controls Factory component settings.

A dialog with the Application Server dashboard opens.

8 Optional function in which SNMP agent sends a heartbeat trap to the alarm destinations at predefined intervals

You have defined the Alarms Destinations in the following section:

Maintenance > **Monitoring** > **Alarms** > **Destinations**

4) Click on **Show services status: – Show**.

   A dialog opens that displays a list of all components that are available for the selected system node:

   - **Component**

     The name of the component is displayed
   - **Critical** to **Normal**

     Shows the quantity and severity of alarms signaled on the system unit
   - **State**

     Displays whether the component is currently started ( ) or stopped ( )
   - **Version**

     The version of the component is displayed.

5) Select the checkbox of the **Personal Workflow Controls Factory component**.

   INFO:

   You can search for all Personal Workflow related instance files by entering “personal workflow*” in the search field and click on **Go**

   ---

6) Click on **Edit**.

   The dialog with the settings of the Personal Workflow Controls Factory component opens.

   Following values can be configured:

   - **BCOMWorkflowTimeout**

     Enter the used time out for BCOM requests.

     Default value is “60000 (milliseconds)”
   - **BusyOnBusy**

     If set to false, caller is routed to next preferred device if callee is busy on first device.

     If set to true, caller gets busy tone if the callee is busy at one device.

     Default value is “false”
   - **LoopDetectionEnabled**

     If set to false, BCOM loop detection will be disabled.

     If set to true, BCOM loop detection will be enabled.

     Default value is “false”

7) Click on **Save** to copy the entries to the system's database.

4.4.10 How to Start / Stop Components

You can start or stop components. A component is only started/stopped for the system node you have selected. The change takes effect immediately.

Prerequisites

Adequate administrative permissions

IMPORTANT:

If you are inexperienced in starting and stopping components, the entire system may have to be restarted as a result. Therefore, start and stop components only if the documentation or service personnel ask you to do so. In some cases you cannot stop and / or start a single component. This requires an individual start or stop sequence with other components then, which is described in the relevant start / stop instructions.

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 for which you want to start or stop a component.

   A dialog with the dashboard of the selected system node opens.
4) Click on **Show services status: – Show** under **Actions**.

   NOTICE:

   This option is not available for all nodes.

   A dialog opens that displays a list of all components that are available for the selected system node. The **State** column displays whether the component is currently started ( ) or stopped ( ).
5) Select the checkboxes of the components you want to start or stop.
6) Click on **Start / Stop**.

   IMPORTANT:

   This step stops or starts the selected components without any further query.

If the selected components were started, they will now be stopped. If they were stopped, they will now be started.

4.4.11 How to Restart a Component

You can start or stop components. If you stop a component and would then like to restart it again, you can also do this with the unique **Restart** feature. The change takes effect immediately.

Prerequisites

Adequate administrative permissions

IMPORTANT:

If you are inexperienced in starting and stopping components, the entire system may have to be restarted as a result. Therefore, start and stop components only if the documentation or service personnel ask you to do so. In some cases you cannot stop and / or start a single component. This requires an individual start or stop sequence with other components then, which is described in the relevant start / stop instructions.

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 for which you want to restart a component.

   A dialog with the dashboard of the selected system node opens.
4) Click on **Show services status: – Show** under **Actions**.

   NOTICE:

   This option is not available for all nodes.

   A dialog opens that displays a list of all components that are available for the selected system node. The **State** column displays whether the component is currently started ( ) or stopped ( ).
5) Select the checkboxes of the components you want to restart.
6) Click on **Restart**.

   IMPORTANT:

   This step stops and restarts the selected components without any further query.

The selected components are stopped and immediately restarted.

4.4.12 How to Restart System Nodes

You can restart all components of a system node with a single command. The change takes effect immediately.

Prerequisites

Adequate administrative permissions

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 **>** to open the actions menu of the node you wish to restart.

   NOTICE:

   This option is not available for all nodes.
4) Click on **Restart Node**.

   IMPORTANT:

   This step stops and immediately restarts the selected system node without any further query.

All components of the selected system node are stopped and immediately restarted.

4.4.13 How to Move a System Node to a Node Group

You can move a system node to a predifined Node Group.

Prerequisites

Adequate administrative permissions

You have created Node Group(s).

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 **>** to open the actions menu of the node you wish to move to a group.

4) Click on **Move to group**.

   A list of all the available groups are displayed.

5) Click the radio button of the group you want to move the selcted node.

6) Click on **Save**

   The node is moved to the group.

4.4.14 How to Configure the Note for a System Node

How to configure the note field for a System Node:

Prerequisites

Adequate administrative permissions

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, you want to configure the note for.

   A dialog with the dashboard of the selected system node opens.

4) Select **Edit** to configure the note.

   The note dialog opens.

5) Specify the desired note under **Edit note**.

6) Select **OK** to save the note.

The new note is displayed in the node's dashboard.

4.4.15 Software Package Overview

The software packet overview displays which software packages are installed on a selected system node of the OpenScape system.

The software packet overview is domain-spanning. It cannot be used by service provider administrators, since these administrators should not be in a position to display the installed components.

What software packets are displayed in the overview depends on the node you open the software packet overview for.

For each software packet the following information is displayed:

- **Software**

  Displays the name of the corresponding software packet.

- **Version#Build**

  Displays the version and build number of the corresponding software packet.

- **Installation Media**

  Displays from what medium the corresponding software packet was installed. If the corresponding RPM packet was installed manually the value **unknown** is shown.
- **Date** (Installation Media)

  Displays when the corresponding software packet was installed.
- **Update Media**

  Displays from what medium the corresponding software packet was updated. If the corresponding RPM packet was updated manually the value **unknown** is shown.
- **Date** (Update Media)

  Displays when the corresponding software packet was updated. If no date is displayed, the software packet has never been updated so far.

If a text is not fully displayed, you can display the full text as tool tip. To open the tool tip move the mouse pointer over the truncated text.

4.4.15.1 How to Display Software Packages

The software packet overview displays which software packages are installed on the available system nodes.

Prerequisites

Adequate administrative permissions

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 for which you want to display the software packages.

A dialog with the dashboard of the selected system node opens.

4) Click on **Show software packages: – Show** under **Actions**.

A dialog opens that displays a list of all software packages that are installed on the selected system nodes.

NOTICE:

The list is displayed according to the **Item/page** value of the window.

---

5) In order to view the whole package name for one of the list entries, place the mouse pointer for a few seconds on top of the concerning entry.

4.4.16 How to Activate Backup version

The multi-partitioning functionality provides the capability to have two versions installed on the same system, where one version is installed on the primary partition and another version, on the secondary partition. This chapter describes how to manage the versions (e.g. see the current installed versions, distinguish between active and backup version and activate backup version).

Prerequisites

Adequate administrative permissions

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 available system nodes and 3rd party system connections is displayed in the work area.
3) Click on the **Name** of the system node for which you want to activate the backup version.

   A dialog with the **Dashboard** of the selected node opens.
4) A list of all installed versions is displayed under the **Dashboard Applications** area.

   NOTICE: Only one version is Active at a time and the other version is used as a Backup.
5) Under **Actions** area, click on **Activate** for Backup version.

   Activate Passive pop-up window is displayed, asking to confirm the selection, since the system will be rebooted.
6) Click **OK** to start the activation of the backup version.

   System returns the summary of the **Activate Passive** process.

   NOTICE:

   In case of a failure, system reports the error and the administrator is prompted to contact the next level of technical support.
7) Click **Close** on **Activate Passive** pop-up window and wait for system reboot.

   NOTICE: In case of integrated simplex, during system's reboot, Application dashboard is not available. Once the reboot is completed the administrator has to re-login in CMP and navigate again to Application dashboard.

   The Application **Dashboard** is refreshed and since system is unavailable, no option is available.
8) The system becomes available again and the administrator refreshes the **Dashboard**.

The **Application** area on the **Dashboard** shows that the ex-backup version became an active version now.

4.4.17 How to Synchronize versions

This Chapter describes How to synchronize the Active version to Backup version.

Prerequisites

Adequate administrative permissions

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 available system nodes and 3rd party system connections is displayed in the work area.
3) Click on the **Name** of the system node for which you want to perform the synchronization.

   A dialog with the **Dashboard** of the selected node opens.
4) A list of all installed versions is displayed under the **Dashboard Applications** area.

   NOTICE: Only one version is Active at a time and the other version is used as a Backup.

5) Under **Actions** area, click on **Synchronize** for Synchronize versions.

   Synchronize Partitions pop-up window is displayed, asking for the confirmation, since the existing data in Backup version will be overwritten by the data from Active version.
6) Click **OK** to start version synchronization.

   System displays **Synchronize Partitions** window with the information about synchronization progress.

   NOTICE: Once version synchronization ends, system returns the following message: `The version synchronization is completed`.

7) Click **Close** to close the **Synchronize Partitionss** pop-up window.

The **Application** area on the **Dashboard** is refreshed and it shows that backup version is synchronized with the active version.

4.4.18 How to Display Applications

How to display the application installed for the OpenScape system:

Prerequisites

Adequate administrative permissions

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** > **Applications**.

You see all applications that are installed for the OpenScape system with the following info:

Application Icon	Type	Active version	Node	IP address/ Hostname
The icon of the application	Application Type depends on the node it is running on. Third Party Applications are also in the list.	Active Version[9] of the Application running on the Nodes	The node name on which the Application is running on. In case the deployment has more nodes ,hosting this Application ,they are also displayed.	The IP address or Hostname of the nodes the Applications are running on. For third party Applications this field is empty.

IMPORTANT:

In case a version Upgrade is in progress for an OpenScape Voice cluster then the **Active version** field displays: `Upgrade Version in progress...` and the **Software Activation** option from the Action menu is de-activated.

[9] The **Activation Version** is displayed with the following naming convention:

Vx Ry.p.e

Where :

x=Major Release, y=Minor Release, p=Patchset,e=Emergency Patch

For example V7 R1.5.2 means Version 7, minor release 1, patchset 5, emergency patch 2

4.4.19 How to Execute an Action for an Application

How to execute an action for an Application:

Prerequisites

Adequate administrative permissions

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** > **Applications**.

   You see all applications that are installed for the OpenScape system.
3) In the list entry of the desired application click on ‣ to open the application's action menu.
4) Select the desired action in the action menu.

The action selected for the relevant application starts.

NOTICE:

What actions are available depends on the relevant application you have chosen.

IMPORTANT:

In case a version Upgrade is in progress for an OpenScape Voice cluster then the **Active version** field displays: `Upgrade Version in progress...` and the **Software Activation** option from the Action menu is de-activated.

4.4.20 OpenScape External Applications

Common Management Platform integrates the following external applications in its User Interface with a Single-Sign-On (SSO) process:

- OSc Fault Management
- OSc Performance Management
- OSc Accounting
- Device Management (OpenScape Deployment Service)

To activate the buttons of the following external applications you must configure their connection beforehand:

- on the CMP Navigation Bar

  the **Fault Management** button opens *OSc Fault Management*

  the **Performance Management** button opens *OSc Performance Management*

  the **Accounting** button opens *OSc Accounting*
- and on the Navigation menu under the Configuration tab

  the **Device Management** button opens *OSc Deployment Service*

NOTICE:

OSc Fault Management and OSc Performance Management run on the same instance so only the Fault Management connection needs to be configured for both external applications and only **OpenScape FM** appears in the Applications list.

IMPORTANT:

After a CMP backup/restore action the Single Sign On process is corrupted so you will have to establish a new connection with the external application.

IMPORTANT:

If you want to remove the connection to an external application or re-access an external applications' configured entry, by selecting **Configured connection**, you must enter a valid Username and password for this external application.

4.4.20.1 How to create a Connection with OpenScape Fault Management or OpenScape Performance Management

How to create a connection with OSc Fault Management or OpenScape Performance Management:

Prerequisites

Adequate administrative permissions

OpenScape Fault Management is registered as an application in CMP with a `OSc FM rpm`

From OSc FM version V8 R0.61.01 onwards OpenScape FM performs a more restrictive check of SSL certificates. This requires some manual configuration steps if self-signed certificates are used. Such certificates can not be verified automatically by the system so the Administrator must follow the steps described in OSc FM manual chapter *" How to configure single sign on (SSO) from CMP to OpenScape FM with self-signed certificates "*

IMPORTANT:

OpenScape Performance Management runs as a different process on the same instance of the operating system Fault

Management is running on, and is delivered in the same package.

IMPORTANT:

During installation Single Sign On is enabled towards OSc FM and CMP is registered with OSc FM

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** > **Applications**.

   You see all applications that are installed for the OpenScape system.

   NOTICE:

   OSc Fault Management and OSc Performance Management run on the same instance so only the Fault Management connection needs to be configured for both external applications and only **OpenScape FM** appears in the Applications list.

3) In the list entry of OpenScape FM click on ‣ to open the application's action menu.

4) Select the **Create connection** action in the action menu.

   The Create Connection - OpenScape FM dialogue opens and following mandatory fields values must be entered:

   - **IP Address/Hostname:**

     Enter the IP address or Hostname of OpenScape FM application you are going to connect to CMP.
   - **Port**

     Enter the Port of the OpenScape FM application you are going to connect to CMP.

     Navigate to the CMP area of the Register section and enter the following:
   - **IP Address/Hostname:**

     Enter the **IP address** or **Hostname** of the CMP server that can be accessed by OpenScape FM
   - **Port**

     Enter the **Port** of the CMP server that can be accessed by OpenScape FM

     IMPORTANT:

     IP Address and **Port** of CMP is populated automatically in these fields but can be edited if necessary.

     Navigate to the **OpenScape FM** area of the Register section to enter the credentials OpenScape FM requires to register CMP:
   - **Username**

     This is the Username OSc FM is expecting so it will allow registration of CMP
   - **Password**

     This is the Password OSc FM is expecting so it will allow registration of CMP

5) Click on the **Retrieve Certificate** button to complete the connection

   The Certificate dialoge opens

6) Click on **Accept Certificate** button

   The field next to **Retrieve Certificate** button is green and **Save** button is now active

7) Click on **Save** to establish the connection with OSc FM

Next steps

The connection is established with OSc FM but this external application requires the appropriate permissions before it is accessed. You must therefore have an OpenScape FM profile assigned to the Administrator User before attempting the access to OpenScape Fault Management application or assign it as described below:

Navigate to **Configuration** > **CMP** > **General** > **Administrators** > **List** click on the **Login Name** of the Administrator User and click on **Profile** tab. **Assign** a OpenScape FM profile to the Administrator User.

NOTICE:

You can choose from the predefined OpenScape FM profiles or customize an OpenScape FM profile from the Profiles page.

4.4.20.2 How to configure a Connection with OpenScape Fault Management

How to confirure a connection with OSc Fault Management:

Prerequisites

Adequate administrative permissions

CMP has already a connection established with OSc FM

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** > **Applications**.

   You see all applications that are installed for the OpenScape system.
3) In the list entry of **OpenScape FM** click on ‣ to open the application's action menu.

4) Select the **Configure connection** action in the action menu.

   The Configure Connection - OpenScape FM dialogue opens and following mandatory fields values can be edited:

   - **IP Address/Hostname:**

     Enter the IP address or Hostname of OpenScape FM application you are going to connect to CMP.
   - **Port**

     Enter the Port of the OpenScape FM application you are going to connect to CMP.

     Navigate to the CMP area of the Register section and enter the following:
   - **IP Address/Hostname:**

     Enter the **IP address** or **Hostname** of the CMP server that can be accessed by OpenScape FM
   - **Port**

     Enter the **Port** of the CMP server that can be accessed by OpenScape FM

     Navigate to the **OpenScape FM** area of the Register section to enter the credentials OpenScape FM requires to register CMP:
   - **Username**

     This is the Username OSc FM is expecting so it will allow registration of CMP
   - **Password**

     This is the Password OSc FM is expecting so it will allow registration of CMP

5) Click on the **Retrieve Certificate** button to complete the connection

   The Certificate dialogue opens.

6) Click on **Accept Certificate** button

   The field next to **Retrieve Certificate** button is green and **Save** button is now active

7) Click on **Save** to configure the connection with OSc FM.

Next steps

The connection is established with OSc FM but this external application requires the appropriate permissions before it is accessed. You must therefore have an OpenScape FM profile assigned to the Administrator User before attempting the access to OpenScape Fault Management application or assign it as described below:

Navigate to **Configuration** > **CMP** > **General** > **Administrators** > **List** click on the **Login Name** of the Administrator User and click on **Profile** tab. **Assign** a OpenScape FM profile to the Administrator User.

NOTICE:

You can choose from the predefined OpenScape FM profiles or customize an OpenScape FM profile from the Profiles page.

4.4.20.3 How to remove a Connection to OpenScape Fault Management

How to remove a connection to OSc Fault Management:

Prerequisites

Adequate administrative permissions

CMP has already a connection established with OSc FM

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** > **Applications**.

   You see all applications that are installed for the OpenScape system.
3) In the list entry of OpenScape FM click on ‣ to open the application's action menu.
4) Select the **Remove connection** action in the action menu.

   The Authentication to OpenScape FM dialogue opens and following mandatory fields values must be entered before your are allowed to remove the connection:

   - **Username**

     This is the Username OSc FM is expecting to authenticate CMP Administrator User.
   - **Password**

     This is the Password OSc FM is expecting to authenticate CMP Administrator User.
5) Click on the **Confirm Remove** button to remove the connection

The Single Sign On support for OSc FM is disabled and the connection is removed but you can re-establish the connection by following the steps described in the relative chapter.

The **Fault Managment** button is not removed and the external OpenScape FM application is still in the list of applications.

4.4.20.4 How to display the OpenScape Fault Management certificate

How to display the OSc Fault Management Certificate:

Prerequisites

Adequate administrative permissions

OpenScape Fault Management is registered as an application in CMP with a `OSc FM rpm`

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** > **Applications**.

   You see all applications that are installed for the OpenScape system.
3) In the list entry of **OpenScape FM** click on ‣ to open the application's action menu.
4) Select the **Configure connection** action in the action menu if the connection is already established or select the **Create connection** .

   The Connection - OpenScape FM dialogue opens.
5) Click on the **Retrieve Certificate** button.

   The Certificate dialogue opens with the following information:

   Issued to:

   Issued by:

   Valid from:

   Valid to :

   Thumbprint:
6) Click on **Download Certificate** button if you want to download or see the SSL certificate.

   You are promped to open or save the Certificate in an octet format.
7) Click on **Save** to configure the connection with OSc FM.

Next steps

The connection is established with OSc FM but this external application requires the appropriate permissions before it is accessed. You must therefore have an OpenScape FM profile assigned to the Administrator User before attempting the access to OpenScape Fault Management application or assign it as described below:

Navigate to **Configuration** > **CMP** > **General** > **Administrators** > **List** click on the **Login Name** of the Administrator User and click on **Profile** tab. **Assign** a OpenScape FM profile to the Administrator User.

NOTICE:

You can choose from the predefined OpenScape FM profiles or customize an OpenScape FM profile from the Profiles page.

4.4.20.5 How to create a Connection with OpenScape Accounting

How to create a connection with OSc Accounting:

Prerequisites

Adequate administrative permissions

OpenScape Accounting is registered as an application in CMP with a `OSc Accounting rpm`

IMPORTANT:

During installation Single Sign On is enabled towards OSc Accounting and CMP is registered with OSc Accounting

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** > **Applications**.

   You see all applications that are installed for the OpenScape system.
3) In the list entry of OpenScape Accounting click on ‣ to open the application's action menu.
4) Select the **Create connection** action in the action menu.

   The Create Connection - OpenScape Accounting dialogue opens and following mandatory fields values must be entered:

   - **IP Address/Hostname:**

     Enter the IP address or Hostname of OpenScape Accounting application you are going to connect to CMP.
   - **Port**

     Enter the Port of the OpenScape Accounting application you are going to connect to CMP.

   Navigate to the CMP area of the Register section and enter the following:
   - **IP Address/Hostname:**

     Enter the **IP address** or **Hostname** of the CMP server that can be accessed by OpenScape Accounting
   - **Port**

     Enter the **Port** of the CMP server that can be accessed by OpenScape Accounting

     IMPORTANT:

     IP Address and **Port** of CMP is populated automatically in these fields but can be edited if necessary.

   Navigate to the **OpenScape Accounting** area of the Register section to enter the credentials OpenScape Accounting requires to register CMP:
   - **Username**

     This is the Username OSc Accounting is expecting so it will allow registration of CMP
   - **Password**

     This is the Password OSc Accounting is expecting so it will allow registration of CMP

5) Click on the **Retrieve Certificate** button to complete the connection

   The Certificate dialoge opens

6) Click on **Accept Certificate** button

   The field next to **Retrieve Certificate** button is green and **Save** button is now active

7) Click on **Save** to establish the connection with OSc Accounting

Next steps

The connection is established with OSc Accounting but this external application requires the appropriate permissions before it is accessed. You must therefore have an OpenScape Accounting profile assigned to the Administrator User before attempting the access to OpenScape Accounting application or assign it as described below:

Navigate to **Configuration** > **CMP** > **General** > **Administrators** > **List** click on the **Login Name** of the Administrator User and click on **Profile** tab. **Assign** a OpenScape Accounting profile to the Administrator User.

NOTICE:

You can choose from the predefined OpenScape Accounting profiles or customize an OpenScape Accounting profile from the Profiles page.

4.4.20.6 How to configure a Connection with OpenScape Accounting

How to configure a connection with OSc Accounting:

Prerequisites

Adequate administrative permissions

CMP has already a connection established with OSc Accounting

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** > **Applications**.

   You see all applications that are installed for the OpenScape system.

3) In the list entry of **OpenScape Accounting** click on ‣ to open the application's action menu.

4) Select the **Configure connection** action in the action menu.

   The Configure Connection - OpenScape Accounting dialogue opens and following mandatory fields values can be edited:

   - **IP Address/Hostname:**

     Enter the IP address or Hostname of OpenScape Accounting application you are going to connect to CMP.
   - **Port**

     Enter the Port of the OpenScape Accounting application you are going to connect to CMP.

     Navigate to the CMP area of the Register section and enter the following:
   - **IP Address/Hostname:**

     Enter the **IP address** or **Hostname** of the CMP server that can be accessed by OpenScape Accounting.
   - **Port**

     Enter the **Port** of the CMP server that can be accessed by OpenScape Accounting

     Navigate to the **OpenScape Accounting** area of the Register section to enter the credentials OpenScape Accounting requires to register CMP:
   - **Username**

     This is the Username OSc Accounting is expecting so it will allow registration of CMP
   - **Password**

     This is the Password OSc Accounting is expecting so it will allow registration of CMP

5) Click on the **Retrieve Certificate** button to complete the connection

   The Certificate dialogue opens.

6) Click on **Accept Certificate** button

   The field next to **Retrieve Certificate** button is green and **Save** button is now active

7) Click on **Save** to configure the connection with OSc Accounting.

Next steps

The connection is established with OSc Accounting but this external application requires the appropriate permissions before it is accessed. You must therefore have an OpenScape Accounting profile assigned to the Administrator User before attempting the access to OpenScape Accounting application or assign it as described below:

Navigate to **Configuration** > **CMP** > **General** > **Administrators** > **List** click on the **Login Name** of the Administrator User and click on **Profile** tab. **Assign** a OpenScape Accounting profile to the Administrator User.

NOTICE:

You can choose from the predefined OpenScape Accounting profiles or customize an OpenScape Accounting profile from the Profiles page.

4.4.20.7 How to remove a OpenScape Accounting Connection

How to remove a connection to OSc Accounting:

Prerequisites

Adequate administrative permissions

CMP has already a connection established with OSc Accounting

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** > **Applications**.

   You see all applications that are installed for the OpenScape system.
3) In the list entry of OpenScape Accounting click on ‣ to open the application's action menu.
4) Select the **Remove connection** action in the action menu.

   The Authentication to OpenScape Accounting dialogue opens and following mandatory fields values must be entered before your are allowed to remove the connection:

   - **Username**

     This is the Username OSc Accounting is expecting to authenticate CMP Administrator User.
   - **Password**

     This is the Password OSc Accounting is expecting to authenticate CMP Administrator User.
5) Click on the **Confirm Remove** button to remove the connection

The Single Sign On support for OSc Accounting is disabled and the connection is removed but you can re-establish the connection by following the steps described in the relative chapter.

The **Accounting** button is not removed and the external OpenScape Accounting application is still in the list of applications.

4.4.20.8 How to display the OpenScape Accounting Certificate

How to display the OSc Accounting Certificate:

Prerequisites

Adequate administrative permissions

OpenScape Accounting is registered as an application in CMP with a `OSc Accounting rpm`

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** > **Applications**.

   You see all applications that are installed for the OpenScape system.
3) In the list entry of **OpenScape Accounting** click on ‣ to open the application's action menu.
4) Select the **Configure connection** action in the action menu if the connection is already established or select the **Create connection** .

   The Connection - OpenScape Accounting dialogue opens.
5) Click on the **Retrieve Certificate** button.

   The Certificate dialogue opens with the following information:

   Issued to:

   Issued by:

   Valid from:

   Valid to:

   Thumbprint:
6) Click on **Download Certificate** button if you want to download or see the SSL certificate.

   You are promped to open or save the Certificate in an octet format.
7) Click on **Save** to configure the connection with OSc Accounting.

4.4.20.9 How to create a Connection with Device Management (OpenScape Deployment Service)

How to create a connection with OSc Deployment Service:

Prerequisites

Adequate administrative permissions

Device Management (OpenScape Deployment Service) is registered as an application in CMP with a *scs_cmp_DeviceManagement_config.rpm*

IMPORTANT:

During installation Single Sign On is enabled towards Device Management (OpenScape Deployment Service) and CMP is registered with Device Management (OpenScape Deployment Service)

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** > **Applications**.

   You see all applications that are installed for the OpenScape system.

3) In the list entry of Device Management click on ‣ to open the application's action menu.

4) Select the **Create connection** action in the action menu.

   The Create Connection - Device Management dialogue opens and following mandatory fields values must be entered:

   - **IP Address/Hostname:**

     Enter the IP address or Hostname of Device Management (DLS) you are going to connect to CMP.
   - **Port**

     Enter the Port of Device Management (DLS) you are going to connect to CMP.

     Navigate to the CMP area of the Register section and enter the following:
   - **IP Address/Hostname:**

     Enter the **IP address** or **Hostname** of the CMP server that can be accessed by Device Management (DLS).
   - **Port**

     Enter the **Port** of the CMP server that can be accessed by Device Management (DLS).

     IMPORTANT:

     IP Address and **Port** of CMP is populated automatically in these fields but can be edited if necessary.

     Navigate to the **Device Management** area of the Register section to enter the credentials OpenScape Accounting requires to register CMP:
   - **Username**

     This is the Username OSc Deployment Service is expecting so it will allow registration of CMP
   - **Password**

     This is the Password OSc Deployment Service is expecting so it will allow registration of CMP

5) Click on the **Retrieve Certificate** button to complete the connection

   The Certificate dialoge opens

6) Click on **Accept Certificate** button

   The field next to **Retrieve Certificate** button is green and **Save** button is now active

7) Click on **Save** to establish the connection with Device Management (OpenScape Deployment Service)

Next steps

The connection is established with OSc Deployment Service but this external application requires the appropriate permissions before it is accessed. You must therefore have an Device Management profile assigned to the Administrator

User before attempting the access to Device Management (OpenScape Deployment Service) application or assign it as described below:

Navigate to **Configuration** > **CMP** > **General** > **Administrators** > **List** click on the **Login Name** of the Administrator User and click on **Profile** tab. **Assign** a Device Management profile to the Administrator User.

NOTICE:

You can choose from the predefined Device Management profiles or customize an Device Management profile from the Profiles page.

4.4.20.10 How to configure a Connection with Device Management

How to configure an established connection with Device Management (OpenScape Deployment Service):

Prerequisites

Adequate administrative permissions

CMP has already a connection established with Device Management (OpenScape Deployment Service)

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** > **Applications**.

   You see all applications that are installed for the OpenScape system.
3) In the list entry of **Device Management** click on ‣ to open the application's action menu.

4) Select the **Configure connection** action in the action menu.

   The Configure Connection - Device Management dialog opens and following mandatory fields values can be edited:

   - **IP Address/Hostname:**

     Enter the IP address or Hostname of Device Management (DLS) you are going to connect to CMP.
   - **Port**

     Enter the Port of Device Management (DLS) you are going to connect to CMP.

     Navigate to the CMP area of the Register section and enter the following:
   - **IP Address/Hostname:**

     Enter the **IP address** or **Hostname** of the CMP server that can be accessed by Device Management (DLS).
   - **Port**

     Enter the **Port** of the CMP server that can be accessed by Device Management (DLS).

     IMPORTANT:

     IP Address and **Port** of CMP is populated automatically in these fields but can be edited if necessary.

     Navigate to the **Device Management** area of the Register section to enter the credentials Device Management (DLS) requires to register CMP:
   - **Username**

     This is the Username Device Management (DLS) is expecting so it will allow registration of CMP
   - **Password**

     This is the Password Device Management (DLS) is expecting so it will allow registration of CMP

5) Click on the **Retrieve Certificate** button to complete the connection

   The Certificate dialogue opens.

6) Click on **Accept Certificate** button

   The field next to **Retrieve Certificate** button is green and **Save** button is now active

7) Click on **Save** to establish the connection with Device Management (OpenScape Deployment Service)

Next steps

The connection is established with Device Management (OpenScape Deployment Service) but this external application requires the appropriate permissions before it is accessed. You must therefore have a Device Management profile assigned to the Administrator User before attempting the access to Device Management (OpenScape Deployment Service) application or assign it as described below:

Navigate to **Configuration** > **CMP** > **General** > **Administrators** > **List** click on the **Login Name** of the Administrator User and click on **Profile** tab. **Assign** a Device Management profile to the Administrator User.

NOTICE:

You can choose from the predefined Device Management profiles or customize an Device Management profile from the Profiles page.

4.4.20.11 How to remove a Device Management Connection

How to remove a connection to Device Management (OSc DLS):

Prerequisites

Adequate administrative permissions

CMP has already a connection established with Device Management (OSc DLS)

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** > **Applications**.

   You see all applications that are installed for the OpenScape system.
3) In the list entry of Device Management click on ‣ to open the application's action menu.
4) Select the **Remove connection** action in the action menu.

   The Authentication to Device Management (OSc DLS) dialog opens and following mandatory fields values must be entered before your are allowed to remove the connection:

   - **Username**

     This is the Username Device Management (OSc DLS) is expecting to authenticate CMP Administrator User.
   - **Password**

     This is the Password Device Management (OSc DLS) is expecting to authenticate CMP Administrator User.
5) Click on the **Confirm Remove** button to remove the connection

The Single Sign On support for Device Management (OSc DLS) is disabled and the connection is removed but you can re-establish the connection by following the steps described in the relative chapter.

The **Device Management** button is not removed and the external Device Management (OSc DLS) application is still in the list of applications.

4.4.20.12 How to display the Device Management Certificate

How to display the Device Management (OSc DLS) Certificate:

Prerequisites

Adequate administrative permissions

Device Management (OpenScape Deployment Service) is registered as an application in CMP with a *scs_cmp_DeviceManagement_config.rpm*

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** > **Applications**.

   You see all applications that are installed for the OpenScape system.
3) In the list entry of **Device Management** click on ‣ to open the application's action menu.
4) Select the **Configure connection** action in the action menu if the connection is already established or select the **Create connection** .

   The Connection - Device Management dialog opens.
5) Click on the **Retrieve Certificate** button.

   The Certificate dialogue opens with the following information:

   Issued to:

   Issued by:

   Valid from:

   Valid to:

   Thumbprint:
6) Click on **Download Certificate** button if you want to download or see the SSL certificate.

   You are promped to open or save the Certificate in an octet format.
7) Click on **Save** to configure the connection with Device Management (OSc DLS).

4.4.21 OpenScape Enterprice Express Applications

Common Management Platform integrates the following enterprice express applications in its User Interface:

- OSc Trace Manager
- OSc Contact Center
- OSc Concierge
- OSc Xpressions

4.4.21.1 How to create a new or configure an existing Connection with OpenScape Enterprice Express Applications

How to create a new or configure an existing connection with OSc Enterprice Express Applications:

Prerequisites

Adequate administrative permissions

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** > **Applications**.

   You see all applications that are installed for the OpenScape system.
3) In the list entry of the desired node click on ‣ to open the application's action menu.
4) Select the **Create connection** action to create a new connection or the Create connection action to configure an existing one.

   The dialogue window opens and following mandatory fields values must be entered:

   - **IP Address/Hostname: IP address** or **Hostname** OS-TM
   - **Port**: 22
   - **Username**: osvtmbackup
   - **Password**

   IMPORTANT:

   Repeat the procedure for all OpenScape Enterprice Express Applications integrated in Common Management Platform.
5) Click on **Save** to establish the connection with the OSc Enterprice Express application.

4.4.21.2 How to remove an Openscape Enterprice Express Applications Connection

How to remove a connection to OSc Enterprice Express Applications:

Prerequisites

Adequate administrative permissions

CMP has already a connection established with the desired OSc Enterprice Express Application

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** > **Applications**.

   You see all applications that are installed for the OpenScape system.

3) In the list entry of the desired node click on ‣ to open the application's action menu.

4) Select the **Remove connection** action in the action menu.

   A pop-up window appears in order to confirm the removal of the connection.

5) Click on **OK** button to remove the connection

4.4.22 Software Activation (User Interface Patching)

Software activation feature allows you to update/hotfix all nodes of a small/ large deployment easily using CMP. Updating using the CMP (UI-patching) is supported for Media Server Standalone, Multiple Communication System and Standard Duplex (small, large and very large) and for Integrated Simplex.

When using CMP (UI-patching) for updating instead of using manually the `osc-setup` tool:

You reduce considerably the number of steps that have to be performed by the Administrator for updating/hotfixing large and very large deployments.

There is a single point for Administrating the update/hotfix of your system.

The parallel update of frontend nodes and media server nodes is easier and smoother.

NOTICE:

CMP (UI-patching) can be used for an OpenScape UC Application update but not for an upgrade.

Software Activation (UI-Patching)

Updates/hotfixes will be applied to all large deployment nodes.

Nodes running with a hotfix newer that the currently applied shall not be downgraded. They will remain on the newer patch level. This can only happen if a hotfix has been applied manually to a specific node and if possible should be avoided.

The backend server is updated first. If the update is successful then all other nodes will be updated in parallel. There is no support for "rolling" updates (i.e. in the case that two mediaservers exist in the solution, first update one and then the other in order to minimize downtime).

4.4.22.1 How to Update/Hotfix in the CMP

How to update/hotfix all nodes of a small/large deployment easily using CMP:

Prerequisites

Adequate administrative permissions

All software is delivered in 1 repository e.g. USB drive instead of multiple repositories on different DVDs.

The feature has been activated with the following script:

`/opt/siemens/servicetools/install/bin/prepareUpdate.sh`

IMPORTANT:

If your UC Application servers are configured to use an HTTP Proxy (see **Yast->Network Services->Proxy** or `/etc/sysconfig/proxy` to determine the configuration) then the HTTP Proxy configuration parameter “No Proxy Domains or NO_PROXY”, respectively will need to include the FQDN’s of all the nodes in your small/large deployment. The FQDN can be obtained using the command “`hostname -f`” on each server.

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** > **Applications**.

You see all applications that are installed for the OpenScape system.

3) In the list entry of **OpenScape UC** click on ‣ to open the application's action menu.

If you are in one of the following UC deployments choose the corresponding Application Types:

a) Media Server Standalone = **Media Server**

Multiple Communication Server admin= **OpenScape CMP**

4) Select the **Software activation...** from the action menu.

The Software activation window opens.

IMPORTANT:

The fields in this window have the values that were used when the last Software Activation was triggered (regardless if it was successful or not). The window is not reset after every attempted activation instead it has a “memory” of

the last Software activation. The fields are empty when the Software Activation is triggered for the first time.

The info bar of the window displays one of the following messages:

- “This feature is not yet activated, please use the `/opt/siemens/servicetools/install/bin/prepareUpdate.sh` script.”

  The Software activation feature is by default deactivated so you must activate it with the script mentioned in the message.
- “No software activation has ever been triggered.”

  This is the first time Software Activation is performed on this Application Server.
- “Software activation was finished successfully on all nodes on “Date time year””

  The last time Software activation was performed it was successful on all nodes.
- “Last software activation has been finished on all nodes but it failed at least on one node.”
- “Software activation finished with Errors.”
- “Software activation is still running on at least one node - This window will autorefresh.”

  This messages appears when Software activation is still running. In this state all fields of the window are not editable and the window auto refreshes every 10 seconds.

5) Navigate to the Synchronize area and click on the check box **Synchronize Active to Passive partitions**

The checkbox is active only if the fallback partitioning is activated.

IMPORTANT:

In case there are fatal errors during the “update” or during runtime right after the “update” and the checkbox is clicked you have the option to do a fallback to the previous version.[10]

It is therefore strongly recommended that you activate the Fallback partitioning and choose to **Synchronize Active to Passive partitions** before initiating Software Activation.

[10] This is possible on commandline level by calling `syncUC fallback` on every node and reboot it afterwards

6) The following options are available:

a) Use only a path hosting the persistent repository:

Enter the repository **Path**

The provided file path needs to point to the new software repository and the file path could be on the local disk or USB device.

- -) In the case of a new UC Applications Minor or Fix Release use "`osc-setup cr`" to create the software repository.

  Example:

  "`osc-setup cr -b /media/OpenScapeUcSuiteApps-Repository-<version>.iso -l /your_path`"
- -) In the case of a new UC Applications Hotfix use "`mount -o loop`" to mount the Hotfix ISO file (which contains the software repository)

  Example:

  "`mount -o loop /media/OpenScapeUcSuiteApps_PATCH-<version>.iso /your_path`"

b) Use path in order to create persistent repository and install a fix release and hotfix in one step:

In the **Build Path** field enter the full mount path or the base ISO repository.

In the **Hotfix Path** field enter the full mount path or the hotfix ISO.

Example: "`/mnt/OpenScapeUcSuiteApps-Repository-<version>.iso /your_path`"

7) Click on **Start** button to initiate the Software activation.

You are prompted with a message explaining that:

a) This action will cause a total outage of UC Applications Services.

All nodes of the selected application (delivered software) will be updated.

All CMP Admin Users will be logged out.

CMP (the backend node) will not be accessible until the node update is completed (successfully).

You may monitor the status of the update via the log file `/var/siemens/common/log/install/uipatching/updateAllNodes.log`

8) Click on **OK** to continue

IMPORTANT:

Once the "update" procedure is initiated, it cannot be stopped and your CMP session is closed. All components on the backend node are not accessible and if there are

any Frontend or Media Servers computers deployed they are shut down.

The “update” of the backend starts.

After triggering UI patching via CMP (Software activation) and check phase has finished successfully, users are redirected to a Web page (https://<BACKEND_IP>:444/OSCbase/ui_patching) where they can get information about the nodes involved in their deployment (installation status).

Each node has 4 states shown by the appropriate icon right next to the node name:

- -)Installation not started
- -)Installation in progress
- -)Installation finished successfully
- -)Installation finished with errors

In this screen the following are available:

- **Activate log** button enables the corresponding log to be shown on the right part of the page.
- **Auto refresh** check box activates automatic download of the activated log eliminating the need to press the Activate log button every time an update of the process is needed.
- **Download All logs** button is available after UC patching has finished and collects all logs involved in the UC patching process.
- **Download active log** delivers the log selected at the time it was pressed.
- **CMP login** button redirects users to the CMP login page.

When the backend starts again you can monitor the actual status of the “update” in the **Information** field of the Software Activation screen.

NOTICE:

Frontends and Media Servers are updated in parallel and you can use the CMP to check if the “update” has already been finished.

If there is an error during the “update” of the backend, the system is no longer accessible via CMP. In the case of a backend update failure you'll have to examine the status of the backend on a commandline level (i.e examine the file `/var/siemens/common/log/install/uipatching/updateAllNodes.status`)providing info on what went wrong.

9) When the update finishes you can see in the info bar the result of the Software activation:

- If the “Software activation was finished successfully on all nodes on “Date time year”” you can click on the **Download** button to retrieve the log files. The software version of installed UC applications is displayed in Software Activation Screen.
- If the “Software activation finished with Errors.” or if the “Last software activation has been finished on all nodes but it failed at least on one

node.” a **Collect** button is activated so you can retrieve Trace files for further analysis.

The **Start** button is replaced by a **Try again** button.

10) Click the **Try again** button to restart the Software Activation.

Software activation restarts and all steps from 6 to 9 repeated

The **Path** field is no longer mandatory. If the field is empty or unchanged the system is updated using the same repository as in the previous execution.

IMPORTANT:

The Synchronize area is greyed out with the values that where chosen in the initial update process. No **Synchronize Active to Passive partitions** is repeated, the initial synchronization is kept.

IMPORTANT:

In the case of a failure you can’t trigger a rollback to an existing partition from CMP.

NOTICE:

After the completion of the upgrade delete the provision of the repository:

“`osc -setup cr -clean`”

The repository should be deleted because if you use mount to provide the necessary files for the upgrade, you cannot unmount.

4.5 Managing Licenses

The legal use of the OpenScape system features requires the corresponding product licenses. You can use the license management to activate these licenses and to view license information. The license management works domain-spanning.

IMPORTANT: You can’t activate OpenScapeVoice licenses nor DLS licenses via the Common Management Platform

---

4.5.1 License Management Concept

Licensing is handled via a centralized license management procedure for the management and activation of licenses. The product/feature is supplied together with a License Authorization Code (LAC) with which a license file is obtained from the Central License Server (CLS). This license file is used for activating licenses. This procedure provides protection against any potential manipulation of the licenses.

Central License Server (CLS) The Central License Server (CLS) generates and manages the license files. A license file is generated when the License Authorization Code is sent to the CLS by Common Management Platform. The transfer of the license file to Common Management Platform occurs automatically via the internet.

IMPORTANT:

When you connect the Common Management Platform computer system to the internet, make sure that the computer system can only connect to the CLS and other selected, secure target systems.

NOTICE:

In certain circumstances the Common Management Platform may not be able to access the internet. In this case it is possible to manually generate the license file at the CLS and to download it. The associated licenses can then be activated in the Common Management Platform with the license file alone and without internet connection.

Every customer or sales partner has a separate license account on the CLS. The accounts can be maintained at the CLS via a separate web-based user interface. All available and already purchased licenses can be displayed.

Monitoring 3rd Party Support

Operating and maintaining a Software Application prerequisites a legal licensing of the used software. CMP supports technicians checking the licensing by comparing the amount of OSV and UC (BackEnd, FrontEnd, Media Server but no redundant systems) nodes with the amount of valid SuSE Upgrade Protection Licenses. The systems that run on SUSE SLES provided by Unify need to be protected by using the patches/ support provided by Novell.

Patches for Operating systems provided by Unify should only be installed if the Novell SLES support licenses are active. In order to monitor the Novell support a license type is used to track these licenses and acts as a reminder for the Novell support extension.

There is no technical consequence of an alarm for missing or expired Novell SUSE Update Protection Subscription, like locked functions or even shutdown. The license type has the Feature Name “Novell SUSE Update Protection Subscription” and is relevant for the OSV and UC nodes.

Common Management Platform

The licenses are activated with Common Management Platform. The Common Management Platform transfers the License Authorization Code (LAC) to the CLS and receives the associated license file.

The licenses and their related information are displayed in Common Management Platform. You can see the total number of licenses. You can see which licenses are assigned to which applications or features, and when these licenses expire. In addition, you can see how many licenses are still free.

IMPORTANT: You can’t activate OpenScapeVoice licenses nor DLS licenses via the Common Management Platform

Grace Period

After purchasing or installing the product/feature, the license for it must be activated within a specified time period - called the grace period. Depending on the product involved, this period may be e. g. 30 days.

During this grace period, the product may be restricted or fully functional. If you do not install a license after the grace period, the product becomes severely restricted or stops working entirely.

Alarms

Alarms will be generated in the following circumstances:

- A **Major** alarm will be triggered on a daily basis starting 30 days before the expiration of a license.
- The Major alarm will be replaced by a **Critical** alarm 2 days before the expiration of a license. The alarms will be fired by the license surveillance service around midnight.
- In case “Novell SUSE Update Protection Subscription” licenses are installed their number is checked against the linux nodes. If the license quantities are not enough the licenses are indicated red and a **Critical** alarm is triggered on a daily basis until the inconsistency is resolved.

NOTICE:

After the license expiration no alarms will be generated.

Locking-ID (MAC Address or Advanced Locking ID)

During production, hardware is assigned a board-specific number called a MAC address which is unique world-wide. To guarantee unique licensing, in case of a Native environment the MAC Address is used as the **Locking ID** and the license file is linked to the hardware's MAC address (for example, network card of the system server).

In case of a Virtual Environment the **Locking ID** is the Advanced Locking ID that is calculated based on Network Characteristics.

Every project/feature license is linked to this locking ID.

4.5.2 License Information

You can use Common Management Platform (CMP) to retrieve licensing information:

- **General license information**

  The general license information contains

  – the system name that is licensed
  – the name of the product for which the license is used
  – the feature name that is licensed
  – the number of licenses already used
  – the licenses validity
- **License locking IDs**

  A locking ID is either a unique feature of a computer system - e. g. the MAC address of a network board or an Advanced Locking ID (ALI) which is an alphanumeric string based on Network characteristics.

  NOTICE:

  In the header of the Locking ID screen you have the info if the system is Virtual or not.

  The purchased licenses are linked to the locking ID. You may have to select a locking ID to which you want to bind licenses the first time you license the system. All further licensing activities are performed with this locking ID.

  IMPORTANT:

  Depending on the target environment either a MAC Address or the Advanced Locking ID has to be used as Locking ID.

  In case of a Native environment the MAC Address is used.

  In case of a Virtual environment the Advanced Locking ID is used.

  If your OpenScape Common Management Platform does not display the Locking ID to use, you can calculate the Advanced Locking ID (ALI) on Central License Server. For this please click on one of the "Calculate Locking ID" buttons and enter the requested system parameters.

IMPORTANT: You can’t activate OpenScapeVoice licenses nor DLS licenses via the Common Management Platform

NOTICE:

When issuing new licenses for any deployment either new or redundant, the licenses must be issued with the exact same content and the only difference must be the "Locking ID" and the "lincense ID".

4.5.2.1 How to Display License Information

To display license information via the Common Management Platform (CMP), proceed as follows:

Prerequisites

Adequate administrative permissions.

Step by Step

1) On the **Maintenance** navigation tab click on the **License** navigation menu item.
2) Select **Information** in the navigation tree.
3) A list of all features available in the OpenScape system is displayed in the work area. This list contains for each entry the following information:

   - **Redundant license available**

     The key image that is on the first column of each entry indicates if there are redundant licenses available or not:

     If the key is yellow the value is false. If you “mouse over” the key image the message “no redundant license available” appears

     If the key is grey the value is true. If you “mouse over” the key image the message “redundant license available” appears

     In a stand by configuration apart from the “license id” the license file of the passive node is identical to the active node license file.

     If the passive node is activated then the redundant license is also activated

     NOTICE:

     If a passive node in a stand by configuration is activated and doesn’t have assigned a redundant license then it uses a 30 day grace period license.

   - **System**

     Displays the system for which the license information is being reported i.e. Backend name for UC system and the cluster name for OSV
   - **Product Name**

     Displays the product for which the license information is being reported e.g., OpenScape UC Application V7.
   - **Feature Name**

     States the feature name associated with the product e.g., OpenScape UC Appl V7 Mobile Client.
   - **Number of used licenses**

     Specifies how many licenses are altogether available for the feature and how many of these are already used e.g., 1 of 30.

     NOTICE:

     In cases that the quantities consumed are less than the quantity introduced by the V9 GPCF (eg. less than

100 User licenses) then the healing mechanism should be activated so that all consumed quantities will be transferred to the new V9 licenses. V7 licenses will still be there.

- **Validity**

  Shows the validity for the feature's licenses by expiration date. License entries are marked red if:

  - They are invalid,

  - They have expired or are about to expire (e.g., Grace Period 30 days.)

  - The number of “Novell SUSE Update Protection Subscription” licenses installed is less than the amount of the linux nodes.

  NOTICE:

  The expiration date displayed for the license type ""“Novell SUSE Update Protection Subscription"” is always the earliest of the system.(e.g. If the system is an OSV cluster with two OSV nodes that have different expiration dates for their Novell SLES support licenses then the earliest of the two will appear in the validity field).

4) The list can be filtered according to specific terms (patterns).

a) Enter the desired filter term in the field **Filter**. You can either enter the complete term or the initial letters followed by * (e. g. *HiPath*).

b) From the list displayed, select whether the filtering is to be applied to the *System*, *Product Name* or *Feature Name* column.

c) Click on **Go** to activate the filter. Only the list elements which correspond to the pattern entered are displayed.

d) Click on **Clear** to deactivate the filter. Filter conditions are deleted. All the list elements are displayed again.

5) Information in the list can be exported to a CSV file.

a) Click the **export data to CSV file** in the work area to the right of the Items/Page controls.

IMPORTANT: If a filter is applied then the extracted data is filtered as well.

b) You are prompt to open / save the .csv file

c) Enter the **Save in:** location and **File Name** and click on **Save**.

d) The CSV file is saved with the following information.

Redundant license available

System Name

Product Name

Feature Name

Number of used licenses

Validity

4.5.2.2 How to Display Bound Licenses

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** > **CMP** > **Administrators** > **List**
2) Select the User. Click **Add/Edit** > **Profiles**

   The list of all Profiles assigned to the User is displayed
3) **Assign** new Profiles or **Unassign** existing ones.
4) Below the list of Profiles click **Show bound licenses**.

The licenses assigned to a user will be displayed.

4.5.2.3 How to Display Bound Licenses of a Foreign User

With this task, it is possible to check the bound licenses assigned to a Foreign 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** > **CMP** > **Administrators** > **Foreign**
2) Select the Foreign User. Click **Edit** > **Profiles**
3) Below the list of Profiles click on **Show bound licenses**.

The licenses assigned to the foreign user will be displayed.

4.5.3 How to Activate Licenses

After you have purchased an OpenScape product, you will have to activate the licenses supplied with it in order to release the product and its features.Licenses can be activated by one of the following two methods:

How to Activate a License Online with License Authorization Code

License activation via the LAC is the standard method. Using the LAC, a license file is generated at the Central License Server (CLS) and forwarded to the Common Management Platform. The license file is used to activate the associated licenses and thus release the products and their features.

How to Activate a License Offline with a License File

License activation with the license file is necessary if you cannot or do not want to perform online activation and if the license file is directly available. The license file was generated at the Central License Server (CLS) earlier and downloaded. The license file is used to activate the associated licenses and thus release the products and their features

IMPORTANT: You can't activate OpenScape Voice licenses nor DLS licenses via the Common Management Platform.

IMPORTANT: You can't retrieve license information on OpenScape Voice licenses via the Common Management Platform.

Process flow for online license activation (example)

1) The order is placed by the customer and entered in the SAP system, for example.
2) The license-relevant order details are stored in the database of the CLS.
3) The CLS automatically generates the license authorization code (LAC) from the data. This LAC is forwarded to the customer (for example, via e-mail) together with the CLS access data.
4) The delivery of the product/feature is initiated.
5) The customer installs the product/feature. The grace period begins during which the product/feature must be licensed.
6) The customer transfers the License Authorization Code to the CLS via the internet by using the Common Management Platform. Some customer-specific hardware data (such as the MAC address of the system server or the Advanced Locking ID) is sent to the CLS along with the LAC.
7) The CLS uses the License Authorization Code and the customer-specific hardware data to generate a license file and then sends this back to the Common Management Platform. The license file contains all the licenses associated with the product/feature.
8) The license management of the Common Management Platforms checks if the Locking ID saved in the license file matches the Locking ID of the system server. If the check succeeds, the licenses of the product/feature are activated. Otherwise, the product/feature is not released.

IMPORTANT:

If the license file does not match the server you are getting a pop error with a string of entries where all available MAC address & Advance Locking IDs [ALIs] are listed for that server - no matter if it is physical -or- virtual server. In case of a Virtual environment, many Advanced Locking IDs (ALI) may be listed. Any of them should work, so it is valid to use any of them to order licenses.i.e use the first Advanced Locking ID (ALI) which is listed.

9) The customer can use the product/feature in the scope purchased.

Process flow for offline license activation (example)

1) The order is placed by the customer and entered in the SAP system, for example.
2) The license-relevant order details are stored in the database of the CLS.
3) The CLS automatically generates the license authorization code (LAC) from the data. This LAC is forwarded to the customer (for example, via e-mail) together with the CLS access data.
4) The delivery of the product/feature is initiated.
5) The customer installs the product/feature. The grace period begins during which the product/feature must be licensed.
6) The customer transfers the **License Authorization Code** to the CLS/CLM. Some customer-specific hardware data (such as the MAC address of the system server or the Advanced Locking ID) is sent to the CLS along with the LAC.
7) The CLS uses the License Authorization Code and the customer-specific hardware data to generate a license file that can be downloaded locally by the customer. The license file contains all the licenses associated with the product/feature.
8) The customer via the Common Management Platforms chooses the offline activation and uploads the license file he has retrieved in previous step. License Management checks if the Locking ID saved in the license file matches the Locking ID of the system server. If the check succeeds, the licenses of the product/feature are activated. Otherwise, the product/feature is not released.

IMPORTANT:

If the license file does not match the server you are getting a pop error with a string of entries where all available MAC address & Advance Locking IDs [ALIs] are listed for that server - no matter if it is physical -or- virtual server. In case of a Virtual environment, many Advanced Locking IDs (ALI) may be listed. Any of them should work, so it is valid to use any of them to order licenses.i.e use the first Advanced Locking ID (ALI) which is listed.

---

9) The customer can use the product/feature in the scope purchased.

4.5.3.1 How to Activate License - Offline

License management can be used to import a new or updated license file offline. A license file is required which can be downloaded from the Central License Server (CLS). The license file is used to activate the associated licenses and thus release the products and their features.

Prerequisites

Adequate administrative permissions

Step by Step

1) On the **Maintenance** navigation tab click on the **License** navigation menu item.

2) Select **Information** in the navigation tree.

IMPORTANT:

OpenScape Voice license activation and OpenScape DLS license activation are not offered via CMP.

3) Click the **Offline Activation...** button in the work area.

   The **License Activation** dialog appears.

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

The license management verifies the signature of the license file against the Locking ID (MAC or ALI) . If the verification is successful, the data are transferred from the file and the licenses are displayed in the Common Management Platform with the associated information.

IMPORTANT:

If the license file does not match the server you are getting a pop error with a string of entries where all available MAC address & Advance Locking IDs [ALIs] are listed for that server - no matter if it is physical -or- virtual server. In case of a Virtual environment, many Advanced Locking IDs (ALI) may be listed. Any of them should work, so it is valid to use any of them to order licenses.i.e use the first Advanced Locking ID (ALI) which is listed.

4.5.3.2 How to Activate License - Online

Online license activation via the LAC (License Authorization Code) is the standard method. Using the LAC, a license file is generated at the Central License Server (CLS) and forwarded to the Common Management Platform. The license file is used to activate the associated licenses and thus release the products and their features.

Prerequisites

Adequate administrative permissions.

Step by Step

1) On the **Maintenance** navigation tab click on the **License** navigation menu item.
2) Select **Information** in the navigation tree.

IMPORTANT:

OpenScape Voice license activation and OpenScape DLS license activation are not offered via CMP.

3) Click the **Online Activation...** button in the work area.

   The **Activate licenses online** dialog appears.

4) Specify under License authorization code (LAC) the license authorization code you have received with the OpenScape product.

5) Select a locking ID under Locking ID. There is no selection option available if only one locking ID is present.

6) Enter the user name and password for accessing the license server under User name and Password.

   NOTICE:

   Certain products can also be anonymously licensed without a user name and password. Deactivate the **I would like to logon at the License Server with the following account** option for this purpose. If you have a valid user ID for the license server you should use it for anonymous licensing also.

7) Click **Activate**.

The connection to the license server is established, and the license is released. As a rule, this operation does not take more than 90 seconds.

4.5.4 How to Display License Locking IDs via CMP

To display license locking IDs via the Common Management Platform (CMP), proceed as follows:

Prerequisites

Adequate administrative permissions

Step by Step

1) On the **Maintenance** navigation tab click on the **License** navigation menu item.

2) Select **Locking IDs** in the navigation tree.

3) A list of all License Locking IDs of the system is displayed in the work area. Next to the “Locking IDs ”header there is the indication if it is a **Virtual System** or a **Native System**.

   This list contains for each entry the following information:

   - **Type**

     Shows the Locking ID type which is either the **MAC** address of the system to which the licenses are registered or the **Advanced** Locking ID that is calculated based on Network Characteristics.
   - **Locking ID**

     IMPORTANT:

     Depending on the target environment either a MAC Address or the Advanced Locking ID has to be used as Locking ID.

     In case of a Native environment the MAC Address has to be used.

     In case of a Virtual environment the Advanced Locking ID has to be used.

     If your OpenScape Common Management Platform does not display the Locking ID to use, you can calculate the Advanced Locking ID (ALI) on Central License Server. For this please navigate to CLS and click on one of the "Calculate Locking ID" buttons and enter the requested system parameters.
   - **Adapter Name**

     Shows the name of the adapter that provides the Locking ID.
   - **Logical Name**

     Specifies the logical name of the adapter that provides the Locking ID.
   - **IP Address**

     Specifies the IP address of the adapter that provides the Locking ID. Here there could be several IP addresses displayed - such as in server scenarios. or no IP address (adapter out of service).

4) If access to the central license server is required, click **Link to the Central License Server**.

4.5.5 Software Subscription License

Software Subscription Licensing (SSL) consists of two parts – the Product Instance and the Monthly Subscription License.

Licensing Structure

- **Product Instance**: For a nominal fee the Product Instance is purchased once for each product. It provides all of the licenses necessary to equip a product to its maximum capacity, including all major features. The Product Instance is time limited each year until January 31st so the customer must renew their Product Instance annually between the first of December and

the end of January. This does not require any additional ordering – just an update of the product license keys.

However, Product Instances are version-specific so a customer upgrading from one major product release to another major release will have to purchase a new Product Instance.

- **Monthly Subscription License**: The Subscription License is the monthly charge for a single user to use a single product.

  For example:

  If a single user utilizes voice, DLS Mobility functionality and Unified Communications (UC), then they would pay for 3 monthly Subscription Licenses.The Product Instances required for these functionalities are:

  OpenScape Voice,

  OpenScape DLS,

  OpenScape UC Application.

  As opposed to perpetual licenses (CapEx licenses), **Monthly Subscription Licenses** are not “purchased” at the initial installation, rather the Subscription Licenses are based upon the license usage that is reported monthly and the cost is calculated at the end of each month based on actual service consumption. The aggregation method used for calculating the service consumption is the high-watermark of the licenses used during the monthly period.

  IMPORTANT: Monthly Subscription Licenses are version-independent, so no upgrade fee is required.

  NOTICE:

  The high-watermark method calculates the peak of license usage during a month.So if SSL reports the usage of 4 UC licenses one day, 6 UC licenses the next day, 20 UC licenses the third day, 1 UC license the fourth day and no UC license usage for the rest of the month, the high-watermark is 20 UC licenses for this month.

SSL License Customers

There are two SSL License Customer types; Service Providers and Enterprise customers. Service Providers resell OpenScape product, while Enterprise customers are end users. SSL licensing is provided based on the Licensing Structure and type of Customer.

4.5.5.1 How to Display Software Subscription License Information

To display Software Subscription License information via the Common Management Platform (CMP), proceed as follows:

Prerequisites

Adequate administrative permissions.

You have installed/activated the Software Subscription Product Instance License at least 24 hours before the SSL information is displayed correctly in CMP.

Step by Step

1) On the **Maintenance** navigation tab click on the **License** navigation menu item.
2) Select **Software Subscription** in the navigation tree.
3) A list of all nodes of the OpenScape system that used Subscription License is displayed in the work area. This list contains for each entry the following information:

   Node Name

   Shows the Node IP or the Node Hostname.

   IMPORTANT:

   Products that are not fully managed from within the CMP over a designated management interface (e.g. OSV soap server used by OSV Assistant) have to start an SNMP server and register to the Subscription Software License service (SSL) server in order to report its license usage.

   Node Type

   Possible Node Types are:

   - **UC** (OpenScape UC Application)
   - **UM** (OpenScape User Management)
   - **OpenScapeVoice**
   - **DLS** (OpenScape Deployment Service)
   - **OpenScape Xpressions**
   - **OpenScape Branch Assistant**
   - **OpenScape Contact Center**

   IMPORTANT: For SNMP nodes (i.e. Xpressions) that are not fully managed by CMP you have to activate the Subscription Software License field when adding/editing the node[11]. The report on the used license will follow the same

[11] Navigate to **Maintenance** > **Nodes** > **Inventory** click on **OSC Xpressions**

schedule as the rest of the SSL licenses so the correct value will not be displayed before the daily report is delivered.

License Type

Specifies the Monthly Subscription License type the nodes use:

License Type for UC : **UCi**

License Type for UM : **USERM**.

License Type for OpenScapeVoice: **Voice**

License Type for OpenScapeVoice: **OpenScape Mobile License**

License Type for OpenScapeVoice: **Encryption License**

License Type for DLS : **DLS Mobility Usage**

License Type for OpenScape Branch: **Branch**

License Type for OpenScape SBC: **OsSBC**

License Type for OpenScape Concierge: **AC**

License Type for OpenScape Concierge: **CCAV**

License Type for OpenScape Contact Center: **CCTA**

License Type for OpenScape Contact Center: **CCMMA**

License Type for OpenScape Contact Center: **CCMgr**

License Type for OpenScape Contact Center: **CCIVR**

Quantity

Quantity of Licenses used by this node is reported in this field and holds the high watermark value that was reached on the **Last collection date** up to the reported month.

This value can only be increased during the reported month and is reported only once a day at 11pm.

When no license are reported from the specific node, this field will hold the **N/A** value

The high watermark of the consumption of “Openscape UCis” is the amount of UC Users configured in the system. This value is reported by OSC UC node.

Product ID

The Product ID is used to uniquely identify the products for billing purposes. It is a unique string; it is created by SAP and corresponds to the Product Instance ID (PIID).

This information is delivered with the license file that is activated by the administrator.

Remaining days

Specifies how many days remain before the expiration of the license.

If the license is time unlimited the field will hold the **unlimited** value.

Collection error

This field can be set to “true” by both element managers (assistants) that provide the information about aggregated usage to Software Subscription License service (SSL) and also the Software Subscription License service itself.

SSL service sets this field to true when an SNMP node has not replied to SSL for more than 2 days.

Element managers (assistants) set it to true according to the following:

OSV Assistant sets the value to true when there is a connection failure of its SOAP connection with the OSV node.

OSV Assistant sets the value to true when there is a connection failure of its SOAP connection with the DLS Application

---

IMPORTANT: UC Assistant and UM never set the Collection error value to true.

Last collection date

This is the latest date and time when the high watermark license usage and the remaining days were collected by SSL.

4) The list can be filtered according to specific terms (patterns).

a) Enter the desired filter term in the field **Search for:**. You can either enter the complete term or the initial letters followed by * (e. g. *HiPath*).

b) From the list displayed, select whether the filtering is to be applied to the **Node Type** or **Product ID** column.

c) Subscription License usage is displayed always for the selected month from the month list.

d) Click on **Search** to activate the filter. Only the list elements which correspond to the pattern entered are displayed.

e) Click on **Show all** to deactivate the filter. Filter conditions are deleted. All the list elements are displayed again.

4.5.6 How to Display SIEL IDs via CMP

To display SIEL-IDs via the Common Management Platform (CMP), proceed as follows:

Prerequisites

Adequate administrative permissions

Step by Step

1) On the **Maintenance** navigation tab click on the **License** navigation menu item.

2) Select **SIEL-IDs** in the navigation tree.

3) A list of all SIEL IDs of the system is displayed in the work area. The SIEL-IDs values are retrieved via license service from the imported license

files to CMP server. OpenScape Branch, OpenScape UC Application and OpenScape Common Management Platform can be included.

This list contains for each entry the following information:

- **Product Name**

  Displays the product for which the SIEL ID information is being reported e.g., OpenScape UC Application V7.
- **SIEL-ID**

  SIEL-ID value is retrieved via license service from the imported license file to CMP server.

4.6 Import and Export of System Data

Data for Common Management Platform (Domain Management, System Management), OpenScape Voice (Assistant data, all Configuration data, Subscriber / Endpoint data) and OpenScape Branch can be imported or exported easily via csv or zip files.

IMPORTANT: In our comma separated value files you may want to use the "," character as part of the displayname and not as a separating character. In this case the separating character must be escaped by using backslash: we must use "/ ," instead of ","

The following data can be imported and exported:

- Data for **Common Management Platform**
  - Domain Management

    Comprises user- and resource-related data. You can use predefined lists (*.csv or *.zip) to import multiple users or multiple resources or

export these to a list. This is an advantage if you need to work with large amounts of data.

IMPORTANT:

Files that are imported to CMP must be UTF-8 encoded.

For Import/Export, please be aware of the following exceptions:

Pins and passwords are not exported.

Domains are exported but can not be imported.

Profiles as profile objects can not be imported. A user can be assigned profiles if they have already been specified, e.g. by the Common Management Platform.

NOTICE:

You can obtain more structure information by experimentally exporting the relevant data.

– Domain Management for Xpressions

  Comprises user- and resource-related data in a format that can be used for an import into a OpenScape Xpressions system.

– System Management

  Comprises the Common Management Platform and OpenScape UC Application configuration data with all nodes and applications.

- Data for **OpenScape Voice**
  - Assistant data (switch-independent)

    Comprises the OpenScape Voice data:

    URL of the DLS,

    DLS job information,
  - Assistant data (switch-specific)

    Comprises the OpenScape Voice data:

    Endpoint templates,

    Subscriber templates used for the OpenScape Voice user management,

    Business group specific default values,

    Customer-specific notes for the OpenScape Voice main entities (business groups, subscribers, feature profiles etc.),

    Gateway URLs (RG 2700).
  - Assistant data (switch-specific with DLS)

    Comprises the OpenScape Voice data:

    URL of the DLS,

    DLS job information,

    Endpoint templates,

    Subscriber templates used for the OpenScape Voice user management,

    Business group specific default values,

    Customer-specific notes for the OpenScape Voice main entities (business groups, subscribers, feature profiles etc.),

    Gateway URLs (RG 2700).
  - All configuration data

    Comprises the OpenScape Voice data:

    Business Group, Subscribers, Endpoints, Endpoint Profile, Feature Profile, Numbering Plan, Office Code, Directory Number, Routing Area, Class of Service, Calling Location, Destinations, E911 Subnets, Authorization Codes, Executive/Assistant, Speed Calling Lists, Departments, Routes, Alias, Time, Destination, Day Schedule, Period Schedule, Weekly Schedule, Media Gateway, Media Gateway Circuits, Code Processing, Origin Destinations, Origin Route, Carrier Destinations, Carrier Route, CAC Groups, CAC Policies, MLHG, Prefix Access Codes, Destination Codes, Location Codes, ENUM Operators, ENUM Servers, Intercepts, Treatment, RTP Parameter, Display Number Modification.
  - Subscriber/endpoint data (ENUM format)

    Comprises the OpenScape Voice data:

    Directory Number

    SIP

- Data for OpenScape Branch

  Comprises the OpenScape Branch configuration file.

  OpenScape Branch CSV

  OpenScape Branch License CSV

- **NOTICE:** This export option is only available if OpenScape Branch is configured.

- Data for OpenScape SBC

  Comprises the OpenScape SBC configuration file

- **NOTICE:** This export option is only available if OpenScape SBC is configured.

NOTICE:

Import/Export of all OpenScape Voice configuration data is not a database restore procedure. If is needed to perform this action, the recommended procedure is to use OpenScape Voice DB Backup-Restore. During Import/Export all OpenScape Voice data are exported but they are re-validated during import. Due to this there are maybe cases where invalid provisioning is rejected due to change of validation rules.

For example, if an OpenScape Voice database was provisioned on a previous OpenScape Voice release/patchset and it was later upgraded to latest/another release, then validation rules on some OpenScape Voice data may have been changed. This will lead to errors later on the Import job for these OpenScape Voice data while some other data where validations rules were not changed, will be imported without errors back to the OpenScape Voice softswitch.

4.6.1 How to Export Data for CMP (Common Management Platform)

How to export data for CMP:

Prerequisites

Adequate administrative permissions

Step by Step

1) Navigate to **Maintenance** > **Recovery** > **Import & Export** > **Export**.

The wizard for exporting data opens.

2) Select in the field **Common Management Platform** one or more options:

- Domain Management
- Domain Management Export for Xpressions
- System Management

3) Click **Next**.

The **Confirm export configuration** window opens. For your control, all configuration settings for the export are displayed.

4) Click **Export**.

   The selected export data are exported and provided for downloading on the Common Management Platform computer system. The duration of this procedure depends on the extent of the exported data.

   If export procedure failed a message window will show the error reason.

5) The export dialog box opens again. At the bottom in **Result of last export** area you find the link to download the export result. Click the **Download last export result** link.

4.6.2 How to Export Assistant Data

Prerequisites

Adequate administrative permissions

Step by Step

1) Navigate to **Maintenance** > **Recovery** > **Import & Export** > **Export**
   The dialog for exporting a configuration is opened.
2) Select in the **OpenScape Voice** field the checkbox **Assistant Data**.
3) From the right pop-up window select one option:
   - switch independent
   - switch specific
   - switch specific with DLS.
4) Define the switch in the field **Select switches**, if you selected a switch specific data file.

NOTICE:

NOTICE:

If there is only one OSV switch connected to the OSV Assistant and you have selected the switch specific Assistant Data this OSV switch will be automatically selected.

---

5) Click **Export**.

   The assistant data is exported to a zip file.

   The default file name is `ExportFile.zip`.

6) The export dialog box opens again. At the bottom in **Result of last export** area you find the link to download the export result. Click the **Download last export result** link.

   A file download browser dialog opens, allowing you to save the zip file to a drive/device on the local system, to a drive/device located on a remote system, or to a network drive.

   The ZIP file exported from the OpenScape Voice Assistant must be decompressed to a local folder - preferably to the folder named `Exported`

`Data/ name_of_zip_file`. This folder will be used as input source for the Offline DB Regeneration Template.

4.6.3 How to Export All OpenScape Voice Configuration Data

Prerequisites

Adequate administrative permissions

Step by Step

1) Navigate to **Maintenance** > **Recovery** > **Import & Export** > **Export**.

The wizard for exporting data opens.

2) Select the desired export options for the OpenScape Voice.

3) Mark the checkbox **All Configuration Data** in OpenScape Voice section.

4) From the right pop-up window, select one of the following options:

- **without default system configuration data** (default): export the OSV data without system default configuration data.
- **include default system configuration data**: export the OSV data with system default configuration data.

5) In drop-down list under **Select switches**, select the OpenScape Voice systems the data of which you want to export.

NOTICE:

If there is only one OSV switch connected to the OSV Assistant, this OSV switch will be automatically selected

---

NOTICE:

Erroneous selection of switches can be corrected (overwritten) by a new selection.

NOTICE:

Import/Export of all OpenScape Voice configuration data is not a database restore procedure. If is needed to perform this action, the recommended procedure is to use OpenScape Voice DB Backup-Restore. During Import/Export all OpenScape Voice data are exported but they are re-validated during import. Due to this there are maybe cases where invalid provisioning is rejected due to change of validation rules.

For example, if an OpenScape Voice database was provisioned on a previous OpenScape Voice release/ patchset and it was later upgraded to latest/another release, then validation rules on some OpenScape Voice data may have been changed. This will lead to errors later on the Import job for these OpenScape Voice data while some other data where validations rules were not changed, will

be imported without errors back to the OpenScape Voice softswitch.

IMPORTANT:

If you have changed the Name of a System Default Entry you will not be able to import them.

---

6) Click **Export**.

The configuration data is exported to a text file.

The Latest Job Status window opens. A Backup is started. Use the link in the area **Result of export job** to download the configuration data.

4.6.4 How to Export OpenScape Voice ENUM (Electronic Number Mapping) Data

How to export ENUM data:

Prerequisites

Adequate administrative permissions

Step by Step

1) Navigate to **Maintenance** > **Recovery** > **Import & Export** > **Export**.

The wizard for exporting data opens.

2) Mark checkbox **Subscriber Numbers in ENUM format**
3) Enter a switch in the **Select switches** field or click **Edit...** and select a switch from the list.

NOTICE:

If there is only one OSV switch connected to the OSV Assistant, this OSV switch will be automatically selected

---

4) Click **OK**
5) Click **Next**.

The **Confirm export configuration** window opens. For your check, all configuration settings for the export are displayed.

6) Click **Export**.

The selected export data are exported and provided for downloading on the Common Management Platform computer system. The ENUM data is exported to a text file. The duration of this procedure depends on the extent of the exported data.

If export procedure failed a message window will show the error reason.

7) The export dialog box opens again. At the bottom in **Result of last export** area you find the link to download the export result. Click the **Download last export result** link.

4.6.5 How to Export Data for OpenScape Branch

Prerequisites

Adequate administrative permissions

Step by Step

1) Navigate to **Maintenance** > **Recovery** > **Import & Export** > **Export**.

   The wizard for exporting data opens.
2) Select the desired export options in the field **OpenScape Branch**.
3) Tick the **Configuration files** check box to activate the **Select appliances** field.

   Tick the **Appliances** and **Licenses** checkbox to export the *OpenScape Branch CSV* and *OpenBranch License CSV* files respectively.

   NOTICE:

   OpenScape Branch CSV and *OpenScape Branch License CSV* files are exported only if at least one configuration file is selected.

   ---
4) Click on **Edit** to select the OpenScape Branch system from which you want to export data.

   The **Select appliances** window opens with a list of all avaialble OSC Branch appliances.
5) Tick the checkbox of all the Branch offices you want to export data and click on **OK** button.

   The **Select appliances** field is populated with the list of **Branch offices** you have selected.
6) Click **Next**.

   The **Confirm export configuration** window opens. For your control, all configuration settings for the export are displayed. If you want to make a correction to the export configuration click on the **Back** button.
7) Click **Export**.

   The selected export data are exported and provided for downloading on the Common Management Platform computer system. The duration of this procedure depends on the extent of the exported data.

   NOTICE:

   If the export procedure fails a message window will show the error reason.

   ---
8) The export dialog box opens again. At the bottom in **Result of last export** area you find the link to download the export result. Click the **Download last export result** link.

4.6.6 How to Export Data for OpenScape SBC (Session Border Controller)

Prerequisites

Adequate administrative permissions

A Centralized SBC branch office is deployed in your configuration.

NOTICE:

If there are no OSC CSBC then the OpenScape SBC section of the Export screen doesn't appear.

Step by Step

1) Navigate to **Maintenance** > **Recovery** > **Import & Export** > **Export**.

The wizard for exporting data opens.

2) Select the desired export options in the field **OpenScape SBC**.

3) Tick the **Configuration files** check box to activate the **Select appliances** field.

4) Click on **Edit** to select the OpenScape SBC system from which you want to export data.

The **Select appliances** window opens with a list of all avaialble OSC SBC appliances.

5) Tick the checkbox of all the Branch offices you want to export data and click on **OK** button.

The Select appliances field is populated with the list of Branch offices you have selected.

6) Click **Next**.

The **Confirm export configuration** window opens. For your control, all configuration settings for the export are displayed. If you want to make a correction to the export configuration click on the **Back** button.

7) Click **Export**.

The selected export data are exported and provided for downloading on the Common Management Platform computer system. The duration of this procedure depends on the extent of the exported data.

NOTICE:

If the export procedure fails a message window will show the error reason.

---

8) The export dialog box opens again. At the bottom in **Result of last export** area you find the link to download the export result. Click the **Download last export result** link.

4.6.7 How to Export Data Scheduled

How to Export Data Scheduled:

Prerequisites

Adequate administrative permissions

Step by Step

1) Navigate to **Maintenance** > **Recovery** > **Import & Export** > **Schedules**.

   The **List of export schedules** window opens.

2) Definition of export schedules:

   - To create a new export schedule: Continue with step 3.
   - To change an existing export schedule: Mark the checkbox of the schedule. Click **Edit**. Continue with step 8.
   - To delete an existing export schedule: Mark the checkbox of the schedule. Click **Delete**.

3) Click **Add**.

   The **Schedule Export** wizard opens.

4) In **Select archive** select an existing archive or create a new one:

   - Type in the name of an archive.
   - Select an archive via Search function **...**.
   - Click **Add...** to add a new archive. Make your settings in the **Add new archive** window. Finish with **Save**.

5) Click **Next**.

   The **Component** window opens.

6) Select a component to export. Click **Next**.

   IMPORTANT:

   Although **OpenScape Branch** and **OpenScape SBC** appliances can be set for normal (manual) export they can't be set for scheduled export and therefore don't appear in the component list. This functionality is not supported by these components.

7) Enter a name for the export schedule.

8) Define the fields **Reoccurs** and **Backup on** (date and time when you want to export).

   IMPORTANT:

   In case, an already created, daily or weekly scheduled job is edited, then after saving the new settings, the job(s) will be executed the next day or next week respectively.

9) Click **Save**.

   An export schedule was defined or changed.

4.6.8 How to Import Data

How to import Data:

Prerequisites

Adequate administrative permissions

IMPORTANT:

Files that are imported to CMP must be UTF-8 encoded.

Step by Step

1) Navigate to **Maintenance** > **Recovery** > **Import & Export** > **Import**.

The dialog for importing a file opens.

2) In the **Import file** field specify the name of the import file (*.csv, *.zip, *.txt).

- Enter the name and path or
- use the **Browse** button to select the file.

IMPORTANT:

It is strongly recommended that you enter a file extension identical to the extension you have downloaded after an export.

---

3) Click on the **Download** button to retrieve the Log file of your last import.

NOTICE:

The Download button is deactivated if there is no log file available.

---

4) Select the **Type of file to be imported**. The pull down menu has the following options:

- Common Management Platform
- OpenScape Voice
- OpenScape Branch
- OpenScape SBC (this option appears only if an SBC is deployed in your system)

5) Select the **Included type of data** to be imported. The pull down menu options depend on the type of file selected in the previous step:

- Common Management Platform

  Domain Management

  System Management
- OpenScape Voice

  All configuration data

  Assistant Data
- OpenScape Branch

  Appliances

  Licenses

  Configuration files (is an option only if OpenScape Branch appliances are deployed in the system)
- OpenScape SBC

  Appliances

  Licenses

  Configuration files (is an option only if OpenScape SBC appliances are deployed in the system)

6) Select the **Target Node** for the file to be imported. Enter the name or use the search function **...**.

NOTICE:

If OpenScape Voice is selected in **Type of file to be imported** and there is only one OSV switch connected to the OSV Assistant, this OSV switch will be automatically selected

---

NOTICE:

Import/Export of all OpenScape Voice configuration data is not a database restore procedure. If is needed to perform this action, the recommended procedure is to use OpenScape Voice DB Backup-Restore. During Import/Export all OpenScape Voice data are exported but they are re-validated during import. Due to this there are maybe cases where invalid provisioning is rejected due to change of validation rules.

For example, if an OpenScape Voice database was provisioned on a previous OpenScape Voice release/ patchset and it was later upgraded to latest/another release, then validation rules on some OpenScape Voice data may have been changed. This will lead to errors later on the Import job for these OpenScape Voice data while some other data where validations rules were not changed, will be imported without errors back to the OpenScape Voice softswitch.

---

7) Click **Import**.

IMPORTANT:

The current log file will be overwritten by the log file of a new import operation.

The import of data is started.

Upon completion of the import a **Report** is generated with a list of system messages (info, warnings, failures) and with a log file available for download.

If the import file is record based, the result of the operation for each record shall be reported.

If the import file is processed as a whole (e.g. the XML file containing the Configuration Data of OSB), the result of the whole operation will be reported.

4.6.8.1 Import Data Report description

The Administrator can view the system generated information/error/warning messages upon completion of an import so he/she can have a quick overview before downloading the log file for further troubleshooting.

After you complete the import process **Maintenance** > **Recovery** > **Import & Export** > **Import** a Report is generated with the following sections:

Summary

Total amount of Errors and Warnings.

Messages

The **Report** screen displays the system generated messages INFO/FAILURES/ WARNINGS.

The maximum amount of messages displayed on the Report screen is 100 items. If this amount is exceeded the following warning is displayed:
`The number of generated messages has exceed the list's capacity. For a complete list of the generated messages please download the log file`

If the import file is record based, the result of the operation for each record shall be reported.If the import file is processed as a whole (e.g. the XML file containing the Configuration Data of OSB), the result of the whole operation will be reported.

File

You can download the file with all the system generated messages by clicking on the **Download** button.

IMPORTANT:

The Report window pops up only after an **Import** action and when you close it you can’t reopen it. However you can download the latest **Import** log file if you navigate to

Maintenance > **Recovery** > **Import & Export** > **Import**

and click **Download**

4.6.9 How to Configure the IM Address by Import

How to configure the IM address by import:

Prerequisites

Adequate administrative permissions

Step by Step

1) Navigate to **Maintenance** > **Recovery** > **Import & Export** > **Export**.

   The wizard for exporting data opens.
2) Export the **Domain Management** component from the Common Management Platform to your local computer.
3) Open the downloaded Zip file.
4) Open the file `Package_domainmanagement_domainmanagement001.zip`.
5) Open the following file with a text editor: `domain_configuration.csv`

   The exported OpenScape UC Application domain information is displayed.
6) Enter the respectively desired voicemail number in the exported file `domain_configuration.csv` in the **imAddress** field of the relevant subscriber entries.

   Example:

##Contact	externalID	...	imAddress	...
Contact	tBrown@system	...	tBrown@imdomain	...

7) Save the supplemented file `domain_configuration.csv` in the CSV format.
8) Overwrite the original file version in the Zip file with the modified file `domain_configuration.csv`.
9) Import the Zip file in the Common Management Platform.

   IMPORTANT:

   Files that are imported to CMP must be UTF-8 encoded.

   You have now created user accounts via the Common Management Platform import feature.

You have configured the Instant Messaging address in the relevant subscriber accounts via the Common Management Platform import feature.

4.6.10 Configuration of Voicemail Numbers

Configuration of user settings are done by the Common Management Platform import feature in OpenScape UC Application, e.g. the voicemail number. This method is particularly useful to configure a setting for a large number of user accounts.

To configure a new voicemail number in user accounts by the Common Management Platform import feature the following steps must be performed:

1) Creation of a new Voicemail Number by Import
2) Configuration of a Voicemail number for User Accounts

4.6.10.1 How to Create a New Voicemail Number by Import

How to create a new voicemail number by import:

Prerequisites

Adequate administrative permissions

Step by Step

1) Export the **Domain Management** component from the Common Management Platform to your local computer.
2) Open the downloaded Zip file.
3) Open the file `Package_domainmanagement_domainmanagement001.zip`.
4) Open the following file with a text editor: `domain_configuration.csv`.

The exported OpenScape UC Application domain information is displayed.

5) Add all voicemail numbers you want to configure in the user accounts in the next section to the exported file `domain_configuration.csv` under **##Voicemail**.

NOTICE:

Always specify phone numbers fully qualified in the GNF format. Example: 492404901100.

---

6) Specify the data for a new voicemail number:

NOTICE:

Separate the fields of an entry from each other with semicolon.

---

a) Enter the reserved name **Voicemails** under **##VoiceMail**. This name defines the entry as entry for a voicemail number.
b) Enter the new voicemail number fully qualified in the GNF format under **id**.
c) Enter the domain to which the new voicemail number shall belong under **domain**.
d) Specify the display name for the new voicemail number under **displayName**.

Example:

##VoiceMail	id	domain	displayName
Voicemails	492404901101	system	492404901101

7) Save the supplemented file `domain_configuration.csv` in the CSV format.
8) Overwrite the original file version in the Zip file with the modified file `domain_configuration.csv`.
9) Import the Zip file in the Common Management Platform.

You have created voicemail numbers via the Common Management Platform import feature.

4.6.10.2 How to Configure a Voicemail Number for User Accounts

How to configure a voicemail number for user accounts:

Prerequisites

Adequate administrative permissions

Voicemail number is created.

Step by Step

1) Export the **Domain Management** component from the Common Management Platform to your local computer.
2) Open the downloaded Zip file.
3) Open the file `Package_domainmanagement_domainmanagement001.zip`.
4) Open the following file `domain_configuration.csv` with a text editor:

   The exported OpenScape UC Application domain information is displayed.

5) Enter the respectively desired voicemail number in the exported file `domain_configuration.csv` in the **assignedVoicemail** field of the relevant user entries.
   a) Go to **##User**
   b) Select the wanted user below **##User** from one of the fields **id** or **displayName**.
   c) Go to field **assignedVoicemail** of this user.
   d) Enter the Voicemail number.

   NOTICE:

   Always specify phone numbers fully qualified in the GNF format. Example: 492404901100.

   Example:

##User	id	domain	displayName	assignedVoicemail
User	tBrown	system	Tony Brown	4924049011001

6) Save the supplemented file `domain_configuration.csv` in the CSV format.
7) Overwrite the original file version in the Zip file with the modified file `domain_configuration.csv`.
8) Import the Zip file in the Common Management Platform.

   IMPORTANT:

   Files that are imported to CMP must be UTF-8 encoded.

You have configured the created voicemail number in the relevant subscriber accounts via the Common Management Platform import feature.

4.6.10.3 How to Create User Accounts by Import

How to create user accounts by import:

Prerequisites

Adequate administrative permissions

Step by Step

1) Export the **Domain Management** component from the Common Management Platform to your local computer.
2) Open the downloaded Zip file.
3) Open the file `Package_domainmanagement_domainmanagement001.zip`.
4) Open the following file with a text editor: `domain_configuration.csv`.

   The exported OpenScape UC Application domain information is displayed.

5) Insert the information of the users that you want to add to the CMP in the exported file `domain_configuration.csv` under **##User** .

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:

Separate the fields of an entry from each other with semicolon.

---

a) Enter the reserved name **User** in the user entry under **##User**. This name defines the entry as user entry.
b) Specify the ID (Login name from CMP) for the new user in the user entry under **id**.
c) Enter the domain to which the new user shall belong in the user entry under **domain**.
d) Specify the display name for the new user in the user entry under **displayName**.

Example:

##User	id	domain	displayName	...
User	tBrown	system	Tony Brown	...

6) Insert the information of the users that you want to add to the CMP in the exported file `domain_configuration.csv` under **##Contact**.

NOTICE:

Separate the fields of an entry from each other with semicolon.

---

a) Enter the reserved name **Contact** in the contact entry under **##Contact**.
b) Enter the user ID from step 5b in the contact entry under **externalId** in the following format: <User ID>@<domain>.
c) Go to field named **assignedSymUserIdentity** in the data structure for ##Contact. This field is used by the OpenScape system when importing data to assign the correct user entry to the contact entry.
d) Specify under **assignedSymUserIdentity** the information from the **externalId** contact field.

Example:

##Contact	externalID	...	assignedSymUserIdentity
Contact	tBrown@system	...	tBrown@system

7) Save the supplemented file `domain_configuration.csv` in the CSV format.
8) Overwrite the original file version in the Zip file with the modified file `domain_configuration.csv`.

9) Import the Zip file in the Common Management Platform.

IMPORTANT:

Files that are imported to CMP must be UTF-8 encoded.

You have created user accounts via the Common Management Platform import feature.

4.6.11 How to Delete Information by Import

You can use the import feature to import configuration information in the OpenScape UC Application database. This method is particularly useful when you need to configure settings for a large number of user accounts.You can use the import feature to also remove a large amount of configuration information from the OpenScape UC Application database. You only need to prefix the relevant entry in the import file with the deletion code d: for this purpose.To remove, for example, a user account with its contact data from the OpenScape UC Application database, import the following lines:

##Use	id	doma	identity	publishedResourc	passw	homeTime	e
d:User	mSamp	syste	mSample@sy	4924	! Osc123+	Europe/ Berlin	de_de

##Contact	externalID	displayName	assignedSymUserIdentity
d:Contact	mSample@system	Monica Sample	mSample@system

```
##User;id;domain;identity;publishedResource;password;homeTimeZone;defaultLocale
```

```
d:User;mSample;system;mSample@system;4924049011001@CS1;!
Ocs123+;Europe/Berlin;de_DE
```

##Contact;externalId;displayName;assignedSymUserIdentity

d:Contact;mSample@system;Monica Sample;mSample@system

4.7 Backup and Restore Concept

You can back up the file systems and the configuration data of the OpenScape system in regular intervals or when required. By using the information backed up in this way you can:

- Completely restore the file systems of the CMP/UC Application computer systems

- Partly or completely restore the configuration data of the OpenScape system

  IMPORTANT:

  For Partial Data backup/restore of UC Data in deployments with more than one UC nodes the following restrictions are applied:

  Partial Data Backup:

  -A node that is down during backup will not be backed-up.

  The Data Restore will be blocked if:

  - A node was backed-up, but during restore is down.

  - A node was not backed-up, but during restore is up.

IMPORTANT:

Starting with OpenScape UC V11R1, the File System Backup/ Restore option is no longer supported for the application server.

Furthermore, OpenScape Web Client data is backed up by an automatic backup process. You can then restore the OpenScape Web Client with its configuration from the backed up data anytime.

IMPORTANT:

Backing up a non-LVM-based file system of a CMP/UC Application computer system for Standard Duplex requires installing the dump RPM package on the relevant computer system.

IMPORTANT:

Backing up the file system of a CMP/UC Application computer system for Standard Duplex requires the hard disk drives of the relevant computer system using ext3/ext2 or be LVM based.

IMPORTANT:

Restoring an LVM file system backup to a **new** hard disk requires that prior to executing `lvRestoreUtility.sh`, it is necessary to create manually the partitions on the new disk, **exactly** as they were on the system, the backup was taken on. Especially the logical volumes on the new disk should have the same name and size.

IMPORTANT:

Although the default `root` directory for **File System** backup is `var/siemens/backup` the file system backup is always saved in `/software/backup/` directory.

IMPORTANT:

If the system is LVM based, there is a remote possibility that during the backup the snapshot of the root partition failed to be removed. In that case a critical alarm is raised to indicate this fact to the administrator. This alarm is critical because a root snapshot that is not removed, is a hanging resource that may lead to performance degradation, instability, and may eventually lead to host system reboot.

If the above occurs you must try and remove the root snapshot manually. You must make sure that no directory is mounted, and then execute the following: `lvremove -f <rootsnapshot_name>`

4.7.1 Archives

Each archive defines a memory location under which created backup sets are stored. It also defines how this memory location can be accessed.

You can specify archives on local or remote computer systems. A remote computer system can be accessed via the following protocols:

- FTP
- SFTP

NOTICE:

You ideally store archives always in parallel on a remote SFTP# FTP server and on the local computer system. In this way you prevent the backup information from getting irretrievably lost in case of a system crash. The backup information is in the ideal case then also locally available.

An archive may contain a configurable number of backup sets. If the number of backup sets you store in an archive is greater than has been configured, the respectively oldest backup sets are overwritten.

You can assign a password to protect an archive from unauthorized access.

4.7.1.1 How to Display Archives

How to display Archives :

Prerequisites

Adequate administrative permissions

Step by Step

1) On the **Maintenance** navigation tab click on the **Recovery** navigation menu item.

2) In the navigation tree, click on **General** > **Archives**

A list of all archives that are configured in the selected domain appears in the work area.

- Archive name

  Name of the archive. Under this name the archive is administered in the Common Management Platform.
- Protocol

  Protocol via which access to the archive is possible.
- Acting node

  The acting node is defined as the node the final backup set will be stored in, not on which node the backup will start initially.
- Path

  Path under which the archive is stored on the specified node.
- Server Address (for FTP or SFTP only)

  Server address of the computer system on which the archive is stored via FTP or SFTP
- Login name (for FTP or SFTP only)

  User name used to access the server computer.

4.7.1.2 How to Add an Archive

Prerequisites

Adequate administrative permissions

IMPORTANT:

You ideally store OpenScape system archives on an external SFTP / FTP server and the local computer system. In this way you prevent the backup information from getting irretrievably lost in case of a system crash and it also locally available.

Step by Step

1) On the **Maintenance** navigation tab click on the **Recovery** navigation menu item.
2) In the navigation tree, click on **General** > **Archives**.

   A list of all archives that are configured in the selected domain appears in the work area.
3) Click on **Add**.

   The dialog with the archive settings opens.
4) Under **Name** enter a short, unique name for the new archive.

   Under this name the archive is administered in the Common Management Platform.

5) In case you have a Large deployment system and you are adding a Data backup archive you must select the Acting node.

NOTICE:

The acting node is defined as the node the final backup set will be stored in, not on which node the backup will start initially.

6) From the Protocol drop-down list select the protocol via which the archive is to be saved.

- **HD**, to locally store the archive on the server computer.

  NOTICE:

  If HD protocol is selected then for Data backup the backed files will be stored at the acting node under the defined path.

- **FTP**, to store the archive via FTP on a computer system in the network.

  NOTICE:

  For the deployment scenario Integrated Simplex of OpenScape UC Application applies: To save an archive via FTP, a corresponding packet filter must be configured in OpenScape Voice.

- **SFTP**, to store the archive via Secure FTP on a computer system in the network.

  NOTICE:

  For the deployment scenario Integrated Simplex of OpenScape UC Application applies: To save an archive via SFTP, a corresponding packet filter must be configured in OpenScape Voice.

7) If you have selected the **HD** protocol, enter in the **Path on file system** field an absolute path in which the archive is to be saved.

```
/var/siemens/backup
```

NOTICE:

Special characters in the path are not supported .

NOTICE:

For the base directory of the entered path the read / #write attributes must have been set. You can set these attributes with the following command: `chmod 777 <Base directory>`

8) When you have selected the **FTP** or **SFTP** protocol, proceed as follows:
   a) In the **Path to server** field enter an absolute path in which the archive is to be stored.

      `/ftp/siemens/backup`

      NOTICE:

      Special characters in the path are not supported .

   b) Enter under **Server address** the server address of the computer system on which the archive is to be stored.
   c) Under **Login name** and **Password**, enter the user name and the password to be used for access to the server computer.

      IMPORTANT:

      The special characters double quotes (") and comma (,) are not supported in the Password field.

9) In the **Maximum number of backup sets** section use the **Data** and **System** fields to specify the maximum number of backup sets of type Data or System to be stored in the archive.
10) If you want to save the archive data encrypted, enter the encryption password under **Encryption password** and **Confirm encryption password**.
11) Click on **Save** to copy the entries to the system's database.

The new archive is saved and displayed in the archives list.

4.7.1.3 How to Edit an Archive's Settings

How to edit an Archive’s Setting:

Prerequisites

Adequate administrative permissions

Step by Step

1) On the **Maintenance** navigation tab click on the **Recovery** navigation menu item.
2) In the navigation tree, click on **General** > **Archives**.

   A list of all archives that are configured in the selected domain appears in the work area.
3) Click on the name of the archive the settings of which you want to edit.

   The dialog with the settings of the relevant archive opens.
4) Perform the desired setting modifications for the relevant archive.
5) Click on **Save** to copy the entries to the system's database.

4.7.1.4 How to Delete an Archive

How to delete an Archive:

Prerequisites

Adequate administrative permissions

Step by Step

1) On the **Maintenance** navigation tab click on the **Recovery** navigation menu item.
2) In the navigation tree, click on **General** > **Archives**.

   A list of all archives that are configured in the selected domain appears in the work area.
3) Select the checkboxes of the archives that you want to delete.

   NOTICE:

   The DEFAULT archive cannot be deleted.
4) Click on **Delete**.
5) Click on **OK** to confirm the deletion of the selected archives.

The selected archives are removed from the system's database and from the list of all archives.

4.7.1.5 How to Test an Archive

Here you can test whether you are able to access an archive. A check is made as to whether the computer system can be accessed and whether files can be created and deleted in the desired directory.

Prerequisites

Adequate administrative permissions

Step by Step

1) On the **Maintenance** navigation tab click on the **Recovery** navigation menu item.
2) In the navigation tree, click on **General** > **Archives**.

   A list of all archives that are configured in the selected domain appears in the work area.
3) Select the checkbox of the archive you want to test.
4) Click on **Test archive**.

   You will be informed about the test results in a separate window.
5) Click on **Close** to close this informational window.

4.7.1.6 How to Display/Edit an Archive's Backup Sets

How to Display an Archive’s Backup Sets

Prerequisites

Adequate administrative permissions

Step by Step

1) On the **Maintenance** navigation tab click on the **Recovery** navigation menu item.
2) In the navigation tree, click on **General** > **Archives**.

   A list of all archives that are configured in the selected domain appears in the work area.
3) Select the checkbox that associates the archive the backup set of which you want to edit.
4) Click on **View backup sets**.

   A window opens that displays the backup sets of the selected archive.
5) To display the content of a backup set, select the checkbox that associates the relevant backup set and click on **Show content**.
6) To display or change the comment of a backup set, select the checkbox that associates the relevant backup set and click on **Edit comment**.
7) To display the information that was created during the generation of the backup set, select the checkbox that associates the relevant backup set and click on **Show reply**.
8) Click on **Close** to close the window.

4.7.1.7 How to Delete an Archive's Backup Sets

How to delete an Archive’s Backup Set:

Prerequisites

Adequate administrative permissions

Step by Step

1) Select in the **Domain** drop-down list of the toolbar the domain in which you want to delete an archive.
2) On the **Operation& Maintenance** navigation tab click on the **Recovery** navigation menu item.
3) In the navigation tree, click on **General** > **Archives**.

   A list of all archives that are configured in the selected domain appears in the work area.

4) Select the checkbox that associates the archive from which you want to remove the backup sets.

NOTICE:

The DEFAULT archive cannot be deleted.

---

5) Click on **View backup sets**.

   A window opens that displays the backup sets of the selected archive.

6) Select the checkboxes of the backup sets that you want to delete.
7) Click on **Delete**.
8) Click on **OK** to confirm the deletion of the selected backup sets.

The selected backup sets are removed from the system's database and from the list of all backup sets.

4.7.2 Backup Sets

A backup set contains all information that was saved for the OpenScape system during a backup run.

System configurations and system data (backup units) can be backed up in a backup set and we distinguish two types of backup units.

- System

  Backup units that contain entire file systems.
- Data

  Backup units that contain configuration data.

Each backup set may only contain backup units of a single type and is saved in an archive.

Each archive can contain several backup sets. If the number of backup sets saved exceeds the value set for the archive, the oldest backup sets are cleared.

You can display all the backup sets present in the system. Alternatively however you can also have all the backup sets for an archive displayed (see).

Backup units

The list of offered backup units depends on the type and number of installed applications. The following backup units may be available:

- **OpenScape Voice**
- **RG 8700**
- **OpenScape Branch**
- **OpenScape SBC**

- **Application Server** (OpenScape UC Application)

  The following subordinate backup units are available for this backup unit when the backup type **Data** is selected:

  – **Audit Log Files**

    Backs up the log information of the audit log.
  – **Backup & Restore Service**

    Backs up the database for backup & restore.
  – **Cmp Syslog Audit**

    Backs up the configuration file for logging via Syslog. This comprises the host ID, audit status and the actual Syslog configuration.
  – **Conferencing Applets Service**

    Backs up the media-server-related files and the configuration file of the conference portal.
  – **Conferencing Service**

    Backs up the conference database and the configuration file of the conference service.
  – **Container Configuration Files**

    Backs up the configuration entries that concern the single OpenScape services.
  – **Deployment Service**

    Backs up the database information and the configuration file of the deplioyment service.
  – **Domain and License Management Service**

    Backs up the database for the domain management, license management and the contact list.
  – **Groupware Service**

    Backs up the groupware-related files and the associated configuration files.
  – **Installation Files**

    Backs up the answer file of the installation.
  – **lib-logging**

    Backs up the files `log4j.xml` and the `default_log4j.xml`.
  – **lib-snmpdbaccess**

    Backs up the SNMP traps that are sent during operation and stored in the database of the error management.
  – **Logfile Audit Configuration**

    Backs up the configuration file for the audit log.
  – **Media Server**

    Backs up the media-server-related files.
  – **OpenScape Branch Assistant Data**

    Backs up the database and the data of the OpenScape Branch Assistant.
  – **OpenScape Voice Assistant Data**

    Backs up the database and the data of the OpenScape Voice Assistant.
  – **Presence Management Component**

Backs up the Presence Acl database.

– **Presence Target Service**

Backs up the Presence Target database.

– **Presence Configuration File**

Backs up the configuration file of the Presence service.

– **Presence Service**

Backs up the Presence database.

– **Presence XMPP Connector**

Backs up the Presence XMPP connector database.

– **Rules Service**

Backs up the Rule database.

– **Scheduler Service**

Backs up the database for the time-controlled jobs of the Scheduler service.

– **svc-alarmhandler**

Backs up alarms received during operation and stored in the database of the error management.

– **svc-faulthandler**

Backs up error messages received during operation and stored in the database of the error management.

– **svc-loggingconfigmanager**

Backs up the file `loggermanager_<guid>_localhost.xml` that contains the configuration for Trace-on-Resource and Online-Trace.

– **svc-onlinetrace**

Backs up the configuration file for Online Trace.

– **Voice Portal**

Backs up the voice-portal-related files.

– **Web Client Configuration Backup**

Backs up the files for configuring the Web Client.

– **Web Client Database Backup**

Backs up the database of the Web Client.

– **Workflow Engine**

Backs up the database of the Workflow Engine.

•

Archives

Each archive defines a memory location under which created backup sets are stored. It also defines how this memory location can be accessed.

You can specify archives on local or remote computer systems. A remote computer system can be accessed via the following protocols:

- FTP
- SFTP

NOTICE:

You ideally store archives always in parallel on a remote SFTP# FTP server and on the local computer system. In this way you prevent the backup information from getting irretrievably lost in case of a system crash. The backup information is in the ideal case then also locally available.

An archive may contain a configurable number of backup sets. If the number of backup sets you store in an archive is greater than has been configured, the respectively oldest backup sets are overwritten.

You can assign a password to protect an archive from unauthorized access.

Backup Schedules

You can use a backup schedule to automatically back up the configuration and data of the OpenScape system.

Jobs

The OpenScape system executes different administration processes in so-called jobs, which you control and monitor in the Common Management Platform. Each job comprises selected backup units that are successively processed by the job.

The following administration processes are executed in the OpenScape system as jobs:

- Backup of system units
- Restore of system units
- Export of configuration data
- Import of configuration data

4.7.2.1 How to Display/Edit the Settings of a Backup Set

How to display all backup sets available in the system:

Prerequisites

Adequate administrative permissions

Step by Step

1) On the **Maintenance** navigation tab click on the **Recovery** navigation menu item.

2) In the navigation tree, click on **General** > **Backup Sets**.

   A list of all backup sets configured in the selected domain appears in the work area with following attributes:

   Archive name

   Name of the archive in which the backup set is saved.
   Creation date

   Date on which the backup set was created.
   Status

   Shows whether or not there are any faults in the backup set.
   Comment

   Comment, entered when the backup set was created (optional).
   Type

   Type of the backup units to be saved in the backup set.
   Service Release

   Version of the application
   Action by

   User that performed the backup action
3) To display the content of a backup set, select the checkbox that associates the relevant backup set and click on **Show content**.
4) To display or change the comment of a backup set, select the checkbox that associates the relevant backup set and click on **Edit comment**.
5) To display the information that was created during the generation of the backup set, select the checkbox that associates the relevant backup set and click on **Show reply**.
6) Click on **Close** to close the window.

4.7.2.2 How to Delete a Backup Set

How to remove a backup set from an archive:

Prerequisites

Adequate administrative permissions

Step by Step

1) On the **Maintenance** navigation tab click on the **Recovery** navigation menu item.
2) In the navigation tree, click on **General** > **Backup Sets**.

   A list of all backup sets configured in the selected domain appears in the work area.
3) Select the checkboxes of the backup sets that you want to delete.
4) Click on **Delete**.
5) Click on **OK** to confirm the deletion of the selected backup sets.

The selected backup sets are removed from the system's database and from the list of all backup sets.

4.7.2.3 How to Restore the Entire System After a Crash

How to restore the entire system after a crash:

Prerequisites

Adequate administrative permissions

You backed up the configuration and data of the OpenScape system in an archive before the crash.

The archive's data have not been damaged by the crash.

You have restored the file system of the computer systems concerned.

IMPORTANT:

You ideally store OpenScape system archives on an external SFTP / FTP server and the local computer system. In this way you prevent the backup information from getting irretrievably lost in case of a system crash. The backup information is in the ideal case then also locally available.

A system crash of the OpenScape system may damage system files. If this happens, you need to reinstall the OpenScape system before you can restore the configuration and the data of the OpenScape system.

When reinstalling, definitely use the answer file you have created for the initial installation for the following reasons:

- 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 restore the OpenScape system on another computer system, you 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 components of the OpenScape system are deactivated on this computer system.

NOTICE:

If you try to restore a database whose version is not compatible with the database version of the OpenScape Voice system, the restoration will not be performed. A corresponding error code will be displayed instead. In this case, please contact the next higher support level. You can avoid this scenario by always creating a

database and file system backup after the following activities: patchset installation, RTP-MOP installation and SolidEngine-MOP installation.

Step by Step

1) On the **Maintenance** navigation tab click on the **Recovery** navigation menu item.

2) In the navigation tree, click on **Backup& Restore** > **Restore**.

The restore wizard dialog opens.

3) Select with **…** the archive in which the desired backup set is stored.

In some cases the restore wizard do not display an archive for restoring the system elements – e. g. after a severe system crash. In this case, execute the following steps to restore the reference to an existing archive:

NOTICE:

When you restore an archive from the local file system, the restoration process operates under the Unix user account sym. Verify that all files of the relevant archive can be accessed with sym. If the system cannot access the files, you will be notified by a corresponding error message.

a) Click on **Add**.

The dialog with the archive settings opens.

b) Enter any archive name in the **Archive name** field.

c) In the **path on file system** field specify the path under which you previously stored the archive that you now want to use for restoring the system elements.

d) Click on **Save**.

The archive can now be selected in the restore wizard provided that the archive data are not damaged.

4) Click on **Next**.

5) Select the backup set that you want to use to restore the OpenScape system.

6) Click on **Next**.

The backup units of the selected backup set are displayed.

7) Select besides the **OpenScape Voice** backup unit all units for restoration.

In doing so be sure to select the units of all representable pages.

NOTICE:

If you do not want to restore specific units, exclude them from your selection.

NOTICE:

If you want to restore the configuration of OpenScape Voice, too, select the **OpenScape Voice** backup unit also.

8) Click on **Start Restore**.

   The restore starts according to the settings made. The restore progress is then graphically displayed.

9) If you use OpenScape UC Application, restart OpenScape UC Application with the following commands.

   a) `/etc/init.d/symphoniad stop`

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

10) The password for the administrator account `administrator@system` is after the data restoration reset to the value that was valid when the backup files were stored. If you want to allocate a new password for the administrator account `administrator@system`, execute the following command.

   - <Osc#Install [12]>`/servicetools/security/resetUserAccount.sh administrator@system` <new password >

4.7.3 Backup Schedules

You can use a backup schedule to automatically back up the configuration and data of the OpenScape system.

NOTICE:

Backing up a non-LVM-based file system of a UC Application computer system for Standard Duplex requires installing the dump RPM package on the relevant computer system

NOTICE:

Backing up the file system of a UC Application computer system for Standard Duplex requires the harddisk drives of the relevant computer systems using ext3 on LVM2

4.7.3.1 How to Display Backup Schedules

How to display a backup schedule:

Prerequisites

Adequate administrative permissions

Step by Step

1) On the **Maintenance** navigation tab click on the **Recovery** navigation menu item.

12 <Osc-Install > is the setup file of the OpenScape system: /opt/siemens/ or /enterprise/

2) In the navigation tree, click on **Backup& Restore** > **Schedules**

A list of all backup schedules configured in the selected domain appears in the work area.

After installation, Default_System_Backup (reoccurs every Sunday at 3:00 AM) and Default_Data_Backup (reoccurs daily at 1:00 AM) schedules are automatically created from the system. Default backup is disabled whenever a user defined backup schedule is defined and active for both the backup methods.

IMPORTANT:

If you have in the list configured schedules from previous versions you must delete them and add them again for this current version. This action must be performed to eliminate any inconsistency in the backup units. The same action should also be performed during HotFix updates within the same version.

---

3) Select the checkbox that associates the backup schedule the settings of which you want to edit.

- Name

  Name of the schedule.
- Archive name

  Name of the archive in which the backup set is saved
- Reoccurs

  Setting showing when and how often the schedule is repeated
- Day (for weekly backup only)

  Day of backup.
- Time

  Time of backup
- Remaining occurences

  Shows how the schedule is repeated

4.7.3.2 How to Add a Backup Schedule

Prerequisites

Adequate administrative permissions

Backing up the file system of a OpenScape UC Application computer system in a Duplex deployment scenario requires the installation of the dump RPM packet on the corresponding computer system.

Backing up the file system of a OpenScape UC Application computer system in a Duplex deployment scenario requires for the hard disk drives of the corresponding computer system the use of the ext3 file system on LVM2.

Backing up the file system of a OpenScape UC Application computer system in a Duplex deployment scenario requires the following lines at the end of the file `etc/sudoers`:

```
sym ALL=NOPASSWD:/opt/siemens/servicetools/backup/
lvBackupManagentUtility.sh

sym ALL=NOPASSWD:/opt/siemens/servicetools/backup/
fsBackup.sh
```

When you have also installed the OS Composer, you must administer backups either by the Composer or CMP only, to avoid conflicts.

Step by Step

1) On the **Maintenance** navigation tab click on the **Recovery** navigation menu item.

2) In the navigation tree, click on **Backup& Restore** > **Schedules**.

A list of all backup schedules configured in the selected domain appears in the work area.

3) Click on **Add**.

The backup wizard dialog opens.

IMPORTANT:

If you have in the list configured schedules from previous versions you must delete them and add them again for this current version. This action must be performed to eliminate any inconsistency in the backup units. The same action should also be performed during HotFix updates within the same version

---

.also during HF updates within the same version

NOTICE:

If you have in the list configured schedules from previous versions you must delete them and add them again for this current version. This action must be performed to eliminate any inconsistency in the backup units.

---

4) Select the archive to which the backup schedule is to be added.

NOTICE:

Backing up the file systems of the OpenScape UC Application computer systems for a Duplex deployment scenario, you must select the DEFAULT archive.

- Use the **…** button to select an existing archive.
- Click on the **Add** button to create a new archive.

5) Click on **Next**.

6) Select the **backup type** of the backup units which are to be backed up.

7) How to back up only selected backup units for OpenScape UC Application:
   a) Click on the name of the Application Server backup unit.

      A dialog box opens displaying the individual OpenScape UC Application backup units.
   b) Select the checkbox of the backup units you want to back up for OpenScape UC Application
   c) Click on **Save**
8) Select the backup units to be saved.
9) Click on **Next**.
10) Enter a short, unique name for the new schedule under **Name**.

    Under this name the schedule is administered in the Common Management Platform.
11) In the **Reoccurs** drop-down list, select the frequency with which the backup is to be repeated.
12) Specify in the **Backup on** field at which time the backup is to start.
13) In the **Occurrences** drop-down list select the frequency with which the backup is to be repeated.
14) Click on **Save** to copy the entries to the system's database.

The new backup schedule is saved and displayed in the list of backup schedules.

4.7.3.3 How to Edit Backup Schedules

How to edit a backup schedule:

Prerequisites

Adequate administrative permissions

Step by Step

1) On the **Maintenance** navigation tab click on the **Recovery** navigation menu item.
2) In the navigation tree, click on **Backup& Restore** > **Schedules**.

   A list of all backup schedules configured in the selected domain appears in the work area.
3) Select the checkbox that associates the backup schedule the settings of which you want to edit.
4) Click on **Edit**

   The dialog with the settings of the relevant backup schedule opens.
5) In the Reoccurs drop-down list, select the frequency with which the backup is to be repeated
6) Specify in the Backup on field at which time the backup is to start.
7) In the Occurrences drop-down list select the frequency with which the backup is to be repeated
8) Click on **Save** to copy the entries to the system's database.

4.7.3.4 How to Delete a Backup Schedule

How to delete a backup schedule:

Prerequisites

Adequate administrative permissions

Step by Step

1) On the **Maintenance** navigation tab click on the **Recovery** navigation menu item.
2) In the navigation tree, click on **Backup& Restore** > **Schedules**.

   A list of all backup schedules configured in the selected domain appears in the work area.
3) Select the checkboxes of the backup schedules that you want to delete.
4) Click on **Delete**.
5) Click on **OK** to confirm the deletion of the selected backup schedules.

The selected backup schedules are removed from the system's database and from the list of all backup schedules.

4.7.4 Jobs

The OpenScapesystem executes different administration processes in so-called jobs, which you control and monitor in the Common Management Platform. Each job comprises selected backup units that are successively processed by the job.

The following administration processes are executed in the OpenScape system as jobs:

- Backup of system units
- Restore of system units
- Export of configuration data
- Import of configuration data

4.7.4.1 How to Display the Job Status

Status information about the last executed or currently active job is stored and displayed in the Common Management Platform. Such jobs can involve backup, restore or an import or export of data.

Prerequisites

Adequate administrative permissions

Step by Step

1) On the **Maintenance** navigation tab click on the **Recovery** navigation menu item.

2) In the navigation tree, click on **General** > **Latest Job**.

   The work area displays status information that concerns the last executed or currently active job and its backup units.

   - **Operation**

     Job type
   - **Archive name**

     Name of the archive used.
   - **Backup type**

     Type of the processed backup units.
   - **Overall status**

     Overall status of the job (OK, ERROR, RUNNING, STOPPED, WAITING)
   - **User**

     The login name of the user that initiated the backup
   - **Backup unit**

     Type of the processed backup units.
   - **Start**

     Time when processing of the respective backup unit started
   - **End**

     Time when processing of the respective backup unit ended.
   - **Status**

     Processing status of the respective backup unit (OK, ERROR, RUNNING, STOPPED, WAITING)
   - **Messages**

     Display of warnings and error messages for processing the respective backup unit.
   - **Percentage**

     Displays the progress during file system backup that is only applicable to an Application Server and OpenScape Voice filesystem backup.

3) The job display refreshes automatically every 20 seconds. You can update the display at any time by clicking on **Refresh**.

4) If you want to display further details of the last performed job, click on **Details**.

   NOTICE: The **Details** button is not available until the job has been fully processed.

4.7.4.2 How to Terminate a Job

A job can be a backup, a restoration or an import or export of data.

Prerequisites

Adequate administrative permissions

Step by Step

1) On the **Maintenance** navigation tab click on the **Recovery** navigation menu item.
2) In the navigation tree, click on **General** > **Latest Job**.

   The work area displays status information that concerns the last executed or currently active job and its backup units.
3) While a job is being executed you can:
   - You can use the **Cancel Running** button to cancel the processing of the backup unit being edited.

     The job will then start processing the next backup unit.

     NOTICE: This button is not available until a job is being processed.
   - You can use the **Cancel All** button to cancel the processing of all backup units.

     The job is then immediately terminated.

     NOTICE: This button is not available until a job is being processed.

NOTICE:

Canceling a backup unit processing will take some time. If processing of a backup unit can be completed within this period, this processing will actually not be canceled.

NOTICE:

Canceling fully works for UC application. For any other, import and restore operations continue in the background. A new import or restoration is possible but the already running will continue.

4.7.5 How to Back Up a Backup Set Manually (Immediate Backup)

Besides the automatic backup schedules you can start the backup also manually.

Prerequisites

Adequate administrative permissions

Backing up the file system of a OpenScape UC Application computer system in a Duplex deployment scenario requires the installation of the dump RPM packet on the corresponding computer system.

Backing up the file system of a OpenScape UC Application computer system in a Duplex deployment scenario requires for the hard disk drives of the corresponding computer system the use of the ext3 file system on LVM2.

Backing up the file system of a OpenScape UC Application computer system in a Duplex deployment scenario requires the following lines at the end of the file `etc/sudoers`:

```
sym ALL=NOPASSWD:/opt/siemens/servicetools/backup/
lvBackupManagentUtility.sh

sym ALL=NOPASSWD:/opt/siemens/servicetools/backup/
fsBackup.sh
```

Enough empty disk space for the directory `/tmp` on the computer system.

NOTICE:

If there is not enough empty disk space for the directory `/tmp`, the backup process will aboard with an error message.

When you have also installed the OS Composer, you must administer backups either by the Composer or CMP only, to avoid conflicts.

Step by Step

1) On the **Maintenance** navigation tab click on the **Recovery** navigation menu item.
2) In the navigation tree, click on **Backup& Restore** > **Backup**.

   The backup wizard dialog opens.
3) Select the archive to which the backup set is to be added.

   NOTICE:

   Backing up the file systems of the OpenScape UC Application computer systems for a Duplex deployment scenario, you must select the DEFAULT archive.

   - Use the **…** button to select an existing archive.
   - Click on the **Add** button to create a new archive.
4) Click on **Next**.
5) Select the **backup type** the backup units of which are to be backed up.
6) Select the **backup units** to be backed up.

   NOTICE:

   For Openscape Enterprice Express applications, **OpenScape Enterprice Express (includes CMP,<OSEE components>)** option is available in order to proceed with the backup of all the configured applications.

   If this option is selected, the Openscape Enterprice Express applications are not displayed separately any more.

   If you choose to backup the File System and also activate the new V7 OpenScape UC script "syncUC" then you must make sure the local hard disk space is sufficient. For new installations the minimum requirement is 300GB

and the table below illustrates the optimum partition configuration to support File System backup and OpenScape UC script "syncUC" :

Partition	Partition Type	Calculation formula	size in GB[13]
Hard disk for syncUC	Hard Disk	N [14]	300
/boot	Primary	2	2
Swap	Primary	2	2
LVM2 memory	Primary	N-4	296
Logical volume group	Logical volume group		
Root partition (/) in the LVM2 memory for active operation of the OpenScape UC Application	Logical	(N-4)/3	98,7
Partition for fallback by means of syncUC	Logical	(N-4)/3	98,7
Partition for File System backup [15]	Logical	0.9*(N-4)/3	88,8
Temporary snapshot [16]	Logical	0.1*(N-4)/3	9,9

IMPORTANT:

The difference of GibiByte (1024^3 as used in SLES) and GB (1000^3 as used by some disc vendors) may lead to different figures when performing partitioning in SLES 11 (1GiB≈1.074GB), However the calculation formula is valid.

If you choose to backup the File System and also activate the new V7 OpenScape UC script "syncUC" but the local hard disk space is not sufficient

[13] For the minimum size of 300 GB

[14] Hard disk size is defined as N

[15] This logical volume is created automatically when the file system is backed up for the first time. It need not be created manually.

[16] This logical volume is created automatically when the file system is backed up. It need not be created manually.

you must use an external USB Hard Disk drive to backup your File System. The relative chapter describes this process.

IMPORTANT:

If the system is LVM based, there is a remote possibility that during the backup the snapshot of the root partition failed to be removed. In that case a critical alarm is raised to indicate this fact to the administrator. This alarm is critical because a rootsnapshot that is not removed, is a hanging resource that may lead to performance degradation, instability, and may eventually lead to host system reboot.

If the above occurs the administrator must try and remove the rootsnapshot manually. He should make sure that no directory is mounted, and then execute the following:
`lvremove -f <rootsnapshot_name>`

7) Click on **Start backup**.

The backup starts according to the settings made.

NOTICE:

The backup percentage completion rate is displayed when backing up a file system as this function takes a long time particularly when backing up the file system to external SFTP/ FTP server.

The percentage completion rate is displayed as “N/A” when backing up the data since this function takes a short time to complete when compared to backing up a file system.

4.7.5.1 How to Back Up a File System with an External USB hard disk on an LVM based deployment.

If you choose to backup the File System and the new V7 OpenScape UC script "syncUC " is *running* then it is possible that your local hard disk space is not sufficient and you must use an external USB Hard Disk drive to backup your File System.

Prerequisites

Adequate administrative permissions

Backing up the file system of a OpenScape UC Application computer system in a Duplex deployment scenario requires the installation of the dump RPM packet on the corresponding computer system.

Backing up the file system of a OpenScape UC Application computer system in a Duplex deployment scenario requires for the hard disk drives of the corresponding computer system the use of the ext3 file system on LVM2.

Backing up the file system of a OpenScape UC Application computer system in a Duplex deployment scenario requires the following lines at the end of the file `etc/sudoers`:

```
sym ALL=NOPASSWD:/opt/siemens/servicetools/backup/
lvBackupManagentUtility.sh

sym ALL=NOPASSWD:/opt/siemens/servicetools/backup/
fsBackup.sh
```

Enough empty disk space for the directory `/tmp` on the computer system.

NOTICE:

If there is not enough empty disk space for the directory `/tmp`, the backup process will aboard with an error message.

The external USB can be used for a File System backup only on an LVM based deployment and must have at least the space calculated in the partition configuration table in step 6.

The local, external USB hard disk must have be formatted with ext3, because NTFS is not natively supported by SLES 11 and FAT32 does not support files bigger than 4 GB.

- The File System backup script `lvBackupManagentUtility.sh` erases the contents of `/backups` directory. If an external USB device is mounted directly to `/backups` all data of this device is deleted.

  To avoid deletion of all data, following mount instruction should be used, i.e. a `backups` directory on the USB drive is used and data is only deleted inside this directory:

  ```
  mount /dev/sdX /mnt
  mkdir /mnt/backups
  mount --bind /mnt/backups /backups
  ```

  `/dev/sdX` is a place holder for the USB device name.

Step by Step

1) On the **Maintenance** navigation tab click on the **Recovery** navigation menu item.
2) In the navigation tree, click on **Backup& Restore** > **Backup**.

   The backup wizard dialog opens.
3) Select the archive to which the backup set is to be added.

   NOTICE:

   Backing up the file systems of the OpenScape UC Application computer systems for a Duplex deployment scenario, you must select the DEFAULT archive.

   - Use the **…** button to select an existing archive.
   - Click on the **Add** button to create a new archive.

4) Click on **Next**.
5) Choose the **FIle system** from the **backup type** to be backed up
6) Select the **Application** from the **backup units** to be backed up.

The table below illustrates the optimum partition configuration to support File System backup and OpenScape UC script "syncUC" when an external USB is mounted to the system:

Partition	Partition Type	Calculation formula	size in GB [17]
On the computer			
Hard disk for syncUC	Hard Disk	N [18]	160
/boot	Primary	2	2
Swap	Primary	2	2
LVM2 memory	Primary	N-4	156
Logical volume group	Logical volume group		
Root partition (/) in the LVM2 memory for active operation of the OpenScape UC Application	Logical	0.95*(N-4)/2	74,1
Partition for fallback by means of syncUC	Logical	0.95*(N-4)/2	74,1
Temporary snapshot [19]	Logical	0.1*(N-4)/2	7,8
On the USB hard disk			
Hard disk for file System backup	Hard disk	0.9*0.95*(N-4)/2	66,7

IMPORTANT:

The difference of GibiByte (1024^3 as used in SLES) and GB (1000^3 as used by some disc vendors) may lead to

[17] For the minimum size of 160 GB

[18] Hard disk size is defined as N

[19] This logical volume is created automatically when the file system is backed up. It need not be created manually.

different figures when performing partitioning in SLES 11 (1GiB≈1.074GB), However the calculation formula is valid.

IMPORTANT:

If the system is LVM based, there is a remote possibility that during the backup the snapshot of the root partition failed to be removed. In that case a critical alarm is raised to indicate this fact to the administrator. This alarm is critical because a rootsnapshot that is not removed, is a hanging resource that may lead to performance degradation, instability, and may eventually lead to host system reboot.

If the above occurs you must try and remove the rootsnapshot manually. You should make sure that no directory is mounted, and then execute the following: `lvremove -f <rootsnapshot_name>`

7) Click on **Start backup**.

The backup starts according to the settings made. The backup progress is then graphically displayed.

4.7.6 How to Back up manually the File System for Standard Duplex on a Non-LVM based deployment.

Apart from the automatic backup using backup schedules, you can also back up manually the file systems of CMP/UC Application computer systems for Standard Duplex. Via the file system backup of a CMP/UC Application computer system, you can completely restore the relevant computer system after a critical system crash

Prerequisites

File system type must be on `ext2` or `ext3` type

The `dump rpm` package is required. (If not installed then install it manually)

The `sudoers` file (under the directory:`/etc/`) must contain the following lines at the end and it applies for all system nodes:

1) `sym ALL=NOPASSWD:/opt/siemens/servicetools/backup/dbRestore.sh`
2) `sym ALL=NOPASSWD:/opt/siemens/servicetools/backup/fsBackup.sh`
3) `sym ALL=NOPASSWD:/opt/siemens/servicetools/backup/lvBackupManagementUtility.sh`
4) `sym ALL=NOPASSWD:/opt/siemens/servicetools/backup/dbBackup.sh`

The Hard disk usage must be <50% of the entire disk

If 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

If Application server System backup is taking place for a Large deployment then backed up data are stored in hard disk at each node and must be manually transferred to external media.

If you perform Application server System backup for non-LVM system with **HD** archive then the final backup file will be placed under the created backup set while the backup file will have the following pattern `NODENAME_Bkup__date_.tar`

Step by Step

1) On the **Maintenance** navigation tab click on the **Recovery** navigation menu item.
2) In the navigation tree, click on **Backup& Restore** > **Backup**.

   The backup wizard dialog opens.
3) **Select archive** to which the backup set is to be added.
   - Use the **…** button to select an existing archive.
   - Click on the **Add** button to create a new archive.
4) Click on **Next**.
5) Select **System** on the **backup type** field.
6) Click on **Application Server**
7) Select the **File System backup** and click on **Save**
8) Click on **Start**.

   The backup of the file system starts

IMPORTANT:

For large deployment systems all system nodes (Backend, Frontend and Media Server) must all follow the same file system structure. This means that all nodes must either be LVM based or non LVM based

---

4.7.7 How to Back up manually the File System for Standard Duplex on a LVM based deployment.

Apart from the automatic backup using backup schedules, you can also back up manualy the file systems of CMP/UC Application computer systems for Standard Duplex. via the file system backup of a CMP/UC Application computer system, you can completely restore the relevant computer system after a critical system crash.

Prerequisites

The `sudoers` file (under the directory:`/etc/`) must contain the following lines at the end and it applies for all system nodes:

1) `sym ALL=NOPASSWD:/opt/siemens/servicetools/backup/dbRestore.sh`
2) `sym ALL=NOPASSWD:/opt/siemens/servicetools/backup/fsBackup.sh`
3) `sym ALL=NOPASSWD:/opt/siemens/servicetools/backup/lvBackupManagementUtility.sh`

4) `sym ALL=NOPASSWD:/opt/siemens/servicetools/backup/dbBackup.sh`

The Hard disk usage must be <50% of the entire disk

If 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

If Application server System backup is taking place for a Large deployment then backed up data are stored in hard disk at each node and must be manually transferred to external media.

If we perform Application server System backup for LVM system with HD archive then the final backup file will be placed under /backups while the backup file will have the following pattern `NODENAME_lvm_file_system_backup.tar`

Step by Step

1) On the **Maintenance** navigation tab click on the **Recovery** navigation menu item.
2) In the navigation tree, click on **Backup& Restore** > **Backup**.

   The backup wizard dialog opens.
3) **Select archive** to which the backup set is to be added.
   - Use the **…** button to select an existing archive.
   - Click on the **Add** button to create a new archive.
4) Click on **Next**.
5) Select **System** on the **backup type** field.
6) Click on **Application Server**
7) Select the **File System Backup** and click on **Save**
8) Click on **Start**.

   The backup of the file system starts

IMPORTANT:

For large deployment systems all system nodes (Backend, Frontend and Media Server) must all follow the same file system structure. This means that all nodes must either be LVM based or non LVM based

---

IMPORTANT:

If the system is LVM based, there is a remote possibility that during the backup the snapshot of the root partition failed to be removed. In that case a critical alarm is raised to indicate this fact to the administrator. This alarm is critical because a rootsnapshot that is not removed, is a hanging resource that may lead to performance degradation, instability, and may eventually lead to host system reboot.

If the above occurs you must try and remove the rootsnapshot manually. You must make sure that no directory

is mounted, and then execute the following: `lvremove -f <rootsnapshot_name>`

4.7.8 How to Back up manually the Backend File System for on a LVM based deployment with Storage Area Network (SAN) Partitions.

For LVM Based deployments with Storage Area Network (SAN) partitions you can backup manually the file systems of CMP/UC Application computer systems and you can completely restore the relevant computer system after a critical system crash.

Prerequisites

Create a file named `SANList.info` under $SYMPHONIA_HOME/servicetools/backup[20]

The template of file `SANList.info` must have the following structure:

```
opt_siemens/opt/siemens
var_siemens/var/siemens
ucSYMDB/ucSYMDB
ucSYMDBlogs/ucSYMDBlogs
```

`/opt/siemens` is the SAN partition (after the alteration in `/etc/fstab`) and `opt_siemens` is an alias. This alias will be the name of the `tar` file that will be created for this partition

The `sudoers` file (under the directory:`/etc/`) must contain the following lines at the end and it applies for all system nodes:

1) `sym ALL=NOPASSWD:/opt/siemens/servicetools/backup/dbRestore.sh`
2) `sym ALL=NOPASSWD:/opt/siemens/servicetools/backup/fsBackup.sh`
3) `sym ALL=NOPASSWD:/opt/siemens/servicetools/backup/lvBackupManagementUtility.sh`
4) `sym ALL=NOPASSWD:/opt/siemens/servicetools/backup/dbBackup.sh`

The Hard disk usage must be <50% of the entire disk

If 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

Step by Step

1) On the **Maintenance** navigation tab click on the **Recovery** navigation menu item.
2) In the navigation tree, click on **Backup& Restore** > **Backup**.

   The backup wizard dialog opens.

[20] `SYMPHONIA_HOME` can be `/opt/siemens` or `/enterprise`

3) **Select archive** to which the backup set is to be added.
   - Use the **…** button to select an existing archive.
   - Click on the **Add** button to create a new archive.
4) Click on **Next**.
5) Select **System** on the **backup type** field.
6) Click on **Application Server**
7) Select the **File System Backup** and click on **Save**
8) Click on **Start**.

   The backup of the file system starts

IMPORTANT:

For large deployment systems all system nodes (Backend, Frontend and Media Server) must all follow the same file system structure. This means that all nodes must be LVM based.

IMPORTANT:

If the system is LVM based, there is a remote possibility that during the backup the snapshot of the root partition failed to be removed. In that case a critical alarm is raised to indicate this fact to the administrator. This alarm is critical because a rootsnapshot that is not removed, is a hanging resource that may lead to performance degradation, instability, and may eventually lead to host system reboot.

If the above occurs you must try and remove the rootsnapshot manually. You should make sure that no directory is mounted, and then execute the following: `lvremove -f <rootsnapshot_name>`

When backup finishes you must have several `.tar` files that include the

- lvm root partition

- SAN partitions

like the following:

Example

“"hostname"”`_lvm_file_system_backup.tar`

“"hostname"”`_opt_siemens.tar`

“"hostname"”`_var_siemens.tar`

“"hostname"”`_ucSYMDB.tar`

“"hostname"”`_ucSYMDBlogs.tar`

For example:

“imola”`_lvm_file_system_backup.tar`

“imola”_opt_siemens.tar

“imola”_var_siemens.tar

“imola”_ucSYMDB.tar

“imola”_ucSYMDBlogs.tar

In this example the host is called imola and:
imola_lvm_file_system_backup.tar is the lvm root partition and the other files are the SAN partitions

/opt/siemens,

/var/siemens,

/ucSYMDB

/ucSYMDBlogs

NOTICE:

These files must be saved in an external USB drive with ext3 format.

4.7.9 How to Restore OpenScape Configuration Data

By using a backup set, you can completely restore the configuration data of the OpenScape system. How to restore the configuration data of the OpenScape system:

Prerequisites

You have previously saved the information to be restored in an archive.

The archive's data are not damaged.

NOTICE:

When restoring data of installed components with data of different versions of the installed components, the restoration will not be performed. A corresponding error code is displayed. In this case, contact the next level of technical support

When you have also installed the OS Composer, you must administer backups either by the Composer or CMP only, to avoid conflicts.

Step by Step

1) Check whether the following conditions apply:

- You wish to restore the configuration data for Standard Duplex (large).
- You have just restored the application computer by a new installation with the original response file.
- You have expanded the original Standard Duplex installation 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) Start Common Management Platform.

3) On the **Maintenance** navigation tab, click on the **Recovery** navigation menu item.

4) In the navigation tree, click on **Backup & Restore** > **Restore**.

The restore wizard dialog opens.

5) 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.

6) Click on **Next**.

7) Select the backup set for restoring the configuration data.

8) Click on **Next**.

The backup units of the selected backup set are displayed.

9) Select the backup units you wish to restore.

If you are going to restore the Application Server then a software compatibility level check is applied and in case the target system software level does not match exactly (DVD + hotfix) the backup set, restore is aborted and a message is presented.

For other units no software compatibility check is performed and they are not affected by a possible restore failure of the Application Server.

IMPORTANT:

For integrated systems where Application Server is part of the OpenScape Voice unit the Configuration Data restore session will be aborted if the software compatibility check applied to the Application Server fails.

10) Click on **Start restore**.

The restore starts according to the settings made.

4.7.10 How to Restore the OpenScape System for Integrated Simplex

You can restore the OpenScape system for Integrated Simplex 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:

Prerequisites

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.

NOTICE:

When restoring data of installed components with data of different versions of the installed components, the restoration will not be performed. A corresponding error code is displayed. In this case, contact the next level of technical support

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 Simplex after a system crash:

NOTICE:

In an Integrated Deployment a File system restore is not supported by CMP.

Step by Step

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 Section “How to Restore the Response File from a Backup Set”

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.

When the following message in the system startup log is displayed, all OpenScape UC Application services have been started.

```
******* 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 any error message.

6) On the reinstalled OpenScape computer system, access the Common Management Platform and log on with the following ID: **administrator@system**.

7) On the **Maintenance** navigation tab click on the **Recovery** navigation menu item.

8) In the navigation tree, click on **Backup & Restore** > **Restore**

   The restore wizard dialog opens.

9) 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.

10) Click on **Next**.

11) Select the backup set for restoring the configuration data.

12) Click on **Next**.

    The backup units of the selected backup set are displayed

13) Select the backup units you wish to restore

14) Click on **Start restore**.

    The restore starts according to the settings made. The restore progress is then graphically displayed.

15) Reboot OpenScape UC Application with the following commands:

    `/etc/init.d/symphoniad stop`

    `/etc/init.d/symphoniad start`

16) 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-Install*
    [21] `>/servicetools/security/resetUserAccount.sh administrator@system` <*new password* >

    You have now restored the OpenScape computer system for Integrated Simplex after a critical system crash.

4.7.11 How to Restore CMP Application for Standard Duplex

Note that 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

21 <*Osc-Install* > is the setup directory of the OpenScape system:

`/opt/siemens/` respectively `/enterprise/`

every CMP computer system of Standard Duplex after a critical system crash by restoring the file system of the relevant computer system. This requires the following:

Prerequisites

The hardware of the CMP Application computer system to be restored has not been damaged.

You backed up the file system of the relevant CMP 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.

NOTICE:

When restoring data of installed components with data of different versions of the installed components, the restoration will not be performed. A corresponding error code is displayed. In this case, contact the next level of technical support

---

After the restoration of the file system, the relevant CMP 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 CMP computer system for Standard Duplex after a system crash:

Step by Step

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 CMP Application computer system:

a) Execute the following command to unzip the 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 restore script to the current directory:

`cp` *<Osc-Install*[22] *>*`/servicetools/backup/Restore.sh .`

c) Execute the following command to start the 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) Wait until the restore script used announces the end of the restoration.

7) Before starting OpenScape CMP Application, delete the contents of these two log files.

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

These files include the system start log information.

8) Execute the following command on the computer system on which you have installed OpenScape CMP Application.
`/etc/init.d/symphoniad start`

OpenScape CMP Application starts. While the system starts, the system start log should not log any errors.

When the following message in the system startup log is displayed, all OpenScape CMP Application services have been started.
`******* Starting all instances done. *******`

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

9) Execute the following command to put out the system startup log.
`tailf /var/siemens/common/log/osgi.log.`

10) Open the following error log file after the OpenScape CMP Application startup has finished.
`/var/siemens/common/log/osgi.err`

The error log file should not contain any error message.

11) 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

22 *<Osc-Install >* is the setup directory of the OpenScape system:

`/opt/siemens/` respectively `/enterprise/`

the **administrator@system** administrator account, execute the following command.

<*Osc-Install*[23]>`/servicetools/security/resetUserAccount.sh administrator@system` <*new password* >

You have now restored the OpenScape CMP Application computer system of Standard Duplex after a critical system crash.

4.7.12 How Restore the Backend File System with Storage Area Network (SAN) Partitions.

Note that 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 CMP computer system after a critical system crash by restoring the file system of the relevant computer system.This requires the following:

Prerequisites

The hardware of the CMP Application computer system to be restored has not been damaged.

You backed up the file system of the relevant CMP 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 CMP Application computer system make sure you have copied the restore script `lvRestoreUtility.sh` to the same location on the external computer system like the backed up data of the CMP Application computer system.

In case you wish to restore an LVM file system backup to a **new** hard disk, it is necessary, before executing `lvRestoreUtility.sh`, to create manually the partitions on the new disk, **exactly** as they were on the system, the backup was taken on. Especially the logical volumes on the new disk should have the same name and size.

After the restoration of the file system, the relevant CMP Application computer system is fully functional again and works with the configuration data existing when the file system backup was performed.

---

23 <*Osc-Install* > is the setup directory of the OpenScape system:

`/opt/siemens/` respectively `/enterprise/`

How to restore a CMP computer system for Standard Duplex after a system crash:

Step by Step

1) Unmount SAN partitions and remove SAN mount-points from `fstab`

2) Unplug all external disks

3) Insert the installation data carrier of the Linux operating system into the disk drive of the computer system you want to restore.

4) Reboot the computer system.

The computer system boots in the rescue mode.

5) If you have to reinstal SUSE Linux on the server you must also create a new vg_backup file as described in the following steps otherwise proceed with step 6:

a) Create `vg_backup` with the new UUIDs. On newly installed system run the vgcfgbackup command:

```
vgcfgbackup -f tmp/vg_backup
```

b) Backup the "old" `vg_backup` file on the external storage

c) Copy the "new" `vg_backup` file to the external storage (replace old one)

The correct UUIDs are in your file system backup.

d) Run the script `lvRestoreUtility.sh`

e) Reboot the server

System will come up in maintenance mode because of mismatched unique disk ids

---

IMPORTANT:

On some servers, you may have to remove or comment out the `/etc/fstab` entry for `/dev/system/backups` because the server may not boot.

---

f) Backup and edit `/etc/fstab`

Change from disk-by-id to volume label - from:

```
/dev/disk/by-id/
scsi-3600508e0000000007af639e93c9c7407-part2/boot

/dev/disk/by-id/
scsi-3600508e0000000007af639e93c9c7407-part1/swap
```

Change from disk/by-id to volume label - to:

```
/dev/sda2/boot

/dev/sda1/swap
```

6) Mount the data carrier on which the backup file of the file system is stored.

7) Extract all other `tar` files (not these under `backups)` in the plugged-in drive contain the SAN partitions content.

NOTICE:

Make sure the SAN partitions are in the `/` directory and not the `/root` directory. You can confirm the directory you need to be in by doing executing the following command: `tar tvf <fileName>.`

---

8) On the data carrier access the directory in which the backup file of the file system is stored.

9) Execute the following command to start the LVM-based restore script:
`sh lvRestoreUtility.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.

10) Wait until the restore script used announces the end of the restoration.

11) Before starting OpenScape CMP Application, delete the contents of these two log files.

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

These files include the system start log information.

12) Execute the following command on the computer system on which you have installed OpenScape CMP Application.
`/etc/init.d/symphoniad start`

OpenScape CMP Application starts. While the system starts, the system start log should not log any errors.

When the following message in the system startup log is displayed, all OpenScape CMP Application services have been started.
`******* Starting all instances done. *******`

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

13) Execute the following command to put out the system startup log.
`tailf /var/siemens/common/log/osgi.log.`

14) Open the following error log file after the OpenScape CMP Application startup has finished.
`/var/siemens/common/log/osgi.err`

The error log file should not contain any error message.

15) 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-Install*[24]>`/servicetools/security/resetUserAccount.sh administrator@system` <*new password* >

You have now restored the OpenScape CMP Application computer system of after a critical system crash.

4.7.13 How to Restore 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.

1) For an unencrypted backup set in:

`Package_Install_installbase_001.zip`

2) For an encrypted backup set in:

`Package_Install_installbase_001.z`

NOTICE:

An independent zip file exists for every Standard Duplex (large) computer system. In the following section of the response file you can see for which computer system an 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:

Step by Step

1) Place the OpenScape product data carrier in the drive of the computer system on which you want to reinstall OpenScape UC Application.

24 <*Osc-Install* > is the setup directory of the OpenScape system:

`/opt/siemens/` respectively `/enterprise/`

2) If the backup set with the enclosed response file was created encrypted, execute the following steps.witch to the CMP.

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 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

4.7.14 Backup Concept for the OpenScape Web Client

The OpenScape Web Client backup concept comprises the following system data of the OpenScape Web Client.

System configuration of the OpenScape Web Client

Journals of all users

Private address books of all users

Private settings of all users

Routing rules of all users

Shared address books

You can customize the backup location, the time and number of system backups. The system is backed up automatically once a day.#

4.7.14.1 Settings for the System Backup of the OpenScape Web Client

The following two configuration files define the settings for the system backup of the OpenScape Web Client:

1) `backup.cfg`

You find this file in the following directory of the computer system on which the OpenScape Web Client is installed:

<*Osc-Install*
[25] `>/config/services/default/BackupService/`

a) CA_BACKUPSERVICE_DB_BIN_DIR

Defines the path to the binary files of the database. If no value has been configured, the system determines this setting automatically.

b) CA_BACKUPSERVICE_BACKUP_HOME

Defines how many system backups are archived. 14 system backups are archived by default.

NOTICE:

Please remember that the more you archive system backups the more memory is occupied. Since the amount of memory used for a system backup strongly depends on the system environment, we cannot detail individual memory use for a system backup here.

---

[25] <*Osc-Install* > is the setup directory of the OpenScape system:

`/opt/siemens/` respectively `/enterprise/`

2) `proc.cfg`

You find this file in the following directory of the computer system on which the OpenScape Web Client is installed:

<*Osc-Install*
[26] `>/config/common/`

In this configuration file you can configure the following setting for the system backup:

NOTICE:

a) BACKUP_TIME

Defines the time at which the daily system data backup occurs. The value for this setting must be specified in the following format:

“<HH>:<MM>:<SS>”

NOTICE:

Back up the system data at times of low system load – e. g. at night.

Using the following command you need to reboot the web server component for changed system backup settings to take effect:

In this configuration file you can configure the following settings for the system backup:

`/etc/init.d/symphoniad restart WebClient`

NOTICE:

The service of the web server component is called **WebClient**

4.7.14.2 How to Restore OpenScape Web Client via System Backup

How to restore the system data of the OpenScape Web Client from a system backup:

1) Stop the web server component of OpenScape UC Application. How to proceed is described in Section “How to Start/Stop Components”.

INFO:

The service of the web server component is called **WebClient**.

---

2) Open a shell on the computer system that hosts OpenScape Web Client.

---

[26] <*Osc-Install* > is the setup directory of the OpenScape system:

`/opt/siemens/` respectively `/enterprise/`

3) Switch to the following directory:

   <*Osc-Install*>[27]/bin/BackupService/
4) Execute the following command in the shell:

   `./restore.sh` "<*backup directory*>"

   Specify for <*backup directory*> the complete directory path under which the system backup to be restored is filed.

   Example:

   `restore.sh "c:/Program Files/siemens/HiPathCA/backups/"`
5) Start the web server component of OpenScape UC Application. How to proceed is described in Section "How to Start/Stop Components"..

4.8 Download Center

You can use the download center to download different resources from a central place.

Among these resources are:

- Software
- Documentation

Software and Documentation

Software and documentation to be provided in the download center for downloading must be stored in the following folders on the OpenScape computer system.

- Software:

  <Osc#Install [28]>`/share/tomcat/webapps/management/downloads/software`
- Documentation:

  <Osc#Install >`/share/tomcat/webapps/management/downloads/documentation`

> **IMPORTANT:**
>
> If the download center is not pre-configured (which is usually the case for a fresh installation) you will have to create the folders for the paths above: `downloads/software` and `downloads/documentation`.

To improve the file management, create in each of these folders a new subfolder – e. g. `CMP_Software`.

[27] <*Osc-Install* > is the setup directory of the OpenScape system:

`/opt/siemens/` respectively `/enterprise/`

[28] <Osc-Install> is the setup directory of the OpenScape system:`/opt/siemens/` or `/enterprise/`

Besides the actual download files both folders must contain a contents file that summarizes all available files with their document information. This contents file must be called `filelist.xml` and have the following general XML structure depending on the resource type:

Table 1: Structure of the contents file for software

```
<filelist>
   <file>
      <filename>pdf-reader.exe</filename>
      <title>PDF Reader 9.2</title>
      <description>PDF Reader for Windows XP</description>
      <version>9.2.1245</version>
   </file>
   …
</filelist>
```

Table 2: Structure of the contents file for documentation

```
<filelist>
   <file>
      <filename>OpenScape_GER.doc</filename>
      <title>OpenScape-Dokumentation</title>
      <language>Deutsch</language>
      <orderNo>10-200-4587-100</orderNo>
   </file>
   <file>
      <filename>OpenScape_ENG.doc</filename>
      <title>OpenScape Documentation</title>
      <language>English</language>
      <orderNo>10-200-4587-200</orderNo>
   </file>
   …
</filelist>
```

4.8.1 How to Provide Software in the Download Center

Before software can be downloaded from the download center, you need to provide it there.

Prerequisites

Adequate administrative permissions

Step by Step

1) Switch to the following folder of the Common Management Platform computer system:

   <Osc#Install[29]`/share/tomcat/webapps/management/downloads/software/…`

2) In this folder look for the `filelist.xml` content file.
   - If the content file is available, open it.
   - If the content file is not available, create a new text file named `filelist.xml` in the described folder and open it.

3) Specify in the content file each software you want to provide in the download center. In doing so use the described XML format for software.

4) Store the modified content file in the following folder:

   <Osc#Install >`/share/tomcat/webapps/management/downloads/software/…`

5) Copy the software files to the following folder:

   <Osc#Install >`/share/tomcat/webapps/management/downloads/software/…`

   The software files must be named exactly as you have described them in the content file under <filename>.

The new software can from now on be downloaded from the download center.

4.8.2 How to Provide Documentation in the Download Center

Before documentation can be downloaded from the download center, you need to provide it there.

Prerequisites

Adequate administrative permissions

Step by Step

1) Switch to the following folder of the Common Management Platform computer system:

   <Osc#Install[30]`/share/tomcat/webapps/management/downloads/documentation/…`

2) In this folder look for the `filelist.xml` content file.
   - If the content file is available, open it.
   - If the content file is not available, create a new text file named `filelist.xml` in the described folder and open it.

29 <Osc-Install > is the setup directory of the OpenScape system: /opt/siemens/ or /enterprise/

30 <Osc-Install > is the setup directory of the OpenScape system: /opt/siemens/ or /enterprise/

3) Specify in the content file each documentation you want to provide in the download center. In doing so use the described XML format for documentation.
4) Store the modified content file in the following folder:
   <Osc#Install >`/share/tomcat/webapps/management/downloads/documentation/…`
5) Copy the documentation files to the following folder:
   <Osc#Install >`/share/tomcat/webapps/management/downloads/documentation/…`
   The documentation files must be named exactly as you have described them in the content file under <filename>.

The new documentation can from now on be downloaded from the download center.

4.8.3 How to Download Software

How to download software from CMP:

Prerequisites

Software was made available in the download center for downloading.

Step by Step

1) On the **Configuration** navigation tab click on the **CMP** navigation menu item.
2) In the navigation tree, click on **Downloads** > **Software**.
   A list of the software that you can download from the download center appears in the work area.
3) Click the title of the software that you want to download.

The software download starts.

4.8.4 How to Download Documentation

How to download documentation in CMP:

Prerequisites

Documentation was made available in the download center.

Step by Step

1) On the **Configuration** navigation tab click on the **CMP** navigation menu item.
2) In the navigation tree, click on **Downloads** > **Documentation**.
   A list of the documentation that you can download from the download center appears in the work area.

3) Click the title of the documentation that you want to download.

The documentation download starts.

4.9 Software Repository

You can store and manage upgrade file packages in the Common Management Platform Software Repository. These packages belong to the various applications of an OpenScape system.

An upgrade file package comprises at least one upgrade file and one reference file. The reference file has the file extension `*.spa` and references all upgrade files contained in the upgrade file package.

How to upgrade an OpenScape application via the Software Repository of the Common Management Platform is described in the relevant manuals of the respective application.

4.9.1 How to Display available Upgrade File Packages of the Repository

How to display avaialble upgrade file packages of the repository:

Prerequisites

Adequate administrative permissions

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** > **Repository**.
A list of all upgrade file packages stored in the Software Repository is displayed in the work area.This list contains for each entry the following information:

1) Product Name

Product the upgrade file belongs to

2) Version

Product version to which the upgrade file package upgrades the product

3) Size

File size of the upgrade file package

4.9.2 How to Upload an Upgrade File Package to the Repository

How to upload an upgradfe file package to the repository:

Prerequisites

Before you can upgrade an application, you need to upload the files of the required upgrade file package to the Software Repository.

NOTICE:

If you wish to upload the files of several upgrade file packages to the Software Repository, you need to execute the described steps for each single upgrade file package.

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** > **Repository**.

   A list of all upgrade file packages stored in the Software Repository is displayed in the work area.
3) Click on **Add**.

   A dialog for uploading files opens.
4) Specify one of the following information items for the upgrade file package to be uploaded.
   - A ZIP file that contains the upgrade files as well as the reference file of the relevant upgrade file package.
   - The upgrade files and the reference file (`*.spa`) of the relevant upgrade file package.

     IMPORTANT:

     Before you instal the OSS you must first load the `(*.spa)` file into the Repository and afterwards the `(*.tar)` file.

     ---
5) When the files are completely uploaded, click on **Save**.

   If an uploaded file is invalid, an error message informs you accordingly. The upgrade file package concerned will not be stored in the Software Repository in this case.

   If an uploaded upgrade file package assumes further upgrade files, you are prompted to upload these upgrade files to the Software Repository also.

The files of the upgrade file package are stored in the Software Repository. The upgrade file package is displayed in the list of stored upgrade file packages.

4.9.3 How to Delete an Upgrade File Package from the Repository

How to delete an upgrade file package from the Repository:

Prerequisites

Adequate administrative permissions

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** > **Repository**.

   A list of all upgrade file packages stored in the Software Repository is displayed in the work area.
3) Select the checkboxes of the upgrade file packages that you want to delete.
4) Click on **Delete**.
5) Click on **OK** to confirm the deletion of the selected upgrade file packages.

The selected upgrade file packages are deleted from the Software Repository and from the list of all upgrade file packages.

4.9.4 How to Increase the Software Repository Size

Follow the instructions below to increase the software repository size.

Prerequisites

Adequate administrative permissions.

Step by Step

1) On the **Maintenance** navigation tab, click on the **Inventory** navigation menu item.
2) In the navigation tree, click on **Nodes**.

   The list of nodes is displayed.
3) Click on the name of the backend node for which you want to increase the software repository size.
   A **Dashboard** window pops up.
4) Click **Show** next to **Show services status** under the **Actions** area.

   A **List of Components** window pops up.
5) Scroll down (or use the search function) to find **Swsupplyfacade Service** and click on it.

   A **Edit Service Configuration** window pops up.
6) Edit the **swsupply.repository.size** field to increase the software repository size. Deafult is 8000000 in KB (8 GB).
7) Click **Save**.
8) Restart symphonia in backend node:

   ```
   /etc/init.d/symphoniad restart
   ```

4.10 Concept of the Consistency Check

The consistency check checks important configuration parameters of OpenScape UC Application and the functionality of its components resulting from this. For example, you can determine whether the configuration of OpenScape UC Application is consistent or faulty configurations hamper the system performance.

The consistency check is based on individual check scripts that determine which components and configurations are checked.

In the Common Management Platform, you can choose from the following default check scripts to perform a consistency check:

- Check script OpenScape UC
- Check script User Configuration

Each of these check scripts controls the performance of individual checks.

Check script OpenScape UC

Checks the following for OpenScape UC Application:

- Related to OpenScape Voice
  - Whether all office codes are fully configured.
  - Whether the CSTA connection is configured.
  - Whether the CSTA interface of OpenScape Voice can be reached.
- Related to the OpenScape Media Server
  - Whether OpenScape Voice is configured as SIP server and can be reached.
  - Whether a TTS system is configured and can be reached.
- Related to the voice portal
  - If OpenScape Xpressions is configured for OpenScape users: Whether the settings for Trusted Transfer Mode (TTM) are configured.
- Related to licenses
  - Whether a valid license is installed for OpenScape UC Application.
  - Whether a valid license is installed for the TTS system.
- Related to the groupware connection
  - Whether the connected groupware system can be reached.
  - Whether the configured account data allows access to the groupware system.
  - Whether e-mails can be sent via the configured SMTP system.

Check script User Configuration

Checks the following for each configured OpenScape user:

- Whether the user account of the user is locked.
- Whether a subscriber has been selected as one-number device for the user.
- Whether the selected one-number device is available as subscriber in the OpenScape Voice System.
- Whether the **ONS in / out** option is activated in the OpenScape Voice system for the selected one-number device.
- Whether CSTA is activated in the OpenScape Voice system for the selected one-number device.

- Whether the OpenScape database contains a contact entry associated to the user.
- Whether the user's contact data contain a phone number.
- Whether a user profile has been assigned to the user.
- Whether a voicemail number has been configured for the user.
- Whether an external ID for the groupware connection has been assigned to the user.
- Whether the groupware system of the configured external ID is configured.

Check script Duplicate ONS

Checks the following for each configured OpenScape UC user:

- Whether in the user account of the user are erroneously assigned two or more ONS devices.

In such a case each of the detected users should be checked and the wrongly ONS devices should be unset.

4.10.1 How to perform the Consistency Check

How to perform the Consistency Check:

Prerequisites

Adequate administrative permissions.

Step by Step

1) On the **Maintenance** navigation tab click on the **Monitoring** navigation menu item.
2) In the navigation tree, click on **Tools & Utilities** > **Consistency Checker**.

   The consistency checker dialog opens.
3) Select the checkboxes of the check scripts you want to execute.
4) Click on **Run Checks**.

   The consistency check starts. Its progress and the check results are displayed in a dialog.
5) If you want to download the check results as check report, click on **Download report**.

NOTICE:

To view a downloaded report, use a text editor that supports UNIX-formatted end-of-line markings

---

4.10.2 How to download the Last Check Report

How to download the Last Check Report:

Prerequisites

Adequate administrative permissions.

Step by Step

1) On the **Maintenance** navigation tab click on the **Monitoring** navigation menu item.
2) In the navigation tree, click on **Tools & Utilities** > **Consistency Checker**.

   The consistency checker dialog opens.
3) Select the checkboxes of the check scripts you want to execute.
4) Click on **Download last report**.

NOTICE:

To view a downloaded report, use a text editor that supports UNIX-formatted end-of-line markings

---

4.11 Further Administrative Tasks

This chapter contains information about additional tasks an Administrator might find useful.

4.11.1 Starting/restarting OpenScape UC Application

When you restart an OpenScape UC Application computer system, all OpenScape services provided by the relevant computer system are interrupted.When starting or restarting the computer systems of OpenScape UC Application please read the following:

1) You can stop and start a single application computer, front-end computer or Media Server computer at will as long as all other computer systems of OpenScape UC Application remain started.
2) If you wish to restart several computer systems, you can stop them in any sequence or simultaneously.
3) If you wish to restart 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 computer systems to access the OpenScape UC Application database when they are started at a later date. After you have started the application computer, wait for a minute before you start the other computer systems in any sequence or simultaneously.
4) If you wish to start several computer systems and the application computer is not among them, you can start them in any sequence or simultaneously.

4.11.2 Saving the Security Certificate for the CMP

When you invoke the Common Management Platform, the web browser usually displays a security alarm that returns with every login.

How to start the file system backup manually:

The reason is that the security certificate of the Common Management Platform is issued by an institution that the web browser does not trust.

You can avoid this security alarm after its first appearance by installing the security certificate of the Common Management Platform as trusted security certificate in the web browser used. How to proceed depends on the web browser used and on its settings.

This section exemplifies how to install the security certificate of the Common Management Platform in the Internet Explorer 8 as trusted.

NOTICE:

Depending on the settings of your Internet Explorer the actual proceedings may deviate from the descriptions.

Start the configuration

How to install the security certificate of the Common Management Platform as trusted:

Step by Step

1) Invoke the CMPin the Internet Explorer.

The dialog with the security alarm opens.

2) Select **View Certificate**.

The dialog with the security certificate information opens.

3) Switch to the **Certification Path** tab.

4) Select the certificate that is marked as not trusted

The restore wizard dialog opens.

5) Select **View Certificate**.

The dialog with the information of the individual security certificate opens.

6) Select **Install Certificate**….

The wizard for installing a certificate opens.

7) Select **Next**.

The dialog for selecting the certificate store opens.

8) Select **Place all Certificates in the following store**.

9) Select in the **Certificate-Store** field the **Trusted Root Certificate Authorities** store.

10) Select **Next**.

In a dialog you can see all the import settings you have selected in the previous dialogs of the wizard.

11) Select **Finish**.

A dialog with a security warning opens.

12) Confirm the security warning with **Yes**.

A dialog with an import confirmation opens.

13) Select **OK**.

14) Select **OK** in the dialog with the information of the individual security certificate.

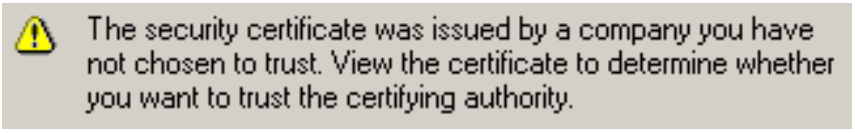
15) Select **OK** in the dialog with the information of the security certificate.

The Internet Explorer trusts the security certificate of the Common Management Platform from now on.

Security alarm for the certificate name

You may also encounter a security alarm that concerns the name of the security certificate.

Example Internet Explorer 6:



The reason is that the security certificate of the Common Management Platform has been issued for a host name different from the one you use for the CMPURL.

You can avoid this security alarm as follows:

1) Invoke the Common Management Platform with the following URL:

`https://adsaext11.site/`

The host name adsaext11.site must then be resolved by the network DNS. If this is not possible, also execute the following step **2**.

2) Change the hosts file on the computers from which you invoke the Common Management Platform .

Supplement the `hosts` file by the following line:

<IP address of the CMPcomputer system > `adsaext11.site`

You find the hosts file in the following directory:

`C:/WINDOWS/system32/drivers/etc`

4.11.3 Synchronizing License Assignments anew

The license database of the OpenScape system may at times contain contradictory information for a profile. The license control of the OpenScape system may then withdraw privileges from users with this profile though these 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:

Step by Step

1) Open the profile for which you have detected inconsistencies in the license database (Section “How to Display/Edit Profiles”,)

2) Change any privilege in the profile.
3) 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
4) Cancel the modification you made in step **2**.

   The restore wizard dialog opens.
5) Save the profile again.

You have now corrected the contradictory information in the license database for the relevant profile.

4.11.4 Changing the IP Address of the Application Computer

You can use the following command under Linux to change the IP address of the application computer after the OpenScape UC Application setup.

```
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:

-C:	Confirm modifications
-P:	Retrieve new values from the user
-F:	Enforce reconfiguration
-t:	Test mode; creates an response file without reconfiguring <command> : `list|change`

Default settings:

input response file:	`/…/servicetools/install/conf/responsefile.txt`
output response file:	`/tmp/responsefile.txt`
HP8K node.cfg file:	`/log/install/changeSFWip.log`

NOTICE:

Command `new ip address|host` can be used only with `-n none`.

Start the configuration

How to change the IP address of the application computer:

Step by Step

1) Switch to the setup directory of OpenScape UC Application on the computer system of the application computer.
2) Stop OpenScape UC Application with the following command:

   ```
   /etc/init.d/symphoniad stop
   ```
3) Change the IP address of the computer system under **YAST** > **Network Devices** > **Network Card**
4) Verify that all relevant DNS servers have been updated accordingly.
5) Restart the application computer with the following command:

   ```
   shutdown -r now
   ```
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 or the host name.

   NOTICE:

   In the following step, specify for <*new IP address or new host name*> the address format used in the response file.

   ---
7) Execute the following command in one line:

   ```
   /servicetools/install/bin/changeSFWip.sh
   -c change-n none
   -a <new IP address or new host name>
   -CF
   ```

   Example of the case that the computer system is in the response file addressed via the IP address:

   ```
   /servicetools/install/bin/changeSFWip.sh
   -c change
   -n none
   -a 172.11.0.30
   -C
   ```

   Example in case of IPv6 address:

   ```
   /servicetools/install/bin/changeSFWip.sh
   -c change
   -n none
   -a [IPv6 address]
   -C
   ```
8) Adjust the firewall settings in OpenScape Voice via startCli.
9) Adjust in OpenScape the settings of the endpoints that belong to the OpenScape Media Server or to the voice and conference portal.
10) Start OpenScape UC Application with the following command:

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

You have now modified the IP address of the application computer.

4.11.5 How to Configure the HTTPS Port for CMP Access

The Common Management Platform uses port 443 for the secured Hypertext Transfer Protocol Secure (HTTPS) by default. You can customize this default setting. Administrators can subsequently only log on to the Common Management Platform via HTTPS.

Step by Step

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#Install [31]>`/common/conf/`
2) Search the property file for the entry with the **CMP_HTTPS_PORT** setting and assign it the desired port number:
   `CMP_HTTPS_PORT = 444`
3) Save the modifications in the property file.
4) Switch to the following directory of the computer system:
   <Osc#Install [32]>`/servicetools/install/bin/`
5) Use the following command to execute the `installlib` script:
   `./installlib.sh reconfiguration.ports`
6) Wait until the script has ended.
7) Reboot 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/`

4.11.6 Activating HTTP Port for Framework

The protocol port **4708** for HTTP is locked in the frameworkof 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.

IMPORTANT:

31 <Osc-Install > is the setup directory of the OpenScape system: /opt/siemens/ or /enterprise/

32 <Osc-Install > is the setup directory of the OpenScape system: /opt/siemens/ or /enterprise/

Activating the HTTP protocol port **4708** in the framework of OpenScape UC Application may lead to a security gap in the OpenScape system.

You can use the CMPto 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 :

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 node connections 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 box with the dashboard of the selected node opens.
4) Clck on **Show** next to **Actions**– **Show services status**

   The dialog opens with a list of all components available for the selected system node.
5) Search the list for the **Connector** component for which the **Uri** setting 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.
6) Tick off the checkbox of the relevant **Connector** component.
7) Click on **Start /Stop**.

You have now manually activated the protocol port **4708** for HTTP in the framework of OpenScape UC Application.

4.11.7 Adjusting the CMP User Interface

You can adjust selected Common Management Platform elements to individual requirements.

Within this scope, you can customize the following Common Management Platform interface elements:

- The Unify logo in the Common Management Platform login dialog

- The Unify logo on the Common Management Platform user interface
- Interface texts based on OpenScape product names
- Various general interface texts

For changing such interface elements there is the `rebrand.sh` script. The configuration settings for this script are stored in the associated configuration file `input`.

During the Common Management Platform installation, the `rebrand.sh` script and its configuration file `input` is stored in the following directory:

<Osc#Install [33]>`/share/tomcat/webapps/management/`

If you operate the OpenScape system as integrated cluster system, you need to adjust the CMP user interface on both nodes.

After a Common Management Platform upgrade or after installing a software patch of the same main version, modifications once performed are maintained. A new installation via setup DVD, however, recreates the original logos, product and interface texts. In this case you need to execute the `rebrand.sh` script once again.

NOTICE:

A new configurator file is created on the folder `rebranding` when the `rebrand.sh` script has completed successfully. This configurator file contains the flag **bluewash** which is marked as **on** when the `rebrand.sh` script is finished. During an upgrade or during installing a software patch of the same main version the system checks the flag **bluewash**. If it is set to **on** the `rebrand.sh` script is automatically executed after the update process in order to maintain the modifications. If the flag **bluewash** is set to **off** the software update reset all modifications to their default.

The `input` configuration file

The `input` configuration file contains the settings for all changeable interface texts. The following tables give an overview of these settings.

NOTICE:

If you change texts in the configuration file `input`, please do not remove blanks from the settings identifiers.

Table 3: Rebrand script parameters for brand and product names

Settings identifier	Assigned interface text
__BRAND_NAME__	Brand name in different pop-up messages
__OS_VOICE__	Product name for the OpenScape Voice component
__OS_BRANCH__	Product name for the component OpenScape Voice Branch

33 <Osc-Install > is the setup directory of the OpenScape system: /opt/siemens/ or /enterprise/

Settings identifier	Assigned interface text
__RG_8700__	Product name for the RG8700 gateway component
__RG_2700__	Product name for the RG2700 gateway component

The following restrictions apply for brand and product names:

- The value of each setting must be one to 20 characters long.
- The value of each setting may contain the following characters of an English or German keyboard:
  - a – z and A – Z
  - 0 – 9
  - Special characters can be provided on the input file, some of them must be protected with single quotes, others with double quotes and other with nothing according to the first two columns of the following table, last column displays characters that are not supported by the input file:

Supported Special Characters:	Used as:	Special Characters NOT supported
!	‘!’	/
@	“@”	/
#	“#”	=
%	“%”	^
&	“&”	$
(	“(“	.
)	“)”	*
_	_	[
-	“-“	]
+	“+”	“
{	“{“	,
}	“}”	`
|	“|”	<
:	“:”	>
;	“;”	
~	“~”	
?	“?”	
‘	“ ‘ ”	

- The value of each setting may contain the following additional characters of a German keyboard:
  - ä, ö, ü, ß, µ, €

NOTICE:

If you wish to use special characters in the `input` configuration file, you need to back up the file in the

UTF-8 format. You can use e.g. the Microsoft Editor (Notepad) for this purpose.

The following areas exist for these brand and product names in the configuration file.

- The definition area, in which the settings to be newly used are defined under the above identifiers.
- The area for the settings of the last modification. The identifiers of the associated settings begin with `OLD`. After you have executed the `rebrand.sh` script, the settings of the definition area are automatically copied into this area.
- The area for default settings. The identifiers of the associated settings begin with `DEFAULT`. Here the settings are defined with which the Common Management Platform was shipped. Never change the settings in this area as they may be needed for restoring the default values for the Common Management Platform.

Table 4: Other rebrand script parameters

Settings identifier	Assigned interface text
FOOTER	Text of the trademark note in the Common Management Platform footer
Framework.alarmDisplayString	Original identifier for the OpenSOA framework in the alarm protocol and for active alarms
Framework.alarmFilterDisplayString	Original identifier for the OpenSOA framework in the alarm protocol filter
INFORMATION_LINK	Is not yet used on the Common Management Platform user interface.
PRIVACY_LINK	Is not yet used on the Common Management Platform user interface.
dc_bcpath	Is not yet used on the Common Management Platform user interface.
alarms.sourceFramework	Original alarm identifier for the OpenSOA framework in the alarm protocol filter
COPYRIGHT	Is not yet used on the Common Management Platform user interface.
editProfile.H8kAst	Application identifier for the associated user profiles
editProfile.RGAssistant	Application identifier for the associated user profiles
editProfile.OpenBranchAssistant	Application identifier for the associated user profiles
ApplicationOverview.OSVOICE	Identifier for the OpenScape Voice connection on the application side
importExportCentralized.ExportOscVoice	Internal identifier for the import / export functionality

The value for the following miscellaneous settings must not exceed 20 characters:

- editProfile.H8kAst
- editProfile.RGAssistant
- editProfile.OpenBranchAssistant

4.11.7.1 How to Adjust the CMP User Interface

The `rebrand.sh` script lets you adjust selected Common Management Platform elements to individual requirements.

Step by Step

1) Back up the following files on the computer system on which the Common Management Platform is installed.

a) <Osc#Install [34]>`/share/tomcat/webapps/management/decorations/img/brandname_logo_bg_login.png`

b) <Osc#Install>`/share/tomcat/webapps/management/decorations/img/banner/brandname.png`

c) <Osc#Install>`/share/tomcat/webapps/management/input`

NOTICE:

If you wish to bring the Common Management Platform user interface back into its original state at a later date, execute the following steps and use the backed up files.

---

2) Create the following directory on the computer system on which the Common Management Platform is installed.

<Osc#Install>`/share/tomcat/webapps/management/rebranding`

3) Proceed with the logo that is to replace the Unify logo in the login dialog as follows:

NOTICE:

The logo must not have a resolution greater than 300x150 pixels. The Common Management Platform will otherwise not display it correctly.

NOTICE:

It is also recommended that the logo is transparent allowing the background carbon color to appear.

---

a) If the logo is not yet available in the PNG format, convert it accordingly and use the file extension `.png`.

b) If the logo file does not yet carry the name `brandname_logo_bg_login.png`, rename it accordingly. Please heed case sensitivity.

c) Store the logo in the `rebranding` directory you have created in step 2.

34 <Osc-Install > is the setup directory of the OpenScape system: /opt/siemens/ or /enterprise/

4) Treat the logo that is to replace the Unify logo in the GUI as follows:

NOTICE:

The logo must not have a resolution greater than 124x45 pixels. The Common Management Platform will otherwise not display it correctly.

NOTICE:

It is also recommended that the logo is transparent allowing the background carbon color to appear.

a) If the logo is not yet available in the PNG format, convert it accordingly and use the file extension `.png`.
b) If the logo file does not yet carry the name `brandname_logo.png`, rename it accordingly. Please heed case sensitivity.
c) Store the logo in the `rebranding` directory you have created in step 2.

5) Start a text editor and open the following file therein:

<Osc#Install>`/share/tomcat/webapps/management/input`

6) Specify the values desired for the different settings of the configuration file.

7) Store the modified `input` file in the `rebranding` directory you have created in step 2.

8) Execute the following command to stop the Symphonia Framework.

```
/etc/init.d/symphoniad stop
```

9) Execute the following command to perform the `rebrand.sh` script.

<Osc#Install>`/share/tomcat/webapps/management/rebrand.sh`

10) Execute the following command to start OpenScape UC Application.

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

11) If you operate the OpenScape system as integrated cluster system, execute steps 11 and 12 on the second node, too.

NOTICE:

To display the interface elements in their modified form, enter `CTRL+F5` in the browser to delete the browser cache

4.11.8 Configuring Single Sign-On (SSO) for CMP

The Single Sign-On (SSO) feature allows users to authenticate to the CMP web application using their existing Windows domain credentials.

When SSO is enabled, the user's authentication is performed using credentials from the Windows login session managed by Active Directory (AD).

Authentication is performed using the Kerberos protocol and the SPNEGO mechanism implemented in Apache Tomcat through the **SpnegoValve** component.

Two different SSO authentication modes are supported:

- the CMP login page contains an **SSO Login** button. When the user clicks this button, SPNEGO authentication is triggered only for that specific request.

  In this mode:

  Users can still log out from CMP.

  Users can choose between standard login and SSO login.
- In the default configuration, SPNEGO authentication is automatically applied to all requests sent to the CMP server.

  In this mode, users cannot explicitly log out because authentication is managed by the Windows domain session.

  If SPNEGO authentication fails, the system falls back to the standard CMP login page.

4.11.8.1 How to Configure Active Directory (AD)

This procedure configures **Kerberos Single Sign-On (SSO)** between Active Directory (AD) and the CMP application running on Apache Tomcat.

Kerberos authentication will allow domain users to log into CMP without entering credentials manually.

Prerequisites

Administrator access to the Domain Controller on Domain Server.

Administrator access to the CMP / Tomcat server.

DNS is properly configured.

System time on both servers is synchronized.

AES256 encryption is enabled in the domain.

Step by Step

1) Create a technical user account in Active Directory (AD) that will be used for SSO connection between AD and CMP.

Example account name: `cmp`

2) Configure the **Account properties** as follows:

a) **User logon name**: HTTP/<cmp_hostname>

b) **Account expires**: Never

c) **Account options**:

a) User cannot change password.

b) Password never expires.

c) This account supports Kerberos AES 256 bit encryption.

NOTICE: All AD technical users who are eligible to login to CMP via SSO, should be configured in the same way.

---

3) Configure Kerberos Encryption Policy:
   a) On the Domain Controller, open **Local Security Policy**.
   b) Go to **Local Policies** > **Security Options**.
   c) Select **Network security** to configure encryption types allowed for Kerberos.
   d) Enable `AES256_HMAC_SHA1`
4) Before generating the keytab, verify that the service account does not already contain a Service Principal Name (SPN):

   ```
   C:/Documents and Settings/Administrator>setspn -L host
   ```

   If the account does not exist, an error similar to the following may appear:

   ```
   FindDomainForAccount: DsGetDcNameWithAccountW failed!
   Cannot find account host
   ```

   This indicates the account has not yet been created in Active Directory.

   NOTICE:

   Important SPN Rules

   When configuring SPNs:

   - Each service should use one dedicated service account.
   - Do not assign multiple SPNs to the same user unless required.

     Duplicate SPNs may cause Kerberos authentication failures.

   ---

5) Open Command Line as administrator and generate the technical user keytab file:

   ```
   ktpass -princ HTTP/CMP_hostname.domain.net@DOMAIN.NET
   -mapuser cmp@domain.net
   -pass <StrongPassword>
   -out c:\krb5.keytab
   -crypto AES256-SHA1
   -ptype KRB5_NT_PRINCIPAL
   ```

   The `ktpass` utility registers a Kerberos service principal in Active Directory and generates a keytab file used by services to authenticate with Kerberos.

   KTpass Command Parameters

princ	Specifies the Kerberos principal to register in the Kerberos realm
mapuser	Specifies the Active Directory service account mapped to the principal.
pass	Password for the service account.
out	Output file containing the generated keytab.

crypto	Encryption algorithm used for the keytab file. This parameter refers to the “Use DES…” setting when SPN user account was created. The **-crypto** parameter specifies the encryption algorithm used in the KEYTAB. Recommended setting: AES256-SHA1 **NOTICE:** Ensure that the encryption type specified with the `-crypto` parameter matches the encryption types enabled for the service account in Active Directory.

6) After running the ktpass command, verify the SPN registration:

```
setspn -L host
```

Expected output:

```
Registered ServicePrincipalNames for
 CN=host,CN=Users,DC=domain,DC=net: HTTP/host.domain.net
```

7) If an incorrect SPN exists, remove it using:

```
setspn -D HTTP/host.domain.net host
```

Alternatively, the service account can be removed from:

```
Administrative Tools → Active Directory Users and
 Computers
```

8) Check the hosts file to verify DNS or Hosts Configuration:

```
C:\WINDOWS\system32\drivers\etc\hosts
```

Example:

```
127.0.0.1 localhost
10.0.250.150 host.domain.net
```

NOTICE: Kerberos authentication requires the fully qualified domain name (FQDN) used by the service to resolve correctly.

If DNS is correctly configured, the hosts entry may not be required.

4.11.8.2 How to Configure CMP

This procedure configures Kerberos Single Sign-On (SSO) between Active Directory and CMP running on Apache Tomcat. Authentication is performed using a Kerberos service principal and keytab file.

Prerequisites

DNS is properly configured.

System time on both servers is synchronized.

AES256 encryption is enabled in the domain.

A service account exists in Active Directory.

Step by Step

1) Copy the generated keytab file to the CMP server under `/opt/siemens`.
2) Esure the `/opt/siemens/krb5.keytab` file has the correct ownership and permissions:
   - Ownership: `sym:sym`
     `chown sym:sym /opt/siemens/krb5.keytab`
   - Permissions: `600`
     `chmod 600 /opt/siemens/krb5.keytab`
3) If needed, check the user's Service Principal Domain information:

   `setspn -L "username"`
   Example: `setspn -L cmp`
4) Edit the `/opt/siemens/common/conf/krb5.conf` file to configure Kerberos.

   Example configuration:

```
[libdefaults]
default_realm = DOMAIN.NET
default_tkt_enctypes = aes256-cts-hmac-sha1-96
default_tgs_enctypes = aes256-cts-hmac-sha1-96
 default_checksum = rsa-md5
kdc_timesync = 0
# kdc_default_options = 0x40000010
 # clockskew = 300
 # check_delegate = 0
# ccache_type = 3
# kdc_timeout = 60000
# udp_preference_limit = 1
[realms]
DOMAIN>NET = {
kdc = xx.xx.xx.xx:88
}
[domain_realm]
.domain.net = DOMAIN.NET
[logging]
 default = krb5.log
```

   NOTICE:

   Multiple Kerberos realms can be configured if required.

5) Edit `/opt/siemens/common/conf/krb5.conf` to ensure that the CMP configuration references the keytab file and Kerberos principal:
   - **useKeytab=** "FILE:/opt/siemens/krb5.keytab"
   - **principal=** "HTTP/CMP_hostname.domain.net@DOMAIN.NET

   The principal must match the following values:
   - The SPN registered in AD
   - The principal used when generating the keytab
   - The fully qualified domain name (FQDN) used by users in their browser

6) Locate the instance configuration file:

```
cd /opt/siemens/common/conf/config-beans
grep -i Spnego
```

Example output:

```
/opt/siemens/common/conf/config-beans/
instance_7a2cc19e-94a1-4d2d-
b4a8-434f618e7aba.xml:<InstanceData
className="com.siemens.symphonia.spnegoiae.impl.SpnegoIae
Impl" displayName="SPNEGO IAE service" enabled="true"
guid="7a2cc19e-94a1-4d2d-b4a8-434f618e7aba"
version="1.0.0">
```

Example instance configuration file: `instance_7a2cc19e-94a1-4d2d-b4a8-434f618e7aba.xml`

a) Edit the instance configuration file and update the Service Principal Name:

```
<Property name="ServicePrincipalName"
value="HTTP/CMP_hostname.domain.net@DOMAIN.NET"/>
```

7) Enable SPNEGO in Tomcat:

```
/opt/siemens/share/tomcat/conf/Catalina/localhost/
management.xml
```

a) Update the following settings:

- **spnegoIaeUrl**: replace localhost with your “CMP_hostname.domain.net”
  `spnegoIaeUrl = CMP_hostname.domain.net`
- **userSsoButton**: replace the value with “true”
  `userSsoButton = true`

8) Restart the Symphonia to apply the changes:

```
/etc/initd/symphonia restart
```

9) Configure CMP Users for SSO:

a) Log in to CMP.
b) Go to **Configuration** > **CMP** > **Administrators** > **List**.
c) Create or edit a user.
d) Select Single Sign-On domain.
e) Type the Active Directory username.

4.11.9 CAC (Common Access Card) Login Method to CMP

The objective of CAC (Common Access Card) login is to use a smart-card in order to be able to login to CMP. Hence, one will use a two-factor authentication method to login to CMP.

The client certificate for https access is installed on the smart-card after entering the smart-card related pin via the card reader/software. Once the smart card is inserted, the certificate is installed on the windows certificate store.

This can be verified by using Windows MMC (Microsoft Management Console) (File -> Add/Remove Snap-in -> Certificates -> Add -> OK). The client certificate should be created with the CN (Common Name) field set (eg. use the

IP/FQDN of client). The certificate should be visible under MMC "Certificates - Current User -> Personal -> Certificates".

Then, using IE/Firefox/Chrome (the Windows MMC does not auto upload the client installed certificates on Firefox/Chrome browsers - one needs to manually import them via each browser related menu eg. Options -> Advanced -> Certificates) and typing the CMP URL, user will be prompted to enter the PIN related to the smart-card and CMP login will take place.

The following prerequisites are necessary:

- Client Certificate created based on the Root CA of the CMP server and set its CN (Common Name) field with the client IP/FQDN.
- Smart-card and card reader connected to the client pc and related smart-card software installed
- http browser (IE, Firefox, Chrome) can access the certificates provided by the smart-card through the corresponding software (either Microsoft or provided with the card reader).
- CMP server certificate in PKCS#12 format (.p12) signed by the Root CA and set its CN (Common Name) field with the server IP/FQDN.
- Root CA certificate in .cer format

Start the configuration

Certificates creation (eg. generated via Microsoft Certificate Authority, XCA tool or other way):

Step by Step

1) Export the CMP server certificate "`uc_server_cert.p12`" with the option PKCS #12 with certificate chain and name it "`tomcat-keystore.p12`"

Upload it to CMP at /tmp directory.

2) Backup the existing keystore.

```
cp -p /opt/siemens/common/conf/tomcat-keystore.p12 /
opt/siemens/common/conf/tomcat-keystore.p12_ORIG
```

3) Import file and copy in the new keystore and set valid ownerships and permissions

```
cp -p /tmp/tomcat-keystore.p12 /opt/siemens/common/
conf/tomcat-keystore.p12
```

```
chown sym:sym /opt/siemens/common/conf/tomcat-
keystore.p12
```

```
chmod 0644 /opt/siemens/common/conf/tomcat-keystore.p12
```

4) Encode the keystore password

```
/opt/siemens/servicetools/cmp/encodePassphrase.sh
```

eg. Provide passphrase to protect: "enter your passphrase" (certificate password)

(Store the output)

Provide passphrase to protect: "enter your passphrase"

Repeat passphrase: "enter your passphrase"

5) Backup the existing server.xml file, apply changes and save the file

`cd /opt/siemens/share/tomcat/conf/`

`cp -p server.xml server.xml_ORIG`

In `/opt/siemens/share/tomcat/conf/server.xml`, Connector `<name="CMP_https>>>` replace `keystorePass=""` with the encoded output from step 4

6) In `/opt/siemens/share/tomcat/conf/server.xml`, Connector `<name="CMP_https>>>` set `clientAuth="true"`

Save the file.

7) Create Truststore and import the trusted RootCA certificate to it.

Upload "`RootCA.cer`" to `/tmp`

NOTICE:

Run the related commands in one line.

```
openssl pkcs12 -export -out /opt/siemens/common/conf/
truststore.p12 -in /tmp/RootCA.cer -nokeys
```

Provide passphrase to protect: "enter your passphrase"

`chmod 0644 trustore.p12`

`chown sym:sym trustore.p12`

8) Encode the truststore password

`/opt/siemens/servicetools/cmp/encodePassphrase.sh for the passphrase used in step 7.`

Provide passphrase to protect: "enter your passphrase"

Repeat passphrase: "enter your passphrase"

(Store the output)

9) Edit the "CMP_https" connector on server.xml file and add information about the truststore

In `/opt/siemens/share/tomcat/conf/server.xml`, under Connector `<name="CMP_https>>>` add.

truststoreAlgorithm="`PKIX`"

truststoreFile="`/opt/siemens/common/conf/trustore.p12`"

truststorePass="`copy encoded passphrase from step 8`"

truststoreType="`PKCS12`"

Save the file `/opt/siemens/share/tomcat/conf/server.xml`

10) Enable SSLSymphoniaAuthenticator valve in management.xml file

```
cd /opt/siemens/share/tomcat/conf/Catalina/localhost
```

```
cp -p management.xml management.xml_ORIG
```

Edit the `management.xml` file

remove the comments (<!-- -->) from following line to enable this needed SSLSymphoniaAuthenticator valve

```
<Valve className=
"com.siemens.symphonia.portal.ssl.clientauth.SSLSymphoniaAuthe
>
```

the value of useSsoButton should be set to "true"

Save the file

11) Link the client certificate on the smart-card with the CMP administrator user

a) Login to CMP and go to administrator user and add the needed externalID using the CN (Common Name) value from the client certificate

b) Configuration - CMP - Administrators - List - edit the administrator - External IDs - click Add and set on fields:

- externalId: "set the value of CN (Common Name) field from the client certificate - eg. the IP/FQDN used on CN field"
- assignedExternalSystemId: PKI_LOGIN
- ProvisioningMaster: unchecked/disable

c) Save the external ID form

d) Logout from CMP

12) Restart the CMP server.
`/etc/init.d/symphoniad restart`

The CAC (Common Access Card) authentication method to login to CMP process, is as follows:

1) The user adds the smart-card (which has already loaded the client certificate with the CN (Common Name) field of certificate, set with the IP/FQDN of client pc) on the card-reader.

2) The smart-card automatically loads the certificate to Windows/ IE http browser.

3) The user is prompt to enter the smart-card PIN.

4) The user enters the correct smart-card PIN.

5) The web server passes the user certificate to the web application (CMP) server for validation checks.

6) If validation checks pass, the CMP allows login, otherwise the CMP rejects the login request.

7) The user enters the CMP IP address for web access. eg. https://10.12.5.100/management.

Login to CMP will take place via the smart-card login method.

The user (administrator) will be able to login either by clicking on the available "CAC Login" button -or- he may enter the CMP user credentials on the related fields.

5 System Monitoring

System monitoring features deliver information on the system, especially alarms and fault messages automatically from the system components as base for maintenance actions. System processes are written to logging files find out different reasons about erroneous behaviour. Audit log logs all important activities performed by the Common Management Platform users.

5.1 Concept of Alarms, Fault Messages and SNMP traps

Alarms inform the administrator about system events which affect the system operation currently or may affect the system operation in the future.

Alarm generation

Alarms can be generated in two ways:

- Directly as alarm via a so-called AlarmReceiver service. This option is e.g. used by OpenScape clients and the OpenScape
- Indirectly, by generating a fault from which the corresponding alarms are derived. This option is used by internal OpenScape services.

Alarm Status

Each alarm has a status of *Confirmed* or *Unacknowledged*.

- An alarm with a status of *Unacknowledged* is called an active alarm.
- If the status of an alarm is changed from *Unacknowledged* to *Confirmed*, the alarm is labeled as *Reset*.
- If the status of an alarm is changed from *Confirmed* to *Unacknowledged*, the alarm is labeled as *Raised*.

When an alarm is created the status is set to *Unacknowledged* by default. The status is changed to *Confirmed* when a raise condition is detected to be valid. The status can then be changed back to *Unacknowledged* when a reset condition is detected to be valid (automatically reset) or when the alarm is manually reset by the administrator or another external Fault Management system.

Framework alarms raised in the system are sent to alarm destinations. These alarm destinations can be displayed in an alarm destination list. An alarm destination consists of an IP address and a TCP/IP port.

Alarm Treatment

All alarms and faults created by the installed OpenScape systems and OpenScape applications can be centrally monitored in the Common Management Platform. Administrators receive in the Common Management Platform an overview of all alarms and faults, can sort and filter them according to various criteria, and can also acknowledge alarms. In addition, the alarms are optionally forwarded to the *OpenScape Fault Management* via SNMP traps.

An alarm is treated by the OpenScape system in the following way:

- Each alarm stays active for a maximum of seven days (active alarm). After this time at the latest, every active alarm is automatically moved to the alarm log and removed from the list of active alarms

- If an active alarm is confirmed, a copy of the alarm is automatically generated in the alarm log. Furthermore, the alarm stays in the list of active alarms to allow the tracking of its processing
- If an active alarm is deleted, the alarm is automatically moved to the alarm log and thus prematurely removed from the list of active alarms.

Alarms and SNMP traps

At Port 8167 SNMP-agent supplies the Management Information Base (MIB) info (SharedServices MIB) to an external SNMP requesting entity. See also section *5.2.3 How to configure SNMP Agent in CMP*

MIB can be found in PRISMA, IFMDB and on UC Backend under `/opt/siemens/servicetools/snmp`. In the MIB file itself you can find description of its semantics.

The SNMP agent sends SNMP-traps to alarm destinations, which can be configured over CMP/UI. For example it can send traps at service status change. See also section *5.2.2.1 How to Add an Alarm Destination*

Alarm Logs

After having moved to the alarm log, an alarm will stay there for a maximum of 14 days for documentation. After this time, it will be automatically deleted from the alarm log.

The automatic moving of active alarms and the deleting of the alarms from the alarm log is accomplished by two independent jobs. The OpenScape system executes these jobs once per hour.

5.2 Alarm Reporting

The alarm reporting feature provides for the reporting of faults detected by the application software executing on OpenScape Voice using the common interface provided by the RTP (Resilient Telco Platform) event manager. Detected faults are identified by RTP events with a priority of 1, 2, or 3 which corresponds to critical, major, and minor alarm levels, respectively.

With an alarm the system generates a notification to an administrator. Alarms could be the result of:

- at least one fault was detected in the system
- exceeding of configured thresholds like number of licenses used, CPU usage, etc.
- a system overload

Alarm Status

Each alarm has a status of *Confirmed* or *Unacknowledged*.

- An alarm with a status of *Unacknowledged* is called an active alarm.
- If the status of an alarm is changed from *Unacknowledged* to *Confirmed*, the alarm is labeled as *Reset*.
- If the status of an alarm is changed from *Confirmed* to *Unacknowledged*, the alarm is labeled as *Raised*.

When an alarm is created the status is set to *Unacknowledged* by default. The status is changed to *Confirmed* when a raise condition is detected to be valid. The status can then be changed back to *Unacknowledged* when a reset

condition is detected to be valid (automatically reset) or when the alarm is manually reset by the administrator or another external Fault Management system.

Framework alarms raised in the system are sent to alarm destinations. These alarm destinations can be displayed in an alarm destination list. An alarm destination consists of an IP address and a TCP/IP port.

Each alarm has an alarm level such as Critical, Major, Minor etc.

Each alarm may belong to an alarm group – e.g. Platform, Application A, Appl. B

Each alarm has an alarm condition. It is the description of the condition under which an alarm is raised or reset. The alarm condition may be e. g. a specific group of faults or specific occurrences of a fault. This can also be used as a way to group faults from the same or related area.

Each alarm can have none or multiple actions. The alarm action is the description of the action to take when the status of an alarm is raised/reset. An alarm action is e. g. setting an SNMP trap, stopping the trace or restarting the malfunctioned component. For an SNMP trap there must be an alarm destination. The desination is the IP address/host name of an external Fault Management system (e.g. HiSpa client of RCC). Every SNMP Trap is sent to the global list of alarm destinations.

Alarms will be cleared automatically when the alarm condition has ended.

5.2.1 Active Alarms

In the Common Management Platform you can manage all alarms currently active in the system. All currently active alarms are displayed. In addition, an overview shows the number of currently active alarms of a particular severity (e. g. Critical, Major, Minor, ...). Through selection of an alarm you can get alarm details.

The following Alarm Details are provided:

Below **General tab** the following information is given:

- **Alarm ID**

  that uniquely identifies an alarm.
- **Severity**

  The severity level shows how critical an alarm is. The following severity levels can be displayed:

  – Critical (red)
  – Major (orange)
  – Minor (yellow)
  – Warning (cyan)
  – Information (blue)
  – Normal (green)

- **Origin**

  Specifies which application or which system has raised the alarm. The following are supported:

  – OpenScape Voice
  – Openscape Voice Assistant
  – UNIFYSharedServices
  – Media Server
  – Xpressions
  – RG8700
  – RG2700
  – IBMSametimeServices
  – OpenScape Branch
  – OpenScape 4000
  – OpenScape SBC
  – OpenScape Branch/SBC Assistant
  – DLS
  – OSCCE
  – HiPath CAPFM
- **Managed Resource (alarm source ID)**

  Describes the entity that has generated the alarm. This is either a Fault Handler or an SNMP Trap Receiver (which makes the connection to the OpenScape Voice system and the RG8700-Gateway). The entity is referenced by a GUID (Global Unique Identifier). This GUID can be used to identify the alarm source in the system management.
- **Source Name:** Alarms source name
- **Alarm Type:**

  Designates the type of alarm.
- **Last Occurred**

  Date and time when this alarm last occurred.

  NOTICE:

  In case of H4k incoming traps, the time when the trap is received in the UC backend, is always displayed.
- **Status**

  Indicates whether the alarm was confirmed by an administrator or whether it has not yet been confirmed.
- **Hit Count**

  Shows how many times an alarm has been triggered since the last acknowledge action.
- **User**

  Name or ID of the user associated with the alarm. If the alarm is unconfirmed the display remains empty.

Below **Description tab** the following information is given:

- This shows you a more detailed description of the selected alarm.

Below **Notes tab** the following information is given:

- This displays additional notes that have been entered for the selected alarm.

Below **Related Faults tab** the following information is given:

- This shows a list of all faults that have caused a selected alarm.

5.2.1.1 How to Display Active Alarms

How to display Active Alarms

Prerequisites

Adequate administrative permissions

Step by Step

1) Navigate to **Maintenance** > **Monitoring** > **Alarms** > **Active** in the navigation tree.

- A list of all active alarms currently active in the selected domain appears in the work area.

NOTICE:

Maybe you can’t see any alarms: Check the area **Advanced** for applied filters.

NOTICE:

Clicking on menu items of the alarm table in the window **Active alarms** sorts the sequence of entries.

---

2) Click on the **Alarm ID** of the desired alarm.

NOTICE:

Check your rights to be authorizised to look at all alarms.

The dialog with the associated information opens.

3) Click the tabs **General**, **Description**, **Notes** to get alarm details.

NOTICE:

Place your mouse on top of each item on the list for a few seconds in order to view the whole name of:

Alarm Type, Managed Resource, Alarn Source Name

5.2.1.2 How to Set a Filter for Active Alarms

The filter feature allows you to search for specific active alarms by defining search criteria in a filter. Once a filter is selected only specific active alarms matching the criteria defined in the filter selected will be displayed. This reduces

the total number of active alarms displayed and makes it easier to find a specific alarm or group of alarms:

Prerequisites

Adequate administrative permissions

Step by Step

1) Navigate to **Maintenance** > **Monitoring** > **Alarms** > **Active** in the navigation tree.

A list of all active alarms currently active in the selected domain appears in the work area.

2) Click **Advanced**.

A dialog showing the filter settings is displayed.

3) Click on the tab **General**.

4) Select an option in the area **Date**:

- **All**: All alarms are displayed.
- **After Date**: Only the alarms after the specified date are displayed
- **Before date**: Only the alarms before the specified date are displayed
- **Between dates**: Only the alarms within the specified date range are displayed.

5) Select an option in the area **User**:

- All users: All alarms of all users are displayed.
- Current user <user ID>: The alarms of the user currently logged in are displayed.

6) Select an option in the area **Alarm ID**:

- All: All alarms are displayed.
- Within alarm ID range: Only the alarms within the specified alarm ID range are displayed.

7) Click on the tab **Severity**.

a) In the area **Severity** deactivate the alarm categories which are not to be displayed.

b) In the area **Acknowledge Status** deactivate the alarm categories which are not to be displayed.

8) Click on the tab **Origin**.

9) Deactivate the systems for which the alarms are not to be displayed in the area **Origin**.

10) Click on the tab **Managed Resources**.

a) Deactivate the option **Disable filtering by resource** to filter the active alarms based on resources.

b) Mark the checkboxes of the resources the active alarms of which you want to display.

11) Click on the **Alarms Source Name** tab

a) Deactivate the option **Disable filtering by source** to filter the active alarms based on alarm sources.

b) Mark the checkboxes of the sources the active alarms of which you want to display.

12) Click **Apply** .

The active alarms list/alarm log only displays the alarms that correspond to the filter settings made.

5.2.1.3 How to Change Filter for Active Alarms

How to change Filter for Active Alarms:

Prerequisites

Adequate administrative permissions

Step by Step

1) Navigate to **Maintenance** > **Monitoring** > **Alarms** > **Active** in the navigation tree.

   A list of all active alarms currently active in the selected domain appears in the work area.
2) Click **Advanced**.

   A dialog showing the filter settings is displayed.
3) Apply changes to the filter settings.
4) Click **Apply**

NOTICE:

If you leave or refresh the filter page the “applied filter “ will reset.

5.2.1.4 How to Delete a Filter for Active Alarms

How to clear a filter for active Alarms:

Prerequisites

Adequate administrative permissions

Step by Step

1) Navigate to **Maintenance** > **Monitoring** > **Alarms** > **Active** in the navigation tree.

   A list of all active alarms currently active in the selected domain appears in the work area.
2) Click **Show All**.

The Filter field displays **No filter applied** and the list of active alarms contains all currently active alarms again.

NOTICE:

If you leave or refresh the filter page the “applied filter “ will reset.

5.2.1.5 How to Mask an Alarm

How to mask an Alarm:

Prerequisites

Adequate administrative permissions

Step by Step

1) Navigate to **Maintenance** > **Monitoring** > **Alarms** > **Active** in the navigation tree.

   A list of all active alarms currently active in the selected domain appears in the work area.
2) Select the checkboxes of the alarms / Alarm IDs you want to mask.
3) Click **Mask ID**.

The alarms with the selected Alarm IDs are masked and no longer visible in the active alarm list.

5.2.1.6 How to Display Masked Alarms

How to display masked alarms:

Prerequisites

Adequate administrative permissions

Step by Step

1) Navigate to **Maintenance** > **Monitoring** > **Alarms** > **Active** in the navigation tree.

   A list of all active alarms currently active in the selected domain appears in the work area.
2) Click **Show Masked**.

   The list shows alarms that are masked and the **Show Masked** button changes to **Show Unmasked** .
3) To unmask alarms displayed tick the relative checkbox and click **Unmask ID**.

5.2.1.7 How to Confirm Alarms

If you have verified an alarm or want to notify the system or other administrators that you are dealing with rectifying the fault, you can confirm this alarm. If an active alarm is confirmed, a copy of the alarm is automatically generated in the alarm log. Furthermore, the alarm stays in the list of active alarms to allow the tracking of its processing

Prerequisites

Adequate administrative permissions

Step by Step

1) Navigate to **Maintenance** > **Monitoring** > **Alarms** > **Active** in the navigation tree.

   A list of all active alarms currently active in the selected domain appears in the work area.
2) Select the checkboxes of the alarms you want to acknowledge.
3) Click **Acknowledge** button.

   The **Acknowledge** window opens. In the field **Add a note** you can enter information.
4) Continue with **Save**.

In the active alarms list the status of the selected alarms changes to a green dot in the column **Acknowledged** and your user ID is entered in the **User** column.

5.2.1.8 How to Cancel an Alarm Acknowledgement

You can cancel the confirmation for confirmed alarms. How to cancel the confirmation for an active alarm:

Prerequisites

Adequate administrative permissions

Step by Step

1) Navigate to **Maintenance** > **Monitoring** > **Alarms** > **Active** in the navigation tree.

   A list of all active alarms currently active in the selected domain appears in the work area.
2) Select the checkboxes of the alarms those acknowledgements you want to cancel.

   NOTICE:

   Only select those alarm confirmations that have the status *Acknowledged* in the column Acknowledged Status.
3) Click **Unacknowledge**.

The active alarms list the confirmation status of the selected alarms changes to Unacknowledged and the user ID is deleted in the **User** column.

5.2.1.9 How to Clear Alarms

If the fault for an alarm has been rectified or the alarm is no longer active for anyother reason, you can clear the alarm. If an active alarm is deleted, the

alarm is automatically moved to the alarm log and removed from the list of active alarms. How to remove an alarm from the active alarms list:

Prerequisites

Adequate administrative permissions

Step by Step

1) Navigate to **Maintenance** > **Monitoring** > **Alarms** > **Active** in the navigation tree.

   A list of all active alarms currently active in the selected domain appears in the work area.
2) Select the checkboxes of the alarms you want to delete.
3) Click **Clear**.

The selected alarms are deleted and no longer displayed in the active alarm list.

5.2.1.10 Alarm Severities

The importance of alarms and events and alarms is classified by the parameter severity.

The kinds of severity:

- Critical
  - service severely impacted
  - requires timely repair
- Major
  - requires timely repair
  - no or little service impact
  - loss of redundancy
- Minor
  - no service impact
  - case for deferred maintenance
  - requires offline analysis
- Warning
  - non-alarmed event, but still reported via SNMP traps
  - no clearance event necessary
  - corrective action in connection with scheduled maintenance
- Information
  - non-alarmed event
  - no clearance event necessary
- Clear / Normal
  - Alarm clearance event

5.2.2 Alarm Email Notification

In OpenScape Voice communication system you have the option to generate an e-mail automaticaly whenever an emergency call is detected.

The Administrator configures a list of recipients that will be automatically notified via e-mail when specific SNMP Trap are detected. The Administrator can also configure the content of the notification e-mail.

5.2.2.1 How to Configure E911 Alarm Email Notification

When an Emergency Call 911 is initiated within OSV an Alarm is generated by the system. The administrator can be notified if the **E911 Alarm Email Notification** service is configured and enabled:

Prerequisites

Adequate administrative permissions

The SMTP (Simple Mail Transfer Protocol) server in CMP has been configured and enabled.

Step by Step

1) Navigate to **Maintenance** > **Monitoring** > **Alarms** > **E911 Alarm Email Notification**.

The **E911 Alarm Email Notification** window opens and next to information icon you can see if SMTP server is enabled or disabled.

2) Select the **Enable Email Notifications**box.

The E911 e-mail notification is enabled if the box is ticked.

NOTICE:

If the **Enable Email Notifications** box is ticked then at least one recipient must be defined.

---

3) Navigate to the Notification Email area and configure the mandatory fields of the mail that will be sent:

a) **From**: A valid email address must be entered
b) **Subject**: Default entry is “E911 Alarm Notification”
c) **Message**: Default entry is “This is an e-mail notification for an E911 Alarm.”

The mail is sent to all recipients with high priority and following Alarm Details automatically append the message text:

-Trap Name: hiQEmergencyCallIdTrap

-Alarm Description: The OSV server is processing an Emergency Call..

-Severity: Warning-Cluster Name:

-Short Text: Emergency Call from endpoint DN = xxx to Emergency Number =yyy

-D1 Repair Text: No action is necessary.

4) Add the recipients of the notification mail as described in the relative chapter.

5) Click **Save**.

The **E911 Alarm Email Notification** is configured.

5.2.2.2 How to Add/Edit Recipients of E911 Alarm Email Notification

How to add/edit recipients of E911 Alarm Email Notification:

Prerequisites

Adequate administrative permissions

The SMTP (Simple Mail Transfer Protocol) server in CMP has been configured and enabled.

Step by Step

1) Navigate to **Maintenance** > **Monitoring** > **Alarms** > **E911 Alarm Email Notification**.

   The **E911 Alarm Email Notification** window opens and next to information icon you can see if SMTP server is enabled or disabled.
2) Select the **Enable Email Notifications**box.

   The E911 e-mail notification is enabled if the box is ticked.

   NOTICE:

   If the **Enable Email Notifications** box is ticked then at least one recipient must be defined.
3) Navigate to the Notification Email area and configure the mandatory fields of the mail that will be sent as described in relative chapter
4) Navigate to the List of recipients area and **Add...** a recipient or **Edit...** an existing one.

   The Recipient window opens.
5) Enter the following mandatory parameters:

   Name: Enter a name of the recipient (this name will not appear in the email notification)

   Email: A valid email address must be entered
6) Click on **Save**

   The recipient is saved to the list.

   NOTICE:

   If Email is already used for another recipient then a validation message appears.

7) Click **Save**.

NOTICE:

If the SMTP server is not configured then a warning message informs you that:

The SMTP server is not configured. The e-mails will not reach the recipients until you have configured the SMTP servert.

The **E911 Alarm Email Notification** is configured.

5.2.3 Alarm Logs

An alarm log provides an alarm history for a longer period of time. If an alarm log is not modified within 14 days, it is automatically deleted.

5.2.3.1 How to Display Alarm Log

How to display Alarm Logs:

Prerequisites

Adequate administrative permissions

Step by Step

1) Navigate to **Maintenance** > **Monitoring** in the navigation tree.
2) Click on the **Logs** > **Alarms**

   A list of all alarms logged in the selected domain appears in the work area.

NOTICE:

Maybe you can’t see any alarms: Check the area **Advanced** for applied filters.

NOTICE:

Clicking on menu items of the alarm table in the window **Alarm Log** sorts the sequence of entries.

3) Click on the **Alarm ID** of the desired alarm log.

NOTICE:

Check your rights to be authorizised to look at all alarms.

   The dialog with the associated information opens.
4) Click the tabs **General**, **Description**, to get alarm log details.

5.2.3.2 How to Set a Filter for Alarm Logs

The filter feature allows you to search for specific alarm logs by defining search criteria in a filter. Once a filter is selected only specific alarm logs matching the criteria defined in the filter selected will be displayed. This reduces the total number of alarm logs displayed and makes it easier to find a specific alarm or group of alarms:

Prerequisites

Adequate administrative permissions

Step by Step

1) Navigate to **Maintenance** > **Monitoring** in the navigation tree.

2) Click on the **Logs** > **Alarms**

A list of all alarms logged in the selected domain appears in the work area.

3) Click **Advanced**.

A dialog showing the filter settings is displayed.

4) Click on the tab **General**.

5) Select an option in the area **Date**:

- **All**: All alarms are displayed.
- **After Date**: Only the alarms after the specified date are displayed
- **Before date**: Only the alarms before the specified date are displayed
- **Between dates**: Only the alarms within the specified date range are displayed.

6) Select an option in the area **User**:

- All users: All alarms of all users are displayed.
- Current user <user ID>: The alarms of the user currently logged in are displayed.

7) Select an option in the area **Alarm ID**:

- All: All alarms are displayed.
- Within alarm ID range: Only the alarms within the specified alarm ID range are displayed.

8) Click on the tab **Severity**.

In the area **Severity** deactivate the alarm categories which are not to be displayed.

9) Click on the tab **Event Type**

   Event Type:specifies the following information about the progress of the alarm:

   - **New**: New Alarm
   - **Reoccurred** : An already existing alarm has reoccurred. The time stamp of the existing alarm is refreshed and the alarm hit count is increased by one.
   - **Confirmed**: An administrator has confirmed the alarm. The alarm is still active.
   - **Unacknowledged** : An administrator has not yet confirmed the alarm. The alarm is still active.
   - **Cleared** : The alarm has been cleared, either by an administrator, by the system, or by a cyclic cleanup feature.
   - **Unknown**: The type of alarm could not be recognized by the system.

10) Click on the tab **Origin**.

11) Deactivate the systems for which the alarms are not to be displayed in the area **Origin**.

12) Click on the tab **Managed Resources**.

    a) Deactivate the option **Disable filtering by resource** to filter the active alarms based on resources.

    b) Mark the checkboxes of the resources the active alarms of which you want to display.

13) Click on the **Alarms Source Name** tab

    a) Deactivate the option **Disable filtering by source** to filter the active alarms based on alarm sources.

    b) Mark the checkboxes of the sources the active alarms of which you want to display.

14) Click **Apply** .

The active alarms list/alarm log only displays the alarms that correspond to the filter settings made.

5.2.3.3 How to Change Filter for Active Alarms

How to change Filter for Active Alarms:

Prerequisites

Adequate administrative permissions

Step by Step

1) Navigate to **Maintenance** > **Monitoring** > **Alarms** > **Active** in the navigation tree.

   A list of all active alarms currently active in the selected domain appears in the work area.

2) Click **Advanced**.

   A dialog showing the filter settings is displayed.

3) Apply changes to the filter settings.

4) Click **Apply**

NOTICE:

If you leave or refresh the filter page the “applied filter “ will reset.

5.2.3.4 How to Delete a Filter for Alarm Log

How to clear a filter for Alarm Log:

Prerequisites

Adequate administrative permissions

Step by Step

1) Navigate to **Maintenance** > **Monitoring** in the navigation tree.
2) Click on the **Logs** > **Alarms**
   A filtered list of all alarms logged in the selected domain appears in the work area
3) Click **Show All**.

The Filter field displays **No filter applied** and the list of active alarms contains all currently active alarms again.

NOTICE:

If you leave or refresh the filter page the “applied filter “ will reset.

5.2.4 System Log Concept

The System logs register all important system activities performed by the Common Management Platform users. Activities comprise all entries and actions at the Common Management Platform.

The size and number of log files can be defined. If the definable size of the log file is exceeded, the file is automatically closed and backed up, and a new file is created.

The System log can be exported and saved as log file. Older log files with past activities can be imported in the system.

System Specific Information

The log files delivers the following information:

- **Date/Time**: Shows the date and time stamp of the logged activities.
- **User**: Shows the user of the logged activities.
- **Job ID**: Shows the Job Id if one is available.
- **Command**: Displays the executed action or command.
- **Result**: Shows the result of the activity or command.

- **Additional Info**: Shows additional information on the activity or command, as e.g. JobName and JobInfo.
- **Parameters**: Shows additional parameter information on the activity or command.

  For *OpenScape Voice Assistant* the **Parameters** displays among other information the following parameters that help to pinpoint the entity that is affected by the activity or command:

  - the action or command Unique Id (Item name etc) that was performed

  - the Switch Name *"switchName*"

  - and the Business Group name “"bgname”" if a BG is involved.

5.2.4.1 How to Display a System Log

Display of all logged activities.

Prerequisites

Adequate administrative permissions

Step by Step

1) Navigate .**Maintenance** > **Monitoring** .

2) In the navigation tree click **Logs** > **System**.

3) Select the audit log of the node selected from the **Node** selection box.

A list of all activities logged for the relevant node appears in the work area.

4) Click on the date/ time specification of the activity for which you want to display the details.

The Audit Log dialog with the associated activity details opens.

5) Click on the **General** tab to display the following fields:

- **Date/Time**: Shows the date and time stamp of the logged activities.
- **User**: Shows the user of the logged activities.
- **Job ID**: Shows the Job Id if one is available.
- **Command**: Displays the executed action or command.
- **Result**: Shows the result of the activity or command.
- **Additional Info**: Shows additional information on the activity or command, as e.g. JobName and JobInfo.

6) Click on the **Parameters** tab to show additional parameter information on the activity or command.

For *OpenScape Voice Assistant* the **Parameters** field displays among other information the following parameters that help to pinpoint the entity that is affected by the activity or command:

- the action or command Unique Id (Item name etc) that was performed

- the Switch Name *"switchName*"

- and the Business Group name “"bgname”" if a BG is involved.

7) Click **Close** to close the activity details window.

5.2.4.2 How to Export a System Log

For externally processing audit logs can be exported and saved as log file.

Prerequisites

Adequate administrative permissions

Step by Step

1) Navigate .**Maintenance** > **Monitoring** .
2) In the navigation tree click **Logs** > **System**.
3) Select the audit log of the node selected from the **Node** selection box.

   A list of all activities logged for the relevant node appears in the work area.
4) Click **Download**.

   The audit log data is downloaded from the server and saved in an XML file.

5.2.4.3 How to Load a System Log

How you can import exported System log data in the system

Prerequisites

Adequate administrative permissions

Step by Step

1) Navigate to **Maintenance** > **Monitoring**.
2) In the navigation tree, click **Logs** > **System**.
3) Select the audit log of the node selected from the **Node** selection box.

   A list of all activities logged for the relevant node appears in the work area.
4) Click **Choose audit file**.

   A window with all loadable log files opens.
5) Select the desired log file.
6) Click **Save**.

   The System log data from the selected log file is imported in the system and displayed in the activities list.

5.2.4.4 How to Set Filter for a System Log

The search for specific activities can be defined by search criteria in a filter. Once a filter is selected, only specific activities matching the criteria defined in the selected filter will be displayed. This reduces the total number of activities displayed and makes it easier to find a specific activity or group of activities.

Prerequisites

Adequate administrative permissions

Step by Step

1) Navigate to **Maintenance** > **Monitoring**.
2) In the navigation tree, click **Logs** > **System**.
3) Select the System log of the node selected from the **Node** selection box.

   A list of all activities logged for the relevant node appears in the working area.
4) Click **Advanced**.

   The dialog with the filter settings opens.
5) If you want to filter according to a specific time range or specific user groups click on the **General** tab and specify the desired filter settings.
6) If you want to filter commands according to certain categories, click the **Category** tab and select the desired category.
7) If you want to filter entries according to successful and/ or faulty entries, click the **Result** tab and mark the desired checkbox.
8) If you want to filter the entries according to a term in the additional information, click the **Additional Info** tab and enter the search item under **Filter information** and/or **Invert Selection Filter**.You can also enter a term that is only part of the full range of additional information.

   IMPORTANT:

   For the **Filter information** field, the filter searches for the requested term without the wildcard (*) character but it is also case sensitive.

   IMPORTANT:

   For the **Invert Selection Filter** field, wildcard pattern "*","?" can be used.

   e.g. *Invocation*|*renewStatement*|*execption*

   ---

9) If you want to filter the entries according to a parameter, click the **Parameters** tab and enter the search term under **Parameter string**. You can also enter a term that is only part of the full range of parameters.
10) Click **Apply**.

    The System log will only display activities that correspond to the filter settings made.

    NOTICE:

    If you leave or refresh the filter page the “applied filter “ will reset.

5.2.4.5 How to Clear Filter for System Log

How to clear filter for System Logs:

Prerequisites

Adequate administrative permissions

A filter was set, this is indicated in the **Filter** field.

Step by Step

1) Navigate to **Maintenance** > **Monitoring**.
2) In the navigation tree, click **Logs** > **System**.
3) Select the System log of the node selected from the **Node** selection box.

   A list of all activities logged for the relevant node appears in the working area.
4) Click **Show All**.

   The **Filter** field displays **No filter applied** and the activities list contains all activities again.

5.2.5 Security Log Concept

The Security logs register all important activities related to security performed by the Common Management Platform users. Activities comprise all entries and actions at the Common Management Platform.

The size and number of log files can be defined. If the definable size of the log file is exceeded, the file is automatically closed and backed up, and a new file is created.

The Security log can be exported and saved as log file. Older log files with past activities can be imported in the system.

Security Specific Information

The log files delivers the following information:

- **Date/Time**: Shows the date and time stamp of the logged activities.
- **User**: Shows the user of the logged activities.
- **Job ID**: Shows the Job Id if one is available.
- **Command**: Displays the executed action or command.
- **Result**: Shows the result of the activity or command.
- **Additional Info**: Shows additional information on the activity or command, as e.g. JobName and JobInfo.
- **Parameters**: Shows additional parameter information on the activity or command.

5.2.5.1 How to Display a Security Log

Display of all Security logged activities.

Prerequisites

Adequate administrative permissions

Step by Step

1) Navigate to **Maintenance** > **Monitoring**.
2) In the navigation tree, click **Logs** > **Security**.

   A list of all activities logged for the relevant node appears in the work area.
3) Click on the date/ time specification of the activity for which you want to display the details.

   The dialog with the associated activity details opens.
4) Click tabs **General** and **Parameters**.

   This displays the detailed information.
5) Click **Close** to close the activity details window.

5.2.5.2 How to Export a Security Log

Security logs can be exported and saved as log file:

Prerequisites

Adequate administrative permissions

Step by Step

1) Navigate .**Maintenance** > **Monitoring** .
2) In the navigation tree click **Logs** > **Security**.
3) Select the audit log of the node selected from the **Node** selection box.

   A list of all activities logged for the relevant node appears in the work area.
4) Click **Download**.

   The Security log data is downloaded from the server and saved in an XML file.

5.2.5.3 How to Load a Security Log

How you can import exported Security log data in the system

Prerequisites

Adequate administrative permissions

Step by Step

1) Navigate to **Maintenance** > **Monitoring**.
2) In the navigation tree, click **Logs** > **Security**.

3) Select the audit log of the node selected from the **Node** selection box.

   A list of all activities logged for the relevant node appears in the work area.

4) Click **Choose audit file**.

   A window with all loadable log files opens.

5) Select the desired log file.

6) Click **Save**.

   The Security log data from the selected log file is imported in the system and displayed in the activities list.

5.2.5.4 How to Set Filter for a Security Log

The search for specific activities can be defined by search criteria in a filter. Once a filter is selected, only specific activities matching the criteria defined in the selected filter will be displayed. This reduces the total number of activities displayed and makes it easier to find a specific activity or group of activities.

Prerequisites

Adequate administrative permissions

Step by Step

1) Navigate to **Maintenance** > **Monitoring**.

2) In the navigation tree, click **Logs** > **Security**.

3) Select the System log of the node selected from the **Node** selection box.

   A list of all activities logged for the relevant node appears in the working area.

4) Click **Advanced**.

   The dialog with the filter settings opens.

5) If you want to filter according to a specific time range or specific user groups,click on the **General** tab and specify the desired filter settings.

6) If you want to filter commands according to certain categories, click the **Category** tab and select the desired category.

7) If you want to filter entries according to successful and/ or faulty entries, click the **Result** tab and mark the desired checkbox.

8) If you want to filter the entries according to a term in the additional information, click the **Additional Info** tab and enter the search item under

Filter information and/or **Invert Selection Filter**.You can also enter a term that is only part of the full range of additional information.

IMPORTANT:

For the **Filter information** field, the filter searches for the requested term without the wildcard (*) character but it is also case sensitive.

IMPORTANT:

For the **Invert Selection Filter** field, wildcard pattern "*","?" can be used.

e.g. *Invocation*|*renewStatement*|*execption*

---

9) If you want to filter the entries according to a parameter, click the **Parameters** tab and enter the search term under **Parameter string**. You can also enter a term that is only part of the full range of parameters.

10) Click **Apply**.

The Security log will only display activities that correspond to the filter settings made.

NOTICE:

If you leave or refresh the filter page the “applied filter “ is reset.

5.2.5.5 How to Clear Filter for Security Log

How to clear filter for Security Logs:

Prerequisites

Adequate administrative permissions

A filter was set, this is indicated in the **Filter** field.

Step by Step

1) Navigate to **Maintenance** > **Monitoring**.

2) In the navigation tree, click **Logs** > **Security**.

3) Select the System log of the node selected from the **Node** selection box.

A list of all activities logged for the relevant node appears in the working area.

4) Click **Show All**.

The **Filter** field displays **No filter applied** and the activities list contains all activities again.

5.2.6 Remote logging for OSV-Trace Manager

Remote logging enables the periodic transfer to the OSV Trace Manager of trace information that is extracted from `symphonia.log` files . The trace file contains all tracing information to track problems encountered with individual phone calls and includes UC and Media Server tracing information.

Remote logging is supported for all OpenScape Application deployment scenarios (StandardDuplexSmall or StandardDuplexLarge) including media server standalone, multiple communication server admin or integrated simplex.

Each of the nodes of a multi node installation sends its trace data independently to the OSV Trace Manager according to the settings you have configured in the Common Management Platform.

When you change the settings of the CMP remote logging screen (**Maintenance** > **Monitoring** > **Remote Logging for OSV-TM**) the changes of these values are applied to all nodes of a multinode installation without the need to restart.

All trace files follow the naming convention of OSV TM, they are gzipped and are transferred to the OSV TM server .

Naming convention of trace files transferred to the OSV-TM server have the following syntax

`<NEType>_<NEName>_<time>_<node-id>_<sequence no>.log.<gz>`
where :

- `NEType` == OSCUC or HMS if it is a Media Server Standalone
- `NEName` == Symphonia Community String to identify a multi node UC installation, e.g. STAREMEA
- time== year,month,day,time
- `node-id` == hostname + “-symphonia”
- `sequence` == index incremented each time a file is sent and is reset to 0 when the service starts sending the files

e.g.: OSCUC_STAREMEA_20100704231015_hermes-symphonia_37.log.gz

When enabling the remote logging, you must make sure adequate disk space is available on the OSV TM to store all the trace files that will be transferred. Periodically, the administrator must check the OSV TM disk space and remove old trace files in order to ensure that the disk doesn’t become completely full.

The following 5 alarms are generated in the CMP if there is a problem to connect to the OSV TM server , to transfer or write to OSV TM trace directory:

ID	Alarm title	Alarm description	Priority
419101	Remote logging service was unable to transfer a logging file to remote server	Unable to transfer a logging file to remote server	4
419102	Remote logging service was unable to connect to the remote server	Unable to connect to the remote server. Check if server is down or otherwise inaccessible	4

ID	Alarm title	Alarm description	Priority
419103	Remote logging service was unable to connect to the remote server	Unable to connect to the remote server because the username or password was incorrect	4
419104	Remote logging service was unable to read the properties file	Unable to read the properties from the properties file. Check if the file exists and if it is readable. Also check the permissions of the folder	3
419105	Remote logging service was unable to read the properties file	Remote logging service was unable to write the properties file. If the file exists check the permissions. Also check folder permissions and disk space	3

5.2.6.1 How to Configure Remote logging for OSV Trace Manager

Remote logging for OSV Trace Manager is configured according to the Trace Manager requirements and therefore the files generated from Symphonia log follow the OSV-TM name conventions (please see naming convention description in chapter “Remote logging for OSV-Trace Manager”). The connection to the OSV-TM server is established over Secure FTP (i.e. sftp) protocol.

Prerequisites

Adequate administrative permissions

A valid directory path of the OSV TM and write access enabled for this directory.

Knowledge of User id and Password for successful creation of sftp session.

Step by Step

1) After logging into CMP navigate to **Maintenance** > **Monitoring**

2) In the navigation tree, click **Logs** > **Remote Logging for OSV-TM**

The Remote Logging for OSV-TM window opens.

3) Check the box **Enable Remote Logging**

4) Select the sequence in which a trace file will be sent to OSV TM.

The **Send every** field can be :

from 5 to 60 **Minutes** with a step of 5 minutes

or

from 1 to 24 **Hours** with a step of 1 hour

NOTICE: The default value of **Send every** field is 5 minutes

---

NOTICE:

So if the **Send every** field is set to 5 minutes:

CMP will send every hour 12 trace files (one every 5 minutes with each one containing symphonia information for the chosen period).

If the **Send every** field is set to 30 minutes:

CMP will send every hour 2 trace files (one every 30 minutes with each one containing symphonia information for the chosen period.)

In any case the trace files sent from CMP will contain all the trace information of the chosen period.

---

5) Configure the **Save the last** field so all trace files of this time period during a transmission failure are saved in CMP and transmitted when possible.

The **Save the last** field can be :

from 5 to 60 **Minutes** with a step of 5 minutes

or

from 1 to 24 **Hours** with a step of 1 hour

NOTICE: The default value of **Save the last** field is1 hour

---

NOTICE:

If there is a transmission failure towards OSV TM and you have set the:

Save the last field to 3 hours

Send every field to 30 minutes

and the transmission to OSV TM is re-established after 5 hours

Then:

the trace files of the first 2 hours of the failure period are deleted and the last 3 hours of the period have generated 6 trace files that are sent to OSV-TM.

---

6) Enter the path[35] to OSV Trace Manager directory in the **Directory** field

---

IMPORTANT:

If no Directory is configured then the trace files will be transmitted to the SFTP User's root folder.

IMPORTANT:

You must have enable write access for the defined OSV TM directory.

---

7) In the field **IP/Hostname**, enter the IP or Hostname of the OSV TM SFTP server.
8) Enter the **Port Number** of the OSV TM SFTP server, default value is 22
9) Enter the **Username** of the OSV TM SFTP server
10) Enter the **Password** of the OSV TM SFTP server
11) Click **Save**.

    At that point the Remote Logging for OSV-TM should be activated and can be updated at any given time.

Next steps

If you want OSVTM to process trace data from continuous tracing you must also activate the specific configuration `log4j-sip-csta.xml`.

To activate this configuration file you must perform the following steps:

1) Follow the steps provided in section 1 How to Activate a Loaded Configuration File
2) Select the checkbox of the configuration file **log4j-sip-csta.xml** to activate for the node
3) Click **Activate**

5.2.7 Backing up the Log Files

In order to keep the storage space required for log files within reasonable limits, older log files are deleted automatically when the number of files exceeds a definable value.

If the log files to be backed up permanently, the backup unit audit log files must be included in the backup concept of Common Management Platform.

NOTICE: According to the concept of Common Management Platform the audit log files will be backed up as an encrypted file.

It is recommended to create a scheduled backup for this purpose.

---

[35] Example of a valid path: /OSUC

The path you enter continues from SFTP User's root folder, so if for example the full path of the root folder is "System_name/User_root" the full path registered is "System_name/User_root/OSUC"

So that you can configure an appropriate backup interval for this scheduled backup, you need to previously determine how long it takes until the log file created first is deleted.

5.2.7.1 How to Estimate Backup Interval

If you want the log files to be backed up permanently, the backup unit audit log files must be included in the backup concept of Common Management Platform. You should create a scheduled backup for this purpose. To configure an appropriate backup interval for this scheduled backup, you need to previously determine how long it takes until the log file created first is deleted. In order to estimate the backup interval, you will need to know the maximum size of the audit log file (maxFileSize) and the maximum number of log files (maxBackupIndex). These values are predefined.

Prerequisites

Adequate administrative permissions

Step by Step

1) On the **Maintenance** navigation tab, click on the **Inventory** navigation menu item.

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 work area

3) Click on the name of the system node you want activate SysLog.

A dialog box with the dashboard of the selected node opens

4) Click on **Show** next to **Actions** -**Show Services Status**

A list of all components available on the selected application computer appears in the working area.

5) In the components list look for the **log file audit component** and click on the component's name.

A window that displays the component's settings opens.

6) Note down the values under maxFileSize and maxBackupIndex, respectively.

Default values: maxFileSize=4000k , maxBackupIndex=50.

7) Click on **Cancel** to close the window with the component's settings without modification.

8) Calculate the storage space by using the formula:

Storage space=maxFileSize×maxBackupIndex

With the above default values, the storage space would be 200 MB (4000000 × 50; max 50 files of 4 MB each).

9) Calculate the maximum number of entries by using the formula:

Max. number of entries = storage space / 2000

The size of an entry is approximately 2 KB. With a storage space of 200 MB, this amounts to a maximum of 100000 possible entries in all log files.

10) Estimate how many entries are written per day, e.g. 1000 entries per day.

11) Divide the maximum possible number of entries by the number of entries approximately written per day: 100000/1000=100

In the example, the maximum possible number of entries is written after 100 days. Subsequently, the log files created first will already be deleted again.

In the example, the backup interval should therefore be less than 100 days.

5.2.8 SysLog

SysLog is an external program which is used to display the System and Security logs.

If the Common Management Platform is installed on several computer systems, the activities of all computer systems can also be forwarded via Syslog. In order to do this, the service must be enabled for each computer system and the IP address of the SysLog server must be configured.

IMPORTANT:

Since the transmission of the System or/and Security log with SysLog does not occur via a secure protocol, no security mechanisms such as authentication or encryption are possible.

SysLog should therefore only be used in secure networks.

If the System or/and Security log is to be transmitted over unsecured networks, it is necessary to also use IPSec for this purpose.

5.2.8.1 How to Enable SysLog for the System or/and SecurityLog

Activation of Syslog to transfer the System or/and Security log to an external program.

Prerequisites

Adequate administrative permissions

If Syslog is used in a system configuration with several nodes, it must be activated for each node.

Step by Step

1) On the **Maintenance** navigation tab, click on the **Inventory** navigation menu item.

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 work area

3) Click on the name of the system node you want activate SysLog.

A dialog box with the dashboard of the selected node opens

4) Click on **Show** next to **Actions** -**Show Service Status**

A list of all components available on the selected application computer appears in the working area.

5) Mark checkbox **Syslog Audit Component** in the component list.
   - The Syslog Audit Component has been stopped, continue with step 7.
   - Otherwise, continue with step 6.
6) Click **Start / Stop** to stop the component.
7) Click **Edit**.

   A window that displays the component's settings opens.
8) Enter the IP address of the desired Syslog server in the **SyslogHost** field.
9) In the active field enter the true value.
10) Click **Save**.
11) Make sure that the **Syslog Audit Component** component is still selected.
12) Click **Start / Stop**.

    The Syslog Audit Component component is started with the new settings.

5.3 Configuration Files

The configuration files contain the settings that define which diagnostics data is to be recorded. These configuration files are xml files and can be customized as needed by using any editor.

Functional Sequence

To customize the configuration files, they can be downloaded from the system, edited locally, and then uploaded to the system again. Multiple configuration files can be loaded on a node, but only one configuration file can be active at any given time.

A default configuration file is provided by the system for every node. Even the default configuration file can be customized with an editor and uploaded back to the node. In addition, the node can also be reset back to the default configuration file.

The following tasks can be performed for a node:

- **Node Info**

  Shows information about selected node.
- **File Info**

  Shows information about configuration file.
- **Start / Stop C.O. (Cyclic Overwriting)**

  Starts or stops the overwriting of log files.
- **Start / StopTrace**

  Starts or stops the online tracing of the selected nodes.
- **Upload to Node**

  Choose a configuration file and upload the file to the selected node.
- **Start new Log File**

  All activities logged from this point are stored in the new log file. For the selected nodes the content of the old log file is stored in a backup log file.
- **Activate default configuration**

  If errors occur in other configuration files you can reset the configuration to the default settings.

System Specific Information

The following detailed information is displayed:

- **Node**

  Name of the node
- **Node Type**

  Type of the node
- **Active file**

  Name of the configuration file on which the node is active.
- **Provider Name**

  Provider name
- **Version**

  Version of the diagnose configuration
- **Description**

  Configuration file description
- **Trace**

  Indicator that shows if an online trace has been started.
- **C.O**

  Shows whether the Round Robin process is activated for the logging

Most common used symphonia loggers and examples

- **log4j_backup_restore.xml** – Logger to be used to troubleshoot backup/ restore issues of Data or Filesystem. Example: Backup of UC data, fails to complete.
- **log4j_bcom.xml** – Logger to be used to troubleshoot call process issues. Example: OWC user A calls OWC user B, but cannot answer the call via call control.
- **log4j_bcom-integrated.xml** - same as above, but to be used in integrated simplex deployments.
- **log4j_bcom-ms.xml** – Logger to be used to troubleshoot call issues and media server issues (If UC media server is on the same server as the BE).
- **log4j_bcom-ms-integrated.xml** – same as above, but to be used in integrated simplex deployments.
- **log4j_cmp_administration.xml** – Logger to be used to troubleshoot CMP related issues. Example: When trying to login to CMP, you get an error that the system is not ready for login or user doesn’t have permission to log in.
- **log4j_conferencing.xml** – Logger to be used to troubleshoot conference issues. User A creates a conference via OWC, adds B and C, but when the conference starts, only user B is alerted.
- **log4j_contactservice.xml** – Logger to troubleshoot contact service related issues (global address book, ldap. Example: When I search for a contact in the address book, I get a timeout.
- **log4j_domain.xml** – Logger to be used to troubleshoot devices assigned to UC users. Example: UC user A has +1234 number assigned via CMP, but in OWC that device is not visible.
- **log4j_dsa.xml** – Logger that troubleshoots assistant related issues. Example: When I try to create a user via CMP, OSV assistant, I get an exception and the user isn’t created.

- **log4j_groupwareservice_contacts_full.xml** – Logger to troubleshoot groupware (Exchange) and contact service related issues. Example: I cannot see in the webclient my private groupware contacts nor search for them.
- **log4j_licensemanagement.xml** – Logger to troubleshoot licensing related issues. Example: I assigned a new UC licensing file for UC users, but the licenses are not activated.
- **log4j_mediaserver_full_log.xml** – Logger to troubleshoot mediaserver issues. Example: After a 1 hour conference, some participants loose speech path
- **log4j_openbranch_administration.xml** – Logger to troubleshoot OSB assistant related issues.Example: In CMP->OSB, I cannot list my OSBs.
- **log4j_openscape_sbc_administration.xml** - Logger to troubleshoot OSB assistant related issues. Example: In CMP->OSB, I cannot list my SBCs
- **log4j_presence.xml** - Logger to troubleshoot presence related issues (im, user presence, media presence). Example: My presence status turns without any action to unavailable
- **log4j_pwf_bcom.xml** - Logger to troubleshoot preffered devices and call process. Example: I have set a device list with 3 devices and I receive a call, the first 2 devices ring, but the third doesn’t
- **log4j_remotelogging.xml** – Logger to be used, to troubleshoot, symphonia logs transfer via sftp to Trace Manager. Example: symphonia logs are not delivered to TM
- **log4j_rules_pwf.xml** – Logger to be used, to troubleshoot cases when setting rules which change prefer devices via UC client. Example: When applying a rule, in which when my presence status is available the call should go to my mobile, the office phone rings.
- **log4j_usermanagement.xml** – Logger to be used, to troubleshoot UM related issues. Example: When trying to provision users via UM, the IM address field is empty

5.3.1 How to Display Configuration Files

How to display configuration files:

Prerequisites

Adequate administrative permissions

Step by Step

1) Click on the tab **Maintenance** > **Monitoring**.

2) Navigate to **Tools&Utilities** > **Configuration Files** in the navigation tree.

   A list of all nodes appears in the work area. This list contains for each entry the detailed information.

   - **Node**

     Name of the node
   - **Node Type**

     Type of the node
   - **Active file**

     Name of the configuration file on which the node is active.
   - **Provider Name**

     Provider name
   - **Version**

     Version of the diagnose configuration
   - **Description**

     Configuration file description
   - **Trace**

     Indicator that shows if an online trace has been started.
   - **C.O**

     Shows whether the Round Robin process is activated for the logging

3) The active configuration file of a node is to be find in the list entry **Active File**.
4) To display all available configuration files of a node click on the name of the desired node.

   A dialog opens, which displays all available configuration files of the node.
5) Click **Close**.

5.3.2 How to Display Metadata of a Configuration File

How to display the configuration files:

Prerequisites

Adequate administrative permissions

Step by Step

1) Click on the tab **Maintenance** > **Monitoring**.
2) Navigate to **Tools&Utilities** > **Configuration Files** in the navigation tree.

   A list of all nodes appears in the work area.
3) Click the name of the node the configuration file of which holds the metadata you want to display.

   Configuration Files window opens, which displays all available configuration files of the node.

4) Click the name of the configuration file for which you want to display the metadata.

   The **Configuration File** dialog opens, which displays all available metadata of the configuration file.

5.3.3 How to Modify Logging Cycle (Appender Configuration)

For the log files each node uses a file system with several files by default. These files are filled with diagnostics data by the Round-Robin procedure.For each appender of a configuration file the following log files are used by default: One current log file and ten backup log files. Each of these files may amount up to 10MB by default

Prerequisites

Adequate administrative permissions

Step by Step

1) Click on the tab **Maintenance** > **Monitoring**.
2) Navigate to **Tools&Utilities** > **Configuration Files** in the navigation tree.

   A list of all nodes appears in the work area.
3) Click the name of the node for which you want to change the settings of the Round-Robin procedure.

   A dialog opens, which displays all available configuration files of the node.
4) Click the name of the configuration file for which you want to change the settings of the Round-Robin procedure.

   A dialog opens, which displays all available metadata of the configuration file.
5) Switch to the **Log File Information** tab.
6) Click the name of the appender for which you want to change the settings of the Round-Robin procedure.

   Appender Configuration window opens, which shows the settings of the Round-Robin procedure.
7) Customize the settings.
8) Click **Save**.

   The entered settings are from now on used for logging.

5.3.4 How to Start / Stop Cyclic Overwriting

If required, the Round-Robin procedure can be temporarily interrupted for logging. This enables the storage of diagnostics data in a single log file for a longer, consecutive period. If the Round-Robin procedure is restarted at a later date, it continues the data storage where it was interrupted.

Prerequisites

Adequate administrative permissions

Step by Step

1) Click on the tab **Maintenance** > **Monitoring**.
2) Navigate to **Tools&Utilities** > **Configuration Files** in the navigation tree.

   A list of all nodes appears in the work area.
3) Select the checkboxes of the nodes for which you want to start a new log file.
4) Click **Start / Stop C.O.**.

IMPORTANT:

The Round-Robin procedure should only be interrupted for a short period. The resulting log file my otherwise become unintentionally large. This may lead to resource problems on the computer system of the relevant node.

-
- If the Round-Robin procedure is **interrupted**:

  From this point on the diagnostics data of the relevant node is not stored in the log file with the backup log files but in a single file.
- If the Round-Robin procedure is **restarted**:

  From this point on the diagnostics data of the relevant node is stored again in the log file and the backup log files

5.3.5 How to Start / Stop an Online Trace

How to start/stop the online trace:

Prerequisites

Adequate administrative permissions

Step by Step

1) Click on the tab **Maintenance** > **Monitoring**.
2) Navigate to **Tools&Utilities** > **Configuration Files** in the navigation tree.

   A list of all nodes appears in the work area.
3) Select the checkboxes of the nodes for which you want to start the online trace.
4) Click **Start / Stop Trace**.
   The online trace is subsequently started / stopped.
5) Invoke the external diagnostics tool to receive the diagnostics data.

5.3.6 How to Activate a Loaded Configuration File

How to activate a configuration file:

Prerequisites

Adequate administrative permissions

Step by Step

1) Click on the tab **Maintenance** > **Monitoring**.
2) Navigate to **Tools&Utilities** > **Configuration Files** in the navigation tree.

   A list of all nodes appears in the work area.
3) Click on the name of the desired node.

   A dialog opens, which displays all available configuration files of the node.
4) Select the checkbox of the configuration file that you want to activate for the node.

   NOTICE: Only one configuration file can be activated
5) Click **Activate**

   The dialog with the additional activation information opens.
6) Enter your **User Data** and the **Reason** on the **General** tab.
7) Click **Activate**.

   The new configuration file is activated. If a configuration file was activated earlier, it will be deactivated automatically.
8) Click **Close**.

5.3.7 How to Upload and Activate a Configuration File

How to upload a configuration file to the node and then activate it:

Prerequisites

Adequate administrative permissions

Step by Step

1) Click on the tab **Maintenance** > **Monitoring**.
2) Navigate to **Tools&Utilities** > **Configuration Files** in the navigation tree.

   A list of all nodes appears in the work area.
3) Select the checkbox of the node to which you want to upload the configuration file.
4) Click **Upload to Node**.

   The file selection window opens.
5) Click **Browse**. Select the file which you want to upload to the node.
6) Click **Load**.to upload the configuration file

   The dialog with the additional activation information opens.
7) Enter **User Data** and the **Reason** on the **General** tab.
8) Click **Activate**.

   The new configuration file is activated. If a configuration file was activated earlier, it will be deactivated automatically.
9) Click **Close**.

5.3.8 How to Backup Configuration Files

How to export configuration files of a node:

Prerequisites

Adequate administrative permissions

Step by Step

1) Click on the tab **Maintenance** > **Monitoring**.
2) Navigate to **Tools&Utilities** > **Configuration Files** in the navigation tree.

   A list of all nodes appears in the work area.
3) Click on the name of the desired node.

   A dialog opens, which displays all available configuration files of the node.
4) Select the checkboxes of the configuration files that you want to export.
5) Click **Download to Client PC**.

   The configuration files are loaded to the client PC as Zip file.
6) Open or save the file as usual.
7) Click **Close**.

5.3.9 How to Delete a Configuration File

How to delete configuration files of a node:

Prerequisites

Adequate administrative permissions

Step by Step

1) Click on the tab **Maintenance** > **Monitoring**.
2) Navigate to **Tools&Utilities** > **Configuration Files** in the navigation tree.

   A list of all nodes appears in the work area.
3) Click on the name of the desired node.

   A dialog opens, which displays all available configuration files of the node.
4) Select the checkboxes of the configuration files that you want to delete.
5) Click **Delete**.
6) Click **OK** to confirm the deletion of the selected configuration files.

   The selected configuration files will be deleted.
7) Click **Close**.

5.3.10 How to Restore the Default Configuration

How to reactivate the default configuration file on a node:

Prerequisites

Adequate administrative permissions

Step by Step

1) Click on the tab **Maintenance** > **Monitoring**.
2) Navigate to **Tools&Utilities** > **Configuration Files** in the navigation tree.

   The **Configuration Files** list view opens, displaying the list of configured nodes, each with its active configuration file for Logging and Tracing.
3) Check the node´s checkbox to select the node for which you want to restore the default configuration.
4) Click **Activate default configuration**

   The default configuration file for Logging and Tracing is restored and activated for the selected node.

5.4 Diagnostics Data

Internal system processes are logged for the entire system in the background and saved as diagnostics data. The configuration files activated on a node determine which specific diagnostics data is recorded.

Functional Sequence

The diagnostics data for each node is recorded individually in log files (*.xml). The diagnostics data for all nodes can be downloaded in the form of a compressed diagnostics file. You can optionally download all saved diagnostics data or selected information (diagnostics components). The diagnostics components offered for downloading depends on the node and the installed applications.

It is also possible to initiate logging with a new diagnostics file to provide better transparency when troubleshooting errors, for example. The data will then be written to a new diagnostics file from that point onward.

5.4.1 How to Export Diagnostics Data

How to export diagnostics data

Prerequisites

Adequate administrative permissions

Step by Step

1) Click on the tab **Maintenance** > **Monitoring**.
2) Navigate to **Tools&Utilities** > **Diagnostics Data Download** in the navigation tree.

   The window **Export diagnostics data** opens.
3) Select the checkboxes of the components that diagnostics data you want to export.
4) Click **Export**.
5) A Zip file is loaded to the client PC, which you can view and/or save as usual.

   The Zip file contains two ZIP files. One contains configuration data, the other contains framework or OpenScape logging data.

6) Click **Close**.

5.4.2 How to Start a new Log File

How to save the log in a new log file:

Prerequisites

Adequate administrative permissions

Step by Step

1) Click on the tab **Maintenance** > **Monitoring**.

2) Navigate to **Tools&Utilities** > **Configuration Files** in the navigation tree.

A list of all nodes appears in the work area.

3) Check the node´s checkbox to select the nodes for which you want to start a new log file.

4) Click on **Start new log file**

For the selected nodes the content of the log file is stored in a backup log file.The diagnostics data logged from this point is stored in the emptied log file.

5.5 Online Trace

An online trace can be used to output the diagnostics data of all nodes to an external diagnostics tool.

Functional Sequence

A network port is reserved for transmitting diagnostics data via an online trace.If this port is already being used by another application, then the port for transmitting diagnostics data must be changed. Subsequently, the port in the diagnostics tool must also be modified to the same value

System Specific Information

Since the transmission of the diagnostics data does not occur via a secure protocol, no security mechanisms such as authentication or encryption are possible. If the diagnostics data is to be transmitted over unsecured networks, it is necessary to also use IPSec for this purpose.

5.5.1 How to Download Trace Files

How to Download Trace Files:

Prerequisites

Adequate administrative permissions

Step by Step

1) Click on the tab **Maintenance** > **Monitoring**.

2) Navigate to **Tools&Utilities** > **Trace File** in the navigation tree.

   The **Generate and Download Trace Files** window opens.

3) Click **Start**.
   The generation of trace file for download is started.

4) Click **Download**.
   The online trace is subsequently downloaded. Trace files can also be found in folder `/enterprise/trace` or `/opt/siemens/trace` for onboard or external assistant, respectively.

5) Click **Close**.

5.5.2 How to Change the Port for an Online Trace

How to change the port for an online trace:

Prerequisites

Adequate administrative permissions

Step by Step

1) On the **Maintenance** navigation tab click on the **Inventory** navigation menu item.

2) In the navigation tree click **System Status** > **Nodes**.

   A list of all system nodes and external links available in the entire system is displayed in the work area.

3) Click the system node name on which OpenScape UC Application is installed.

   A dashboard of the selected node opens.

4) Click **Show** next to **Actions** - **Show services status**.
   A dialog box opens with a list of all components that are available for the selected system node.

5) Look in the list for the **Online Trace** component and select the associated checkbox.

6) Stop the online trace if running: Click **Start / Stop**.

   The **Online Trace** is stopped.

7) Click **Edit**.

   The dialog with the settings of the Online Trace component opens.

8) Enter the port number that is to be used for the online trace in the **portNr.** field.

9) Click **Save**.

   The dialog with the settings of the **Online Trace** component opens.

10) Verify that in the components list the checkbox for the **Online Trace** component is still selected.

11) Click **Start / Stop**.

    The Online Trace is started with the new settings.

12) Change in the external diagnostics tool the communication port used to the same value.

5.6 SNMP Notifications

In the Common Management Platform you can configure SNMP protocol in order to monitor the various systems health connected with CMP.

The administrator is able to setup v3 security parameters for the USM security model like user, engineid, authentication passphrase and encryption passprase for incoming traps from other systems and outgoing traps/informs.

It is possible to see both snmp v3 and v2 traps as alarms to the system. It is also possible to send authenticated and encrypted informs to external systems.

Receiver which consists of SNMP V3 Users and Security configuration is responsible for rap reception.

Sender which consists of Alarm Destinations and SNMP V3 Configuration sends traps to third party components.

5.6.1 SNMP V3 Users

SNMP V3 Users configuration is required for SNMP V3 protocol in order for a system to be able to receive notifications.

5.6.1.1 How to Add an SNMP V3 User

How to add an SNMP V3 User:

Prerequisites

Adequate administrative permissions

Step by Step

1) Navigate to **Maintenance** > **Monitoring** > **SNMP Notifications** > **Receiver** > **V3 Users**.

   The **SNMP V3 Users** window opens with the list of all SNMP V3 users in the selected domain.
2) Click **Add**.

   The dialog **Add SNMP V3 Users** with SNMP V3 Users settings opens for adding a new SNMP V3 User.
3) Enter the Description of the new SNMP V3 User into the field **Description**.
4) Enter the Engine id of the new SNMP V3 User into the field **Engine id**.
5) Enter the User name of the new SNMP V3 User into the field **User**.
6) Select the **Authentication Type** from the drop-down menu.
7) Enter the Authentication Passphrase of the Authentication Type into the field **Authentication Passphrase**.

   NOTICE:

   The length of the Authentication Passphrase should be at least 8 characters.

   ---
8) Select the **Encryption Type** from the drop-down menu.

9) Enter the Encryption Passphrase of the Encryption Type into the field **Encryption Passphrase**.

NOTICE:

The length of the Encryption Passphrase should be at least 8 characters.

---

10) Click **Save**.

The new SNMP V3 User is saved and displayed in the SNMP V3 Users list.

5.6.1.2 How to View and Edit an SNMP V3 User

How to view and edit an SNMP V3 User:

Prerequisites

Adequate administrative permissions

Step by Step

1) Navigate to **Maintenance** > **Monitoring** > **SNMP Notifications** > **Receiver** > **V3 Users**.

   The **SNMP V3 Users** window opens with the list of all SNMP V3 users in the selected domain.

2) Mark the checkbox of the desired alarm destination and click **Edit** or click on the action menu arrow and choose the **Edit** option

   The following information is shown:

   - **Description**
   - **Engine id**
   - **User**
   - **Authentication Type**
   - **Authentication Passphrase**
   - **Encryption Type**
   - **Encryption Passphrase**

3) Apply changes if wanted.
4) Click **Save**.

5.6.1.3 How to Delete SNMP V3 Users

How to delete SNMP V3 Users:

Prerequisites

Adequate administrative permissions

Step by Step

1) Navigate to **Maintenance** > **Monitoring** > **SNMP Notifications** > **Receiver** > **V3 Users**.

   The **SNMP V3 Users** window opens with the list of all SNMP V3 users in the selected domain.
2) Select the checkboxes of the SNMP V3 users you want to delete and click on the **Delete** button or if you want to delete just one SNMP V3 user click on its action menu arrow and choose the **Delete** option.

5.6.2 How to Configure SNMP Security

How to configure SNMP Security:

Prerequisites

Adequate administrative permissions

Step by Step

1) Navigate to **Maintenance** > **Monitoring** > **SNMP Notifications** > **Receiver** > **Security**.

   The **Security** dialog window opens.
2) Navigate to Disable/Enable receiving SNMP V2 notifications section and check or uncheck the **Disable SNMP V2** checkbox in order to enable or disable the SNMP V2 notifications.
3) Navigate to Configure SNMP V3 Security Level section and select from the **SNMP V3 Security Level** drop down list one of the available security levels.
4) Click **Save**.

5.6.3 Alarm Destination

Framework alarms raised in the system are sent to alarm destinations. These alarm destinations can be displayed in an alarm destination list. An alarm destination consists of an IP address and a Layer-3 port.

For SNMP traps, the alarm destination is the IP address or the host name of an external fault management system and the default value for the port is 162. Every SNMP Trap is sent to the global list of alarm destinations.

5.6.3.1 How to Add an Alarm Destination

How to add an Alarm Destination:

Prerequisites

Adequate administrative permissions

Step by Step

1) Navigate to **Maintenance** > **Monitoring** > **SNMP Notifications** > **Sender** > **Destinations**.

   The **Alarm Destinations (external Fault Management System)** window opens with the list of all alarm destinations in the selected domain.

2) Click **Add**.

   The dialog **Alarm Destination** with the alarm destination settings opens for adding a new alarm destination.

3) Enter the IP address of the new alarm destination into the field **IP address**.

4) Enter the port into the field **Port**.

   The port will be used for the SNMP (Simple Network Management Protocol) communication with the alarm destination. The default port is 162.

5) Enter the communication string into the field **Community String**.

   The SNMP community name will be sent to the alarm destination with SNMP traps.

6) Select the SNMP **Version**.

7) Select the **Security Level** from the drop down list.

   NOTICE: Security level drop down list will be enabled only when V3 is selected.

8) Click **Save**.

The new alarm destination is saved and displayed in the alarm destination list.

5.6.3.2 How to View and Edit an Alarm Destination

How to view and edit an Alarm Destination:

Prerequisites

Adequate administrative permissions

Step by Step

1) Navigate to **Maintenance** > **Monitoring** > **SNMP Notifications** > **Sender** > **Destinations**.

   The **Alarm Destinations (external Fault Management System)** window opens with the list of all alarm destinations in the selected domain.

2) Mark the checkbox of the desired alarm destination and click **Edit** or click on the action menu arrow and choose the **Edit** option

   The following information is shown:

   - **IP address/Hostname**
   - **Port**: Layer-3 port used for the SNMP communication with the alarm destination. The SNMP default is 162.
   - **Community String**: The SNMP community name sent to the alarm destination with SNMP traps. User groups and thus privileges are assigned to this SNMP community name in the SNMP system.
   - **Version**: The SNMP Version.
   - **Security Level**: .

3) Apply changes if wanted.
4) Click **Save**.

5.6.3.3 How to Clear Alarm Destinations

How to clear Alarm Destinations:

Prerequisites

Adequate administrative permissions

Step by Step

1) Navigate to **Maintenance** > **Monitoring** > **SNMP Notifications** > **Sender** > **Destinations**.

   The **Alarm Destinations (external Fault Management System)** window opens with the list of all alarm destinations in the selected domain.
2) Select the checkboxes of the alarm destinations you want to delete and click on the **Delete** button or if you want to delete just one alarm destination click on its action menu arrow and choose the **Delete** option.

5.6.4 How to Configure SNMP V3 Settings

How to configure SNMP V3 settings:

Prerequisites

Adequate administrative permissions

Step by Step

1) Navigate to **Maintenance** > **Monitoring** > **SNMP Notifications** > **Sender** > **V3 Configuration**.

   The **SNMP V3 settings** dialog window opens.

2) Enter the Engine id of the new SNMP V3 Agent into the field **Engine id**.

NOTICE:

For the Engine id value, the following HEX types are supported: 00FAC8D31B (plain HEX), 00:FA:C8:D3:1B (MAC-address style HEX), 0xFAC8D31B (C-style HEX).

3) Enter the User name of the new SNMP V3 Agent into the field **User**.

4) Enter the Authentication Passphrase into the field **Authentication Passphrase**.

NOTICE:

The length of the Authentication Passphrase should be at least 8 characters.

NOTICE:

The Authentication algorithm is SHA.

5) Enter the Encryption Passphrase into the field **Encryption Passphrase**.

NOTICE:

The length of the Encryption Passphrase should be at least 8 characters.

NOTICE:

The Encryption algorithm is AES.

6) Click **Save**.

6 Alarms

This chapter provides information about the following topics:

- Framework Alarms
- Alarms for OpenScape assistant
- Alarms for OpenScape Xpressions

Framework Alarms

ID	Alarm title	Alarm description	Priority
100211	“Default Alarm”	This alarm is generated because the appropriate alarm definition could not be found in the database or the alarm definition table in the database is empty.	2
100212	“Default Rule Executed”	The default rule is executed because no other rule was responsible for this fault.	2
100213	“Default Rule Executed”	The default rule is executed because there is no fault specification for the incoming fault available.	2
100214	“Default Rule Executed”	The default rule is executed because there are no rules in the database.	4
100301	Connector: communication problem!	a Message, Failure or Exception could not be sent	3
100302	Connector: configuration problem!	a configuration problem for the performance counter found.	3
100303	Connector: overload!	an overload situation in the connector occured.	3
101001	“Start Service”	A configuration exception occured while setting attributes	0
101002	“Start Service”	Failed to get guid: for subItems of container	0
101003	“Start Service”	Failed to get configuration for guid	0
102001	“Discovery: Could not be initialized!”	IP address of the host not properly configured.	5
102002	“Discovery: CS could not be started!”	Cannot start JCS replicated TreeCache - check the JCS properties and your network configuration.	5

ID	Alarm title	Alarm description	Priority
103001	“License Management: No directory for license files”	The Licenses are based on license files. Those license files are activated in a running system but also deployed during installation time. To be able to access those licenses a specific folder is monitored by the license management system. If this folder does not exist the license management will try to create that folder. In case of occurrence of this alarm it was not possible to create or access that folder. To fix this error check the access rights of the folder and the parent folder and the available disk space. The location of the folder "license" is depending on the specific installation.	4
103002	“License Management: Database access failure”	The access to the database failed for unknown reason. Please check if the database engine is running. If not start the database engine else restart the system.	4
103003	“License Management: Time limited licenses”	This alarm occurs when a time limited license is about to expire or already is expired. Please refer to the fault specification which issue is valid for this alarm. It is highly recommended that you activate a new license file covering a new time limitation or a license file that is not time limited at all. If you do not intend to use the license any more you can ignore this alarm.	2
103004	“License Management: Database inconsistency detected”	The license management detected an inconsistency in the license database. The consistency was recovered by relying on the original license files in the database. Please verify with the management platform that the expected licenses for the system are still available.	4

ID	Alarm title	Alarm description	Priority
103005	“License Management: Rehost of license key required”	License files are bound to the hardware the license is bought for. You also need to add a second prefix access code so that the user can transfer the conference device by dialing “*” (with just the extension) and transfer the conference call to another extension. In that case the license files are no longer valid. You have to create new license files and must activate them on this machine. SysUpTime: :: RtpEvtCurrId: RtpEvtSet: RtpEvtNum: RtpEvtReportingObject: RtpNm01 RtpEvtFaultyObject: RtpNm01 RtpEvtEndkey: noRecoveryDefined RtpEvtAlarmType: DEFAULT0 RtpEvtShortText: Process RtpAdmCli01 is fully functional. For re-hosting you have to log on the Central License Server (CLS). On CLS you invoke the re-host process. More information about re-hosting is available in the CLS online help (or the web based training). Re-host requires a valid login for the CLS. If you do not have a valid login for the CLS refer to the CLS homepage and contact the CLS help desk (-> https://www.central-license-server.com).	2
104001	“Start Service”	Could not start service, as could not be added	0
104002	“Start Service”	Starting instance error	0
104003	“Start Service”	Could not start service, as could not be installed	0
104004	“Start Service”	Could not start service, as bundle for component could not be identified	0
104005	“Stop Service”	Stopping instance error	0
104006	“Stop Service”	Could not stop service, as bundle for component could not be identified	0
104007	“Request Termination”	Could not terminate the start thread in the limited time	0
104008	“Init”	Property not set. Cannot use default	0

ID	Alarm title	Alarm description	Priority
105001	“License Management: Parsing error”	The license key can not be parsed. Mainly this alarm occurs when you tried to activate a non license key. No damage is done to the system since the file was simply ignored. However if you copied the file to the license import folder you should remove it from there to avoid later confusion. If you are convinced that the license file you want to use really is a license file, please consider that those files must be handled as binary information. You must not alter the content of that file. If you transfer a license file across different operating systems please ensure that the file transfer is binary and no replacement of any characters is done. Do not open the license file in an editor and save it to another location in order to transfer a license file. The original license key is still available on the Central License Server (CLS). If you have a license authorization code (LAC) you can use the online license activation of the common management platform to recover the already generated license file(s). In	2
105003	“License Management: Software integrity problem”	The system was not able to load an important internal component. Please reinstall the software.	5
106001	“Alarm Trap Sending Error”	The snmp-service could not sent an alarm record as an snmp-trap to the configured trap destinations. If the problem occurs further on please restart the database and the system.	4
106002	“Trap Destination Reading Error”	The snmp-service could not read the configured trap destinations from the symAlarmDestinations-database. If the problem occurs further on please restart the database and the system.	4
108001	“Could not instantiate SyMOM.”	Could not instantiate SyMoM component.	5
108002	“The symom configuration file does not exist.”	The symom configuration file does not exist.	5
108003	“Symomcomponent message.”	Unable to register SyMoM component.	5

ID	Alarm title	Alarm description	Priority
108004	“Cannot unregister SyMoM component.”	Cannot unregister SyMoM component e.g. because Registration is not running.	5
108005	“There is not exactly one instance of SyMoM.”	There is not exactly one instance of SyMoM.	4
108006	“Could not locate any instances of SyMoM.”	Could not locate any instance of SyMoM.	4
109001	“MBean creation”	Deamon MBean could not be created	0
109002	“MBean registration”	Daemon MBean could not be registered	0
109003	“Mbean deregistration”	Could not unregister Mbeans	0
109004	“MBean creation”	Node MBean could not be created	0
109005	“MBean registration”	Node MBean could not be registered	0
109006	“Configuration data”	Get node config data failed	0
109007	“Configuration data”	Get node instance config data failed	0
109008	“Configuration data”	Set node instance config data failed	0
109009	“MBean creation”	Application MBean could not be created	0
109010	“MBean registration”	Application MBean could not be registered	0
110001	“failure to start syslog audit”	An exception is thrown during start the syslogauditcomponent. The audit via syslog may not works if this alarm occurs. The syslog port may blocked by an other application. You can check this with netstat at the command line. If the syslog port is not longer blocket you can try to restart the syslogauditcomponent. Get the diagnostic data from the framework and send the data to the service.	4

ID	Alarm title	Alarm description	Priority
111001	“crypto failure”	An exception is thrown inside the logfileauditcomponent during create the encryption part. Audit data inside the log file may not crypted. Get the diagnostic data from the framework and send the data to the service.	4
113001	“ServiceDiscovery: wrong Configuration!”	missing or wrong configuration	4
201001	“Database failure”	Unable to close Hibernate session factory from the database	3
202001	“Database failure”	Unable to close Hibernate SessionFactory from database. If the problem occurs further on please restart the database and the system.	3
203001	“Failed to open verifier key store for authentication.”	Failed to open verifier key store for authentication.	5
203002	“Unable to get the authentication statement, but the message checksum is set.”	Unable to get the authentication statement, but the message checksum is set.	4
203003	“Message Checksum for authentication is present, but no subject key available.”	Message Checksum for authentication is present, but no subject key available.	4
203004	“Wrong type of message during authentication processing.”	This received message during authentication verification is not of the expected type. This is an internal programming error.	4
203005	“An incoming JMS message was not handled by the pipeline of port.”	An incoming JMS message was not handled by the pipeline of port. This is an internal programming error.	4
203006	“Unexpected exception in the processing of an received JMS Message.”	Unexpected exception in the processing of an received JMS Message. This is an internal programming error.	4

ID	Alarm title	Alarm description	Priority
203007	“Incoming message could not be processed, because no MessageHandler is registered on the ReceiveChannel of Port.”	Incoming message could not be processed, because no MessageHandler is registered on the ReceiveChannel of Port. This is an internal programming error.	5
203008	“Invalid URI specified in symom.config.file property of the symom.properties file.”	Invalid URI specified in symom.config.file property of the symom.properties file.	5
203009	“Could not read the URL property file.”	Could not read the URL property file. Currently only the symom.properties file is read here. So it seems that the file is present but not readable.	5
203010	“Invalid URI is processed.”	Invalid URI is processed.	5
203011	“Too many faults of a certain fault id will cause a loss of further faults with this id. This might be caused by a DoS.”	Too many faults of a certain fault id will cause a loss of further faults with this id. This might be caused by a DoS.	4
204001	“Execution of a service method exceeded the specified timeout (default 60 sec).”	Execution of a service method exceeded the specified timeout (default 60 sec).	3
204002	“The CommandPool for executing Service methods has exceeded the absolute maximum.”	The CommandPool for executing Service methods has exceeded the absolute maximum (default 200).	5

ID	Alarm title	Alarm description	Priority
204003	“The execution supervision for service method failed and will be switched off.”	The execution supervision for service methods failed and will be switched off.	3
205001	“audit encryption failure”	Error during encrypt audit data. Get the diagnostic data from the framework and send the data to the service.	2
205002	“audit decryption failure”	Error during decrypt an AuditRecord. This error may occur if an audit log file is attacked and modified. Please get the audit log files (symphonia_audit.log.xml.*) and framework log files (symphonia.log.xml.*) and send these files to the service / development for diagnostic purpose.	4
205003	“audit publishing failure”	An exception occurs during publishing an AuditRecord. Audit data may be not logged to the audit log file or other audit destinations like syslog. The responsible component may be not available. Get the diagnostic data from the framework and send the data to the service.	4
205004	“missing AuditReceiver”	There is No auditReceiver subscribed to the audit system.The audit system can not publish the audit information. Audit components may be not active or removed from the container. Get the diagnostic data from the framework and send the data to the service.	4
205005	“Invalid AuditRecord”	A failure occurs during publishing an AuditRecord. An AuditRecord is null. This is not allowed and is a possible coding failure. Get the diagnostic data from the framework and send the data to the service.	2
205006	“Invalid AuditReceiver during subscribe”	An invalid AuditReceiver try to subscribe with null. This is not allowed and is a possible coding failure. Get the diagnostic data from the framework and send the data to the service.	2
205007	“Invalid AuditReceiver during unsubscribe”	An invalid AuditReceiver try to unsubscribe with null. This is not allowed and is a possible coding failure. Get the diagnostic data from the framework and send the data to the service.	2

ID	Alarm title	Alarm description	Priority
205008	“remove AuditReceiver failed”	An exception occured during remove an AuditReceiver. This indicates a possible coding failure. Get the diagnostic data from the framework and send the data to the service.	2
205009	“audit command null”	Try to create an AuditRecord with a CommandName=null. An AuditRecord must contain a command unlike null. This failure indicates an incorrect use of the audit system by other services. Get the diagnostic data from the framework and send the data to the service.	2
205010	“audit scope null”	Try to create an AuditRecord with a Scope=null. An AuditRecord must contain a scope unlike null. This failure indicates an incorrect use of the audit system by other services. Get the diagnostic data from the framework and send the data to the service.	2
205011	“audit user null”	Try to create an AuditRecord with a User=null. An AuditRecord must contain a user unlike null. This failure indicates an incorrect use of the audit system by other services. Get the diagnostic data from the framework and send the data to the service.	2
205012	“invalid audit user”	Try to create an AuditRecord with an invalid User. An AuditRecord must contain a user which achieve the pattern user@domain. This failure indicates an incorrect use of the audit system by other services. Get the diagnostic data from the framework and send the data to the service.	2
205013	“AuditRecord null”	Try to audit an AuditRecord, which is null. An AuditRecord must contain useful audit data and should not be null. This failure indicates an incorrect use of the audit system by other services. Get the diagnostic data from the framework and send the data to the service.	2
205100	“generic test alarm”	This alarm should only used for internal test of the audit library and should not occur at real live systems	0
206001	ClientProxy: communication problem!	a Message, Failure or Exception could not be sent.	4

ID	Alarm title	Alarm description	Priority
206002	ClientProxy: service target problem	problem to reach the service target of a Message, Failure or Exception.	4
206003	ClientProxy: configuration problem!	wrong or missing Configuration.	4
206004	ClientProxy: external problem!	wrong usage of clientproxy.	3
300001	“AlarmHistory Database Initialization Error”	It is not possible to initialize the Alarm History Database. If the problem occurs further on please restart the database and the system.	4
300002	“AlarmHistoryHandler Configuration Read Error”	It is not possible to read from the AlarmHistoryHandler instance file. Please restart the system and if the problem occurs further on a reinstallation is necessary.	4
300003	“Alarm Database Initilization Error”	It is not possible to initialize the Alarm Database. If the problem occurs further on please restart the database and the system.	4
300004	“AlarmHandler Configuration Read Error”	It is not possible to read from the AlarmHistoryHandler instance file. Please restart the system and if the problem occurs further on a reinstallation is necessary.	4
300005	“Invalid FaultHandler-Delegate Error”	It is not possible to access the FaultHandler Delegate. If the problem occurs further on please restart the system.	4
300006	“Alarm Event Processing Error”	Errors occured during database handling. If the problem occurs further on please restart the database and the system.	4
300007	“AlarmHistory Database Handling Error”	Reading or writing the alarm history database is not possible. If the error occurs further on please restart the database and the system.	4
300008	“AlarmHistoryHandler Removing Alarm from AlarmHistory Error”	An error occured during removing an alarm history entry from the alarm history database. If the error occurs further on please restart the database and the system.	3

ID	Alarm title	Alarm description	Priority
300009	“Alarm Database Handling Error”	An error occured during reading or writing the alarm database. If the error occurs further on please restart the database and the system.	4
300010	“AlarmHandler Error”	An error occured during alarm database handling. If the error occurs further on please restart the database and the system.	4
300011	“Configuration Database Error”	An error occured during configuration, reading or writing the configuration database. If the error occurs further on please restart the database and the system.	4
300012	“Event channel Initialisation Error”	An error occured during the initialisation of the AlarmHandlerEventChannel. If the error occurs further on please restart the system.	4
300013	“Error reading EventChannel Configuration”	It is not possible to read from the AlarmHandlerEventChannel instance file or no configuration property is set in the instance file. Please restart the system and if the problem occurs further on a reinstallation is necessary.	4
300014	“AlarmHandler Scheduler Error”	An error occured during setting up a scheduled task using the Scheduler Service. If the error occurs further on please restart the system.	4
300015	“Overload LCS Alarm”	An overload-alarm is generated because the number of incoming alarms exceeds the configured number for low condition.	4
301001	“authentication authority Service cannot run”	Failed to open some config files.	5
302001	“Backup set creation failed”	Failed to create a backup set.	3
302002	“Backup set restoration failed”	Failed to restore a backup set.	3
302003	“Scheduled Export failed”	Failed to generate scheduled export.	3
305001	“domain database access error”	DataAccessException: An error occured when trying to access the domain database.	5

ID	Alarm title	Alarm description	Priority
305002	“domain database validation error”	InvalidStateException: A validation error occured.	2
305003	“domain hibernate database validation error (findUser, updateUser)”	InvalidStateException: A validation error occured, when findUserByID was called with too long parameter.	2
305004	“domain database inconsistency”	Database Inconsistency	4
305005	“domain hibernate initialization error”	Initialization Failure: Failed to initialize Hibernate	5
305006	“domain policy engine initialization error”	Initialization Failure: Failed to initialize the Policy Engine	5
306001	“EventBroker: GENERAL_FAILURE”	General Failure.	2
306003	“EventBroker: MISSING_PLUGIN_ERROR”	EventBroker: A client tries to subscribe for an event for that no plugin is available. Check if all plugins are running (in System View)!	4
306004	“EventBroker: INVALID_SESSION_ID_ERROR”	Many Client requests with Ivalid Session IDs. Might be a session guessing attack.	2
307001	“Alarm Destinations Read Error”	The Alarm destinations could not be read from Database. Check the correct configuration of the trap destinations. If the problem occurs further on please restart the database and the system.	4
307002	“Alarm Destinations Write Error”	The Alarm destinations could not be written into the database. Check the correct configuration of the trap destinations. If the problem occurs further on please restart the database and the system.	4
307003	“Fault Record Read Error”	The Fault Records could not be read from Database. If the problem occurs further on please restart the database and the system.	4

ID	Alarm title	Alarm description	Priority
307004	“Alarm Read Error”	The Alarm Records could not be read from Database. If the problem occurs further on please restart the database and the system.	4
307005	“Alarm not in Database”	The Alarm is not available in the Alarm Database.	3
307006	“Doubled Sourcetypes”	There is a doubled sourceType definition while reading the faultspecifications. Please contact the development.	2
307007	“Service not found error”	The alarmreceiver-service could not be contacted. Please contact the development.	4
307008	“Scheduler setup failure”	Error setting-up the schedule in Scheduler for the faultHandler service. If the problem occurs further on please restart the system.	4
307009	“Deletion Failure of faults”	Deletion of all FaultRecords older than the given timestamp failed. It is not possible to access the database. If the problem occurs further on please restart the database and the system.	4
307010	“Reading configuration failure”	Reading of the FaultHandler configuration failed. Please restart the system and if the problem occurs further on a new installation is necessary.	4
308001	“License Management: Internal software error”	An internal software error occurred while accessing the database. Please restart the system. If the error still remains please reinstall the database.	4

ID	Alarm title	Alarm description	Priority
309001	“License Management: License file parsing error”	The license key can not be parsed. Mainly this alarm occurs when you tried to activate a non license key. No damage is done to the system since the file was simply ignored. However if you copied the file to the license import folder you should remove it from there to avoid later confusion. If you are convinced that the license file you want to use really is a license file, please consider that those files must be handled as binary information. You must not alter the content of that file. If you transfer a license file across different operating systems please ensure that the file transfer is binary and no replacement of any characters is done. Do not open the license file in an editor and save it to another location in order to transfer a license file. The original license key is still available on the Central License Server (CLS). If you have a license authorization code (LAC) you can use the online license activation of the common management platform to recover the already generated license file(s). In	2
309003	“License Management: internal leak of resources”	If this error occurs more often please restart the system.	2
309004	“License Management: Service processing error”	During the service invocation an unspecified error occured. if the problem occurs more often please restart the system.	3
309005	License Management: Required licenses missing	There is at least one profile assigned to at least one user, which requires licenses which are not installed at the system	2

ID	Alarm title	Alarm description	Priority
309006	“License Management: License file invalid”	The license key can not be parsed. Mainly this alarm occurs when you tried to activate a non license key. No damage is done to the system since the file was simply ignored. However if you copied the file to the license import folder you should remove it from there to avoid later confusion. If you are convinced that the license file you want to use really is a license file, please consider that those files must be handled as binary information. You must not alter the content of that file. If you transfer a license file across different operating systems please ensure that the file transfer is binary and no replacement of any characters is done. Do not open the license file in an editor and save it to another location in order to transfer a license file. The original license key is still available on the Central License Server (CLS). If you have a license authorization code (LAC) you can use the online license activation of the common management platform to recover the already generated license file(s). In	2
309007	“License Management: internal software error”	If the latest version of the software is installed please escalate this error.	5
309010	“License Management: Adding license file not allowed”	The provided license file can not be added to the database since the file (or a newer file) already exists or the provided license file is not accepted (e.g. invalid). Please ensure you have the most current version of the license file you want to add.	4

ID	Alarm title	Alarm description	Priority
309011	“License Management: Invalid Locking ID”	A license file cannot be activated because the locking ID of the license file does not fit to the locking ID of the system. License files are bound to the hardware the license is bought for. You also need to add a second prefix access code so that the user can transfer the conference device by dialing “*” (with just the extension) and transfer the conference call to another extension. In that case the license files are no longer valid. You have to create new license files and must activate them on this machine. SysUpTime: :: RtpEvtCurrId: RtpEvtSet: RtpEvtNum: RtpEvtReportingObject: RtpNm01 RtpEvtFaultyObject: RtpNm01 RtpEvtEndkey: noRecoveryDefined RtpEvtAlarmType: DEFAULT0 RtpEvtShortText: Process RtpAdmCli01 is fully functional. For re-hosting you have to log on the Central License Server (CLS). On CLS you invoke the re-host process. More information about re-hosting is available in the CLS online help (or the web based training). Re-host requires a valid login for the CLS. If you do not have a valid login for the CLS refer to the CLS homepage and contact the CLS help desk (-> https://www.central-license-server.com).	2
309012	“License Management: Mapping file parsing error”	The system was not able to load an important internal component. Please reinstall the software.	2
310001	“LoggingConfigManager faild to load logging-log4j.xsd”	The file logging-log4j.xsd is missed inside the framework configuration folder. The configuration is corrupted. The reload of diagnostic configurations may fail. Please reinstall the missed schema file.	2
310002	“LoggingConfigManager faild to load logging-rules.xsd”	The file logging-rules.xsd is missed inside the framework configuration folder. The configuration is corrupted. The reload of diagnostic configurations may fail. Please reinstall the missed schema file.	2
310003	“LoggingConfigManager logging-log4j.xsd is invalid”	SAXException during parse the file logging-log4j.xsd. The configuration is corrupted. The reload of diagnostic configurations may fail. The file logging-log4j.xsd is invalid. Please reinstall the original logging-log4j.xsd file.	2

ID	Alarm title	Alarm description	Priority
310004	“LoggingConfigManager: logging-rules.xsd is invalid”	SAXException during parse the file logging-rules.xsd. The configuration is corrupted. The reload of diagnostic configurations may fail. The file logging-rules.xsd is invalid. Please reinstall the original logging-rules.xsd file.	2
310005	“LoggingConfigManager: logging-log4j.xsd not loaded”	Cannot load a logging confguration because the schema file logging-log4j.xsd is not loaded. Check if the file is available inside the framework configuration folder.	2
310006	“LoggingConfigManager: logging-rules.xsd not loaded”	Cannot load a logging confguration because the schema file logging-rules.xsd is not loaded. Check if the file is available inside the framework configuration folder.	2
310007	“LoggingConfigManager: logging configuration parse error”	This alarm occurs if a new diagnostic configuration (may be a log4.xml file) should load and the parsing of the xml file failed. Please get the diagnostic data from the framework, attach the diagnostic configuration which is invalid and send the data to the development.	2
310008	“LoggingConfigManager: Bundle start failed”	The Logging features are organized as bundles, though activating a feature orders the LifecycleManagement to start a bundle. This command failed. The technician should download the tracefiles symphonia*.log.xml and send the files to the support.	2
310009	“LoggingConfigManager: Bundle stop failed”	The Logging features are organized as bundles, though activating a feature orders the LifecycleManagement to start a bundle. This command failed. The technician should download the tracefiles symphonia*.log.xml and send the files to the support.	0
310010	“LoggingConfigManager: Load file failed”	Unable to load a logging configuration File. Maybe the file system is wrong or needed files are deleted at the filesystem. The technician should download the tracefiles symphonia*.log.xml and send the files to the support. Call ls -lisa inside the framework configuration directory and attach the output to the bug report.	2

ID	Alarm title	Alarm description	Priority
310011	“LoggingConfigManager: Missing Information in Configuration”	The current configuration is invalid due to missing data for a feature. This error occurs, if a feature shall be accessed (e.g. start / stop online trace) that are not configured in the configuration file. The technician should download the tracefiles symphonia*.log.xml and send the files to the support. Please collect also the file loggermanager.xml from the framework configuration folder and attach this file to the bug report.	2
310012	“LoggingConfigManager: missing privileges”	This alarm is deprecated and should not occur!	2
310013	“LoggingConfigManager: failed to generate a configuration file”	The LoggingConfigManager failed to create a diagnostic configuration files. Maybe the file access privileges inside the framework configuration folder are not ok. Please call at the command ls -lisaR inside the framework configuration folder and get the diagnostic data from the framework. Send the diagnostic data and the output from the ls command to the service.	2
310014	“LoggingConfigManager: failed to validate diagnostic configuration”	The LoggingConfigManager failed to validate a diagnostic configuration. This alarm occurs if you try to activate a new diagnostic configuration (e.g. a log4.xml file) and the configuration file is invalid. Please check the diagnostic configuration file.	2
310015	“LoggingConfigManager: exception during validate diagnostic configuration”	The LoggingConfigManager failed to validate a diagnostic configuration. This alarm occurs if you try to activate a new diagnostic configuration (e.g. a log4.xml file) and the configuration file is invalid. Please check the diagnostic configuration file.	2
310016	“LoggingConfigManager: wrong file name during upload”	The administrator try to upload a new logging configuration. The filename for the diagnostic configuration was wrong.	2
310017	“LoggingConfigManager: overwrite default logging configuration files is not allowed”	The administrator try to upload a default diagnostic configuration. It is not allowed to overwrite the default configuration.	2

ID	Alarm title	Alarm description	Priority
310018	“LoggingConfigManager no xml file”	The administrator try to upload a diagnostic configuration file, but the filename ends not with the extension .xml. This is not allowed.	2
310019	“LoggingConfigManager file write failed”	The administrator try to upload a new diagnostic configuration. An IO error occurs during writing the file to the folder diagnostic_configurations. Check the privileges of these folder.	2
310020	“LoggingConfigManager predefined logging configuration file does not exists”	The administrator try to modify a predefined diagnostic configuration, but the selected files does not exists. Check content of the folder diagnostic_configurations which is placed inside the framework configuration folder. For further diagnosis you need the framework log files and the framework configuration files	2
310021	“LoggingConfigManager predefined logging configuration file is write protected”	The administrator try to modify a predefined diagnostic configuration, but the selected files is write protected. Check file rights of the file inside the folder diagnostic_configurations which is placed inside the framework configuration folder. This error may occur, if you modify the files inside the folder diagnostic_configurations with tools like WinSCP instead of the management platform. For further diagnosis you need the framework log files and the framework configuration files	2
310022	“LoggingConfigManager error during modify a logging configuration”	The administrator try to modify a predefined diagnostic configuration, but an unexpected exception occurs. For further diagnosis you need the framework log files and the framework configuration files	2
310023	LoggingConfigManager error during parsing a logging configuration	The administrator tried to upload a new logging configuration, but an unexpected exception occurs.For further diagnosis you need the framework log files	2
310024	LoggingConfigManager No configuration data found in log file.	Unable to load a logging configuration. The file appears to have no configuration data. This error occurs if no configAppender with the name: 'SYMPHONIA_CONFIGURATION' is found in the logging configuration file.	2

ID	Alarm title	Alarm description	Priority
310025	LoggingConfigManager: Cyclic Overwrite feature is disabled.	The cyclic overwrite feature in Symphonia log files is disabled. Please verify that you have enough disk space and consider moving older symphonia log files to a different system. This warning occurs every two days.	3
310026	LoggingConfigManager: Unable to setup a schedule task with the scheduler service.	The system was unable to add a schedule task that will notify the administrator every two days that the cyclic overwrite feature is disabled. This is not a critical problem.	3
310100	“LoggingConfigManager: generic test alarm”	This alarm should only used for internal test of the logging config manager and should not occur at real live systems	0
311001	“Logon Service cannot run”	Failed to open some config files	5
311002	“Logon Service domain problem”	domain connection failed for logon	4
311003	“Logon Mechanism Failure”	wrong setup of encodings, algorithms ...	4
312001	“Socket failed”	The onlinetrace can not create a socket connection on the configured port, because the port is blocked. This means that the onlinetrace does not work, and you can not view the trace online with chainsaw. The port may be blocked by an other application or by the framework itself. This may be a faulty configuration if two application or services uses the same port. Please check on the commandline with netstat if the port is blocked by an other application. If the port is no longer blocked, you must restart the Online Trace Service or the container.	4
314001	“error 9470”	Database Inconsistency: Duplicate user entry found.	4
314002	“error 9480”	ProvisioningException: An error occured in modify method.	2
314003	“error 9490”	ProvisioningException: An error occured in create method.	2
314004	“error 9500”	ProvisioningException: An error occured in upload method.	2

ID	Alarm title	Alarm description	Priority
315001	“Schedule Execution Failed”	Execution of scheduled task failed, may be caused by invalid schedule task, unavailable database or scheduling service at the moment.	4
315002	“Schedule Storage Failed”	Storage of schedule failed caused by an internal error.	2
316001	“AlarmTrap initialisation failure of SNMP Service”	The snmp-service could not load the archived alarmtraps from the alarmtrap-database. If the problem occurs further on please restart the database and the system.	4
316002	“Node initialisation failure of SNMP Service”	The attempt to read the node-properties especially to get the local node failed. Restart the system and if the problem occurs further on please reinstall the system.	4
316003	“Container initialisation failure of SNMP Service”	The attempt to read the container-properties failed. Restart the system and if the problem occurs further on please reinstall the system.	4
316004	“Application initialisation failure of SNMP Service”	The attempt to read the application-properties failed. Restart the system and if the problem occurs further on please reinstall the system.	4
316005	“Service initialisation failure of SNMP Service”	The attempt to read the service-properties failed. Restart the system and if the problem occurs further on please reinstall the system.	4
316006	“SNMP Session failure of SNMP Service”	The snmp service can not receive or send snmp messages. Check if the port no. 161 is already used from another service or application.	4
317001	“Unexpected exception”	Error while creating a SystemAppManagerException	0
317002	“System manager target ID”	Unable to get a target ID for the system manager service	0
317003	“Application state workflow”	Response failure	0
317004	“Application data workflow”	Request failed	0
317005	“Different applications in merge”	Different applications in merge	0

ID	Alarm title	Alarm description	Priority
317006	“Overall-Node-Interface-Array is null”	Overall-Node-Interface-Array is null	0
317007	“At least one interface has no instance”	At least one interface has no instance	0
317008	“No application/ service found”	No application/service found	0
320001	“System Management Error”	SystemManagement internal error	4
320002	“Configuration Access Error”	Error with Configuration	4
320003	“Restart System Error”	Restart System Error	4
320004	“System Synchronization Error”	Error with Systemconfiguration Synchronization	4
320005	“Node Error”	Node Error	4
320006	“Process Error”	Error with Process	4
320007	“Instance Error”	Error with Instance	3
320008	“Application Error”	Application Error	3
320009	“Import/Export Error”	Import/Export Error	3
321001	Configuration failure	Error while getting configuration data	4
322001	Error setting up snmp client	Error setting up snmp client. Could not register mib file for collecting ssl data	5
322002	Error while retrieving information for snmp node	Could not retrieve identification information for a snmp node. Snmp agent running at external node?	5
322003	Error while retrieving licensing information for snmp node	Could not retrieve licensing information for snmp node. Possible invalid licensing data returned.	5

ID	Alarm title	Alarm description	Priority
322004	License violation detected for ssl node	Subscription license violation detected for a SSL node. Verify licenses at node	5
322005	Software Subscription license Service error	Could not read ssl data from database. Please check database	5
400001	“Link failure to communication system”	The control link to communication system is down.	4
400002	“Monitor reset problem.”	Monitor control to an endpoint cannot be resumed.	4
400003	“DataBase resource error”	Resource is assigned to more than one user.	4
400004	“DataBase office code error”	Office Code is incomplete.	4
400005	“DataBase private code error”	Private Code is incomplete.	4
401001	Database access error	DataAccessException: An error occured when trying to access the contactlist database.	5
401002	Initialization failed	InitializationException: Failed to initialize Hibernate.	5
401003	Authentication statement invaild	The provided authentication statement is invalid.	4
403001	“Failed to access Presence service”	Presence Event Handler Plugin failed to access Presence service	2
403002	“Failed to access Event Channel”	Presence Event Handler Plugin failed to subscribe or unsubscribe event with Event Channel	2
403003	“Failed to access Event Channel”	Presence Event Handler Plugin failed to subscribe or unsubscribe event with Event Channel	2
403004	“Failed to initialize Hibernate”	Presence Service: Failed to initialize Hibernate	2

ID	Alarm title	Alarm description	Priority
403005	“Failed to publish event”	Presence Service: Failed to publish events	2
414001	Service communication error	ServiceReplyException: Sending reply or failure fails	4
414002	DB access error	An error occurs during DB access	4
416001	“Contact Service validation failure”	A client has sent invalid parameters to the Contact Service.	2
416002	“Contact Service general error”	A general failure has occured. May be one of the directory connectors is not working properly. Check the related faults.	2
416003	“Contact Service update of private contact failed”	Contact Service update of private contact from global pendant failed. Check the related faults.	2
416004	“Contact Service authorization failure”	An attempt has been made to write to a public directory without a proper authorization.	2
416005	“Contact Service picture problem”	The size of the given picture file is too big.	5
418001	“Ldap Connector size limit exceeded”	The result recieved exceeds the maxResults limit.	0
418002	Ldap Connector service is unavailable	The configured ldap connection is reachable but does not respond.	3
418003	Ldap Connector result incomplete	The result received does not contain all possible entries.	1
418004	Ldap Connector connection error	The configured ldap connection cannot be reached.	3
418005	Ldap Connector connection interrupted	The configured ldap connection has been interrupted.	3
418006	Ldap Connector configuration error	The configuration provided by the instance file is invalid..	4

ID	Alarm title	Alarm description	Priority
418007	Ldap Connector configuration not written	The configuration could not be written to the insatnce file.	4
418008	Ldap Connector search error	The requested query failed to return any results.	3
418009	“Ldap Connector password coding error”	The connection password could not be decoded.	4
419101	Remote logging service was unable to transfer a logging file to remote server	Unable to transfer a logging file to remote server	4
419102	Remote logging service was unable to connect to the remote server	Unable to connect to the remote server. Check if server is down or otherwise inaccessible	4
419103	Remote logging service was unable to connect to the remote server	Unable to connect to the remote server because the username or password was incorrect	4
419104	Remote logging service was unable to read the properties file	Unable to read the properties from the properties file. Check if the file exists and if it is readable. Also check the permissions of the folder	3
419105	Remote logging service was unable to read the properties file	Remote logging service was unable to write the properties file. If the file exists check the permissions. Also check folder permissions and disk space	3
600001	“Crossfunctional test for fireFault.”	Test with rules definition.	5
99000001	“Reading configuration failure”	Error while getting configuration data	4
99000002	“Default rule executed”	The default rule is executed because no other rule was responsible for this fault	2

Alarms for OpenScape assistant

ID	Alarm title	Alarm description	Priority
500001	“OpenScape Assistant Not Available”	At least one OpenScape Assistant Service is not available.	5
500002	“OpenScape Assistant Waiting”	OpenScape Assistant is waiting for availability of other services or resources	2

Alarms for OpenScape Xpressions

ID	Alarm title	Alarm description	Priority
501001	“Xpressions Not Available”	At least one OpenScape Assistant Service is not available.	5
501002	“Xpressions Waiting”	OpenScape Assistant is waiting for availability of other services or resources	2

7 Application server certificates

CMP uses SSL/TLS for the authentication and encryption of the communication of the administrator's browser with the Application Server. The CMP application server system needs to be integrated in the security policy of the customer's network. This integration requires a key pair with associated certificate which identifies the application server. The identification is done through the fully qualified host name (FQHN) of the application server which is included in the certificate. If the certificate's name does not match the server's hostname, the web browser will display a warning to the user.

IMPORTANT:

The Certificate Configuration of CMP application server is included/saved only in a *File System* backup and not in a *Data* Backup. Therefore when you restore your *Data* from a Backup you must also go through the process described in this chapter to configure again the certificates. This is not required when you restore your File System.

The following diagrams show the various OpenScape deployment scenarios:

- Integrated Simplex,
- Standard Duplex (small),
- Standard Duplex (large) (one front-end computer)
- Standard Duplex (large) (several front-end computer)

All components that are part of the OpenScape solution are highlighted red. The configuration of the CMP certificates is performed only on the server that hosts CMP.

NOTICE:

CMP now supports:

- TLS v1
- TLS v1.1
- TLS v1.2 connections to the Tomcat Web Server
- TLS v1.2 connections to the Axis SOAP server (port 4709)
- TLS v1.2 connections from the Axis SOAP client (OSV/ Branch/4k/DLS/FM etc)

and the following cipher suite order in all server/client interfaces above:

- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
- TLS_RSA_WITH_AES_128_GCM_SHA256
- TLS_RSA_WITH_AES_256_GCM_SHA384
- TLS_RSA_WITH_AES_128_CBC_SHA
- TLS_RSA_WITH_AES_256_CBC_SHA

The following algorithms are no longer supported (certificates):

- SSLv3
- RC4
- MD5withRSA
- DH keySize < 768

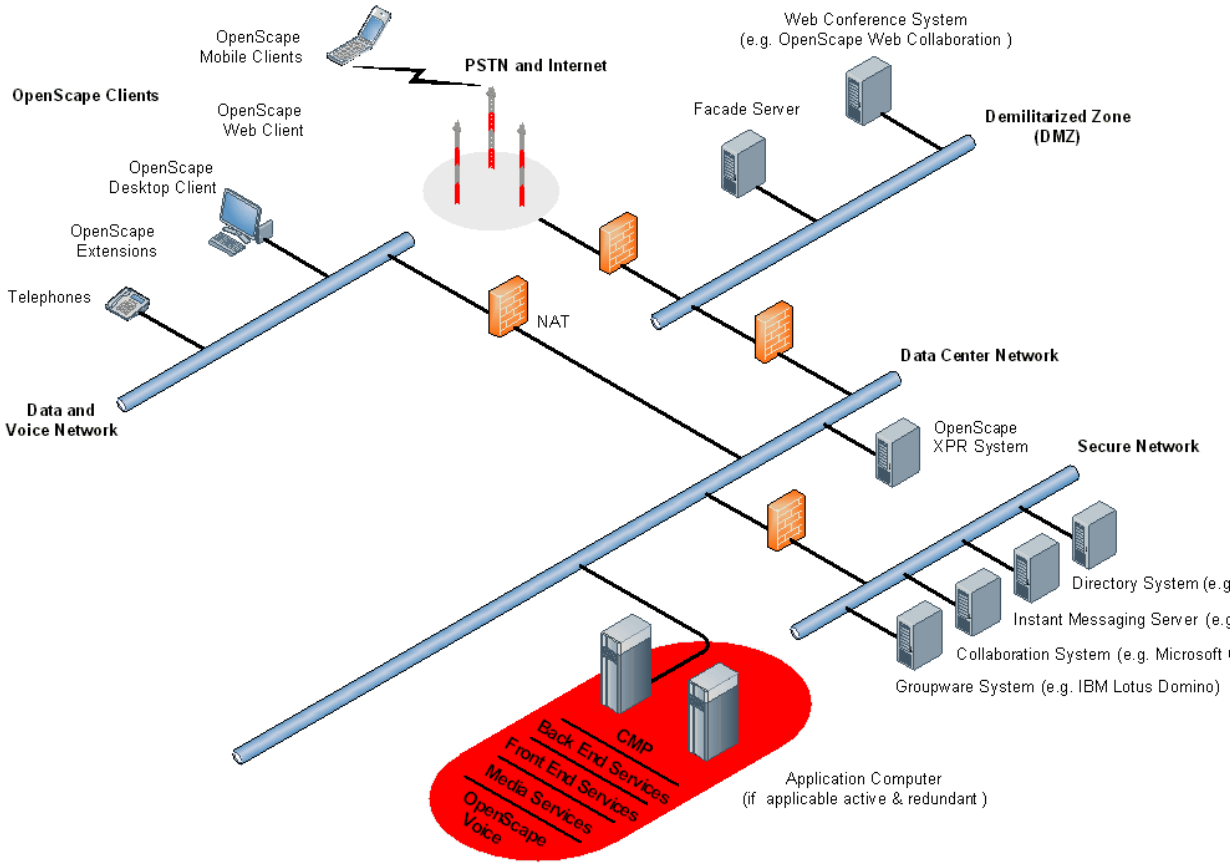


Figure 1: Deployment Scenario Integrated Simplex

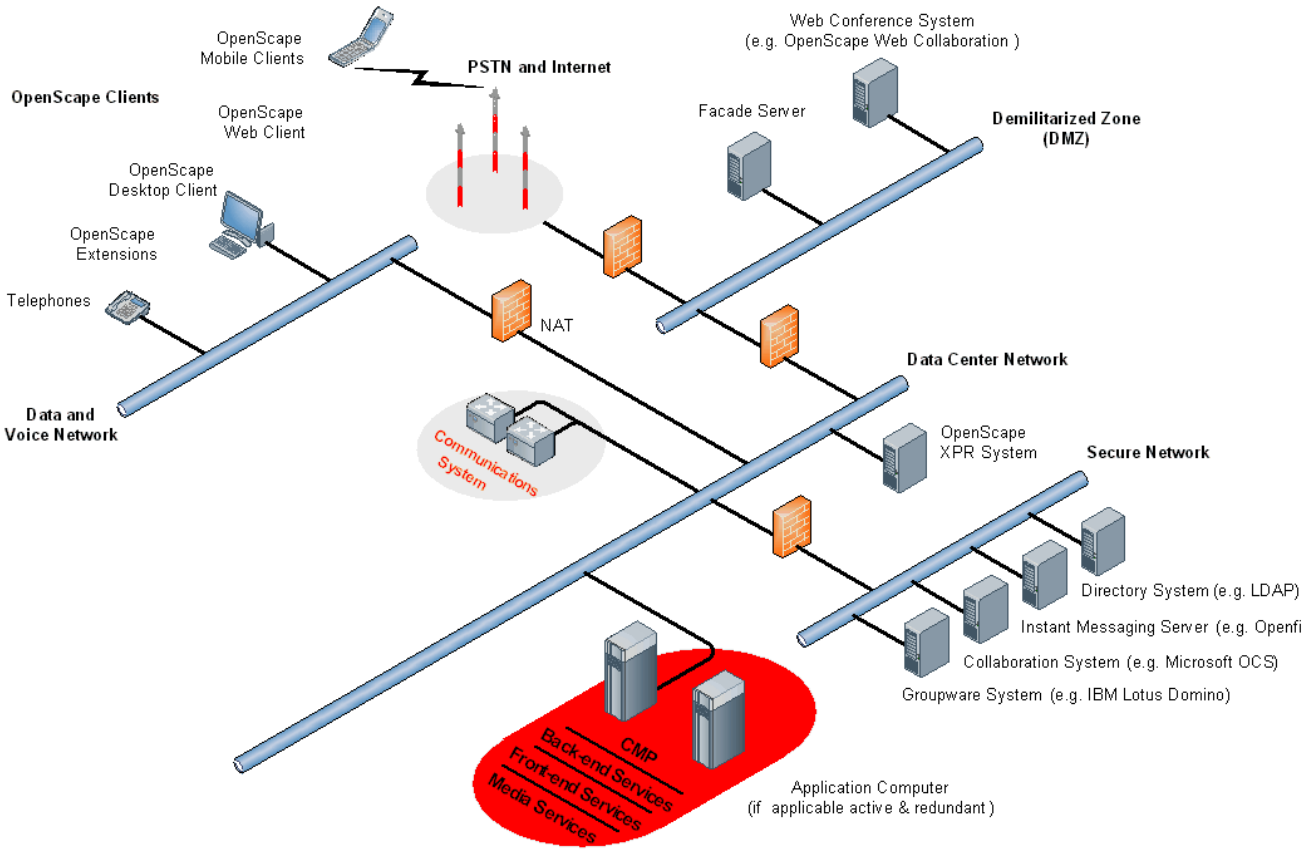


Figure 2: Deployment Scenario Standard Duplex

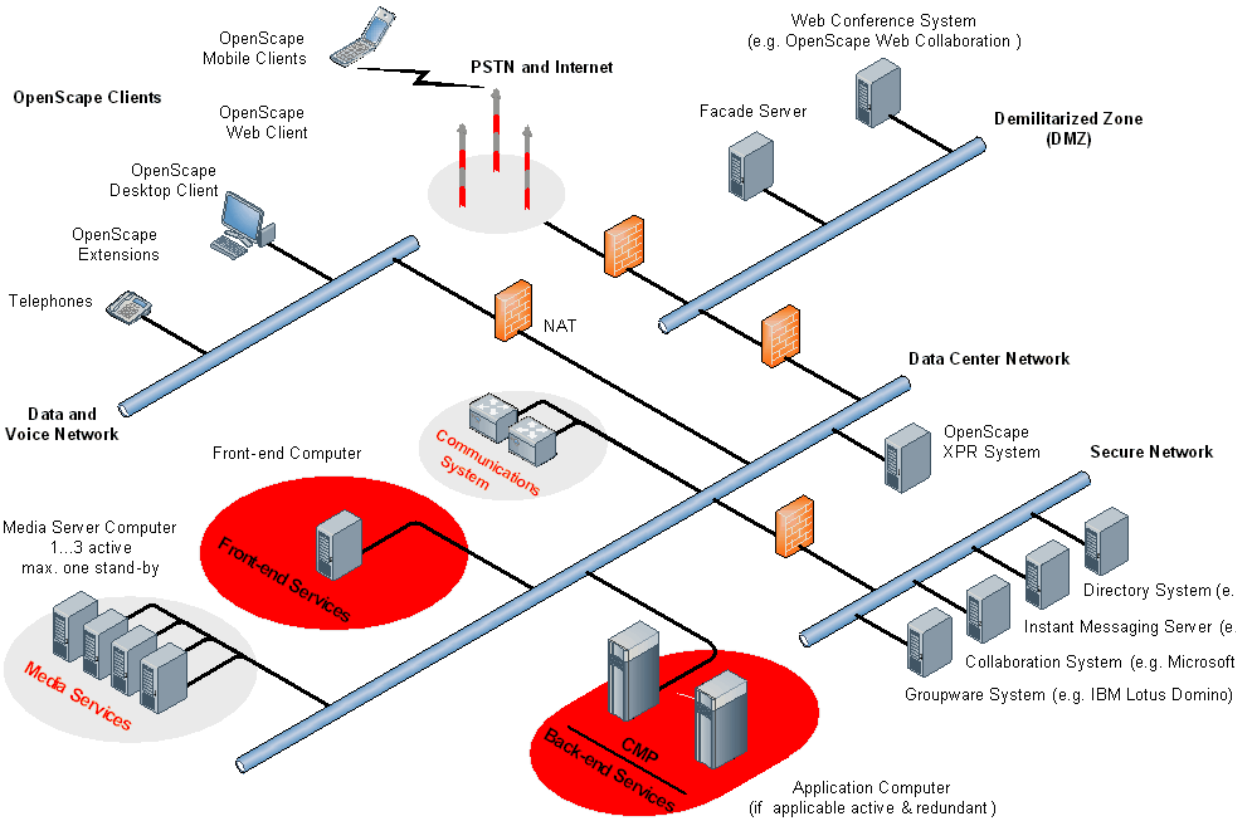


Figure 3: Deployment Scenario Standard Duplex (large) (one front end computer)

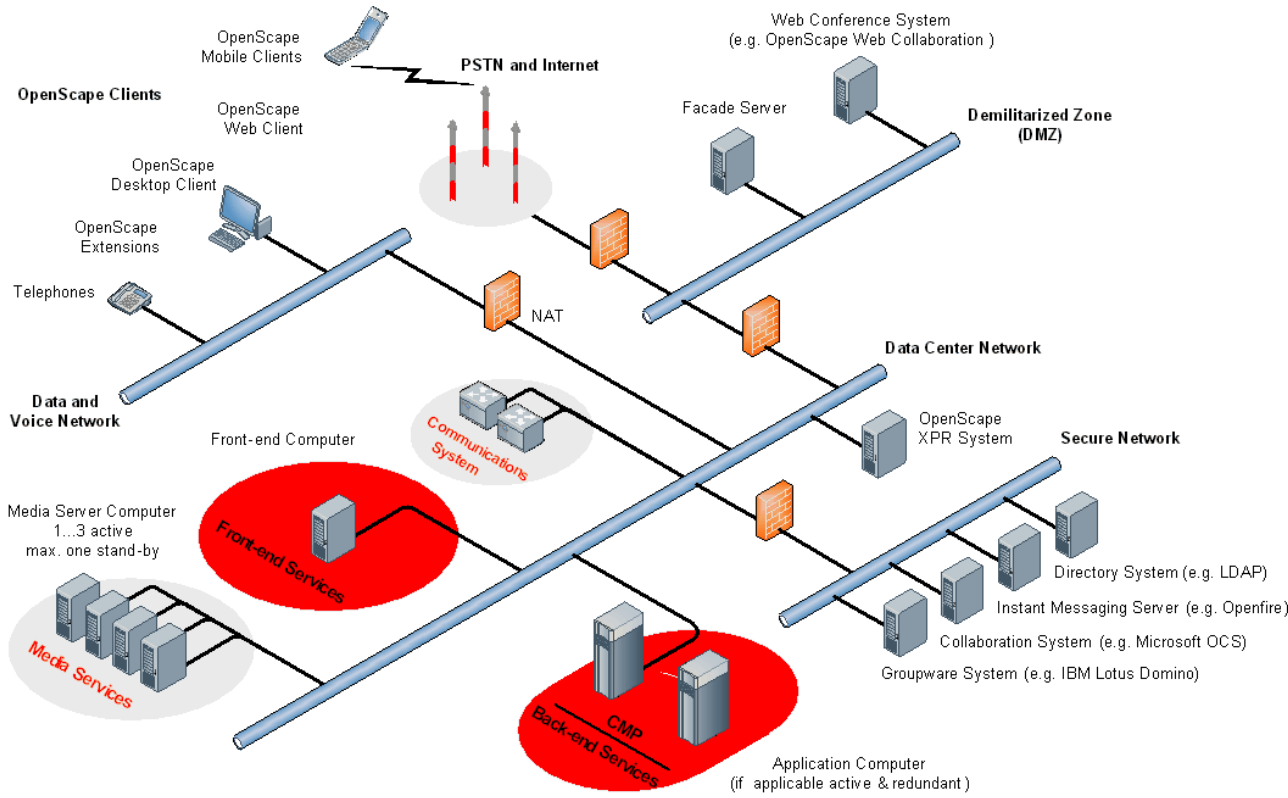


Figure 4: Deployment Scenario Standard Duplex (large) (several front end computers)

7.1 Customer Environments

The integration of the CMP Application Server in the security policy of the customer network depends, among other things, on the customer environment.

In the following sections various customer environments are described and at the required configuration steps are presented

- Customer Environment 1 (ENV 1) – PKI with self-maintained CA
- Customer Environment 2 (ENV 2) – PKI with self-maintained CA and CSR
- Customer Environment 3 (ENV 3) – PKI with a commercial CA
- Customer Environment 4 (ENV 4) –No PKI available

7.1.1 Customer Environment 1 (ENV 1)– PKI with self-maintained CA

The network already supports Public Key Infrastructure (PKI) with a Certificate Authority (CA) that is maintained by the customer. The customer can provide

the required key pairs and associated certificates for the Application Server directly as a PKCS#12 keystore file.

In order for the keystores to be usable for CMP, the following restrictions 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 !$%()*+,-./:;=?@[/]^_`{|}~
- In case the keystore and the private key has been protected with separate passwords, the password for a PKCS#12 keystore file and the password for the private key must be the same
- The password for the PKCS#12 keystore file must be known in order to configure CMP webserver
- The alias name tomcat must have been configured for the CMP application server certificate in the PKCS#12 keystore file

In order for the certificates to be of adequately security, 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 SHA256RSA.

In order for the CMP users' browser to trust the issued Application Server's certificate, the root certificate of the self-maintained CA used must have been imported in the browser's truststore

7.1.2 Customer Environment 2 (ENV 2)– PKI with self-maintained CA and CSR

The network already supports Public Key Infrastructure (PKI) with a Certificate Authority (CA) that is maintained by the customer. Specific certificates for the CMP application server will be issued and need to be signed by the self-maintained CA. In order to perform this, a Certificate Sign Request (CSR) is required

In order for the CMP users' browser to trust the issued Application Server's certificate, the root certificate of the self-maintained CA used must have been imported in the browser's truststore

7.1.3 Customer Environment 3 (ENV 3)– PKI with a commercial CA

The network already supports Public Key Infrastructure (PKI) with a commercial Certificate Authority (CA). Specific certificates for the CMP application server

will be issued and need to be signed by the commercial CA. In order to perform this, a Certificate Sign Request (CSR) is required

In order for the CMP users' browser to trust the issued Application Server's certificate, the root certificate of the commercial CA used must have been imported in the browser's truststore

7.1.4 Customer Environment 4 (ENV 4)– No PKI available

The network does not support Public Key Infrastructure (PKI) but secure access to the CMP Application Server is required.

7.2 Overview of the Configuration Steps

Depending on the customer environment some of the configuration steps presented in the following sections may not be required. The following table displays the configuration steps required in order to enable the SSL/TLS access to the CMP application server depending on the customer environment.

Configuration Step	**Customer environment:**	**ENV1**	**ENV2**	**ENV**
Preparing the Configuration of the Certificate Strategy				
Determining the Setup Directory of CMP		☐	☐	☐
Defining an X.500 Distinguished Name			☐	☐
Creating a new Certificate Authority				
Preparation for the Certificate Authority				
Creating self-signed CA Certificate				
Creating the CMP Application Server Certificates			☐	☐
Preparation for the Application Server Certificates			☐	☐
Creating a key pair for the Application Computer			☐	☐
Creating a Certificate Sign Request for the Application Server			☐	☐
Signing a Certificate Sign Request			☐	☐
Creating a PKSCS#12 keystore			☐	☐
Activating the CMP Application Server keystores		☐	☐	☐
Activating the application server keystore for CMP Tomcat Web Server		☐	☐	☐
Obfuscating the keystore password in the CMP Tomcat's server.xml		☐	☐	☐
Activating the application server certificates for CMP Apache Web server		☐	☐	☐

Configuration Step		Customer environment:	ENV1	ENV
Importing the Root Certificate in the Client Browsers				
	Inspecting the Root Certificate			
	Validating the root certificate			
	Installing the root certificate			

Example

A graphic representation shows you in every configuration chapter for which of these customer environments you need to execute the relevant configuration steps.

Execute these steps for:	ENV1		ENV3	

You need to execute the configuration steps of the respective configuration chapter for customer environments 1 and 3 only.

Some of the configuration steps may require the additional information that can be found in the Section “Additional Instructions”

Chapters of this section are the following:

- Creating a secure Password
- Combining multiple certificate files in a certificate chain
- Converting a certificate chain from DER format to PEM format
- Converting a certificate chain from PKCS#12 format into PEM format

7.3 Preparing the Configuration of the Certificate Strategy

You need to execute the following preparatory steps before you can configure the certificate strategy

- Determining the Setup Directory of CMP
- Defining an X.500 Distinguished Name

7.3.1 Determining the Setup Directory of CMP

Execute these steps for:	**ENV1**	**ENV2**	**ENV3**	**ENV4**

To configure a computer system for the certificate strategy you need to know the directory in which CMP was installed on the Application Server

Step by Step

1) Open a shell on the Application Server 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 CMP setup directory.

Example:

```
SYMPHONIA_HOME=/opt/siemens
```

In the following configuration steps we name the CMP Application Server setup directory:

`<SymphoniaHome >`

Document the Application Serversetup directory:

	Application Server
<SymphoniaHome >	

7.3.2 Defining an X.500 Distinguished Name

Execute these steps for:		**ENV2**	**ENV3**	**ENV4**

Each new certificate has a unique name, the Distinguished Name (DN).The distinguished name contains the following mandatory information :

- **CN** – Common Name

  Must match the Fully Qualified Host Name (FQHN) of the computer system for which the certificate and the associated key pair will be issued:

  Example: webserver.domain.com

  In case of a Certificate Authority (CA), CN must define the name of the certificate authority.

  Example: Custom CA
- **OU** – Organization Unit

  Must define the organization unit the computer system belongs to– e. g. a department or division.

  Example: Unit

  Furthermore, the distinguished name contains the following **optional** information:
- **O** – Organization Name

  May define the name the organization the computer system belongs to

  Example: Organization
- **L** – Locality

  May define the geographic location for the computer system– e. g. the name of a city.

  Example: City

- **C** – Country

  May define the two-digit country code for the location of the computer system.

  Example: US
- **ST** – State Name

  May define the name of the location of the computer system.

  Example: State

  NOTICE:

  The existing customer environment uses in most cases already defined information for setting up a distinguished name

Example of a distinguished name in the format accepted by *OpenSSL*:

```
/CN=webserver.domain.com/OU=Unit/O=Organization/L=City/
C=US/ST=State
```

Define a distinguished name for the CMP Application Server.

	CH(FQHN)	OU (Org-Unit)	O(Org-Name)	L(Locality)	C(C
Application server					

In the following configuration steps we generally name a distinguished name:`<DistinguishedName >`

7.4 Creating a new Certificate Authority

Execute these steps for:				**ENV4**

The following steps configure a new certificate authority for the CMP application server. The OpenSSL toolkit is used for this purpose which is pre-installed with the SLES distribution of the Linux operating system.

The certificate authority configured this way should only be used for testing purposes for the following reasons:

- A certificate authority should always be configured and operated on a separate computer system
- The random number generator used in the following should better be pre-set for a certificate authority

The certificate authority is configured in the following steps:

- Preparation for the Certificate Authority
- Creating self-signed CA Certificate

NOTICE:

You find further information about the software OpenSSL under:
http://www.openssl.org/

7.4.1 Preparation for the Certificate Authority

Execute these steps for:				ENV4

The creation of the certificate authority requires a working directory where all the required files will be stored. If it does not exist, it should be created. The working directory that will be used is:

CA working directory:

<SymphoniaHome>/common/conf/ca

In the following configuration steps we name the working directory of the certificate authority as follows:

<CaBaseDir>

	Application server
<CaBaseDir>	

Creating a certificate authority:

Step by Step

1) Open a shell on the application server and log on as root user.
2) Execute the following command to create the new working directory:

   ```
   [ -d <CaBaseDir> ] || mkdir -p <CaBaseDir>
   ```

   e.g.

   ```
   [ -d /opt/siemens/common/conf/ca/CaBaseDir ] || mkdir -
   p /opt/siemens/common/conf/ca/CaBaseDir
   ```

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 create a new file named <CaBaseDir>/openssl.cnf
5) Enter the following text in the new file. Use the 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=sha256
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= <Your Local CA name>
OU=<OU>
O=<O>
L=<L>
C=<C>
ST=<ST>



[ 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
```

NOTICE:

<CaBaseDir> should be the absolute path. For example, /opt/siemens/common/conf/ca/CaBaseDir.

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:

```
[ -d "private" ] || mkdir "private"

[ -d "ca_certs.d" ] || mkdir "ca_certs.d"

[ -f "ca.db.index" ] || touch ca.db.index

[ -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"
```

7.4.2 Creating self-signed CA Certificate

Execute these steps for:				**ENV4**

A self-signed certificate acts as the root certificate of the CA. This self-signed certificate is also used to sign certificate sign requests.

Creating a self-signed certificate for the certificate authority:

Step by Step

1) Create a strong password to use for creating the self-signed certificate. You can use the procedure from Section “Creating a secure Password ”for this purpose:

   In the following configuration steps we name this password <CaKeyPassword>
2) Open a shell on the application server 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 key pair that contains a private and a public key.

```
openssl genrsa
-rand "$HOME/.rnd"
-out private/ca_root.key
-des3 2048
```

System will prompt you to for a pass phrase to protect the generated key.

System will prompt you to verify the pass phrase.

NOTICE:

OpenSSL allows specifying passwords on the command line as well. This is not recommended because the shell saves all issued commands in a plain text file that could end up being read by a malicious user. We suggest that you allow openssl to prompt you for passwords instead

---

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 self-signed certificate for the new key pair.

```
openssl req -config openssl.cnf -x509 -sha256 -days 3652
 -new -key private/ca_root.key -passin '<CaKeyPassword>'
 -out ca_root.pem
```

Enter the desired pass phrase that protects the CA by replacing the **<**`CaKeyPassword`**>**

The new self-signed certificate is stored under the name `ca_root.pem` in the directory `<CaBaseDir>`.The certificate is valid for 10 years (3652 days)

NOTICE:

The maximum permissible validity of a certificate should be adapted according to the security policy of the customer. To do so, adjust the value for the `-days` option accordingly.

---

6) Execute the following command in one line to convert the self-signed certificate in the DER format

```
openssl x509 -outform DER -in ca_root.pem -out
 ca_root.der
```

The new self-signed certificate in DER format is stored under the name `ca_root.der` in the directory `<CaBaseDir>`

7) Execute the following commands to allow only the root user to access the key pair and the self signed 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 self-signed certificate:

```
openssl x509 -in ca_root.pem -text -fingerprint -certopt
 no_sigdump,no_pubkey -noout
```

The output has the following format

```
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            d5:a4:35:f1:af:a5:5b:ee
        Signature Algorithm: md5WithRSAEncryption
        Issuer: CN=Custom CA, OU=Unit, O=Organization, L=City, C=US, ST=State
        Validity
            Not Before: Oct 12 11:18:18 2011 GMT
            Not After : Oct 11 11:18:18 2021 GMT
        Subject: CN=Custom CA, OU=Unit, O=Organization, L=City, C=US, ST=State
        X509v3 extensions:
            X509v3 Basic Constraints: critical
                CA:TRUE
            X509v3 Key Usage:
                Certificate Sign, CRL Sign
            X509v3 Subject Key Identifier:
                B3:74:F9:6C:54:13:7D:6F:99:0C:5F:32:B1:48:CA:11:A2:C1:31:33
            X509v3 Authority Key Identifier:
                keyid:B3:74:F9:6C:54:13:7D:6F:99:0C:5F:32:B1:48:CA:11:A2:C1:31:33
                DirName:/CN=Custom CA/OU=Unit/O=Organization/L=City/C=US/ST=State
                serial:D5:A4:35:F1:AF:A5:5B:EE

SHA1 Fingerprint=78:FE:01:B7:61:20:55:4B:B3:DA:5D:EC:55:D1:1C:9D:92:B4:B7:56
```

7.5 Creating the CMP Application Server Certificates

Execute these steps for:		**ENV2**	**ENV3**	**ENV4**

The following steps configure the certificates of the CMP Application Server. The OpenSSL toolkit is used for this purpose which is pre-installed with the SLES distribution of the Linux operating system

7.5.1 Preparation for the Application Server Certificates

Execute these steps for:		**ENV2**	**ENV3**	**ENV4**

The working directory that will be used for the creation of the application server certificates is:

PKI working directory (If it does not exist, it should be created):

```
<SymphoniaHome>/common/conf/pki
```

In the following configuration steps we name the working directory of the certificate authority as follows:

```
<PKIBaseDir>
```

Document the certificate authority working directory:

	Application server
<PKIBaseDir>	

Preparation for the creation of the application server certificates:

Step by Step

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:

   ```
   [ -d <PKIBaseDir> ] || mkdir -p <PKIBaseDir>
   ```

   e.g.

   ```
   [ -d /opt/siemens/common/conf/pki/PKIBaseDir ] || mkdir
    -p /opt/siemens/common/conf/pki/PKIBaseDir
   ```
3) Execute the following command to grant exclusively the root user all privileges for the new working directory

   ```
   chmod 700 <PKIBaseDir>
   ```
4) Execute the following command to switch to the working directory of the certificate authority.

   ```
   cd <PKIBaseDir>
   ```
5) Execute the following commands to create further directories and files required by the certificate authority:

   ```
   [ -d "private" ] || mkdir "private"
   ```

   ```
   [ -d "cert" ] || mkdir "cert"
   ```
6) Execute the following commands to allow only the root user to access the new directories:

   ```
   chmod 700 "private" "cert"
   ```

7.5.2 Creating a key pair for the Application Computer

Execute these steps for:		ENV2	ENV3	ENV4

You need to create a key pair that will be used to identify the CMP application server:

Creating a key pair for the application server:

Step by Step

1) Open a shell on the application computer on which the certificate authority has been configured and log on as root use
2) Create a strong password to use for creating the self-signed certificate. you can use the procedure from e. g. Section “Creating a secure Password”

   This password is used to protect both the keystore and the private key from unauthorized access.

   In the following configuration steps we name this password:

   `<Key/StorePassword>`
3) Execute the following command:

   ```
   cd <PKIBaseDir>
   ```
4) Execute the following command in one line to create a keystore that contains key pair (private and a public key.):

   ```
   openssl genrsa -out private/server.key -des3 2048
   ```

   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)

   System will prompt you to for a pass phrase to protect the generated key.

   System will prompt you to verify the pass phrase.
5) Execute the following command to allow only the root user to access the server key:

   ```
   chmod 600 "private/server.key"
   ```

The new server key pair is stored as a standalone file in `<PKIBaseDir>/private/server.key`.

7.5.3 Creating a Certificate Sign Request for the Application Server

Execute these steps for:		ENV2	ENV3	ENV4

The key pair of the application server must be signed by a certificate authority in order to verify that this specific key identifies the application server. In order to do this, a Certificate Sign Request (CSR) must be created for the key pair.

Creating a certificate sign request for the key pair of an application server:

Step by Step

1) Open a shell on the application server and log on as root user

2) Execute the following command:

```
cd <PKIBaseDir>
```

3) Execute the following command in one line to create a certificate sign request for the pair of keys of the application computer:[36]

```
openssl req -new -days 3652 -key private/server.key -
subj "<DistinguishedName>" -out server_csr.pem
```

For example:

```
openssl req -new -days 3652 -key private/server.key -
subj "/CN=webserver.domain.com/OU=Unit/O=Organization/
L=City/C=US/ST=State" -out server_csr.pem
```

NOTICE:

The maximum permissible validity of a certificate should be adapted according to the security policy of the customer. To do so, adjust the value for the `-days` option accordingly.

System will prompt you to enter pass phrase that protects the server key; enter the `<Key/StorePassword>`.

The certificate sign request is stored under the name server_csr.pem in the `<PKIBaseDir >` directory.

Execute the following command to display the contents of the certificate sign request.

```
openssl req -in server_csr.pem -text -reqopt
no_sigdump,no_pubkey -noout
```

The output has the following format:

```
Certificate Request: Data: Version: 0 (0x0) Subject:
CN=webserver.domain.com, OU=Unit, O=Organization,
L=City, C=US, ST=State Attributes: a0:00
```

---

[36] Here you define the Distinguished Name for the application computer in use. The CN (Common Name) must match the Fully Qualified Host Name (FQHN) of the computer system for which the certificate and the associated key pair will be issued, e.g. webserver.domain.com

In case of a Certificate Authority (CA), CN must define the name of the Certificate Authority, e.g. Your Local Custom CA name

More info can be found in section "Defining an X.500 Distinguished Name"

The following example shows the entry format for this value:“/CN=webserver.domain.com/OU=Unit/O=Organization/L=City/C=US/ST=State”

7.5.4 Signing a Certificate Sign Request

Execute these steps for:		ENV2	ENV3	ENV4

The application server key pair must be signed by a trusted entity that confirms the identity of the associated computer. To accomplish this, the certificate sign request is signed by a certificate authority. The result of the signing operation is a certificate that contains the following:

- The public key of the computer system
- Information that identifies the computer system
- General information about the certificate itself

You can sign the certificate sign requests in one of the following two ways:

- By a self-maintained or a commercial certificate authority that is used to create certificates for the customer environment. In this case, proceed as described in the documentation of the certificate authority and skip this section.
- By the certificate authority you have created in Section “Creating a new Certificate Authority”. In this case, proceed to the following steps:

Signing a certificate sign request

Step by Step

1) Open a shell on the application server and log on as root user

2) Move the certificate sign request `server_csr.pem` from the directory `<PKIBaseDir> (/opt/siemens/common/conf/pki/PKIBaseDir)` to the working directory of the certificate authority:

```
<CaBaseDir> (/opt/siemens/common/conf/ca/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 `server_csr.pem` of the application server with the root certificate of the certificate authority.

System will prompt you to enter pass phrase that protects the CA key; enter the `<CaKeyPassword>`

```
openssl ca -config openssl.cnf -days 3652 -notext -batch
 -in server_csr.pem -out server.pem
```

The newly created certificate is stored under the name `server.pem` in the working directory `<CaBaseDir>`. It is valid for 10 years (3652 days).

NOTICE:

The maximum permissible validity of a certificate should be adapted according to the security policy of the customer. To do so, adjust the value for the `-days` option accordingly

5) Delete the certificate sign request `server_csr.pem` from the directory `<CaBaseDir>`
6) Move the certificate server.pem from the folder `<CaBaseDir>` to the directory `<PKIBaseDir >/cert`
7) Execute the following command to allow only the root user to access the server certificate:

```
chmod 600 <PKIBaseDir >cert/server.pem
```

The new signed certificate is stored under the name `server.pem` in the directory `<PKIBaseDir>/cert` and is valid for 10 years (3652 days).

8) Execute the following command to display the contents of the self-signed certificate

```
openssl x509 -in <PKIBaseDir >cert/server.pem -text -
fingerprint -certopt no_sigdump,no_pubkey -noout
```

The output has the following format:

```
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number: 3 (0x3)
        Signature Algorithm: md5WithRSAEncryption
        Issuer: CN=Custom CA, OU=Unit, O=Organization, L=City, C=US, ST=State
        Validity
            Not Before: Oct 12 13:48:36 2011 GMT
            Not After : Oct 11 13:48:36 2021 GMT
        Subject: C=US, ST=State, L=City, O=Organization, OU=Unit,
CN=webserver.domain.com
        X509v3 extensions:
            X509v3 Basic Constraints:
                CA:FALSE
            Netscape Comment:
                OpenSSL Generated Certificate
            X509v3 Subject Key Identifier:
                5D:B2:03:FE:13:10:25:AA:B2:CF:4D:55:89:5F:06:86:51:A9:14:32
            X509v3 Authority Key Identifier:
                keyid:B3:74:F9:6C:54:13:7D:6F:99:0C:5F:32:B1:48:CA:11:A2:C1:31:33


SHA1 Fingerprint=E7:8C:E3:30:90:48:4D:FF:B1:BF:F0:4A:D7:4C:45:E7:D2:D7:6F:4B
```

7.5.5 Creating a PKSCS#12 keystore

Execute these steps for:		ENV2	ENV3	ENV4

To enable CMP to use the key pair and signed certificate of the application server they must be stored in a PKCS#12 keystore file.

Creating a PKCS#12 keystore:

Step by Step

1) Open a shell on the application server and log on as root user
2) Execute the following command:

```
cd <CaBaseDir> (/opt/siemens/common/conf/ca/CaBaseDir)
```

Copy the server.pem, server.key to <CaBaseDir> from <PKIBaseDir>

```
cp -p /opt/siemens/common/conf/pki/PKIBaseDir/cert/
server.pem .

cp -p /opt/siemens/common/conf/pki/PKIBaseDir/private/
server.key .
```

3) Execute the following command to import the signed certificate in the keystore that contains the server's private key:.

```
openssl pkcs12 -export -in server.pem -inkey server.key
 -certfile ca_root.pem -name tomcat -out keystore.p12
```

The system will first prompt you to enter pass phrase for the server key. Enter the pass phrase you used in the previous steps in Creating the CMP Application Server Certificates on page 368.

The system will then prompt you for the export password that will protect the keystore. Enter the `<Key/StorePassword>`. The password does not need to be the same as the one used in previous steps.

The system will finally prompt you to verify the export password. Enter the `<Key/StorePassword>` again.

NOTICE:

Further intermediate certificates may be required to ascertain the correctness of the certificate server.pem. In this case, use the file the parameter `-certfile` to provide the PEM file containing the certificate chain of intermediate certificates up to the certificate of the root CA

NOTICE:

How to combine several certificates to a certificate chain is described in Section "Combining multiple certificate files in a certificate chain "

---

4) Execute the following command to allow only the root user to access the server certificate:

   ```
   chmod 600 keystore.p12
   ```

   The new PKCS#12 keystore is stored under the name `keystore.p12` in the directory `<PKIBaseDir> (/opt/siemens/common/conf/ca/CaBaseDir)`

5) Execute the following command to display the contents of the keystore.

   ```
   openssl pkcs12 -in keystore.p12  -nokeys
   ```

   System will prompt you to for the password to display the keystore.p12 - enter the password you used on previous steps (section "Creating the CMP Application Server Certificates").

   The output has the following format:

```
Enter Import Password:
MAC verified OK
Bag Attributes
    friendlyName: tomcat
    localKeyID: E7 8C E3 30 90 48 4D FF B1 BF F0 4A D7 4C 45 E7 D2 D7 6F 4B
subject=/C=US/ST=State/L=City/O=Organization/OU=Unit/CN=webserver.domain.com
issuer=/CN=Custom CA/OU=Unit/O=Organization/L=City/C=US/ST=State
-----BEGIN CERTIFICATE-----
MIIDzTCCArWgAwIBAgIBAzANBgkqhkiG9w0BAQQFADBmMRIwEAYDVQQDEwlDdXN0
b20gQ0ExDTALBgNVBAsTBFVuaXQxFTATBgNVBAoTDE9yZ2FuaXphdGlvbjENMAsG
A1UEBxMEQ210eTELMAkGA1UEBhMCVVMxDjAMBgNVBAgTBVN0YXRlMB4XDTExMTAx
MjEzNDgzNloXDTIxMTAxMTEzNDgzNlowcTELMAkGA1UEBhMCVVMxDjAMBgNVBAgT
BVN0YXRlMQ0wCwYDVQQHEwRDaXR5MRUwEwYDVQQKEwxPcmdhbml6YXRpb24xDTAL
BgNVBAsTBFVuaXQxHTAbBgNVBAMTFHdlYnNlcnZlci5kb21haW4uY29tMIIBIjAN
BgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA3XFuARv09Elz+mRj2MXinDatFwL/
jIBe+GTq1r8qcwDnEPH3itKqUal1+ZkyyBmOv1i/TDd838woKzD4r3MmoKDohbg/
oFLwhOOsHfFhu85uunHkqhx6skn8dbo62bY8pCEtP0YoDFQLhCsQ0BA8rdg+2bQY
k4XaxjoafqqLsQ86R3QqrZ9NGVIM6IeVCUvglYTYXBv79BXTpr9xdyvGgldpVOSg
Z9VzFBwhTEnxdiGzh7bgLx/+HU2zjCqDdNp+rLRGRrezOAZh/yIkrKp0zA63kQtZ
1MwTDOH0zWR7HMlktPvPi9OfaBu8nOPFdlJm98KGwfnLxX3YmaEgAMDPXwIDAQAB
o3sweTAJBgNVHRMEAjAAMCwGCWCGSAGG+EIBDQQfFh1PcGVuU1NMIEdlbmVyYXRl
ZCBDZXJ0aWZpY2F0ZTAdBgNVHQ4EFgQUXbID/hMQJaqyz01ViV8Ghl GpFDIwHwYD
VR0jBBgwFoAUs3T5bFQTfW+ZDF8ysUjKEaLBMTMwDQYJKoZIhvcNAQEEBQADggEB
AJiM2wNwLbCOMeJceQPv6xp4Y4vvMMlDqKdxxMmUnWpwfuDkqABAiA85DmWt5AvB
aYf0RkTFAJB8AHHWnsBgVKX3NBFt4EqTBQuMxtxdfGEcodZ/Dm5DrcIgZU1Y4Z2S
q+1LtrNIGj3mEXrALkte/hpXcxU2LUnuj9//3B36qVCB35ivRjJLMNpT3XpDxUu9
htKqEG7ZDr3mmGeHIOmLRH8r7W+eele+95Y1KtvVNacmfgW7wWKz62fFgXTu3LE+
UiR9fd1IhGovuqBgmbxP934pc84J+aZZLUm7bLIEZ25+ErRh1YQuN9chU8SriZWo
63ROGPs+5t+5tddZCV/7DE4=
-----END CERTIFICATE-----
Bag Attributes: <No Attributes>
subject=/CN=Custom CA/OU=Unit/O=Organization/L=City/C=US/ST=State
issuer=/CN=Custom CA/OU=Unit/O=Organization/L=City/C=US/ST=State
-----BEGIN CERTIFICATE-----
MIIEKzCCAxOgAwIBAgIJANWkNfGvpVvuMA0GCSqGSIb3DQEBBAUAMGYxEjAQBgNV
BAMTCUN1c3RvbSBDQTENMAsGA1UEChMEVW5pdDEVMBMGA1UEChMMT3JnYW5pemF0
aW9uMQ0wCwYDVQQHEwRDaXR5MQswCQYDVQQGEwJVUzEOMAwGA1UECBMFU3RhdGUw
HhcNMTExMDEyMTExODE4WhcNMjExMDExMTExODE4WjBmMRIwEAYDVQQDEwlDdXN0
b20gQ0ExDTALBgNVBAsTBFVuaXQxFTATBgNVBAoTDE9yZ2FuaXphdGlvbjENMAsG
A1UEBxMEQ210eTELMAkGA1UEBhMCVVMxDjAMBgNVBAgTBVN0YXRlMIIBIjANBgkq
hkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAriYsCqnYo7/60qkz66bY80meHTxvaidC
UPWH+fgsglBcRZ+8NZwtNZG/f1Tvhf11GbBRniY56NegNzEYpY01e/m+P1EZopD+
xW9/oi0RfeuqU8evlqc/xOkIBk2VTvbuWvuxTMjADAvXuDhQI3sHft2xA2GbHJ78
2IE7vNa9rfl/DYzptWUIr3V0yn8Jw3y6UHAROOx9kyrGma17kVtaEaOQG+suxML0
/Oxpo3/OxD2CoN+EMrwVz1hQ31F3yW7XOnUHEk6w+Dv5mPwb1PKq1qRkPA3Hgg2R
L6OQtxh6wOdreF2RGtSu0nJ93gT8547DP3E+jhiDO9H+/B2Lj1LdzQIDAQABo4Hb
MIHYMA8GA1UdEwEB/wQFMAMBAf8wCwYDVR0PBAQDAgEGMB0GA1UdDgQWBBSzdPls
VBN9b5kMXzKx3MoRoxExMzCBmAYDVR0jBIGQMIGNgBSzdPlsVBN9b5kMXzKx3MoR
oxExM6FqpGgwZjE8MBAGA1UEAxMJQ3VzdG9tIENBMQ0wCwYDVQQLEwRVbml0MRUw
EwYDVQQKEwxPcmdhbml6YXRpb24xDTALBgNVBAcTBENpdHkxCzAJBgNVBAYTAlVT
MQ4wDAYDVQQIEwVTdGF0ZYIJANWkNfGvpVvuMA0GCSqGSIb3DQEBBAUAA4IBAQCJ
gzsNsx3H/moQdJvZp6hB8MQRHpysIv20sMP77UXw7ZGZoPt5Yu7K/vGtAc/Y133x
3G7ABol5i0aGcQsVaKyjR7giV1SnVRBkrpbNrW/CvLkImnTOjnwJExCL5tDVxjw6
XUdLr+Tz28SuQwdgWlzWRqBc0iOOuKTkA5/szyXNRjNDMQvW/WDhr4ndxW1bhMOF
id3wGfrNKHj0NHbyc9ZIJNjtTOeTiMiNbxoOBMCJriXP9ByOpU8ZeBmlzq4bbcJp
6Ht8UGE5ZZpfDydJP37p2eaGrmIbryjkMyLBaYztPvUgZE+WnIEafyjUjL1lErDr
w61cTmhTAd8Tv2UT1hb3
-----END CERTIFICATE-----
```

7.6 Activating the CMP Application Server keystores

Execute these steps for:	ENV1	ENV2	ENV3	ENV4

The following steps configure the CMP web servers to use the Application Server's keystore. The keystore password that is required to access it may be stored in obfuscated form in the web servers' configuration files for additional security

7.6.1 Activating the application server keystore for CMP Tomcat Web Server

Execute these steps for:	ENV1	ENV2	ENV3	ENV4

When a user accesses the Common Management Platform with a web browser, the web browser validates the CMP web server certificate. This ensures that:

- the web browser authenticates the CMP web server
- data between the browser and the server are transmitted encrypted.

The PKCS#12 keystore containing the certificate and private key of the application server that was either provided by the self-maintained or commercial certificate authority (ENV1/ENV2) or was created by following this guide (ENV3/ ENV4) must be enabled in CMP's Tomcat web server configuration in order to enable the secure access to CMP

NOTICE:

Tomcat uses keys and certificates stored in a keystore.The keystore is protected from unauthorized access by a password. Each key pair stored in a keystore can also be protected from unauthorized access by a key password.

Activating the application server keystore in CMP Tomcat web server

Step by Step

1) Open a shell on the application server and log on as root user

2) Backup the original PKCS#12 tomcat-keystore.p12 file on directory `<SymphoniaHome>/common/conf`

```
cp -p /opt/siemens/common/conf/tomcat-keystore.p12 /opt/
siemens/common/conf/tomcat-keystore.p12_ORIG
```

Copy the PKCS#12 keystore file to the directory <SymphoniaHome>/common/conf under the name tomcat-keystore.p12

NOTICE:

The application server keystore.p12 created by following this guide is stored under `<CaBaseDir> (/opt/siemens/common/conf/ca/CaBaseDir/keystore.p12)`

---

3) Execute the following three (3) commands to set the correct owenership and permissions to the `tomcat-keystore.p12` file:

```
chown sym tomcat-keystore.p12

chgrp sym tomcat-keystore.p12

chmod 644 tomcat-keystore.p12
```

4) Backup the existing server.xml file, apply changes and save the file

```
cd /opt/siemens/share/tomcat/conf

cp -p server.xml server.xml_ORIG
```

Start a text editor (vi) and open the following file

```
<SymphoniaHome>/share/tomcat/conf/server.xml
```

5) Search the file for the section of the connector for which the following settings have been configured:

```
name="CMP_https"port="443"scheme="https"
```

6) Add/modify the following attributes in the CMP connector section

One needs to encode the keystore password used on previous steps (section "Creating the CMP Application Server Certificates") using the provided script;

```
/opt/siemens/servicetools/cmp/encodePassphrase.sh ,
```

and enter the encoded keystore password on section;

keystorePass="encoded keystore password"

```
<Connector...cmpPassphraseProtect="true"

keystoreType="PKCS12"

keyAlias= "tomcat"

keystoreFile="<SymphoniaHome>/common/conf/tomcat-
keystore.p12

keystorePass="<Key/StorePassword>"...</Connector>
```

7) Save the changes

8) Execute the following command to restart the CMP web server in order to use the new configuration:

```
/etc/init.d/symphoniad restart TomcatServletContainer
```

7.6.1.1 Obfuscating the keystore password in the CMP Tomcat's server.xml

Execute these steps for:	ENV1	ENV2	ENV3	ENV4

The keystore password in the server.xml configuration file of CMP's Tomcat web server can be stored in obfuscated form.

Activating the application server keystore in CMP Tomcat web server

Step by Step

1) Open a shell on the application server and log on as root user
2) Use the following utility to obfuscate the `<Key/StorePassword>`:

   ```
   <SymphoniaHome>/servicetools/cmp/encodePassphrase.sh
   ```

   System will prompt for the passphrase to protect; provide the `<Key/StorePassword>`

   System will ask to verify the provided passphrase; provide the `<Key/StorePassword>` again.

   System will output in the screen the obfuscated `<Key/StorePassword>`

   Store the obfuscated `<Key/StorePassword>` in a temporary location; you will need this in step 5.

   NOTICE:

   Obfuscating the `<Key/StorePassword>` may take a few seconds

   ---

3) Start a text editor and open the following file

   ```
   <SymphoniaHome>/share/tomcat/conf/server.xml
   ```

4) Search the file for the section of the connector for which the following settings have been configured:

   ```
   name="CMP_https"port="443"scheme="https"
   ```

5) Add/modify the following attributes in the CMP connector section

   ```
   <Connector...cmpPassphraseProtect="true"keystorePass="obfuscated
    <Key/StorePassword>"...</Connector>
   ```

6) Save the changes

7) Execute the following command to restart the CMP web server in order to use the new configuration:

```
/etc/init.d/symphoniad restart
```

Below is an example of the server.xml section that contains the obfuscated password:

```
<Connector
...
cmpPassphraseProtect="true"
keystorePass="rO0ABXNyADJjb20uc211bWVucy5zeW1waG9uaWEuc2VjdXJpdH11YXN1L1Byb3R1Y3
R1ZE91amVjdAAAAAAAAAArAwAAeHB1cgACW0Ks8xf4BghU4AIAAHhwAAADa6ztAAVzcgAOamF2YS5sYW
5nLkxvbmc7i+SQzI8j3wIAAUoABXZhbHV1eHIAEGphdmEubGFuZy5Od W11ZXKGrJUdC5TgiwIAAHhwAA
AAAAAACtzcgBIY29tLnNpZW11bnMuc31tcGhvbmlhLnN1Y3VyaXR5YmFzZS5Qcm90ZWN0ZWRPYmp1Y3
QkUHJvdGVjdGVkT2JqZWN0SGVhZGVyAAAAAAAAAABCAAZMABFjaGVja3N1bUFsZ29yaXRobXQAEkxqYX
ZhL2xhbmcvU3RyaW5nO0wAD2NoZWNrc3VtS2V5SW5mb3QAPExjb20vc211bWVucy9zeW1waG9uaWEvc2
VjdXJpdH11YXN1L1Byb3R1Y3R1ZE91amVjdCRLZX1JbmZvO1sAE2VuY3J5cHRpb25BbGdQYXJhbXN0AA
JbQkwAE2VuY3J5cHRpb25BbGdvcml0aG1xAH4ABEwAEWVuY3J5cHRpb25LZX1JbmZvcQB+AAVMAA51bm
NyeXB0aW9uTW9kZXEAfgABeHB0AAhIbWFjU0hBMXNyAEtjb20uc211bWVucy5zeW1waG9uaWEuc2VjdX
JpdH11YXN1L1Byb3R1Y3R1ZE91amVjdCRQYXNzcGhyYXN1RGVyaXZ1ZEtleU1uZm8AAAAAAAAAAQIAA0
wACUt1eUx1bmd0aHQAE0xqYXZhL2xhbmcvSW50ZWdlcjtMAA5pdGVyYXRpb25Db3VudHEAfgAKWwAEc2
FsdHEAfgAGeHIAOmNvbS5zaWVtZW5zLnN5bXBob25pYS5zZWN1cml0eWJhc2UuUHJvdGVjdGVkT2JqZW
N0JEt1eU1uZm8AAAAAAAAAAQIAAUwABWt1eU1kcQB+AAR4cHQAFPBhc3NwaHJhc2VEZXJpdmVkS2V5c3
IAEWphdmEubGFuZy5JbnR1Z2VyEuKgpPeBhzgCAAPJAAV2YWx1ZXhxAH4AAQAAABBzcQB+AA4AAAC+dX
IAA1tCrPMX+AYIVOACAAB4cAAAAAq1NEQCBnVUydFBdXEAfgARAAAAEgQQrBi+hYGzcy1Zs544ucA+VX
QAA0FFU3NxAH4ACXEAfgANc3EAfgAOAAAAEHNxAH4ADgAAAL51cQB+ABEAAAAK+5fQ2rmDYJeUXHQAFE
FFUy9DQkMvUEtDUzVQYWRkaW5ndXEAfgACAAAAUNCJTOTwL3+BhWbmfZnJDZC9os2Jeq/
mpO2XmBo1ZHXgV2UXebK0wfSmhdy1Wh0KqJtb+fAb/
KRdV+1TKTHQ7xeyfvNSK05phgI1oiKs1PLheA--"
...
</Connector>
```

7.6.2 Activating the application server certificates for CMP Apache Web server

Execute these steps for:	ENV1	ENV2	ENV3	ENV4

In order for OpenBranch to be able to download Software/Phone Software using https, the Apache2 web server must be configured to use the application server's certificates

The certificate/private key files in PEM format that were either provided by the self-maintained or commercial certificate authority (ENV1/ENV2) or were created by following this guide (ENV3/ENV4) must be enabled in CMP's Apache web server configuration in order to enable the secure OpenBranch Software/ Phone Software download.

Follow the instructions for creating a Certificate Sign Request (CSR) mentioned in the relevant chapter 6.5.3 "Creating a Certificate Sign Request for the Application Server".

Activating the application server certificates for CMP Apache Web server :

Step by Step

1) Open a shell on the application server and log on as root user

2) Copy the server private key PEM file stored in <CaBaseDir>
`(/opt/siemens/common/conf/ca/CaBaseDir/private/server.key)`
to
`/etc/apache2/ssl.key/sen_key.pem`
3) Copy the server certificate PEM file stored in <CaBaseDir>
`(/opt/siemens/common/conf/ca/CaBaseDir/cert/server.pem)`
to
`/etc/apache2/ssl.crt/sen_cert.pem`
4) If additional intermediate certificates are required to validate the application servers certificate, merge them in one file and copy it to `/etc/apache2/ssl.crt/cacert.pem`
How to combine several certificates to a certificate chain is described in "Combining multiple certificate files in a certificate chain"
5) Use the following utility to obfuscate the `<Key/StorePassword>`:
`<SymphoniaHome>/servicetools/cmp/encodePassphrase.sh`
System will prompt for the passphrase to protect; provide the `<Key/StorePassword>`
System will ask to verify the provided passphrase; provide the `<Key/StorePassword>` again.
System will output in the screen the obfuscated `<Key/StorePassword>`
6) Store the obfuscated `<Key/StorePassword>` in the file `/etc/apache2/ssl.key/apache_httpd_pass`
7) Restart the Apache2 server: `rcapache2 restart`

7.6.3 Configuring and Rotating Cryptographic Keys for Symphonia

Prerequisites

1) Ensure you have **administrator access** to the Symphonia host.
2) Identify the **Java installation used by Symphonia**.
3) Back up the existing `cryptoKeystore.jks` file.
4) Plan a maintenance window if required, as incorrect configuration may prevent login.

Starting with Symphonia **version 10.6.18.0**, Tomcat's `/shared/classes` directory includes the following files:

- `cryptoKeystore`: Contains the RSA key pair used for encryption.
- `cryptohelper.properties`: Contains the configuration required to access the keystore and keys.

Step by Step

1) To generate a New Key Pair, use the keytool utility from the Java installation used by Symphonia.

> **NOTICE:** You may leave the prompted fields blank to accept the default `Unknown` values.

a) At the final proompt, review and type `yes` to confirm.

> **NOTICE:**
>
> Ignore the warning about migrating to the PKCS12 standard.
>
> CMP's Java compiler settings require the **JKS format** for compatibility.

Example

The passwords shown below (`changeit`) are examples only. Use values that comply with your organization's security policy.

```
# /opt/siemens/share/ibm-java-x86_64-80/jre/bin/
keytool \
-genkeypair \
-alias cryptoKey \
-keyalg RSA \
-keysize 2048 \
-keystore cryptoKeystore.jks \
-storepass changeit \
-keypass changeit
What is your first and last name?
  [Unknown]:
What is the name of your organizational unit?
  [Unknown]:
What is the name of your organization?
  [Unknown]:
What is the name of your City or Locality?
  [Unknown]:
What is the name of your State or Province?
  [Unknown]:
What is the two-letter country code for this unit?
  [Unknown]:
Is CN=Unknown, OU=Unknown, O=Unknown, L=Unknown,
 ST=Unknown, C=Unknown correct? (type "yes" or "no")
  [no]:  yes


Warning:
The JKS keystore uses a proprietary format. It is
 recommended to migrate to PKCS12 which is an industry
 standard format using "keytool -importkeystore
 -srckeystore cryptoKeystore.jks -destkeystore
 cryptoKeystore.jks -deststoretype pkcs12".
```

2) Change the ownership of the new `cryptoKeystore.jks` keystore file to the **Symphonia** user and group.

   ```
   chown sym:sym cryptoKeystore.jks
   ```

   Adjust user and group names as required for your environment.
3) Replace the existing `cryptoKeystore.jks` keystore file in Tomcat's `/shared/classes` directory with the newly generated one.
4) Update the `cryptohelper.properties` file with the values used during key creation:

   ```
   keystore.password=<storepass value>
   keystore.key.alias=<alias value>
   keystore.key.password=<keypass value>
   decrypt.base64.fallback.enabled=true
   ```

   The `decrypt.base64.fallback.enabled` option controls whether Base64 encoding is used as a fallback during password encryption.

   If an encryption error occurs:

   - If the value is set to `true`, the password will be Base64 encoded, and the login will succeed.
   - If the value is set to `false`, an empty password will be sent and the login will fail.
5) Restart the Symphonia/Tomcat service.
6) Verify that users can authenticate successfully.

7.7 Importing the Root Certificate in the Client Browsers

The CMP application server authenticates itself with the configured certificates to the client browsers of the CMP users. In order for the users' browsers to trust these server certificates you need to import the root certificate of the CA that was used to sign the application server certificate in the client browsers truststore

This chapter describes this operation in Internet Explorer 8. The following steps are required.

- Inspecting the Root Certificate
- Validating the root certificate
- Installing the root certificate

7.7.1 Inspecting the Root Certificate

Execute these steps for:				**ENV4**

Before you can import the root certificate in the Internet Explorer, you should inspect it via Internet Explorer

Displaying the Root Certificate

Step by Step

1) Connect to CMP via the Internet Explorer using HTTPS

   The Internet Explorer issues the following message to point out that it has received a certificate it canot trust:

   There is a problem with this website's security certificate.

   The security certificate presented by this website was not issued by a trusted certificate authority
2) Select the option **Continue to this website (not recommended)**.
3) The Internet Explorer displays the CMP login page and displays the **Certificate Error** next to the address bar.
4) Click on Certificate Error

   A popup 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

7.7.2 Validating the root certificate

Execute these steps for:				**ENV4**

Before you import the displayed root certificate in the Internet Explorer, validate its authenticity. This will ensure that the presented root certificate is actually the one you installed in the application server

Validating the root certificate

Step by Step

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 SHA1 fingerprint of the original root certificate used.(section A.5.2)

   IMPORTANT:

   Both thumbprints must match

   If both thumbprints match, the received root CAcertificate was actually the one used to sign the application server certificate. The received server certificate can then be trusted.

7.7.3 Installing the root certificate

Execute these steps for:				**ENV4**

After validating the root certificate can be trusted, you can import it in the Internet Explorer's truststore

Installing the root certificate

Step by Step

1) In the dialog that displays 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.

7.8 Additional Instructions

You may need the following additional instructions to configure the certificate strategy in a customer environment.

- Creating a secure Password
- Combining multiple certificate files in a certificate chain
- Converting a certificate chain from DER format to PEM format
- Converting a certificate chain from PKCS#12 format into PEM format

7.8.1 Creating a secure Password

Execute the following steps to create a random string that you can use as a password:

Step by Step

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)}'
```

```
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)}'
```

System outputs a string that satisfies the following restrictions:

- 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 string is eight characters long . If you want to create a longer password, specify the desired number of characters in section of following section of the command:

```
print substr($0,2,<number of characters>)
```

IMPORTANT:

The password should be at least eight characters for security reasons

3) Store the generated string is a secure location

7.8.2 Combining multiple certificate files in 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.

Combining multiple certificate files in a certificate chain

Step by Step

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 CA certificate `ca_root.pem` with the intermediate certificates `im_cert1.pem` and `im_cert2.pem`.

NOTICE:

You can combine as many certificates as you required

```
catca_root.pemim_cert1.pemim_cert2.pem >ca_chain.pem
```

The certificate chain is stored under the name `ca_chain.pem` in the current directory.

7.8.3 Converting a certificate chain from DER format to PEM format

You can convert a certificate chain into the PEM format if it is provided in the DER format.

Converting a certificate chain from DER format to PEM format:

Step by Step

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.

7.8.4 Converting a certificate chain from PKCS#12 format into PEM format

You can convert a certificate chain into the PEM format if it is available in the PKCS#12 format.

Converting a certificate chain from PKCS#12 format into PEM format:

How to convert a certificate chain from the PKCS#12 format into the PEM format by executing the following steps on an -OpenScape computer system:

Step by Step

1) Open a shell and log on as root user
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.

8 OpenScape User Management Overview

OpenScape User Management (OS UM) represents a new functionality in Common Management Platform (CMP), that allows assignment of communications equipment (resources) to the users of this equipment.

OS UM supports assignment, modification and deletion of the following resource types:

- OpenScape Voice resource and OpenScape Voice Softphone resource
- OpenScape 4000 resource
- OpenScape Xpressions
- Unified Communications
- External

In general, the OS UM application is composed of three parts:

- **Administration**
- **Provisioning**
- **Unify Phone**

It is very important, at the beginning, to distinguish between three different types of Users that may appear within the OS UM. These Users are:

- UM User (described in details, in the chapters that follow)
- UC User (Unified Communication (Web Client) Account)
- CMP Admin User
- Unify Phone User

NOTICE: A User can become an Administrator if one or more administrator profiles have been assigned to him.

Besides the Users that belong to the selected domain, it is also possible to create Foreign Users. The Foreign Users are external Users, or administrators from another domain, that have specific rights in the selected domain. It is possible to assign the profiles from the selected domain, but the profiles from other domains cannot be assigned. Assigning the resources to the Foreign Users is not allowed.

NOTICE:

OpenScape Voice can currently only be operated with one domain – the predefined system domain **System**. Therefore, no Foreign Users are currently supported.

---

9 OpenScape User Management License Management

OpenScape User Management is licensed product and thus it requires licenses in order to work.

Depending on the software version (i.e., OS UM V7 or V7R2) to which you wan to upgrade your current system, the following licensing models will be applied:

- Licensing model for OS UM V10
- Licensing model for OS UM V7R2
- Licensing model for OS UM V7

Licensing mechanism in OS User Management V10

In the new licensing model for OpenScape User Management V10, a license is:

- **consumed** at the moment the first resource or an administrator profile is successfully assigned to a UM User
- **released** at the moment the last assigned resource is successfully unassigned from a UM User and no administrator profiles are assigned.

Licensing mechanism in OS User Management V7R2

In the new licensing model for OpenScape User Management V7R2, a license is:

- **consumed** at the moment the first resource is successfully assigned to a UM User
- **released** at the moment the last assigned resource is successfully unassigned from a UM User.

IMPORTANT:

OS UM V7R2 does not allow access to any of its features (even to the non-UI interfaces, such as LDAP or SPML), if the number of installed and activated OS UM licenses (GPCF or purchased) is less than the number of UM Users (**that have assigned resources**) stored in the system.

This allows easier introduction of OS User Management in the customers environment. It will be possible, for example, to use an OS UM trial license (e.g., 30 UM User licenses), synchronize the whole LDAP directory in OS UM and from there select which will be those 30 employees that will be managed through OS UM.

Licensing mechanism in OS User Management V7

In the licensing model for OpenScape User Management V7, a license is:

- **consumed** for each created UM User
- **released** whenever a UM user is deleted from the system.

IMPORTANT:

OS UM V7 does not allow access to any of its features (even to the non-UI interfaces, such as LDAP or SPML), if the number of installed and activated OS UM licenses (GPCF or purchased)

is less than the number of UM Users currently stored in the system.

This approach has led to the difficulties in the field trials, because it was not easy to restrict the number of created UM Users to the number of available trial licenses. Also, this licensing model may create potential problems in the full deployments as well, since the customers may not have as many UM licenses as the employees.

In order to overcome these restrictions a change in the licensing model was requested and a new licensing model has been introduced in OS UM V7R2.

9.1 Licensing model for upgrading to OS User Management V10

This chapter describes the UM User licenses management when upgrading the current OS UM version to OS UM V10.

When upgrading to OS UM V10, the following actions will take place:

- a new consumption model for UM User licenses will be applied
- once the upgrade procedure completes, the system consumes one UM license for each UM User that has administrator profiles and no resources assigned
- after applying the new license model, the number of used licenses will be equal to the number of UM users that have resources and/or administrator profiles assigned. To see the license information, navigate to **CMP** > **Maintenance** > **Licenses** > **Management** > **Information** > **License Information** and see the number of used licenses for **OS CMP User Management User**.

9.2 Licensing model for upgrading to OS User Management V7R2

This chapter describes the UM User licenses management when upgrading the current OS UM version to OS UM V7R2.

When upgrading to OS UM V7R2, the following actions will take place:

- a new consumption model for UM User licenses will be applied
- once the upgrade procedure completes, the system releases one UM license for each UM User that has no resources assigned
- after applying the new license model, the number of used licenses will be equal to the number of UM users that have resources assigned. (To see the license information, navigate to **CMP** > **Maintenance** > **Licenses** > **Management** > **Information** > **License Information** and see the number of used licenses for **OS CMP User Management User**).

9.2.1 License consumption in OS User Management V7R2

The UM User licenses in OS UM V7R2 are consumed (released) in the following cases:

- during manual resource assignment (unassignment)
- during bulk resource assignment (unassignment)

- during UM Users deletion
- during bulk assignment of the resources using the User Templates
- during import of UM Users via CSV file
- during creation of UM Users and their resources from HPUM
- during creation of UM Users from UC Accounts
- during creation of UM Users from OSV Subscribers
- during Synchronization of UM Users from LDAP.

9.3 Licensing model for upgrading to OS User Management V7

This chapter describes the supported scenarios for OS User Management License Upgrade to V7, while at the same time, keeping the option of 50 free licenses for the new customers.

OS User Management licenses are introduced initially in V6 and include the default license file of 50 free UM User licenses which are not bounded to the hardware/OS instance (GPCF file, but without time limitation). The customer has an option to purchase a higher number of licenses over a hardware/OS bound license file and to replaces the default file.

The follwoing are the rules for OS UM license upgrade to V7:

1) V7 GPCF is similar to V6 file, with the respect to Base and User licenses, but does not contain licenses for the Feature Packages (LDAP and OS ILA). Therefore there shouldn’t be the upgrade scenarios for any remaining time-limited FP1/FP2 licenses from V6.

2) V7 GPCF is always installed (fresh/upgrade), regardless of whether the licenses have been purchased in V6 or the customer used only the V6 GPCF.

3) If V6 GPCF is present when upgrading to V7, the consumed User licenses in V6 GPCF have to be transferred to V7 GPCF.

4) UM User Licenses for V7 are different than the ones for V6 and that’s why they need to be available at installation time (and activated after the upgrade).

5) In OS UM V7, after startup, the User Management Service needs to verify that there are at least as many licenses as there are Users and keep the result in its state. Upon every method call, User Management Service will always check against this (cached) result, and, if negative, respond with an error message (LicenseViolationException).

6) New license activation should be announced with an event by the Licensing Service. User Management Service listens for this event, re-checks that there are adequate licenses (saves the need of a restart) and re-populates the result in its state.

9.3.1 How to Install and Load OS UM V7 GPCF licenses on a System with V6 GPCF

Prerequisites

Adequate administrative permissions

Customer has only consumed some/all of the 50 free (GPCF) OS UM User licenses in V6, i.e., has not purchased a commercial license for V6.

Step by Step

The Administrator upgrades CMP to V7.

System installs the OS UM GPCF file for V7.

At startup, system loads the V7 GPCF licenses for OS UM, by also transferring the number of consumed UM User licenses to the license record for V7 (V6 is replaced).

9.3.2 How to Install and Load OS UM V7 GPCF licenses on a System with commercial V6 OS UM license file

This chapter describes the most common scenario while upgrading to V7.

Prerequisites

Adequate administrative permissions

Customer has purchased a commercial license for V6 (RLF) and has consumed more than 50 OS UM User licenses.

Step by Step

The Administrator upgrades CMP to V7.

System installs the OS UM GPCF file for V7.

At startup, System loads the V7 GPCF licenses for OS UM, by also setting the counter of consumed licenses equal to the number of total (50) OS UM User licenses in the GPCF file.

IMPORTANT:

No access to OS User Management tab is possible (System responds with a License Violation Error).

9.3.3 How to Install and Load OS UM V7 commercial licenses

This chapter describes how to Install and Load OS UM V7 commercial licenses on system with commercial V6 OS UM license file (and GPCF V7).

Prerequisites

Adequate administrative permissions

Customer has purchased a commercial license for V6 and has consumed more than 50 OS UM User licenses in V6.

Customer's system has been upgraded to V7 and the GPCF V7 file has been installed and loaded.

Step by Step

The Administrator uploads and activates commercial V7 license file containing OS UM User licenses.

After startup, System loads the commercial UM User licenses by also setting the counter of consumed licenses equal to the V6 consumed ones.

IMPORTANT:

Access to OS User Management tab is allowed.

9.4 How to check if OS UM User licenses are sufficient

OS UM V7 does not allow access to any of its features (even to the non-UI interfaces, such as LDAP or SPML), if the number of installed and activated OS UM licenses (GPCF or purchased) is less than the number of UM Users currently stored in the system. On the other hand, the newer version of OS UM (i.e., V7R2) does not allow access to any of its features (including the non-UI interfaces, such as LDAP or SPML), if the number of installed and activated OS UM licenses (GPCF or purchased) is less than the number of UM Users (**that have assigned resources**) stored in the system

Prerequisites

Adequate administrative permissions

IMPORTANT:

At startup of OpenScape User Management V7, system verifies that there are at least as many UM User licenses activated, as there are UM Users stored in the system, and stores a positive result in its state.

In case, system finds less UM User licenses than the UM Users stored in the system, a negative result will be stored in the system.

IMPORTANT:

At startup of OpenScape User Management V7R2, system verifies that there are at least as many UM User licenses activated as there are UM Users with assigned resources stored in the system, and stores a positive result in its state.

In case, system finds less UM User licenses than the UM Users with assigned resources stored in the system, a negative result will be stored in the system.

Step by Step

1) Navigate to **User Management** tab.

System displays the **User Management** navigation tree and the homepage.

2) Click on any menu item of **User Management** you have access to (including non-UI interfaces).

   System checks against its state for a potential license violation.

   NOTICE:

   If system finds a negative result in its state, it responds with a License Violation Error: `There are no sufficient OSC UM User Licenses. Access to OSC UM is restricted.`

Based on the available UM licenses, the system allows or restricts the access to the OS UM.

9.5 How to grant access to OS UM as soon as sufficient licenses are activated

In case the access to OS UM has been restricted due to insufficient licenses, once the administrator activates licenses over the CMP, the access will be "re-gained".

Prerequisites

Adequate administrative permissions that allows access to OS UM and License Activation.

Access to OS UM has been restricted due to the insufficient licenses.

Step by Step

1) On the **Maintenance** navigation tab click on the **License** navigation menu item.
2) Select **Information** in the navigation tree.
3) Click **Offline Activation...** or **Online Activation...** button in the work area, to activate the UM licenses.

   A new license file for OS UM, containing:

   - **a)** at least as many User licenses as there are UM Users on the system (for OS UM V7), or
     b) at least as many User licenses as there are UM Users with assigned resources stored in the system (for OS UM V7R2)

   has been activated.
4) Navigate to any area within the **User Management** you have access to (including non-UI interfaces).

System checks against its state for a potential license violation and allows the access to the OS UM.

10 OpenScape User Management Administration

The OpenScape User Management **Administration** is consisted of Basic Features administration and Advanced Features administration.

The OS UM Basic Features include:

- **Users & Resources**
- **Localities**

Besides them, OS UM also contains features that can be declared as Advanced:

- **User Templates**
- **OSV Migration Settings**.

An administrator can be:

- **CMP Administrator**
- **UM Locality Administrator**.

When creating users, or user templates and for other configurations that require the creation of identifiers, you must refer to the character restrictions. For more information, see Appendix A: Character Restrictions on page 691.

10.1 Users & Resources

For the proper understanding of OpenScape User Management concept, it is necessary to define clearly the term User.

Besides the CMP Admin User and UC User, the most important role within the OS UM is assign to the UM User.

NOTICE: A new UM User is a physical person (an employee of the company), who is exploiting the resources assigned to him, while using the telephony services.

The UM User is described with the following groups of attributes:

- Feature attributes

  These attributes describe the configuration settings, or the features supported by the resource. The examples of these attributes are: the feature profile, the individual features, the registration type, or the protocol of an OpenScape Voice Subscriber.

  The attributes of this category are covered by Resource Templates and defined and stored in element managers.
- Local attributes

  These attributes do not specifically belong to the resource, but they are necessary for resource creation and they are mainly bounded to the location (membership) of the Users.

  Local attributes specify references to the countable systems resources, groups or the rule sets to which the resource is supposed to be connected, assigned to or ruled by (in the context of the system it resides on). Such

attributes are: Numbering Plan, Office Code, Branch Office (OpenScape Voice), or the Address Translation Context (OpenScape UC Application).

In general, Localities are used to predefine common data for all Resources of a specific type on a specific location.

- Unique attributes

  These attributes are unique for the resource and they represent identifiers, or credentials, such as the Extension, or PEN (OpenScape 4000).

The Local attributes together with the Unique attributes are covered by the introduction of Localities and defined and stored as specific entities in OpenScape User Management.

The table of UM Users attributes, grouped by their importance, as well as the initial set of visible columns, is given below:

Table 5: Available Attributes

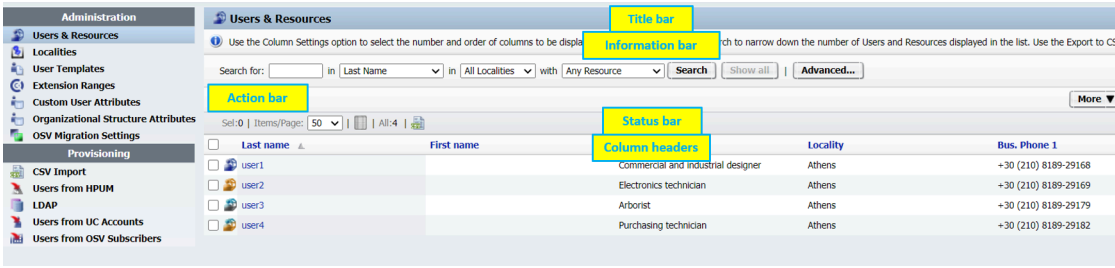
#	Attribute	Sorting	Searching	Search Type	Initially visible
	High Importance				
1	Last Name	yes*	yes	Type I	yes
2	First Name	yes*	yes	Type I	yes
3	Middle Name	yes*	yes	Type I	
4	Company Name	yes	yes	Type I	yes
5	Locality	yes	yes	Type II	yes
6	Notice	no	yes	Type I	
7	Bus. Phone 1	yes	yes	Type I	yes
8	Bus. Phone 2	yes	yes	Type I	
9	Mobile Phone	yes	yes	Type I	
10	Home Phone	yes	yes	Type I	
11	Fax Number	yes	yes	Type I	
12	E-mail Address 1	yes	yes	Type I	
13	E-mail Address 2	yes	yes	Type I	
14	Resources	yes	yes	Type II	yes
15	User ID	yes*	yes	Type I	
16	ONS Number	yes	yes	Type I	

#	Attribute	Sorting	Searching	Search Type	Initially visible
	Medium Importance				
17	Display Name	yes*	yes	Type I	
18	Description	no	yes	Type I	
19	Department	yes	yes	Type I	
	Low Importance				
20	Gender	yes	yes	Type II	
21	Language	no	yes	Type I	
22	Home time zone	no	yes	Type I	
23	IM Address	yes	yes	Type I	
24	Home URL	no	yes	Type I	
25	Source	yes	yes	Type I	
	Locality related information				
26	Building	yes	yes	Type I	
27	Room	yes	yes	Type I	
28	Street	yes	yes	Type I	
29	Postal Code	yes	yes	Type I	
30	City	yes	yes	Type I	
31	State/ Province	yes	yes	Type I	
32	Country	no	yes	Type I	

NOTICE: Case-Insensitive sorting is supported for all attributes that contain "*" in the column Sorting. For all other attributes, sorting is Case-Sensitive, i.e. uppercase is different from the lowercase and uppercase comes first.

User Management Web Interface

The OpenScape User Management Web interface is located under the Common Management Platform (CMP), tab **User Management** (see picture below).



In general, the OS UM interface is consisted of the following layout elements:

- **Title bar** (includes the table Icon, the Text for the table title and the Help Button/Icon).
- **Information bar** (contains Information Icon followed by the Information Text that describes the content of the table).
- **Search/Filter bar** (this area includes fields and action buttons related to Search/Filtering. Also, an Advanced search can be applied to the list in order to extract only the rows that match search criteria)

NOTICE: Typing the "*" symbol in the search bar and selecting any attribute in the **in:** field, filters out all results that have an empty value in the selected field. For example entering "*" in the search bar and selecting **First Name** will display only Users that have a value in their **First Name** attribute. The same applies for the Advanced Search.

.

- **Action bar** (refers to the actions that can be applied to the multiple items selected at once such as: Add, Edit, or Delete button).
- **Status bar** (Status bar is located above Column Headers and it contains all information necessary for managing data presentation).
- **Column header** (contains the column header for each column of the table. Columns that can be sorted have their corresponding Headers marked as links. Clicking on such a Header will sort the corresponding column in ascending order and the Sorting icon will appear next to the column.)
- **Table rows** (appear one after another in different colors. Each row starts with a Check box, followed by the representative Icon and the distinctive Columns. At the end of each row, there is the item's Action Menu that contains the actions, such as Edit, or Delete, that are available for the particular item).

The UM User can have different icons, depending on some characteristics:

- A simple UM User has the following icon:

- A UM User that is also an LDAP User, has the following icon

- A UM User that is also a CMP Administrator, has the following icon:

- A UM User that is also a CMP Administrator and LDAP User, has the following icon

All UM User details are grouped into seven application tabs:

- **General** tab

  Contains important User Details, as well as User Resources. Some of the fields, such as **User ID**, **Last name** and **Display name** are obligatory (written in bold letters). Some other fields, located on the **General** tab, are optional (**First name**, **Email address 1, Business phone 1**, etc.)

  NOTICE: Since in the real world there are persons with the same combination of **First name** and **Last name**, the OpenScape User Management follows the same logic and supports “non unique” UM Users’ names combination.

  Resources area contains the following Resource types that are supported in OS UM:

  – OpenScape Voice resource, OpenScape Voice Softphone resource & OpenScape Mobile resource
  – OpenScape 4000 resource
  – OpenScape Xpressions
  – Unified Communications.
  – External.

    NOTICE:

    Currently, the E/A - Cockpit UC Resource is not supported via OS UM. For creation/assignment of E/A Cockpit use the UC Application menu.

  – Unify Phone
  – Zoom
  – IP Device
  – Mobile User
- **Advanced** tab

  Contains address and personal data divided into the following areas:

  – **Personal** area
  – **Location** area
  – **Phone & E-mail**.
- **Custom User Attributes** tab

  Contains the Custom User Attributes of the UM user

  This tab appears only when custom user attributes have been configured.
- **Organizational Structures** tab

  Contains the attributes of the user’s organizational structure
- **Visibility Groups** tab

  Contains the Visibility Groups of the UC resource that are assigned to the User

- **PINs** tab

  Contains the station PINs of all the 4K resources that are assigned to the User.

  NOTICE:

  – In case 4K EM is not installed the PINs tab is not displayed.
  – In case user does not have any 4K resources assigned the PINs tab is displayed in disabled state.

10.1.1 How to Display Users

Displaying the list of UM Users is one of the basic OpenScape User Management functions. The UM Users list can be customized and search functionality may be applied to this list.

Prerequisites

Adequate administrative permission that allows Management of UM Users and Resources.

- **Column Settings** functionality has been enabled in order to customize the way the UM User list is displayed (column visibility can be adjusted). **Column Settings** does the following:
  – Shows the number of selected items.
  – Shows the number of items per page.
  – Launches the Column Settings (clicking on the corresponding icon).
  – Shows the number of All available items.
  – Launches **Exporting data to CSV file** functionality (clicking on the corresponding icon).
  – Shows the number of pages and page navigation (visible only if the number of All available items is bigger than the number of items shown per page).

NOTICE:

All UM User attributes, available for displaying in the UM Users list, are shown in the Table: Available Attributes. Additionally, **User Template**, **Status**, **Groups**, **Modified by** and **Last Modified** can be selected.

Default values for following attributes for pre-existing UM users are:

-) Modified by = internal@system

-) Last Modified = Jan 1, 1970 2:00:00 AM

These attributes shall be updated on cases that involve:

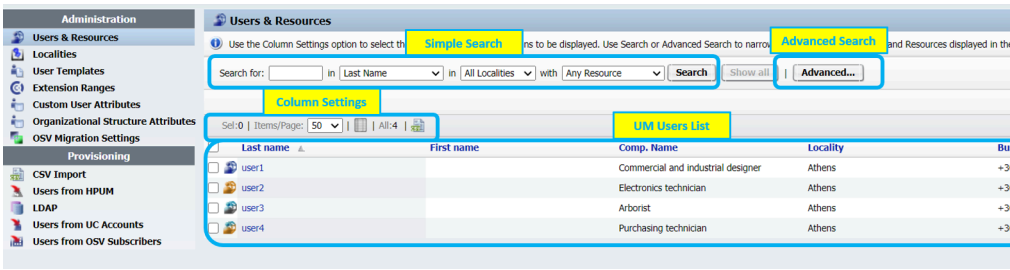
-)UM user creation or deletion

-)UM user modification of attributes

-)UM user resource creation or modification or deletion

Step by Step

1) Navigate to **User Management** > **Administration** > **Users&Resources**. A list of the existing UM Users is displayed.



NOTICE: In case you are logged in as an UM Locality Administrator, system displays only the UM Users that belong to the Localities of this UM Locality Administrator.

NOTICE:

The list of UM Users, among others, displays the status of User to User Template association.

The columns **User Template** shows the User Template associated with each User, whereas the column **Status** (hover over to see the status message) shows the current status of User to User Template association.

The UM User can have different icons, depending on some characteristics:

- A simple UM User has the following icon:

- A UM User that is also an LDAP User, has the following icon

- A UM User that is also a CMP Administrator, has the following icon:

- A UM User that is also a CMP Administrator and LDAP User, has the following icon

2) Navigate to the UM Users list.

   System displays the list of UM Users, sorted per first visible column in ascending order, according to the administrator's preferences.

   NOTICE:

   The UM Users created via LDAP synchronization are displayed with a different icon within the UM Users list.

   Besides the icon, the UM User's attribute **Source** is also used to distinguish the Users created via LDAP, from the Users created manually or by other provisioning methods.

   NOTICE: Steps 3-7 may be performed in any order.

3) Select to modify displayed columns of the UM Users list using the **Column Settings**.
4) Select to sort the UM Users list by any displayed column that supports sorting (see the Table: Available Attributes).
5) Click **Search** to perform Simple search operation using the following rule:

   `Search for:` **<User input>** `in` **<Attributes list>** `in` **<Locality list>** `with` **<Resource list>**.

   a) **<Attribute list>** contains the following items:

      All High Importance Attributes (as defined in the Table: Available Attributes), excluding Locality and Resources attributes. Pickup Group, Hunt Group and Modified by, are also included.

   b) **<Locality list>** contains the following items:

      All Localities {all defined Localities}

   c) **<Resource list>** contains the following items:

      Any Resource {all defined Resource Types}

6) Click **Advanced** to perform advanced search operations, specifying criteria for one or more UM Users attributes:

   `Search for:` **<User input>** `in` **<Attributes list>**.

   a) **<User input>** contains values relevant to the selected drop-down item.

   b) **<Attributes list>** contains values from the Table: Available Attributes and Pickup Group, Hunt Group, Status, User Template, Modified by, Last Modified Before, Last Modified After.

      NOTICE:

      To add a Pickup Group as criteria provide a (part of the) Pickup **Group Number** or a (part of the) **Pickup Group Name** (wildcards are supported) and choose the **Pickup Group** from the drop-down list.

      From the other side, to add a Hunt Group as criteria provide either a **Hunt Group Pilot Number** or a Hunt **Group Name**

(entering a part of it, or entering wildcards) and choose the **Hunt Group** from the drop-down list.

More than one Pickup/Hunt Group can be added in the search criteria.

NOTICE:

Among others, Advanced search functionality allows to search for the UM Users created via LDAP, by putting the text "LDAP" for the Source attribute.

NOTICE: Simple and Advanced Search support the use of wildcards. By typing the "*" symbol in the <**Search for**> field and selecting an attribute from <**Attributes list**> you can filter out results that do not have any value in the selected attribute field.

System displays the UM User(s) that satisfy Search criteria.

System displays the UM Users list, based on the new administrator's preferences.

10.1.2 How to Display Users' Resources

The UM Users can have various communications equipment (**Resources**) assigned. This chapter describes how to display the resources that have been assigned to the Users.

Prerequisites

Adequate administrative permission that allows management of UM Users and Resources.

Step by Step

1) Navigate to **User Management** > **Administration** > **Users&Resources**.
   A list of the existing UM Users is displayed and the assigned **Resources** are shown in the last column of this list.

   NOTICE: In case you are logged in as an UM Locality Administrator, system displays only the UM Users that belong to the Localities of this UM Locality Administrator.

2) Click on the specific UM User within the list to have a closer look at the **Resources** assigned to this user.

   A pop-up window **Edit User & Resources** is displayed.

3) Navigate to the **General** tab.

   A list of all Resources assigned to the UM User is displayed and it contains the following attributes (columns):

   - – **Number/ID**

- **Type**
- **Name**
- **Status**
- **Resource function**
- **Pickup Group**
- **Hunt Group**
- **ONS** (One Number Service)

NOTICE:

The list of Resources, among others, displays the deviation of User's Resources from the linked User Template's rules.

The columns **Status** (hover over to see the status message) shows the current status of User's Resources to User Template association, whereas the column **Resource Function** represents the function (in case the Resource is associated with the User Template).

Once the UM User Resource is displayed, the following advanced actions can be performed:

- Add a new Resource to the UM User
- Assign the existing Resources to the UM User
- Remove (unassign/delete) the existing Resources from the UM User.

NOTICE:

In case the OpenScape Voice or OpenScape 4000 resources appear in the UM User's resource list with the question mark (,), this means that these resources have been deleted from the corresponding system (OSV or OpenScape 4000), but they are still assigned to the UM User.

10.1.3 How to Create Users

The scenario for creating the new UM Users (in current Domain) and assigning to them the new, or the existing Resources, is given below.

Prerequisites

Adequate administrative permission that allows creation of UM Users and Resources.

Step by Step

1) Navigate to **User Management** > **Administration** > **Users&Resources**. A list of the existing UM Users is displayed.

NOTICE: In case you are logged in as an UM Locality Administrator, system displays only the UM Users that belong to the Localities of this UM Locality Administrator.

2) Click **Add** to create a new UM User.

   A pop-up window **Add User & Resources** is displayed.

3) Fill in the following UM User information, that has been grouped into four application tabs (**General**, **Advanced**, **Custom Fields**, **Resources**):

Table 6: User Attributes

General	Advanced	Custom Fields	Resources
User ID characters that are not allowed are: - ' (single quote) - @ - ; (Semicolon) - < - > - / - \\ (and their encoded chars "%3C", "%3E", "%5C") - " and ' and & , their encoded chars ("%22", "%27", "%26" respectively) and their HTML encodings javascript: and style= - " " (white space) at the start, or at the end of the User ID.	Middle name	Client Matter Code 1	Resources (shows the list of Resources assigned to the UM User, with the functionality to Create New/ Assign Existing/ Modify/Remove/ Delete Resource)
Display name	Gender	Client Matter Code 2	
Explicit display name	Salutation	Client Matter Code 3	
Last name	Title	Client Matter Code 4	
First name	Language	Client Matter Code 5	
Business phone 1	Description	Client Matter Code 6	

General	Advanced	Custom Fields	Resources
E-mail address 1	Home Time Zone	Custom Field 1	
Locality	Country	Custom Field 2	
Photo	State or Province	Custom Field 3	
Notice	City	Custom Field 4	
	Postal Code	Custom Field 5	
	Company	Custom Field 6	
	Department		
	Building		
	Room		
	Street		
	Business phone 2		
	Mobile phone		
	Home phone		
	FAX number		
	E-mail address 2		
	IM address		
	Home URL		

General	Advanced	Custom Fields	Resources
	Video		

NOTICE:

Mandatory fields are written in bold letters.

INFO:

When the value of Video attribute is non-numeric without the prefix "sip:", then this prefix is automatically added to the value.

a) Under **General** tab, fill in the **User ID** attribute.

- **If** the same **User ID** is already used by another User (e.g. UM User, CMP Admin or UC User):
  - System displays the following error message:

    `A user with the specified User ID already exists.`

b) Click … to choose the **Locality** attribute from the list of available localities.

System informs that the attributes under the **Address** tab will be updated with the address information specified in the selected **Locality**.

NOTICE: In case you are logged in as an UM Locality Administrator, system lists only the Localities of the UM Locality Administrator in the UM Users Locality selection.

NOTICE: This behavior is specific for the manual creation/modification of the UM Users. In general, when the Locality attribute of one UM User is modified (e.g. via LDAP synchronization), the address related attributes are not modified.

c) Click **Browse** to select and upload the photo of the UM User.

- The supported photo formats are JPEG, JPG, JFIF, PJPEG, PJP and PNG.
- The maximum allowed photo size is 16384 bytes.

d) In the **Resources** area, click **Assign** to add a new resource, or to assign the existing resources to the UM User.

4) Click the **Custom User Attributes** tab. This tab appears only when a Custom User Attribute has been created under: **Administration > Custom User Attributes**. Here you can assign attributes to the user you are creating.

5) Click the **Organizational Structures** tab. This tab shows a list with the names of Organizational Structure Attributes as configured in the **User**

Management > Administration > Organizational Structure Attributes section. Here you can configure zero to seven attributes.

a) a) Click **Assign** to assign an existing organizational structure to the user you are creating.

A pop-up window **Assign Organizational Structure** appears, showing all the existing structures, apart from the one already assigned to the user. Select a structure and click **OK**. The structure is now assigned to the user. You can use the search fields to filter all attributes and assign a desirable to the user. The search fields are case insensitive and you can use wildcards, such as **"*"**.

A structure is created when assigned to a user and is deleted when it's not assigned to any user.

b) In the **When the Attributes of the user's Organizational Structures are modified** field select one of the following radio buttons:

- **Update User's Organizational Structure**: This radio button updates the user's structure
- **Update current Organizational Structure for all Users**: This radio button updates all the users that had the same structure previously, with the new structure.

c) Configure the Organizational Structure attributes you want and click **Save** to assign the organizational structure to the user. A new structure is automatically created in case it didn't exist before.

6) Select **Save** to confirm your entries.

The System...

a) ... verifies that supplied information is correct and all required attributes are filled in

b) ... verifies that there is a UM User license available

c) ... creates a new UM User using the provided **User ID** as a user name

d) ... adds specified, new resources to the UM User, or assigns the existing one.

NOTICE:

An UM User license will be consumed at the moment the first resource is successfully assigned to a User. In case more than one resource is going to be assigned to the user, the system does not need to consume any additional UM User licenses.

A new UM User is displayed in the UM User list.

10.1.3.1 How to Create PINs for a User's OpenScape 4000 station

This Chapter describes how to create one or more PINs for a User's OpenScape 4000 Resource.

Prerequisites

Adequate administrative permission that allows creation of UM Users and Resource.

Selected UM User has at least one OpenScape 4000 resource assigned.

Step by Step

1) Navigate to **User Management** > **Administration** > **Users&Resources**. A list of the existing UM Users is displayed.

> **NOTICE:** In case you are logged in as an UM Locality Administrator, system displays only the UM Users that belong to the Localities of this UM Locality Administrator.

2) Select a UM User in one of the following ways:

- Click on the **Last name** of UM User.
- Check the box in front of the UM User and click **Edit**.
- In the row of a respective UM User, click on ▸ to open application action menu and then select **Edit**.

A pop-up window **Edit User & Resources** is displayed and system retrieves all UM User attributes that have been defined during the UM User creation.

3) Navigate on **PINs** tab and click on **Add** button.

A pop-up window **Add OpenScape 4000 PIN** is displayed.

4) Fill in the following information:

a) **Resource**

From the drop-down list select one of the OpenScape 4000 Resources assigned to the User.

b) **PIN Class**

From the drop-down list select one of the PIN classes allowed for station PINs. PIN classes are retrieved from the system the selected OpenScape 4000 Resource belongs to.

c) **Individual PIN**

Tick the checkbox if you want the PIN to be created only for the selected class. In other case the system creates the PIN for all the available classes.

d) **PIN Number**

Select **Generate automatically** in order the system to set the PIN or **Specify manually** in order to set the PIN manually.

5) Click **Add** to add the new PIN to the PINs list.

6) Select **Save** to confirm your entries.

The System...

a) ... verifies that supplied information is correct and all required attributes are filled in

b) ... creates the PIN for the OpenScape 4000 Resource

c) ... triggers a delta synchronization to update the UM database with the new PIN.

A new PIN is created for the User’s OpenScape 4000 station.

10.1.4 How to Create a Resource or Select an existing one

The administrator has an opportunity to create a new or add an existing Resources to the UM Users.

Prerequisites

Adequate administrative permission that allows creation of UM Users and Resources.

Step by Step

1) Navigate to **User Management** > **Administration** > **Users&Resources**. A list of existing UM Users is displayed.

2) Choose to create a new Resource or to add an existing one to the UM User.

- In case the UM User already exists within the UM Users list, click on the specific UM User to have a closer look at the **Resources** assigned to this user.

  A pop-up window **Edit User & Resources** is displayed.
- In case the UM User does not exist, select to create a new UM User clicking on the button **Add**.

  A pop-up window **Add User & Resources** is displayed.

3) Navigate to the **Resources**.

A list of all Resources assigned to the specific UM User is displayed.

4) Click **Assign**.

NOTICE: Steps 4-8 are repeated for every new Resource that is going to be assign to the UM User.

A pop-up window **Assign Resource – Resource Center** is displayed, containing only the types of Resources that are supported in the specific deployment.

NOTICE: A UM Locality administrator cannot assign/ unassign resources to Users from the User's resources list screen. Resources can be created only via User Templates.

---

5) Choose one of the available Resource types.

- In case the existing Resource needs to be assigned to the UM User, click ...

  A pop-up window is displayed, containing a list of available Resources that correspond to the previously selected Resource type.

  Check the box in front of the Resource you want to assign to the UM User and click **OK**.
- In case a new Resource needs to be assigned to the UM User, click the button **Add**.

  Based on a previously selected Resource type, the corresponding pop-up window is displayed.

The System does the following:

a) Retrieves the available Resource Templates for the selected Resource type from the relevant Element Manager.

b) Retrieves all the attributes required for the creation of the specific Resource type.

> **NOTICE:**
>
> An exhaustive list of all attributes, required for the creation of the specific Resource type, is given in the chapters that follow.

c) Fills in the values of the Resource attributes that have been defined in the Users' Locality for the selected Resource type. The chosen Resource type should be active in the selected Locality.

a) If the UM User doesn't have Locality assigned:

- – System uses only the domain (Default) Locality to fill in the values for the Resource attributes.

b) If the UM User has a Locality assigned, but the selected Resource type is not specified in the assigned Locality, or it is specified but it has been deactivated:

- – System uses only the domain (Default) Locality to fill in the values for the Resource attributes.

d) ... fills in the values of the Resource attributes that haven't been defined in the UM Users' Locality using information from the Default Locality. The selected Resource type should be active in the Default Locality.

a) If system does not find any relevant information for the selected Resource type neither in the user's, nor in the domain (Default) Locality, or the selected Resource has been deactivated, both in the user's and the domain (Default) Locality:

- – System does not fill in any values for the Resource attributes.

e) ... displays all Resource attributes reported by the Element Manager, indicating the mandatory attributes. All the attributes are editable.

6) Fill in the remaining Resource attributes to create a new Resource, or choose the Resource from list of the existing Resource.

7) Click **OK** to save the data.

System verifies that supplied information is correct and all required attributes are filled in.

8) On the pop-up window **Assign Resource – Resource Center**, click **OK** to save Resource changes.

   System stores the supplied Resource information in the Resource list, under the **Resources**.

9) Click **Save** to save changes to the UM User.

   The pop-up window closes and you are back to the **User Management** > **Administration** > **Users&Resources**.

10) System creates the specified Resources and assigns them to the UM User.

NOTICE:

An UM User license will be consumed at the moment the first resource is successfully assigned to a User. In case more than one resource is going to be assigned to the user, the system does not need to consume any additional UM User licenses.

The new Resources assigned to the UM User are displayed in the column **Resources**, within the UM Users list.

10.1.4.1 How to Create an OpenScape Voice Resource or Select an existing one

The steps below describe how to create a new or add an existing OpenScape Voice Resource.

Prerequisites

Adequate administrative permission that allows creation of UM Users and Resources.

Check the CMP **System Settings** to enable/disable **Domain to Business Group Mapping**:

1) Navigate to **Configuration** > **CMP** > **General** > **System Settings**.

   A pop-up window **System Settings** is displayed.

NOTICE:

When **Use Domain to Business Group Mapping** option is enabled, system will restrict each CMP domain to access the data of the mapped Business Group only. The Domain to Business Group mapping is defined in the OpenScape Voice Business Group page.

(Navigate to **Configuration** > **OpenScape Voice** > **Business Group** > **Business Group List** > **Add** the BG you want to map.

Click on the **tab General** to choose, in the Domain field, the domain you want to assign to this Business Group.)

NOTICE: By default, the value for the **Use Domain to Business Group Mapping option** is "disabled".

---

2) Select to enable or disable **Use Domain to Business Group Mapping** option.

   a) **If** the option **Use Domain to Business Group Mapping** is enabled:

   - – The Local attribute **Business Group** is disabled in the OpenScape Voice Element Manager (it doesn't appear on the **Add OpenScape Voice resource** window).
   - – System provides the CMP Domain and no **Business Group**.
   - – Only the Resource Templates from the **Business Group** mapped to the current Domain are available in the OpenScape Voice Resource creation and OpenScape Voice Resource specific values in the User Template.
   - – OpenScape Voice Assistant Synchronization uses the **Domain to Business Group Mapping** during the synchronization process.

   b) **If** the option **Use Domain to Business Group Mapping** is disabled:

   - – The Local attribute **Business Group** is enabled in the OpenScape Voice Element Manager (it becomes visible on the **Add OpenScape Voice resource** window).
   - – The **Numbering Plan** and the **Branch Office** values that are available when creating an OpenScape Voice Resource are depended on the selected **Business Group**.
   - – The Resource Templates from all **Business Group** are available in the OpenScape Voice Resource creation and OpenScape Voice Resource specific values in the User Template.
   - – System provides the **Business Group** in addition to the CMP Domain.
   - – OpenScape Voice Assistant Synchronization ignores the **Domain to Business Group Mapping** and synchronizes everything in the Default system domain. Any existing **Domain to Business Group Mapping** will be ignored.

Step by Step

1) Navigate to **Assign Resource – Resource Center** pop-up window, following the first four steps from the Chapter How to Create a Resource or Select an existing one.

   Only the types of Resources that are supported in the specific deployment are displayed.

2) Choose to create a new or to add the existing OpenScape Voice Resource to the UM User.

- In case the existing OpenScape Voice Resource needs to be assigned to the UM User, click ....

  A pop-up window **Select OpenScape Voice resource** is displayed, containing a list of available OpenScape Voice Resources.

  Check the box in front of the OpenScape Voice Resource you want to assign to the UM User and click **OK**.
- In case a new OpenScape Voice Resource needs to be assigned to the UM User, click the button **Add**.

  A pop-up window **Add OpenScape Voice resource** is displayed.

NOTICE: In case an existing OpenScape Voice Resource is the Main Device of an **OpenScape Mobile (OSMO)** Resource and is assigned to a UM User, then the corresponding **OpenScape Mobile** Resource is automatically assigned to the User as well.

NOTICE: In case a new OpenScape Voice Resource is created to serve as an OpenScape Mobile Resource's Main Device, then the attributes **SIP Authentication Username** and **SIP Authentication Password** need to be filled. If an existing OpenScape Voice Resource is used as a Main Device to create an OpenScape Mobile Resource, then the OpenScape Voice Resource should be edited so that the two aforementioned attributes are filled, in case they are not already filled.

---

3) The system...

a) ... retrieves the available Resource Templates for the selected Resource type (OpenScape Voice Resource) from the relevant Element Manager.

NOTICE:

In case the option **Use Domain to Business Group Mapping** is disabled and there is more than one OSV switch deployed on the system, the names of the available Resource Templates, available in the drop-down list, will appear in the form of: `subscriber_template_name@business_group_name@switch_id`.

From the other side, if only one OSV switch is present, switch_id will be omitted from the Resource Template name and it will contain only: `subscriber_template_name@business_group_name`.

---

b) ... retrieves other attributes required for the creation of OpenScape Voice Resource (see table below).

Table 7: OpenScape Voice Resource Attributes:

#	Name	Mandatory for resource creation	Type	Values	Comments
	Local				
1	Business Group *	X	List		Conditionally visible depending on the value of the System Setting "Use Domain to Business Group Mapping". The value displayed in the list shall be "commSystemName-bgName".
2	Numbering Plan **	X	List		
3	Branch Office **		List		
4	Office Code	X	List		
5	Routing Area		List		
6	Class Of Service		List		
7	Realm		Text		
	Unique				
1	Suffix	X	Text/List		This field is validated against characters. Only digits are allowed.
2	Type	X	Combo box	Public, Private	

#	Name	Mandatory for resource creation	Type	Values	Comments
3	Resource Name		Text		The resource normalized number is used as the resource name if this field is left empty.
4	Display Name		Text		This attribute must be updated with both Display Name and External Display Name in the OSV Subscriber.
5	Alphanumeric SIP URI		Text		
6	SIP Authentication User Name		Text		
7	SIP Authentication Password		Text		Click on to hide/ show the typed password.
8	DLS Mobile User Password		Text		Click on to hide/ show the typed password.

NOTICE:

* In case the values for "commSystemName" and/or "bgName" are modified after the Locality has been

configured, the Locality data will become invalid and the Administrator needs to update them manually.

** If these attributes have been defined both, in the selected Resource Template, as well as in the Locality, the value of the Locality shall take precedence.

NOTICE:

The attribute **Office code** has to be preconfigured as a part of Global Numbering Plan of OSV, before being used in the User Management for OSV resource creation. Otherwise, an error message will appear and the OSV resource will not be assigned to the UM User.

The attribute **Home Directory Numbers (DNs)**, if not existing, will be created by the system along with the creation of the OSV resource.

When list option is selected for attribute **Suffix**, only the vacant numbers appear in the list.

---

c) ... fills in the values of the Resource attributes that have been defined in the Users' Locality for the OpenScape Voice Resource type. The OpenScape Voice Resource type should be active in the selected Locality.

a) If UM User doesn't have Locality assigned:

- – System uses only the domain (Default) Locality to fill in the values for the Resource attributes.

b) If UM User has a Locality assigned, but the selected Resource type is not specified in the assigned Locality, or it is specified but it has been deactivated:

- – System uses only the domain (Default) Locality to fill in the values for the Resource attributes.

d) ... fills in the values of the Resource attributes that haven't been defined in the Users' Locality using information from the Default Locality. The selected Resource type should be active in the Default Locality.

a) If system does not find any relevant information for the selected Resource type neither in the user's, nor in the domain (Default) Locality, or the selected Resource has been deactivated, both in the user's and the domain (Default) Locality:

- – System does not fill in any values for the Resource attributes.

e) ... displays all Resource attributes reported by the Element Manager, indicating the mandatory attributes. All the attributes are editable.

4) Fill in the remaining Resource attributes to create a new OpenScape Voice Resource.

5) Click **OK** to save the data.

System verifies that supplied information is correct and all required attributes are filled in.

6) On the pop-up window **Assign Resource – Resource Center**, click **OK** to save the OpenScape Voice Resource changes.

   System stores the supplied Resource information in the Resources list, under the **Resources** tab.

7) Click **Save** to save changes to the UM User.

   The pop-up window closes and you are back to the **User Management** > **Administration** > **Users&Resources**.

8) System creates the OpenScape Voice Resource and assigns it to the UM User.

   - The newly created OpenScape Voice Resource appears in the column **Resources**, within the UM User list.

NOTICE:

In order for the related OpenScape Voice resource to be created also as Device in the Deployment Server (DLS) the following are needed:

- DLS server should be added on **Common Management Platform (CMP)**.
- DLS server should be then added on the related OSV - Business Group.
- The related OSV/Subscriber Template/Applications tab should be set to **Create device in DLS**.
- The related User Management/OpenScape Voice Resource Template, should be set to use the above related OSV/Subscriber Template.
- To create a Mobile User during the creation of an Openscape Voice/ Openscape Voice Softphone, a Subscriber Template with Mobile User and a DLS Mobile User Password is required. An IP Device will be created in the Deployment Server when a Subscriber Template with IP Device configuration is selected.

NOTICE:

In case a Deployment Server (DLS) is connected to CMP and one or more of the selected OpenScape Voice resources have IP device(s) or Mobile User(s), these will also be assigned automatically.

10.1.4.2 How to Create an OpenScape Voice Softphone Resource or Select an existing one

The steps below describe how to create a new or add an existing OpenScape Voice Softphone Resource.

Prerequisites

Adequate administrative permission that allows creation of UM Users and Resources.

Check the CMP **System Settings** to enable/disable **Domain to Business Group Mapping**:

1) Navigate to **Configuration** > **CMP** > **General** > **System Settings**.

A pop-up window **System Settings** is displayed.

NOTICE:

When **Use Domain to Business Group Mapping** option is enabled, system will restrict each CMP domain to access the data of the mapped Business Group only. The Domain to Business Group mapping is defined in the OpenScape Voice Business Group page.

(Navigate to **Configuration** > **OpenScape Voice** > **Business Group** > **Business Group List** > **Add** the BG you want to map.

Click on the **tab General** to choose, in the Domain field, the domain you want to assign to this Business Group.)

NOTICE: By default, the value for the **Use Domain to Business Group Mapping option** is "disabled".

---

2) Select to enable or disable **Use Domain to Business Group Mapping** option.

a) If the option **Use Domain to Business Group Mapping** is enabled:

- – The Local attribute **Business Group** is disabled in the OpenScape Voice Element Manager (it doesn’t appear on the **Add OpenScape Voice Softphone resource** window).
  – System provides the CMP Domain and no **Business Group**.
  – Only the Resource Templates from the **Business Group** mapped to the current Domain are available in the OpenScape Voice Softphone Resource creation and OpenScape Voice Softphone Resource specific values in the User Template.
  – OpenScape Voice Assistant Synchronization uses the **Domain to Business Group Mapping** during the synchronization process.

b) If the option **Use Domain to Business Group Mapping** is disabled:

- – The Local attribute **Business Group** is enabled in the OpenScape Voice Element Manager (it becomes visible on the **Add OpenScape Voice Softphone resource** window).
  – The **Numbering Plan** and the **Branch Office** values that are available when creating an OpenScape Voice Softphone Resource are depended on the selected **Business Group**.
  – The Resource Templates from all **Business Group** are available in the OpenScape Voice Softphone Resource creation and OpenScape Voice Softphone Resource specific values in the User Template.
  – System provides the **Business Group** in addition to the CMP Domain.
  – OpenScape Voice Assistant Synchronization ignores the **Domain to Business Group Mapping** and synchronizes everything in the Default system domain. Any existing **Domain to Business Group Mapping** will be ignored.

Step by Step

1) Navigate to **Assign Resource – Resource Center** pop-up window, following the first four steps from the Chapter How to Create a Resource or Select an existing one.

   Only the types of Resources that are supported in the specific deployment are displayed.

2) Choose to create a new or to add an existing OpenScape Voice Resource to the UM User.

   - In case the existing OpenScape Voice Softphone Resource needs to be assigned to the UM User, click .

     A pop-up window **Select OpenScape Voice Softphone resource** is displayed, containing a list of available OpenScape Voice Resources.

     Check the box in front of the OpenScape Voice Resource you want to assign to the UM User, as a Softphone resource and then click **OK**.
   - In case a new OpenScape Voice Softphone Resource needs to be assigned to the UM User, click the button **Add**.

     A pop-up window **Add OpenScape Voice Softphone resource** is displayed.

3) The system...

   a) ... retrieves the available Resource Templates for the selected Resource type from the relevant Element Manager.

   NOTICE:

   In case the option **Use Domain to Business Group Mapping** is disabled and there is more than one OSV switch deployed on the system, the names of the available Resource Templates, available in the drop-down list, will appear in the form of: `subscriber_template_name@business_group_name@switch_id`.

   From the other side, if only one OSV switch is present, switch_id will be omitted from the Resource Template name and it will contain only: `subscriber_template_name@business_group_name`.

   b) ... retrieves other attributes required for the creation of OpenScape Voice Softphone Resource (see table below).

   Table 8: OpenScape Voice Resource Attributes:

#	Name	Mandatory for resource creation	Type	Values	Comments
	Local				

#	Name	Mandatory for resource creation	Type	Values	Comments
1	Business Group *	X	List		Conditionally visible depending on the value of the System Setting "Use Domain to Business Group Mapping". The value displayed in the list shall be "commSystemName-bgName".
2	Numbering Plan **	X	List		
3	Branch Office **		List		
4	Office Code	X	List		
5	Routing Area		List		
6	Class Of Service		List		
7	Realm		Text		
	Unique				
1	Suffix	X	Text/List		This field is validated against characters. Only digits are allowed.
2	External Caller ID	X	Text		This field is validated against characters. Only digits are allowed.

#	Name	Mandatory for resource creation	Type	Values	Comments
3	Type	X	Combo box	Public, Private	
4	Resource Name		Text		The resource normalized number is used as the resource name if this field is left empty.
5	Display Name		Text		This attribute must be updated with both Display Name and External Display Name in the OSV Subscriber.
6	Alphanumeric SIP URI		Text		
7	User Name		Text		
8	SIP Authentication Password		Text		Click on to hide/ show the typed password.
89	DLS Mobile User Password		Text		Click on to hide/ show the typed password.

NOTICE:

* In case the values for "commSystemName" and/or "bgName" are modified after the Locality has been

configured, the Locality data will become invalid and the Administrator needs to update them manually.

** If these attributes have been defined both, in the selected Resource Template, as well as in the Locality, the value of the Locality shall take precedence.

NOTICE:

The attributes: **Office code** and **Home Directory Numbers (DNs)** have to be preconfigured as a part of Global Numbering Plan of OSV, before being used in the User Management for OSV resource creation. Otherwise, an error message will appear, showing that Home DN can not be find and the OSV resource can not be assigned to the UM User.

When list option is selected for attribute **Suffix**, only the vacant numbers appear in the list.

---

c) ... fills in the values of the Resource attributes that have been defined in the Users' Locality for the OpenScape Voice Softphone Resource type. The OpenScape Voice Softphone Resource type should be active in the selected Locality.

a) If UM User doesn't have Locality assigned:

- – System uses only the domain (Default) Locality to fill in the values for the Resource attributes.

b) If UM User has a Locality assigned, but the selected Resource type is not specified in the assigned Locality, or it is specified but it has been deactivated:

- – System uses only the domain (Default) Locality to fill in the values for the Resource attributes.

d) ... fills in the values of the Resource attributes that haven't been defined in the Users' Locality using information from the Default Locality. The selected Resource type should be active in the Default Locality.

a) If system does not find any relevant information for the selected Resource type neither in the user's, nor in the domain (Default) Locality, or the selected Resource has been deactivated, both in the user's and the domain (Default) Locality:

- – System does not fill in any values for the Resource attributes.

e) ... displays all Resource attributes reported by the Element Manager, indicating the mandatory attributes. All the attributes are editable.

4) Fill in the remaining Resource attributes to create a new OpenScape Voice Softphone Resource.

5) Click **OK** to save the data.

System verifies that supplied information is correct and all required attributes are filled in. Among others, it also validates that the **External Caller ID** of the

selected resource matches one of the OpenScape Voice resources assigned to the User.

NOTICE:

In case the **External Caller ID** of the selected OpenScape Voice Softphone resource does not match any of the OpenScape Voice resources assigned to the User, the system displays a warning message, but it allows to create the OpenScape Voice Softphone resource.

---

6) On the pop-up window **Assign Resource – Resource Center**, click **OK** to save the OpenScape Voice Softphone Resource changes.

System stores the supplied Resource information in the Resources list, under the **Resources** tab.

7) Click **Save** to save changes to the UM User.

The pop-up window closes and you are back to the **User Management** > **Administration** > **Users&Resources**.

8) System creates the OpenScape Voice Softphone Resource and assigns it to the UM User.

- The newly created OpenScape Voice Softphone Resource appears in the column **Resources**, within the UM User list.

NOTICE:

In order for the related OpenScape Voice resource to be created also as Device in the Deployment Server (DLS) the following are needed:

- DLS server should be added on **Common Management Platform (CMP)**.
- DLS server should be then added on the related OSV - Business Group.
- The related OSV/Subscriber Template/Applications tab should be set to **Create device in DLS**.
- The related User Management/OpenScape Voice Resource Template, should be set to use the above related OSV/Subscriber Template.
- To create a Mobile User during the creation of an Openscape Voice/ Openscape Voice Softphone, a Subscriber Template with Mobile User and a DLS Mobile User Password is required. An IP Device will be created in the Deployment Server when a Subscriber Template with IP Device configuration is selected.

NOTICE:

In case a Deployment Server (DLS) is connected to CMP and one or more of the selected OpenScape Voice Softphone resources have IP device(s) or Mobile User(s), these will also be assigned automatically.

10.1.4.3 How to Create an OpenScape Mobile Resource

The steps below describe how to create a new OpenScape Mobile Resource.

Prerequisites

Adequate administrative permission that allows creation of UM Users and Resources.

An **OpenScape Voice Resource** should be assigned to the UM User prior to creating an **OpenScape Voice Mobile (OSMO) Resource**. The **OpenScape Voice Resource** that will serve as the Main Device should have the **SIP Authentication Username** and the **SIP Authentication Password** configured.

Check the CMP **System Settings** to enable/disable **Domain to Business Group Mapping**:

1) Navigate to **Configuration** > **CMP** > **General** > **System Settings**.

A pop-up window **System Settings** is displayed.

NOTICE:

When **Use Domain to Business Group Mapping** option is enabled, system will restrict each CMP domain to access the data of the mapped Business Group only. The Domain to Business Group mapping is defined in the OpenScape Voice Business Group page.

(Navigate to **Configuration** > **OpenScape Voice** > **Business Group** > **Business Group List** > **Add** the BG you want to map.

Click on the **tab General** to choose, in the Domain field, the domain you want to assign to this Business Group.)

NOTICE: By default, the value for the **Use Domain to Business Group Mapping option** is "disabled".

---

2) Select to enable or disable **Use Domain to Business Group Mapping** option.

a) If the option **Use Domain to Business Group Mapping** is enabled:

- – The Local attribute **Business Group** is disabled in the OpenScape Voice Element Manager (it doesn’t appear on the **Add OpenScape Voice resource** window).
- – System provides the CMP Domain and no **Business Group**.
- – Only the Resource Templates from the **Business Group** mapped to the current Domain are available in the OpenScape Voice Resource creation and OpenScape Voice Resource specific values in the User Template.
- – OpenScape Voice Assistant Synchronization uses the **Domain to Business Group Mapping** during the synchronization process.

b) If the option **Use Domain to Business Group Mapping** is disabled:

- – The Local attribute **Business Group** is enabled in the OpenScape Voice Element Manager (it becomes visible on the **Add OpenScape Voice resource** window).

- The **Numbering Plan** and the **Branch Office** values that are available when creating an OpenScape Voice Resource are depended on the selected **Business Group**.
- The Resource Templates from all **Business Group** are available in the OpenScape Voice Resource creation and OpenScape Voice Resource specific values in the User Template.
- System provides the **Business Group** in addition to the CMP Domain.
- OpenScape Voice Assistant Synchronization ignores the **Domain to Business Group Mapping** and synchronizes everything in the Default system domain. Any existing **Domain to Business Group Mapping** will be ignored.

Step by Step

1) Navigate to **Assign Resource – Resource Center** pop-up window, following the first four steps from the Chapter How to Create a Resource or Select an existing one.

Only the types of Resources that are supported in the specific deployment are displayed.

2) In order to assign a new **OpenScape Mobile Resource** to the UM User, click the button **Add**. A pop-up window **Add OpenScape Mobile resource** is displayed.

NOTICE:

An existing **OpenScape Mobile (OSMO) Resource** is automatically assigned to a UM User when the corresponding Main Device is assigned to him.

---

3) The system...

a) ... retrieves the available Resource Templates for the selected Resource type (**OpenScape Mobile** Resource) from the relevant Element Manager.

NOTICE:

In case the option **Use Domain to Business Group Mapping** is disabled and there is more than one OSV switch deployed on the system, the names of the available Resource Templates, available in the drop-down list, will appear in the form of: `subscriber_template_name@business_group_name@switch_id`.

From the other side, if only one OSV switch is present, switch_id will be omitted from the Resource Template name and it will contain only: `subscriber_template_name@business_group_name`.

---

b) ... retrieves other attributes required for the creation of OpenScape Voice **OpenScape Mobile** Resource (see table below).

Table 9: OpenScape Mobile Resource Attributes:

#	Name	Mandatory for resource creation	Type	Values	Comments
	Main Device (ONS)				The normalized phone number of the related/ parent OSV subscriber: • Business Phone 1 • Business Phone 2 • User attribute
1	Branch Office **				
2	**Numbering Plan** **	X	List		
3	**Office Code**	X	List		
4	Routing Area		List		
5	Class Of Service		List		
6	Address Translator Context		Text		
7	Extension Range				
	Unique				
1	Suffix	X	Text/List		This field is validated against characters. Only digits are allowed.

#	Name	Mandatory for resource creation	Type	Values	Comments
2	**OsmoProfile**	X	List		Default Mobile Client Profile@System-Wide@Default

---

NOTICE:

* In case the values for "commSystemName" and/or "bgName" are modified after the Locality has been configured, the Locality data will become invalid and the Administrator needs to update them manually.

** If these attributes have been defined both, in the selected Resource Template, as well as in the Locality, the value of the Locality shall take precedence.

NOTICE:

The attribute **Office code** has to be preconfigured as a part of Global Numbering Plan of OSV, before being used in the User Management for OSV resource creation. Otherwise, an error message will appear and the OSV resource will not be assigned to the UM User.

When list option is selected for attribute **Suffix**, only the vacant numbers appear in the list.

---

c) ... fills in the values of the Resource attributes that have been defined in the Users' Locality for the OpenScape Mobile Resource type. The OpenScape Voice Resource type should be active in the selected Locality.

a) If UM User doesn't have Locality assigned:

- – System uses only the domain (Default) Locality to fill in the values for the Resource attributes.

b) If UM User has a Locality assigned, but the selected Resource type is not specified in the assigned Locality, or it is specified but it has been deactivated:

- – System uses only the domain (Default) Locality to fill in the values for the Resource attributes.

d) ... fills in the values of the Resource attributes that haven't been defined in the Users' Locality using information from the Default Locality. The selected Resource type should be active in the Default Locality.

a) If system does not find any relevant information for the selected Resource type neither in the user's, nor in the domain (Default) Locality, or the selected Resource has been deactivated, both in the user's and the domain (Default) Locality:

- – System does not fill in any values for the Resource attributes.

e) ... displays all Resource attributes reported by the Element Manager, indicating the mandatory attributes. All the attributes are editable.

4) Fill in the remaining Resource attributes to create a new **OpenScape Mobile** Resource.
5) Click **OK** to save the data.

   System verifies that supplied information is correct and all required attributes are filled in.
6) On the pop-up window **Assign Resource – Resource Center**, click **OK** to save the **OpenScape Mobile** Resource changes.

   System stores the supplied Resource information in the Resources list, under the **Resources** tab.
7) Click **Save** to save changes to the UM User.

   The pop-up window closes and you are back to the **User Management** > **Administration** > **Users&Resources**.
8) System creates the **OpenScape Mobile Resource** and assigns it to the UM User.
   - The newly created **OpenScape Mobile Resource** appears in the column **Resources**, within the UM User list.

10.1.4.4 How to Create an OpenScape 4000 Resource or Select an existing one

This Chapter describes the configuration of default values for OpenScape 4000 Resource.

Prerequisites

Adequate administrative permission that allows creation of UM Users and Resource.

Step by Step

1) Navigate to **Assign Resource – Resource Center** pop-up window, following the first four steps from the Chapter How to Create a Resource or Select an existing one.

   Only the types of Resources that are supported in the specific deployment are displayed.
2) Choose to create a new or to add an existing OpenScape 4000 Resource to the UM User.
   - In case the existing OpenScape 4000 Resource needs to be assigned to the UM User, click ....

     A pop-up window **Select OpenScape 4000 Resource** is displayed, containing a list of available OpenScape 4000 Resources.

     Check the box in front of the OpenScape 4000 Resource you want to assign to the UM User and click **OK**.
   - In case a new OpenScape 4000 Resource needs to be assigned to the UM User, click the button **Add**.

     A pop-up window **Add OpenScape 4000 Resource** is displayed.

3) System does the following:

a) retrieves the available Resource Templates for the selected Resource type (OpenScape 4000 Resource) from the relevant Element Manager.

b) retrieves other attributes required for the creation of OpenScape 4000 Resource (see table below).

Table 10: OpenScape 4000 Resource Attributes:

#	Name	Mandatory for resource creation	Type	Values	Comments
	Local				
1	Switch Name	X	List		
2	Virtual Node	X	List		
3	Dial Plan	X	List		Shows a list of already synchronized OpenScape 4000 Dial Plans, in the device model, that are compatible with the Numbering Plan Type (public/ private) of the Numbering Plan of the specified Virtual Node #.
	Unique				
1	Extension	X	Text/List		This field is validated against characters. Only digits are allowed.

#	Name	Mandatory for resource creation	Type	Values	Comments
2	PEN	X	Text		Only digits in format 1-XX-XXX-XXX are allowed.
3	COS Template	X	List		
4	Resource Name		Text		The resource normalized number is used as the resource name if this field is left empty.
5	Display Name		Text		
6	HFA Password		Text		Minimum 6, maximum 20 characters. Click on to hide/ show the typed password.
7	IPDA		List		
8	Source Group		Text		
9	Address Translator Context		List		

NOTICE:

The field **PEN** (Port Equipment Number) describes an access point on the Hicom/OpenScape 4000 system. PEN contains a four-part value in the form of 1-XX-XXX-XXX, where the first three parts identify the board (more

precisely, the mounting location of the board) and the fourth value, defines an access point on the board.

PEN format: LTG-LTU-SLOT-CCT (see the table below).

Table 11: PEN format

Element	Possible values	Remark
LTG -Line Trunk Group	1	
LTU - Line Trunk Unit	1...15	in HHS (Host Shelf)
	16	Not defined
	17...99	in AP (Access Point Shelf)
SLOT - Slot in the frame	1...121	
CCT - Circuit number (the connection point on the board)	0..254	

NOTICE:

When list option is selected for attribute **Extension**, only the vacant DNs appear in the list.

c) fills in the values of the Resource attributes that have been defined in the Users' Locality for the OpenScape 4000 Resource type. The OpenScape 4000 Resource type should be active in the selected Locality

   a) If UM User doesn't have Locality assigned:

   - – System uses only the domain (Default) Locality to fill in the values for the Resource attributes.

   b) If UM User has a Locality assigned, but the selected Resource type is not specified in the assigned Locality, or it is specified but it has been deactivated:

   - – System uses only the domain (Default) Locality to fill in the values for the Resource attributes.

d) fills in the values of the Resource attributes that haven't been defined in the Users' Locality using information from the Default Locality. The selected Resource type should be active in the Default Locality.

   a) If system does not find any relevant information for the selected Resource type neither in the User, nor in the domain (Default) Locality, or the selected Resource has been deactivated, both in the user's and the domain (Default) Locality:

   - – System does not fill in any values for the Resource attributes.

e) displays all Resource attributes reported by the Element Manager, indicating the mandatory attributes. All attributes are editable.

4) Fill in the remaining Resource attributes to create a new OpenScape 4000 Resource.

NOTICE:

To configure **Resource Template** and **COS Template**, perform the following steps in OpenScape 4000 Assistant:

- navigate to **Configuration Management** > **Station** > **Station** and select a station

- navigate to **Action** menu and choose **Save As Template**

- to configure a new template, check the box for **User Management Template**, or check both boxes, for **User Management Template** and **COS Template**, depending on the preferences.

---

5) Click **OK** to save the data.

System verifies that supplied information is correct and all required attributes are filled in.

If creating a OpenScape 4000 Resource, the system is not able to complete the operation in one step, then:

- – The resource is created in CMP, but not in the OpenScape 4000 System.
- – System provides a link that must be visited in order to complete the creation of the OpenScape 4000 Resource.(If you don't visit the link, it will expire and you will need to go to the OpenScape 4000 System and complete the creation manually).
- – Once the resource is successfully created, CMP is notified by the OpenScape 4000 System.

NOTICE:

The "corrupted" resource will appear in the UM Users's resource list with the different icon ( ) than the "normal" OpenScape 4000 Resource. In order to resolve this, go to the OpenScape 4000 System and recreate the corresponding resource, so that it becomes again available for the UM Users.

---

6) On the pop-up window **Assign Resource – Resource Center**, click **OK** to save the OpenScape 4000 Resource changes.

System stores the supplied Resource information in the Resource list, under the **Resources**.

7) Click **Save** to save changes to the UM User.

The pop-up window closes and you are back to the **User Management** > **Administration** > **Users&Resources**.

8) The system...
   a) ...enforces OSV routings to be updated
   b) ...creates the OpenScape 4000 Resource and assigns it to the UM User.

   • The newly created OpenScape 4000 Resource appears in the column **Resources**, within the UM Users list.

NOTICE:

Countries like Italy or Belgium could have empty either ISDN_AreaCode or ISDN_LocalCode in their OpenScape 4000 numbering plan schemes. This was causing synchronization issues between CMP and OpenScape 4000 in the past which are now resolved. As a result 4000 ONS UC accounts can be set with such Italian or Belgium OpenScape 4000 numbers.

NOTICE:

In case a Deployment Server (DLS) is connected to CMP and one or more of the selected OpenScape 4000 resources have IP device(s) or Mobile User(s), these will also be assigned automatically.

10.1.4.5 How to Create an OpenScape Xpressions Resource or Select an existing one

This Chapter describes the configuration of default values for OpenScape Xpressions Resource.

Prerequisites

Adequate administrative permission that allows creation of UM Users and Resources.

IMPORTANT:

As soon as a new Xpression node is added in the CMP (**Maintenance** > **Inventory** > **Nodes & Application** > **Nodes** > **Add OSC Xpressions...**), system automatically initiates the Xpressions resources synchronization. Additionally, the option to manually synchronize Xpressions accounts is provided, allowing the administrator to assign an existing Xpressions resource to the UM User.

Step by Step

1) Navigate to **Assign Resource – Resource Center** pop-up window, following the first four steps from the Chapter How to Create a Resource or Select an existing one.

   Only the types of Resources that are supported in the specific deployment are displayed.

2) Choose to create a new or to add an existing OpenScape Xpressions Resource to the UM User.
   - In case the existing OpenScape Xpressions Resource needs to be assigned to the UM User, click ....

     A pop-up window **Select OpenScape Xpressions resource** is displayed, containing a list of available OpenScape Xpressions Resources.

     Check the box in front of the OpenScape Xpressions Resource you want to assign to the UM User and click **OK**.
   - In case a new OpenScape Xpressions Resource needs to be assigned to the UM User, click the button **Add**.

     A pop-up window **Add OpenScape Xpressions resource** is displayed.
3) The system...
   a) ... retrieves the available Resource Templates for the selected Resource type (OpenScape Xpressions Resource) from the relevant Element Manager.

      NOTICE: The standard, pre-installed Groups defined in Xpressions will be used as a Resource Template. Custom Groups defined in the Xpressions server are not supported.

   b) ... retrieves other attributes required for the creation of OpenScape Xpressions Resource (see table below).

Table 12: OpenScape Xpressions Resource Attributes:

#	Name	Mandatory for resource creation	Type	Values	Default Value
	Local				
1	Preferred Address	X	Text		MAILBOX
2	Voice Mail System	X	Text		PHONEMAIL
3	User options for voice mail system		Text		
4	Internal mailbox	X	Text		Internal mailbox
5	CTI Journal		Check box	Yes No	
6	Fax G3 Headline		Text		
7	Language	X	List	List of supported languages	

#	Name	Mandatory for resource creation	Type	Values	Default Value
8	Home Time Zone	X	List	List of Time zones	
	Unique				
1	User ID	X	Text	Maximum 62 characters	the preferred userID, i.e., name.surname or the assigned DirectoryNumber
2	Common Name	X	Text		the preffered CommonName, i.e., name.surname the assigned DirectoryNumber
3	PIN		Text	(Only Numeric or empty values are allowed)	
4	Voice Mail	X	Text		the assigned DirectoryNumber, i.e., 302107001212

#	Name	Mandatory for resource creation	Type	Values	Default Value
5	Business Phone	X	Text	Accept (not mandate) a leading “+” or a leading “p”. When number is public, it will be prepended by '+'. When number is private, it will be prepended by 'p'.	the assigned DirectoryNumber, i.e.,302107001212
6	UC_Mode		Dropdown menu	- Xpressions mode / Not set = "X" - UC mode = "U" - Xpressions mode with option to UC mode = "O" - UC mode with option to Xpressions mode = "N" - UC WebClient > XPR Web Assistant Access disabled = "D"	- Xpressions mode / Not set = "X"

#	Name	Mandatory for resource creation	Type	Values	Default Value
7	Mobile Phone		Text		
8	Business Fax		Text		
9	E-mail		Text		
10	Windows account		Text		
11	Microsoft Exchange account		Text		
12	Lotus Notes account		Text		
13	CONUSER		Text	In order to integrate OpenScape Xpressions to UC, the CONUSER value must be set to "**UC Login Name@Domain**".	
14	Password		Text		

IMPORTANT:

When the PIN value is empty, the default PIN configured in Xpressions will be used.

NOTICE:

Click on to hide/show the typed password.

c) ... fills in the values of the Resource attributes that have been defined in the Users' Locality for the OpenScape Xpressions Resource type. The

OpenScape Xpressions Resource type should be active in the selected Locality

a) **If** UM User doesn't have Locality assigned:

- – System uses only the domain (Default) Locality to fill in the values for the Resource attributes.

b) **If** UM User has a Locality assigned, but the selected Resource type is not specified in the assigned Locality, or it is specified but it has been deactivated:

- – System uses only the domain (Default) Locality to fill in the values for the Resource attributes.

d) ... fills in the values of the Resource attributes that haven't been defined in the Users' Locality using information from the Default Locality. The selected Resource type should be active in the Default Locality.

a) **If** system does not find any relevant information for the selected Resource type neither in the user's, nor in the domain (Default) Locality, or the selected Resource has been deactivated, both in the user's and the domain (Default) Locality:

- – System does not fill in any values for the Resource attributes.

4) Fill in the remaining Resource attributes to create a new OpenScape Xpressions Resource.

5) Click **OK** to save the data.

System verifies that supplied information is correct and all required attributes are filled in.

6) On the pop-up window **Assign Resource – Resource Center**, click **OK** to save the OpenScape Xpressions Resource changes.

System stores the supplied Resource information in the Resources list, under the **Resources** tab.

7) Click **Save** to save changes to the UM User.

The pop-up window closes and you are back to the **User Management** > **Administration** > **Users&Resources**.

8) System creates the OpenScape Xpressions Resource and assigns it to the UM User.

IMPORTANT:

Whenever Xpressions Web Assistant is used to add a new, modify or delete an existing Xpressions resource, an event is sent to CMP, triggering the synchronization of the new/modified/deleted Xpressions resources to CMP/UM database. Consequently, CMP creates, updates or deletes the specified Xpression resource.

In case the connection to the Xpression server fails and Xpressions resources in the CMP are not aligned with the Xpression server data, the administrator has to manually trigger the Xpressions node synchronization process (navigate to **Maintenance** > **Inventory** > **Nodes & Application** > **Nodes**, in the In the row of a respective

Xpressions node click on the application action menu and then select **Synchronize**).

- The newly created OpenScape Xpressions Resource appears in the column **Resources**, within the UM Users list.

10.1.4.6 How to Create a Unified Communications Resource or Edit an existing one

The steps below describe how to create a new or add the existing OpenScape UC Application (UC) Resource.

Prerequisites

Adequate administrative permission that allows creation of UM Users and Resource.

Step by Step

1) Navigate to **Assign Resource – Resource Center** pop-up window, following the first four steps from the Chapter How to Create a Resource or Select an existing one.

   Only the types of Resources that are supported in the specific deployment are displayed.

   NOTICE:

   Currently, the E/A - Cockpit UC Resource is not supported via OS UM. For creation/assignment of E/A Cockpit, navigate to **Configuration** > **Unified Communications** > **Accounts** > **List** > **Add Users** > **Profiles**.

2) Choose to create a new or to add the existing OpenScape UC Application Resource to the UM User.

   - In case the existing OpenScape UC Application Resource needs to be modified, click **Edit**.

     A pop-up window **Edit Unified Communications resource** is displayed.
   - In case a new OpenScape UC Application Resource needs to be assigned to the UM User, click the button **Add**.

     A pop-up window **Add Unified Communications resource** is displayed.

3) The system...

a) ... retrieves the available Resource Templates for the selected Resource type (OpenScape UC Application Resource).

b) ... retrieves other attributes required for the creation of OpenScape UC Application Resource (see table below).

Table 13: Unified Communications (UC) Resource Attributes:

#	Name	Mandatory for resource creation	Type	Values	Comments
			Configuration		
	Local				
1	Translator Context		List		
2	VoiceMailNumber		List		
	Unique				
1	Select resource to use as ONS	X	List		Exactly one telephone number must be defined as ONS for UC Resource.
2	Select resource to use as WebRTC		List		Only one telephone number can be defined as WebRTC for UC Resource.
3	Assign WebRTC Profile		Checkbox		The WebRTC profile is mandatory for the WebRTC feature to be functional. Check the checkbox to assign the WebRTC profile. You can configure the WebRTC along with another profile (for example, Team with WebRTC). In this case, don't check the checkbox (no additional licenses will be used in case of having both the checkbox checked and the WebRTC permission existing in another chosen profile).
4	IM Address	X	Text		
	Subscription Codes of the WebRTC Subscriber **NOTICE:** This section is only enabled for configuration when a resource is set as WebRTC.				
5	Toggle MLHG Make Busy		Text	e.g. *21	Enter a value for the Make Busy Multi Line Hunt Group option.
6	Toggle MLHG Stop Hunt		Text	e.g. *22	Enter a value for the Stop Multi Line Hunt Group option.
7	Group Call Pickup		Text	e.g. *23	Enter a value for the Group Call Pickup option.
			Authentication		

#	Name	Mandatory for resource creation	Type	Values	Comments
8	Password	X	Text		• The option **Set new password** is, by default,checked, so that it is mandatory to fill in the **Login password**. Click on to hide/show the typed password. • Select the **Send Password via E-mail** option to receive the password via an e-mail. When you check this option, the attribute **User has to change login password at next login** is enabled. • Select the **Generate automatically** option to generate the password automatically. When selecting this option, the field **Login password** is greyed out • Select the option **Login password never expires** to not let the password expire
9	Telephony PIN	X	Text		• The option **Set new Telephony PIN** is, by default checked, so that it is mandatory to fill in the **Telephony PIN**. Click on to hide/ show the typed PIN. • Select the **Send telephony PIN via E-mail** option to receive the PIN via an email. When you check this option, the attribute **User has to change telephony PIN at next login** is enabled. • Select the **Generate automatically** option to generate the telephony PIN automatically. When selecting this option, the field **Telephony PIN** is greyed out.
					• Select the option **Telephony PIN never expires** to not let the PIN expire
10	Groupware Assignment	X	Drop-down list		If the Groupware connector is not configured (via **Configuration** > **Unified Communications** > **Configuration** > **Connections** > **Groupware**), the **Groupware Assignment** options will not be visible.
11	Microsoft Teams Integration	Not mandatory for creation	Text		Only visible when MS Teams is configured at Openscape UC

NOTICE: The option **Set new telephony PIN** is, by default, checked and disabled, which means that **Telephony PIN** is mandatory attribute. The reason for this is that, system sometimes requires additional, not

"strictly" mandatory information that, if not provided during creation, would result in a non-functional resource. As a result, the **Telephony PIN** attribute is not required when creating an UC User Account in the OpenScape UC Application, but it is required when assigning an UC Resource, in the OS UM. Otherwise, if **Telephony PIN** is not present, the UC will not work properly.

NOTICE: The checkboxes for attributes **Send Password via E-mail**, **Send telephony PIN via E-mail** and **Generate automatically** only appear when the SMTP server is configured from CMP > SMTP Server.

IMPORTANT: In case the option **Send Password via E-mail**, **Send telephony PIN via E-mail** or **Generate automatically** are checked, the E-Mail address of the UM User is mandatory.

IMPORTANT: The **IM Address** becomes a mandatory field starting with UC V6R1. However, since CMP V6 is used to manage both UC V6 and V6R1, this field is made mandatory also for UC V6 installations. In case there is an OpenScape V6 customer that does not want to use the **IM Address** (considered an extremely rare case), the creation of this additional attribute will not imply any functional modifications or restrictions.

c) ... fills in the values of the Resource attributes that have been defined in the Users' Locality for the OpenScape UC Application Resource type. The UC Resource type should be active in the selected Locality

   a) If the UM User doesn't have Locality assigned:

   - – System uses only the domain (Default) Locality to fill in the values for the Resource attributes.

   b) If the UM User has a Locality assigned, but the selected Resource type is not specified in the assigned Locality, or it is specified but it has been deactivated:

   - – System uses only the domain (Default) Locality to fill in the values for the Resource attributes.

d) ... fills in the values of the Resource attributes that haven't been defined in the Users' Locality using information from the Default Locality. The selected Resource type should be active in the Default Locality.

   a) If system does not find any relevant information for the selected Resource type neither in the user's, nor in the domain (Default) Locality, or the selected Resource has been deactivated, both in the user's and the domain (Default) Locality:

   - – System does not fill in any values for the Resource attributes.

e) ... displays all Resource attributes reported by the Element Manager, indicating the mandatory attributes. All the attributes are editable.

NOTICE: The value of the attribute **IM Address** is prefilled with the IM address of the UM Users.

---

4) To create the **Groupware Assignment**, i.e., allow the assignment of the UM User to a Groupware connector (MS Exchange server or IBM Domino), fill in the following:

a) **Mailbox ID**

b) **Mailbox Address**

IMPORTANT:

The presence of **Groupware Assignment** option indicates that the UM User has the Groupware assignment configured.

If the Groupware connector is not configured (via **Configuration** > **Unified Communications** > **Configuration** > **Connections** > **Groupware**), the **Groupware Assignment** options will not be visible on the **Add Unified Communications resource** window.

The Groupware connector can be created only when creating a new UC resource (either manually or via a User Template).

System creates the Groupware assignment (for details, see the OpenScape UC Configuration manual).

5) To enable the **Single Sign-On,** select the following:

For **Webclient SSO** select:

a) **External System**: this attribute can take the following values: **Disabled** or **<external Systems that have been configured in JAAS file>**.

b) **Account** (usename@domain): mandatory field when an external system is selected, validation rule username@domain.

NOTICE:

The **Single Sign-On** area (option) is visible only if the SSO external system is configured in the JAAS.cfg Webclient configuration file. Otherwise, this area will not appear.

For **SPNEGO/SOAP SSO** select:

a) **Domain**: this attribute can take the following values: **Disabled** or **<external Systems that have been configured in krb.conf>**.

b) **Username**: mandatory field when an external system is selected.

NOTICE:

If SPNEGO/SOAP SSO is not configured the **SPNEGO/ SOAP SSO** section is not displayed.

---

6) To configure **UC-Microsoft Teams Integration**:
   a) **MS Teams External System**: this attribute can take the following values: **Disabled**, **<external Systems that have been configured in JAAS file>**.
   b) **MS Teams Account** (usename@domain): this attribute can take the following values: **Use E-mail address 1**,**Use E-mail address 2**, **User Attribute** or **LDAP Attribute**.

> **NOTICE:** The presence of **MS Teams Connector** option indicates that the MS Teams is configured at Openscape UC. Instructions to configure MS Teams Presence may be found at *OpenScape UC Application V10, Configuration and Administration, Administrator Documentation, Chapter: Synchronising the MS Teams Presence with Openscape UC*.

7) Fill in the remaining Resource attributes to create a new OpenScape UC Application Resource.
8) Click **OK** to save the data.

   System verifies that supplied information is correct and all required attributes are filled in.
9) On the pop-up window **Assign Resource – Resource Center**, click **OK** to save the UC Resource changes.

   System stores the supplied Resource information in the Resource list, under the **Resources** tab.
10) Click **Save** to save changes to the UM User.

    The pop-up window closes and you are back to the **User Management** > **Administration** > **Users&Resources**.

> **IMPORTANT:**
>
> When setting an OpenScape Voice or OpenScape Voice Softphone resource as webRTC, the OpenScape Voice or OpenScape Voice Softphone subscriber is automatically set as Trusted.

11) System creates the UC Resource and assigns it to the UM User.
    - The newly created UC Resource appears in the column **Resources**, within the UM Users list.

10.1.4.7 How to Create an External Resource

This Chapter describes the configuration of default values for External Resource.

Prerequisites

Adequate administrative permission that allows creation of UM Users and Resource.

Step by Step

1) Navigate to **Assign Resource – Resource Center** pop-up window, following the first four steps from the Chapter How to Create a Resource or Select an existing one.

   Only the types of Resources that are supported in the specific deployment are displayed.
2) Click on **Add** to create a new External Resource to the UM User.

   A pop-up window **Add External Resource** is displayed.
3) Fill in the Name and Number (mandatory field which is validated against characters, only digits are allowed) External Resource attributes to create a new External Resource.
4) Click **OK** to save the data.

   System verifies that supplied information is correct and all required attributes are filled in.
5) On the pop-up window **Assign Resource – Resource Center**, click **OK** to save the External Resource changes.

   System stores the supplied Resource information in the Resource list, under the **Resources**.
6) Click **Save** to save changes to the UM User.

   The pop-up window closes and you are back to the **User Management** > **Administration** > **Users&Resources**.
7) System creates the External Resource and assigns it to the UM User.
   - The newly created External Resource appears in the column **Resources**, within the UM Users list.

10.1.4.8 How to Create a Unify Phone Resource

The UM Users can have various communications equipment (Resources) assigned. This chapter describes how to create a Unify Phone resource.

Prerequisites

1) Adequate administrative permissions.
2) An API Key for Unify Phone must be configured.
3) There must be at least one SBC configuration for Unify Phone users. For detailed steps, see How to Create a new SBC configuration for Unify Phone users on page 677.
4) The user must have an OpenScape Voice resource with OpenScape Mobile.

   To configure how to create an OpenScape Voice resource see How to Create an OpenScape Voice Resource or Select an existing one on page 412.

   To configure how to create an OpenScape Mobile resource see How to Create an OpenScape Mobile Resource on page 425.
5) The user must have either **Email address 1** or **Email address 2** configured. The email address is used as a unique identifier when creating a Unify Phone resource.

Step by Step

1) Click the **User Management** navigation tab.
2) In the navigation tree, click **AdministrationUsers & Resources**.

   A **Users & Resources** window opens, displaying the existing UM users.
3) Click the UM user for whom you want to create a Unify Phone resource.
   The **Edit User & Resources** window opens.
4) Click **Assign** under the **Resources** tab.
   The **Assign Resource - Resource Center** window opens.

   NOTICE:

   If the Unify Phone Settings have not been configured, a warning message is displayed: **Unify Phone Settings are not configured properly.** To configure the Unify Phone Settings, see Unify Phone Configurations on page 677 .
5) Click **Add** under the **Unify Phone** area.
   The **Add Unify Phone resource** window opens.
6) From the **Tenant** drop-down menu, select the tenant for which you want to create the Unify Phone Resource.
7) From the **Configuration** drop-down menu, select the Unify Phone configuration.
8) Select the **Phone Number (ONS)**.
9) Click **OK**.
10) Click **Save** to save the settings.

    NOTICE: A warning message informs you that your business phone 1 number has been changed to your ONS number.

    The newly created resources are assigned to the user. The assigned resources are shown in the last column of the UM Users list.

10.1.4.9 How to Create a Zoom Resource

The UM Users can have various communications equipment (Resources) assigned. This chapter describes how to create a Zoom resource.

Prerequisites

1) Adequate administrative permissions
2) There must be at least one SBC configuration for Zoom users. For detailed steps, see How to Create a new Zoom configuration on page 684.
3) The user must have either Email address 1 or Email address 2 configured. The email address is used as a unique identifier when creating a Unify Phone resource.

Step by Step

1) Click the **User Management** navigation tab.

2) In the navigation tree, click **Administration** > **Users & Resources**.

   The **Users & Resources** page appears, displaying the existing UM users.

3) Click the UM user for which you want to create a Zoom resource.
   The **Edit User & Resources** window opens.

4) Click **Assign** under the **Resources** tab.
   The **Assign Resource - Resource Center** window opens.

5) Click **Add** under the **Zoom** area.
   The **Add Zoom resource** window opens.

6) From the **Configuration** drop-down list, select the Zoom configuration.

7) Select the **Phone Number (ONS)**.

8) Enter the **Voicemail**.

9) Click **OK**.

10) Click **Save** to save the settings.

NOTICE: A warning message informs you that your *Business phone 1* number has been changed to your *ONS number*.

The newly created resources are assigned to the user. The assigned resources are shown in the last column of the UM Users list.

10.1.5 How to Modify Users

This chapter describes how to Modify UM Users.

Prerequisites

Adequate administrative permission that allows modification of UM Users and Resources.

Step by Step

1) Navigate to **User Management** > **Administration** > **Users&Resources**.
   A list of the existing UM Users is displayed.

NOTICE: In case you are logged in as an UM Locality Administrator, system displays only the UM Users that belong to the Localities of this UM Locality Administrator.

---

2) Select to modify a UM User in one of the following ways:

   - Click on the **Last name** of UM User you want to modify.
   - Check the box in front of the UM User you want to modify and click **Edit**.
   - In the row of a respective UM User, click on ▸ to open application action menu and then select **Edit**.

   A pop-up window **Edit User & Resources** is displayed and system retrieves all UM User attributes that have been defined during the UM User creation.

3) Click on **General** tab.

NOTICE: User ID attribute is a read-only and after UM User is created, it can not be modified.

NOTICE:

The list of Resources, among others, displays the deviation of User's Resources from the linked User Template's rules.

The columns **Status** (hover over to see the status message) shows the current status of User's Resources to User Template association, whereas the column **Resource Function** represents the function (in case the Resource is associated with the User Template).

4) Fill in, or modify the remaining UM User attributes, found under two application tabs (**General** and **Advanced**).

NOTICE: The UM User attributes that are mapped to the LDAP attributes as shown as read-only. The administrator is allowed to modify only the UM User attributes that are not synchronized with the LDAP, because once the synchronization occurs, these attributes will be overwritten.

- To modify UM User **Locality**, click ... to choose a new **Locality** from the list of available localities.

NOTICE: In case you are logged in as an UM Locality Administrator, system lists only the Localities of the UM Locality Administrator in the UM Users Locality selection.

System informs that the attributes under the **Address** tab will be updated with the address information specified in the selected **Locality**.

NOTICE: This behavior is specific for the manual creation/modification of the UM Users. In general, when the Locality attribute of one UM User is modified (e.g. via

LDAP synchronization), the address related attributes are not modified.

- Click **Browse** to modify (select and upload a new) **Photo** of the UM User.

NOTICE:

Regarding the size of the photography, there is a restriction that does not allow to assign photos larger than16384 bytes.

If the UM User's photo is already uploaded, system provides an option to **Clear** the photo, or **View** it in a new window.

- To modify UM User **Resources** and:

a) to create a new Resource for the UM User, click **Assign** (see How to Create a Resource or Select an existing one).

b) to assign existing Resource to the UM User, click **Assign** and after that click ... . For more information, see How to Create a Resource or Select an existing one.

c) to edit Resource that is already assigned to the UM User, in the row of a respective Resource, click on ▸ to open application action menu and then select **Edit** (see How to Modify Users' Resources).

d) to remove (unassign/delete) existing Resource from the UM User, in the row of a respective Resource, click on ▸ to open an application action menu and then select **Unassign** (see How to Delete or Unassign User's Resources).

5) On the pop-up window **Edit User & Resources**, click **Save** to save the changes to the UM User attributes.

The System...

a) ... verifies that supplied information is correct and all required attributes are filled in.

b) ... creates a new Resource for the UM User.

c) ... assigns the existing Resources to the UM User.

d) ... removes (unassign/delete) the Resources from the UM User.

e) ... updates UM User using the supplied information.

6) Click the **Visibility Groups** tab. Here you can see the connected Visibility Groups.

IMPORTANT:

The Visibility Groups tab appears only when:

The Visibility Groups have been created in UC

The user has been assigned UC resources

7) To connect the user to a new Visibility Group, click **Connect...** A new pop-up window **Connect Visibility Groups to User** appears. Here you can see a list with only the Visibility Groups that are not yet connected to the UM User. Select one or more Visibility Groups from the list and click **OK**

8) To disconnect the user from a Visibility Group, select one or more from the list of **User's Visibility Groups** and click **Disconnect**.

9) System applies changes to UM User attributes.

The UM User has been modified and displayed in the UM Users list.

10.1.6 How to Modify Users' Resources

The following procedure describes how to Modify UM Users' Resources.

Prerequisites

Adequate administrative permission that allows modification of UM Users and Resources.

Step by Step

1) Navigate to **User Management** > **Administration** > **Users&Resources**. A list of existing UM Users is displayed.

   NOTICE: In case you are logged in as an UM Locality Administrator, system displays only the UM Users that belong to the Localities of this UM Locality Administrator.

2) Select to modify a UM User in one of the following ways:
   - Click on the **Last name** of UM User you want to modify.
   - Check the box in front of the UM User you want to modify and click **Edit**.
   - In the row of a respective UM User, click on ▸ to open application action menu and then select **Edit**.

   A pop-up window **Edit User & Resources** is displayed.

3) Navigate to the **Resources** area.

   A list of all Resources assigned to the specific UM User is displayed.

   NOTICE:

   The list of Resources, among others, displays the deviation of User's Resources from the linked User Template's rules.

   The columns **Status** (hover over to see the status message) shows the current status of User's Resources to User Template association, whereas the column **Resource Function** represents the function (in case the Resource is associated with the User Template).

4) In the row of a respective Resource, click on ▸ to open the application action menu and then select **Edit**.

   A pop-up window corresponding to the specific Resource type is displayed.

   NOTICE:

   For OpenScape Voice Resource, OpenScape Voice Softphone Resource and OpenScape 4000 Resource, in the row of a respective UM User, you can click on ▸ to open application action menu and then select **Change Name** in case you want to modify the Resource Name attribute.

5) The System retrieves all Resource attributes that have been defined once the UM User is created.
   a) In case the administrator selects to configure a Xpressions resource, that has been already assigned to the UM User, a new window (Xpressions account configuration screen) will be automatically opened. The current Xpressions resource will appear in Xpressions Web Assistant and due to the Single Sign-On mechanism, no username/password is required.
   b) In case the administrator selects to configure an OpenScape Voice or OpenScape Voice Softphone resource that have been assigned to the UM User, a new window (OpenScape Voice Assistant resource configuration screen) will be automatically opened.
6) Fill in the values of the Resource attributes that haven't been defined before, or modify existing Resource attributes.
   a) Whenever Xpressions Web Assistant is used to add a new, modify or delete an existing Xpressions resource, an event is sent to CMP, triggering the synchronization of the new/modified/deleted Xpressions resources to CMP/UM database. Consequently, CMP creates, updates or deletes the specified Xpression resource.

      In case the connection to the Xpression server fails and Xpressions resources in the CMP are not aligned with the Xpression server data, the administrator has to manually trigger the Xpressions node synchronization process (navigate to **Maintenance** > **Inventory** > **Nodes & Application** > **Nodes**, in the In the row of a respective **Xpressions** node click on the application action menu and then select **Synchronize**).

      IMPORTANT:

      The **Groupware Assignment** option indicates whether the Groupware connector is configured or not.

      In case the UC resource (you want to modify) has a Groupware assignment, but the connector has been removed, the system will displays the UC resource as it has been saved, i.e., with the Groupware and it will allow modification of the UC resource. You will be able either to select a different groupware connector or disable the groupware (if there are no other groupware connectors in the system).

      ---

7) Depending of the previously selected Resource type you wanted to modify, click **OK**, or **Save** to save the data.

   System verifies that supplied information is correct and that all required attributes are filled in.
8) On the pop-up window **Edit User & Resources**, click **Save** to save changes to the Resource attributes.
   a) In case you explicitly assign a Resource to a User who already has assigned Resources that are linked with a User Template, the dissociation of the User from the User Template will take place, because a User may need special configuration that is not covered by any of the available User Templates.

      System removes the User Template to Resource association from all the User's Resources and updates the User to User Template association for the modified User.

b) in case you explicitly un-assign a Resource from a User who already has Resources assigned and linked with a User Template, the dissociation of the User with the User Template will take place, because a User may need special configuration not covered by any of the available User Templates.

System unassigns the Resource from the User, removes the User Template to Resource association from all the User's Resources and updates the User to User Template association for the modified User.

The System updates Resource using newly supplied information.

9) System applies changes to UM User.

The UM Users' Resources have been modified and displayed in the UM Users list.

Next steps

The User's Resources will be updated:

1) after changes in the User's data (the User should be associated with a User Template)

2) after changes in the User's assigned Locality (the modified Locality should be assigned to one or more Users).

To define how to handle the Resources that are already assigned to a User but are not defined in the User Template, choose one of the following options:

1) • **associate the User with the User Template without affecting the additional resources**

(resources that were previously manually assigned to a User or applied with a different User Template will stay intact)

• **un-assign the additional resources**

(resources that were previously manually assigned to a User or applied with a different User Template will be unassigned)

• **un-assign and delete the additional resources**

(resources that were previously manually assigned to a User or applied with a different User Template will be unassigned and deleted).

• **un-assign phones and delete other resources**

Un-assign resources of specific type and delete resources of other types

(resources that were previously manually assigned to a User or applied with a different User Template will be unassigned and deleted).

NOTICE:

When a User Template with Xpressions Resources is applied to a User and a modification in the User Template takes place where only the User ID field in the User Template has been changed, then the **un-assign and delete the additional resources** rule is only applied, even if any other choice has been selected.

The system will apply the User Template rules for:

1) each Resource that was affected by the modified User's contact data

2) each Resource that was modified in the Locality
3) each User that was assigned to the modified Locality.

10.1.6.1 How to Modify Users' Attributes in the bulk mode

This chapter explains how to modify the UM User attributes by performing bulk editing operation.

Prerequisites

Adequate administrative permission that allows modification of UM Users and Resources.

Step by Step

1) Navigate to **User Management** > **Administration** > **Users&Resources**. A list of existing UM Users is displayed.

   NOTICE: In case you are logged in as an UM Locality Administrator, system displays only the UM Users that belong to the Localities of this UM Locality Administrator.

2) Select to edit UM Users' attributes for:
   - more than one UM User, by checking the box in front of these Users
   - select all UM Users by choosing the option "All" (this option is visible only when the number of items in the UM User list is bigger than the number of items per page).

   Button **Edit** is enabled now.
3) Click **Edit**.

   A pop-up window **Bulk Edit Users** is displayed.
4) Modify one or more UM Users' attributes (see the table below). All attributes are divided into two groups:
   - The attributes that are disabled and do not support Bulk edit.

     NOTICE:

     All Resource related attributes and operations are disabled.
   - The UM Users attributes that support Bulk edit and they are disabled with an option to become enabled.

     When enabled, any value provided in these attributes (fields) shall be applied to all selected UM Users. If the field is empty, the value that belongs to the selected UM Users shall be erased (this is applicable to the fields that allow empty values).

Table 14: User Attributes bulk edit behavior

Attribute	Bulk Edit	Empty value allowed
User ID	no	not available
Display name	no	not available

Attribute	Bulk Edit	Empty value allowed
Last name	no	not available
First Name	no	not available
E-mail address 1	no	not available
Business phone 1	no	not available
Locality	yes	yes
Photo	yes	yes
Notice	yes	yes
Middle Name	yes	yes
Gender	no	not available
Solution	yes	yes
Title	yes	yes
Language	yes	no
Description	yes	yes
Home time zone	yes	no
Country	yes	yes
State or Province	yes	yes
City	yes	yes
Postal Code	yes	yes
Company	yes	yes
Department	yes	yes
Building	yes	yes
Room	yes	yes
Street	yes	yes
Business phone 2	no	not available
Mobile phone	yes	yes
Home phone	yes	yes
FAX number	yes	yes
E-mail address 2	yes	yes
IM address	yes	yes
Home URL	yes	yes

NOTICE:

When you are bulk editing the Organizational Structures, you can only use the **Update User's Organizational Structure** radio button, either when creating or assigning organizational structures. The radio button **Update current Organizational Structure for all Users** is greyed out.

5) Click **Save** to save changes to the attributes.

INFO: In case no UM Users' attributes have been modified, system displays the following message: `In order to save the changes, at least one attribute must be modified`. System displays the **Bulk Edit Users** screen.

System displays the progress of the operation.

6) Click **Cancel** to stop an ongoing operation.

System completes all operations which are pending for the current UM User and also does not roll-back any performed operation.

7) Upon completion, or cancellation of bulk edit operation, a **Bulk Edit Users - Report** window is displayed, containing the following information:

- Number of successfully modified UM Users
- Number of UM Users that failed to be edited

System updates users' attributes using the supplied information.

8) Click **Download Report** to download a log file with the details of the latest performed operation.

A log file contains information such as: Date and Time of the operation, Number of Users selected for modification, the attributes that are going to be modified and their selected values, etc.

NOTICE:

Log files are stored on the server, under the following

path:

- **for integrated Simplex =** `/log/OSCUM/`

- **for all other deployments =** `/var/siemens/common/log/OSCUM/`

---

9) Click **Close** to close the **Bulk Edit Users - Report** window.

The UM Users' attributes have been modified by performing the Bulk edit operation.

10.1.7 Moving Resources (OpenScape 4000 Resource)

One of the most common operations performed in OpenScape 4000 network is the move of OpenScape 4000 station from one location to another. Depending on the OpenScape 4000 network configuration and the OpenScape 4000 station type, there are various types of move operations (for more information, refer to OpenScape 4000 Manager V7, previously known as HiPath 4000 Manager, user documentation).

So far, moving of OpenScape 4000 Resource was possible either with the OpenScape 4000 Manager or with HiPath User Management.

A new feature in OpenScape User Management supports move operations for OpenScape 4000 resources that are assigned to the users. It ensures that any other user's resource (e.g., OpenScape UC Application ONS, or Xpressions

voice mail) that is affected by OpenScape 4000 Resource move operation, will be updated accordingly.

NOTICE:

The following operations are not supported in OpenScape User Management:

- Two-phase move operation for OpenScape 4000 station.

(Two-phase move includes: the first phase, during which a temporary station is created and assigned the new PEN and the second phase, in which the temporary station is replaced by the station that is going to be moved. Also, the old PEN is deleted.)

- The move of an Xpressions resource to a different Xpressions server after the OpenScape 4000 Resource move operation.

- Simultaneous connection of OpenScape 4000 Manager to both, HiPath User Management and OpenScape User Management.

10.1.7.1 How to Move an OpenScape 4000 Resource

The following procedure describes how to move an OpenScape 4000 Resource and let the system automatically update those User's resources that are affected by the move operation.

Prerequisites

Adequate administrative permission that allows modification of UM Users and Resources.

Step by Step

1) Navigate to **User Management** > **Administration** > **Users&Resources**. A list of existing UM Users is displayed.

   NOTICE: In case you are logged in as an UM Locality Administrator, system displays only the UM Users that belong to the Localities of this UM Locality Administrator.

2) Select to move the User’s OpenScape 4000 Resource, in one of the following ways:

   - Click on the **Last name** of UM User you want to modify.
   - Check the box in front of the UM User you want to modify and click **Edit**.
   - In the row of a respective UM User, click on ▸ to open application action menu and then select **Edit**.

   A pop-up window **Edit User & Resources** is displayed.

3) Navigate to the **Resources** area.

   A list of all Resources assigned to the specific UM User is displayed.

4) In the row of a respective OpenScape 4000 Resource, click on ▸ to open the application action menu and then select **Move**.
   a) The System verifies that the selected resource belongs to a switch that is managed by a HiPath 4000 Manager Version 7 or higher, or to a self managed HiPath 4000 Version 7 or higher.

> **NOTICE:**
>
> In case the selected OpenScape 4000 Resource belongs to a HiPath 4000 Version 6 or lower, or it is managed by a HiPath 4000 Manager Version 6 or lower, system will display an error message and not allow moving of OpenScape 4000 Resource.

   A pop-up window **Move OpenScape 4000 Station** is displayed.

5) Select to perform one of the following move operations:
   - **Change only station PEN** (see How to Change PEN for an OpenScape 4000 Resource)
   - **Move station** (see How to Move an OpenScape 4000 Resource using wizard).

> **NOTICE:** In case move operation requires additional manual steps, an external link will be provided in order to accomplish this move operation. All the resources (i.e., OpenScape UC Application Resource or OpenScape Xpressions Resource) that are linked to the selected OpenScape 4000 Resource have to be updated manually.

   a) In case you want to explicitly move (migrate) an OpenScape 4000 Resource of a User who is linked with a User Template, this will lead to the dissociation of the User with the User Template.

      System will move (migrate) an OpenScape 4000 Resource, removes the User Template to Resource association from all the User's Resources and updates the User to User Template association for the modified User.

6) The System:
   a) triggers a delta sync request in order to update the OpenScape UC Application Resource database.

      This action ensures that the OpenScape UC Application Resource that is assigned to the User will be implicitly updated to use the new OpenScape 4000 Resource.
   b) updates the User’s OpenScape Xpressions Resource (that used the OpenScape 4000 Resource which was moved) to use the new OpenScape 4000 Resource (see the **Next steps** at the end of this Chapter).
   c) displays the summary of the performed operations, i.e., if the move operation for the selected OpenScape 4000 Resource was successful and if the User's OpenScape UC Application Resource and OpenScape

Xpressions Resource, that used the OpenScape 4000 Resource, were successfully updated.

NOTICE:

In case multiple OpenScape Xpressions Resource are assigned to the User and are affected by the OpenScape 4000 Resource move, the outcome of each Xpression Resource will be displayed in a separate line along with the resource identifier.

The selected OpenScape 4000 Resource has been successful moved.

Next steps

Once the OpenScape 4000 Resource is successfully moved and its DN modified, the OpenScape Xpressions Resource that was linked to this OpenScape 4000 Resource, has to be updated.

The system:

- verifies that the OpenScape Xpressions Resource assigned to the User is linked to the moved OpenScape 4000 Resource
- verifies that the OpenScape 4000 Resource DN is modified
- verifies that the Voice mail attribute of the OpenScape Xpressions Resource contains the old OpenScape 4000 Station extension (or the old OpenScape 4000 Station E.164 number)
- informs that the corresponding OpenScape Xpressions Resource must be updated and that a new Xpressions group must be manually selected.

  From the drop-down list, choose the new Xpressions group, so that the system can update OpenScape Xpressions Resource and click **Update** button.

  NOTICE:

  If you click **Cancel** and close the group selection window, no updates of the OpenScape Xpressions Resource will be performed.

- updates the following fields in the OpenScape Xpressions Resource:
  - Voice mail number
  - CTI number (if it is configured)
  - MWI (Message Waiting Indication) field (if it is configured).

10.1.7.2 How to Move an OpenScape 4000 Resource using wizard

In order to easily perform the OpenScape 4000 Resource move operation use the wizard that will take you through various move options (e.g., change physical switch, Dial Plan, PEN).

Prerequisites

Adequate administrative permission that allows modification of UM Users and Resources.

Step by Step

1) Navigate to **User Management** > **Administration** > **Users&Resources**. A list of existing UM Users is displayed.

> **NOTICE:** In case you are logged in as an UM Locality Administrator, system displays only the UM Users that belong to the Localities of this UM Locality Administrator.

2) Select to move the User's OpenScape 4000 Resource, in one of the following ways:

- Click on the **Last name** of UM User you want to modify.
- Check the box in front of the UM User you want to modify and click **Edit**.
- In the row of a respective UM User, click on ▸ to open application action menu and then select **Edit**.

A pop-up window **Edit User & Resources** is displayed.

3) Navigate to the **Resources** area.

A list of all Resources assigned to the specific UM User is displayed.

4) In the row of a respective OpenScape 4000 Resource, click on ▸ to open the application action menu and then select **Move**.

a) The System verifies that the selected resource belongs to a switch that is managed by a HiPath 4000 Manager Version 7 or higher, or to a self managed HiPath 4000 Version 7 or higher.

> **NOTICE:**
>
> In case the selected OpenScape 4000 Resource belongs to a HiPath 4000 Version 6 or lower, or it is managed by a HiPath 4000 Manager Version 6 or lower, system will display an error message and not allow moving of OpenScape 4000 Resource.

A pop-up window **Move OpenScape 4000 Station** is displayed.

5) To perform move operation using wizard, select the option **Move station**.

> **NOTICE:** In case move operation requires additional steps by the administrator, an external link will be provided in order to accomplish this move operation. Also, each resource (i.e., OpenScape UC Application Resource or OpenScape Xpressions Resource) that is linked to the selected OpenScape 4000 Resource have to be updated manually.

6) Select the switch by choosing one of the following options:

- **Stay on the same physical switch**
- **Change physical switch**

  From the list of all the physical switches that are available in the current OpenScape 4000 Manager domain choose one of the switches.

  IMPORTANT:

  In order to change physical switch both switches have to be managed by the same OpenScape 4000 Manager Version 7 or higher.

- **Change subswitch**

  From the list of all the sub-switches that are available in the current VNR (Virtual Numbering Plan) switch, choose one of the sub-switches.

  IMPORTANT:

  This option is available only if the selected OpenScape 4000 Resource belongs to a VNR switch.

7) Click **Next**.

System retrieves the list of all the Virtual Nodes that are available in the selected switch.

In case the VNR sub-switch, which has a single VN available, was selected, the system will skip the VN selection step (8) and directly move to Dial Plan selection step (9).

NOTICE:

If the option **Stay on the same physical switch** was selected, the Virtual Node where the resource currently belongs to will be preselected in the drop-down list.

In all other cases, the default Virtual Number of the selected switch will be preselected in the list.

8) Select the Virtual Node and click **Next**.

System displays the list of available Dial Plans for the selected Virtual Node.

NOTICE:

If Virtual Node has not been changed, the Dial Plan that resource currently has will be preselected in the drop-down list.

Otherwise, the default Dial Plan of the selected Virtual Node will preselected in the list.

9) Select the Dial Plan and click **Next**.

   System displays the available options for PEN.

   In case the VNR sub-switch was selected and you choose to return to the previous step, the system will skip the VN selection (step 8) and directly move to Switch selection (step 6).

10) Choosing one of the following options for PEN (for more details related to PEN, see the Chapters: How to Create a OpenScape 4000 Resource or Select an existing one and How to Change PEN for an OpenScape 4000 Resource):

   - **Do not change PEN**
   - **Select the first available PEN on:**

     - **any shelf/IPDA**

     - **a specific shelf/IPDA**
   - **Set the PEN manually**

11) Click **Move resource** button to start the OpenScape 4000 Resource move operation.

NOTICE:

In order to perform OpenScape 4000 Resource move operation, at least one of the aforementioned attributes has to be modified. Otherwise, the system will display an error message.

NOTICE:

In case you want to explicitly move (migrate) an OpenScape 4000 Resource of a User who is linked with a User Template, this will lead to the dissociation of the User with the User Template.

System will move (migrate) an OpenScape 4000 Resource, removes the User Template to Resource association from all the User's Resources and updates the User to User Template association for the modified User.

---

12) The System:

   a) triggers a delta sync request in order to update the OpenScape UC Application Resource database.

      This action ensures that the OpenScape UC Application Resource that is assigned to the User will be implicitly updated to use the new OpenScape 4000 Resource.

   b) updates the User’s OpenScape Xpressions Resource (that used the OpenScape 4000 Resource which was moved) to use the new OpenScape 4000 Resource.

   c) displays the summary of the performed operations, i.e., if the move operation for the selected OpenScape 4000 Resource was successful and if the User's OpenScape UC Application Resource and OpenScape

Xpressions Resource that used the OpenScape 4000 Resource, were successfully updated.

NOTICE:

In case multiple OpenScape Xpressions Resource are assigned to the User and are affected by the OpenScape 4000 Resource move, the outcome of each Xpression Resource will be displayed in a separate line along with the resource identifier.

The selected OpenScape 4000 Resource has been successful moved.

Next steps

Once the OpenScape 4000 Resource is successfully moved and its DN modified, the OpenScape Xpressions Resource, that was linked to this OpenScape 4000 Resource, has to be updated.

The system:

- verifies that the OpenScape Xpressions Resource assigned to the User is linked to the moved OpenScape 4000 Resource
- verifies that the OpenScape 4000 Resource DN is modified
- verifies that the Voice mail attribute of the OpenScape Xpressions Resource contains the old OpenScape 4000 Station extension (or the old OpenScape 4000 Station E.164 number)
- informs that the corresponding OpenScape Xpressions Resource must be updated and that a new Xpressions group must be manually selected.

  From the drop-down list, choose the new Xpressions group, so that the system can update OpenScape Xpressions Resource and click **Update** button.

  NOTICE:

  If you click **Cancel** and close the group selection window, no updates of the OpenScape Xpressions Resource will be performed.

- updates the following fields in the OpenScape Xpressions Resource:
  - Voice mail number
  - CTI number (if it is configured)
  - MWI (Message Waiting Indication) field (if it is configured).

10.1.7.3 How to Change PEN for an OpenScape 4000 Resource

The PEN (Port Equipment Number) for the OpenScape 4000 Resource can be changed either manually or automatically, both when creating as well as when moving the OpenScape 4000 Resource.

Prerequisites

Adequate administrative permission that allows modification of UM Users and Resources.

Step by Step

The following options are provided:

a) Choose to **Select the first available PEN**:

- regardless of shelf/IPDA (i.e., the option **any shelf/IPDA**). The system will select the first available PEN in the designated shelf/IPDA.

- specifying the shelf/IPDA for the new PEN (i.e., the option **a specific shelf/ IPDA**).

b) Select the option to **Set the PEN manually** and click ... to open the list of all available PENs. This list supports sorting and filtering based on the PEN number.

Once the PEN is selected, click **OK** to commit your changes.

NOTICE:

In case you are performing the OpenScape 4000 Resource move, click the button **Move resource** to start the move operation.

Otherwise (in case of OpenScape 4000 Resource creation), click the button **OK**.

The PEN for the selected OpenScape 4000 Resource has been changed.

10.1.8 How to Delete Users

This chapter describes how to delete the UM Users, where UM Users' Resources can be either unassigned, or unassigned and completely deleted from the respective system. At he moment the last assigned resource is successfully unassigned from an UM User, the system releases consumed UM User licenses and removes any other access right that this User may have on the system. Currently, the CMP Admin User rights are removed. In case any additional, unknown Profiles are detected, system does not allow the deletion of UM Users.

Prerequisites

Adequate administrative permission that allows deletion of UM Users and Resources.

Step by Step

1) Navigate to **User Management** > **Administration** > **Users&Resources**. A list of existing UM Users is displayed.

NOTICE: In case you are logged in as an UM Locality Administrator, system displays only the UM Users that belong to the Localities of this UM Locality Administrator.

---

2) Select to delete one or more UM Users in one of the following ways:
   - Check the box in front of the UM Users you want to delete and click **Delete**.
   - In the row of a respective UM User, click on ▸ to open an application action menu and then select **Delete**.

   A pop-up window **Delete Users** is displayed.
3) Select one of the following options and click **OK**:
   - **Unassign resources**
   - **Unassign and also delete resources**.
   - **Unassign phones and delete other resources**.

   System requests verification to delete the UM User(s).

   IMPORTANT:

   IP Device and Mobile User resources are automatically unassigned, whether they are selected or not, when the associated OpenScape Voice, OpenScape Voice Softphone or OpenScape 4000 resources are unassigned via CMP UM.

4) Click **OK** to verify deletion.

   System displays the progress of the operation.

   a) **If** the option **Unassign resources** has been chosen, system:
      - verifies that Profiles assigned to the UM User include:
        - UM Profile
        - Profiles that belong to the OpenScape UC Application (in case, the UC Resource is assigned to the UM User)
        - Profiles that belong to the E/A-Cockpit Application
        - CMP Admin User Profiles
      - unassigns any OpenScape UC Application Profile assigned to the UM User and releases any consumed license.
      - unassigns any E/A-Cockpit Application Profile assigned to the UM User and releases any consumed license.
      - unassigns the UM Profile and any CMP Admin User Profiles from the UM User.
      - unassigns corresponding Resources assigned to the UM User.

   b) **If** the option **Unassign and also Delete resources** has been chosen, system:
      - performs the same actions described for **Unassign resources** option.
      - completely deletes corresponding Resources assigned to the UM User from the respective system.

      NOTICE:

      An UM User license will be released at the moment the last assigned resource is successfully unassigned from an UM User. In case there are still resources assigned to the User, the consumed UM User license will not be released.

5) Click **Cancel** to stop an ongoing operation.

   System completes all operations which are pending for the current UM User and also does not roll-back any performed operation.

6) Upon completion, or cancellation of delete operation, a **Delete Users - Report** window is displayed, containing the following information:

   - Number of successfully deleted UM Users
   - Number of UM Users that failed to be deleted

   System deletes the UM User(s) from the UM Users list.

7) Click **Download Report** to download a log file with the details of the latest performed operation.

   A log file contains information such as: Date and Time of the operation, Number of Users selected for deletion, a summary of the performed operation, etc.

   NOTICE:

   Log files are stored on the server, under the following

   path:

   - **for integrated Simplex =** `/log/OSCUM/`

   - **for all other deployments =** `/var/siemens/common/log/OSCUM/`

8) Click **Close** to close the **Delete Users - Report** window.

   The UM User(s) have been deleted from the UM Users list.

   NOTICE:

   When you delete a UM user with Administrator profiles assigned, the respective administrator will also be deleted.

IMPORTANT:

If the **Unassign phones and delete other resources** option is selected, IP Device & Mobile User resources are automatically unassigned along with the respective OpenScape Voice, OpenScape Voice Softphone or OpenScape 4000 resource.

10.1.9 How to Delete or Unassign User’s Resources

This chapter describes how to delete or unassign Resources from one specific UM User. The Resources can be either unassigned, or unassigned and completely deleted from the respective system.

Prerequisites

Adequate administrative permission that allows deletion/unassignment of UM Users and Resources.

Step by Step

1) Navigate to **User Management** > **Administration** > **Users&Resources**. A list of existing UM Users is displayed.

   NOTICE: In case you are logged in as an UM Locality Administrator, system displays only the UM Users that belong to the Localities of this UM Locality Administrator.

2) Select to delete/unassign Resources from the specific UM User, in one of the following ways:

   - Click on the **Last name** of UM User which Resources you want to delete/ unassign.
   - Check the box in front of the UM User and click **Edit**.
   - In the row of a respective UM User, click on ▸ to open application action menu and then select **Edit**.

   A pop-up window **Edit User & Resources** is displayed.

3) Navigate to **General** tab, **Resource** area.

   A list of all Resources assigned to the specific UM User is displayed.

4) Select to delete/unassign one or more Resources, in one of the following ways:

   - Check the box in front of the Resource you want to delete/unassign and click **Unassign**.
   - In the row of a respective Resource, click on ▸ to open application action menu and then select **Unassign**.

   A pop-up window **Unassign Resources** is displayed.

   NOTICE: A UM Locality administrator cannot assign/ unassign resources to Users from the User's resources list screen. Resources can be created only via User Templates.

   IMPORTANT:

   IP Device and Mobile User resources are automatically unassigned, whether they are selected or not, when the associated OpenScape Voice, OpenScape Voice Softphone or OpenScape 4000 resources are unassigned via CMP UM.

5) Click **OK** to unassign Resources from the UM User, without completely deleting them from the system.

   NOTICE: In case you want to unassign and completely delete Resources from the respective system, check the box **Also delete unassigned resources** and then click **OK**.

6) System displays the action to be performed and requests verification for the deletion/unassignment of UM User Resources.

7) Click **OK** to verify deletion/unassignment.

   System checks that selected Resources can be unassigned/deleted and performs the action.

   NOTICE:

   In case the UC or Unify Phone Resources are selected for deletion, this is the first type of Resource that is removed in order to release any assigned ONS numbers.

   Also, when removing the UC Resource and the Groupware connector is configured, the User Assignment shall also be removed.

   INFO: If one of the selected Resources is marked as an ONS, system does not modify it.

8) Back to the window **Edit User & Resources**, click **Save** to save changes made to the UM User.

   NOTICE:

   An UM User license will be released at the moment the last assigned resource is successfully unassigned from an UM User. In case there are still resources assigned to the User, the consumed UM User license will not be released.

   The Resources have been deleted/unassigned from the UM User.

10.1.9.1 How to Delete or Unassign Users' Resources in bulk mode

This chapter describes how to perform "bulk" action over the UM Users' Resources. The Resources can be either unassigned from the UM User, or unassigned and completely deleted from the respective system. At he moment the last assigned resource is successfully unassigned from an UM User, the system releases consumed UM User licenses and removes any other access right that this User may have on the system.

Prerequisites

Adequate administrative permission that allows deletion/unassignment of UM Users and Resources.

Step by Step

1) Navigate to **User Management** > **Administration** > **Users&Resources**. A list of existing UM Users is displayed.

   NOTICE: In case you are logged in as an UM Locality Administrator, system displays only the UM Users that belong to the Localities of this UM Locality Administrator.

2) On the UM Users list, check the box in front of the UM Users which Resources you want to delete/unassign and then click **Unassign Resources**.

A pop-up window **Unassign Resources** is displayed.

NOTICE: A UM Locality administrator cannot assign/ unassign resources to Users from the User's resources list screen. Resources can be created only via User Templates..

---

3) Select either to unassign the Resources, or to unassign and completely delete them from the respective system (see the options below) and click **OK**:

- **Select types to unassign:**

  - all types of assigned Resources

  - only one specific type of Resources

  - more than one type of Resources.

NOTICE: Selection is done among the available Resource types of the specific deployment.

IMPORTANT:

IP Device and Mobile User resources are automatically unassigned, whether they are selected or not, when the associated OpenScape Voice, OpenScape Voice Softphone or OpenScape 4000 resources are unassigned via CMP UM.

- **Also delete unassigned resources**

System displays the action to be performed and requests verification for the deletion/unassignment of UM User’s Resources.

NOTICE:

In case of UC Resources it is not possible just to unassign the resource, it will be deleted automatically if you select to unassing it from a user.

---

4) Click **OK** to verify deletion/unassignment.

a) System:

- checks that selected Resources can be unassigned/deleted and performs the action.

INFO: In case the UC or Unify Phone Resources are selected for deletion, this is the first type of Resources

that is removed in order to release any assigned ONS numbers.

INFO: If one of the selected Resources is marked as an ONS, system does not modify it.

- displays **Unassign Resources – Report**, with the summary about resource deletion/unassignment action

NOTICE:

An UM User license will be released at the moment the last assigned resource is successfully unassigned from an UM User. In case there are still resources assigned to the User, the consumed UM User license will not be released.

5) Click **Download Report** to download a log file with the details of the latest performed operation.

NOTICE:

Log files are stored on the server, under the following

path:

- **for integrated Simplex =** `/log/OSCUM/`

- **for all other deployments =** `/var/siemens/common/log/OSCUM/`

6) Click **Close**.

A pop-up window **Unassign Resources – Report** closes and you are back to **User Management** > **Administration** > **Users&Resources** screen.

The Resources have been unassigned from the UM Users, or unassigned and completely deleted from the respective system.

10.1.10 How to perform bulk operations with All UM Users

This Chapter introduces a new functionality that allows selection of all Users in the UM Users list in order to apply different bulk operations.

Prerequisites

Adequate administrative permission that allows Management of UM Users and Resources.

- **Column Settings** functionality has been enabled in order to customize the way the UM User list is displayed (column visibility can be adjusted).

IMPORTANT: Option "All" is visible only if the number of items in the UM User list is bigger than the number of items per page (see Column Settings in chapter How to Display Users).

Step by Step

1) Navigate to **User Management** > **Administration** > **Users&Resources**.
A list of the existing UM Users is displayed.

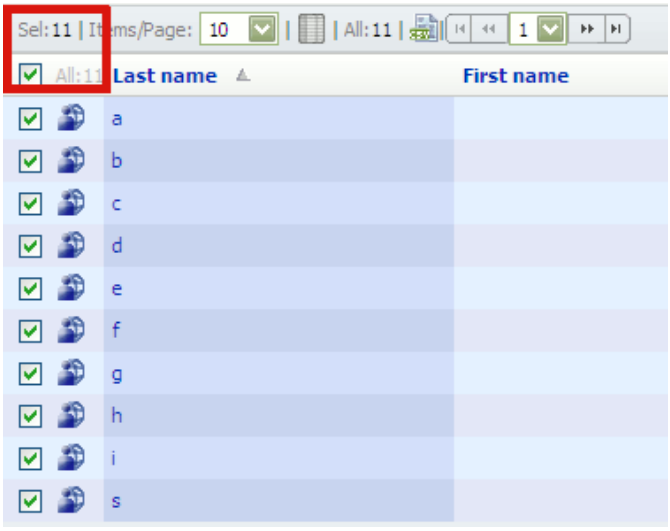
NOTICE: In case you are logged in as an UM Locality Administrator, system displays only the UM Users that belong to the Localities of this UM Locality Administrator.

---

2) Navigate to the UM Users list.

System displays the list of UM Users, sorted per first visible column in ascending order, according to the administrator's preferences.

Also, the Column header of the UM Users list shows the option "All" to select all UM Users (see picture below).



3) Click on the link **All**to select all Users in the UM User list.

System displays the number of all UM Users in the Selected item indicator.

IMPORTANT:

In case the administrator deselects an item in the current page, or he changes page, "All" option will be canceled and system will display the selected items in the current page in the selected item indicator.

---

4) Select to apply one of the following bulk operations for all UM Users:

- Bulk Edit UM User attributes (refer to How to Modify Users' Attributes in the bulk mode).
- Bulk create Resources using the User Templates (for more information see How to create Resource for selected Users based on the User Template).
- Delete UM Users (refer to How to Delete Users).
- Unassign/Delete UM Users' Resources (for more information see How to Delete or Unassign Users' Resources in bulk mode).

System applies the selected bulk operation on all UM Users, independent of paging.

10.1.11 Pickup and Hunt Groups within the User Management

OpenScape User Management has been enhanced to provide more convenient, User-Centric approach to Pickup and Hunt Groups for assigned OSV resources.

The management of Pickup and Hunt Groups is available in the "User" level, as well as in the "Resource" level, of each individual UM User. Based on this fact, the following operations are supported:

- Add UM User(s) and/or User Resources to Pickup Groups.
- Remove UM User(s) and/or User Resources from Pickup Groups.
- Add UM User(s) and/or User Resources to Hunt Groups.
- Remove UM User(s) and/or User Resources from Hunt Groups.
- Display Pickup Group/Hunt Group information in the UM Users List
- Display Pickup Group/Hunt Group information in the Resources list of the UM User screen
- Perform simple search for UM Users using Pickup/Hunt Group as criteria
- Perform advanced search for UM Users using Pickup/Hunt Group as criteria.

NOTICE:

Within the "Resource" level of a UM User, each individual resource that will be added to a group has to be selected.

The most common action related to Pickup and Hunt Group would be to create these groups for UM Users that have just one OSV resource assigned, or all of the OSV resources belonging to the same OSV Business Group.

More complex scenarios of UM Users having more than one OSV resource are also supported (in the User level), by allowing the administrator to select resources from the list of available resources, for each UM User.

NOTICE:

Combined scenarios (i.e. Pickup Groups that include both OSV and OpenScape 4000 resources), scenarios involving Pickup Groups containing subscribers from more than one OSV Business Group, as well as involving Pickup Groups containing subscribers from more than one OSV Communication System, are not currently supported by OpenScape UM.

NOTICE:

Though it is recommended to perform the Pickup and Hunt Group operations on 10 to 20 UM Users, there are no technical limitations on the number of UM Users that the administrator can select.

10.1.11.1 How to Add Users to a Pickup Group

This feature allows adding multiple UM Users to a new or existing Pickup Group, without managing Users' resource one by one.

Prerequisites

Adequate administrative permission that allows Management of UM Users and Resources.

All the Resources that are going to be added to the Pickup Group have been assigned to a User.

The Resource types that are going to be added to the Pickup Group are OSV subscribers only.

The Resources that are going to be added to the Pickup Group must belong to the same OSV Business Group.

A Resource can be added to the Pickup Group only if it is not already assigned to the Pickup Group. In other words, each Resource can be assigned to only one Pickup Group.

The Resources that are going to be added to a Pickup Group must belong to an OSV Switch that supports the BG/Pickup Group synchronization.

Step by Step

1) Navigate to **User Management** > **Administration** > **Users&Resources**. A list of the existing UM Users is displayed.

NOTICE: In case you are logged in as an UM Locality Administrator, system displays only the UM Users that belong to the Localities of this UM Locality Administrator.

---

2) Check the box in front of the UM User(s) you want to add to the Pickup Group.

3) Click on the button **More** and from the drop-down menu choose the **Add to Pickup Group** option.

a) If the OSV Resources of the selected User(s) belong to the different Business Groups, the **Add to Pickup Group - Multiple Business Group** dialog opens.

Select the Business Group and click **Next**.

b) If the User(s) have more than one OSV Resource that belongs to the same Business Group, the **Add to Pickup Group - Multiple resources available** dialog opens.

Select the UM Users Resource(s) and click **Next**.

The **Add to Pickup Group** dialog opens.

4) Select the Pickup Group:

- to add the User(s) to a new Pickup Group, choose **Create a new Pickup Group**.

  NOTICE:

  The **Group Number** is an integer number ranging from 1 to 10000.

- to add the User(s) to the existing Pickup Group, choose **Select an existing Pickup Group** and click ....

  NOTICE:

  In case the selected Business Group does not contain any Pickup Group, this option will be disabled.

  The **Select an existing Pickup Group** dialog opens.

  Select one of the existing Pickup Groups to add the selected Users and click **OK**.

  NOTICE:

  The Pickup Group list supports searching for **Group Name** or **Group Numbe**r.

5) Click **Save** to save the selected Pickup Group.
System:

a) • ensures that all selected UM Users can be added to the Pickup Group

• proceeds with the creation/modification of the Pickup Group.

The UM User(s) have been added to a newly created, or existing Pickup Group and this information is shown in the UM Users list, column **Groups**.

10.1.11.2 How to Add Users to a Hunt Group

This Chapter describes how to add multiple UM Users to a new or existing Hunt Group, without managing Users' resource one by one.

Prerequisites

Adequate administrative permission that allows Management of UM Users and Resources.

All the Resources that are going to be added to the Hunt Group have been assigned to a User.

The Resource types that are going to be added to the Hunt Group are OSV subscribers only.

The Resources that are going to be added to the Hunt Group must belong to the same OSV Business Group.

A Resource can be Hunt Group Pilot candidate only if it is not already a Pilot in another Hunt Group. Each Users' Resource can be assigned to more than one Hunt Group, but it can be Pilot in only one group.

The Resources that are going to be added to a Hunt Group must belong to an OSV Switch that supports the BG/Pickup Group synchronization.

Step by Step

1) Navigate to **User Management** > **Administration** > **Users&Resources**. A list of the existing UM Users is displayed.

NOTICE: In case you are logged in as an UM Locality Administrator, system displays only the UM Users that belong to the Localities of this UM Locality Administrator.

---

2) Check the box in front of the UM User(s) you want to add to the Hunt Group.

3) Click on the button **More** and from the drop-down menu choose the **Add to Hunt Group** option.

a) If the OSV Resources of the selected User(s) belong to the different Business Groups, the **Add to Hunt Group - Multiple Business Group** dialog opens.

Select the Business Group and click **Next**.

b) If the User(s) have more than one OSV Resource that belongs to the same Business Group, the **Add to Hunt Group - Multiple resources available** dialog opens.

Select the UM Users Resource(s) and click **Next**.

The **Add to Hunt Group** dialog opens.

4) Select the Hunt Group:

- to add the User(s) to a new Hunt Group, choose **Create a new Hunt Group**.

  NOTICE:

  In case that all selected Users' Resources are already Pilots in the Hunt Groups, this option will be disabled.

  NOTICE:

  The **Hunt Group Pilot Number** drop-down list contains UM User’s Lastname, Fistname and Resource Number of the Resources that are not already Pilots in a Hunt Group.

- to add the User(s) to the existing Hunt Group, choose **Select an existing Hunt Group** and click ....

  NOTICE:

  In case the selected Business Group does not contain any Hunt Group, this option will be disabled.

  The **Select an existing Hunt Group** dialog opens.

  NOTICE:

  The Hunt Group list supports searching for/ sorting by **Pilot Number** and **Name**.

  Select one of the existing Hunt Groups to add the selected Users and click **OK**.

5) Click **Save** to save the selected Hunt Group.
System:

   a) • ensures that all selected UM Users can be added to the Hunt Group
   • proceeds with the creation/modification of the Hunt Group.

The UM User(s) have been added to a newly created, or existing Hunt Group and this information is shown in the UM Users list, column **Groups**.

10.1.11.3 How to Remove Users from a Pickup Group

This feature allows removing multiple UM Users from a Pickup Group, without managing Users' resource one by one.

Prerequisites

Adequate administrative permission that allows Management of UM Users and Resources.

The Resource types that can be removed from the Pickup Group are OSV subscribers only.

The Resources that are going to be removed from the Pickup Group must belong to an OSV Switch that supports the BG/Pickup Group synchronization.

Step by Step

1) Navigate to **User Management** > **Administration** > **Users&Resources**. A list of the existing UM Users is displayed.

   NOTICE: In case you are logged in as an UM Locality Administrator, system displays only the UM Users that belong to the Localities of this UM Locality Administrator.

2) Check the box in front of the UM User(s) you want to remove from the Pickup Group.
3) Click on the button **More** and from the drop-down menu choose the **Remove from Pickup Group** option.
   a) If selected User(s) belong to Pickup Groups from different Business Groups, the **Remove from Pickup Group - Multiple Business Group** dialog opens.

      Select the Business Group and click **Next**.
   b) If selected User(s) belong to more than one Pickup Group, the **Remove from Pickup Group** dialog opens.

      Select the Pickup Group(s) and click **Next**.

   System displays the action to be performed and requests confirmation to remove the selected User(s) from the Pickup Group.
4) Click **OK** to confirm.

   System removes the selected User(s) from the corresponding Pickup Group.

   NOTICE:

   If all UM Users of one Pickup group have been removed, system provides the option to delete also the Pickup Group.

The UM User(s) have been removed from the Pickup Group and the column **Groups** of the UM Users list has been updated.

10.1.11.4 How to Remove Users from a Hunt Group

This Chapter describes how to remove multiple UM Users from a Hunt Group, without managing Users' resource one by one.

Prerequisites

Adequate administrative permission that allows Management of UM Users and Resources.

The Resource types that can be removed from the Hunt Group are OSV subscribers only.

The Resources that are going to be removed from the Hunt Group must belong to an OSV Switch that supports the BG/Pickup Group synchronization.

Step by Step

1) Navigate to **User Management** > **Administration** > **Users&Resources**. A list of the existing UM Users is displayed.

   NOTICE: In case you are logged in as an UM Locality Administrator, system displays only the UM Users that belong to the Localities of this UM Locality Administrator.

2) Check the box in front of the UM User(s) you want to remove from the Hunt Group.
3) Click on the button **More** and from the drop-down menu choose the **Remove from Hunt Group** option.
   a) If selected User(s) belong to Hunt Groups from different Business Groups, the **Remove from Hunt Group - Multiple Business Group** dialog opens.

      Select the Business Group and click **Next**.
   b) If selected User(s) belong to more than one Hunt Group, the **Remove from Hunt Group** dialog opens.

      Select the Hunt Group(s) and click **Next**.

      NOTICE:

      If some of the selected User(s) are Hunt Group Pilot(s), system displays a warning message saying that removing the Pilot will result in removing the whole Hunt Group.

   System displays the action to be performed and requests confirmation to remove the selected User(s) from the Hunt Group.
4) Click **OK** to confirm.

   System removes the selected Users' Resources from the corresponding Hunt Group.

   NOTICE:

   If some of the selected User(s) are Hunt Group Pilot(s), system will remove the whole Hunt Group.

The UM User(s) have been removed from the Hunt Group and the column **Groups** of the UM Users list has been updated.

10.1.11.5 How to Display Pickup and Hunt Group information in the UM Users list

This Chapter describes how to search and display the Pickup and Hunt Group related information of the UM User(s) without having to view each individual User's details.

Prerequisites

Adequate administrative permission that allows Management of UM Users and Resources.

The Resources belong to an OSV Switch that supports the BG/Pickup Group synchronization.

Step by Step

1) Navigate to **User Management** > **Administration** > **Users&Resources**.
   A list of the existing UM Users is displayed, sorted per first visible column in ascending order, according to the administrator's preferences.

   NOTICE: In case you are logged in as an UM Locality Administrator, system displays only the UM Users that belong to the Localities of this UM Locality Administrator.

   ---

2) Click **Column Settings** and select to display the **Groups** column of the UM Users list.

   System displays the following information in the **Groups** column:

   a) • Icon to show that at least one of the UM User's Resources belongs to the Pickup Group.

      When hovering over the Icon, the Pickup Group IDs (Pickup Group Number and Name) the Users' Resources belong to are displayed.

      • Icon to show that at least one of the UM User's Resources belongs to the Hunt Group, but no Resource is a Pilot of a Hunt Group.

      When hovering over the Icon, the Hunt Group IDs the Users' Resources belong to are displayed.

      • Icon to show that at least one of the UM User's Resources is a Hunt Group Pilot.

      When hovering over the Icon, the Hunt Group IDs the Users' Resources is Pilot to are displayed prefixed with the word "Pilot", while the Hunt Group ID the Users' resources belong to as members are displayed normally.

      NOTICE:

      Once any of the Pickup or Hunt Group related operations occur, the UM Users list becomes updated and instantly displays the current UM Users' Group status.

      ---

3) Click **Export data to CSV file** to export the UM Users list in a CSV format.

   System exports, in the separated columns, the information from the UM Users list regarding Pickup and Hunt Group.

4) Click **Search** to perform simple search operation using the following rule:

   `Search for:` <**User input**> `in` <**Attributes list**> `in` <**Locality list**> `with` <**Resource list**>.

   a) to search for the UM User(s) that belong to the specific Pickup Group provide a (part of the) Pickup **Group Number** or a (part of the) **Pickup Group Name** (wildcards are supported) and choose the **Pickup Group** from the **drop-down Attributes list**.

      System displays the UM User(s) that belong to the specified Pickup Group.

   b) to search for the UM User(s) that belong to the specific Hunt Group provide the Hunt **Group Name** or **Hunt Group Pilot Number** (entering

a part of it, or entering wildcards) and choose the **Hunt Group** from the **drop-down Attributes list**.

System displays the UM User(s) that belong to the specified Hunt Group.

5) Click **Advanced** to perform advanced search operations, specifying criteria for one or more UM Users attributes:

a) to add a Pickup Group as a criteria provide a (part of the) Pickup **Group Number** or a (part of the) **Pickup Group Name** (wildcards are supported) and choose the **Pickup Group** from the drop-down list.

NOTICE:

More than one Pickup Group can be added in the search criteria.

---

b) to add a Hunt Group as a criteria provide either a **Hunt Group Pilot Number** or a Hunt **Group Name** (entering a part of it, or entering wildcards) and choose the **Hunt Group** from the drop-down list.

NOTICE:

More than one Hunt Group can be added in the search criteria.

System displays the UM User(s) that satisfy Search criteria.

System displays the UM Users list, based on the new administrator's preferences.

10.1.11.6 How to Add User's Resources to a Pickup Group

This feature provides a way to add the UM User's Resource to a Pickup Group, without having to manage the actual Pickup Group.

Prerequisites

Adequate administrative permission that allows Management of UM Users and Resources.

The Resource types that are going to be added to the Pickup Group are OSV subscribers only.

The Resources that are going to be added to a Pickup Group must belong to an OSV Switch that supports the BG/Pickup Group synchronization.

Step by Step

1) Navigate to **User Management** > **Administration** > **Users&Resources**. A list of the existing UM Users is displayed (column **Resources** shows all the Resources assigned to the specific UM User).

NOTICE: In case you are logged in as an UM Locality Administrator, system displays only the UM Users that belong to the Localities of this UM Locality Administrator.

---

2) Click on the specific UM User within the list to have a closer look at the **Resources** assigned to this user.

   A pop-up window **Edit User & Resources** is displayed.

3) Navigate to the **General** tab, **Resources** area.

   A list of all Resources assigned to the specific UM User is displayed.

4) To add one of the UM Users' supported Resources to a Pickup Group, in the row of a respective Resource, click to open an Action menu and then select **Add to Pickup Group**.

   The **Add to Pickup Group** dialog opens.

5) Select the Pickup Group:

   - to add the User's Resources to a new Pickup Group, choose **Create a new Pickup Group**.

     NOTICE:

     The **Group Number** is an integer number ranging from 1 to 10000.

   - to add the User's Resources to the existing Pickup Group, choose **Select an existing Pickup Group** and click ....

     NOTICE:

     In case the selected Business Group does not contain any Pickup Group, this option will be disabled.

     The **Select an existing Pickup Group** dialog opens.

     Select one of the existing Pickup Groups to add the selected Users' Resource and click **OK**.

     NOTICE:

     The Pickup Group list supports searching for/ sorting by **Group Name** or **Group Numbe**r.

6) Click **Save** to save the selected Pickup Group.
   System:

   a) • ensures that the selected Resources can be added to the Pickup Group

   • proceeds with the modification of the Pickup Group.

The UM Users' Resource has been added to a newly created, or existing Pickup Group and this information is shown in the Resources list, column **Pickup Groups**, after the administrator saves and reopens the form.

10.1.11.7 How to Add User’s Resources to a Hunt Group

This Chapter describes how to add the UM User's Resource to a Hunt Group, without having to manage the actual Hunt Group.

Prerequisites

Adequate administrative permission that allows Management of UM Users and Resources.

The Resource types that are going to be added to the Pickup Group are OSV subscribers only.

A Resource can be Hunt Group Pilot candidate only if it is not already a Pilot in another Hunt Group. Each Users’ Resource can be assigned to more than one Hunt Group, but it can be Pilot in only one group.

The Resources that are going to be added to a Pickup Group must belong to an OSV Switch that supports the BG/Pickup Group synchronization.

Step by Step

1) Navigate to **User Management** > **Administration** > **Users&Resources**. A list of the existing UM Users is displayed (column **Resources** shows all the Resources assigned to the specific UM User).

   NOTICE: In case you are logged in as an UM Locality Administrator, system displays only the UM Users that belong to the Localities of this UM Locality Administrator.

2) Click on the specific UM User within the list to have a closer look at the **Resources** assigned to this user.

   A pop-up window **Edit User & Resources** is displayed.

3) Navigate to the **General** tab, **Resources** area.

   A list of all Resources assigned to the specific UM User is displayed.

4) To add one of the UM Users’ supported Resources to a Hunt Group, in the row of a respective Resource, click ▸ to open an Action menu and then select **Add to Hunt Group**.

   The **Add to Hunt Group** dialog opens.

   NOTICE:

   If the selected resource is a Hunt Group Pilot and the selected BG does not contain any Hunt Group other than the one this resource is Pilot in, system displays an error message. In order to add this Resource as a member to a Hunt Group, a new Hunt Group must be created.

5) Select the Hunt Group:

- to add the User's Resource to a new Hunt Group, choose **Create a new Hunt Group**.

  NOTICE:

  In case the selected Users' Resource is already a Pilot in the Hunt Group, this option will be disabled.

  NOTICE:

  The **Hunt Group Pilot Number** drop-down list contains UM User's Lastname, Fistname and Resource Number of the Resources that are not already Pilots in a Hunt Group.

- to add the User's Resource to the existing Hunt Group, choose **Select an existing Hunt Group** and click ....

  NOTICE:

  In case the selected Business Group does not contain any Hunt Group, this option will be disabled.

  The **Select an existing Hunt Group** dialog opens.

  NOTICE:

  The Hunt Group list supports searching for/ sorting by **Pilot Number** and **Name**.

  Select one of the existing Hunt Groups to add the selected Users' Resource and click **OK**.

6) Click **Save** to save the selected Hunt Group.
System:

a)
- ensures that all selected UM Users can be added to the Hunt Group
- proceeds with the creation/modification of the Hunt Group.

The UM Users' Resource has been added to a newly created, or existing Hunt Group and this information is shown in the Resources list, column **Hunt Groups**, after the administrator saves and reopens the form.

10.1.11.8 How to Remove User's Resources from a Pickup Group

This feature allows removing the UM User's Resource from a Pickup Group, without having to manage the actual Pickup Group.

Prerequisites

Adequate administrative permission that allows Management of UM Users and Resources.

The Resources that are going to be removed from the Pickup Group must belong to an OSV Switch that supports the BG/Pickup Group synchronization.

Step by Step

1) Navigate to **User Management** > **Administration** > **Users&Resources**. A list of the existing UM Users is displayed (column **Resources** shows all the Resources assigned to the specific UM User).

   NOTICE: In case you are logged in as an UM Locality Administrator, system displays only the UM Users that belong to the Localities of this UM Locality Administrator.

2) Click on the specific UM User within the list to have a closer look at the **Resources** assigned to this user.

   A pop-up window **Edit User & Resources** is displayed.

3) Navigate to the **General** tab, **Resources** area.

   A list of all Resources assigned to the specific UM User is displayed.

4) To remove one of the assigned UM Users' Resources from the Pickup Group, in the row of a respective Resource, click ▸ to open an Action menu and then select **Remove from Pickup Group**.

   System displays the action to be performed and requests confirmation to remove the selected User(s) from the Pickup Group.

5) Click **OK** to confirm.

   System removes the selected Users' Resources from the corresponding Pickup Group.

   NOTICE:

   If all the Resources of one Pickup group have been removed, system provides the option to delete also the Pickup Group.

6) Click **Save** to save changes.
   System:

   a) • ensures that the selected Resources can be removed from the Pickup Group

   • proceeds with the modification of the Pickup Group.

The UM User's Resource has been removed from the Pickup Group and the column **Pickup Group** of the Resources list is updated, after the administrator saves and reopens the form.

10.1.11.9 How to Remove User's Resources from a Hunt Group

This Chapter describes how to remove the UM User's Resource from a Hunt Group, without having to manage the actual Hunt Group.

Prerequisites

Adequate administrative permission that allows Management of UM Users and Resources.

The Resources that are going to be removed from the Hunt Group must belong to an OSV Switch that supports the BG/Pickup Group synchronization.

Step by Step

1) Navigate to **User Management** > **Administration** > **Users&Resources**.
   A list of the existing UM Users is displayed (column **Resources** shows all the Resources assigned to the specific UM User).

   NOTICE: In case you are logged in as an UM Locality Administrator, system displays only the UM Users that belong to the Localities of this UM Locality Administrator.

2) Click on the specific UM User within the list to have a closer look at the **Resources** assigned to this user.

   A pop-up window **Edit User & Resources** is displayed.

3) Navigate to the **General** tab, **Resources** area.

   A list of all Resources assigned to the specific UM User is displayed.

4) To remove one of the assigned UM User's Resources from the Hunt Group, in the row of a respective Resource click ▸ to open an Action menu and then select **Remove from Hunt Group**.

   A pop-up window **Remove from Hunt Group** is displayed, showing the list of all Hunt Group(s) the User's Resource belongs to.

5) Select the Hunt Group(s) and click **Next**.

   NOTICE:

   If the selected User's Resource is a Hunt Group Pilot, system displays a warning message saying that removing this Pilot will result in removing the whole Hunt Group.

   System displays the action to be performed and requests confirmation to remove the selected User's Resource from the Hunt Group(s).

6) Click **OK** to confirm.

   System removes the selected User's Resource from the corresponding Hunt Group(s).

   NOTICE:

   In case the selected User's Resource was a Pilot in the Hunt Group, this Hunt group will be deleted.

7) Click **Save** to save changes.
   System:

   a) • ensures that the selected Resources can be removed from the Hunt Group

   • proceeds with the modification of the Hunt Group.

The UM User's Resource has been removed from the Hunt Group and the column **Hunt Group** of the Resources list is updated, after the administrator saves and reopens the form.

10.1.11.10 How to Display Pickup and Hunt Group information in the UM User's Resources list

This Chapter describes how to display which User's Resource belongs to which Pickup or Hunt Group, without having to manage the actual Pickup (Hunt) group.

Prerequisites

Adequate administrative permission that allows Management of UM Users and Resources.

The Resources belong to an OSV Switch that supports the BG/Pickup Group synchronization.

Step by Step

1) Navigate to **User Management** > **Administration** > **Users&Resources**. A list of the existing UM Users is displayed (column **Resources** shows all the Resources assigned to the specific UM User).

NOTICE: In case you are logged in as an UM Locality Administrator, system displays only the UM Users that belong to the Localities of this UM Locality Administrator.

---

2) Click on the specific UM User within the list to have a closer look at the **Resources** assigned to this user.

A pop-up window **Edit User & Resources** is displayed.

3) Navigate to the **General** tab, **Resources** area.

- For each UM User's supported Resource that belongs to the Pickup Group, the **Pickup Group Number** and **Pickup Group Name** will be displayed in the column **Pickup Group**.
- For each UM User's supported Resource that belongs to the Hunt Group, the **Hunt Group Pilot Number** and **Hunt Group Name** will be displayed in the column **Hunt Group**.

NOTICE:

If the Resource is a Pilot of the Hunt Group, the text Pilot will be prefixed to the Hunt Group identifier.

---

4) Click on the Pickup or Hunt Group the Resource belongs to.

The list of the UM Users, that are members of the specific group, has been displayed and it contains three columns: **Last Name**, **First Name** and **Number** (Resource identifier).

NOTICE:

If selected Resource belongs to more than one Hunt Group, the option to select the Hunt Group is available (drop-down list).

After the administrator performs Resource modification operations, he needs to save and reopen the UM User's Resource list in order to see the updated information related to the Pickup and Hunt groups.

10.2 Localities

Locality is a designated entity that comprises: address related data (street, city, building number, etc.), organization data (company name, department, etc.), as well as locality related systems data (branch). The UM User can have at most one reference to the Locality.

A way how to model the real world and exploit Locality, is up to the customers: customer with the large number of branches will probably create one locality for each branch, in order to benefit from the "easy-branch" concept. Other customers, with only few office buildings, served by a single OpenScape Voice system, may choose to assign all users to the same locality.

In general, Locality contains the following areas of information:

- address information
- organization information
- list of local attributes and values
- list of unique attributes and values (wherever applicable).

NOTICE:

The last two should be offered in a system context, i.e. first the system type is selected, then the attribute names (valid for the selected system type) are listed, and then one of these attributes is selected and a value is specified (listed values for local attributes).

There is also a need for a domain-wide default Locality. The values specified in the Default Locality will apply in the following cases:

- if no other Locality has been defined so far
- if the customer does not want to create localities and assign them to the users.
- if the customer wishes to define the values for local, or unique attributes, which would apply across the localities.

The Default Locality is automatically created upon the installation of OpenScape User Management, but it remains empty as long as the administrator does not want to exploit this functionality. This locality cannot be deleted and also, the address data are not editable. The only things, related to the Default Locality, that can be specified are the default values for resource creation.

The effects of picking a Locality for the UM User, when the User is created for the first time, are multiple. Once UM User creation starts, the Locality should be defined. The address fields will be pre-populated with the address specified in the Locality. The administrator can keep this address, or choose to type a different one. In any case, the address information is stored along with the UM Users explicitly and belongs to the Users, even if it is exactly the same one recommended by the Locality. A link to the Locality is stored in order to serve the creation of the resources.

Basically, the "bulk" update of UM Users' attributes by changing the Locality, simply links the UM Users to a new Locality. It does not affect any other UM User's or Resources' attributes.

10.2.1 How to Display Localities

A list of Localities can be displayed on different ways, depending on the search functionality.

Prerequisites

- Adequate administrative permission that allows management of Localities.
- Simple **Search** functionality has been enabled for the Localities list.
- The Default Locality has been created.
  - This special Locality is automatically created during the installation.
  - The attribute **Name** for the Locality is **Default Locality**.
  - The **Description** attribute for the Locality is "**The Default Locality is used for providing default values for the creation of resources. When creating a resource for a User, system shall use these values if the resource attributes are not specified in the User's assigned Locality, or if the UM User has no Locality assigned.**"
  - **Default Locality** can not be deleted.
  - The address related data of **Default Locality** is not editable.

Step by Step

1) Navigate to **User Management** > **Administration** > **Localities**.
A list of existing Localities is displayed.

NOTICE: In case you are logged in as an UM Locality Administrator, system displays only the Localities assigned to the UM Locality Administrator. The **Default Locality** is not displayed.

Initially, system displays all Localities defined in the current Domain and sorts them per first column **Name**, in ascending order.

NOTICE: Steps 2-3 may be performed in any order.

---

2) Click on the column name to sort the list of Localities by any displayed attribute that supports sorting.

Table 15: Localities list Attributes

#	Attribute	Sort	Search	Search Type	Comments
1	Name	yes	yes	N/A	
2	Description	no	yes	N/A	

#	Attribute	Sort	Search	Search Type	Comments
3	Number of users	no	no	N/A	The number of User that have this Locality assigned.

3) Click **Search** to perform Simple **Search** functionality using the following rule:

`Search for:` <**User input**> `in` <**Attributes list**> `of status` <**Status list**>.

a) <**User input**> may contain any character. The asterisk character (*) is used as a substitution of zero or more characters.

> **NOTICE:**
>
> In case, the administrator hasn't specified search expression, i.e. <**User input**> is empty, system treats the empty field as the asterisk (*) wildcard for the selected Attribute in the <**Attribute list**>.

b) <**Attribute list**> contains the following items: **Name** and **Description**.

c) <**Status list**> contains the following values: **Any**, **Assigned** and **Unassigned**.

System applies **Search** criteria and displays the Localities list, based on the administrator's preferences.

> **NOTICE:** The criteria for the Localities list stay applied, as long as they are not explicitly cleared, or the user's session does not expire.

10.2.2 How to Create Localities

This Chapter describes How to create the Locality that contains location specific information for UM Users and related Resource types.

Prerequisites

Adequate administrative permission that allows management of UM Users and Localities.

Step by Step

1) Navigate to **User Management** > **Administration** > **Localities**.
A list of existing Localities is displayed, sorted per first column **Name**, in ascending order.

> **NOTICE:** In case you are logged in as an UM Locality Administrator, system displays only the Localities assigned to the UM Locality Administrator. The **Default Locality** is not displayed.

2) Click **Add** to create a new Locality.

   A pop-up window **Add locality** is displayed.

3) Fill in the following Locality attributes:

Table 16: Locality attributes

Details	Locality information	Rules for resources configuration
Locality	Home Time Zone	OpenScape Voice
Description	Country	OpenScape Voice Softphone
	State or Province	OpenScape 4000
	City	OpenScape Xpressions
	Postal Code	Unified Communications
	Company	
	Department	
	Building	
	Room	
	Street	

NOTICE:

Mandatory fields are written in bold letters.

Rules for resources configuration area

Shows separate sections for each resource type (OpenScape Voice, OpenScape Voice Softphone, OpenScape 4000, OpenScape Xpressions, Unified Communications) that is supported by the current deployment.

NOTICE:

Regarding the OpenScape Voice resources, you can configure up to two different sets of rules (for example, using different Office Code configuration). To enable the section for the second set of rules, you must enable the first set of rules (as shown in steps 4 and 5).

4) Click **Configure...** to configure the default values for the resource creation of the supported resource types.

   The corresponding resource configuration screen is displayed.

5) In **Edit <Resource type> attributes** window, select the following:

   a) **Operation Mode**

   a) • **Disabled** to disable the use of default values for the resource creation of the supported resource types when a specific locality is selected.

- **Enabled** to enable all local attributes and use them as default values for the resource creation of the supported resource types when a specific locality is selected.

b) **Attributes**

NOTICE:

For detailed information about the default values for the specific resources types, see chapters related to How to Define default values for different Resource types.

---

6) Click **OK** to confirm the configuration.

System verifies that supplied information is correct and all required attributes are filled in.

NOTICE: The corresponding Resource type section shows that the use of the default values for the specific resource is enabled/disabled.

---

7) Click **Save** to create a new Locality.

a) System:

- verifies that supplied Locality information is correct and that all required attributes are filled in
- adds all new Resources to the Locality
- creates a new Locality.

A new Locality has been created and displayed in the list of the existing Localities.

10.2.3 How to Edit Localities

In order to have more accurate information when creating a new UM User, the administrator can modify the Name, Description, Address Data, or Resource types for the Locality. Optionally, he can update all UM Users assigned to one Locality with the Locality's Address Data and ensures the consistency of Users' Address Information.

Prerequisites

Adequate administrative permission that allows management of UM Users and Localities.

Step by Step

1) Navigate to **User Management** > **Administration** > **Localities**.
A list of existing Localities is displayed.

IMPORTANT:

Default Locality can be edited, but not deleted.

NOTICE: In case you are logged in as an UM Locality Administrator, system displays only the Localities assigned to the UM Locality Administrator. The **Default Locality** is not displayed.

---

2) Select to edit Locality in one of the following ways:

- Click on the **Name** of Locality you want to modify.
- Check the box in front of the Locality you want to modify and then click **Edit**.
- In the row of a respective Locality, click ▸ to open an application action menu and then select **Edit**.

A pop-up window **Edit locality** is displayed.

NOTICE: In case you are logged in as an UM Locality Administrator the Locality name/description/address data are editable.All the Locality resource configuration options are read-only.

---

3) The System retrieves all Locality attributes that were defined once the Locality was created.

a) If the selected Locality is assigned to at least one UM User:

- – An additional option **When saving, update the Address Data of the User currently using this locality with the data below** is displayed. It allows updating the UM Users currently using this Locality, by **replacing**, **disabling to replace**, or **merging** the Users' Address Data with the Locality Address Data.

NOTICE:

Regarding the OpenScape Voice resources, you can configure up to two different sets of rules (for example, using different Office Code configuration). To enable the section for the second set of rules, set the Operation Mode of the first set of rules to “Enabled”.

IMPORTANT:

When the Operation Mode of a set of OpenScape Voice rules is set to “Disabled” while editing a locality, the previously configured rules are deleted.

---

4) Fill in, or modify the Locality attributes (see the Table: Locality attributes).

NOTICE:

All attributes, including the Locality Name, are editable.

---

5) If the option **When saving, update the Address Data of the User currently using this locality with the data below** is displayed, select one of the following:

- to modify only the Locality's Address Data without updating the UM Users' Address data associated to this Locality, select the option **Disabled** from the drop-down list.
- to replace all Address Data of the UM Users currently using this Locality, with the Locality's Address Data, check the option **Replace Address data** from the drop-down list.
- to merge the changes made to Locality's Address Data with the UM Users' Address data associated to this Locality, select the option **Merge Address data**.

  When this option is selected, during the update of the Address Data of a UM User assigned to the modified Locality, system will compare the value of each field to the value contained in the Locality before the modification and only if these two values are equal, the Users' value will be updated to the new Locality data.

NOTICE: This behavior is specific for the manual creation/ modification of the UM User. In general, when Locality attribute of the UM User is modified (e.g. via LDAP synchronization), the address related attributes are not modified.

---

6) Click **Configure...** to reconfigure the default values for the resource creation of the supported resource types.

   The corresponding resource configuration screen is displayed.

7) In **Edit <Resource type> attributes** window, modify one of the following:

   a) **Operation Mode**

   a) • **Disabled** to disable the use of default values for the resource creation of the supported resource types when a specific locality is selected.

   • **Enabled** to enable all local attributes and use them as default values for the resource creation of the supported resource types when a specific locality is selected.

   b) **Attributes**

NOTICE:

For detailed information about the default values for the specific resources types, see chapters related to How to Define default values for different Resource types.

---

8) Click **OK** to confirm the modification of the selected resource types.

System verifies that supplied information is correct and all required attributes are filled in.

NOTICE: The corresponding Resource type section shows that the use of the default values for the specific resource is enabled/disabled.

---

9) Click **Save**.

NOTICE:

In case the option **Replace Address data** or the option **Merge Address data** are selected, system displays the progress of the operation.

---

a) System:

- verifies that updated Locality information is correct and that all required attributes are filled in
- modifies and updates the Resources of the Locality.

NOTICE:

In case the **Cancel** button has been pressed, system completes the operation that is pending for the current UM User and does not roll-back any performed operation.

---

10) Upon completion, or cancellation of edit operation, a **Update Locality Address Data - Report** window is displayed, containing the following information:

- Number of successfully modified UM Users
- Number of UM Users that failed to be updated.

a) System:

- updates Locality using the supplied information
- assigns the new Resources to the Locality
- removes (deletes/deactivates) existing Resources from the Locality.

The UM Users' Locality has been modified.

10.2.3.1 How to Define default values for OpenScape Voice Resource

In order to configure Locality specific attributes for the OpenScape Voice Resource type, fill in the following fields:

Table 17: OpenScape Voice Resources Locality Attributes

#	Name	Type	Value	Default Value
	Local			

#	Name	Type	Value	Default Value
1	Business Group	List		Conditionally visible depending on the value of the System Setting "Use Domain to Business Group Mapping". The value displayed in the list shall be "commSystemName-bgName".
2	Branch Office	List		
3	Office Code	List		
4	Class Of Service	List		
5	Address Translator Context	List		
6	Numbering Plan	List		
7	Routing Area	List		
8	Realm	Text		
9	Extension Range	List		

10.2.3.2 How to Define default values for OpenScape Voice Softphone Resource

In order to configure the default values for the local attributes of OpenScape Voice Softphone resource, fill in the following fields:

Table 18: OpenScape Voice Softphone Resources Locality Attributes

#	Name	Type	Value	Default Value
	Local			

#	Name	Type	Value	Default Value
1	Business Group	List		Conditionally visible depending on the value of the System Setting "Use Domain to Business Group Mapping". The value displayed in the list shall be "commSystemName-bgName".
2	Branch Office	List		
3	Office Code	List		
4	Class Of Service	List		
5	Address Translator Context	List		
6	Numbering Plan	List		
7	Routing Area	List		
8	Realm	Text		
9	Extension Range	List		

10.2.3.3 How to Define default values for OpenScape 4000 Resource

The attributes needed for the OpenScape 4000 Resources creation are given in the following table:

Table 19: OpenScape 4000 Resources Locality Attributes:

#	Name	Type	Value	Default Value
	Local			
1	Switch Name (System)	List		
2	Virtual Node # (Domain)	List		
3	Dial Plan	List		
4	IPDA	List		
5	Source Group	Text		

#	Name	Type	Value	Default Value
6	Address Translator Context	List		

10.2.3.4 How to Define default values for Xpressions Resource

Once an administrator selects to define the OpenScape Xpressions Resource type, system responds with the following attributes that are classified as Location specific:

Table 20: Xpressions Resources Locality Attributes:

#	Name	Type	Values	Default Value
	Local			
1	Preferred Address	Text	STAND-IN MAILBOX SMTP TCPIP DIS LDAP NIL NILOK PRESENCE SAPSMTP SFOD STOD VPIM XPRESSIONS XPRESSIONS/ LISTPROC	MAILBOX
2	User options for voice mail system	Text		
3	CTI Journal	Check box		
4	Language	Drop-down list		
5	Voice Mail System	Text	VMS PHONEMAIL ERGO	PHONEMAIL

#	Name	Type	Values	Default Value
6	Internal mailbox	Text		Internal mailbox
7	Fax G3 Headline	Text		
8	Language	Drop-down list	List of system available l languages	
9	Home Time Zone	Drop-down list	List of Time zones	

10.2.3.5 How to Define default values for UC Resource

For the creation of OpenScape UC Application Resource type, fill in the following fields:

Table 21: UC Resources Locality Attributes:

#	Name	Type	Value	Default Value
	Local			
1	Translator Context	List		
2	Voice Mail Number	List		

10.2.4 How to Delete Localities

The objective of this Chapter is to show How to delete Localities.

Prerequisites

Adequate administrative permission that allows deletion of Localities.

IMPORTANT:

It is allowed to delete only Localities that are not assigned to any UM User, or User Template.

Step by Step

1) Navigate to **User Management** > **Administration** > **Localities**.
A list of existing Localities is displayed, sorted per first column **Name**, in ascending order.

NOTICE: In case you are logged in as an UM Locality Administrator, system displays only the Localities assigned

to the UM Locality Administrator. The **Default Locality** is not displayed.

NOTICE:

At this moment, **Delete** button is inactive.

2) Perform the Simple **Search** operation using the following criteria, in order to retrieve a list of all Localities that are not assigned to the UM Users, or User Templates:

`Search for:` **<User input>** `in` **<Attributes list>** `of status` **<Status list>**.

a) **<User input>** may contain any character. The asterisk character (*) is used as a substitution of zero or more characters.

NOTICE:

In case, the administrator hasn't specified search expression, i.e. **<User input>** is empty, system treats the empty field as the asterisk (*) wildcard for the selected Attribute in the **<Attribute list>**.

b) **<Attribute list>** contains the following items: **Name** and **Description**.

c) **<Status list>** must be set to: **Unassigned**.

3) Click **Search** to apply provided criteria.

The appropriate list of Localities is displayed.

4) Select to delete Localities, in one of the following ways:

- Check the box in front of the Localities you want to delete and click **Delete**.
- In the row of the respective Locality, click on ▸ to open application action menu and then select **Delete**.

System displays the action to be performed and requests verification for the deletion of Localities.

a) If all selected Localities are assigned to the existing UM Users, or User Templates:

- – System doesn't allow the deletion and displays the following error message:

  `The selected N localities are assigned to users and can not be deleted.`

b) If among selected Localities only some of them are assigned to the UM Users, or User Templates:

- – System will proceed only with the deletion of the Localities, that are not assigned to any UM User, or User Template and the following error message will be displayed:

  `You have selected totally N localities to delete. X localities are also assigned to users and can not be deleted. Please verify that you want to continue with the delete action.`

5) Click **OK** to verify deletion.

IMPORTANT:

Default Locality can not be deleted.

a) System:

- performs the action

INFO: In case **Cancel** button is pressed, delete operation will be cancelled and the list of Localities will remain the same.

- displays a pop-up window, with the summary of Locality deletion operation.

The selected Localities have been deleted from the Localities list.

10.3 User Templates

The OpenScape User Management represents a single point of entry for the entire CMP system. It eliminates the need to navigate to the different Element managers in order to perform a single function.

The primary goal of User Template is to minimize administrator’s efforts related to the creation and assignment of UM Users and Resource. Especially when it comes to the technical attributes, which are usually dependable of the system on which the resource is created, User Templates play important role and:

- Make possible for the administrator to configure rules and values that will govern the future creation of Resources for a group of Users.
- Eases the creation of Resource, by utilizing the information stored in the User Templates and information stored in the Locality, in order to get the predefined set of rules.

  These rules can be either static or dynamic, i.e., they can be configured either by using the static values or by applying the mapping which retrieve data directly from an LDAP directory.

Initially, the User Templates were used only for Resource creation. This imposed a very serious limitation: after a resource was created, the changes in the data used for the creation of this resource, were not propagated to the resource.

Thus, the User Templates functionality has been extended to allow updating the User's resources using the rules defined in a User Template. This can be done either manually or automatically (during LDAP synchronization).

The OpenScape User Management has been enhanced to keep track of the association between a Resource and a User Template. Once this association is established, each User is associated with a User Template transitively through the assigned resources.

In other words, you can associate UM User’s Resources with a single User Template, but also associate an UM Users with a single User Template and

see the status of this association via OS UM User Interface or OS UM SPML Interface.

The status of that association can be:

- **not associated**

  the User/Resource is not associated with a User Template
- **ok**

  the User/Resource is associated with a User Template and the User Template rules were applied successfully
- **warning**

  the User/Resource is associated with a User Template but there have changes in the rules that need to be applied
- **error**

  the User/Resource is associated with a User Template but there was an error when applying the User Template rules.

In order to reduce complexity regarding the User Template associations the following postulates have been declared:

- Each User and his Resources shall be associated with the same User Template or be completely dissociated
- When a User Template is applied to a User, the User's Resources will be assigned, un-assigned or modified in order to match the rules defined in the User Template.

The User Templates are very important for the OpenScape User Management efficiency and that’s why we are going to describe it in details.

10.3.1 How to Display User Templates

Follow the steps below in order to display User Templates.

Prerequisites

Adequate administrative permission that allows management of User Templates.

Step by Step

1) Navigate to **User Management** > **Administration** > **User Templates**. A list of the existing User Templates is displayed, sorted per first column **Name**, in ascending order.

NOTICE:

The column **Associated Users** displays the number of Users that are currently associated with each User Template.

---

2) Click on the column **Name** to sort the list of User Templates.

3) Select to display the User Template in one of the following ways:
   - Click on the **Name** of User Template you want to see.
   - Check the box in front of the User Template you want to modify and click **Edit**.
   - In the row of a respective User Template, click on to open application action menu and then select **Edit**.

   A pop-up window **Edit User Template** is displayed.
4) Navigate to the **Settings** area to see the following information:
   a) **Name**

      This is the mandatory and unique field that represents the name of the User Template.
   b) **Description**

      Briefly describes the User Template.
5) Navigate to the **Rules** area where various **Resource Types** are displayed.

NOTICE:

The following Resource Types are supported by the current deployment: OpenScape Voice, OpenScape Voice Softphone, OpenScape 4000, OpenScape Xpressions, Unified Communications and External.

10.3.2 How to Create / Clone User Template

This chapter describes how to create User Templates in order to support the automatic resource creation. Also, it explains how the User Templates can be used to create multiple resource of the same type. Subsequently, it also describes the option to clone a UM user template.

Prerequisites

Adequate administrative permission that allows management of User Templates.

NOTICE:

In order to use the LDAP attributes for creating the resources in User Templates, the following prerequisites have to be fulfilled:

LDAP connection has to be enabled in OS UM.

The OS UM Users have been created via LDAP synchronization.

The resource templates required for the resource creation have to be available.

Step by Step

1) Navigate to **User Management** > **Administration** > **User Templates**

   A list of the existing User Templates is displayed.
2) Click **Add** to create a new User Template.

   A pop-up window **Add User Template** is displayed.

3) Navigate to the **Settings** area and fill in the following information:
   a) **Name**

      This is a mandatory and unique field that represents the name of the User Template.
   b) **Description**

      Briefly describes the User Template.
4) Navigate to the **Rules** area and from the drop-down list select the **Resource Type** you would like to configure.

   NOTICE:

   The following Resource Types are supported by the current deployment: OpenScape Voice, OpenScape Voice Softphone, OpenScape 4000, OpenScape Xpressions, Unified Communications, CMP administrator and External.
5) Click **Add** to configure the automatic creation of one of the supported resource type(s).

   The configuration screen related to the corresponding resource is displayed.
6) In the **Rules for automatic resource creation** window navigate to the **Setting** area to define:
   a) **Function**

      NOTICE:

      The resource **Function** field is available only for the resources that can be added multiple times, i.e.,OpenScape Voice, OpenScape Voice Softphone, OpenScape 4000 and OpenScape Xpressions.

      The only exception is that OpenScape Xpressions resource supports only the **Fax** and **Other** resource function.

   From the drop-down list select one of the following functions (flavors):

   a)
   - **Business Phone 1**
   - **Business Phone 2**
   - **Fax**

- **Other**

NOTICE:

Any of the resource **Function** values can be set at most once in each User Template, except the type **Other** which can be specified multiple times.

b) **Operation Mode**

From the drop-down list choose one of the following options:

a)
- **Create new resources**

  system will monitor all the rules specified in the User Template and when any of these changes, an update of the Resource itself will be triggered.
- **Match existing Resources**

  system will monitor the rules that generate the Resources identifier only and the rest of the rules will be ignored.
- **Create new and match existing resources**

  system will create the resource that are not found in the User Template, but afterwards it will behave as described in the **Match existing Resources** operation mode.

NOTICE:

In the case where the selected resource type is **Unified Communications**, **CMP administrator** or **OpenScape Mobile (OSMO)**, the only available option is **Create new resources**.

7) In the **Rules for automatic resource creation** window navigate to the **Attributes** area to define the parameters for the automatic completion of the unique/mandatory fields.

Among others, you have to select the **Resource Template** that will be used for the creation of the specific resource.

NOTICE:

At least one Resource Template per each Resource type must be specified.

As long as OS UM is connected to the LDAP directory, it is allowed to specify mapping to LDAP attributes for any attribute required for the resource creation.

NOTICE:

For detailed information about the rules for Automatic completion of the mandatory fields for the supported Resource Types, see the chapters that follow.

8) Click **OK** to confirm the configuration.

Once the system verifies that supplied information is correct and all required attributes are filled in, the corresponding Resource will be added to the list of the existing Resources.

9) Click **Save** to save changes to the User Template.

a) System:

- verifies that supplied information is correct
- creates and stores the new User Template.

NOTICE:

If the User Template configuration screen is closed without changes being saved, any modification of the mapped LDAP attributes will be lost.

---

10) A new User Template has been created and it is displayed in the list of the existing User Templates.

NOTICE:

In case of upgrade to V7, the pre-existing User Templates (i.e., the Templates that have already been created in the older versions) will be automatically configured to have the value **Other** for the resource **Function**

---

11) Supplementary to creating a UM user template, you also have the option to create an identical to an already existing one. You are able to clone a User Template in order to avoid cumbersome configuration where a lot of different User Templates are needed.

a) Navigate to **User Management** > **Administration** > **User Templates**

A list of the existing User Templates is displayed.Choose a User Template from that list.

b) Click **Clone** to create a clone of this User Template.

c) A pop-up window **Clone User Template** is displayed.

d) Navigate to the **Settings** area and fill in the following information:

- **Name**

  This is a mandatory and unique field that represents the name of the User Template. Most common action in naming a Clone Template is `Copyof<NameofUserTemplate>`

- **Description**

  Briefly describes the User Template.

e) Proceed as previous in creating a User Template.

f) Click **Save** to save changes to the cloned User Template.

Related concepts

Appendix A: Character Restrictions on page 691

10.3.2.1 How to Create User Template with the OpenScape Voice Resource

The following chapter describes how to add the OpenScape Voice Resources to the User Template.

Prerequisites

Adequate administrative permission that allows management of User Templates.

NOTICE:

In order to use the LDAP attributes for creating the resources in User Templates, the following prerequisites has to be fulfilled:

LDAP connection has to be enabled in OS UM.

The OS UM Users have been created via LDAP synchronization.

The resource templates required for the resource creation have to be available.

Step by Step

1) Navigate to **User Management** > **Administration** > **User Templates**

A list of the existing User Templates is displayed.

2) Click **Add** to create a new User Template.

A pop-up window **Add User Template** is displayed.

3) Navigate to the **Settings** area and fill in the following information:

a) **Name**

This is a mandatory and unique field that represents the name of the User Template.

b) **Description**

Briefly describes the User Template.

4) Navigate to the **Rules** area and from the drop-down list select the **OpenScape Voice** resource.

5) Click **Add** to configure the automatic creation of the **OpenScape Voice** resource.

The configuration window (**Rules for automatic resource creation**), related to the **OpenScape Voice** resource is displayed.

NOTICE:

To create multiple OpenScape Voice Resources within a single User Template repeat this step and each time select different value (flavor) for the resource **Function**.

Any of the resource **Function** values can be set at most once in one User Template, except the type **Other** which can be specified multiple times.

---

6) In the **Rules for automatic resource creation** window navigate to the **Setting** area to define:

a) **Function**

NOTICE:

The resource **Function** field is available only for the resources that can be added multiple times, i.e.,OpenScape Voice, OpenScape Voice Softphone, OpenScape 4000, OpenScape Xpressions and External.

From the drop-down list select one of the following functions (flavors):

a) • **Business Phone 1**
• **Business Phone 2**
• **Fax**
• **Other**

b) **Operation Mode**

From the drop-down list choose one of the following options:

a) • **Create new resources** to create a new OpenScape Voice subscriber and assign it to the User. If an existing OpenScape Voice subscriber matches the specified criteria, it will not be assigned to the User.
• **Match existing Resources** to assign an OpenScape Voice subscriber to the User only if an OpenScape Voice subscriber that matches the specified criteria already exists in the system. A new OpenScape Voice subscribers will not be created.
• **Create new and match existing resources** to assign an OpenScape Voice subscriber to the User. System will search for an existing OpenScape Voice subscriber that matches the specified criteria and if it exists, it will be assigned to the User. In case it does not exist, a new OpenScape Voice subscriber will be created.

c) **Resource Name**

From the drop-down list choose one of the following options:

a) • **Use resource ID** (default value)
• **Use resource function name**
• **Constant value**
• **User attribute**

IMPORTANT:

For users not connected with LDAP (e.g. display name can be filled with IM address)

Select one of the available values from the **User Attribute** drop-down list (see the Table: UM User attributes)

• **LDAP attribute**

7) In the **Rules for automatic resource creation** window navigate to the **Attributes** area to define the parameters for the automatic completion of the unique/mandatory fields (see the table below).

Table 22: Automatic completion rules for OSV Resource

Attribute	Rule
Resource Template	Drop-down list is populated with the available Subscriber Templates (for more information refer to the Chapter: *Subscriber Templates* of *OpenScape Voice V6 Administrator Documentation*), User attribute and the LDAP attribute.
Preserve Subscriber Settings	It should be checked in order for the subscriber-level features not to be reset to profile-level, while applying the user template. **This setting takes effect only in case of "Create New Resources" Operation Mode.**
Display Name	In case of existing phones see the section at the end of the table. One of the following contact information are used as the attributes for the Display Name in case of a new resource: - Display Name - Last Name - First Name Last Name - Last Name, First Name - User attribute - LDAP attribute

Attribute	Rule
Directory Number	One of the following is used as an attribute to generate the Suffix: **a)** Information **Inferred from User's details**, that can be: - Business Phone 1 - Business Phone 2 - User attribute - LDAP attribute **b)** **Automatic assignment** of the resource's suffix from the LDAP attribute or from the list of the predefined ranges. This option is disabled when the resource creation rules are configured with Operation Mode **Match existing Resources**. (The available Extension ranges for the selected OpenScape Voice switch are displayed in the form of `Range name – switch name`. In case there is a single communication system, the `switch name` is not displayed.)
Type	Selection of one of the available values: - Public - Private. - User attribute. - LDAP attribute
Alphanumeric SIP URI	One of the following options are provided: - User attribute - LDAP attribute.
SIP Authentication Username	Selection of one of the available values: - Constant Value - Resource ID - User attribute. - LDAP attribute

Attribute	Rule
SIP Authentication Password	Selection of one of the available values: - Constant Value - Resource ID - User attribute. - LDAP attribute

Display name in case of existing phones

Depending on the selected **operation mode**, different options are given regarding the display name.

- **1.** If the selected operation mode is "**Create new resources**", then the below cases exist for the display name:

  -) "**In case of match**" refers to resources that already exist, which is not applicable.

  -) "**In case of create**" refers to resources that will be created. The selected value in the drop down list will be used to populate the new OpenScape Voice resource's display name from the corresponding option (UM user's property or LDAP attribute).

- **2.** If the selected operation mode is "**Match existing resources**", then the below cases exist for the display name:

  -) "**In case of match**" refers to resources that already exist:

  If the checkbox is checked then any matching OpenScape Voice resource will keep its display name

  If the check box is unchecked then the display name of the OpenScape Voice resource will be populated from the corresponding option (UM user's property or LDAP attribute).

  The accompanying text "**In case of match**" is moved in this case to accompany the below drop box option.

  -) "**In case of create**" refers to resources that will be created, which is not applicable.

- **3.** If the selected operation mode is "**Create new and match existing resources**", then the below cases exist for the display name:

  -) "**In case of match**" refers to resources that already exist:

  If the check box is checked then any matching OpenScape Voice resource will keep its display name. For resources that will be created the selected value in the drop down list will be used to populate the new

OpenScape Voice resource's display name from the corresponding option (UM user's property or LDAP attribute).

If the check box is unchecked then the display name of the OpenScape Voice resource (new or existing) will be populated from the corresponding option (UM user's property or LDAP attribute).

The accompanying text "**In case of match**" disappears and the below drop box's text changes from "**In case of create**" to "**In case of create/ match**".

NOTICE:

At least one Resource Template per each Resource type must be specified.

NOTICE:

In case the option **Use Domain to Business Group Mapping** is disabled and there is more than one OSV switch deployed on the system, the names of the available Resource Templates, available in the drop-down list, will appear in the form of: `subscriber_template_name@business_group_name@switch_id`.

From the other side, if only one OSV switch is present, switch_id will be omitted from the Resource Template name and it will contain only: `subscriber_template_name@business_group_name`.

As long as OS UM is connected to the LDAP directory, it is allowed to define:

a) a direct mapping to LDAP attributes for any attribute required for the resource creation

b) an advanced mapping to LDAP attributes for any attribute required for the resource creation.

   Click **Advanced...** and then in the **Advanced Mapping** pop-up window define the Advanced Mappings rules.

NOTICE:

You can select previously defined advanced rule. In case where a new advanced rule is created, this new rule is going to replace previously defined rule.

---

8) Click **OK** to confirm the configuration.

Once the system verifies that supplied information is correct and all required attributes are filled in, the OpenScape Voice Resource will be added to the list of the existing Resources.

9) Click **Save** to save changes to the User Template.

a) System:

- verifies that supplied information is correct
- creates and stores the new User Template.

NOTICE:

If the User Template configuration screen is closed without changes being saved, any modification of the mapped LDAP attributes will be lost.

A new User Template is displayed in the list of the existing User Templates. The column **Resources** shows the icon that represents the OpenScape Voice resource.

10.3.2.2 How to Create User Template with the OpenScape Voice Softphone Resource

The following chapter describes how to add the OpenScape Voice Softphone Resources to the User Template.

Prerequisites

Adequate administrative permission that allows management of User Templates.

NOTICE:

In order to use the LDAP attributes for creating the resources in User Templates, the following prerequisites has to be fulfilled:

LDAP connection has to be enabled in OS UM.

The OS UM Users have been created via LDAP synchronization.

The resource templates required for the resource creation have to be available.

Step by Step

1) Navigate to **User Management** > **Administration** > **User Templates**

A list of the existing User Templates is displayed.

2) Click **Add** to create a new User Template.

A pop-up window **Add User Template** is displayed.

3) Navigate to the **Settings** area and fill in the following information:

a) **Name**

This is a mandatory and unique field that represents the name of the User Template.

b) **Description**

Briefly describes the User Template.

4) Navigate to the **Rules** area and from the drop-down list select the **OpenScape Voice Softphone** resource.

5) Click **Add** to configure the automatic creation of the **OpenScape Voice Softphone** resource.

   The configuration window (**Rules for automatic resource creation**), related to the **OpenScape Voice Softphone** resource is displayed.

   NOTICE:

   To create multiple OpenScape Voice Softphone Resources within a single User Template repeat this step and each time select different value (flavor) for the resource **Function**.

   Any of the resource **Function** values can be set at most once in one User Template, except the type **Other** which can be specified multiple times.

   ---

6) In the **Rules for automatic resource creation** window navigate to the **Setting** area to define:

   a) **Function**

   NOTICE:

   The resource **Function** field is available only for the resources that can be added multiple times, i.e.,OpenScape Voice, OpenScape Voice Softphone, OpenScape 4000, OpenScape Xpressions and External.

   From the drop-down list select one of the following functions (flavors):

   a)
   - **Business Phone 1**
   - **Business Phone 2**
   - **Fax**
   - **Other**

   b) **Operation Mode**

   From the drop-down list choose one of the following options:

   a)
   - **Create new resources** to create a new OpenScape Voice Softphone resource and assign it to the User. If an existing OpenScape Voice Softphone matches the specified criteria, it will not be assigned to the User.
   - **Match existing Resources** to assign an OpenScape Voice Softphone resource to the User only if an OpenScape Voice Softphone resource that matches the specified criteria already exists in the system. A new OpenScape Voice Softphone resource will not be created.
   - **Create new and match existing resources** to assign an OpenScape Voice Softphone resource to the User. System will search for an existing OpenScape Voice Softphone resource that matches the specified criteria and if it exists, it will be assigned to the User. In case it does not exist, a new OpenScape Voice Softphone resource will be created.

   c) **Resource Name**

   From the drop-down list choose one of the following options:

   a)
   - **Use resource ID** (default value)

- **Use resource function name**
- **Constant value**
- **User attribute**

IMPORTANT:

For users not connected with LDAP (e.g. display name can be filled with IM address)

Select one of the available values from the **User Attribute** drop-down list (see the Table: UM User attributes)

- **LDAP attribute**

7) In the **Rules for automatic resource creation** window navigate to the **Attributes** area to define the parameters for the automatic completion of the unique/mandatory fields (see the table below).

Table 23: Automatic completion rules for OSV Resource

Attribute	Rule
Resource Template	Drop-down list is populated with the available Subscriber Templates (for more information refer to the Chapter: *Subscriber Templates* of *OpenScape Voice V6 Administrator Documentation*), the User attribute and the LDAP attribute.
Preserve Subscriber Settings	It should be checked in order for the subscriber-level features not to be reset to profile-level, while applying the user template. **This setting takes effect only in case of "Create New Resources" Operation Mode.**
Type	Selection of one of the available values: - Public - Private - User attribute - LDAP attribute
OSV resource	One of the following options are provided: - Use User’s Business Phone 1 - Use User’s Business Phone 2 - Use Template’s Business Phone 1 - Use Template’s Business Phone 2 - User attribute - LDAP attribute.
Append these digits to OSV resource to generate the Softphone number	Enter the digits that will be appended in order to create the Softphone number. (Minimum number of digits is 1 and maximum 5.)

Attribute	Rule
Alphanumeric SIP URI	One of the following options are provided: - User attribute - LDAP attribute.
SIP Authentication Username	Selection of one of the available values: - Constant Value - Resource ID - User attribute - LDAP attribute
SIP Authentication Password	Selection of one of the available values: - Constant Value - Resource ID - User attribute - LDAP attribute
Registration via Central SBC Allowed	Selection of one of the available values: - Disabled - Enabled - User attribute - LDAP attribute

NOTICE:

At least one Resource Template per each Resource type must be specified.

NOTICE:

In case the option **Use Domain to Business Group Mapping** is disabled and there is more than one OSV switch deployed on the system, the names of the available Resource Templates, available in the drop-down list, will appear in the form of: `subscriber_template_name@business_group_name@switch_id`.

From the other side, if only one OSV switch is present, switch_id will be omitted from the

Resource Template name and it will contain only:
`subscriber_template_name@business_group_name`.

As long as OS UM is connected to the LDAP directory, it is allowed to define:

a) a direct mapping to LDAP attributes for any attribute required for the resource creation
b) an advanced mapping to LDAP attributes for any attribute required for the resource creation.

   Click **Advanced...** and then in the **Advanced Mapping** pop-up window define the Advanced Mappings rules.

NOTICE:

You can select previously defined advanced rule. In case where a new advanced rule is created, this new rule is going to replace previously defined rule.

8) Click **OK** to confirm the configuration.

Once the system verifies that supplied information is correct and all required attributes are filled in, the OpenScape Voice Softphone Resource will be added to the list of the existing Resources.

9) Click **Save** to save changes to the User Template.

a) System:

- verifies that supplied information is correct
- creates and stores the new User Template.

NOTICE:

If the User Template configuration screen is closed without changes being saved, any modification of the mapped LDAP attributes will be lost.

A new User Template is displayed in the list of the existing User Templates. The column **Resources** shows the icon that represents the OpenScape Voice Softphone resource.

10.3.2.3 How to Create User Template with the OpenScape Mobile (OSMO) Resource

The following chapter describes how to add the OpenScape Mobile (OSMO) Resources to the User Template.

Prerequisites

Adequate administrative permission that allows management of User Templates.

The resource templates required for the resource creation have to be available.

Step by Step

1) Navigate to **User Management** > **Administration** > **User Templates**

   A list of the existing User Templates is displayed.

2) Click **Add** to create a new User Template.

   A pop-up window **Add User Template** is displayed.

3) Navigate to the **Settings** area and fill in the following information:

   a) **Name**

      This is a mandatory and unique field that represents the name of the User Template.

   b) **Description**

      Briefly describes the User Template.

4) Navigate to the **Rules** area and from the drop-down list select the **OpenScape Mobile** resource.

5) Click **Add** to configure the automatic creation of the **OpenScape Mobile (OSMO)** resource.

   The configuration window (**Rules for automatic resource creation**), related to the **OpenScape Mobile (OSMO)** resource is displayed.

6) In the **Rules for automatic resource creation** window navigate to the **Setting** area:

   - The only available **Operation Mode** is to create a new **OpenScape Mobile (OSMO) resource** (i.e., **Create new resources**) and assign it to the UM User.

   NOTICE:

   An existing **OpenScape Mobile (OSMO) Resource** is automatically assigned to a UM User when the corresponding Main Device is assigned to them. In this case, an OSMO resource in not needed for the template..

7) In the **Rules for automatic resource creation** window navigate to the **Attributes** area to define the parameters for the automatic completion of the unique/mandatory fields (see the table below).

Table 24: Automatic completion rules for OpenScape Mobile (OSMO) Resource

Attribute	Rule
Mobile Client Profile	Drop-down list is populated with the available Mobile Client Profiles (for more information refer to *Mobile Client Profiles*).
Main Device (ONS)	The normalized phone number of the related/ parent OSV subscriber: - Business Phone 1 - User attribute

Attribute	Rule
Directory Number	The normalized phone number of the OSMO subscriber: - **Use the Main Device (Main Device (ONS))** - **User attribute** - **LDAP attribute**
Digits to append	Append these digits to generate the OSMO directory number.Valid only in case the **Use the Main Device** is selected.

NOTICE:

At least one Resource Template per each Resource type must be specified.

As long as OS UM is connected to the LDAP directory, it is allowed to define:

a) a direct mapping to LDAP attributes for any attribute required for the resource creation

b) an advanced mapping to LDAP attributes for any attribute required for the resource creation.

Click **Advanced...** and then in the **Advanced Mapping** pop-up window define the Advanced Mappings rules.

NOTICE:

You can select previously defined advanced rule. In case where a new advanced rule is created, this new rule is going to replace previously defined rule.

8) Click **OK** to confirm the configuration.

Once the system verifies that supplied information is correct and all required attributes are filled in, the OpenScape Mobile (OSMO) Resource will be added to the list of the existing Resources.

9) Click **Save** to save changes to the User Template.

a) System:

- verifies that supplied information is correct
- creates and stores the new User Template.

NOTICE:

If the User Template configuration screen is closed without changes being saved, any modification of the mapped LDAP attributes will be lost.

A new User Template is displayed in the list of the existing User Templates. The column **Resources** shows the icon that represents the OpenScape Mobile (OSMO) resource.

IMPORTANT:

In order to use the LDAP attributes for creating the resources in User Templates, the following prerequisites has to be fulfilled:

- LDAP connection has to be enabled in OS UM.
- The OS UM Users have been created via LDAP synchronization.
- The resource templates required for the resource creation have to be available.

10.3.2.4 How to Create User Template with the OpenScape 4000 Resource

The following chapter describes how to add the OpenScape 4000 Resources (e.g., HFAs, cordless station, etc.) to the User Template.

Prerequisites

Adequate administrative permission that allows management of User Templates.

NOTICE:

In order to use the LDAP attributes for creating the resources in User Templates, the following prerequisites has to be fulfilled:

LDAP connection has to be enabled in OS UM.

The OS UM Users have been created via LDAP synchronization.

The resource templates required for the resource creation have to be available.

Step by Step

1) Navigate to **User Management** > **Administration** > **User Templates**

A list of the existing User Templates is displayed.

2) Click **Add** to create a new User Template.

A pop-up window **Add User Template** is displayed.

3) Navigate to the **Settings** area and fill in the following information:

a) **Name**

This is a mandatory and unique field that represents the name of the User Template.

b) **Description**

Briefly describes the User Template.

4) Navigate to the **Rules** area and from the drop-down list select the **OpenScape 4000** resource.

5) Click **Add** to configure the automatic creation of the **OpenScape 4000** resource.

The configuration window (**Rules for automatic resource creation**), related to the **OpenScape 4000** resource is displayed.

NOTICE:

To create multiple OpenScape 4000 Resources within a single User Template repeat this step and each time select different value (flavor) for the resource **Function**.

Any of the resource **Function** values can be set at most once in one User Template, except the type **Other** which can be specified multiple times.

---

6) In the **Rules for automatic resource creation** window navigate to the **Settings** area to define:

a) **Function**

NOTICE:

The resource **Function** field is available only for the resources that can be added multiple times, i.e.,OpenScape Voice, OpenScape Voice Softphone, OpenScape 4000, OpenScape Xpressions and External.

From the drop-down list select one of the following functions (flavors):

a)
- **Business Phone 1**
- **Business Phone 2**
- **Fax**
- **Other**

b) **Operation Mode**

From the drop-down list choose one of the following options:

a)
- **Create new resources** to create a new OpenScape 4000 resource and assign it to the User. If an existing OpenScape 4000 resource matches the specified criteria, it will not be assigned to the User.
- **Match existing Resources** to assign an OpenScape 4000 resource to the User only if an OpenScape 4000 resource that matches the specified criteria already exists in the system. A new OpenScape 4000 resource will not be created.
- **Create new and match existing resources** to assign an OpenScape 4000 resource to the User. System will search for an existing OpenScape 4000 resource that matches the specified criteria and if it exists, it will be assigned to the User. In case it does not exist, a new OpenScape 4000 resource will be created.

c) **Resource Name**

From the drop-down list choose one of the following options:

a)
- **Use resource ID** (default value)
- **Use resource function name**
- **Constant value**

- **User attribute**

  IMPORTANT:

  For users not connected with LDAP (e.g. display name can be filled with IM address)

  Select one of the available values from the **User Attribute** drop-down list (see the Table: UM User attributes)
- **LDAP attribute**

7) In the **Rules for automatic resource creation** window navigate to the **Attributes** area to define the parameters for the automatic completion of the unique/mandatory fields (see the table below).

Table 25: Automatic completion rules for OpenScape 4000 Resource

Attribute	Rule
Resource Template	Drop-down list is populated with the available Resource Templates and the LDAP attribute.
COS template	Drop-down list is populated with the available COS templates and the LDAP attribute.
Extension	In order to generate the Extension the following options are provided: **a) Infer from User's details** one of the following contact information will be used as the attributes to generate the Extension: - Business Phone 1 - Business Phone 2 - User attribute - LDAP attribute **b) Assign automatically** **allows to automatically assign the** resource's suffix from the LDAP attribute or from the list of the predefined ranges. This option is disabled when the resource creation rules are configured with Operation Mode **Match existing Resources**. (The available Extension ranges for the selected OpenScape 4000 switch are displayed in the form of `Range name - switch name`. In case there is a single communication system, the `switch name` is not displayed.)

Attribute	Rule
PEN	One of the following contact information are used as the attributes for PEN: - Use the first available PEN (the first available PEN applicable for the selected resource template will be assigned) - User attribute - LDAP attribute
Display Name	In case of existing phones see the section at the end of the table. One of the following contact information are used as the attributes for the Display Name in case of a new resource: - Display Name - Last Name - First Name Last Name - Last Name, First Name. - User attribute - LDAP attribute
HFA Password	Selection of one of the available values: - Constant value - User attribute - LDAP attribute.

Display name in case of existing phones

Depending on the selected **operation mode**, different options are given regarding the display name.

- **1.** If the selected operation mode is "**Create new resources**", then the below cases exist for the display name:

  -) "**In case of match**" refers to resources that already exist, which is not applicable.

  -) "**In case of create**" refers to resources that will be created. The selected value in the drop down list will be used to populate the new

OpenScape 4000 resource's display name from the corresponding option (UM user's property or LDAP attribute).

- **2.** If the selected operation mode is "**Match existing resources**", then the below cases exist for the display name:

  -) "**In case of match**" refers to resources that already exist:

  If the checkbox is checked then any matching OpenScape 4000 resource will keep its display name

  If the check box is unchecked then the display name of the OpenScape 4000 resource will be populated from the corresponding option (UM user's property or LDAP attribute).

  The accompanying text "**In case of match**" is moved in this case to accompany the below drop box option.

  -) "**In case of create**" refers to resources that will be created, which is not applicable.

- **3.** If the selected operation mode is "**Create new and match existing resources**", then the below cases exist for the display name:

  -) "**In case of match**" refers to resources that already exist:

  If the check box is checked then any matching OpenScape 4000 resource will keep its display name. For resources that will be created the selected value in the drop down list will be used to populate the new OpenScape 4000 resource's display name from the corresponding option (UM user's property or LDAP attribute).

  If the check box is unchecked then the display name of the OpenScape 4000 resource (new or existing) will be populated from the corresponding option (UM user's property or LDAP attribute).

  The accompanying text "**In case of match**" disappears and the below drop box's text changes from "**In case of create**" to "**In case of create/ match**".

As long as OS UM is connected to the LDAP directory, it is allowed to define:

a) a direct mapping to LDAP attributes for any attribute required for the resource creation
b) an advanced mapping to LDAP attributes for any attribute required for the resource creation.

   Click **Advanced...** and then in the **Advanced Mapping** pop-up window define the Advanced Mappings rules.

NOTICE:

You can select previously defined advanced rule. In case where a new advanced rule is created, this new rule is going to replace previously defined rule.

---

8) Navigate to the **PINs** tab and click **Add**.

A pop-up window **Add OpenScape 4000 PIN** is displayed.

9) Fill in the following information:

a) **PIN number**

From the drop-down list choose one of the following options:

a)
- **Constant value** (default value)
- **Generate automatically**
- **User attribute**
- **LDAP attribute**

b) **PIN Class**

From the drop-down list select one of the following options:

a)
- PIN classes allowed for station PINs. PIN classes are retrieved from the system the selected OpenScape 4000 Resource belongs to.
- **User attribute**
- **LDAP attribute**

c) **Individual PIN**

Tick the checkbox if you want the PIN to be created only for the selected class. In other case the system creates the PIN for all the available classes.

10) Click **Add** to add the new PIN to the PINs list.

11) Click **OK** to confirm the configuration.

Once the system verifies that supplied information is correct and all required attributes are filled in, the OpenScape 4000 Resource will be added to the list of the existing Resources.

12) Click **Save** to save changes to the User Template.

a) System:

- verifies that supplied information is correct
- creates and stores the new User Template.

NOTICE:

If the User Template configuration screen is closed without changes being saved, any modification of the mapped LDAP attributes will be lost.

NOTICE:

Countries like Italy or Belgium could have empty either ISDN_AreaCode or ISDN_LocalCode in their OpenScape 4000 numbering plan schemes. This was causing synchronization issues between CMP and OpenScape 4000 in the past which are now resolved. As a result 4000 ONS UC accounts can be set with such Italian or Belgium OpenScape 4000 numbers.

A new User Template is displayed in the list of the existing User Templates. The column **Resources** shows the icon that represents the OpenScape 4000 resource.

10.3.2.5 How to Create User Template with the OpenScape Xpressions Resource

The following chapter describes how to add the OpenScape Xpressions Resources to the User Template.

Prerequisites

Adequate administrative permission that allows management of User Templates.

NOTICE:

In order to use the LDAP attributes for creating the resources in User Templates, the following prerequisites has to be fulfilled:

LDAP connection has to be enabled in OS UM.

IMPORTANT:

Except for users not connected with LDAP (User Attributes with direct mapping, where display name can be filled with IM address)

The OS UM Users have been created via LDAP synchronization.

The resource templates required for the resource creation have to be available.

Step by Step

1) Navigate to **User Management** > **Administration** > **User Templates**

A list of the existing User Templates is displayed.

2) Click **Add** to create a new User Template.

A pop-up window **Add User Template** is displayed.

3) Navigate to the **Settings** area and fill in the following information:

a) **Name**

This is a mandatory and unique field that represents the name of the User Template.

b) **Description**

Briefly describes the User Template.

4) Navigate to the **Rules** area and from the drop-down list select the **OpenScape Xpressions** resource.

5) Click **Add** to configure the automatic creation of the **OpenScape Xpressions** resource.

   The configuration window (**Rules for automatic resource creation**), related to the **OpenScape Xpressions** resource is displayed.

   NOTICE:

   To create multiple OpenScape Xpressions Resources within a single User Template repeat this step and each time select different value (flavor) for the resource **Function**.

   Any of the resource **Function** values can be set at most once in one User Template, except the type **Other** which can be specified multiple times.

6) In the **Rules for automatic resource creation** window navigate to the **Setting** area to define:

   a) **Function**

   NOTICE:

   The resource **Function** field is available only for the resources that can be added multiple times, i.e.,OpenScape Voice, OpenScape Voice Softphone, OpenScape 4000, OpenScape Xpressions and External.

   From the drop-down list select one of the following functions (flavors):

   a) • **Fax**

   NOTICE:

   The FAX number of UM User is filled with the Business Fax attribute of User Template.

   In case Business Fax attribute is disabled, the FAX number of UM User will not be filled.

   • **Other**

   b) **Operation Mode**

   From the drop-down list choose one of the following options:

   a) • **Create new resources** to create a new OpenScape Voice Xpressions account and assign it to the User. If an existing OpenScape Voice Xpressions account matches the specified criteria, it will not be assigned to the User.

   • **Match existing Resources** to assign an OpenScape Xpressions account to the User only if an OpenScape Xpressions account that matches the specified criteria already exists in the system. A new OpenScape Xpressions account will not be created.

   • **Create new and match existing resources** to assign an OpenScape Xpressions account to the User. System will search for an existing OpenScape Xpressions account that matches the specified criteria and if it exists, it will be assigned to the User. In case it does not exist, a new OpenScape Xpressions account will be created.

7) In the **Rules for automatic resource creation** window navigate to the **Attributes** area to define the parameters for the automatic completion of the unique/mandatory fields (see the table below).

Table 26: Automatic completion rules for OpenScape Xpressions Resource

Attribute	Rule
Create the Xpressions User ID using	One of the following contact information are used (as it is, or only the part of it with the variable number of digits) - Template's Business Phone 1 - Template's Business Phone 2 - Template's Fax - an OSV resource already assigned to the User - an OpenScape 4000 resource already assigned to the User - User's Business Phone 1 - User's Business Phone 2. - User's Fax number - UM User ID - User attribute. Select one of the available values from the **User Attribute** drop-down list (see the Table: UM User attributes). - LDAP attribute.
Resource Template	Resource Templates are related to the Xpressions node connected to the CMP server. In case more than one Xpressions server is added to the system, the Resource Templates are distinguished using @<*IP of the Xpressions*> notation. If the Xpressions node is removed from the system and a new one is added, all User Templates that contain Xpressions resources have to be updated (a simple edit-save action with no other changes), so that the new Resource Templates are loaded. Also, Resource Template can be mapped to the LDAP attribute.

Attribute	Rule
Voice Mail	One of the following information is used: - Use Template’s Business Phone 1 - Use Template’s Business Phone 2 - Use Template’s Fax - Use an OSV resource already assigned to the User - Use an OpenScape 4000 resource already assigned to the User - Use User’s Business Phone 1 - Use User’s Business Phone 2. - Use User’s Fax number - User attribute. - LDAP attribute.
Business Phone	One of the following information is used: - Use Template’s Business Phone 1 - Use Template’s Business Phone 2 - Use Template’s Fax - Use an OSV resource already assigned to the User - Use an OpenScape 4000 resource already assigned to the User - Use User’s Business Phone 1 - Use User’s Business Phone 2. - Use User’s Fax number - User attribute. - LDAP attribute.
Cost info	One of the following information is used: - Disabled - Use User’s Business Phone 1 - Use User’s Business Phone 2. - Use User’s Fax number - User attribute. - LDAP attribute.

Attribute	Rule
UC_Mode	You can select one of the following values: - Xpressions mode / Not set = "X" (default) - UC mode = "U" - Xpressions mode with option to UC mode = "O" - UC mode with option to Xpressions mode = "N" - UC WebClient > XPR Web Assistant Access disabled = "D" - User attribute - LDAP attribute **NOTICE:** The expected mapped values from CMP/UM when a User or LDAP attribute is set by the administrator are the valid values from XPR side too: X, U, O, N, D or empty. In case a different value is set via User or LDAP attribute (which should be an exceptional case, since the drop down menu with valid values protects the administrator from such an error), this value will be sent and should be handled properly from XPR side.

Attribute	Rule
Business Fax	One of the following information is used: - Disabled - Use Template’s Business Phone 1 - Use Template’s Business Phone 2 - Use Template’s Fax - Use an OSV resource already assigned to the User - Use an OpenScape 4000 resource already assigned to the User - Use User’s Business Phone 1 - Use User’s Business Phone 2. - Use User’s Fax number - User attribute. - LDAP attribute
Common Name	In case of existing phones see the section at the end of the table. One of the following contact information are used as the attributes for the Common Name in case of a new resource: - Display Name - Last Name - First Name Last Name - Last Name, First Name. - User attribute. - LDAP attribute
Mobile Phone	One of the following information is used: - Disabled - Use User’s Business Phone 1 - Use User’s Business Phone 2. - Use the Mobile phone - User attribute. - LDAP attribute

Attribute	Rule
E-mail	One of the following information is used: - Disabled - Use E-mail address 1 - Use E-mail address 2 - User attribute. - LDAP attribute
Password	One of the following is used: - Constant value - User attribute. - LDAP attribute
PIN	One of the following is used: - Constant value (only numeric or empty values are allowed) - User attribute. - LDAP attribute
Windows ID	To configure the Single Sign-On, one of the following is used: - Disabled - Use E-mail address 1 - Use E-mail address 2 - Use IM Address - User attribute. - LDAP attribute
Microsoft Exchange	To configure the Single Sign-On, one of the following is used: - Disabled - Use E-mail address 1 - Use E-mail address 2 - Use IM Address - User attribute. - LDAP attribute

Attribute	Rule
Lotus Notes	To configure the Single Sign-On, one of the following is used: - Disabled - Use E-mail address 1 - Use E-mail address 2 - Use IM Address - User attribute. - LDAP attribute

IMPORTANT:

When the PIN value, configured in the Xpressions rules of the User Template, is empty, the default PIN configured in Xpressions will be used.

Common name in case of existing phones

Depending on the selected **operation mode**, different options are given regarding the display name.

- **1.** If the selected operation mode is "**Create new resources**", then the below cases exist for the display name:

  -) "**In case of match**" refers to resources that already exist, which is not applicable.

  -) "**In case of create**" refers to resources that will be created. The selected value in the drop down list will be used to populate the new

Xpressions resource's common name from the corresponding option (UM user's property or LDAP attribute).

- **2.** If the selected operation mode is "**Match existing resources**", then the below cases exist for the display name:

  -) "**In case of match**" refers to resources that already exist:

  If the checkbox is checked then any matching Xpressions resource will keep its common name

  If the check box is unchecked then the common name of the Xpressions resource will be populated from the corresponding option (UM user's property or LDAP attribute).

  The accompanying text "**In case of match**" is moved in this case to accompany the below drop box option.

  -) "**In case of create**" refers to resources that will be created, which is not applicable.

- **3.** If the selected operation mode is "**Create new and match existing resources**", then the below cases exist for the common name:

  -) "**In case of match**" refers to resources that already exist:

  If the check box is checked then any matching Xpressions resource will keep its common name. For resources that will be created the selected value in the drop down list will be used to populate the new Xpressions resource's common name from the corresponding option (UM user's property or LDAP attribute).

  If the check box is unchecked then the display name of the Xpressions resource (new or existing) will be populated from the corresponding option (UM user's property or LDAP attribute).

  The accompanying text "**In case of match**" disappears and the below drop box's text changes from "**In case of create**" to "**In case of create/ match**".

  NOTICE:

  At least one Resource Template per each Resource type must be specified.

As long as OS UM is connected to the LDAP directory, it is allowed to define:

a) a direct mapping to LDAP attributes for any attribute required for the resource creation
b) an advanced mapping to LDAP attributes for any attribute required for the resource creation.

   Click **Advanced...** and then in the **Advanced Mapping** pop-up window define the Advanced Mappings rules.

   NOTICE:

   You can select previously defined advanced rule. In case where a new advanced rule is created, this new rule is going to replace previously defined rule.

   ---

8) Click **OK** to confirm the configuration.

   Once the system verifies that supplied information is correct and all required attributes are filled in, the OpenScape Xpressions Resource will be added to the list of the existing Resources.

9) Click **Save** to save changes to the User Template.

   a) System:

   - verifies that supplied information is correct
   - creates and stores the new User Template.

> **NOTICE:**
>
> If the User Template configuration screen is closed without changes being saved, any modification of the mapped LDAP attributes will be lost.

A new User Template is displayed in the list of the existing User Templates. The column **Resources** shows the icon that represents the OpenScape Xpressions resource.

Next steps

> **NOTICE:**
>
> In case of upgrade to V7, the pre-existing User Templates with the OpenScape Xpressions resource that use one of the obsolete rules (see the table below, column Obsolete rule) for the attributes (column Attribute), will be automatically replaced based on the new behavior (see the column New behavior).

Table 27: Obsolete rules for OpenScape Xpressions resource

Attribute	Obsolete rule	New behavior
Create the Xpressions User ID using	the OSV resource assigned to this User Template	**If the User Template does not contain rules for a UC resource:** - The OSV resource created with this template is modified to have the value **Business Phone 1** for the resource **Function** - The User ID selection rule is changed to **User's Business Phone 1**
		If the User Template does not contain rules for a UC resource and the UC resource ONS rule has been migrated to have the value Business Phone 1 for the resource Function and that resource is an OSV: - The User ID selection rule is changed to **User's Business Phone 1**

Attribute	Obsolete rule	New behavior
		If the User Template does contain rules for a UC resource and the UC resource ONS rule has been migrated to have the value Business Phone 1 for the resource Function and that resource is an OpenScape 4000: - The OSV resource created with this template is modified to have the value **Business Phone 2** for the resource **Function** - The User ID selection rule is changed to **User's Business Phone 2**
		If the User Template does contain rules for a UC resource and the UC resource ONS rule has not been migrated to have any values for the resource Function: - The OSV resource created with this template is modified to have the value **Business Phone 1** for the resource **Function** - The User ID selection rule is changed to **User's Business Phone 1**
	the HiPath 4000 resource assigned to this User Template	**If the User Template does not contain rules for a UC resource:** - The OpenScape 4000 resource created with this template is modified to have the value **Business Phone 1** for the resource **Function** - The User ID selection rule is changed to **User's Business Phone 1**
		If the User Template does not contain rules for a UC resource and the UC resource ONS rule has been migrated to have the value Business Phone 1 for the resource Function and that resource is an OpenScape 4000: - The User ID selection rule is changed to **User's Business Phone 1**
		If the User Template does contain rules for a UC resource and the UC resource ONS rule has been migrated to have the value Business Phone 1 for the resource Function and that resource is an OSV: - The OpenScape 4000 resource created with this template is modified to have the value **Business Phone 2** for the resource **Function** - The User ID selection rule is changed to **User's Business Phone 2**

Attribute	Obsolete rule	New behavior
		If the User Template does contain rules for a UC resource and the UC resource ONS rule has not been migrated to have any values for the resource Function: - The OpenScape 4000 resource created with this template is modified to have the value **Business Phone 1** for the resource **Function** - The User ID selection rule is changed to **User's Business Phone 1**
Voice Mail	Use the OSV resource assigned to this User Template	**If the User Template does not contain rules for a UC resource:** - The OSV resource created with this template is modified to have the value **Business Phone 1** for the resource **Function** - The Voice Mail selection rule is changed to **Use User's Business Phone 1**
		If the User Template does not contain rules for a UC resource and the UC resource ONS rule has been migrated to have the value Business Phone 1 for the resource Function and that resource is an OSV: - The Voice Mail selection rule is changed to **Use User's Business Phone 1**
		If the User Template does contain rules for a UC resource and the UC resource ONS rule has been migrated to have the value Business Phone 1 for the resource Function and that resource is an OpenScape 4000: - The OSV resource created with this template is modified to have the value **Business Phone 2** for the resource **Function** - The Voice Mail selection rule is changed to **Use User's Business Phone 2**
		If the User Template does contain rules for a UC resource and the UC resource ONS rule has not been migrated to have any values for the resource Function: - The OSV resource created with this template is modified to have the value **Business Phone 1** for the resource **Function** - The Voice Mail selection rule is changed to **Use User's Business Phone 1**

Attribute	Obsolete rule	New behavior
	Use the HiPath 4000 resource assigned to thisUser Template	**If the User Template does not contain rules for a UC resource:** - The OpenScape 4000 resource created with this template is modified to have the value **Business Phone 1** for the resource **Function** - The Voice Mail selection rule is changed to **Use User's Business Phone 1**
		If the User Template does not contain rules for a UC resource and the UC resource ONS rule has been migrated to have the value Business Phone 1 for the resource Function and that resource is an OpenScape 4000: - The Voice Mail selection rule is changed to **Use User's Business Phone 1**
		If the User Template does contain rules for a UC resource and the UC resource ONS rule has been migrated to have the value Business Phone 1 for the resource Function and that resource is an OSV: - The OpenScape 4000 resource created with this template is modified to have the value **Business Phone 2** for the resource **Function** - The Voice Mail selection rule is changed to **Use User's Business Phone 2**
		If the User Template does contain rules for a UC resource and the UC resource ONS rule has not been migrated to have any values for the resource Function: - The OpenScape 4000 resource created with this template is modified to have the value **Business Phone 1** for the resource **Function** - The Voice Mail selection rule is changed to **Use User's Business Phone 1**
Business Phone	Use the OSV resource assigned to this User Template	**If the User Template does not contain rules for a UC resource:** - The OSV resource created with this template is modified to have the value **Business Phone 1** for the resource **Function** - The Business Phone selection rule is changed to **Use User's Business Phone 1**

Attribute	Obsolete rule	New behavior
		If the User Template does not contain rules for a UC resource and the UC resource ONS rule has been migrated to have the value Business Phone 1 for the resource Function and that resource is an OSV: - The Business Phone selection rule is changed to **Use User's Business Phone 1**
		If the User Template does contain rules for a UC resource and the UC resource ONS rule has been migrated to have the value Business Phone 1 for the resource Function and that resource is an OpenScape 4000: - The OSV resource created with this template is modified to have the value **Business Phone 2** for the resource **Function** - The Business Phone selection rule is changed to **Use User's Business Phone 2**
		If the User Template does contain rules for a UC resource and the UC resource ONS rule has not been migrated to have any values for the resource Function: - The OSV resource created with this template is modified to have the value **Business Phone 1** for the resource **Function** - The Business Phone selection rule is changed to **Use User's Business Phone 1**
	Use the HiPath 4000 resource assigned to this User Template	**If the User Template does not contain rules for a UC resource:** - The OpenScape 4000 resource created with this template is modified to have the value **Business Phone 1** for the resource **Function** - The Business Phone selection rule is changed to **Use User's Business Phone 1**
		If the User Template does not contain rules for a UC resource and the UC resource ONS rule has been migrated to have the value Business Phone 1 for the resource Function and that resource is an OpenScape 4000: - The Business Phone selection rule is changed to **Use User's Business Phone 1**

Attribute	Obsolete rule	New behavior
		If the User Template does contain rules for a UC resource and the UC resource ONS rule has been migrated to have the value Business Phone 1 for the resource Function and that resource is an OSV: - The OpenScape 4000 resource created with this template is modified to have the value **Business Phone 2** for the resource **Function** - The Business Phone selection rule is changed to **Use User's Business Phone 2**
		If the User Template does contain rules for a UC resource and the UC resource ONS rule has not been migrated to have any values for the resource Function: - The OpenScape 4000 resource created with this template is modified to have the value **Business Phone 1** for the resource **Function** - The Business Phone selection rule is changed to **Use User's Business Phone 1**
Business Fax	Use the OSV resource assigned to this User Template	**If the User Template does not contain rules for a UC resource:** - The OSV resource created with this template is modified to have the value **Business Phone 1** for the resource **Function** - The Business Fax selection rule is changed to **Use User's Business Phone 1**
		If the User Template does not contain rules for a UC resource and the UC resource ONS rule has been migrated to have the value Business Phone 1 for the resource Function and that resource is an OSV: - The Business Fax selection rule is changed to **Use User's Business Phone 1**
		If the User Template does contain rules for a UC resource and the UC resource ONS rule has been migrated to have the value Business Phone 1 for the resource Function and that resource is an OpenScape 4000: - The OSV resource created with this template is modified to have the value **Business Phone 2** for the resource **Function** - The Business Fax selection rule is changed to **Use User's Business Phone 2**

Attribute	Obsolete rule	New behavior
		If the User Template does contain rules for a UC resource and the UC resource ONS rule has not been migrated to have any values for the resource Function: - The OSV resource created with this template is modified to have the value **Business Phone 1** for the resource **Function** - The Business Fax selection rule is changed to **Use User's Business Phone 1**
	Use the HiPath 4000 resource assigned to this User Template	**If the User Template does not contain rules for a UC resource:** - The OpenScape 4000 resource created with this template is modified to have the value **Business Phone 1** for the resource **Function** - The Business Fax selection rule is changed to **Use User's Business Phone 1**
		If the User Template does not contain rules for a UC resource and the UC resource ONS rule has been migrated to have the value Business Phone 1 for the resource Function and that resource is an OpenScape 4000: - The Business Fax selection rule is changed to **Use User's Business Phone 1**
		If the User Template does contain rules for a UC resource and the UC resource ONS rule has been migrated to have the value Business Phone 1 for the resource Function and that resource is an OSV: - The OpenScape 4000 resource created with this template is modified to have the value **Business Phone 2** for the resource **Function** - The Business Fax selection rule is changed to **Use User's Business Phone 2**
		If the User Template does contain rules for a UC resource and the UC resource ONS rule has not been migrated to have any values for the resource Function: - The OpenScape 4000 resource created with this template is modified to have the value **Business Phone 1** for the resource **Function** - The Business Fax selection rule is changed to **Use User's Business Phone 1**

10.3.2.6 How to Create User Template with the Unified Communications Resource

The following chapter describes how to add the Unified Communications Resources to the User Template.

Prerequisites

Adequate administrative permission that allows management of User Templates.

NOTICE:

In order to use the LDAP attributes for creating the resources in User Templates, the following prerequisites have to be fulfilled:

LDAP connection has to be enabled in OS UM.

The OS UM Users have been created via LDAP synchronization.

The resource templates required for the resource creation have to be available.

You must configure the SMTP server from **CMP > SMTP Server** and have an e-mail for the feature **Send password and PIN via E-mail** to work properly.

Step by Step

1) Navigate to **User Management** > **Administration** > **User Templates**

A list of the existing User Templates is displayed.

2) Click **Add** to create a new User Template.

A pop-up window **Add User Template** is displayed.

3) Navigate to the **Settings** area and fill in the following information:

a) **Name**

This is a mandatory and unique field that represents the name of the User Template.

b) **Description**

Briefly describes the User Template.

4) Navigate to the **Rules** area and from the drop-down list select the **Unified Communications** resource.

5) Click **Add** to configure the automatic creation of the **Unified Communications** resource.

The configuration window **Rules for automatic resource creation**, related to the **Unified Communications** resource is displayed.

6) In the **General** tab, navigate to the **Settings** area.

The only available **Operation Mode** is to create a new Unified Communications resource (i.e., **Create new resources**) and assign it to the User.

7) Navigate to the **Attributes** area to define the parameters for the automatic completion of the unique/mandatory fields (see the table below).

Table 28: Automatic completion rules for UC Resource (part one)

Attribute	Rule
Attributes	
UC Profile	Selection of one of the following: - Essential - Professional - Team - Team Administrator - Team with Xpressions - User attribute. - LDAP attribute.
ONS Number	Selection of one of the following: - Use Template's Business Phone 1 (OpenScape Voice and OpenScape 4000 resources are supported) - Use Template's Business Phone 2 (OpenScape Voice and OpenScape 4000 resources are supported) - User attribute - LDAP attribute
WebRTC Number	Selection of one of the following: - Use Template's Business Phone 1 (OpenScape Voice, OpenScape Voice Softphone and OpenScape 4000 resources are supported) - Use Template's Business Phone 2 (OpenScape Voice, OpenScape Voice Softphone and OpenScape 4000 resources are supported) - User attribute - LDAP attribute
Assign WebRTC Profile	The WebRTC profile is mandatory for the WebRTC feature to be functional.Check the checkbox to assign the WebRTC profile. You can configure the WebRTC along with another profile (for example, Team with WebRTC). In this case, you don't need to check the checkbox (no additional licenses will be used in case of having both the checkbox checked and the WebRTC permission existing in another chosen profile).

Attribute	Rule
IM Address	The following options are used in order to extract the IM Address: - **Use IM Address** In this case OpenScape User Management does not need to do anything when creating the UC Resource, since the IM Address of the UM User is stored in the same field of the same contact record. **- UC Account Login Name@XMPP Domain** Use UC Resource's username appended by the XMPP Domain Name. The XMPP Domain Name can be found by the UC Assistant querying presence (**CMP** > **Configuration** > **Unified Communications** > **Presence and IM** > **Presence and Instant Messaging Configuration**). **- User attribute** **- LDAP attribute**
	Subscription Codes of the WebRTC Subscriber **NOTICE:** This section is only enabled for configuration if we have set a value for the option **WebRTC Number**.
Toggle MLHG Make Busy Toggle MLHG Stop Hunt Group Call Pickup	Selection of one of the following: - No value (default) **NOTICE:** Keeping the default blank value, will result in the template not affecting the user's already assigned MLHG Codes - Constant value **NOTICE:** Not entering a value when selecting the constant value option, will result in the deletion of the previously assigned code. - User attribute - LDAP attribute

NOTICE:

The first two options for ONS Number are available only when the OSV Element manager is registered in the system, whereas the next two options are available only when the OpenScape 4000 Element manager is registered.

INFO:

Currently, the E/A - Cockpit UC Resource is not supported via OS UM. To create/assign the E/A Cockpit, navigate to

Configuration > **Unified Communications** > **Accounts** > **List** > **Add Users** > **Profiles**.

8) Navigate to the **Authentication** area to define the parameters for the user authentication (see the table below).

In the **Send E-mail area**, you can generate automatically the UC password and telephony PIN or receive them via e-mail.

Send password and PIN via E-mail: Check this checkbox to receive password and PIN via e-mail. When you enable this attribute, the attributes **User has to change login password at next login** in the **Login** and **Telephony PIN** fields are enabled automatically and become unconfigurable, for security purposes. You can select to send the "Constant Value" or the "User attribute" values, not only the "Generate automatically" one.

In the **Login** and **Telephony PIN** areas, configure the following parameters:

Table 29: Automatic completion rules for UC Resource (part two)

Attribute	Rule
Login password	Selection of one of the following: - Constant value -Generate automatically. When you select this option, the attributes **Send password and PIN via E-mail** and **User has to change login password at next login** are automatically selected. - User attribute - LDAP attribute To force the UM User to change the password on the first login, tick the option **User has to change login password at next login**.

Attribute	Rule
Telephony PIN	Selection of one of the following: - Constant value -Generate automatically. When you select this option, the attributes **Send password and PIN via E-mail** and **User has to change Telephony PIN at next login** are automatically selected. - User attribute - LDAP attribute To force the UM User to change the telephony PIN on the first login, tick the option **User has to change telephony PIN at next login**.

As long as OS UM is connected to the LDAP directory, it is allowed to define:

a) a direct mapping to LDAP attributes for any attribute required for the resource creation

b) an advanced mapping to LDAP attributes for any attribute required for the resource creation.

Click **Advanced...** and then in the **Advanced Mapping** pop-up window define the Advanced Mappings rules.

NOTICE:

You can select previously defined advanced rule. In case where a new advanced rule is created, this new rule is going to replace previously defined rule.

9) Click the **Visibility Groups** tab. You can select to:

- Keep the previously connected Visibility Groups and add the ones configured in the User Template
- Disconnect the previously connected Visibility Groups and connect the ones configured in the User Template

10) Click **Add**. A pop-up window **Configure Visibility Groups in User Template** appears. Configure the following parameters:

- **Visibility Group Name**: Select the Visibility Group you want to configure
- **Advanced**: Click this button to use advanced mapping. A pop-up window **Advanced Mappings** appears, where you can create and test an expression. After saving the expression will be mapped to the selected attribute. For more information, see How to perform Advanced Attribute Mapping

NOTICE:

The **Advanced...** button is activated only for LDAP/ User attribute as **Visibility Group Name**.

11) You can select any Visibility Group and click **Edit** to modify its Advanced Mapping parameters.

12) To remove a Visibility Group, select it and click **Delete**.

13) Click **OK** to confirm the configuration.

System verifies that supplied information is correct.

14) Click **Save** to save changes to the User Template.

a) System:

- verifies that supplied information is correct
- creates and stores the new User Template.

NOTICE:

If the User Template configuration screen is closed without changes being saved, any modification of the mapped LDAP attributes will be lost.

A new User Template is displayed in the list of the existing User Templates.

Next steps

Once **Unified Communications** resource is added to the User Template and the Groupware, SSO, Xpressions and MS Teams Integration features have been configured in the system, the following advanced resource creation rule can be set:

- To configure the Groupware and allow the assignment of the UM Users to a Groupware connectors (MS Exchange server or IBM Domino), click on ▸ to open **Groupware** pop-up and then select:

  1) Groupware Assignment

  this attribute can take the following values: **Disabled** or **Default LineId**

  2) Mailbox ID

  this attribute can take the following values: **Use User ID** or **LDAP attribute**.

  3) Mailbox Address

  this attribute can take the following values: **Use E-mail address 1**,**Use E-mail address 2** or **LDAP attribute**.

  NOTICE:

  Groupware option is visible only if the groupware connectors are configured.

- To configure the Single Sign-On, click on ▸ to open **Single Sign On** pop-up window and then:

  For **Webclient SSO** select:

  1) **External System**

     this attribute can take the following values: **Disabled**, **<external Systems that have been configured in JAAS file>** or **LDAP Attribute**.
  2) **Account** (usename@domain)

     this attribute can take the following values: **Use E-mail address 1**,**Use E-mail address 2**, **User IM Address** or **LDAP Attribute**.

  NOTICE:

  If Webclient SSO is not configured, the **Webclient SSO** section is not displayed.

  For **SPNEGO/SOAP SSO** select:

  1) **Domain**

     this attribute can take the following values: **Disabled**, **<external Systems that have been configured in krb.conf>** or **LDAP Attribute**.
  2) **Username**

     this attribute can take the following values: **Use E-mail address 1**,**Use E-mail address 2**, **User IM Address** or **LDAP Attribute**.

  NOTICE:

  If SPNEGO/SOAP SSO is not configured the **SPNEGO/ SOAP SSO** section is not displayed.

- To configure the MS Teams Integration, click on ▸ to change to the desired option.

  For **UC-Microsoft Teams Integration** select:

  1) **MS Teams External System**

     this attribute can take the following values: **Disabled**, **<external Systems that have been configured in JAAS file>**.
  2) **MS Teams Account** (usename@domain)

     this attribute can take the following values: **Use E-mail address 1**,**Use E-mail address 2**, **User Attribute** or **LDAP Attribute**.

  NOTICE: The presence of **MS Teams Connector** option indicates that the MS Teams is configured at Openscape UC. Instructions to configure MS Teams Presence may be found at *OpenScape UC Application V10, Configuration and Administration, Administrator Documentation, Chapter: Synchronising the MS Teams Presence with Openscape UC*.

- To enable/disable the Xpressions Integration, click on to change to the desired option.

NOTICE:

Xpressions integration option is visible only if the Xpressions Element Manager is available in the system.

10.3.2.7 How to Create User Template with the External Resource

The following chapter describes how to add the External Resources to the User Template.

Prerequisites

Adequate administrative permission that allows management of User Templates.

NOTICE:

In order to use the LDAP attributes for creating the resources in User Templates, the following prerequisites has to be fulfilled:

LDAP connection has to be enabled in OS UM.

The OS UM Users have been created via LDAP synchronization.

The resource templates required for the resource creation have to be available.

Step by Step

1) Navigate to **User Management** > **Administration** > **User Templates**

A list of the existing User Templates is displayed.

2) Click **Add** to create a new User Template.

A pop-up window **Add User Template** is displayed.

3) Navigate to the **Settings** area and fill in the following information:

a) **Name**

This is a mandatory and unique field that represents the name of the User Template.

b) **Description**

Briefly describes the User Template.

4) Navigate to the **Rules** area and from the drop-down list select the **External** resource.

5) Click **Add** to configure the automatic creation of the **External** resource.

The configuration window (**Rules for automatic resource creation**), related to the **External** resource is displayed.

NOTICE:

To create multiple External Resources within a single User Template repeat this step and each time select different value (flavor) for the resource **Function**.

Any of the resource **Function** values can be set at most once in one User Template, except the type **Other** which can be specified multiple times.

---

6) In the **Rules for automatic resource creation** window navigate to the **Setting** area to define:

a) **Function**

NOTICE:

The resource **Function** field is available only for the resources that can be added multiple times, i.e.,OpenScape Voice, OpenScape Voice Softphone, OpenScape 4000, OpenScape Xpressions and External.

From the drop-down list select one of the following functions (flavors):

a)
- **Business Phone 1**
- **Business Phone 2**
- **Fax**
- **Other**

b) **Resource Name**

From the drop-down list choose one of the following options:

a)
- **Use resource ID** (default value)
- **Use resource function name**
- **Constant value**
- **User attribute**

IMPORTANT:

For users not connected with LDAP (e.g. display name can be filled with IM address)

- **LDAP attribute**

7) In the **Rules for automatic resource creation** window navigate to the **Attributes** area to define the **Resource Number** attribute.

From the drop-down list choose one of the following options:

a)
- **User's home phone** (default value)
- **User's mobile phone**
- **Constant value**

- **User attribute**

  IMPORTANT:

  For users not connected with LDAP (e.g. display name can be filled with IM address)

- **LDAP attribute**

As long as OS UM is connected to the LDAP directory, it is allowed to define:

a) a direct mapping to LDAP attributes for any attribute required for the resource creation

b) an advanced mapping to LDAP attributes for any attribute required for the resource creation.

   Click **Advanced...** and then in the **Advanced Mapping** pop-up window define the Advanced Mappings rules.

   NOTICE:

   You can select previously defined advanced rule. In case where a new advanced rule is created, this new rule is going to replace previously defined rule.

8) Click **OK** to confirm the configuration.

Once the system verifies that supplied information is correct and all required attributes are filled in, the External Resource will be added to the list of the existing Resources.

9) Click **Save** to save changes to the User Template.

a) System:

- verifies that supplied information is correct
- creates and stores the new User Template.

NOTICE:

If the User Template configuration screen is closed without changes being saved, any modification of the mapped LDAP attributes will be lost.

A new User Template is displayed in the list of the existing User Templates. The column **Resources** shows the icon that represents the External resource.

10.3.2.8 How to Create User Template with the Xpressions/UC Integration Resource

The creation of User Templates that contain Xpressions/UC Integration type of resources is no longer supported. Starting from OS UM V7 the aforementioned resource type has been appropriately replaced in the User Template (for more information, please refer to the *Next steps* at the end of this chapter and also see the chapter " *How to Create User Template with the OpenScape Xpressions Resource*").

Prerequisites

Adequate administrative permission that allows management of User Templates.

Step by Step

1) Navigate to **User Management** > **Administration** > **User Templates**

A list of the existing User Templates is displayed.

2) Click **Add** to create a new User Template.

A pop-up window **Add User Template** is displayed.

3) Fill in the following User Template information:

a) **Details**:

- – **Name**

  This is a mandatory and unique field that represents the name of the User Template.

- – **Description**

  Briefly describes the User Template.

b) **Available Resource Types**

Shows separate sections for each resource type (OpenScape Voice, HiPath 4000, OpenScape Xpressions, Unified Communications, Xpressions/UC Integration) that is supported by the current deployment.

4) Within the **Xpressions/UC Integration** section, click **Configure...** to configure the integration of the OpenScape Xpressions and Unified Communications accounts.

The **Rules for automatic resource creation** window is displayed.

5) Specify the following:

a) **Operation Mode**

a) • **Disabled** to disable the Integration of OpenScape Xpressions and Unified Communications accounts.

• **Enabled** to enable the Integration of OpenScape Xpressions and Unified Communications accounts.

b) **OpenScape Xpressions/Unified Communications integration**

NOTICE:

When operation mode is set to **Enabled**, system will update the value of the CONUSER attribute of the User's Xpressions resource with the User's UC account information (UC Account Login Name@UC domain).

---

6) Click **OK** to confirm the configuration.

System verifies that supplied information is correct.

7) Click **Save** to save changes to the User Template.

a) System:

- verifies that supplied information is correct
- creates and stores the new User Template.

A new User Template is displayed in the list of the existing User Templates.

Next steps

Starting from OS UM V7 all pre-existing User Templates with the Xpressions/UC Integration resource type will be migrated based on the following rules:

1) When an existing template contains both, the Xpessions/UC Integration resource and Unified Communications resource, then this template will be migrated to contain Unified Communications resource with the enabled **Xpressions Integration** option (refer to the chapter " *How to Create User Template with the Unified Communications Resource*").
2) When an existing template contains only the Xpessions/UC Integration resource and there are no Unified Communications resources, then:
   a) The old template becomes obsolete, but you can still use it. It is allowed to modify the rules for automatic resource creation, but you can not add a new or remove the existing resources creation rules from that template.
   b) The Xpessions/UC Integration resource present in the obsolete template is represented as a separate entry in the Resource list (see the table below):

Resource Type	Resource Function	Operation Mode
OpenScape Xpessions	Xpressions/UC integration	Match existing resources as an Operation Mode

   c) All other types of resources from the obsolete template remain the same.

NOTICE:

It is suggested to replace the obsolete template with a new User Template that contains Unified Communications resource and enables Xpressions Integration (i.e., **Xpressions Integration** option is enabled).

10.3.2.9 How to Create User Template with the Common Management Platform Administrator

The following chapter describes how to add the CMP Administrator Resources to the User Template. This allows you to create CMP users through UM. This action consumes OS CMP User Management User licenses for every UM User and Administrator created.

Prerequisites

Adequate administrative permission that allows management of User Templates.

NOTICE:

To use the LDAP attributes for creating the resources in User Templates, the following prerequisites have to be fulfilled:

- LDAP connection has to be enabled in OS UM.

- The OS UM Users have been created via LDAP synchronization.

Step by Step

1) Navigate to **User Management** > **Administration** > **User Templates**

A list of the existing User Templates is displayed.

2) Click **Add** to create a new User Template.

A pop-up window **Add User Template** is displayed.

3) Navigate to the **Settings** area and fill in the following information:

a) **Name**

This is a mandatory and unique field that represents the name of the User Template.

b) **Description**

Briefly describes the User Template.

4) Navigate to the **Rules** area and from the drop-down list select the **CMP Administrator** resource.

5) Click **Add** to configure the automatic creation of the **CMP Administrator** resource.

The configuration window **Rules for automatic resource creation**, related to the **CMP Administrator** resource is displayed.

6) Navigate to the **Settings** area.

The only available **Operation Mode** is to create a new CMP Administrator resource (meaning, **Create new resources**) and assign it to the User.

7) Click the **Authentication** tab to define the parameters for the user authentication (see the table below).

Table 30: Automatic completion rules for CMP Resource

Attribute	Rule
Login password	Select one of the following: - Constant value - User attribute - LDAP attribute • To force the CMP Administrator User to change the password on the first login, tick the option **User has to change login password at next login**. • To lock the user, tick the option **User locked** • To make the password never to expire, tick the option **Login password never expires** • To allow Call Admission Control, tick the option **CAC**

Attribute	Rule
Single Sign-On	Select one of the following values for the **Domain** parameter: - Disabled - EXAMPLE.NET When you select the EXAMPLE.NET value, you have an SSO configured and a valid domain, you can select one of the following values for the Username parameter: - Use E-mail address 1 - Use E-mail address 2 - User attribute - LDAP attribute

As long as OS UM is connected to the LDAP directory, it is allowed to define:

a) a direct mapping to LDAP attributes for any attribute required for the resource creation

b) an advanced mapping to LDAP attributes for any attribute required for the resource creation.

Click **Advanced...** and then in the **Advanced Mapping** pop-up window define the Advanced Mappings rules.

NOTICE:

You can select previously defined advanced rule. In case where a new advanced rule is created, this new rule is going to replace previously defined rule.

---

8) Click the **Profiles** tab.Here you can configure the administrator's profiles.

9) Click **Add**. A pop-up window **Configure CMP Administrator Profiles in User Template** appears. Configure the following parameters:

- **Application**: Select the application you want to apply to the CMP Administrator profile. The available values are:
  - – CMP
  - – Device Management
  - – H8kAst
  - – OSSBC Assistant
  - – OpenScape Accounting
  - – OpenScape FM
  - – Symphonia
  - – User Attribute
  - – LDAP Attribute

  When you select User Attribute or LDAP Attribute, the **Advanced** option is configurable
- **Profile Name**: Depending on the value you selected for the **Application** parameter, you get the relevant values for the **Profile Name**

10) Click **Add** to apply your settings. You can add multiple profiles to the CMP Administrator
11) You can select any Profile and click **Edit** to modify its parameters. To remove a Profile, select it and click **Delete**
12) Click the **External ID** tab. Here you can configure external IDs to the CMP Administrator. The External IDs are unique for each user
13) Click **Add**. A pop-up window **Configure CMP Administrator External IDs in User Template** appears. Configure the following parameters:
    - **External ID**: Available values:
      - – Constant value
      - User attribute
      - LDAP attribute
    - **Assigned External System ID**: Available values:
      - – Constant value
      - User attribute
      - LDAP attribute

      NOTICE:

      You can't select Constant value for both parameters, to avoid having the same External IDs for more than one users
14) Click **OK** to save your settings

NOTICE:

When a User Template with CMP Administrator rules is re-applied to a UM User, the password rules are not applied. To re-apply the password rules, change the password rule or reset the configuration. The password will also be modified when another User Template is applied to the same UM User

NOTICE:

When you remove a profile from the Profile Rules of the template and re-apply the template to a UM user, the extra profiles are not removed. When a different template is applied, the extra profiles are removed

NOTICE:

When you apply templates with External IDs Rules, the existing External IDs of the UM user are not removed

10.3.2.10 How to Create User Template with the Unify Phone

You can add the Unify Phone Resources to the User Template. This allows you to create Unify Phone users through UM.

Prerequisites

Adequate administrative permission that allows management of User Templates.

A User Template with the OpenScape Voice Resource and a User Template with the OpenScape Mobile (OSMO) Resource must have been created.

Step by Step

1) Navigate to **User Management** > **Administration** > **User Templates**

   A list of the existing User Templates is displayed.
2) Click **Add** to create a new User Template.

   The **Add User Template** window opens.
3) Navigate to the **Settings** area and enter the following information:
   a) **Name**- Mandatory and unique field representing the name of the User Template.
   b) **Description** - Briefly describes the User Template.
4) Navigate to the **Rules** area and select the **Unify Phone** resource from the drop-down list.
5) Click **Add** to configure the automatic creation of the **Unify Phone** resource.

   The **Rules for automatic resource creation**configuration window opens.
6) Navigate to the **Settings** area.

   The only available **Operation Mode** is **Create new resources**, which creates a new Unify Phone resource and assigns it to the user.
7) Navigate to the **Attributes** area to define the parameters for automatic completion of unique/mandatory fields:

Table 31: Automatic completion rules for OSV Resource

Attribute	Rule
Tenant	From the drop-down list, select the tenant for which you want to create a User Template with Unify Phone. **NOTICE:** Each template can be associated with only one tenant. To use the same configurations for another tenant, create a separate template.

Attribute	Rule
Resource Name	From the drop-down list, select one of the suggested resource names: - Use E-mail address 1 - Use E-mail address 2 - User attribute - LDAP attribute
Phone Number (ONS)	From the drop-down list, select how to assign the phone number for the user: - Use Template's Business Phone 1 - Use Template's Business Phone 2 - User attribute - LDAP attribute
Configuration	From the drop-down list, select the SBC configuration and specify the attribute: - User attribute - LDAP attribute For more information, see How to Create a new SBC configuration for Unify Phone users on page 677.

As long as OS UM is connected to the LDAP directory, you can define:

a) A direct mapping to LDAP attributes for any attribute required for the resource creation.

b) An advanced mapping to LDAP attributes for any attribute required for resource creation.

   Click **Advanced...** to open the **Advanced Mapping** window and define Advanced Mappings rules.

NOTICE:

You can select a previously defined advanced rule.
If a new advanced rule is created, it will replace any previously defined rule.

---

8) Click **OK** to confirm the configuration.

Once the system verifies that the supplied information is correct and all required attributes are filled in, the Unify Phone Resource will be added to the list of the existing Resources.

9) Click **Save** to apply the changes.

The system:

- Verifies that supplied information is correct.
- Creates and stores the new User Template.

NOTICE:

If the User Template configuration screen is closed without saving changes, any modifications of the mapped LDAP attributes will be lost.

NOTICE:

If the Unify Phone Settings have not been configured, the following message is displayed: **Unify Phone Settings are not configured properly**.

To configure the Unify Phone Settings see Unify Phone Configurations on page 677.

10.3.2.11 How to Create User Template with Zoom

The following chapter describes how to add the Zoom Resources to the User Template. This allows you to create Zoom users through UM.

Prerequisites

1) Adequate administrative permission that allows management of User Templates.
2) A User Template with the OpenScape Voice Resource.
3) Connection with a CloudLink tenant.

Step by Step

1) Navigate to **User Management** > **Administration** > **User Templates**

   A list of the existing User Templates is displayed.
2) Click **Add**.

   The **Add User Template** window opens.
3) Navigate to the **Settings** area and fill in the following information:
   a) **Name**- Mandatory and unique field that represents the name of the User Template.
   b) **Description**- Briefly describes the User Template.
4) Navigate to the **Rules** area and select the **Zoom** resource from the drop-down list.
5) Click **Add** to configure the automatic creation of the **Zoom** resource.

   The **Rules for automatic resource creation** window opens.
6) Navigate to the **Settings** area.

   The only available **Operation Mode** is **Create new resources**, which creates a new Unify Phone resource and assigns it to the user.

7) Navigate to the **Attributes** area to define the parameters for automatic completion of unique/mandatory fields:

Table 32: Automatic completion rules for OSV Resource

Attribute	Rule
Resource Name	From the drop-down list, select one of the suggested resource names: - Use E-mail address 1 - Use E-mail address 2 - User attribute
Phone Number (ONS)	From the drop-down list, select how to assign the phone number for the user: - Use Template's Business Phone 1 - Use Template's Business Phone 2 - User attribute
Configuration	From the drop-down list, select the SBC configuration and specify the attribute: - User attribute - LDAP attribute For more information, see How to Create a new Zoom configuration on page 684.
Voicemail	From the drop-down list, specify the attribute: Constant value User attribute

8) Click **OK** to confirm the configuration.

Once the system verifies that supplied information is correct and all required attributes are filled in, the Zoom Resource will be added to the list of the existing Resources.

9) Click **Save** to save changes to the User Template.

The system:

- Verifies that supplied information is correct
- Creates and stores the new User Template.

10.3.3 How to Edit User Templates

The following paragraphs explain how to modify User Templates.

Prerequisites

Adequate administrative permission that allows management of User Templates.

NOTICE:

In order to use the LDAP attributes for creating the resources in User Temples, the following prerequisites has to be fulfilled:

LDAP connection has to be enabled in OS UM.

The OS UM Users have been created via LDAP synchronization.

The resource templates required for the resource creation have to be available.

Step by Step

1) Navigate to **User Management** > **Administration** > **User Templates**

A list of the existing User Templates is displayed.

2) Select to edit the User Template in one of the following ways:

- Click on the **Name** of User Template you want to modify.
- Check the box in front of the User Template you want to modify and click **Edit**.
- In the row of a respective User Template, click on ▸ to open application action menu and then select **Edit**.

A pop-up window **Edit User Template** is displayed.

3) System retrieves all User Template attributes that have been defined once User Template was created.

NOTICE: All attributes, including the User Template name, are editable.

4) Navigate to the **Settings** area to modify the following information:

a) **Name**

This is the mandatory and unique field that represents the name of the User Template.

b) **Description**

Briefly describes the User Template.

5) Navigate to the **Rules** area, where various **Resource Types** are specified, in order to modify resources' information.

NOTICE:

The following Resource Types are supported by the current deployment: OpenScape Voice, OpenScape Voice Softphone, OpenScape 4000, OpenScape Xpressions, Unified Communications and External.

a) to add the new resources to the template, select the **Resource Type** you would like to configure from the drop-down list and then click **Add**.

b) to modify the existing resource, perform one of the following:

- check the box in front of the Resource you want to modify and then click **Edit**.

- in the row of a respective Resource, click on ▸ and then select **Edit**.

The configuration screen related to the corresponding resource is displayed.

6) In the **Rules for automatic resource creation** window navigate to the **Setting** area to modify:

a) **Function**

NOTICE:

The resource **Function** field is available only for the resources that can be added multiple times, i.e.,OpenScape Voice, OpenScape Voice Softphone, OpenScape 4000 and OpenScape Xpressions.

The only exception is that OpenScape Xpressions resource supports only the **Fax** and **Other** resource function.

From the drop-down list select one of the following functions (flavors):

a)
- **Business Phone 1**
- **Business Phone 2**
- **Fax**
- **Other**

NOTICE:

Any of the resource **Function** values can be set at most once in each User Template, except the type **Other** which can be specified multiple times.

---

b) **Operation Mode**

From the drop-down list choose one of the following options:

a)
- **Create new resources**

  system will monitor all the rules specified in the User Template and when any of these changes, an update of the Resource itself will be triggered.
- **Match existing Resources**

  system will monitor the rules that generate the Resources identifier only and the rest of the rules will be ignored.
- **Create new and match existing resources**.

  system will create the resource that are not found in the User Template, but afterwards it will behave as described in the **Match existing Resources** operation mode.

NOTICE:

In case where the selected resource type is **Unified Communications**, the only available option is **Create new resources**.

NOTICE:

When LDAP synchronization is performed with User Template mapping configured in operation mode “**Match existing resources**” or “**Create and Match existing**

---

resources" the already existing OSV resource is assigned to UM user without any modification in Display Name.

During the next DLAP synchronization even if the mappings are modified or the Display Name rule is changed in the associated User Template, the Display Name of the OSV subscriber remains as it was configured in the existing OSV subscriber.

If the operation mode will be modified to "Create new resources" in OSV resource rules of User Template, the Display Name will be changed in the OSV assigned resources.

In case:

- -) a new LDAP synchronization is performed,
- -) User Template is manually re-applied,
- -) the Display Name rule is modified in UT and triggers the re-apply of UT,
- -) any of the User attributes is modified and triggers the re-apply of UT

the Display Name will be modified.

c) **Resource Name**

NOTICE:

The **Resource Name** field is available for OpenScape Voice, OpenScape Voice Softphone, OpenScape 4000 and External.

From the drop-down list choose one of the following options:

a)
- **Use resource ID** (default value)
- **Use resource function name**
- **Constant value**
- **LDAP attribute**

7) In the **Rules for automatic resource creation** window navigate to the **Attributes** area to modify the parameters for the automatic completion of the unique/mandatory fields:

Among others, you have to select the **Resource Template** that will be used for the creation of the specific resource.

NOTICE:

At least one Resource Template per each Resource type must be specified.

As long as OS UM is connected to the LDAP directory, it is allowed to specify mapping to LDAP attributes for any attribute required for the resource creation.

From the other side, when the LDAP connection is inactive and the User Template you want to modify contains the attributes that have been mapped to the LDAP attributes, the system will display the current configuration of

User Template including LDAP mappings and it will allow to modify the User Template rules to values other than LDAP mappings.

IMPORTANT:

The **Groupware Assignment** option for Unified Communications resources indicates whether the Groupware connector is configured or not.

In case the template with the Unified Communications resource has a Groupware assignment, but the connector has been removed, the system will displays the template as it has been saved, i.e., with the Groupware and it will allow modification of the Unified Communications resource. You will be able either to select a different groupware connector or disable the groupware (if there are no other groupware connectors in the system).

8) Click **OK** to confirm modified configuration.

Once the system verifies that supplied information is correct and all required attributes are filled in, the corresponding Resource will be added to the list of the existing Resources or it will be simple modified.

9) Click **Save** to save changes to the User Template.

a) System:

- verifies that supplied information is correct
- updates and stores information related to the User Template.

a) **If** the Resource template selected during the creation of the User Template is not available at the time of editing:

- – System displays the following warning message: `The resource template "xyz" for "abc" resource type is not available. Please select a different resource template to re-enable the "abc" resource.`
  – System sets the value of the Resource template for the respective Resource type to **Please select...** and disables the rule-selection fields.
  – Administrator selects a different Resource template.
  – System enables the rule-selection fields populated with the previously stored values.

NOTICE:

If the User Template configuration screen is closed without changes being saved, any modification of the mapped LDAP attributes will be lost.

The User Template has been modified and displayed in the User Templates list.

NOTICE:

For every User associated with the modified User Template, the system will apply the User Template rules for each

Resource type that was modified based on the User Template configuration.

Next steps

In order to deleted one or more resources from the User Template, perform one of the following actions:

1) check the box in front of the Resource(s) you want to modify and then click **Delete**.
2) in the row of a respective Resource, click on and then select **Delete**.

The selected Resources are going to be deleted from the list of resources.

10.3.4 How to Delete User Template

The following paragraphs show a way to delete the User Template from the list of the existing User Templates.

Prerequisites

Adequate administrative permission that allows deletion of User Templates.

Step by Step

1) Navigate to **User Management** > **Administration** > **User Templates**.

   A list of the existing User Templates is displayed.

   Delete button is inactive.
2) Select to delete one or more User Templates in one of the following ways:
   - Check the box in front of the User Template(s) you want to delete and then click **Delete**.
   - In the row of a respective User Template, click on to open application action menu and then select **Delete**.

   NOTICE:

   In case the selected User Template is associated with the UM Users, the system displays a warning message and requests verification for the deletion of the specific User Template.
3) Click **OK**.

   System deletes selected User Template(s), so that it does not appear any more in the User Template list.

   NOTICE:

   In case the selected User Template was associated with the UM Users, the system dissociates the Resources that were associated with the removed User Template and updates the User to User Template association.

10.3.5 Modifying Resource Attributes during User Template re-apply

The resource attributes are modified during the User Template re-apply. These modifications depend on the value of the **Operation Mode** of the User Template.

IMPORTANT:

It is not recommended to change the Operation Mode of a User Template, which has associated users.

IMPORTANT:

When a user is already associated with a User Template, do not apply a different User Template to that user.

Operation Mode: Create new resources

All attributes that can be configured from the User Template, can be modified when the **Operation Mode** is set to "Create new resources". So when any resource Rule or any attribute (user/LDAP) mapped to the resource rule is modified, then during the re-apply of the User Template the respective resource attribute will be modified accordingly.

NOTICE:

When you modify a resource attribute outside of the User Management (for example, when you modify the Display Name of the OSV resource or the XPR PIN from the XPR Assistant) then the User Template re-apply will not modify the resource attribute with the respective resource rule mapping, since the UM is not informed about this modification.

The following attributes are not modified during User Template re-apply:

- **OSV**: Type
- **OSMO**: Mobile Client Profile
- **OS4K**: Resource Template / COS Template

Operation Mode: Match existing Resources

When the User Template is applied to the UM user, none of the resource attributes are modified apart from the Display Name (OSV/Softphone/OS4K) and Common Name (XPR) based on the respective configuration (Keep Display/Common Name) in the resource rules. The same applies after each User Template is re-applied to the UM user.

Operation Mode: Create new and match existing resources

When the User Template is applied to the UM user and the resource does not exist, then it will be created and assigned to the UM user. When the resource exists, it will be assigned to the UM user without any modification in its attributes apart from the Display Name (OSV/Softphone/OS4K) and Common Name (XPR) based on the respective configuration (Keep Display/Common Name) in the resource rules.

After each User Template is re-applied to the UM user, none of the resource attributes will be modified apart from the Display Name (OSV/Softphone/ OS4K) and Common Name (XPR) based on the respective configuration (Keep Display/Common Name). The resource rules modification or the modification of the respective attributes configured in the resource rules do not affect the resource attributes, when the User Template is re-applied to the UM user.

10.3.6 Applying the User Template’s rules

The User Template rules can be applied to a single Resource, as well as to the multiple Resources, anytime, regardless if the Resource is assigned to a User or not.

Resources that are defined in the User Template

In case the single Resource is already assigned to a User, the system will update the Resource’s attributes according to the rules defined in User Template.

Otherwise (when the Resource is not assigned to the User), the system will create (assign) the Resource to the User following the rules defined in the User Template’s operation mode.

Resources that are not defined in the User Template

To handle the Resources that are already assigned to a User but are not defined in the User Template, the following options are provided:

- **associate the User with the User Template without affecting the additional resources**

  (resources that were previously manually assigned to a User or applied with a different User Template will stay intact)
- **un-assign the additional resources**

  (resources that were previously manually assigned to a User or applied with a different User Template will be unassigned)
- **un-assign and delete the additional resources**

  (resources that were previously manually assigned to a User or applied with a different User Template will be unassigned and deleted).
- **un-assign phones and delete other resources**

  Un-assign resources of specific type and delete resources of other types

  (resources that were previously manually assigned to a User or applied with a different User Template will be unassigned and deleted).

NOTICE:

When a User Template with Xpressions Resources is applied to a User and a modification in the User Template takes place where only the User ID field in the User Template has been changed, then the **un-assign and delete the additional resources** rule is only applied, even if any other choice has been selected.

IMPORTANT:

When the PIN value, configured in the Xpressions rules of the User Template, is empty, the default PIN configured in Xpressions will be used.

10.3.7 Manage Users associated with a User Template

The following chapters describe how to manage UM Users that are associated with a User Template.

10.3.7.1 How to add Resource for selected Users based on the User Template

Taking advantage of the User Templates, the Administrator can automatically create or modify resources for one or more UM Users. All necessary values for the resource creation are defined in the User's Contact data, Locality and User Template. In addition, during resource creation, the required licenses may be consumed.

Prerequisites

Adequate administrative permission that allows management of User Templates.

The Unique attributes necessary for the Resource creation are populated by the rules that have been defined in the selected User Template.

The selected UM User(s) has Locality assigned.

NOTICE:

While applying a User Template to a UM User, you can create OpenScape Voice Resources with different configuration (for example, different Office Codes) as long as more than one set of OpenScape Voice rules are configured in the respective locality.

NOTICE:

In order to create resources (for the users), that are based on an User Template that directly uses LDAP attribute for any attribute required for the resource creation, the following prerequisites has to be fulfilled:

LDAP connection has to be enabled in OS UM.

The OS UM Users have been created via LDAP synchronization.

The resource templates required for the resource creation have to be available.

Step by Step

1) Navigate to **User Management** > **Administration** > **Users & Resources**.

A list of the existing UM Users is displayed.

2) Select one or more UM Users from the UM Users list.

3) Click on the button **More** and from the drop-down menu choose the **Add Resources from Template** option.

   The **Add resources from User template** dialog opens.

4) Navigate to **Configuration** area to define how to handle the Resources that are already assigned to a User but are not defined in the User Template.

   Selected one of the following options:

   - **associate the User with the User Template without affecting the additional resources**

     (resources that were previously manually assigned to a User or applied with a different User Template will stay intact)
   - **un-assign the additional resources**

     (resources that were previously manually assigned to a User or applied with a different User Template will be unassigned)
   - **un-assign and delete the additional resources**

     (resources that were previously manually assigned to a User or applied with a different User Template will be unassigned and deleted).
   - **un-assign phones and delete other resources**

     Un-assign resources of specific type and delete resources of other types

     (resources that were previously manually assigned to a User or applied with a different User Template will be unassigned and deleted).

NOTICE:

When a User Template with Xpressions Resources is applied to a User and a modification in the User Template takes place where only the User ID field in the User Template has been changed, then the **un-assign and delete the additional resources** rule is only applied, even if any other choice has been selected.

NOTICE:

No matter if you choose to apply the same User Template to one User multiple times or you apply a User Template to an existing User who is already linked to a different User Template, you will be provided with the aforementioned options.

---

5) Navigate to **Select Template and Start process** area to select one of the available User Templates from the drop-down list.

NOTICE:

In case the User Template you want to assign to the Users contains multiple entries for a resource type, all those resources of the same type will be assigned to the User(s).

IMPORTANT: In case the User Template you want to assign to the Users contains UC resource rules with the option **Send password and PIN via E-mail** checked or **Generate Automatically** for either the UC Password or the Telephony PIN, the Users' E-Mail address must be filled.

---

6) Click **Start** to initiate the process of adding Resources from the User Template.

NOTICE:

In multitenant deployments the bulk operations should be allowed to run concurrently across domains. Consequently, it is possible to perform the bulk operations simultaneously in different domains, but it is not allowed to perform them simultaneously within the same domain.

---

a) If the operation has already been initiated by the different administrator in the same domain:

- – System does not allow the operation to start:
- – System reports the error displaying the following message: `The operation has already been started by another Administrator. This operation cannot be executed multiple time simultaneously. Please try again later.`

b) If the operation has already been initiated by the same administrator and is running in the background:

- – System restores the window with the progress bar, updated with the current progress of the operation.

The System...

a) ...verifies that the rules for the population of mandatory and unique attributes for the resources creation have been defined in the selected User Template.

NOTICE:

The rules for the automatic completion of mandatory fields of each supported Resource type are summarized

in the table Automatic completion rules at the end of this chapter.

---

a)

NOTICE:

In case the User template contains OpenScape Voice Softphone resource, system verifies that the **External Caller ID** of the selected resource matches one of the OpenScape Voice resources assigned to the User.

If this is not the case (i.e., **External Caller ID** of the selected OpenScape Voice Softphone resource does not match any of the OpenScape Voice resources assigned to the User), the system displays a warning message, but it allows to create the OpenScape Voice Softphone resource.

The following substeps are repeated for each selected UM User.

b) ... in case the User Template is applied to a User that does not have Resources assigned, the system:

a) • – applies the rules for each Resource defined in the User Template
– updates the User to User Template association.

c) ... in case the User Template is applied to a User who already has resources assigned, but they are not linked with a User Template, either because the resources were assigned manually to the User or because they were created using a User Template prior to the support or the Resource to User Template association, the system:

a) • – applies the rules for each Resource defined in the User Template
– handles any Resource that is not present in the User Template
– updates the User to User Template association.

d) ...verifies that selected UM Users have Locality assigned.

a) **If** the User does not have Locality assigned.

• – System uses the Default Locality instead.

e) ...verifies that the values of the mandatory attributes for the Resource creation are available in the User's data (Contact data and assigned Locality)

a) **If** the values for one or more mandatory attributes are not available:

• – System does not create Resource.

– System reports the error as “incomplete information” upon completion of the operation.

NOTICE: The next two substeps are repeated for each resource defined in the selected User Template.

f) ...creates Resource.

IMPORTANT:

The Resources are created in the following order: OpenScape Voice -> OpenScape Voice Softphone -> OpenScape 4000 -> OpenScape Xpressions -> Unified Communications.

In case system performs matching and assignment of OpenScape 4000 resource using User Template, the OpenScpe 4000 phone will be assign to the User.

Also, if selected User Template uses a OpenScape 4000 resource as ONS for the automatic UC resource creation, the UM User will have assigned the UC resource that have a OpenScape 4000 phone as ONS.

a) If the automatic creation of OpenScape Voice and OpenScape 4000 resources uses a predefined extension range:

- – System verifies that the selected Extension range definition is compatible with the values calculated by the rest of the Template's rules (e.g., Switch/BG/Office Code)
- – System retrieves a list of the vacant resources in the specified range
- – System retrieves the first vacant resource and:

  - validates that the vacant resource does not match any of the Reserve criteria defined in the selected Extension Range

  - retrieves the next vacant resource
- – System creates the OpenScape Voice and OpenScape 4000 resources.

b) If resource creation for one or more User is selected with a User Template that has OSV resource security configuration:

- – System uses the User’s Locality to retrieve the OSV resource’s Realm.
- – System uses the User's User Template to retrieve the OSV resource's Username and Password.
- – System calculates the OSV resource's Username and Password.

– System creates the OSV resource with the collected security data.

NOTICE:

In case none of the security data are configured in the Locality/User Template, system creates the OSV resource without security configuration.

In case some but not all of the security data are specified, OSV resource creation fails.

c) If an error occurs during Resource creation:

- – System does not create the Resource.
  – System shows the error reported by the Element Manager, in the general errors section, upon completion of the operation.

IMPORTANT:

While applying a User Template with a Unified Communications resource where an OpenScape Voice or OpenScape Voice Softphone resource is set as webRTC, the OpenScape Voice or OpenScape Voice Softphone subscriber will automatically be set as Trusted.

g) ...assigns the Resource to the UM User.

NOTICE:

An UM User license will be consumed at the moment the first resource is successfully assigned to a User. In case more than one resource is going to be assigned to the user, the system does not need to consume any additional UM User licenses.

h) ...reports the progress of the operation using a progress bar, along with the appropriate text.

7) Click **Cancel** to stop an ongoing operation.

NOTICE: System does not rollback already created Resources and it does not leave Resource in an inconsistent state.

8) Depending on the operation outcome, upon its completion, a pop-up window containing one of following information/error messages is displayed:

- `Operation completed successfully. Please download the log file for more details.`

  (Information message)
- `Operation completed successfully. Please download the log file for more details.`

  (Warning)
- `The operation was cancelled. Please download the log file for more details.`

  (Error)

9) Click **Close**.

The pop-up window closes and you are back to the **Add resources from User template** screen.

10) System stores the following information in the log file:

- `Initiation timestamp`

  Timestamp of the operation initiation.
- `Operation mode`

  Operation mode for each resource type
- `Step timestamp`

  Timestamp of each step.
- `Processed User`
- `Created Resource`
- `Creation success/failure`
- `Reason for failure`

  Any failure in the verification listed in the step 5 above, plus any failure reported by the Resource creation itself.
- `Summary`

  At the end of the log file, a summary of the operation is created and it contains the following:

  – – Selected Users
  – Processed Users (UM User with assigned Locality and proper rules for the creation of all Resources specified in the User Template)
  – Users skipped due to incomplete info (UM Users with either no Locality assigned, or improper rules for the creation of any Resource specified in the User Template)
  – Users skipped due to cancellation (appears only if the operation was canceled)
  – Successfully created Resources (per Resource type)
- `It is explicitly reported if the operation is cancelled by the User.`
- `Completion timestamp`

  Timestamp of operation completion.

11) Click **Download report** to download a log file with the details of the latest operation.

NOTICE:

Log files are stored on the server, under the following

path:

- **for integrated Simplex =** `/log/OSCUM/`

- **for all other deployments =** `/var/siemens/common/log/OSCUM/`

---

12) Click **Close**.

The pop-up window with the User Templates closes and you are back to the **User Management** > **Administration** > **Users & Resources**.

Table 33: Automatic completion rules

Attribute	Rule Provider	Rule
OpenScape Voice Resource		
Numbering Plan	Locality	N/A
Office Code	Locality	N/A
Realm	Locality	N/A
Directory Number	User Template	One of the following is used as an attribute to generate the Suffix: **1)** Information **Inferred from User's details**, that can be: - Business Phone 1 - Business Phone 2 - User attribute - LDAP attribute **2)** **Automatic assignment** of the resource's suffix from the LDAP attribute or from the list of the predefined ranges. This option is disabled when the resource creation rules are configured with Operation Mode **Match existing Resources**. (The available Extension ranges for the selected OpenScape Voice switch are displayed in the form of `Range name - switch name`. In case there is a single communication system, the `switch name` is not displayed.)

Attribute	Rule Provider	Rule
Type	User Template	Selection of one of the available values: - Public - Private - User attribute - LDAP attribute
Display Name	User Template	One of the following contact information are used as the attributes for the Display Name: - Display Name - Last Name - First Name Last Name - Last Name, First Name - User attribute - LDAP attribute
SIP Authentication Username	User Template	Selection of one of the available values: - Constant Value - Resource ID - User attribute - LDAP attribute
SIP Authentication Password	User Template	Selection of one of the available values: - Constant Value - Resource ID - User attribute - LDAP attribute
OpenScape Voice Softphone Resource		
Numbering Plan	Locality	N/A
Office Code	Locality	N/A
Display Name	User Template	The name retrieved using the rules for selecting the OpenScape Voice resource defined in the User Template.
Directory Number	User Template	The number of the selected OpenScape Voice resource suffixed by the digits provided in the User Template.
External Caller ID	User Template	Normalized number of the selected OSV resource.

Attribute	Rule Provider	Rule
Type	User Template	The following values are available: - Public - Private - User attribute - LDAP attribute
OpenScape 4000		
Dial Plan	Locality	
Virtual Node	Locality	
COS template	User Template	Populated with the available COS templates and the LDAP attribute.
Extension	User Template	In order to generate the Extension the following options are provided: **1) Infer from User's details** one of the following contact information will be used as the attributes to generate the Extension: - Business Phone 1 - Business Phone 2 - User attribute - LDAP attribute **2) Assign automatically** **allows to automatically assign the** resource's suffix from the LDAP attribute or from the list of the predefined ranges. This option is disabled when the resource creation rules are configured with Operation Mode **Match existing Resources**. (The available Extension ranges for the selected OpenScape 4000 switch are displayed in the form of `Range name - switch name`. In case there is a single communication system, the `switch name` is not displayed.)

Attribute	Rule Provider	Rule
PEN	User Template	One of the following contact information are used as the attributes for PEN: - Use the first available PEN (the first available PEN applicable for the selected resource template will be assigned) - User attribute - LDAP attribute
Display Name	User Template	One of the following contact information are used as the attributes for the Display Name: - Display Name - Last Name - First Name Last Name - Last Name, First Name - User attribute - LDAP attribute
HFA Password	User Template	Selection of one of the available values: - Constant value - User attribute - LDAP attribute.
Unified Communications (UC)		
UC Profile	User Template	One of the following is used: - Essential - Professional - Team - Team Administrator - Team with Xpressions - User attribute - LDAP attribute.

Attribute	Rule Provider	Rule
ONS Number	User Template	One of the following is used: - Use Template's Business Phone 1 (OpenScape Voice and OpenScape 4000 resources are supported) - Use Template's Business Phone 2 (OpenScape Voice and OpenScape 4000 resources are supported) - User attribute - LDAP attribute
WebRTC Number	User Template	One of the following is used: - Use Template's Business Phone 1 (OpenScape Voice, OpenScape Voice Softphone and OpenScape 4000 resources are supported) - Use Template's Business Phone 2 (OpenScape Voice, OpenScape Voice Softphone and OpenScape 4000 resources are supported) - User attribute - LDAP attribute
Assign WebRTC Profile	User Template	The WebRTC profile is mandatory for the WebRTC feature to be functional. Check the checkbox to assign the WebRTC profile. You can configure the WebRTC along with another profile (for example, Team with WebRTC). In this case, you don't need to check the checkbox (no additional licenses will be used in case of having both the checkbox checked and the WebRTC permission existing in another chosen profile).

Attribute	Rule Provider	Rule
IM Address	User Template	The following options are used in order to extract the IM Address: - **Use IM Address** In this case OpenScape User Management does not need to do anything when creating the UC Resource, since the IM Address of the UM User is stored in the same field of the same contact record. **- UC Account Login Name@XMPP Domain** Use UC Resource's username appended by the XMPP Domain Name. The XMPP Domain Name can be found by the UC Assistant querying presence (**CMP** > **Configuration** > **Unified Communications** > **Presence and IM** > **Presence and Instant Messaging Configuration**). **- LDAP attribute**
Login password	User Template	One of the following is used: - Constant value - User attribute - LDAP attribute To force the UM User to change the password on the first login, tick the option **User has to change login password at next login**.
Telephony PIN	User Template	One of the following is used: - Constant value - User attribute - LDAP attribute To force the UM User to change the telephony PIN on the first login, tick the option **User has to change telephony PIN at next logi**n.
OpenScape Xpressions		
Xpressions server ID	Locality	N/A
PIN	Locality	N/A The default value is 123456

Attribute	Rule Provider	Rule
Create the Xpressions User ID using	User Template	One of the following contact information are used (as it is, or only the part of it with the variable number of digits) - Template’s Business Phone 1 - Template’s Business Phone 2 - Template’s Fax - an OSV resource already assigned to the User - an OpenScape 4000 resource already assigned to the User - User’s Business Phone 1 - User’s Business Phone 2. - User’s Fax number - UM User ID - User attribute - LDAP attribute. The default value is the preferred userID, i.e., name.surname or the assigned DirectoryNumber.
Common Name	User Template	One of the following contact information are used as the attributes for the Common Name: - Display Name - Last Name - First Name Last Name - Last Name, First Name - User attribute - LDAP attribute The default value is the preferred CommonName, i.e., name.surname or the assigned DirectoryNumber.

Attribute	Rule Provider	Rule
Voice Mail	User Template	One of the following information is used: - Use Template’s Business Phone 1 - Use Template’s Business Phone 2 - Use Template’s Fax - Use an OSV resource already assigned to the User - Use an OpenScape 4000 resource already assigned to the User - Use User’s Business Phone 1 - Use User’s Business Phone 2. - Use User’s Fax number - User attribute - LDAP attribute.
Mobile Phone	User Template	One of the following information is used: - Disabled - Use User’s Business Phone 1 - Use User’s Business Phone 2. - Use the Mobile phone - User attribute - LDAP attribute

Attribute	Rule Provider	Rule
Business Number	User Template	One of the following contact information are used as the attributes for the Business Number: - Use Template’s Business Phone 1 - Use Template’s Business Phone 2 - Use Template’s Fax - Use an OSV resource already assigned to the User - Use an OpenScape 4000 resource already assigned to the User - Use User’s Business Phone 1 - Use User’s Business Phone 2. - Use User’s Fax number - User attribute - LDAP attribute. *When the DN is public, it will be prepended by '+'. When the DN is private, it will be prepended by 'p'. The default value is the assigned DirectoryNumber.
E-mail	User Template	One of the following information is used: - Disabled - Use E-mail address 1 - Use E-mail address 2 - User attribute - LDAP attribute

Attribute	Rule Provider	Rule
Business Fax	User Template	One of the following information is used: - Disabled - Use Template’s Business Phone 1 - Use Template’s Business Phone 2 - Use Template’s Fax - Use an OSV resource already assigned to the User - Use an OpenScape 4000 resource already assigned to the User - Use User’s Business Phone 1 - Use User’s Business Phone 2. - Use User’s Fax number - User attribute - LDAP attribute
Password	User Template	One of the following is used: - Constant value - User attribute - LDAP attribute
PIN	User Template	One of the following is used: - Constant value (only numeric values are allowed) - User attribute - LDAP attribute
Windows ID	User Template	To configure the Single Sign-On, one of the following is used: - Disabled - Use E-mail address 1 - Use E-mail address 2 - Use IM Address - User attribute - LDAP attribute

Attribute	Rule Provider	Rule
Microsoft Exchange	User Template	To configure the Single Sign-On, one of the following is used: - Disabled - Use E-mail address 1 - Use E-mail address 2 - Use IM Address - User attribute - LDAP attribute
Lotus Notes	User Template	To configure the Single Sign-On, one of the following is used: - Disabled - Use E-mail address 1 - Use E-mail address 2 - Use IM Address - User attribute - LDAP attribute
OpenScape Xpressions/ Unified Communications Integration		Section is visible only when both, Xpressions and Unified Communications are deployed. Starting from OS UM V7 this resource type is no longer supported and it has been appropriately replaced in the User Template.

Attribute	Rule Provider	Rule
CONUSER	User Template	Set CONUSER to: - Empty - UC Login Name@Domain **IMPORTANT:** • In case the Xpressions Resource is enabled in the User template, the CONUSER of this resource is set. • In case the Xpressions Resource is not enabled in the User Template, system checks for already assigned Xpresssions resource and if it exists, the CONUSER of this resource is set. • In case multiple Xpressions Resources are assigned to an User, the CONUSER of the first one is set.

10.3.7.2 How to Reset the configuration of all User's Resources to default

This chapter describes how to apply the same User Template to a User and force the system to apply the rules defined in the User template to all User's Resources.

Prerequisites

Adequate administrative permission that allows management of User Templates.

The User is associated with a User Template.

Step by Step

1) Navigate to **User Management** > **Administration** > **Users & Resources**.

A list of the existing UM Users is displayed.

2) Select one or more UM Users from the UM Users list.

3) Click on the button **More** and from the drop-down menu choose the **Reset configuration of assigned resources** option.

NOTICE:

This option is used only if all the User's Resource were manually manipulated outside of OS UM.

The **Reset configuration of assigned resources** dialog opens.

4) Navigate to **Configuration** area and selects to reset the User's Resources configuration according to the following rules defined in the User Template that is associated with the User.

- **associate the User with the User Template without affecting the additional resources**

  (resources that were previously manually assigned to a User or applied with a different User Template will stay intact)
- **un-assign the additional resources**

  (resources that were previously manually assigned to a User or applied with a different User Template will be unassigned)
- **un-assign and delete the additional resources**

  (resources that were previously manually assigned to a User or applied with a different User Template will be unassigned and deleted).
- **un-assign phones and delete other resources**

  Un-assign resources of specific type and delete resources of other types

  (resources that were previously manually assigned to a User or applied with a different User Template will be unassigned and deleted).

NOTICE:

When a User Template with Xpressions Resources is applied to a User and a modification in the User Template takes place where only the User ID field in the User Template has been changed, then the **un-assign and delete the additional resources** rule is only applied, even if any other choice has been selected.

---

5) Click **Reset** to initiate the process.

The System...

a) ... applies the reset Resource workflow to each resource that is assigned to the User

b) ... handles any resource that is not present in the associated User Template.

6) Depending on the operation outcome, upon its completion, a pop-up window containing one of following information/error messages is displayed:

- `Operation completed successfully. Please download the log file for more details.`

  (Information message)
- `Operation completed successfully. Please download the log file for more details.`

  (Warning)
- `The operation was cancelled. Please download the log file for more details.`

  (Error)

7) System stores the following information in the log file:

- `Initiation timestamp`

  Timestamp of the operation initiation.
- `Operation mode`

  Operation mode for each resource type
- `Step timestamp`

  Timestamp of each step.
- `Processed User`
- `Created Resource`
- `Creation success/failure`
- `Reason for failure`

  Any failure in the verification listed in the step 5 above, plus any failure reported by the Resource creation itself.
- `Summary`

  At the end of the log file, a summary of the operation is created and it contains the following:

  – – Selected Users
    – Processed Users (UM User with assigned Locality and proper rules for the creation of all Resources specified in the User Template)
    – Users skipped due to incomplete info (UM Users with either no Locality assigned, or improper rules for the creation of any Resource specified in the User Template)
    – Users skipped due to cancellation (appears only if the operation was canceled)
    – Successfully created Resources (per Resource type)
- `It is explicitly reported if the operation is cancelled by the User.`
- `Completion timestamp`

  Timestamp of operation completion.

8) Click **Download report** to download a log file with the details of the latest operation.

NOTICE:

Log files are stored on the server, under the following

path:

- **for integrated Simplex =** `/log/OSCUM/`

- **for all other deployments =** `/var/siemens/common/log/OSCUM/`

---

9) Click **Close**.

The pop-up window with the User Templates closes and you are back to the **User Management** > **Administration** > **Users & Resources**.

10.3.7.3 How to Manually dissociate a User from an User Template

This chapter describes how to dissociate a User from a User Template.

Prerequisites

Adequate administrative permission that allows management of User Templates.

The selected User has one or more Resources linked to a User Template.

Step by Step

1) Navigate to **User Management** > **Administration** > **Users & Resources**.

   A list of the existing UM Users is displayed.

2) Select one or more UM Users from the UM Users list.

3) Click on the button **More** and from the drop-down menu choose the **Dissociate users from user templates** option.

   The **Dissociate users from user templates** dialog opens.

4) Click **Dissociate** to dissociate one or more Users from a User Template.

   System displays the action to be performed and requests confirmation to dissociate the User(s) from User Template.

5) Click **OK** to confirm.

   The System...

   a) ... removes the User Template to Resource association from all the User's Resources

   b) ... updates the User to User Template association for the selected User(s).

6) Depending on the operation outcome, upon its completion, a pop-up window containing one of following information/error messages is displayed:

- `Operation completed successfully. Please download the log file for more details.`

  (Information message)
- `Operation completed successfully. Please download the log file for more details.`

  (Warning)
- `The operation was cancelled. Please download the log file for more details.`

  (Error)

7) System stores the following information in the log file:

- `Initiation timestamp`

  Timestamp of the operation initiation.
- `Operation mode`

  Operation mode for each resource type
- `Step timestamp`

  Timestamp of each step.
- `Processed User`
- `Created Resource`
- `Creation success/failure`
- `Reason for failure`

  Any failure in the verification listed in the step 5 above, plus any failure reported by the Resource creation itself.
- `Summary`

  At the end of the log file, a summary of the operation is created and it contains the following:

  – – Selected Users
    – Processed Users (UM User with assigned Locality and proper rules for the creation of all Resources specified in the User Template)
    – Users skipped due to incomplete info (UM Users with either no Locality assigned, or improper rules for the creation of any Resource specified in the User Template)
    – Users skipped due to cancellation (appears only if the operation was canceled)
    – Successfully created Resources (per Resource type)
- `It is explicitly reported if the operation is cancelled by the User.`
- `Completion timestamp`

  Timestamp of operation completion.

8) Click **Download report** to download a log file with the details of the latest operation.

NOTICE:

Log files are stored on the server, under the following

path:

- **for integrated Simplex =** `/log/OSCUM/`

- **for all other deployments =** `/var/siemens/common/log/OSCUM/`

---

9) Click **Close**.

The pop-up window with the User Templates closes and you are back to the **User Management** > **Administration** > **Users & Resources**.

NOTICE:

Dissociation of Users from User Template is available also during: Locality modification, User Template modification or Manually UM user attribute modification.

10.4 Extension Ranges

One of the mandatory attributes required for the creation of a telephony resource is the extension. This attribute combined with the Office Code results in the resource's Directory Number.

So far, OpenScape User Management supported the automatic creation of a resource by providing the following rules for computing the extension in the User Template:

- use the data stored in the User's contact data and determine the extension by "subtracting" the defined Office Code
- use the data directly from the LDAP directory and determine the extension by "subtracting" the defined Office Code.

However, the User's telephone number may not be known at the time the User is created. Moreover, it may not even be relevant as long as the system can automatically assign a number from a predefined range. This allows the administrators to automatically create resources without specifying the extensions in advance.

The OpenScape User Management now provides the option to define a group of numbers in the form of an expression (e.g., a range excluding explicit numbers, or a pattern) and make them available in the User Template rules for the telephone number extension.

This feature also gives the opportunity to see the total number of the vacant numbers in each defined range.

10.4.1 How to Define an Extension Range

This Chapter describes How to define a range of extensions that will be used for the automatic resource creation.

Prerequisites

Adequate administrative permission that allows management of Extension ranges.

Step by Step

1) Navigate to **User Management** > **Administration** > **Extension Ranges**. A list of the existing Extension Ranges is displayed, sorted per first column **Name**, in ascending order.

   The drop-down list (located near the button **Add**) displays the available OSV and OpenScape 4000 switches.

2) To define an extension range for an OSV switch, select the OSV switch from the drop-down list.

   Otherwise, select the OpenScape 4000 switch.

3) Click **Add** to create the new Extension Range.

   A pop-up window **Add Extension Range @ switch_name** is displayed.

   a) In case the OSV switch is selected, fulfill the following information:

      a)
      - **Name** - mandatory field that describes the Extension Range name
      - **Description**
      - **Office code** - contains the list of Office codes defined in the selected Business Group or all the Office codes of one switch
      - **Specific range** defines the range between the **Start** and the **End** numerical values
      - **Wildcard range** defined by Numeric values and **"*"** character
      - **Reserved extensions** (for more info, see How to Define a Reserved Extension Range)

   b) In case the OpenScape 4000 switch is selected, fulfill the following information:

      a)
      - **Name** - mandatory field that describes the Extension Range name
      - **Description**
      - **Virtual Node** - contains the list of Virtual Nodes defined in the selected switch
      - **Reserved extensions** (for more info, see How to Define a Reserved Extension Range)

4) Click **Save** to create a new Extension Range.

   a) System:

   - verifies that supplied information is correct and that all required attributes are filled in
   - creates a new Extension Range.

A new Extension Range has been created and displayed in the list of the existing Extension Ranges.

10.4.2 How to Define a Reserved Extension Range

To define a range of extensions (with reserved sub ranges) by excluding some numbers, i.e., Reserved Extensions, follow the steps below:

Prerequisites

Adequate administrative permission that allows management of Extension ranges.

Step by Step

1) Navigate to **User Management** > **Administration** > **Extension Ranges**. A list of the existing Extension Ranges is displayed, sorted per first column **Name**, in ascending order.

   The drop-down list (located near the button **Add**) displays the available OSV and OpenScape 4000 switches.

2) To define an extension range for an OSV switch, select the OSV switch from the drop-down list and click **Add**.

   Otherwise, select the OpenScape 4000 switch and click **Add**.

   A pop-up window **Add Extension Range @ switch_name** is displayed.

3) In the **Add Extension Range @ switch_name** window navigate to the **Reserved extensions** area and click **Add**.

   A pop-up window **Add Reserved Extension** is displayed.

4) To define one or more Reserved Extension, define the following ranges:

   - **reserve specific range** (defines the range between the **Start** and the **End** numerical values)
   - **reserve by pattern** (defines the pattern for the Reserved range. For example, Wildcard pattern: Numeric values and "*" means any number of digits, whereas "?"" means a single digit)
   - **reserved set** (contains the specific extensions separated by comma).

5) Click **Add** to add a new Reserved Extension Range.

   a) System:

      - verifies that supplied information is correct and that all required attributes are filled in
      - creates a new Reserved Extension Range.

A new Reserved Extension Range has been created and displayed in the list of the existing Reserved Extension.

10.4.3 How to Display Extension Ranges

In order to see the defined Extension Ranges and how many vacant extensions are still available in each range, perform the following steps:

Prerequisites

Adequate administrative permission that allows management of Extension ranges.

Step by Step

Navigate to **User Management** > **Administration** > **Extension Ranges**.
A list of the existing Extension Ranges is displayed, sorted per first column **Name**, in ascending order.

It also contains the following columns:

- – **Name** of the specific range
  – **Description**
  – **Reserved extensions**
  – **Available Extensions**
  – **Switch Name**

NOTICE:

In case one Extension Range has one or more Reserved ranges defined, the system will retrieve the number of available extensions and will not apply the reservation restrictions (i.e., displayed number will be the maximum number of available extensions), or it will display the approximate number of available extensions.

In case the OpenScape 4000 range has more than 5000 extensions available (CORBA limitation), system will displays the text "**5000 (or more)**" for the available extensions, no matter if a reserved range is defined, or not.

10.5 Custom User Attributes

The Custom User Attributes offer the ability to have a variable number of custom fields, providing advanced configuration for the UM users' provisioning. All fields configured in the Custom User Attribute list are assigned to all UM users.

The administration of these fields are configurable through the User Interface. It's possible to create, delete Custom User Attributes and modify their name.

Moreover these attributes (using the **attribute Id** parameter) can be managed via csv import and SPML.

10.5.1 How to Add a Custom User Attribute

Follow the steps below to create a Custom User Attribute.

Prerequisites

Adequate administrative permissions.

Step by Step

1) Navigate to **User Management** > **Administration** > **Custom User Attributes**.
   A list of the existing Custom User Attributes is displayed, sorted per **Name**, in ascending order.
2) Click **Add** to create the new Custom User Attribute.

   A pop-up window **Add Custom User Attribute** is displayed. Here you can define the rules for the new custom user attribute you are going to add. Configure the following parameters:

   a) **Attribute Id**: The attribute's identifier. This parameter is unique for each Attribute, as two attributes can have the same name, but the Id must be different. The value must start with"_" or letter and no special character, apart from "_" should be used.
   b) **Name**: The name of the Custom User Attribute
   c) **Type**: Select a value from the drop-down menu to characterize the Custom User Attribute. The available values are:

      - – Check Box
        – Text Field
        – Choices

   d) **Choices values**: Configure this parameter when you have selected Choices in the **Type** parameter. Use the ';' symbol after each value you give as user's option. Use the ";" after the last value too.
3) Click **Save** to create a new Custom User Attribute.

A new Custom User Attribute has been created and displayed on the list of the existing Custom user Attributes and also in the tab **Custom user Attributes**, created in the **Add User & Resources - system** pop-up window.

10.5.2 How to Edit a Custom User Attribute

Follow the steps below to edit a custom user attribute

Prerequisites

Adequate administrative permissions.

Step by Step

1) Navigate to **User Management** > **Administration** > **Custom User Attributes**.
   A list of the existing Custom User Attributes is displayed, sorted per **Name**, in ascending order. Select a Custom User Attribute you want to edit and click **Edit** or click on the Custome User Attribute.

2) A pop-up window **Edit Custom User Attribute** is displayed.

   You can edit only the following parameter:

   a) **Name**: The name of the Custom User Attribute

3) Click **Save** to finalize the Custom User Attribute.

When you want to edit more parameters of an existing Custom User Attribute, you have to delete it and create a new one with new parameters.

10.5.3 How to Delete a Custom User Attribute

Follow the steps below to delete a custom user attribute

Prerequisites

Adequate administrative permissions.

Step by Step

1) Navigate to **User Management** > **Administration** > **Custom User Attributes**.
   A list of the existing Custom User Attributes is displayed, sorted per **Name**, in ascending order. Select a Custom User Attribute you want to delete and click **Delete**.
2) A pop-up confirmation window is displayed. Click **OK**. The Custom User Attribute will be deleted.

10.6 Organizational Structure Attributes

The values of the Organizational Structure Attributes offer the ability to create, select or assign an Organizational Structure to a UM user. The administration of these fields are configurable through the CMP. There are seven already created Organizational Structure Attributes in the list and you can't add more.You can only modify the name of the Organizational Structure Attributes.

The values of the attributes (using the **attribute Id** parameter) can be managed via csv import, SPML and LDAP synchronization.

10.6.1 How to Edit an Organizational Structure Attribute

Follow the steps below to edit the name of an Organizational Structure

Prerequisites

Adequate administrative permissions.

Step by Step

1) Navigate to **User Management** > **Administration** > **Organizational Structure Attributes**.
   A list of the existing Organizational Structure Attributes is displayed, sorted per **Attribute Id** or **Name**. Select an Organizational Structure attribute you want to modify, click **Edit** or click on the **Attribute Id**.

2) A pop-up window **Edit Organizational Structure Attribute** is displayed.

You can modify only the following parameter:

a) **Name**: The name of the Organizational Structure Attribute. Two **Attribute Id**'s can have the same name. The default values are Org1, Org2.. Org7

3) Click **Save** to finalize your changes.

10.7 E-Mail Templates

E-mail templates allow you to change the information of password notification e-mails.

10.7.1 How to set up E-mail Templates

This Chapter describes how to set up E-Mail Templates to send password notification emails to UM users with UC resources. These emails are sent when a new password is created or an existing password is updated.

Prerequisites

Adequate administrative permission that allows the Management of Users and Resources.

Step by Step

1) Navigate to **User Management** > **Administration** > **E-Mail Templates**.

A pop-up window **E-Mail Templates** is displayed.

2) If you want to set up an e-mail template for the creation of new UC resources stay on the **Creation** tab.

3) If you want to set up an e-mail template for the update of login passwords and/or telephony PINs of existing UC resources, go to the **Update** tab.

4) Edit or keep the default text for the following:

a) **Sender:** the sender's email address as it will appear for the recipient.

b) **Subject:** the subject line of the email.

c) **Message:** the content you want in the message body. This field supports HTML tags to customize your message, like for example using bold formatting. For more information on HTML use and Email template customization please refer to section:

IMPORTANT:

The **$ucPassword** variable is required in the Message body, both in the **Creation** tab and in the **Update** tab. If omitted, a pop-up window is displayed with an error message to remind you that this variable is mandatory in the **Message** text field.

---

5) Click **Save** to save your changes.

10.7.2 How to Customize E-mail Templates

This Chapter describes how to customize the E-Mail Templates to send password notification emails to UM users with UC resources.

Prerequisites

Adequate administrative permission that allows the Management of Users and Resources.

Step by Step

1) Navigate to `/opt/siemens/common/conf/umEmailTemplates`, i.e. the default path that contains the E-mail templates.
2) To change the default logo used in the e-mails, copy and paste your desired image file under the aforementioned directory and rename it to **`brandname_custom_logo.png`**.
3) To customize the HTML body used in the e-mails, create a new file named **`CustomMailTemplateHTMLContent.html`** that will contain your custom HTML code.

   NOTICE: You can use the file `MailTemplateHTMLContent.html`files as a guide. However, it is not recommended to delete the initial **`MailTemplateHTMLContent.html`** and **`brandname_logo.png`** files as they serve as backup files.

4) In the `CustomMailTemplateHTMLContent.html` file, use the **$Subject** and **$Message** variables in your HTML code, as placeholders to determine where your custom subject and message text will be displayed. Use the **cid:image** placeholder to determine where your custom logo will appear.

To reset your E-mail template message and logo to the default ones, simply delete the **`CustomMailTemplateHTMLContent.html`** and **`brandname_custom_logo.png`** files under `/opt/siemens/common/conf/umEmailTemplates`.

10.8 Resource Migration

For installations that use both, OpenScape Voice and OpenScape 4000 resources, User Management supports migration of an OpenScape 4000 resource to an OpenScape Voice resource and vice versa, with minimal effort.

Resource migration is done through the following steps:

- OSV Migration settings

  CMP Administrator has to define Migration configuration parameters.
- Migrate to OSV resource

  Once Migration is configured, CMP Administrator can simply select the UM User that has one or more OpenScape 4000 resources and initiate the Migration process.

- Migrate to Openscape 4000 resource

  CMP Administrator can simply select the UM User that has one or more OSV resources and initiate the Migration process.

10.8.1 How to configure OSV Migration Settings

Before Resource Migration takes place, necessary mappings between OpenScape 4000 and OpenScape Voice attributes, must be configured.

Prerequisites

Adequate administrative permission that allows User Management and Provisioning.

IMPORTANT:

In order to be able to connect the User Management with the OpenScape 4000 Manager/Nodes, the “UM_control” process of OpenScape 4000 should be up and running.

In other words, the administrator needs to enter the OpenScape 4000 Unix machine and type the following command: `UM_control activate`.

Step by Step

1) Navigate to **User Management** > **Administration** > **OSV Migration Settings**.

A pop-up window containing **Attribute Mappings for OpenScape 4000 to OSV Migration** is displayed.

2) Selects to configure the mappings for OpenScape 4000 to OSV Migration.

3) System retrieves the drop-down list of the **External System ID for OSV** in the OpenScape 4000 Manager.

- **If** Multiple OpenScape 4000 Manager Nodes are defined:
  - System retrieves the list of **External System ID for OSV** defined in all specified OpenScape 4000 Manager Nodes and creates the list of "distinct" values.

NOTICE: The name of the external system that refers to the OSV must be the same in all OpenScape 4000 Managers. This is in done in order to define properly the **OpenScape 4000 Manager External System ID for OSV** attribute.

---

4) Select the required value in the **OpenScape 4000 Manager External System ID for OSV** drop-down list.

This attribute is defined once per CMP domain.

5) Select the required value in the **OpenScape 4000 Switch** that represents OpenScape 4000 Managed Node.

   Following substeps will be worked off by the system:

   The System...

   a) ... retrieves any attribute mappings defined for the selected **OpenScape 4000 Switch** (OpenScape 4000 Managed Node).

   b) ... retrieves the values of the **COS**/**LCOS-Voice** attributes, as well as the available **OSV Template**.

   Steps 6-8 are repeated for all **OpenScape 4000 Switches**.

6) Select a pair **COS/LCOS-Voice** attributes for the OpenScape 4000 Managed Node.

7) Select an **OSV Template**.

NOTICE:

In case the option **Use Domain to Business Group Mapping** is disabled and there is more than one OSV switch deployed on the system, the names of the available Resource Templates, available in the drop-down list, will appear in the form of: `subscriber_template_name@business_group_name@switch_id`.

From the other side, if only one OSV switch is present, switch_id will be omitted from the Resource Template name and it will contain only: `subscriber_template_name@business_group_name`.

---

8) Click **Add**.

   A new mapping is added to the list of attribute mappings for the selected **OpenScape 4000 Switch**.

   - **If** the group of attributes **OpenScape 4000 Switch**/**COS**/**LCOS-Voice** has already been mapped to an **OSV Template**:
     – System overwrites the mapping definition.

9) To remove an already defined mappings for an attribute value pair, select them from the list of attribute mappings for the specific **OpenScape 4000 Switch**.

   Delete button is now active

10) Click **Delete**.

    The selected records (mappings) are deleted from the list of attribute mappings for the specific OpenScape 4000 Switch.

11) Select **Save** to confirm your entries.

10.8.2 How to Migrate to OSV resource

The subject of this chapter is the migration of OpenScape 4000 resources to the OpenScape Voice resources.

Prerequisites

Adequate administrative permission that allows the management of Users and Resources.

System supports OpenScape 4000 resources.

System supports OpenScape Voice resources.

Attribute mapping for the **COS/LCOS-Voice** combination of the selected OpenScape 4000 resource has been defined (see How to configure OSV Migration Settings).

The attribute Office Code must be defined in the target OSV system.

The attribute Directory Number must be defined in the target OSV system.

Selected UM User has at least one OpenScape 4000 resource assigned.

1) Navigate to **Configuration** > **CMP** > **General** > **System Settings**.

A pop-up window **System Settings** is displayed.

NOTICE:

When **Use Domain to Business Group Mapping** option is enabled, system will restrict each CMP domain to access the data of the mapped Business Group only. The Domain to Business Group mapping is defined in the OpenScape Voice Business Group page.

(Navigate to **Configuration** > **OpenScape Voice** > **Business Group** > **Business Group List** > **Add** the BG you want to map.

Click on the **tab General** to choose, in the Domain field, the domain you want to assign to this Business Group.)

NOTICE: By default, the value for the **Use Domain to Business Group Mapping option** is "disabled".

---

2) Select to enable/disable **Use Domain to Business Group Mapping** option.

a) **If** the option **Use Domain to Business Group Mapping** is enabled:

- – The Local attribute **Business Group** is disabled in the OpenScape Voice Element Manager (it doesn't appear on the **Migrate to OSV resource** window).
- – System provides the CMP Domain and no **Business Group**.
- – Only the Resource Templates from the **Business Group** mapped to the current Domain are available in the OpenScape Voice Resource creation and OpenScape Voice Resource specific values in the User Template.
- – OpenScape Voice Assistant Synchronization uses the **Domain to Business Group Mapping** during the synchronization process.

b) **If** the option **Use Domain to Business Group Mapping** is disabled:

- – The Local attribute **Business Group** is enabled in the OpenScape Voice Element Manager (it is displayed on the **Migrate to OSV resource** window).
- – The **Numbering Plan** and the **Branch Office** values that are available when creating an OpenScape Voice Resource are depended on the selected **Business Group**.

- The Resource Templates from all **Business Group** are available in the OpenScape Voice Resource creation and OpenScape Voice Resource specific values in the User Template.
- System provides the **Business Group** in addition to the CMP Domain.
- OpenScape Voice Assistant Synchronization ignores the **Domain to Business Group Mapping** and synchronizes everything in the Default system domain. Any existing **Domain to Business Group Mapping** will be ignored.

Step by Step

1) Navigate to **User Management** > **Administration** > **Users & Resources**.

A list of the existing UM Users is displayed sorted per name.

The column **Resources** shows the resources assigned to the UM User.

2) Select the migration to the OpenScape Voice resources from the UM Users that already have the OpenScape 4000 resources (the sign in the column **Resources** indicates the presence of OpenScape 4000).

3) Click on the Arrow action button ( ) located on the right side of the column **Resources**.

An action menu containing **Migrate to OSV resource** is displayed.

4) Click **Migrate to OSV resource**.

A pop-up window **Migrate to OSV resource** is shown.

5) Following substeps will be worked off by the system:

The System...

a) ... collects the following information required for the creation of the new OSV resource:

- Resource Template: retrieved from the attribute mapping of **COS/LCOS-Voice** to OSV resource template (see How to configure OSV Migration Settings).

  NOTICE:

  In case the option **Use Domain to Business Group Mapping** is disabled and there is more than one OSV switch deployed on the system, the names of the available Resource Templates, available in the drop-down list, will appear in the form of: `subscriber_template_name@business_group_name@switc`

  From the other side, if only one OSV switch is present, switch_id will be omitted from the Resource Template name and it will contain only: `subscriber_template_name@business_group_name`.

- Branch Office: specified in the UM User's locality (OSV resource type).
- Numbering Plan: specified in the UM User's locality (OSV resource type).
- Office Code: defined for the selected OpenScape 4000 resource.
- Suffix: defined for the selected OpenScape 4000 resource

– Display Name: defined for the selected OpenScape 4000 resource.

NOTICE:

Though the OpenScape 4000 station can have more than one Display Name set, only one Display Name will be visible in the **Migrate to OSV resource** form.

– Type (private/public): specified in the synchronized OpenScape 4000 resource (private/public phone).

b) ... displays the **Migrate to OSV resource** pop-up window pre-populated with all collected information.

c) ... displays the value of the attribute **OpenScape 4000 Manager External System ID for OSV** in the information area of the pop-up window.

NOTICE: The value of the **OpenScape 4000 Manager External System ID for OSV** attribute in OSV migration Settings has to be specified in order to start the migration process.

6) If required, modify any attribute displayed on the **Migrate to OSV resource** pop-up window.

7) Click **Migrate** to start the resource migration.

- **If** There is more than one OpenScape 4000 resource assign to the UM User:
  – System allows either to migrate the first assigned OpenScape 4000 resource and move to the next, or to directly "skip" to the next assigned OpenScape 4000 resource, by clicking **Skip this Resource**.
- **If** The selected OpenScape 4000 resource belongs to a "Self-Managed" OpenScape 4000 Node:
  – System informs about the existence of "Self-Managed" OpenScape 4000 Node and skips to the next assigned OpenScape 4000 resource.

NOTICE: The migration of OpenScape 4000 resources belonging to "Self-Managed" OpenScape 4000 Nodes is not supported.

8) Following substeps will be worked off by the system:

The System...

a) ... creates the new OSV resource and assigns it to the UM User.

b) ... sets this resource as the ONS of the UC resource for UM User (if applicable).... migrates the OpenScape 4000 resource to the newly created OSV resource.

c) ... removes the migrated OpenScape 4000 resource from the CMP database.

d) ... informs that the OpenScape 4000 resource has been successfully migrated.

- **If** an error occurs during the creation of a new OSV resource:
  – – System handles the error displaying information related to the Resource.

– The OpenScape 4000 Resource remains intact, due to the migration failure.

10.8.3 How to Migrate to OpenScape 4000 resource

The subject of this chapter is the migration of OpenScape Voice resources to the OpenScape 4000 resources.

Prerequisites

Adequate administrative permission that allows the management of Users and Resources.

System supports OpenScape 4000 resources.

System supports OpenScape Voice resources.

Selected UM User has at least one OpenScape Voice resource assigned.

Step by Step

1) Navigate to **User Management** > **Administration** > **Users & Resources**.

A list of the existing UM Users is displayed sorted per name.

The column **Resources** shows the resources assigned to the UM User.

2) Select the migration to the OpenScape 4000 resources from the UM Users that already have the OpenScape Voice resources.

3) Click on the Arrow action button (▶) located on the right side of the column **Resources**.

An action menu containing **Migrate to OpenScape 4000 resource** is displayed.

4) Click **Migrate to OpenScape 4000 resource**.

A pop-up window **Migrate to OpenScape 4000 resource** is shown.

5) Following substeps will be worked off by the system:

The System...

a) ... collects the following information required for the creation of the new OpenScape 4000 resource:

- – Resource Template
  – Resource Name: specified in the UM User's locality (OSV resource type).
  – Extension: specified in the UM User's locality (OSV resource type).

b) ... displays the **Migrate to OpenScape 4000 resource** pop-up window pre-populated with all collected information.

6) If required, modify any attribute displayed on the **Migrate to OpenScape 4000 resource** pop-up window.

7) Click **Migrate** to start the resource migration.

- **If** There is more than one OpenScape 4000 resource assign to the UM User:

  – System allows either to migrate the first assigned OpenScape Voice resource and move to the next, or to directly "skip" to the next assigned OpenScape 4000 resource, by clicking **Skip this Resource**.

8) Following substeps will be worked off by the system:

The System...

a) ... creates the new OpenScape 4000 resource and assigns it to the UM User.

b) ... removes the migrated OSV resource from the CMP database.

c) ... updates the routing in OSV.

d) ... updates the routing in OpenScape 4000.

NOTICE:

Routing notifications should be configured and enabled.

---

e) ... updates CMP database with the following actions:

- -) deletes OSV P hone Object.
- -) creates OpenScape 4000 Phone Object.
- -) associates OpenScape 4000 Phone Object with UC User.

f) ... informs that the OpenScape 4000 resource has been successfully migrated.

- **If** OSV resource was the voice-mail for an Xpressions resource, the Xpressions resource will be updated.
- **If** an error occurs during the creation of a new OpenScape 4000 resource:
  - – System handles the error displaying information related to the Resource.
  - – The OSV Resource remains intact, due to the migration failure.

11 OpenScape User Management Provisioning

OpenScape User Management supports various provisioning scenarios (both for the new installations, as well as for the existing ones), that help faster and easier creation of UM Users and their Resources.

For the new installation, the automatic creation of UM Users and Resources can be easily performed using:

- Import of the CSV file
- Synchronization with an LDAP Directory

For the existing installations, automatic UM Users creation and Resources assignment is supported through:

- Unified Communications
- OpenScape Voice
- Installations managed by HiPath User Management (HPUM).

11.1 How to Import Users and Resources with a CSV file

This Chapter describes How to Import UM Users and Resources using the Comma-separated values (CSV) file.

Prerequisites

Adequate administrative permission that allows the Management of Users and Resources.

Step by Step

1) Navigate to **User Management** > **Provisioning** > **CSV Import**.

A pop-up window **Import Users via CSV** is displayed.

2) Navigate to the **Configuration** area to define how to handle the Resources that are already assigned to a User but are not defined in the User Template.

Select one of the following options:

a) • **associate the User with the User Template without affecting the additional resources**

(resources that were previously manually assigned to a User or applied with a different User Template will stay intact)

NOTICE:

There are cases where a recreation or change of the OSMO subscriber(s) is needed which are already assigned to Main OSV DNs. i.e. During migration of Circuit subscribers to Unify phone.

Currently the UM does not offer a mechanism to match existing OSMO resources and alter them. Only the creation of new OSMO resources is supported.

In such cases, initially import a CSV file containing the OSV subscribers and the template for the

creation of the desired resources (OSV subscriber, OSMO, UC, etc). As a second step, import the exact same CSV again. After the second import, the OSMO resources are successfully assigned to the UM user.

- **un-assign the additional resources**

  (resources that were previously manually assigned to a User or applied with a different User Template will be unassigned)

- **un-assign and delete the additional resources**

  (resources that were previously manually assigned to a User or applied with a different User Template will be unassigned and deleted).

NOTICE:

When a User Template with Xpressions Resources is applied to a User and a modification in the User Template takes place where only the User ID field in the User Template has been changed, then the **un-assign and delete the additional resources** rule is only applied, even if any other choice has been selected.

3) In the **Organizational Structures** area, the following options are available when the attributes of the user's organizational structures are modified:

   - – **Update User's Organizational Structure**: Assigns a new structure to the user
   - – **Update current Organizational Structure for all Users**: This option is updates the current Organizational Structure for the users that previously had the same organizational structure.

4) Click **Choose File** to select the desired CSV file.

IMPORTANT:

For detailed specification of CSV file, refer to the table CSV Columns, at the end of this chapter.

When creating the CSV file, the following things have to be taken into consideration:

- It must contain all 47 column headers

- Columns, for which there is no data available, can remain empty, but all column headers must be present in the table. Otherwise, the CSV import operation will fail.

- The order of the column headers is not important, as long as all 47 of them are included in the CSV file.

- The column separator must be semicolon character ";".

- Files that are imported must be ANSI encoded. In case the file contains non-ASCII characters (eg. Umlauts) it is recommended to be encoded with option "UTF-8 without BOM" (eg. using Notepad++ tool).

- You can optionally add Custom User Attributes through a CSV file. The Custom User Attribute's Id must be

put at the end of the text string and always in the form: `<customeruserattributeid1>;<customuserattributeid2>`..

The Custom User Attributes' Ids can be found in **User Management > Administration > Custom UserAttributes**

- You can optionally add Organizational Structure Attributes through a CSV file. The Organizational Structure Attribute's Id must be put at the end of the text string and always in the form: `<orgStrAttr1>;<orgStrAttr2>`..

The Organizational Structure Attributes' Ids can be found in **User Management > Administration > Organizational Structure Attributes**

NOTICE:

In order to create the valid CSV column headers, for your own convenience, place the following text string within the same row:

`id;domain;userid;lastName;firstName;middleName;gender;sa`

Then enter on following row (on second row/cell A2), the related values to create a UM user. To create more UM users add related values on more rows.

;system;alice.dere;Dere;Alice;;;;;de_DE;Europe/Berlin;Alice.Dere;;;;;

in different domains, but it is not allowed to perform them simultaneously within the same domain.

a) In case importing procedure is already initiated by a different administrator in the same domain:

- – system does not allow execution of the procedure
  – system informs that the operation is not possible because the procedure has already been started.

b) In case the UM User's attribute **Locality**, which has been specified in the CSV file, does not exist in the system:

- – the creation of the UM User fails
  – the error is reported in the log file

c) If the UM User's attribute **User Template**, which has been specified in the CSV file, does not exist in the system:

- – the creation of the UM User fails
  – the error is reported in the log file.

7) Click **Cancel** to stop an ongoing operation.

NOTICE: System does not rollback already created UM Users and it does not leave a UM User in an inconsistent state.

Depending on the operation outcome, upon its completion, a pop-up window containing information or error messages is displayed.

8) Click **Close** to shut down the pop-up window and get back to the **Import Users via CSV** screen.

System stores information about all operations performed during the latest import operation in the log file

9) Click **Download Report** to download a log file with the details of the latest performed operation.

NOTICE:

Log files are stored on the server, under the following

path:

- **for integrated Simplex =** `/log/OSCUM/`

- **for all other deployments =** `/var/siemens/common/log/OSCUM/`

10) Click **Close** to shut down the **Import Users via CSV** pop-up.

NOTICE:

In order to view the imported data, the UM Users list needs to be explicitly accessed. This means that after you close the **Import Users via CSV** pop-up, you need to navigate to the **Users&Resources** screen and refresh it, so that you see the new UM Users.

Table 34: CSV Columns

Name	Description	Mandatory	Notes
id			sequential number/not used for user creation.
domain		yes	CMP domain where the User will be created.
userid	User ID	yes	Not allowed characters: - " ’ " (Apostrophe) - "@" - ";" (Semicolon) - " " (white space) at the start, or at the end of the User ID.
lastName	Last Name	yes	
firstName	First Name		
middleName	Middle name		
gender			
salutation			
title	Personal Title		
language	Language	yes	
homeTimeZone	Home Time Zone	yes	
displayName	Display Name	yes	
explicitDisplayName	explicit Display Name	yes	
notice			
description	Description		
locality	Locality		Locality’s name is case sensitive
building	Building		
room	Room		
street	Street		
postalCode	Postal Code		
city	City		
stateProvince	State/Province		
country	Country		

Name	Description	Mandatory	Notes
company	Comp. Name / Company		
department	Department		
businessPhone1	Bus. Phone 1		
businessPhone2	Bus. Phone 2		
mobilePhone	Mobile Phone		
homePhone	Home Phone		
video	Video		
fax	Fax Phone / Fax #		
emailAddress	Email Address / Mail		
alternateEmailAddress	Email Address 2		
imAddress	IM Address		
homeURL	Home URL		
userTemplate	User Template		User Template' s name is case sensitive
clientMatterCode1	Client Matter Code 1		
clientMatterCode2	Client Matter Code 2		
clientMatterCode3	Client Matter Code 3		
clientMatterCode4	Client Matter Code 4		
clientMatterCode5	Client Matter Code 5		
clientMatterCode6	Client Matter Code 6		
customField1	Custom Field 1		
customField2	Custom Field 2		
customField3	Custom Field 3		
customField4	Custom Field 4		
customField5	Custom Field 5		
customField6	Custom Field 6		

11.2 How to Import Users from HPUM

The scope of this Chapter is to show the most effective way of creating the UM Users and assigning to them Resources by importing the CSV file from HiPath User Management (HPUM).

Prerequisites

Adequate administrative permission that allows User Management and Provisioning.

Step by Step

1) Navigate to **User Management** > **Provisioning** > **Users from HPUM**.
2) Click **Users from HPUM** to import Users' data from the CSV file that is exported from HPUM.

   A pop-up window **Create Users from HPUM** is displayed.
3) Select one of the available values from the drop-down list to create the rules for generation of **User ID**.

   `From HPUM use:`<**User ID**> <**Delimiter**>

   - where <**User ID**> can be:

User ID
User ID
Local part of email address
User Account
Windows Account

   - and <**Delimiter**> has one of the below values:

Delimiter
and replace space(s) with "."
and replace space(s) with "_"
and remove space(s)

   NOTICE: In case duplicate logins are generated by the rule specified below, the system appends an incremental number to the **User ID** (i.e. JohnDoe, JohnDoe1, JohnDoe2 etc.).
4) Click **Browse** to select the desired CSV file exported from HPUM.

   NOTICE: The specification for the CSV file columns is given in the HPUM CSV Columns, at the end of this

chapter. The CSV file column separator is the semicolon character (';').

A pop-up window **Choose file/File Upload** is displayed.

- **If** the selected CSV file does not contain the same columns specified in the table HPUM CSV Columns:
  - System does not allow the execution of the procedure.
  - System informs that importing operation is not possible due to the CSV file format.

5) Select the CSV file stored locally and click **Open**.

The CSV file is chosen to be imported.

IMPORTANT:

Files that are imported must be UTF-8 encoded.

6) Click **Start** to initiate the import procedure.

NOTICE:

In multitenant deployments the bulk operations should be allowed to run concurrently across domains. Consequently, it is possible to perform the bulk operations simultaneously in different domains, but it is not allowed to perform them simultaneously within the same domain.

The System:

a) performs either the creation of the new UM Users, or modification of the existing ones, during the import procedure.

NOTICE: In case the User specified in the CSV file does not exist, a new UM User will be created.

b) validates that the resource specified in the CSV file exists in the database.

c) checks that the resource specified in the CSV file is not assigned to an UM User.

d) assigns the Resource to the UM User.

e) reports the progress of the operation using a progress bar along with the appropriate text.

a) **If** the procedure has already been initiated by a different administrator in the same domain:

- – System does not allow the execution of the procedure.
  – System informs that the operation is not possible because the procedure has already been started.

b) **If** the resource specified in the HPUM CSV file does not exist in the database:

- – The resource it is not created.

– The error is reported in the log file.

c) If the resource specified in the HPUM CSV file is already assigned to the UM User:

- – The resource it skipped from the assignment to the UM User.
  – The error is reported in the log file.

7) Click **Cancel** to stop an ongoing operation.

NOTICE: System does not rollback already created UM Users and it does not leave a UM User in an inconsistent state.

---

8) Depending on the operation outcome, upon its completion, a pop-up window containing information or error messages is displayed.

9) Click **Close**.

The pop-up window closes and you are back to the **Create Users from HPUM** screen.

10) System stores information about all operations performed during the latest import operation in the log file.

11) Click **Download Report** to download a log file with the details of the latest performed operation.

NOTICE:

Log files are stored on the server, under the following

path:

- **for integrated Simplex =** `/log/OSCUM/`

- **for all other deployments =** `/var/siemens/common/log/OSCUM/`

---

12) Click **Close** to shut down the **Create Users from HPUM** pop-up window.

NOTICE:

In order to view the imported data, the UM Users list needs to be explicitly accessed. This means that after you close the **Create Users from HPUM** pop-up, you need to navigate to the **Users&Resources** screen and refresh it, so that you see the new UM Users.

Example

Table 35: HPUM CSV Columns

Name	Mapped UM attribute	Comments
LastName	LastName	
FirstName	FirstName	
Personal Title	Title	

Name	Mapped UM attribute	Comments
Primary Phone #	BusinessPhone1	Only the resource set as Primary Phone on the HPUM User is exported. If HPUM User has more than one resource (of any type) assigned, they will not be exported.
Fax #	Fax	
Mail	E-mail/(used for User ID creation)	
User Account	(not used)	
Windows Domain	(not used)	
Windows Account	(used for User ID creation)	
Cost Center	(not used)	
Pin Number-PIN Class	(not used)	
Organization	(not used)	
Org 1	(not used)	
Org 2	(not used)	
Org 3	(not used)	
Room	Room	
Building	Building	
Locality	Locality	
Street	Street	
PostalCode	PostalCode	
City	City	
Country	Country	
Xpressions User ID	(not used)	
Cit	(not used)	
Company	Company	
Status	(not used)	
CDS-Key	(not used)	
User ID	(used for User ID creation)	

11.3 Synchronization with an LDAP Directory

OpenScape User Management LDAP functionality allows to synchronize the UM Users with the existing LDAP directory.

In order to perform the synchronization, the Administrator has to specify connection parameters to the LDAP directory and to define mappings between the UM User attributes and LDAP attributes.

NOTICE:

In order to be able to automatically discover, populate and map the LDAP attributes from an LDAP server V3 to CMP V7 OpenScape UM LDAP menu, it is required to use the LDAP schema version 3.

Synchronization with the LDAP directory can be triggered manually or via scheduler, which is configured to perform the LDAP synchronization at regular time intervals.

11.3.1 How to Setup LDAP Connection

This Chapter describes how to configure all required connection parameters for LDAP directory in order to allow synchronization with the UM Users.

Prerequisites

Adequate administrative permission that allows User Management and Provisioning.

The default (initial) state of LDAP connection is set to "deactivated".

Step by Step

1) Navigate to **User Management** > **Provisioning** > **LDAP**.
2) Click **Connection...** in order to configure the LDAP Connection.

   A pop-up window **LDAP Connection** is displayed.
3) Check the **Enable LDAP Connection** option in order to enable the connection.

   LDAP Connection information attributes appear to be editable now.

4) Check the **Use Secure Connection** option to establish a secure TLS LDAP connection. In case an IP Port is also provided, then the button **Retrieve Certificate** is activated.

NOTICE:

Since, at various cases below we will assume that specific environment variables exist the following command will allow their proper population in a new SSH session:

```
source /etc/sysconfig/siemens/symphonia
```

Any environment variables created and populated after the aforementioned command will be lost upon the termination of the SSH session.

A new properties file containing security related configuration parameters has been added under the path:

```
$SYMPHONIA_HOME/common/conf/application-external/trust-store.properties
```

A short description of the security properties included in the aforementioned configuration file is given in the table below:

Table 36: Security properties in trust-store.properties file

Property name	Type of Value	Default Value	Comments
trustoreFile	a sting containing the absolute path to the trust store file	`$SYMPHONIA_HOME/common/conf/application-external/ldapcacerts`	This is a Java key store which is used as the trust store for the LDAP certificate that will be downloaded.

Property name	Type of Value	Default Value	Comments
trustorePass	a string containing the encrypted password that was used to create a trust store file	encrypted value of a pre-decided password	The following commands allow the encryption and decryption of a password string (for demonstration purposes, we will assume the dummy password "123456"): • Encrypt the dummy password "123456" so as to use the encrypted value to populate the "trustorePass" configuration property: $SYMPHONIA_HOME/servicetools/cmp/encodePassphrase.sh 123456 For convenience, the above encrypted password may be kept in a temporary (session scope) environment variable. For convenience purposes, we will assume that this temporary environment variable is called TRUST_STORE_PASS • Decrypt the above encrypted value so as to verify that the origin password is the "123456" $SYMPHONIA_HOME/servicetools/cmp/decodePassphrase.sh $TRUST_STORE_PASS
trustoreType	a string containing the type of the trust store	"jks"	Currently, ONLY the value "jks" is allowed.
trustPolicyType	a string specifying the desired trust policy	"TRUSTED"	Possible values are "NONE", "TRUSTED" or "FULL"
ocspFilePath	a string specifying an absolute file path to the OCSP responder's certificate	empty	This configuration property is mandatory forenabling the OCSP revocation check.

Property name	Type of Value	Default Value	Comments
trustAnchorAlias	a string value corresponding to the alias name used to manually import a trusted certificate into the trust store	empty	This configuration property is mandatory forenabling the OCSP revocation check.
sslProtocol	string value	"TLS"	Possible values are "TLS" or "TLSv1.2"
keystoreFile	a sting containing the absolute path to the key store file	see comments	By default it is populated with the value contained in the same attribute of the service Catalina's connector in the file:"`$SYMPHONIA_HOME/share/tomcat/conf/server.xml`"
keystorePass	a string containing the encrypted password that was used to create a key store file	see comments	By default it is populated with the encrypted value copied from the same attribute of the service Catalina's connector in the file:"`$SYMPHONIA_HOME/share/tomcat/conf/server.xml`"
keystoreType	a string containing the type of the keystore	see comments	By default it is populated with the corresponding value from the same attribute of the service Catalina's connector in the file:"`$SYMPHONIA_HOME/share/tomcat/conf/server.xml`"

IMPORTANT:

When you want to use a special character, such as "**=**" `trustorePass` or `keystorePass`, always use it in the form "/=" or use the CMP LDAP SSL CLI Utility described below, which automatically encodes the password. Otherwise you will receive an error.

CMP LDAP SSL CLI Utility

Use the `ldapConfigureSSL.sh` script below as a utility, that will allow you to perform the following two actions:

- – retrieve the clear password of either the trust store or the key store
  – change either the trust store or the key store password

```
$ ${SYMPHONIA_HOME}/servicetools/cmp/
ldapConfigureSSL.sh ${SYMPHONIA_FW}/conf/application-
external/trust-store.properties set trustorePass
 123456

$ ${SYMPHONIA_HOME}/servicetools/cmp/
ldapConfigureSSL.sh ${SYMPHONIA_FW}/conf/application-
external/trust-store.properties get trustorePass

------------------------------------------------------------

$ ${SYMPHONIA_HOME}/servicetools/cmp/
ldapConfigureSSL.sh ${SYMPHONIA_FW}/conf/application-
external/trust-store.properties set keystorePass
 123456

$ ${SYMPHONIA_HOME}/servicetools/cmp/
ldapConfigureSSL.sh ${SYMPHONIA_FW}/conf/application-
external/trust-store.properties get keystorePass
```

For security purposes, you can interactively set the trustore or keystorePass also by using the following command that will prompt you to type the password:

```
$ ${SYMPHONIA_HOME}/servicetools/cmp/ldapConfigureSSL.sh
 ${SYMPHONIA_FW}/conf/application-external/trust-
store.properties set trustorePass

$ ${SYMPHONIA_HOME}/servicetools/cmp/ldapConfigureSSL.sh
 ${SYMPHONIA_FW}/conf/application-external/trust-
store.properties set keystorePass
```

Upon installation the keystore related properties (i.e. **keystoreFile**, **keystorePass**, **keystoreType**) in the file $SYMPHONIA_HOME/common/conf/application-external/trust-store.properties are populated from the values of the corresponding attributes of the **Connector** element's attributes under the Catalina service element of the file $SYMPHONIA_HOME/share/tomcat/conf/server.xml.

If ANY of the keystore related attributes (i.e. **keystoreFile**, **keystorePass**, **keystoreType**) is changed in the aforementioned part of the Apache Tomcat **server.xml**, then the modified value should propagated to the corresponding property value of the file **trust-store.properties**.

The table below specifies the corresponding property in the file **trust-store.properties** for each related attribute of the Apache Tomcat **server.xml**.

Apache Tomcat Keystore Configuration Parameters	
$SYMPHONIA_HOME/share/tomcat/conf/server.xml.	**$SYMPHONIA_HOME/common/conf/application-external/trust-store.properties**
keystoreFile	keystoreFile

Apache Tomcat Keystore Configuration Parameters	
keystorePass	keystorePass
keystoreType	keystoreType

Additionally, in the file

`$SYMPHONIA_JAVA/lib/security/java.security`

the following properties should be edited:

Table 37: Security properties in java.security file

Property name	Type of Value	Default Value	Comments
ocsp.enable	true" or "false"	empty	This configuration property is mandatory for enabling the OCSP revocation check
ocsp.responder.URL	string value containing a valid URL	empty	This configuration property is mandatory for enabling the OCSP revocation check, unless the certificate under validation contains a valid AIA extension field

NOTICE:

In order for the changes in the file "**java.security**" to take effect within the JVM (Java Virtual Machine) a symphonia restart is needed, which may be performed with the command `/etc/init.d/symphoniad restart`

Detailed instructions on how to configure the LDAP security for CMP are given in chapter "How to configure LDAP security"

5) Click on **Retrieve Certificate** button and a pop-up window Certificate is displayed. The certificate overview contains the following information:

- Issued to: The certificate holder’s name.
- Issued by: The digital signature of the certificate issuing authority.
- Valid from: The certificate’s validation date.
- Valid to: The certificate’s expiration date.
- Thumbprint: A copy of the certificate holder’s public key.

a) Click **Download Certificate** to download the Server’s LDAP certificate.

b) Click **Accept Certificate** to accept the Server’s LDAP certificate. Accept the Certificate to be able to save the Secure Connection.

NOTICE:

In case the certificate has been expired a "**Certificate Status**: Expired" will appear.

In case the server is not providing a Certificate the Overview section will be empty and the Accept Certificate button disabled.

6) Enter the following required information to configure the connection:

- **Hostname/IP** (mandatory field)
- **Port** (mandatory field)
- **User name** (mandatory field)
- **Password** (non mandatory field)

IMPORTANT:

The special character "§" is not supported as part of a password.

- **Source base** (mandatory field)

When working with Global Catalog Search, use 3268 (LDAP) and 3269 (LDAPS) instead of the standard LDAP 389 or LDAPS 636 port number.

7) Click **Save** in order to commit the changes to the LDAP Connection.

System:

a) • verifies that the supplied information is correct

• notifies that the changes made to the LDAP connection parameters have been applied successfully.

If an LDAP synchronization has been performed at least once in the past on the system, a warning is displayed in order to notify the user that a full synchronization will be needed after the modification of the LDAP filter or the LDAP connection.

NOTICE:

The following warning message appears:

"A modification in the existing LDAP filter was detected.

Please, perform a full LDAP synchronization in order to avoid inconsistencies."

11.3.1.1 How to configure the LDAP security for CMP

The successful configuration of a secure LDAP connection requires an initial setup on the CMP server host through an ssh connection. Below you may find detailed instructions on how to properly populate the necessary configuration files.

Prerequisites

Adequate administrative permission that allows User Management and Provisioning in each domain that user wants to administer.

Step by Step

1) Establish an SSH session with the server where CMP is installed and import into the current shell session the need environment variables with the following command: `source /etc/sysconfig/siemens/symphonia`

2) Change directory with the following command: `cd $SYMPHONIA_HOME/common/conf/application-external`

NOTICE:

Since, in the following steps the value of the environment variable "**$SYMPHONIA_HOME**" will be needed, the command `echo $SYMPHONIA_HOME` retrieves its value.

---

3) Edit the new properties file "**$SYMPHONIA_HOME/common/conf/application-external/trust-store.properties**" and populate the "trustoreFile" property with the value `trustoreFile=/opt/siemens/common/conf/application-external/ldapcacerts`, where we have assumed that the environment variable "**$SYMPHONIA_HOME**" is populated with the value "/opt/siemens".

4) The `ldapcacerts` trust store password needs to be provisioned before its creation. Otherwise, if a secure LDAP connection is attempted, then the `ldapcacerts` trust store will be created and encrypted with the default password (which is shipped with the fresh installation). The `ldapcacerts` trust store is created and encrypted with the `trustorePass` upon the first secure LDAP connection (either successful or not). The modification of the `ldapcacerts` trust store password is not supported.

   a) The following command populates the `trustorePass` key in the trust-store.properties file with the newly desired password (properly encrypted). The password needs to be typed in clear text on the command line terminal.

   ```
   ${SYMPHONIA_HOME}/servicetools/cmp/ldapConfigureSSL.sh ${SYMPHONIA_FW}/conf/application-external/ trust-store.properties set trustorePass 123456
   ```

   b) If the previously provisioned `trustorePass` password needs to be read in clear text, then this may be achieved with the following command.

   ```
   ${SYMPHONIA_HOME}/servicetools/cmp/ldapConfigureSSL.sh ${SYMPHONIA_FW}/conf/application-external/ trust-store.properties get trustorePass
   ```

   c) An additional interactive mode is also available, so that the new trusto-rePass password does not need to be typed in clear text on the command line terminal. For example, the following command will request from the administrator to enter the new trustorePass password twice (for verification purposes), without having the new password displayed in clear text on the terminal session.

   ```
   ${SYMPHONIA_HOME}/servicetools/cmp/ldapConfigureSSL.sh ${SYMPHONIA_FW}/conf/application-external/ trust-store.properties set trustorePass
   ```

   d) Almost the same commands may be used for the keystorePass keys store password (of the Apache Tomcat key store), with the apparent difference that the property name changes from trustorePass to

keystorePass.In summary, the corresponding commands are provided below:

a) If UM User doesn't have Locality assigned:

- – Change the `keystorePass` password of the Apache Tomcat key store to 123456 (in a non-interactive mode).

  `${SYMPHONIA_HOME}/servicetools/cmp/ldapConfigureSSL.sh ${SYMPHONIA_FW}/conf/application-external/trust-store.properties set keystorePass 123456`

b) • – Retrieve the `keystorePass` password of the Apache Tomcat key store in clear text.

`${SYMPHONIA_HOME}/servicetools/cmp/ldapConfigureSSL.sh ${SYMPHONIA_FW}/conf/application-external/trust-store.properties get keystorePass`

c) • – Change the `keystorePass` password of the Apache Tomcat key store to a new value, but this time interactively. The administrator will be asked to enter the new password twice for verification purposes. In addition the twice typed password will not be visible on the command line terminal.

`${SYMPHONIA_HOME}/servicetools/cmp/ldapConfigureSSL.sh ${SYMPHONIA_FW}/conf/application-external/trust-store.properties get keystorePass`

5) Download in the current directory the chosen trust anchor's certificate which in our case for convenience is named "**trusted-anchor-certificate.cer**". In addition, change both its user and group ownership with the command `chown sym:sym trusted-anchor-certificate.cer`

6) Edit the "**trust-store.properties**" file and populate the "**trustAnchorAlias**" property with the alias name that will be used to identify the imported trusted anchor certificate into the trust store, e.g. `trustAnchorAlias=trusted-anchor-alias`

7) If the Java utility "**keytool**" is not included by default in the $PATH environment variable, the command `export PATH=$SYMPHONIA_JAVA/bin:$PATH` will allow it to be included.

8) Import the trusted anchor certificate "**trusted-anchor-certificate.cer**" into the "**ldapcacerts**" trust store and associate it with the alias name "**trusted-anchor-alias**" with the command `keytool -import -noprompt -keystore ldapcacerts -storetype jks -storepass 123456 -alias trusted-anchor-alias -file trusted-anchor-certificate.cer`

NOTICE:

If the assumed trust store file "**ldapcacerts**" does not exist it will be created and it will be owned by the root user. The trusted anchor alias value "**trusted-anchor-alias**" is the alias that will be used to import and associate the previously downloaded trusted anchor certificate file into the trust store file "**ldapcacerts**".

---

9) Change the ownership of the trust store file "**ldapcacerts**" to user "**sym**" and group "**sym**" with the command `chown sym:sym ldapcacerts`

10) Verify that the above trusted anchor alias name has been created successfully and the corresponding trusted anchor certificate has been successfully imported into the trust store with the command `keytool -v -list -keystore ldapcacerts -storetype jks -storepass 123456 -alias trusted-anchor-alias`

NOTICE:

In case where the trusted anchor is the same host with the OCSP responder, then the trusted anchors certificate could be the same with the OCSP responder's certificate.

---

11) Populate the "**ocspFilePath**" property with absolute path of the location where the OCSP responder's certificate has been downloaded, e.g. `ocspFilePath=/opt/siemens/common/conf/application-external/ocsp-responder-certificate.cer`

This is the OCSP responder's certificate which we need so as to authenticate the OCSP responder itself. It has been assumed here that the environment variable "**$SYMPHONIA_HOME**" has the value "/opt/siemens". This file needs to be downloaded into the aforementioned absolute path. In addition, it's ownership needs to be set to user "**sym**" and group "**sym**" with the command `chown sym:sym $SYMPHONIA_HOME/common/conf/application-external/ocsp-responder-certificate.cer`

or in two steps:

```
cd $SYMPHONIA_HOME/common/conf/application-external
chown sym:sym ocsp-responder-certificate.cer
```

12) Enable the OCSP check by editing the file "**$SYMPHONIA_JAVA/lib/security/java.security**". Populate the property "**ocsp.enable**" with the "**true**" value, i.e. `ocsp.enable=true`

13) Populate the "**ocsp.responderURL**" property in the file "**$SYMPHONIA_JAVA/lib/security/java.security**" with the URL where the OCSP responder is serving OCSP requests and sends OCSP responde messages.

NOTICE:

In order for the changes in the file "**java.security**" to take effect within the JVM (Java Virtual Machine) a symphonia restart is needed, which may be performed with the command `/etc/init.d/symphoniad restart`

---

14) In order to facilitate the troubleshooting of a repeatedly failing secure LDAP connection, the following script may be used. It is recommended to be executed twice. Once, before the attempt for a secure LDAP connection

and an additional one right afterwards. This way, a differential analysis of the collected logs may speed up the root cause analysis.

a) Before an attempt for a secure LDAP connection.

```
${SYMPHONIA_HOME}/servicetools/cmp/
ldapCollectLogs.sh /tmp/before-ldap-ssl-collect-
logs.tar.gz
```

b) After an attempt for a secure LDAP connection.

```
${SYMPHONIA_HOME}/servicetools/cmp/
ldapCollectLogs.sh /tmp/after-ldap-ssl-collect-
logs.tar.gz
```

11.3.2 How to Deactivate LDAP Connection

The scope of this Chapter is to show How to disable the LDAP Connection.

Prerequisites

Adequate administrative permission that allows User Management and Provisioning.

The LDAP connection is enabled.

Step by Step

1) Navigate to **User Management** > **Provisioning** > **LDAP**.

2) Click **Connection...** in order to disable the LDAP Connection.

A pop-up window **LDAP Connection** is displayed.

3) Uncheck the **Enable LDAP Connection** option in order to disable the connection.

LDAP Connection information fileds are not editable any more.

4) Click **Save** in order to commit the changes made to the LDAP Connection.

System:

a)
- clears the configuration values
- disables any scheduled LDAP Synchronization tasks
- does not allow any Manual LDAP Synchronization
- does not allow any Automatic LDAP Synchronization
- displays the following warning message on the information area of the main LDAP screen: `LDAP connection has not been set. Synchronisation is not possible`.

11.3.3 How to configure different LDAP synchronization per CMP Domain

This procedure describes How to set up different LDAP connection, mappings and synchronization schedule per domain, so that multi-tenancy scenarios, where each customer uses a specific domain in CMP, are supported.

Prerequisites

Adequate administrative permission that allows User Management and Provisioning in each domain that user wants to administer.

Step by Step

1) Navigate to **User Management** > **Provisioning** > **LDAP**.

2) Configure the following LDAP elements:

- connection (for more information see How to Setup LDAP Connection)
- mappings (see How to perform LDAP Attribute Mappings)
- synchronization (for more information see How to perform Scheduled and Manual Synchronization).

3) Select to changes domain in one of the following ways:

- directly, by selecting a different domain from the **Domain** drop-down list, located on the CMP System bar (the header of CMP screen).
- by logging out and then logging back in to CMP, using different domain.

The domain has been changed.

4) Configure different LDAP connection, mappings and synchronization than before, in Step 2.

A new LDAP synchronization has been configured per CMP Domain.

11.3.4 How to retrieve the available LDAP Attributes

The Administrator has an opportunity to select the available LDAP attributes of the specified LDAP connection and create mappings between these attributes and UM attributes. Using this functionality, there is no need to enter manually any custom defined attributes.

Prerequisites

Adequate administrative permission that allows User Management and Provisioning.

The LDAP connection is enabled.

NOTICE:

In order to be able to automatically discover, populate and map the LDAP attributes from an LDAP server V3 to CMP V7 OpenScape UM LDAP menu, it is required to use the LDAP schema version 3.

Step by Step

1) Navigate to **User Management** > **Provisioning** > **LDAP**.
   A list of the existing LDAP Attribute Mappings is displayed sorted per column **UM**.
2) Click **LDAP Attributes...** to define the attributes.

   A pop-up window **LDAP Attributes to use** is displayed.
3) Choose the Object Class from the **Select Object Class** list and click **Select**.

   System retrieves the LDAP attributes of the specified LDAP directory and displays them in the **Attributes** list.
4) Select the Object Class attribute from the **Attributes** list and click **Add**.

   The selected attributes appear in the **Select attributes to use** list.

   NOTICE:

   The list of selected attributes supports multiple selection. This implies that you can select multiple attributes at once and by just one click on the **Delete** button, delete all of them.
5) Click **Save** to save the LDAP attributes list.

   System displays the action to be performed and requests confirmation to replace the current list of the LDAP attributes with the latest selected attributes.
6) Click **OK** to save changes.

   System saves the new LDAP attributes retrieved from the LDAP directory.

11.3.5 How to perform LDAP Attribute Mappings

The subject of this Chapter is the mapping between UM User attributes to LDAP attribute or Constant values and LDAP attributes to UM User attribute.

Prerequisites

Adequate administrative permission that allows User Management and Provisioning.

IMPORTANT: The mandatory User attributes (see the Table: UM User attributes) are always listed in the list of mappings, even if no mapping is defined. These User attributes cannot be removed from the attribute mapping list.

IMPORTANT:

In order an LDAP user to be assigned to a specific user template, the user has to assign the user template to LDAP mapping.

NOTICE: The list of all available **LDAP Attributes** is shown in the drop-down list. In addition to these attributes, administrator

can specify **New LDAP Attributes** and map them to the UM User attributes.

Step by Step

1) Navigate to **User Management** > **Provisioning** > **LDAP**.
A list of the existing LDAP Attribute Mappings is displayed sorted per column **UM**.
2) Select to configure mapping between the User attribute and the LDAP Directory attribute.

NOTICE: Steps 3-5 are repeated for all **User attributes** that are going to be mapped to the **LDAP Attribute**.

3) Select one of the available values from the **User attribute** drop-down list (see the Table: UM User attributes).
The **User attribute** are sorted by name.
4) Select the **LDAP Attribute** (see How to retrieve the available LDAP Attributes) from the drop-down list or specify a **New LDAP Attribute**.

NOTICE: The custom, **New LDAP Attribute** is not appended to the pre-configure **LDAP Attributes**.

5) Click **Add** to map the **User attribute** to the **LDAP attribute**.

NOTICE: In case the selected **User attribute** is already in the mapped attributes list, system updates the selected **User attribute** with the newly specified **LDAP Attribute**.

The new mapping of two attributes will appear within the list of the existing LDAP Attribute Mappings.
6) Select to configure mapping between the User attributes and Constant Value (these Values are system defined and can be selected from the drop-down list, so that there is no need to look for them or make syntax errors).

NOTICE: Steps 7-9 are repeated for all **User attributes** that will be mapped to the **Constant Value**.

7) Select one of the available values from the **User attribute** drop-down list (see the Table: UM User attributes).
The **User attribute** are sorted by name.
8) Select one the available values from the **Constant Value** drop-down list, for the following attributes:

- **Language**
- **Home Time Zone**
- **Country**
- **Locality**
- **User Template**

INFO: For more information about the Constant Values, see the tables: Language values for constant mapping,

Home Time Zone values for constant mappings and Country values for constant mapping.

IMPORTANT:

If no Constant values have been specified for the selected attribute, system displays an empty drop-down list and does not allow to add mappings.

9) Click **Add** to map the **User attribute** to the **Constant Value**.

NOTICE: In case the selected **User attribute** is already in the mapped attributes list, system updates selected **User attribute** with the newly specified **Constant Value**.

10) Select to configure mapping between the LDAP Directory attribute and the User attribute.

NOTICE: Steps 11-13 are repeated for all **LDAP attributes** that are going to be mapped to the **User Attribute**.

11) Select the **LDAP Attribute** (see How to retrieve the available LDAP Attributes) from the drop-down list.

12) Select one of the available values from the **User attribute** drop-down list (see the Table: UM User attributes).

The **User attribute** are sorted by name.

NOTICE: The attributes that are mandatory for the User Creation cannot be selected.

13) Click **Add** to map the **LDAP attribute** to the **User attribute**.

NOTICE: In case the selected **User attribute** is already used in an LDAP to UM mapping, system will not add the UM to LDAP mapping and will display an error message.

The new mapping of two attributes will appear within the list of the existing LDAP Attribute Mappings. Column **Mapping Direction** indicates the direction of the LDAP mapping (UM to LDAP or LDAP to UM).

IMPORTANT:

When the UM User's attribute **Locality** is modified via LDAP synchronization, the address related attributes of this UM User will not be updated.

On the other side, when manually crating, or modifying the UM Users, an option **When saving, update the Address Data of the User currently using this locality with the data below** is introduced under **User Management** > **Administration** > **Localities** > **Edit locality**. This option allows managing how the UM Users, currently using one Locality, will be updated: either by **replacing**, by **disabling**

to replace or by **merging** the Users' Address Data with the Locality Address Data.

Table 38: UM User attributes

UM Attribute	Mandatory	Notes
User ID	yes	Not allowed characters: - " ’ " (Apostrophe) - "@" - ";" (Semicolon) - " " (white space) at the start, or at the end of the User ID.
Last Name	yes	
First Name		
Middle Name		
Gender		
Salutation		
Title		
Language	yes	
Home time zone	yes	
Display Name	yes	
Notice		
Description		
Locality		
City		
State/Province		
Country		
Company		
Department		
Building		
Room		
Street		
Postal Code		
Bus. Phone 1		
Bus. Phone 2		
Mobile Phone		
Home Phone		

UM Attribute	Mandatory	Notes
FAX number		
Explicit Display Name		
E-mail address		
E-mail address 2		
IM Address		
Home URL		
JPEG Photo		Photo size up to 16384 bytes
User Template		

Table 39: LDAP attributes

LDAP Attribute	Description
c	Country-Name
cn	Common-Name
co	Text-Country
company	Name
department	Department
displayName	Display-Name
distinguishedName	Obj-Dist-Name
givenName	Given-Name
l	City-Name
mail	E-mail-Addresses
mailNickname	
mobile	Phone-Mobile-Primary
name	RDN
postalCod	Post or ZIP codUser IDe
sn	Surname
st	State name
street	Street-Address
streetAddress	Address
telephoneNumber	Telephone-Number
title	Job Title

Table 40: Language values for constant mapping

Name	Value
German	de_DE
American English	en_US
British English	en_GB
Chinese	zh_CN
French	fr_FR
Spanish	es_ES
Italian	it_IT
Portuguese	pt_PT
Portuguese (Brazil)	pt_BR

Table 41: Gender values

Name	Value
Male	male
Female	female

Table 42: Home Time Zone values for constant mappings

Name	Value	Name	Value	Name	Value	Name	Value
(UTC-11:00) Samoa	Pacific/ Samoa	(UTC-4:00) Guyana	America/ Guyana	(UTC +2:00) Cairo	Africa/ Cairo	(UTC +8:00) Brunei	Asia/ Brunei
(UTC-11:00) American Samoa	US/ Samoa	(UTC-4:00) La Paz	America/ La_Paz	(UTC +2:00) Johannesburg	Africa/ Johannesburg	(UTC +8:00) Hong Kong	Asia/ Hong_Kong
(UTC-10:00) Honolulu	Pacific/ Honolulu	(UTC-4:00) Manaus	America/ Manaus	(UTC +2:00) Lusaka	Africa/ Lusaka	(UTC +08:00) Irkutsk (RTZ 7)	Russia Time Zone 7
(UTC-10:00) Tahiti	Pacific/ Tahiti	(UTC-4:00) Santiago (Chile)	America/ Santiago	(UTC +2:00) Tripoli	Africa/ Tripoli	(UTC +8:00) Kuala Lumpur	Asia/ Kuala_Lumpur
(UTC-9:00) Anchorage	America/ Anchorage	(UTC-4:00) Bermuda Islands	Atlantic/ Bermuda	(UTC +2:00) Beirut	Asia/ Beirut	(UTC +8:00) Manila	Asia/ Manila
(UTC-9:00) Alaska Standard Time	US/ Alaska	(UTC-4:00) Atlantic Standard Time	Canada/ Atlantic	(UTC +2:00) Amman	Asia/ Amman	(UTC +8:00) Makassar (Central Indonesia)	Asia/ Makassar

Name	Value	Name	Value	Name	Value	Name	Value
(UTC-9:00) Gambier	Pacific/Gambier	(UTC-3:30) Newfoundland	Canada/Newfoundland	(UTC+2:00) Damascus	Asia/Damascus	(UTC+8:00) Shanghai	Asia/Shanghai
(UTC-8:00) Los Angeles	America/Los_Angeles	(UTC-3:00) Belem (Brazil)	America/Belem	(UTC+2:00) Istanbul	Asia/Istanbul	(UTC+8:00) Singapore	Asia/Singapore
(UTC-8:00) Vancouver	America/Vancouver	(UTC-3:00) Buenos Aires	America/Buenos_Aires	(UTC+2:00) Nicosia	Asia/Nicosia	(UTC+8:00) Taipei	Asia/Taipei
(UTC-8:00) Yukon	Canada/Yukon	(UTC-3:00) Cayenne (French Guiana)	America/Cayenne	(UTC+2:00) Tel Aviv	Asia/Tel_Aviv	(UTC+8:00) Ulan Bator	Asia/Ulan_Bator
(UTC-8:00) Pacific Standard Time	US/Pacific	(UTC-3:00) Nuuk (West Greenland)	America/Godthab	(UTC+2:00) Central African Time	CAT	(UTC+8:00) Western Standard Time (Australia)	Australia/West
(UTC-8:00) Pitcairn	Pacific/Pitcairn	(UTC-3:00) Montevideo	America/Montevideo	(UTC+2:00) Athens	Europe/Athens	(UTC+8:00) Chinese Standard Time	CTT
(UTC-7:00) Dawson Creek	America/Dawson_Creek	(UTC-3:00) Sao Paulo	America/Sao_Paulo	(UTC+2:00) Bucharest	Europe/Bucharest	(UTC+9:00) Dili (East Timor)	Asia/Dili
(UTC-7:00) Denver	America/Denver	(UTC-2:00) South Georgia	Atlantic/South_Georgia	(UTC+2:00) Helsinki	Europe/Helsinki	(UTC+9:00) Jayapura (East Indonesia)	Asia/Jayapura
(UTC-7:00) Edmonton	America/Edmonton	(UTC-2:00) Fernando de Noronha (Brazil)	Brazil/DeNoronha	(UTC+2:00) Kiev	Europe/Kiev	(UTC+9:00) Tokyo	Asia/Tokyo
(UTC-7:00) Hermosillo	America/Hermosillo	(UTC-2:00) Scoresbysund (East Greenland)	America/Scoresbysund	(UTC+2:00) Minsk	Europe/Minsk	(UTC+9:00) Seoul	Asia/Seoul
(UTC-7:00) Mazatlan	America/Mazatlan	(UTC-1:00) Azores	Atlantic/Azores	(UTC+2:00) Riga	Europe/Riga	(UTC+09:00) Yakutsk (RTZ 8)	Russia Time Zone 8

Name	Value	Name	Value	Name	Value	Name	Value
(UTC-7:00) Phoenix	America/ Phoenix	(UTC-1:00) Cape Verde	Atlantic/ Cape_Verde	(UTC +2:00) Sofia	Europe/ Sofia	(UTC +9:30) Central Standard Time (Northern Territory Australia)	Australia/ North
(UTC-7:00) Shiprock	America/ Shiprock	(UTC-0:00) Accra	Africa/ Accra	(UTC +2:00) Tallinn	Europe/ Tallinn	(UTC +9:30) Central Standard Time (South Australia)	Australia/ South
(UTC-7:00) Yellowknife	America/ Yellowknife	(UTC-0:00) Casablanca	Africa/ Casablanca	(UTC +2:00) Vilnius	Europe/ Vilnius	(UTC +10:00) Vladivostok, Magadan (RTZ 9)	Russia Time Zone 9
(UTC-7:00) Baja California Sur	Mexico/ BajaSur	(UTC-0:00) Dakar	Africa/ Dakar	(UTC +3:00) Addis Ababa	Africa/ Addis_Ababa	(UTC +12:00) Anadyr, Petropavlovsk-Kamchatsky (RTZ 11)	Russia Time Zone 11
(UTC-7:00) Mountain Standard Time	US/ Mountain	(UTC-0:00) Monrovia	Africa/ Monrovia	(UTC +3:00) Nairobi	Africa/ Nairobi	(UTC +10:00) Eastern Standard Time (New South Wales, Australia)	Australia/ ACT
(UTC-7:00) Navajo Time	Navajo	(UTC-0:00) Reykjavik	Atlantic/ Reykjavik	(UTC +3:00) Baghdad	Asia/ Baghdad	(UTC +10:00) Brisbane (Queensland)	Australia/ Brisbane
(UTC-6:00) Belize	America/ Belize	(UTC-0:00) Canary Islands	Atlantic/ Canary	(UTC +3:00) Kuwait	Asia/ Kuwait	(UTC +10:00) Melbourne (Victoria)	Australia/ Melbourne
(UTC-6:00) Chicago	America/ Chicago	(UTC-0:00) Dublin	Europe/ Dublin	(UTC +3:00) Riyadh	Asia/ Riyadh	(UTC +10:00) Sydney (New South Wales)	Australia/ Sydney

Name	Value	Name	Value	Name	Value	Name	Value
(UTC-6:00) El Salvador	America/ El-Salvador	(UTC-0:00) London	Europe/ London	(UTC +3:00) Eastern African Time	EAT	(UTC +10:00) Queensland	Australia/ Queensland
(UTC-6:00) Mexico City	America/ Mexico_City	(UTC-0:00) Lisbon	Europe/ Lisbon	(UTC +03:00) Moscow, St. Petersburg, Volgograd (RTZ 2)	Russia Time Zone 2	(UTC +10:00) Tasmania	Australia/ Tasmania
(UTC-6:00) North Dakota Center	America/ North_Dakota/ Center	(UTC-0:00) Western European Time	WET	(UTC +3:30) Tehran	Asia/ Tehran	(UTC +10:00) Victoria	Australia/ Victoria
(UTC-6:00) Tegucigalpa (Honduras)	America/ Tegucigalpa	(UTC +1:00) Algiers	Africa/ Algiers	(UTC +4:00) Baku	Asia/ Baku	(UTC +10:00) Port Moresby (Papua New Guinea)	Pacific/ Port_Moresby
(UTC-6:00) Winnipeg	America/ Winnipeg	(UTC +1:00) Brazzaville	Africa/ Brazzaville	(UTC +4:00) Dubai	Asia/ Dubai	(UTC +10:00) Saipan	Pacific/ Saipan
(UTC-6:00) Saskatchewan	Canada/ Saskatchewan	(UTC +1:00) Lagos	Africa/ Lagos	(UTC +4:00) Tbilisi (Georgia)	Asia/ Tbilisi	(UTC +10:00) Guam	Pacific/ Guam
(UTC-6:00) East Saskatchewan	Canada/ East_Saskatchewan	(UTC +1:00) Kinshasa	Africa/ Kinshasa	(UTC +4:00) Yerevan (Armenia)	Asia/ Yerevan	(UTC +10:30) Lord Howe Islands	Australia/ Lord_Howe
(UTC-6:00) Central Standard Time	US/ Central	(UTC +1:00) Tunis	Africa/ Tunis	(UTC +4:00) Samara	Europe/ Samara	(UTC +11:00) Salomon Islands	Pacific/ Guadalcanal
(UTC-5:00) Bogota	America/ Bogota	(UTC +1:00) Windhoek	Africa/ Windhoek	(UTC +4:00) Mahe (Seychelles)	Indian/ Mahe	(UTC +11:00) Noumea (New Caledonia)	Pacific/ Noumea
(UTC-5:00) Cayman Islands	America/ Cayman	(UTC +1:00) Central European Time	ECT	(UTC +4:00) Mauritius	Indian/ Mauritius	(UTC +11:00) Efate (Vanuatu)	Pacific/ Efate

Name	Value	Name	Value	Name	Value	Name	Value
(UTC-5:00) Detroit	America/ Detroit	(UTC +1:00) Amsterdam	Europe/ Amsterdam	(UTC +4:00) Reunion	Indian/ Reunion	(UTC +11:30) Norkfolk Time	Pacific/ Norfolk
(UTC-5:00) Fort Wayne	America/ Fort_Wayne	(UTC +1:00) Belgrade	Europe/ Belgrade	(UTC +4:30) Kabul	Asia/ Kabul	(UTC +12:00) Auckland	Pacific/ Auckland
(UTC-5:00) Turks and Caicos Islands	America/ Grand_Turk	(UTC +1:00) Berlin	Europe/ Berlin	(UTC +5:00) Aqtobe (Kazakhstan)	Asia/ Aqtobe	(UTC +12:00) New Zealand Standard Time	NST
(UTC-5:00) Guayaquil	America/ Guayaquil	(UTC +1:00) Bratislava	Europe/ Bratislava	(UTC +5:00) Ashgabat (Turkmenistan)	Asia/ Ashgabat	(UTC +12:00) Fiji Islands	Pacific/ Fiji
(UTC-5:00) Havana	America/ Havana	(UTC +1:00) Brussels	Europe/ Brussels	(UTC +5:00) Bishkek (Kyrgyzstan)	Asia/ Bishkek	(UTC +12:00) Tuvalu Islands	Pacific/ Funafuti
(UTC-5:00) Indianapolis	America/ Indianapolis	(UTC +1:00) Budapest	Europe/ Budapest	(UTC +5:00) Dushanbe (Tajikistan)	Asia/ Dushanbe	(UTC +12:00) Majuro (Marshall Islands)	Pacific/ Majuro
(UTC-5:00) Iqaluit	America/ Iqaluit	(UTC +1:00) Copenhagen	Europe/ Copenhagen	(UTC +5:00) Karachi	Asia/ Karachi	(UTC +12:00) Gilbert Islands (Kiribati)	Pacific/ Tarawa
(UTC-5:00) Jamaica	America/ Jamaica	(UTC +1:00) Ljubljana	Europe/ Ljubljana	(UTC +5:00) Tashkent (Uzbekistan)	Asia/ Tashkent	(UTC +12:00) Kamchatka	Asia/ Kamchatka
(UTC-5:00) Louisville (Kentucky)	America/ Kentucky/ Louisville	(UTC +1:00) Luxembourg	Europe/ Luxembourg	(UTC +5:00) Yekaterinburg (RTZ 4)	Russia Time Zone 4	(UTC +12:45) Chatham Islands (New Zealand)	Pacific/ Chatham
(UTC-5:00) Monticello (Kentucky)	America/ Kentucky/ Monticello	(UTC +1:00) Madrid	Europe/ Madrid	(UTC +5:00) Maldives	Indian/ Maldives	(UTC +13:00) Tonga Islands	Pacific/ Tongatapu

Name	Value	Name	Value	Name	Value	Name	Value
(UTC-5:00) Lima	America/ Lima	(UTC +1:00) Malta	Europe/ Malta	(UTC +5:30) Calcutta	Asia/ Calcutta	(UTC +13:00) Phoenix Islands (Kiribati)	Pacific/ Enderbury
(UTC-5:00) Montreal	America/ Montreal	(UTC +1:00) Oslo	Europe/ Oslo	(UTC +5:30) Indian Standard Time	IST	(UTC +14:00) Kiritimati (Kiribati)	Pacific/ Kiritimati
(UTC-5:00) Nassau	America/ Nassau	(UTC +1:00) Paris	Europe/ Paris	(UTC +5:45) Kathmandu (Nepal)	Asia/ Katmandu	(UTC +02:00) Kaliningrad (RTZ 1)	Russia Time Zone 1
(UTC-5:00) New York	America/ New_York	(UTC +1:00) Prague	Europe/ Prague	(UTC +6:00) Colombo	Asia/ Colombo	(UTC +7:00) Omsk	Asia/ Omsk
(UTC-5:00) Panama	America/ Panama	(UTC +1:00) Rome	Europe/ Rome	(UTC +6:00) Dhaka	Asia/ Dhaka	(UTC +04:00) Izhevsk, Samara (RTZ 3)	Russia Time Zone 3
(UTC-5:00) Acre (Brazil)	Brazil/ Acre	(UTC +1:00) Sarajevo	Europe/ Sarajevo	(UTC +06:00) Novosibirsk (RTZ 5)	Russia Time Zone 5	(UTC +11:00) Chokurdakh (RTZ 10)	Russia Time Zone 10
(UTC-5:00) East Indiana (US)	US/ East-Indiana	(UTC +1:00) Skopje	Europe/ Skopje	(UTC +6:00) Thimphu (Bhutan)	Asia/ Thimbu		
(UTC-5:00) Eastern Standard Time	US/ Eastern	(UTC +1:00) Stockholm	Europe/ Stockholm	(UTC +6:30) Rangoon (Myanmar)	Asia/ Rangoon		
(UTC-4:00) Antigua	America/ Antigua	(UTC +1:00) Tirane	Europe/ Tirane	(UTC +6:30) Cocos Islands	Indian/ Cocos		
(UTC-4:00) Asuncion	America/ Asuncion	(UTC +1:00) Vaduz	Europe/ Vaduz	(UTC +7:00) Bangkok	Asia/ Bangkok		
(UTC-4:00) Barbados	America/ Barbados	(UTC +1:00) Vienna	Europe/ Vienna	(UTC +7:00) Jakarta	Asia/ Jakarta		

Name	Value	Name	Value	Name	Value	Name	Value
(UTC-4:00) Boa Vista	America/ Boa_Vista	(UTC +1:00) Warsaw	Europe/ Warsaw	(UTC +07:00) Krasnoyarsk (RTZ 6)	Russia Time Zone 6		
(UTC-4:00) Caracas	America/ Caracas	(UTC +1:00) Zagreb	Europe/ Zagreb	(UTC +7:00) Phnom Penh	Asia/ Phnom_Penh		
(UTC-4:00) Amazon Standard Time	America/ Cuiaba	(UTC +1:00) Zurich	Europe/ Zurich	(UTC +7:00) Ho Chi Minh	Asia/ Saigon		
(UTC-4:00) Goose Bay	America/ Goose_Bay	(UTC +2:00) Eastern European Time	ART	(UTC +7:00) Vientiane	Asia/ Vientiane		

Table 43: Country values for constant mapping

Name	Value
AF	Afghanistan
AX	Aland Islands
AL	Albania
DZ	Algeria
AS	American Samoa
AD	Andorra
AO	Angola
AI	Anguilla
AQ	Antarctica
AG	Antigua and Barbuda
AR	Argentina
AM	Armenia
AW	Aruba
AC	Ascension Island
AU	Australia
AT	Austria
AZ	Azerbaijan
BS	Bahamas
BH	Bahrain
BB	Barbados

Name	Value
BD	Bangladesh
BY	Belarus
BE	Belgium
BZ	Belize
BJ	Benin
BM	Bermuda
BT	Bhutan
BW	Botswana
BO	Bolivia
BA	Bosnia and Herzegovina
BV	Bouvet Island
BR	Brazil
IO	British Indian Ocean Territory
BN	Brunei Darussalam
BG	Bulgaria
BF	Burkina Faso
BI	Burundi
KH	Cambodia
CM	Cameroon
CA	Canada
CV	Cape Verde
KY	Cayman Islands
CF	Central African Republic
TD	Chad
CL	Chile
CN	China
CX	Christmas Island
CC	Cocos (Keeling) Islands
CO	Colombia
KM	Comoros
CG	Congo
CD	Congo, Democratic Republic
CK	Cook Islands
CR	Costa Rica
CI	Cote D'Ivoire (Ivory Coast)
HR	Croatia (Hrvatska)

Name	Value
CU	Cuba
CY	Cyprus
CZ	Czech Republic
CS	Czechoslovakia (former)
DK	Denmark
DJ	Djibouti
DM	Dominica
DO	Dominican Republic
TP	East Timor
EC	Ecuador
EG	Egypt
SV	El Salvador
GQ	Equatorial Guinea
ER	Eritrea
EE	Estonia
ET	Ethiopia
FK	Falkland Islands (Malvinas)
FO	Faroe Islands
FJ	Fiji
FI	Finland
FR	France
FX	France, Metropolitan
GF	French Guiana
PF	French Polynesia
TF	French Southern Territories
MK	F.Y.R.O.M. (Macedonia)
GA	Gabon
GM	Gambia
GE	Georgia
DE	Germany
GH	Ghana
GI	Gibraltar
GB	Great Britain (UK)
GR	Greece
GL	Greenland
GD	Grenada

Name	Value
GP	Guadeloupe
GU	Guam
GT	Guatemala
GN	Guinea
GW	Guinea-Bissau
GY	Guyana
HT	Haiti
HM	Heard and McDonald Islands
HN	Honduras
HK	Hong Kong
HU	Hungary
IS	Iceland
IN	India
ID	Indonesia
IR	Iran
IQ	Iraq
IE	Ireland
IL	Israel
IM	Isle of Man
IT	Italy
JE	Jersey
JM	Jamaica
JP	Japan
JO	Jordan
KZ	Kazakhstan
KE	Kenya
KI	Kiribati
KP	Korea (North)
KR	Korea (South)
KW	Kuwait
KG	Kyrgyzstan
LA	Laos
LV	Latvia
LB	Lebanon
LI	Liechtenstein
LR	Liberia

Name	Value
LY	Libya
LS	Lesotho
LT	Lithuania
LU	Luxembourg
MO	Macau
MG	Madagascar
MW	Malawi
MY	Malaysia
MV	Maldives
ML	Mali
MT	Malta
MH	Marshall Islands
MQ	Martinique
MR	Mauritania
MU	Mauritius
YT	Mayotte
MX	Mexico
FM	Micronesia
MC	Monaco
MD	Moldova
MA	Morocco
MN	Mongolia
MS	Montserrat
MZ	Mozambique
MM	Myanmar
NA	Namibia
NR	Nauru
NP	Nepal
NL	Netherlands
AN	Netherlands Antilles
NT	Neutral Zone
NC	New Caledonia
NZ	New Zealand (Aotearoa)
NI	Nicaragua
NE	Niger
NG	Nigeria

Name	Value
NU	Niue
NF	Norfolk Island
MP	Northern Mariana Islands
NO	Norway
OM	Oman
PK	Pakistan
PW	Palau
PS	Palestinian Territory, Occupied
PA	Panama
PG	Papua New Guinea
PY	Paraguay
PE	Peru
PH	Philippines
PN	Pitcairn
PL	Poland
PT	Portugal
PR	Puerto Rico
QA	Qatar
RE	Reunion
RO	Romania
RU	Russian Federation
RW	Rwanda
GS	S. Georgia and S. Sandwich Isls.
KN	Saint Kitts and Nevis
LC	Saint Lucia
VC	Saint Vincent and the Grenadines
WS	Samoa
SM	San Marino
ST	Sao Tome and Principe
SA	Saudi Arabia
SN	Senegal
YU	Serbia and Montenegro
SC	Seychelles
SL	Sierra Leone
SG	Singapore
SI	Slovenia

Name	Value
SK	Slovak Republic
SB	Solomon Islands
SO	Somalia
ZA	South Africa
ES	Spain
LK	Sri Lanka
SH	St. Helena
PM	St. Pierre and Miquelon
SD	Sudan
SR	Suriname
SJ	Svalbard and Jan Mayen Islands
SZ	Swaziland
SE	Sweden
CH	Switzerland
SY	Syria
TW	Taiwan
TJ	Tajikistan
TZ	Tanzania
TH	Thailand
TG	Togo
TK	Tokelau
TO	Tonga
TT	Trinidad and Tobago
TN	Tunisia
TR	Turkey
TM	Turkmenistan
TC	Turks and Caicos Islands
TV	Tuvalu
UG	Uganda
UA	Ukraine
AE	United Arab Emirates
UK	United Kingdom
US	United States
UM	US Minor Outlying Islands
UY	Uruguay
SU	USSR (former)

Name	Value
UZ	Uzbekistan
VU	Vanuatu
VA	Vatican City State (Holy See)
VE	Venezuela
VN	Viet Nam
VG	British Virgin Islands
VI	Virgin Islands (U.S.)
WF	Wallis and Futuna Islands
EH	Western Sahara
YE	Yemen
ZM	Zambia
ZR	Zaire
ZW	Zimbabwe

11.3.5.1 How to perform Automatic Resource creation via User Template

This procedure describes how to create automatically the UM User’s resources upon successful creation of UM Users via LDAP, using the predefined User Templates.

Prerequisites

Adequate administrative permission that allows User Management and Provisioning.

Step by Step

1) Navigate to **User Management** > **Provisioning** > **LDAP**.
   A list of the existing LDAP Attribute Mappings is displayed, sorted per column **UM**.
2) Select the **User Template** from the **User attribute** drop-down list.

3) Select to map the User Template to one of the fallowing options:

- **LDAP Attribute**

  Choose the **LDAP Attribute** from the drop-down list and then select one of the available values (for more information, see How to retrieve the available LDAP Attributes).
- **New LDAP Attribute**

  Define a new LDAP attribute that will be mapped to the User Template.
- **Constant Value**

  Choose the **Constant Value** from the drop-down list and then select one of the available values (see Step 6 of How to perform LDAP Attribute Mappings).

> **NOTICE:**
>
> In case of Constant value, the available User Temples are the ones defined in the system, in the specific domain.
>
> If no Constant values have been specified for the User Template, system displays an empty drop-down list and does not allow adding mappings.

4) Click **Add** to map the User Template to the specified LDAP attribute.

> **NOTICE:** In case the **User Template** has been already mapped, system updates this **User Template** with the newly specified **LDAP Attribute**.

The new mapping for User Templates will appear within the list of the existing LDAP Attribute Mappings.

5) Initiate either Scheduled (see How to perform LDAP Scheduled Synchronization), or Manual LDAP Synchronization (Chapter: How to perform LDAP Manual Synchronization).

System:

a)
- creates the new UM Users from the LDAP directory
- applies the User Template to the newly created UM Users

> **IMPORTANT:** The following Resource types are supported for the automatic resource creation: OpenScape Voice resource, OpenScape Xpressions and OpenScape UC Application resource.

> **IMPORTANT:** In case where User Template with the LDAP attributes mapping is selected, the system will use this mapping defined in the User Template to create resources for the synchronized Users.

- prepares a log file with the details of the synchronization procedure and automatic resource creation operation.

- If selected User Template or UM User's Locality does not exist in the system:
  - System will not create the UM Users.
  - System will report this error in the log file.
- If valid User Template is selected, but no mapping for the Locality attribute is defined:
  - System creates the UM User and attempts to create the resources using the default values for the resource specific attributes, defined in the Default Locality.

The new UM Users have been created by performing Scheduled or Manual LDAP Synchronization and the Resources haven been automatically assigned to these Users via User Templates.

11.3.6 How to perform Advanced Attribute Mapping

This Chapter describes how to define additional, Advanced mappings using string manipulation functions and allow assignment of more than one LDAP attribute to the UM User attribute.

Prerequisites

Adequate administrative permission that allows User Management and Provisioning in each domain that user wants to administer.

The LDAP connection is enabled.

Advanced Attribute Mappings must conform to the Expression Language (EL) syntax.

Step by Step

1) Navigate to **User Management** > **Provisioning** > **LDAP**.
A list of the existing LDAP Attribute Mappings is displayed, sorted per column **UM**.

2) Click **Advanced...** to define the Advanced Mappings rules.

A pop-up window **Advanced Mapping** is displayed.

3) Select one of the available values from the **User Attribute** drop-down list (see the Table: UM User attributes).

The User Attributes are sorted by name.

NOTICE:

If selected User attribute has been already mapped to the expression using Advanced Mapping, Constant mapping (Constant value) or Direct mapping (LDAP attribute), Mapped LDAP attribute will appear in the **Expression**

section of the **Advanced Mapping** screen and it will be available for the modification.

System retrieves the LDAP attributes of the specified LDAP directory.

4) Choose one of the available LDAP Attributes from the **LDAP Attribute** list.

Select button, located under **LDAP Attribute** list, is active now.

5) Click **Select**.

Selected LDAP attribute appears within the **Expression** text area.

6) Click **Value Mapping** to create and insert the conditional values for the attribute mappings (for more information refer to How to perform Value Mapping).

A new Value Mapping appears within the **Expression** text area.

7) Select one of the available values from the **Functions** list.

Select button, located under **Functions** list, is active now.

8) Click **Select** to insert the supported string manipulation function with proper syntax.

Selected Function appears within the **Expression** text area.

9) Check the **Expression** for syntax errors.
System:

a)
- generates the expression based on the provided data.
- populates the **Testing LDAP attributes** text area with all LDAP attributes that have been used in the **Expression**.

10) Add (modify) the values for the LDAP attributes, located in the **Testing LDAP attributes** text area, in order to validate the expression.

11) Click **Test** to evaluate the expression.
System:

a)
- evaluates the expression using the specified values for the LDAP attributes
- displays the result in the **Result** text area.

NOTICE:

If EL expression contains syntax errors, system displays the warning message and returns to the **Advanced Mapping** screen.

12) Click **Save** to map the expression to the selected User attribute.

A new mapping has been added in the LDAP Attributes Mapping list, where column **LDAP** contains the Advanced Mapping function and column **Mapping Direction** indicates the direction of the LDAP mapping (UM to LDAP or LDAP to UM).

Concat (concatenation) function

The selected User Attribute is mapped to LDAP attribute 'sAMAccountName' with a concatenation of @DE.GEIS-GROUP.NET value:

```
sAMAccountName.concat('@DE.GEIS-GROUP.NET')
```

or the selected User Attribute is mapped to the constant value 'GEIS-DE/' which is concatenated with the LDAP attribute 'sAMAccountName', by converting all characters to upper-case.

```
('GEIS-DE/').concat(sAMAccountName.toUpperCase()).
```

Next steps

In order to modify an Advanced Mapping in the row of the mapping, click on to open application action menu and then select **Edit**.

11.3.6.1 How to perform Value Mapping

The Value Mappings feature can be considered as a supplement to the Advanced Attribute Mapping that helps automatically generating expressions based on the predefined conditions.

Prerequisites

Adequate administrative permission that allows User Management and Provisioning in each domain that user wants to administer.

The LDAP connection is enabled.

Advanced Attribute Mappings must conform to the Expression Language (EL) syntax.

Step by Step

1) Navigate to **User Management** > **Provisioning** > **LDAP**.
   A list of the existing LDAP Attribute Mappings is displayed sorted per column **UM**.
2) Click **Advanced...** to define the Advanced Mappings rules.

   A pop-up window **Advanced Mapping** is displayed.
3) Select one of the available values from the **User Attribute** drop-down list (see the Table: UM User attributes).

   System retrieves the LDAP attributes of the specified LDAP directory.
4) Choose one of the available LDAP Attributes from the **LDAP Attribute** list.

   Value Mapping button, located under **LDAP Attribute** list, is active now.
5) Click **Value Mapping** to create the conditional values for the attribute mappings.

   A pop-up window **Value Mapping** is displayed.
6) Fill in the **Default Value** for previously selected LDAP attribute.

NOTICE:

The LDAP attribute will take the Default Value only if the LDAP value is not found in the Value Mapping list.

---

7) Create the rule for LDAP attribute which will look like:

`Value <`**value**`> maps to <`**Alternative LDAP value**`>`.

NOTICE:

The above rule will have the meaning similar to IF_THEN_ELSE clause. In other words, IF the <**value**> is found in the Vale Mapping list, THEN <**Alternative LDAP value**> will be assigned to the LDAP attribute; ELSE < **Default Value** > will be assign to the LDAP attribute.

---

8) Click **Add**.

A new attribute mapping has been added in the Value Mapping list.

9) Click **OK**.
System:

a) • generates the expression based on the provided data.

• populates the **Testing LDAP attributes** text area with the LDAP attributes that have been used in the **Expression**.

A new Vale mapping has been declared for the LDAP attribute.

The selected user attribute (eg Home Time Zone) is mapped to specific value depending on the content of LDAP attribute 'c'. A default value (WET) is set in case the expected content is not found in 'c' LDAP attribute

```
(c.equals('DE'))?'Europe/Berlin':
(c.equals('FR'))?'Europe/Paris':
(c.equals('US'))?'US/Eastern':'WET'
```

and the corresponding value mapping with LDAP attribute 'l' and default value: "Zeven"

```
(l.equals('Wittenburg'))?'Wittenburg':
(l.equals('Kodak'))?'Kodak':
(l.equals('Bondoufle'))?'Bondoufle':
(l.equals('Zeven'))?'Zeven':'Zeven'
```

11.3.7 Partial LDAP synchronization

The LDAP synchronization in OpenScape User Management has been enhanced to support the Partial synchronization of the LDAP Users.

This can be achieved in two different, but not mutually exclusive ways:

- by defining a filter on the LDAP source base.

  The following filters are provided:

  – simple LDAP filter
  – advanced LDAP filter

- by synchronizing data only for the existing UM Users that have been imported with a method other than LDAP synchronization.

If an LDAP synchronization has been performed at least once in the past on the system, a warning is displayed in order to notify the user that a full synchronization will be needed after the modification of the LDAP filter or the LDAP connection.

NOTICE:

The following warning message appears:

"A modification in the existing LDAP filter was detected.

Please, perform a full LDAP synchronization in order to avoid inconsistencies."

11.3.7.1 How to define a Simple LDAP filter

Specifying a Simple filter which retrieves a subset of the LDAP Users that belong to the specified source base, allows an administrator to control the number of UM Users that will be created.

Prerequisites

Adequate administrative permission that allows User Management and Provisioning in each domain that user wants to administer.

Step by Step

1) Navigate to **User Management** > **Provisioning** > **LDAP**.
Filter... button is active.
2) Click **Filter...** to define a filter for the specified source base.

   A pop-up window **LDAP Filter** is displayed.
3) Navigate to the **Filter Definition** area and select **Define the filter using a list of conditions** in order to specify a Simple LDAP filter for the specified source base.

   NOTICE:

   Perform the following steps for all the LDAP attributes that are required to define the filter.

   a) From the first drop-down list select an **LDAP attribute**.

   NOTICE:

   The list of LDAP attributes always includes a “hard-coded” attribute called "*objectClass*".

   b) From the second drop-down list select the **filter operation.**

   Possible values for the filter operations are:

   - – equals
   - – not equals

- starts with
- ends with
- does not start with
- does not end with
- grater or equal
- less or equal
- is present
- is not present
- contains
- does not contain.

c) Specify the value for the filter.

NOTICE:

The following filter operations do not need require the values: **is present** and **is not present**.

d) Click **Add** to add the operation to the filter.

The LDAP attributes in the criteria list are displayed in alphabetical ascending order.

NOTICE:

In case the LDAP attribute is already defined in the filter, system adds the same attribute again, by performing logical OR operation.

A new Simple LDAP filter has been specified and its representation is dynamically updated by the system in the **LDAP filter expression** field.

Next steps

Use Simple filters to construct the common expressions.

In case you want to further refine Simple filter in order to create an Advance filter, use the representation of the Simple filter (i.e., **LDAP filter expression** area) and fine tune it.

11.3.7.2 How to define an Advanced LDAP filter

In case the subset of the LDAP Users that belong to the specified source base can not be defined with the Simple filter, you have the opportunity to specify an Advanced filter and control the number of UM Users that will be created.

Prerequisites

Adequate administrative permission that allows User Management and Provisioning in each domain that user wants to administer.

Step by Step

1) Navigate to **User Management** > **Provisioning** > **LDAP**.
Filter... button is active.

2) Click **Filter...** to define a filter for the specified source base.

   A pop-up window **LDAP Filter** is displayed.

3) Navigate to the **Filter Definition** area and select **Define the filter manually** in order to specify an Advanced LDAP filter for the specified source base.

4) Within the **LDAP filter expression** field enter the filter in LDAP filter format (i.e., RFC 2254).

5) Click **Save** to save the Advanced filter.

   The system validates the specified filter against the LDAP filter format and in case it is valid, stores the filter.

> **NOTICE:**
>
> If the specified filter is not valid, the system displays the error message, so that you can modify (correct) the filter.

A new Advanced LDAP filter has been specified.

Next steps

In case you want to modify previously specified advanced LDAP filter, go to the representation of the Advanced filter (i.e., **LDAP filter expression** area) and fine tune it.

11.3.7.3 How to switch from Advanced to Simple LDAP filter

The following steps describe how to modify an Advanced LDAP filter and instead of specifying it manually, specify it using the conditions list.

Prerequisites

Adequate administrative permission that allows User Management and Provisioning in each domain that user wants to administer.

An Advanced filter has already been configured for the LDAP connection.

Step by Step

1) Navigate to **User Management** > **Provisioning** > **LDAP**.
   Filter... button is active.

2) Click **Filter...** to modify an Advanced filter for the specified source base.

   A pop-up window **LDAP Filter** is displayed.

3) Navigate to the **Filter Definition** area.

> **NOTICE:**
>
> The Simple filter view (i.e., the option **Define the filter using a list of conditions**) has been disabled, whereas the Advanced filter option (i.e.,**Define the filter manually**) has been enabled by the system.

4) Enable the Simple filter by select the option **Define the filter using a list of conditions**.

   The system warns you that you have slected to specify the filter using the conditions list and because of that, the advanced filter which you have specified before will be overwritten with the filter produced from the list of conditions.

5) To continue specifying the filter using the conditions list. click **OK**.

   The System...

   a) ... overwrites the Advanced filter with the filter that has just been produced from the list of conditions
   b) ... enables the Simple filter view
   c) ... disables the Advanced filter view.

   NOTICE:

   In case where the Advanced filter is the same as the filter that will be produced from the list of conditions., the system does not display any warnings, but it enables the Simple filter view and disables the Advanced filter view.

6) To decline specifying the filter using the conditions list click **Cancel**.

   The System stays in Advanced filter view and does not change to the Simple filter view.

11.3.8 LDAP Scheduled Synchronization

A list of all LDAP synchronization Schedules configured in the selected domain appears in the work area.

LDAP synchronization Schedules are used to schedule (automatic) Synchronization of the LDAP Directory with the UM Users.

The list of LDAP synchronization represents the active scheduled LDAP synchronizations. Each schedule entry provides the following information:

- **Schedule Name**

  Name of the LDAP synchronization schedule.
- **Reoccurs**

  Setting showing when and how often the schedule is repeated.
- **Day (for weekly LDAP synchronization only)**

  Day of LDAP synchronization schedule.
- **Time**

  Time of LDAP synchronization schedule.
- **Remaining occurrences**

  Shows how the LDAP synchronization schedule is repeated.

To display the content of an LDAP synchronization schedule, select the checkbox that associates the relevant schedule and click on **Edit** button.

To remove a LDAP synchronization schedule, select the checkbox that associates the relevant schedule and click on **Delete** button.

Click on **Close** to close the window.

NOTICE:

All existing LDAP synchronization schedules are active. In order to deactivate an LDAP synchronization schedule, the administrator should delete it from the list.

NOTICE:

In case of upgrade to V9, the pre-existing LDAP synchronization schedule (i.e., the LDAP synchronization schedule that has already been created in the older versions) will be automatically configured to have the value LDAP_SYNCHRONIZATION_{domain}

(e.g. system) for the Schedule Name.

One needs to open and save the LDAP synchronization schedule form with this configured name LDAP_SYNCHRONIZATION_{domain}

(e.g. system) ,in order the button "Download" to become available after the execution of the scheduled LDAP synchronization.

11.3.8.1 How to setup LDAP Scheduled Synchronization

This Chapter describes How to configure parameters for Scheduled (automatic) Synchronization of the LDAP Directory with the UM Users.

Prerequisites

Adequate administrative permission that allows User Management and Provisioning.

The LDAP Directory connection has been enabled and properly configured (see How to Setup LDAP Connection).

The mapping between mandatory UM User's attributes and LDAP attributes have been configured (see How to perform LDAP Attribute Mappings).

Step by Step

1) Navigate to **User Management** > **Provisioning** > **LDAP**. **Schedules...** button is active.
2) Click **Schedules...** to list the existing LDAP synchronization Schedules.
3) Click **Add...** to configure the parameters of the new LDAP synchronization schedule.

   A pop-up window **Schedule synchronization between LDAP and CMP** is displayed.

   NOTICE:

   To display/modify the content of a LDAP synchronization schedule, select the checkbox that associates the relevant schedule and click on **Edit…** button

4) Navigate to the **Configuration** area to specify the details related to the scheduled synchronization and control if during the synchronization the new entries will be created in OS UM or not.

a) go to the **Create** area to define the cases where a new user is added to the LDAP directory

- – to specify that during the LDAP synchronization the new UM Users will be created from the new LDAP entries and the existing Users will be updated, select **create a new user in User Management**
- – to specify that during the LDAP synchronization the existing UM Users will be updated to the LDAP data, but no new UM Users will be created from the new LDAP entries, select **do not create a new user in User Management**

In both cases, the system:

a)
- retrieves and parses the retrieved LDAP data
- for each LDAP User, system uses the LDAP mappings to determine the LDAP attribute that is mapped to the **userID** UM User attribute
- verifies that a UM User with **userID** equal to the value of the mapped attribute exists
- updates the UM User's attributes according to the Create operation mode.

NOTICE:

If no UM User with the specified **userID** exists:

- in the first case the system creates a new UM User and updates all the attributes that have a mapping defined

- in the second case, the system does not create a new UM User.

---

b) go to the **Update** area to define the cases where for a mapped user attribute there are no data in the LDAP directory

- – to specify that during the LDAP synchronization the mapped user attributes will not be updated if the corresponding LDAP attribute do not contain any data, select **do not modify the user data of the user attribute in User Management**
- – to specify that during the LDAP synchronization the mapped user attributes will be cleared if the corresponding LDAP attribute do not

contain any data, select **modify and clear the data of the user attribute in User Management**

In both cases, the system:

a)
- retrieves and parses the retrieved LDAP data
- for each LDAP User, the system uses the LDAP mappings to determine user attributes that are mapped to LDAP attributes
- verifies that the LDAP attribute data are not empty
- updates the UM User's attributes according with the LDAP data.

NOTICE:

If the LDAP attribute does not contain any data:

- in the first case, the system does not update the user attribute

- in the second case the system does update the user attribute and clear any data stored in User Management

---

c) go to the **Update** area to define how to handle the Resources that are already assigned to a User but are not defined in the User Template.

Selected one of the following options:

a)
- **associate the User with the User Template without affecting the additional resources**

  (resources that were previously manually assigned to a User or applied with a different User Template will stay intact)
- **un-assign the additional resources**

  (resources that were previously manually assigned to a User or applied with a different User Template will be unassigned)
- **un-assign and delete the additional resources**

  (resources that were previously manually assigned to a User or applied with a different User Template will be unassigned and deleted).
- **un-assign phones and delete other resources**

  Un-assign resources of specific type and delete resources of other types

  (resources that were previously manually assigned to a User or applied with a different User Template will be unassigned and deleted).

Select the **With or without User Template LDAP mapping existing, apply the already associated User Template to the UM User** checkbox in case you want the existing association of the User Template to have priority over the LDAP mapping.

NOTICE:

When a User Template with Xpressions Resources is applied to a User and a modification in the User Template takes place where only the User ID field in the User

Template has been changed, then the **un-assign and delete the additional resources** rule is only applied, even if any other choice has been selected.

d) go to the **Delete** area and in order to delete the UM Users that have been deleted from the LDAP directory during scheduled LDAP synchronization, check the option **Delete Users during synchronization**.

The following options are provided regarding the resources that are assigned to the Users that have to be deleted:

- – to unassign any resources assigned to the deleted User, select the option **Unassign Resources**
  – to unassign and delete any resources assigned to the deleted User, select the option **Delete and Unassign Resources**
  – to unassign phones and delete other resources assigned to the deleted User, select the option **Unassign phones and delete other resources**

To specify a threshold value that will disable automatic deletion if the number of deleted Users exceeds the specified threshold, check the option **Enable threshold for User deletion during synchronization** and select one of the following:

- – **Do not delete users if more than X Users will be deleted.**

  X represents the absolute number of Users.
  – **Do not delete users if more than X % of the Users will be deleted.**

  X represent percentage of the number of User.

e) go to the **Delta Synchronization** area and in order to enable the Delta LDAP synchronization, check the option **Enable Delta LDAP synchronization based on latest LDAP synchronization and modifyTimestamp LDAP attribute**.

This option uses the modifyTimestamp LDAP attribute of each LDAP user in order to filter the users to be synchronized, comparing it against:

- "Either the last LDAP synchronization,
- "Or a customer-specific time stamp provided by the administrator.

The Timestamp for Delta LDAP synchronization information is in the form of: **<date> <month> <year> <time_hour>:<time_minutes> <time_seconds> <PM/AM>.**

For the unique case that the feature is installed and no LDAP synchronization has taken place prior to the first time configuration of the feature, these fields contain the current time. This means that the administrator should modify these fields and apply a known timestamp that would be as close as possible to the last known synchronization.

In all other cases (synchronization, delta or full, has taken place), these fields are automatically populated and contain the **start time** of the last successful LDAP synchronization. Nevertheless, it is still possible for the administrator to modify those values.

NOTICE: The deletion of UM LDAP users during Delta LDAP synchronization is triggered when amongst the deletion of user(s) in LDAP, also creation or modification

in LDAP has been performed to any of the LDAP user(s) that had already been synchronized to UM.

5) Navigate to the **Schedule** area to define the following:

a) **Schedule Name**

This is a mandatory and unique field that represents the name of the LDAP synchronization Schedule Name.

NOTICE:

Only [A-Za-z_][A-Za-z0-9_-]* characters are allowed in the "Schedule Name" field.

b) **Frequency**

The drop -down list contains the following values: **Weekly/ Daily/15min/30min/1 hour/2 hours/4 hours/8 hours/12 hours**.

c) **Synchronize on**

The information is in the form of: **<time_hour>:<time_minutes> <PM/ AM> < Week day>**.

d) **Occurrences**

The drop -down list contains the following values: **infinitely/finite number of times <number>**.

NOTICE: Information area displays he time when the last synchronization has occurred, or "not available" if that information is not available.

6) To commit the changes made to the Scheduled Synchronization parameters, Click **Save**.

NOTICE:

In multitenant deployments the bulk operations should be allowed to run concurrently across domains. Consequently, it is possible to perform the bulk operations simultaneously in different domains, but it is not allowed to perform them simultaneously within the same domain.

NOTICE:

In case the LDAP synchronization (either manual or scheduled) is running in the domain at the time that the scheduled synchronization starts, a fault will be fired with an

appropriate rule, to both raise an alarm in CMP and send out an SNMP trap.

System:

a)
- checks the threshold before attempting to delete the Users
- verifies that supplied information is correct
- creates and stores the new LDAP synchronization schedule.

A new LDAP synchronization schedule has been created and it is displayed in the list of the existing LDAP synchronization Schedules.

IMPORTANT:

System provides a "sanity check" mechanism to prevent accidental deletion of Users in exception scenarios (for example, in the case the connection to the LDAP directory has problems or the LDAP if offline).

If the number of Users missing from the LDAP directory is more than the threshold value, the system will not attempt to delete any User, but instead it will fire a fault with an appropriate rule to both, raise an alarm in the CMP and to send out an SNMP trap.

The following User Management - LDAP Synchronization generated alarms will be raised: "User Management - LDAP Synchronization Completed Successfully" alarm, "User Management - LDAP Synchronization Unsuccessfully" alarm and "User Management - LDAP Synchronization User Deletion Threshold Reached" alarm (for more information, see the CMP Appendix for the Alarms).

System also re-applies the User Template to each User that has a User Template mapping.

NOTICE:

The following alternative scenarios are possible when applying the User Templates during LDAP synchronization:

- if the LDAP mapping resolves to a User Template different than the one associated with the User, the system will apply the new User Template to the User

- if the LDAP mapping resolves to an empty string, the system dissociates the User from the User Template

- if the LDAP mapping resolves to a non existing template, the system logs an LDAP synchronization error.

7) Navigate to **Report** area and click **Download** to download a log file with the details of the latest scheduled synchronization of the specific Schedule.

NOTICE:

Log files are stored on the server, under the following

path:

- **for integrated Simplex =** `/log/OSCUM/`

- **for all other deployments =** `/var/siemens/common/log/OSCUM/`

NOTICE:

The Report Area is only available when the LDAP synchronization schedule is edited.

The new UM Users have been created by performing Scheduled Synchronization with the LDAP directory.

NOTICE:

In order to view the imported data, the UM Users list needs to be explicitly accessed (navigate to the **Users&Resources** screen and refresh it, so that you see the new UM Users).

The UM Users created via LDAP synchronization are displayed with a different icon within the UM Users list.

The photo (JPEG format; up to 16384 bytes in size) of the UM User has been retrieved from the LDAP directory and stored in the **Photo** field (**General** tab) of the UM User. In case more than one photo is assigned to an LDAP user, the first one will be retrieved and stored as a photo for the UM User.

11.3.9 How to perform LDAP Manual Synchronization

This Chapter describes the Manual Synchronization of the UM Users with the LDAP Directory data.

Prerequisites

Adequate administrative permission that allows User Management and Provisioning.

The LDAP Directory connection has been enabled and properly configured (see How to Setup LDAP Connection).

The mapping between mandatory Users' attributes and LDAP attributes have been configured (see How to perform LDAP Attribute Mappings).

IMPORTANT:

There can be only one instance of the manual synchronization process per CMP domain.

Step by Step

1) Navigate to **User Management** > **Provisioning** > **LDAP**.
Synchronize Now... button is active.
2) Click **Synchronize Now...** to manually synchronize the LDAP Directory User data with the UM Users.

   A pop-up window **Manually Synchronize LDAP** is displayed.
3) Navigate to the **Configuration** area to specify the behavior of the Create/ Update/Delete operations during manual synchronization (i.e., if the new entries will be created in OS UM or not; how the existing entries will be modified and if the entries are going to be deleted).
   a) Navigate to the **Create** area to define the cases where a new user is added to the LDAP directory
      - – to specify that during the LDAP synchronization the new UM Users will be created from the new LDAP entries and the existing Users will be updated, select **create a new user in User Management**
      - – to specify that during the LDAP synchronization the existing UM Users will be updated to the LDAP data, but no new UM Users will be created from the new LDAP entries, select **do not create a new user in User Management**

      In both cases, the system:

      a)
      - retrieves and parses the retrieved LDAP data
      - for each LDAP User, system uses the LDAP mappings to determine the LDAP attribute that is mapped to the **userID** UM User attribute
      - verifies that a UM User with **userID** equal to the value of the mapped attribute exists
      - updates the UM User's attributes according to the Create operation mode.

      NOTICE:

      If no UM User with the specified **userID** exists:

      - in the first case the system creates a new UM User and updates all the attributes that have a mapping defined

      - in the second case, the system does not create a new UM User.

   b) Navigate to the **Update** area to define the cases, where no data exists for a mapped user attribute in the LDAP directory
      - – to specify that during the LDAP synchronization the mapped user attributes will not be updated if the corresponding LDAP attribute do not contain any data, select **do not modify the user data of the user attribute in User Management**
      - – to specify that during the LDAP synchronization the mapped user attributes will be cleared if the corresponding LDAP attribute do not

contain any data, select **modify and clear the data of the user attribute in User Management**

In both cases, the system:

a)
- retrieves and parses the retrieved LDAP data
- for each LDAP User, the system uses the LDAP mappings to determine user attributes that are mapped to LDAP attributes
- verifies that the LDAP attribute data are not empty
- updates the UM User's attributes according with the LDAP data.

NOTICE:

If the LDAP attribute does not contain any data:

- in the first case, the system does not update the user attribute

- in the second case the system does update the user attribute and clear any data stored in User Management

---

c) Navigate to the **Update** area to define how to handle the Resources that are already assigned to a User but are not defined in the User Template.

Select one of the following options:

a)
- **associate the User with the User Template without affecting the additional resources**

  (resources that were previously manually assigned to a User or applied with a different User Template will stay intact)
- **un-assign the additional resources**

  (resources that were previously manually assigned to a User or applied with a different User Template will be unassigned)
- **un-assign and delete the additional resources**

  (resources that were previously manually assigned to a User or applied with a different User Template will be unassigned and deleted).
- **un-assign phones and delete other resources**

  Un-assign resources of specific type and delete resources of other types

  (resources that were previously manually assigned to a User or applied with a different User Template will be unassigned and deleted).

Select the **With or without User Template LDAP mapping existing, apply the already associated User Template to the UM User** checkbox in case you want the existing association of the User Template to have priority over the LDAP mapping.

NOTICE:

When a User Template with Xpressions Resources is applied to a User and a modification in the User Template takes place where only the User ID field in the User

Template has been changed, then the **un-assign and delete the additional resources** rule is only applied, even if any other choice has been selected.

d) Navigate to the **Delete** area and in order to delete the UM Users that have been deleted from the LDAP directory during manual LDAP synchronization, check the option **When a user is deleted from the LDAP directory, delete from User Management as well**.

The following options are provided regarding the resources that are assigned to the Users that have to be deleted:

- – to unassign any resources assigned to the deleted User, select the option **Unassign Resources**
- – to unassign and delete any resources assigned to the deleted User, celect the option **Delete and Unassign Resources**
- – to unassign phones and delete other resources assigned to the deleted User, select the option **Unassign phones and delete other resources**

e) Navigate to the **Organizational Structures** area. Set the following options, when the attributes of the user's organizational structures will be modified:

- – **Update User's Organizational Structure**: Modifies the user's organizational structure
- – **Update current Organizational Structure for all Users**: This option updates the current Organizational Structure for the users that previously had the same organizational structure assigned.

f) Navigate to the **Delta Synchronization** area and in order to enable the Delta LDAP synchronization, check the option **Enable Delta LDAP synchronization based on latest LDAP synchronization and modifyTimestamp LDAP attribute**.

This option uses the modifyTimestamp LDAP attribute of each LDAP user in order to filter the users to be synchronized, comparing it against:

- Either the last LDAP synchronization,
- Or a customer-specific time stamp provided by the administrator.

The Timestamp for Delta LDAP synchronization information is in the form of: **<date> <month> <year> <time_hour>:<time_minutes> <time_seconds> <PM/AM>.**

For the unique case that the feature is installed and no LDAP synchronization has taken place prior to the first time configuration of the feature, these fields contain the current time. This means that the administrator should modify these fields and apply a known timestamp that would be as close as possible to the last known synchronization.

In all other cases (synchronization, delta or full, has taken place), these fields are automatically populated and contain the **start time** of the last successful LDAP synchronization. Nevertheless, it is still possible for the administrator to modify those values.

NOTICE: The deletion of UM LDAP users during Delta LDAP synchronization is triggered when amongst the deletion of user(s) in LDAP, also creation or modification

in LDAP has been performed to any of the LDAP user(s) that had already been synchronized to UM.

4) Navigate to the **Control** area to perform the following actions:

a) to calculate the number Users that are going to be deleted, click **Calculate**

Once calculation finishes and the number of users is greater than zero, the **Download** button becomes available and and you can download a report file that containing the list of all the Users that are going to be deleted from the LDAP directory.

b) to simulate the synchronization and get better overview of the changes that will be done in the UM Users database, click the button **Simulate**

Once simulation starts, the system does the following:

a) • displays the LDAP synchronization progress bar (as if the actual synchronization is performed) with an indication in the title that the synchronization runs in simulation mode

• performs the synchronization without modifying any data in the UM Users database

• displays a report of the operations and provides a log file in CSV format for downloading. (The log file contains the following information: dn (LDAP User identifier), User ID (resulting UM User identifier based on the specified mappings), Lastname (resulting UM Lastname based on the specified mappings), Display name (resulting UM Display name based on the specified mappings), UM operation (Create/Update/Delete).

c) to start the synchronization, click **Start**.

NOTICE:

In multitenant deployments the bulk operations should be allowed to run concurrently across domains. Consequently, it is possible to perform the bulk operations simultaneously in different domains, but it is not allowed to perform them simultaneously within the same domain.

NOTICE:

In case the LDAP synchronization (either manual or scheduled) is running in the domain at the time that the scheduled synchronization starts, a fault will be fired with

an appropriate rule, to both raise an alarm in CMP and send out an SNMP trap.

System:

a)
- initiates the synchronization procedure
- displays the current operation (create/modify/delete UM User)
- displays a progress bar of the synchronization process progress
- displays an overview of the results of the operations performed at each time (success or failures)
- prepares a log file with the details of the synchronization procedure
- re-applies the User Template to each User that has a User Template mapping

NOTICE:

The following alternative scenarios are possible when applying the User Templates during LDAP synchronization:

- if the LDAP mapping resolves to a User Template different than the one associated with the User, the system will apply the new User Template to the User

- if the LDAP mapping resolves to an empty string, the system dissociates the User from the User Template

- if the LDAP mapping resolves to a non existing template, the system logs an LDAP synchronization error.

- If the synchronization process cancels:
  - the operation is cancelled after the operation on the current User is completed (i.e. User/Resource creation/modification)
  - the modifications made up to the point when the operation was cancelled are committed. There is no roll-back functionality.

NOTICE:

In case the progress dialog is closed and the manual synchronization is selected again, system shall display the progress of the current ongoing operation.

5) Navigate to **Report** area and click **Download** to download a log file with the details of the latest synchronization.

NOTICE:

Log files are stored on the server, under the following

path:

- **for integrated Simplex =** `/log/OSCUM/`

- **for all other deployments =** `/var/siemens/common/log/OSCUM/`

The new UM Users have been created by performing Manual Synchronization with the LDAP directory.

NOTICE:

In order to view the imported data, the UM Users list needs to be explicitly accessed (navigate to the **Users&Resources** screen and refresh it, so that you see the new UM Users).

The UM Users created via LDAP synchronization are displayed with a different icon within the UM Users list.

The photo (JPEG format; up to 16384 bytes in size) of the UM User has been retrieved from the LDAP directory and stored in the **Photo** field (**General** tab) of the UM User. In case more than one photo is assigned to an LDAP user, the first one will be retrieved and stored as a photo for the UM User.

11.3.10 How to delete the LDAP Attribute Mapping

The following paragraphs describe how to delete LDAP Attribute Mapping.

Prerequisites

Adequate administrative permission that allows User Management and Provisioning.

Step by Step

1) Navigate to **User Management** > **Provisioning** > **LDAP**.
   A list of the existing LDAP Attribute Mappings is displayed sorted per column **UM**.
2) Check the box in front of the attribute mapping that needs to be deleted.

   Button **Delete** is active now.

3) Click **Delete** to remove the mapping between two attributes.

   The deleted attribute mapping is removed from the mapped attributes list.

   - **If** the mapping selected for removal includes the mandatory **User attribute**, system will:
     – remove the mapping of this attribute, but does not remove the **User attribute** from the mapped attributes list.
     – display the following information message:

       `< User_attribute_name> is mandatory and can not be deleted.`
     – enable the **User attribute** in the **User attribute** drop-down list.

The attribute mapping has been removed from the LDAP Attribute Mappings list.

11.4 How to Create UM Users based on the UC Accounts

This Chapter describes How to create automatically the UM Users using the existing UC Accounts.

Prerequisites

Adequate administrative permission that allows User Management and Provisioning.

Step by Step

1) Navigate to **User Management** > **Provisioning** > **Users from UC Accounts**.
2) Click **Users from UC Accounts** to create the UM Users based on the UC Accounts.

   A pop-up window **Create Users from UC accounts** is displayed.
3) Select one of the available values from the drop-down list to create the rules for the generation of missing information for the UM Users' mandatory fields (in this case, **Last name**).

   `From the UC account use the <`**Last name**`>, the part <`**after/ before**`> the delimiter <`**Delimiter**`>`

   - The <**Last name**> can get the following values:

Last name
Login Name (as is)
Login Name
Display Name

   - The <**Delimiter**> has one of the below values:

Delimiter
,
.

Delimiter
–
{space}
,{space}

NOTICE: When a **Delimiter** is specified, system uses all the characters before/after the delimiter to populate the respective field. In case the **Delimiter** is not found, the whole source field is used.

In case the existing UC account does not have a contact record, one of the following rules will be used to automatically generate the **Last name** of the UM User:

- – **Login Name (as is)** i.e. the complete **Login Name**.
  – first token of **Login Name**, after specifying appropriate **Delimiter**.
  – second token of **Login Name**, after specifying appropriate **Delimiter**.
  – first token of **Display Name**, after specifying appropriate **Delimiter**.
  – second token of **Display Name**, after specifying appropriate **Delimiter**.

4) Click **Start** to initiate the procedure of automatic creation of UM Users based on the UC accounts.

NOTICE:

In multitenant deployments the bulk operations should be allowed to run concurrently across domains. Consequently, it is possible to perform the bulk operations simultaneously in different domains, but it is not allowed to perform them simultaneously within the same domain.

The System...

- ... creates a new UM User for each UC account that is not already linked to an existing UM User.

NOTICE: The criterion for the creation of a UM User is the absence of the UM User profile in the UC account.

NOTICE: The creation of the UM User is performed by assigning the UM User profile to the UC Account and creating the related contact record, if required.

- ... displays the progress of the operation using a progress bar along with appropriate text.

a) **If** the procedure has already been initiated by a different administrator in the same domain:

- – System does not allow the execution of the procedure.
  – System informs that the operation is not possible because the procedure has already been started.

5) Click **Cancel** to stop an ongoing operation.

NOTICE: System does not rollback already created UM Users and it does not leave a UM User in an inconsistent state.

---

6) Depending on the operation outcome, a pop-up window with the following information is displayed:
   - – number of created UM Users:

     `<number> UM were created.`
   - – a list of UC Accounts for which the creation of the new UM Users was not possible:

     `Conversion failed for <number> UC accounts.`

7) System stores the information about the all operations performed during the latest import action in the log file.
8) Click **Download report** to download a log file with the details of the latest performed operation.

NOTICE:

Log files are stored on the server, under the following

path:

- **for integrated Simplex =** `/log/OSCUM/`

- **for all other deployments =** `/var/siemens/common/log/OSCUM/`

---

9) Click **Close** to close the **Create Users from UC accounts** pop-up window.

NOTICE:

In order to view the imported data, the UM Users list needs to be explicitly accessed. This means that after you close the **Create Users from UC accounts** pop-up, you need to navigate to the **Users&Resources** screen and refresh it, so that you see the new UM Users.

11.4.1 How to create UM Users from the existing UC Accounts on a new CMP installation

On a new CMP installation, system will propose to start the procedure of creating the UM Users from the existing UC Accounts.

Step by Step

1) The System:

a) ... verifies that the CMP Administrator has enabled the following permission of the CMP Application: **CMP** > **User Management** > **Provisioning** > **Users from UC Accounts**.

b) ... verifies that the startup window **Create Users from UC accounts** is enabled.

NOTICE:

The system-wide setting that enables/disables the pop-up of **Create Users from UC accounts** window, just after logging in, is available under the following menu: **Configuration** > **CMP** > **System Settings**.

This setting will not be displayed if the deployment does not include OpenScape UC Application.

---

c) ... checks that the UC Accounts not assigned to the UM Users exist in the system.

System displays the appropriate message at the startup window, that comes as a result of checking if there are some unassigned UC Accounts in the system.

NOTICE:

If no unassigned UC Accounts exist, the **Next** button is disabled.

---

2) Choose to:

- – Click **Next** to start immediately the procedure of creating the UM Users from the existing UC Accounts.
- – Click **Cancel** to dismiss the message, but display it again on the next login.

11.5 How to Create UM Users based on the OSV Subscribers

This Chapter describes How to automatically create the UM Users from existing OSV Subscribers.

Prerequisites

Adequate administrative permission that allows User Management and Provisioning.

Step by Step

1) Navigate to **User Management** > **Provisioning** > **Users from OSV Subscribers**.
2) Click **Users from OSV Subscribers** to create the UM Users based on the OSV Subscribers.

   A pop-up window **Create Users from OSV Subscribers** is displayed.
3) Select one of the available values from the drop-down list to create the rules for the generation of missing information for UM Users' mandatory fields (i.e., **User ID**, **Display Name**, **Last Name**, **Home Time Zone**, **Language**).

   - One of the following rules will be used to automatically generate the **User ID** for the UM User**:**

     `From OSV use` <**User ID**> <**way**> `the part` <**before/after**> `the delimiter` <**Delimiter**>.

     The following values are available for <**User ID**>, <**way**> and <**Delimiter**>:

User ID	way	Delimiter
Display Name	**as is** **as is, only replace space with a dot** **as is, only replace space with an underscore** **as is, only remove space**	
Directory Number	**as is, only without space & non numeric characters**	

     If duplicated logins are detected, the following rule will be used:

     `In case of duplicates` <**append an incremental number/ report as error (don't create)**>.

     – – where <**append an incremental number**> means to append a number to the **User ID** (i.e. JohnDoe, JohnDoe1, JohnDoe2 etc.)

     – <**report as error (don't create)**> means that the system will not create duplicate UM Users and it will report them as the errors.

     The rules to automatically generate the **User ID** for the UM User are:

     – – the complete **Directory Number as is, only without space & non numeric characters** (i.e. after removing any spaces and all non numeric characters).

     – the complete **Display Name** as is, or after replacing spaces on one of the above **ways**.

     – first token of **Display Name**, after specifying the appropriate **Delimiter**.

– second token of **Display Name**, after specifying the appropriate **Delimiter**.

- One of the following rules will be used to automatically generate the **Display Name** for the UM User**:**

  `From OSV use <`**Display Name**`> as is.`

  – – where **<Display Name>** can get the following values:

Display Name
Display Name
Directory Number

- One of the following rules will be used to automatically generate the **Last Name** for the UM User**:**

  `From OSV use <`**Last Name**`> <`**way**`> the part <`**before/after**`> the delimiter <`**Delimiter** `>`.

  The following values are available for **<Last Name>**, **<way>** and **<Delimiter>**:

Last Name	way	Delimiter
Display Name	**as is**	
Directory Number	**as is**	

– The rules to automatically generate the **Last Name** of the UM User are:

– – the complete **Directory Number** and **Display Name as is**.
– first token of **Display Name**, after specifying the appropriate **Delimiter**.
– second token of **Display Name**, after specifying the appropriate **Delimiter**.

- Specify the **Home Time Zone** (see the Table Home Time Zone values for constant mappings).
- Specify the **Language** (see the Table Language values for constant mapping).

4) Select one of the available values from the drop-down list to create the rules for the generation of missing information for the UM Users' optional fields (**Locality**, **First Name** and **Middle Name**).

NOTICE: The rules for the optional fields may remain undefined.

- From the drop-down list of all available Localities, choose the **Locality** for the UM User.

NOTICE:

Although the Locality is an optional field, it may be assigned to the users in order to have the attributes of

the resource in place, once it comes to the resource creation.

Be aware that during resource creation process, locality information will not be assigned to already created UM users (in general, during all bulk actions (e.g., editing of UM users) the address data remains unchanged).

In case the locality data of already created UM users has to be updated, go to the locality which has been created, select the option **Replace Address Data** and click **Save**. As a result, all related locality information will be applied to the previously created UM users that are associated with this locality.

- One of the following rules will be used to automatically generate the **First Name** for the UM User**:**

  `From OSV use` <**First Name**> <**way**> `the part` <**before/after**> `the delimiter` <**Delimiter**>.

  The following values are available for <**First Name**>, <**way**> and <**Delimiter**>:

First Name	way	Delimiter
Display Name	**as is**	
Directory Number	**as is**	

  The rules to automatically generate the **First Name** of the UM User are:

  – – the complete **Directory Number** and **Display Name as is**.
  – first token of **Display Name**, after specifying the appropriate **Delimiter**.
  – second token of **Display Name**, after specifying the appropriate **Delimiter**.

- One of the following rules will be used to automatically generate the **Middle Name** for the UM User**:**

  `From OSV use` <**Middle Name**> <**way**> `the part` <**before/after**> `the delimiter` <**Delimiter**>.

  The following values are available for <**Middle Name**>, <**way**> and <**Delimiter**>:

Middle Name	way	Delimiter
Display Name	**as is**	
Directory Number	**as is**	

  The rules to automatically generate the **Middle Name** of the UM User are:

  – – the complete **Directory Number** and **Display Name as is**.
  – first token of **Display Name**, after specifying the appropriate **Delimiter**.

– second token of **Display Name**, after specifying the appropriate **Delimiter**.

NOTICE: When **Delimiter** is specified, system uses all the characters before/after the delimiter to populate the respective field. In case the **Delimiter** is not found, the whole source field will be used.

5) Click **Start** to initiate the procedure of automatic creation of UM Users based on the OSV Subscribers.

NOTICE:

In multitenant deployments the bulk operations should be allowed to run concurrently across domains. Consequently, it is possible to perform the bulk operations simultaneously in different domains, but it is not allowed to perform them simultaneously within the same domain.

The System:

- – creates a new UM User for each OSV Subscriber that is not already linked to an existing UM User.

NOTICE: The criterion for the creation of a UM User is the absence of UM, or UC User with the specific OSV resource assigned.

NOTICE: The creation of the UM User is performed by creating the UM User using the specified rules and then assigning to this UM User the specific OSV resource.

NOTICE: The **Directory Number** (DN) as it is, will be used to generate the Business Phone 1.

a) In case the **Use Domain to Business Group Mapping** option is enabled, system creates UM Users for the subscribers that belong to the Business Groups that is mapped to the current CMP domain.

b) In case the **Use Domain to Business Group Mapping** option is disabled, system creates UM Users for the subscribers that belong to any Business Group.

c) In case the **Use Domain to Business Group Mapping** option is disabled and more than one OSV switch has been configured,

system creates the UM Users for the subscribers that belong to any Business Group of the first available OSV switch only.

– reports the progress of the operation using a progress bar along with appropriate text.

a) If the procedure has already been initiated by a different administrator in the same domain:

- – System does not allow the execution of the procedure.
  – System informs that the operation is not possible because the procedure has already been started.

6) Click **Cancel** to stop an ongoing operation.

NOTICE: System does not rollback already created UM Users and it does not leave an UM User in an inconsistent state.

---

7) Depending on the operation outcome, a pop-up window containing the following information is displayed:

- –
  – a list of OSV Subscribers for which the creation of a new UM Users was not possible.

    `Conversion failed for <number> OSV subscribers.`
  – number of created UM Users

    `<number> Users created successfully.`

8) System stores information about all operations performed during the latest import operation in the log file.

9) Click **Download Report** to download a log file with the details of the latest performed operation.

NOTICE:

Log files are stored on the server, under the following

path:

- **for integrated Simplex =** `/log/OSCUM/`

- **for all other deployments =** `/var/siemens/common/log/OSCUM/`

---

10) Click **Close** to close the **Create Users from OSV Subscribers** pop-up window.

NOTICE:

In order to view the imported data, the UM Users list needs to be explicitly accessed. This means that after you close the **Create Users from OSV Subscribers** pop-up, you need to navigate to the **Users&Resources** screen and refresh it, so that you see the new UM Users.

---

12 OpenScape User Management Unify Phone

The **OpenScape User Management Unify Phone** contains the list of SBC Configurations for Unify Phone Users and the list of the existing Unify Phone Users.

Configurations for Unify Phone Resources are described in:

- Unify Phone Configurations on page 677

As CMP Administrator you can view the list of Unify Phone Users and perform actions as described in:

- Unify Phone Users on page 679

When creating users and for other configurations that require the creation of identifiers, you must refer to the character restrictions. For more information, see Appendix A: Character Restrictions on page 691.

12.1 Unify Phone Configurations

OpenScape Unify Phone supports SBC configurations, which enable the assignment of a Unify Phone resource to UM Users.

Before configuring a Unify Phone in User Accounts, ensure the following actions are completed:

1) Configure the Unify Phone servers (see How to Configure Unify Phone Servers on page 68).
2) Create a new SBC configuration for User Accounts (see How to Create a new SBC configuration for Unify Phone users on page 677).

12.1.1 How to Create a new SBC configuration for Unify Phone users

Prerequisites

Adequate administrative permissions

Unify Phone Server configurations have been completed successfully

> **NOTICE:**
>
> In case the Unify Phone Server has not been configured, the following warning message is displayed: **Unify Phone Settings are not configured properly**.

Step by Step

1) Click on the **User Management** navigation tab.
2) In the navigation tree, click **Unify Phone** > **Configurations**.

   A list of existing SBC configurations is displayed.
3) From the **Tenant** drop-down menu, select the tenant for which you want to create an SBC configuration.

4) Click **Add**.
The **Add configuration** window opens.
5) Enter the following information:
   - **Name**

     The name of the SBC configuration.
   - **IP/FQDN address**

     The IP or FQDN address of the SBC configuration.
   - **Port**

     The port to be used.
   - **Protocol**

     The protocol to be used (e.g. TLS).
   - **Type**

     The type of the SBC configuration (e.g. OSV).
6) Click **Save** to apply the settings.
The newly created SBC configuration appears in the list.

12.1.2 How to Edit a SBC configuration for Unify Phone users

Follow the recommended steps to edit a SBC configuration for Unify Phone Users.

Prerequisites

Adequate administrative permissions

Unify Phone Server configurations have been completed successfully

---

NOTICE:

If the Unify Phone Server is not configured, the following warning message is displayed: **Unify Phone Settings are not configured properly**.

To configure the Unify Phone Settings see How to Configure Unify Phone Server.

Step by Step

1) Click the **User Management** navigation tab.
2) In the navigation tree, click **Unify Phone** > **Configurations**.

   A list of existing SBC configurations is displayed.
3) From the **Tenant** drop-down menu, select the tenant whose SBC configuration you want to edit.
4) Select the SBC configuration you want to edit in one of the folllowing ways:
   - Click the **SBC Configuration Name**, or
   - Select the checkbox on the left side of the **SBC Configuration Name** you want to edit and click **Edit**.

   The **Edit configuration** window opens.

5) Edit any of the following as needed:

- **Name**

  The name of the SBC configuration.
- **IP/FQDN address**

  The IP or FQDN address of the SBC configuration.
- **Port**

  The port to be used.
- **Protocol**

  The protocol to be used (e.g. TLS).
- **Type**

  The type of the SBC configuration (e.g. OSV).

6) Click **Save** to apply the settings.

12.2 Unify Phone Users

You can view a list of the existing Unify Phone Users.

You can also add, edit or delete a Unify Phone User and reinvite them by sending them an invitation via email to join Unify Phone.

Users that do not own UM licences can perform these actions only from the Unify Phone **Users** menu and not from the existing UM menu.

12.2.1 How to Display Unify Phone Users list

This section describes how to view the existing Unify Phone users and perform search actions.

Prerequisites

Adequate administrative permissions

Unify Phone Server Configuration has been completed.

Step by Step

1) Click the **User Management** navigation tab.

2) In the navigation tree, click **Unify Phone** > **Users**.

3) From the **Tenant** drop-down menu, select the tenant whose information you want to view.

A list of the existing Unify Phone Users is displayed, sorted per first column **E-mail**.

4) To search a Unify Phone User, enter a keyword in the **Search for:** field.

NOTICE: Wildcards are not required. The search is always performed as a greedy search.

---

5) Select an item from the drop-down search list. The list contains the following options:

   - **E-mail**
   - **Name**
   - **Phone Number**
   - **Configuration**

   Example: Search for `new` in **E-mail**.

   If you select **Configuration**, the adjacent drop-down list is enabled.. Then you can select to search Unify Phone Users with a specific configuration.

   Example: Search for `sbcConfStaging` in **Configuration**.

   NOTICE: If you select **Configuration**, the keyword search field is disabled (grayed out).

12.2.2 How to Add a Unify Phone User

This section describes how to add a new Unify Phone User.

Prerequisites

Adequate administrative permissions

Unify Phone Server configurations have been completed successfully

Step by Step

1) Click the **User Management** navigation tab.
2) In the navigation tree, click **Unify Phone** > **Users**.
3) From the **Tenant** drop-down menu, select the tenant for which you want to add a Unify Phone user.

   A list of existing Unify Phone Users is displayed.
4) Click **Add...** to create a new Unify Phone User.

   The **Add Unify Phone User** window opens.

5) Configure the following:

- **Email**: Enter a valid email address.

  NOTICE: Once configured, the **Email** of a user cannot be changed. Each user is assigned a unique email address that is used as their identifier.

- **First Name**: Enter the first name of the user.
- **Last Name**: Enter the last name of the user.
- **Phone number**: Click to select a preconfigured phone number.

  A **Select OpenScape Voice resource** window pops up, containing a list of available phone numbers.

  Check the box in front of the phone number you want to select and click **OK**.
- **Configuration**: Select the SBC configuration you want from the drop-down list.

Unify Office Tenant Configuration (if applicable)

If you need to configure a Unify Office tenant, edit the file `SYMPHONIA_HOME/common/conf/UnifyPhoneFlagsConfig.txt` accordingly.

This file contains two entries corresponding to the following flags:

- **skipRcEmail**
- **isUnifyOfficeTenant**

By default, both flags are set to **false**.

These flags are CMP-wide, meaning they affect all tenants configured from the CMP.

For a Unify Office tenant, set the flag **isUnifyOfficeTenant** to true.

NOTICE:

The **skipRcEmail** flag can only be true if **isUnifyOfficeTenant** is also true.

If **isUnifyOfficeTenant** flag is set to false, both flags are considered false.

NOTICE:

`(*)SYMPHONIA_HOME` corresponds to `/opt/siemens` for duplex deployments and to `/enterprise` for simplex deployments.

6) Click **Save** to apply the settings.

12.2.3 How to Edit a Unify Phone User

This section describes how to edit a Unify Phone User.

Prerequisites

Adequate administrative permissions

Unify Phone Server configurations have been completed successfully

Step by Step

1) Click the **User Management** navigation tab.
2) In the navigation tree, click **Unify Phone** > **Users**.
3) From the **Tenant** drop-down menu, select the tenant whose Unify Phone user you want to edit.

   A list of existing Unify Phone Users is displayed.
4) Select a Unify Phone User to edit in one of the following ways:
   - Click the email of the Unify Phone User you want to edit.
   - Select the checkbox next to the Unify Phone User you want to edit and click **Edit**.
   - In the row of a respective Unify Phone User, click ▸ to open the application action menu, then select **Edit**.

   The **Edit Unify Phone User - [email of the user]** window opens.
5) Edit any of the following as needed:
   - **First Name**
   - **Last Name**
   - **Phone Number**:
     – Click **Clear** to remove the assigned phone number.
     – Click to assign a new phone number.

       A **Select OpenScape Voice resource** window opens, containing a list of available phone numbers.
     – Check the box next to the phone number you want to select and click **OK**.
   - **Configuration**
   - **VoiceMail**

     NOTICE: You cannot change the **Email** of a user. Each user is assigned a unique email address, which is used as their identifier.
6) Click **Save** to apply the settings.

12.2.4 How to Delete a Unify Phone User

This section described how to delete a Unify Phone User.

Prerequisites

Adequate administrative permissions

Unify Phone Server configurations have been completed successfully

Step by Step

1) Click the **User Management** navigation tab.
2) In the navigation tree, click **Unify Phone** > **Users**.
3) From the **Tenant** drop-down menu, select the tenant whose Unify Phone user you want to delete.

   A list of the existing Unify Phone Users is displayed.
4) Select to delete a Unify Phone User in one of the following ways:

   - Check the box next to the Unify Phone User you want to delete and click **Delete**.
   - In the row of a respective Unify Phone User, click ▸ to open application action menu, then select **Delete**.

   A **Delete Unify Phone User** window opens.
5) Select one of the following options:

   - **Delete User from Unify Phone Server only**
   - **Delete User from Unify Phone Server and Unify Video**
6) Click **Delete**.

12.2.5 How to Reinvite a Unify Phone User

When you add a Unify Phone User, an email is sent to the user with the prompt to join Unify Phone. In case the user has not accepted the invitation to join Unify Phone, you can reinvite the user by sending another email. In case a Unify Phone User has accepted the invitation, the **Reinvite** feature is disabled.

Prerequisites

Adequate administrative permissions

Unify Phone Server configurations have been completed successfully

Step by Step

1) Click the **User Management** navigation tab.
2) In the navigation tree, click **Unify Phone** > **Users**.
3) From the **Tenant** drop-down menu, select the tenant whose Unify Phone user you want to reinvite.

   A list of the existing Unify Phone Users is displayed.
4) In the row of a respective Unify Phone User, click ▸ on to open application action menu, then select **Reinvite**.

NOTICE:

If notifications for successful completion of an action are enabled, a **Confirmation** window pops up displaying the message **The action has been completed successfully**.

If the **Reinvite** action fails, an **Error** window pops up displaying the message **The action has failed**.

---

13 OpenScape User Management for Zoom

The **OpenScape User Management Zoom** area provides access to the list of Zoom configurations and existing Zoom Users.

As a CMP administrator, you can create new Zoom configurations and provision Zoom users.

Before proceeding, ensure that the CloudLink Daemon is installed and the CloudLink and Zoom configurations are completed.

CloudLink configuration references:

- Chapter 4.2.18 **How to Configure CMP-CloudLink Daemon connection**.
- For SBC-CloudLink Daemon connection, refer to OpenScape Solution V11, Mitel Phone System Integration (PSI) with Zoom, User Guide and the OpenScape SBC V11 Administration Guide.

Zoom configuration references:

- OpenScape Solution V11, Mitel Phone System Integration (PSI) with Zoom, User Guide.
- Zoom support page.

To create a new Zoom configuration, follow the steps described in:

- How to Create a new Zoom configuration on page 684

You can view the list of Zoom users and manage them (add, edit, or delete) as described in:

- Zoom Users Configuration on page 687

When creating users or performing other configurations requiring identifiers, ensure you adhere to the character restrictions. For more information, see **Appendix A: character restrictions**.

After creating the Zoom configuration, you can create a User Template with Zoom and a Zoom Resource. For detailed instructions, refer to the following chapters:

- How to Create User Template with Zoom on page 558.
- How to Create a Zoom Resource on page 447.

13.1 How to Create a new Zoom configuration

As a CMP administrator, you can create a new Zoom Phone configuration.

Prerequisites

1) Adequate administrative permissions
2) The **CloudLink Daemon RPM** is installed, and **CloudLink configurations** have been completed successfully.
3) **Zoom users** have been configured in the Zoom tenant. For more infromation, refer to **OpenScape Solution Set V11 Zoom Phone with OpenScape SBC and OpenScape Voice (Phone System Integration)** and the Zoom support page.

Step by Step

To create a new Zoom configuration:

1) Click the **User Management** navigation tab.
2) In the navigation tree, click **Zoom** > **Configurations**.

   A list of the existing Zoom configurations is displayed.
3) Click **Add**.
   The **Add configuration** window opens.
4) Configure the following:
   - **Name**

     Name of the Zoom configuration.
   - **IP/FQDN address**

     IP or FQDN address of the Zoom configuration.
   - **Port**

     Specify the used port.
   - **Protocol**

     Specify the used protocol (**TLS**, **TCP** or **UDP**).
5) Click **Save** to apply the settings.
   The newly created Zoom configuration is displayed in the list.

Next steps

After creating the Zoom configuration, you can create a **User Template with Zoom** and a **Zoom Resource**. For detailed instructions, refer to OpenScape Common Management Platform V10 Administrator Documentation.

13.2 How to Edit a Zoom configuration

Follow the recommended steps to edit a Zoom Phone configuration.

Prerequisites

1) Adequate administrative permissions
2) The **CloudLink Daemon RPM** is installed, and **CloudLink configurations** have been completed successfully.
3) **Zoom users** have been configured in the Zoom tenant. For more infromation, refer to **OpenScape Solution Set V11 Zoom Phone with OpenScape SBC and OpenScape Voice (Phone System Integration)** and the Zoom support page.

Step by Step

1) Click the **User Management** navigation tab.
2) In the navigation tree, click **Zoom** > **Configurations**.

   A list of the existing Zoom configurations is displayed.
3) To edit the Zoom settings:
   - Select the Zoom configuration you want to edit by clicking on the Zoom Configuration Name, or
   - Select the checkbox on the left side of the Zoom Configuration Name and click **Edit**.

   The **Edit Zoom configuration** window opens.

4) Edit the information in any of the following fields:
   - **Name**: Name of the Zoom configuration.
   - **IP/FQDN address**: The WAN public IP or FQDN address of the Zoom configuration.
   - **Port**: The used port.
   - **Protocol**: The protocol used for establishing a secure connection.
5) Click **Save** to apply the changes.

14 Zoom Users Configuration

You can view a list of the existing Zoom Users.

You can also add, edit or delete a Zoom User.

IMPORTANT:

Editing or deleting Zoom configurations does not automatically impact the relevant Zoom user data. You must manually re-provision each Zoom user.

14.1 How to Add a Zoom User

This section describes how to add a new Zoom User.

Prerequisites

1) Adequate administrative permissions.
2) The CloudLink Daemon RPM is installed, and CloudLink configurations have been completed successfully.
3) Zoom users have been configured in the Zoom tenant. For more infromation, refer to **OpenScape Solution Set V11 Zoom Phone with OpenScape SBC and OpenScape Voice (Phone System Integration)** and the Zoom support page.

Step by Step

To add a new Zoom user:

1) Click the **User Management** navigation tab.
2) In the navigation tree, click **Zoom** > **Users**.

   A list of the existing Zoom Users is displayed.
3) Click **Add...**.

   The **Add Zoom User** window opens.

4) Configure the following:

- **Email**: Enter a valid email address.

  NOTICE: Once configured, the user's **Email** cannot be changed. Each user is assigned a unique email address that is used as their identifier.

- **First Name**: Enter the first name of the user.
- **Last Name**: Enter the last name of the user.
- **Phone number**: Click to assign a preconfigured phone number.

  The **Select OpenScape Voice resource** window opens, containing a list of available phone numbers.

  Select the checkbox next to the desired phone number and click **OK**.

  NOTICE: The administrator must know which OSV subscribers are configured for Zoom connection.

- **Configuration**: Select the Zoom configuration you want from the drop-down list.
- **VoiceMail**

5) Click **Save** to save the settings.

NOTICE: If the entered email does not corespond to a Zoom User, the error message **"The action has failed"** is displayed.

When the integration between an OSV subscriber and a Zoom user is completed:

- In CMP, the new user is added to the **Zoom Users** list.
- In the **Zoom Phone System Integration** menu area, under **Integrated Users**, the status and information of the newly created Zoom user are updated.
- In the **CloudLink User Management** menu area, the new user is added under the **Users** list.

14.2 How to Display Zoom Users

This section describes how to view the existing Zoom users and perform search actions.

Prerequisites

1) Adequate administrative permissions
2) The CloudLink Daemon RPM is installed.
3) CloudLink and Zoom configurations have been completed successfully.
4) At least one user must be configured in the system.

Step by Step

1) Click the **User Management** navigation tab.

2) In the navigation tree, click **Zoom** > **Users**.

   A list of the existing Zoom Users is displayed, sorted per first column **E-mail**.

3) To search a Zoom User, enter a keyword in the **Search for:** field.

   NOTICE: Wildcards are not required. The search is always performed as a greedy search.

4) Select any of the following from the drop-down search list:

   - **E-mail**
   - **First Name**
   - **Last Name**
   - **Phone Number**

   Example:

   Search for: `new` in **E-mail**.

14.3 How to Edit a Zoom User

This section describes how to edit a Zoom User.

Prerequisites

1) Adequate administrative permissions.
2) The CloudLink Daemon RPM is installed.
3) CloudLink and Zoom configurations have been completed successfully.

Step by Step

1) Click the **User Management** navigation tab.
2) In the navigation tree, click **Zoom** > **Users**.

   A list of the existing Zoom Users is displayed.

3) Select a Zoom User to edit in one of the following ways:

   - Click the email of the Zoom User you want to edit.
   - Check the box next to the Zoom User you want to edit and click **Edit**.
   - In the row of a respective Zoom User, click ▶ to open application action menu, then select **Edit**.

   The **Edit Zoom Phone User - [email of the user]** window opens.

4) Edit any of the following as needed:

- **First Name**
- **Last Name**
- **Phone Number**:
  - Click **Clear** to remove the assigned phone number.
  - Click to assign a new phone number.

    A **Select OpenScape Voice resource** window opens, containing a list of available phone numbers.
  - Check the box next to the phone number you want to select and click **OK**.
- **Configuration**

> **NOTICE:** You cannot change the **Email** of a user. Each user is assigned a unique email address, which is used as their identifier.

5) Click **Save** to apply the changes.

14.4 How to Delete a Zoom User

This section described how to delete a Zoom User.

Prerequisites

1) Adequate administrative permissions.
2) The CloudLink Daemon RPM is installed.
3) CloudLink and Zoom configurations have been completed successfully.

Step by Step

1) Click the **User Management** navigation tab.
2) In the navigation tree, click **Zoom** > **Users**.

A list of the existing Zoom Users is displayed.

3) Select to delete a Zoom User in one of the following ways:

- Check the box next to the Zoom User you want to delete and click **Delete**.
- In the row of a respective Zoom User, click ▸ to open application action menu, then select **Delete**.

The **Zoom User** window opens.

4) Click **Delete**.

15 Appendix A: Character Restrictions

The Common Management Platform uses the name of the user (along with some other info) as a unique identifier in some URLs to open a popup corresponding to the user selected. Please see the information below for character restrictions when creating users, user templates, or other configurations that require the creation of identifiers.

Characters that are not allowed are: ' (single quote), < , > , /, \\ (and their encoded chars "%3C", "%3E", "%5C"), ", ' and &, their encoded chars ("%22", "%27", "%26" respectively) and their HTML encodings, javascript:, style= and " " (white space) at the start, or at the end of the User ID.

Index

Numerics

3rd party node 96
3rd party node connection 96
3rd Party Node Connection
    Deleting 98
    Editing Settings 98
3rd Party Node Connections
    Displaying 96
3rd Party Nodes Connection
    Adding 97

A

Activate License Offline 180
Activate License Online 181, 181
Activate Licenses 178
Active sessions
    terminate 61
Adding 222
Advanced Features 395
Advanced search for the UM 402
Alarm Indicator 62
Application
    Display 147
    Executing an Action 148
Application Dashboard 125
Archive
    Adding 209
    Deleting 212
    Deleting a Backup Set 213
    Displaying a Backup Set 213
    Editing a Backup Set 213
    Editing Settings 208, 211
    Testing 212
Assistant data
    export 192
    types of data 192

B

Backing up Manually 227
Backup Schedule 222
    Deleting 225
    Editing Settings 221, 224
backup schedules 221
Backup Set 227
    Backing up Manually 230
    Deleting 218
    Deleting a Backup Set of an Archive 213
    Displaying a Backup Set of an Archive 213
    Displaying Settings 217
    Editing a Backup Set of an Archive 213
    Editing Settings 217
Backup version activation 145
Basic Features 395

C

changeSFWip.sh 265
Changing the CMP administrator password 25
CMP 22
    adjusting the interface 268
    Alarm Indicator 30
    Alarm Preferences 30
    customizing the interface 272
    Displaying the Installed Software Versions 27
    Navigation Bar 30
    Navigation Tree 32
    Opening the Online Help 27
    System Bar 23
    Work Area 33
CMP administrator locked 74
CMP administrator permission 74
CMP administrator user
    display 42
CMP Administrator User
    delete 52
CMP Browser requirements 19
CMP Default Profiles 76
CMP export 191
CMP Pop-ups
    Allowing them generally 19
    Allowing them selectively 19
CMP show bound license 178
    foreign User 178
Column Settings 35, 400
Comma-separated values (CSV) file 605
Common Management Platform (see CMP) 22
Communication System Dashboard 128
Component
    Editing the Setting 134
    restart 141
    starting 140
    stopping 140
Configuration data
    export 193
    file type for re-import 193
configuration voicemail 202
Configuring HTTPS Port f. CMP Access 267
Consistency Check 260, 261
create user accounts import 205
Customer Profile 74

D

Dashboard
    Display 125

Data
Export 188
Import 188
Default Locality 488
Default Profile
OpenScape Voice Assistant 84
Default Profiles CMP 76
Default User Profile 73
Delta Synchronization
Delta Synch interval value 120
Device Management 148
Certificate 165
Configure a Connection 162
Creating a Connection 160
Remove a Connection 164, 166
DLS 148
Domain 39
Download Center 253
Downloading Software 256
How to Download Documentation 256
Providing Documentation 255
Providing Software 255
download last check report 261

E

E911 Alarm Email Notification 292
email Notification 292
ENUM Data
export 194
Export of data 188
External Identifier
Configure 67
External IDs
Configure 67
External Resource 445

F

File System backupt
USB disk 230
Foreign Users 388
Frontend Dashboard 127

H

h4kNodeManagerAssistant
Remove 111
HiPath 4000 Dashboard 129
HiPath 4000 Node Connection
Adding 107
configure routing 113
editing 109
manual delta synchronizing 117
Synchronization Exeptions 105
synchronizing 115, 119
HiPath User Management (HPUM) 611
HiPath4000 Node 103
HiPath4000 Node Connection
Adding 107
manual delta synchronizing 117
Synchronization Exeptions 105
synchronizing 115, 119

I

import Configure IM address 201
import delete information 206
Import of data 188

J

Job
Canceling 226
Displaying the Status 225

L

LDAP Directory 615
LDAP Manual Synchronization 661
LDAP Scheduled Synchronization 655
License Information 175
License Locking id 182
License Management Concept 172
License type
software subscription license 184
Localities 487

M

Media Server Dashboard 130
MIB 283

N

new CMP installation 671
Node
Editing Personal Workflow Controls Factory component 138
Editing SNMP Service 136
Editing the Component Setting 134
Node Cluster
Deleting 96
Node Group 94
Adding 94
Displaying 94
Editing 95
Node Note
Configuring 143
Nodes Cluster 92

O

OpenScape 4000 Resource 429
OpenScape 4000 station PINs 408

OpenScape Accounting 148
OpenScape Deployment Service
Configure a Connection 162
OpenScape Fault Management 148
OpenScape FM 148
OpenScape Mobile Resource 425
OpenScape Performance Manager 148
OpenScape PM 148
OpenScape Voice ENUM Data
export 194
OpenScape Voice Resource 412
OpenScape Voice Softphone Resource 418
OpenScape Xpressions Resource 434
OSc Accounting 148
Creating a Connection 157
Remove a Connection 159
OSc Accounting Application
Creating a Connection 156
Remove a Connection 159
OSc Concierge 165
OSc Contact Center 165
OSc Deployment Service 148
Creating a Connection 160
OSc DLS
Certificate 165
Remove a Connection 164, 166
OSc FM 148
OSc FM Application
Certificate 154
Creating a Connection 150, 152
Remove a Connection 154
OSc Performance Management 148
OSc Trace Manager 165
OSc Xpressions 165
OSEE Applications
Creating a Connection 166
OSV Subscribers 671

P

Password policy
Parameter LockoutTime 57
Parameter MaximumAge 55
Parameter MaximumFailedAttempts 56
Parameter MaximumLength 56
Parameter MaximumRepeatedCharacters 56
Parameter MinimumAge 55
Parameter MinimumDigits 56
Parameter MinimumLength 56
Parameter MinimumSpecialCharacters 56
Parameter MinimumUpperCaseCharacters 56
Parameter PasswordHistoryDepth 57, 57, 57
Password policy;Policy
user password 53
Passwort policy
change 57
Personal Workflow Controls Factory component
Edit 138
Profile
Customer 74
Provisioning 605
Proxy Server
Add 64
delete 66
display 65

R

Rebrand script 268, 272
Remote Logging for OSV Trace Manager 305
Repository 257
Resource type 399
Restore
Restoring the entire System after a Crash 219
RG8700 Dashboard 132
Role Based Access description 74

S

Schedules 654
SIEL ID 187
SMTP server 66
SNMP Dashboard 134
SNMP MIB 283
SNMP Node 121
SNMP Node Connection
adding 121
deleting 124
editing 122
SNMP Service
Edit 136
Software Activation 167
Software Activation creating 168
Software Package Overview 143
Software Packages
Displaying 144
Software repository 257
deleting upgrade file package 259
displaying upgrade file package 257
uploading upgrade file package 258
Speed dial list
modify 68, 69, 202, 677, 678
Storage Area Network 236
Symphonia CMP mapping table 76
Symphonia permissions mapping 76
System Dashboards, general 125
system management 39
System Management 92
System Node
Move to Group 142
Restarting 142
System Nodes
Displaying 93
System Overview
Applications 93
Nodes 92

System Overview, general 92
System settings 63
System User Profile 74

T

Trace
    start 323, 326
Trace Files
    download 320
    Generate 320

U

UC Accounts 668
UI Patching 167
UI Patching creating 168
UM User 395
UM Users attributes 395
Unified Communications Resource 440
Upgrade file package
    deleting 259
    displaying 257
    uploading 258
Use Domain to Business Group Mapping 412, 419, 425
User Account f. Administrators 42
User Management Concept 388
User Management Web Interface 397
User Profile 72
    Adding 89
    Copy 90
    Default 73
    Deleting 91
    Edit 88
    System 74
User Templates 500

V

Versions synchronization 146

X

Xpresions Node Connection
    Adding 99
    Synchronize 101
Xpression Node 99
Xpressions Dashboard 131
Xpressions Node Connection
    editing 100, 103

© 2026 Mitel Networks Corporation. All Rights Reserved. Mitel and the Mitel logo are trademark(s) of Mitel Networks Corporation. Unify and associated marks are trademarks of Unify Software and Solutions GmbH & Co. KG. All other trademarks herein are the property of their respective owners.