A MITEL
PRODUCT
GUIDE

Unify OpenScape Session Border Controller

OpenScape SBC V11

Administration Guide
12/2025

A31003-S5300-M101-19-76A9

Mitel

Notices

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

Trademarks

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

© Copyright 2025, Mitel Networks Corporation

All rights reserved

Contents

1 OpenScape SBC Assistant – Introduction 11
1.1 About This Guide 11
1.2 OpenScape Session Border Controller — Overview 12
1.3 Navigation 27

2 OpenScape SBC Assistant – Primary Administration 29
2.1 Business Groups and Branch Offices 29
2.2 How to Add or Delete an OpenScape SBC to OpenScape SBC Assistant 30
2.3 How to Display an OpenScape SBC Via OpenScape SBC Assistant 31
2.4 How to Update SBC Status 32
2.5 How to Change the Password in the Local Assistant Database 34

3 OpenScape SBC Assistant – Maintenance 36
3.1 System Information and Monitoring 36
3.1.1 The OpenScape SBC Dashboard via CMP 36
3.1.1.1 How to Display the OpenScape SBC Dashboard via CMP 39
3.1.1.2 How to Display Active Alarms 39
3.1.1.3 How to Display Alarm Details 41
3.1.1.4 How to Start Rapidstat to Perform a Health Check 42
3.1.1.5 How to Display Detailed Version Information 43
3.1.1.6 How to Display System Information for OpenScape SBC 44
3.1.1.7 How to Display the Services Status of an earlier-than-V8 OpenScape SBC 45
3.1.1.8 How to Display, Export and Clear Log Files for an earlier-than-V8 OpenScape SBC 47
3.1.1.9 How to Restart the System 49
3.1.2 General System Information 50
3.1.2.1 How to Display a List of Registered Subscribers 52
3.1.2.2 How to Display a List of Dynamic IP Remote Endpoints 53
3.1.2.3 How to Display a List of Statistics 55
3.2 Serviceability 56
3.2.1 OpenScape SBC File System 57
3.2.1.1 How to Load and Apply New Configuration Files 58
3.2.1.2 How to Select a Configuration File for Import 59
3.2.1.3 How to Export Configuration Files 61
3.2.2 Software Updates and Upgrades 62
3.2.2.1 How to Activate Software on a Particular OpenScape SBC or Branch Device via CMP 63
3.2.3 Job Management 64
3.2.3.1 How to View Batch Jobs 64
3.2.3.2 How to Create a New Batch Job 65
3.2.3.3 How to Edit or Cancel a Batch Job 66
3.3 Password Management 67
3.4 General Installation - Overview 68
3.4.1 OpenScape SBC Assistant - Configuration 69
3.4.1.1 How to Configure OpenScape SBC Assistant - General Settings 70
3.4.2 Simplified Installation Steps 70
3.4.2.1 How to Download Installation Files Into the CMP 73
3.4.2.2 How to Configure a Windows DHCP Servers 74
3.4.2.3 How to Configure a LINUX DHCP Server 76
3.4.2.4 How to Configure a Cisco Router Utilizing the DHCP Server 78
3.4.2.5 How to Add an Endpoint in OpenScape Voice for OpenScape SBC 80
3.4.2.6 How to Add or Delete an OpenScape SBC to OpenScape SBC Assistant 82
3.4.2.7 How to Configure the Software Load and Hardware Type 83

3.4.2.8 How to Configure the Data Configuration File..... 84
3.4.2.9 How to Configure the MAC Address..... 85
3.4.2.10 How to Install Hardware for Simplified Installation..... 86
3.4.2.11 How to Troubleshoot Installation Errors and Alarms..... 88
3.5 OpenScape SBC Licensing Files..... 92
3.5.1 OpenScape SBC Regular License File..... 94
3.5.2 OpenScape SBC Software Subscription License File..... 95
3.5.2.1 OpenScape SBC Software Subscription License (SSL) Monitoring and Reporting - Details..... 96
3.5.3 OpenScape SBC Evaluation License File..... 100
3.5.4 OpenScape SBC Base License..... 101
3.5.5 OpenScape SBC Session License..... 101
3.5.6 Upgrade License - Overview..... 102
3.6 Managing Licenses..... 102
3.6.1 License Management Concept..... 102
3.6.2 License Information..... 104
3.6.2.1 How to Display License Information via CMP..... 105
3.6.2.2 How to Display Software Subscription License Information via CMP..... 106
3.6.2.3 How to Display License Locking IDs via CMP..... 108
3.6.2.4 How to Display License Information via OpenScape SBC Assistant..... 108
3.6.2.5 How to Display and Manage Licensing Thresholds via OpenScape SBC Assistant..... 109
3.6.2.6 How to Display Licensing for an OpenScape SBC Via OpenScape SBC Assistant..... 110
3.6.2.7 How to Configure and Clear Licensing for an OpenScape SBC Via OpenScape SBC Assistant..... 113
3.6.2.8 How to Display Licensing Warnings for an OpenScape SBC..... 115
3.6.3 Activating Licenses..... 116
3.6.3.1 How to Activate License - Online..... 118
3.6.3.2 How to Activate License - Offline..... 119
3.6.4 License Enforcement and Update..... 119
3.6.5 License Security..... 121

4 OpenScape SBC Assistant – Configuration..... 122
4.1 Alarm Configuration Overview..... 122
4.1.1 Alarm Settings..... 122
4.1.1.1 How to Display Alarms Settings..... 123
4.1.1.2 How to Display Alarms Settings for earlier-than-v8 OpenScape SBC devices..... 126
4.1.1.3 How to Edit Alarms Settings..... 129
4.1.1.4 How to Edit Alarms Settings for earlier-than-v8 OpenScape SBC devices..... 130
4.1.1.5 How to Edit and Add Trap Destinations..... 132
4.1.1.6 How to Edit and Add Trap Destinations for earlier-than-v8 OpenScape SBC devices..... 133
4.1.1.7 How to Display and Delete Trap Destinations..... 135
4.1.1.8 How to Display and Delete Trap Destinations for earlier-than-v8 OpenScape SBC devices..... 136
4.2 Logging Configuration Overview..... 138
4.2.1 Logging for OpenScape Session Border Controller..... 138
4.2.1.1 How to Edit Settings for Logs..... 140
4.2.1.2 How to Edit Settings for Logs for earlier-than-v8 OpenScape SBC devices..... 141
4.2.2 Debugging..... 144
4.2.2.1 How to Use Debugging Tools..... 144
4.2.2.2 How to Use Debugging Tools for earlier-than-v8 OpenScape SBC devices..... 146
4.2.3 Continuous Tracing and On Demand Trace..... 147
4.2.3.1 How to Configure Continuous Tracing..... 149
4.2.3.2 How to Configure Continuous Tracing for earlier-than-v8 OpenScape SBC devices..... 151
4.2.3.3 How to Start, Stop and Configure On Demand Tracing..... 152
4.2.3.4 How to Start, Stop and Configure On Demand Tracing for earlier-than-v8 OpenScape SBC devices..... 154
4.3 Network Services — Overview..... 155
4.3.1 How to Configure the Interfaces..... 162

4.3.2 How to Configure the Interfaces for earlier-than-v8 OpenScape SBC devices..... 165
4.3.3 How to Configure the Default Gateway Addresses..... 168
4.3.4 How to Configure the Default Gateway Addresses for earlier-than-v8 OpenScape SBC devices..... 169
4.3.5 How to Add, Edit or Delete a Route..... 170
4.3.6 How to Add, Edit or Delete a Route for earlier-than-v8 OpenScape SBC devices..... 171
4.3.7 Traffic Shaping..... 172
4.3.7.1 How to Configure Traffic Shaping..... 173
4.3.7.2 How to Configure Traffic Shaping for earlier-than-v8 OpenScape SBC devices..... 175
4.3.8 How to Configure System NTP Settings..... 178
4.3.9 How to Configure System NTP Settings for earlier-than-v8 OpenScape SBC devices..... 179
4.3.10 How to Synchronize Manually with the NTP Server..... 181
4.3.11 How to Synchronize Manually with the NTP Server for earlier-than-v8 OpenScape SBC devices..... 182
4.3.12 Configuration of DNS Server..... 183
4.3.12.1 How to Configure System DNS Settings..... 184
4.3.12.2 How to Configure System DNS Settings for earlier-than-v8 OpenScape SBC devices..... 187
4.4 Security Configuration — Overview..... 189
4.4.1 TLS Certificates and Shared Secret Files..... 190
4.4.1.1 How to Manage TLS Certificates..... 192
4.4.1.2 How to Create, Edit and Delete Certificate Profiles..... 194
4.4.1.3 How to Configure Certificate Expiration Checking..... 199
4.4.1.4 How to Display and Configure the Certificate Revocation List (CRL)..... 200
4.4.1.5 How to Select a Shared Secret File for Use..... 203
4.4.1.6 How to Display, Add and Delete Shared Secret Files..... 204
4.4.2 Network Intrusion Detection and Prevention (Message Rate Control)..... 205
4.4.2.1 How to Configure Message Rate Control Rules..... 206
4.4.3 Firewall Configuration..... 207
4.4.3.1 How to Configure the Firewall..... 215
4.4.3.2 How to Configure Port Forwarding..... 219
4.4.4 Configuration of Administrative Access Control..... 221
4.4.4.1 How to Configure Administrative Access Control Settings..... 221
4.4.5 RADIUS Support - Overview..... 223
4.4.5.1 How to Configure Radius..... 224
4.5 Survivability and Redundancy — Overview..... 226
4.5.1 How to Configure Redundancy Settings..... 228
4.6 System Settings — Overview..... 230
4.6.1 How to Display and Change License Server Location..... 231
4.6.2 How to Change or Reset the Password..... 232
4.6.3 How to Import/Export and Select Configuration Files via OpenScape SBC Assistant..... 234
4.7 Voice over Internet Protocol Configuration — Overview..... 236
4.7.1 SIP VoIP Port Configuration and Display..... 237
4.7.1.1 How to Configure VoIP SIP Settings..... 237
4.7.1.2 How to Display Registered Subscribers Port Mapping Settings..... 241
4.7.1.3 How to Display Backup Port Mapping Settings..... 242
4.7.2 Configuration of Remote Endpoints and SIP Service Providers - Overview..... 243
4.7.2.1 How to Configure Remote Endpoints - General..... 247
4.7.2.2 How to Configure Remote Endpoints - Emergency Services..... 254
4.7.2.3 How to Configure OpenScape SBC SIP Service Provider Profiles..... 256
4.7.3 Media Server Profile Configuration — Overview..... 260
4.7.3.1 How to Configure a Media Server Profile..... 261
4.7.3.2 How to Configure a Media Server Profile for earlier-than-v8 OpenScape SBC devices..... 262
4.7.4 Quality of Service Configuration..... 264
4.7.4.1 How to Configure VoIP QoS Rules..... 264
4.7.5 Communication System Settings..... 266
4.7.5.1 How to Configure the Communication System for OpenScape SBC..... 270
4.7.6 How to Configure Timers and Thresholds..... 273
4.7.7 Configuration of Remote Subscribers - Overview..... 274

4.7.7.1 How to Configure Remote Subscribers - General....274
4.7.7.2 How to Configure Remote Subscribers - Emergency Services....277
4.7.7.3 How to Configure Remote Subscribers - Domain....280
4.7.7.4 How to Configure Throttling and Registration Expiry....280

5 OpenScape SBC Local Management Platform Overview....282
5.1 Dashboard....283
5.1.1 Alarms....283
5.1.2 System Status....284
5.1.3 Services Status....285
5.1.4 Registered Subscribers....287
5.1.5 SSP Connectivity Status....287
5.1.6 Dynamic Port Mapping....288
5.1.7 CloudLink panel....288
5.1.7.1 Integrating SBC with CloudLink Daemon....289
5.1.8 Dynamic IP Remote Endpoints....290
5.1.9 Denial of Service Mitigation....290
5.1.10 SIP Load Balancer status....291
5.1.11 System Info....291
5.1.12 Software Info....292
5.2 System....292
5.2.1 Settings....292
5.2.2 Licenses....293
5.2.2.1 Open source software license....295
5.2.3 Branding....295
5.3 Network / Net Services....296
5.3.1 Settings....296
5.3.1.1 Physical Network Interface....296
5.3.1.2 Interface Configuration....298
5.3.1.3 Realm Profile....302
5.3.1.4 Routing....303
5.3.1.5 Redundancy....303
5.3.1.6 Core Link Connectivity Check....305
5.3.1.7 External Health Check....305
5.3.2 DNS....306
5.3.2.1 DNS Configuration > DNS Server....306
5.3.2.2 DNS > Administer Custom DNS Files....307
5.3.3 NTP > NTP Settings....307
5.3.4 Traffic Shaping....308
5.3.5 QoS Settings....309
5.4 VOIP....311
5.4.1 SIP Server Settings....312
5.4.1.1 Clustered Servers....315
5.4.1.2 Other Trusted Servers....316
5.4.1.3 Direct Routing Configuration....317
5.4.2 Port and Signaling Settings....318
5.4.2.1 Port and Signaling Settings > Port Range....319
5.4.2.2 Port and Signaling Settings > Signaling and Transport Settings....320
5.4.2.3 Port and Signaling Settings > Miscellaneous....322
5.4.3 Media....322
5.4.3.1 Media Profile....325
5.4.3.2 Media Realm Group Configuration....332
5.4.4 QoS Monitoring....333
5.4.5 VoIP > SIP Headers Manipulation Rules (HMR)....333
5.4.5.1 VoIP > SIP Headers Manipulation Rules (HMR) > SIP HMR Profile....334
5.4.5.2 Troubleshooting SIP Headers Manipulation Rules (HMR)....336

5.5 Features....337
5.5.1 Remote Subscribers....338
5.5.1.1 Remote Subscriber Configuration....343
5.5.2 Remote Endpoints....344
5.5.2.1 SIP Service Provider....345
5.5.2.2 Remote Endpoints Configuration....359
5.5.2.3 Remote Location Domain....366
5.5.2.4 Firewall Settings....369
5.5.2.5 Emergency Calling....369
5.5.2.6 Emergency Calling Subnet....370
5.5.2.7 Media Server Profile....371
5.5.3 SIP Load Balancer....372
5.5.4 Push Notification Service....373
5.6 Security....375
5.6.1 General....375
5.6.1.1 Certificate Management....376
5.6.1.2 Certificate Management > Certificate Profile....379
5.6.1.3 Certificate Management > Generate CSR File....382
5.6.1.4 Certificate Management > Certificates Upload....384
5.6.1.5 Certificate Management > Certificate Revocation....385
5.6.1.6 User Accounts....385
5.6.1.7 Certificate Management > CRL Viewer....388
5.6.1.8 Security > General > PKI Configuration....388
5.6.2 Firewall Overview....388
5.6.2.1 Port Forward....390
5.6.3 Message Rate Control....390
5.6.4 RADIUS....391
5.6.5 Security > Tunnel Connections....392
5.6.6 Denial of Service Mitigation....393
5.7 Diagnostics and Logs....394
5.7.1 Settings....394
5.7.2 Debugging....396
5.7.3 Continuous Tracing....400
5.7.4 On Demand Trace....401
5.7.5 Statistics....401
5.7.6 Serviceability....401
5.8 Alarms....402
5.8.1 Alarms > Alarm Settings....402
5.8.2 Alarms > SNMP Configuration....403
5.9 Maintenance....405
5.9.1 Import/Export....406
5.9.2 Install/Upgrade....407
5.9.3 Bulk Configuration (Delta XML)....408
5.9.4 Restart....410
5.9.5 Scheduled Maintenance....412

6 Appendix - Overview....414
6.1 Alarm Information - Overview....414
6.1.1 Concept of the Alarms and Fault Messages....414
6.1.2 Alarm Information....414
6.1.3 Alarm Severities....415
6.1.4 Alarm Type....416
6.1.5 Alarm Groups....416
6.1.5.1 Alarm Group: Admin....416
6.1.5.2 Alarm Group: Communication....416
6.1.5.3 Alarm Group: Ethernet....417

6.1.5.4 Alarm Group: Hardware....417
6.1.5.5 Alarm Group: License....417
6.1.5.6 Alarm Group: Resource....417
6.1.5.7 Alarm Group: Software....417
6.1.5.8 Alarm Group: Usage....418
6.1.6 Alarm List....418
6.1.6.1 +1.5V high voltage....418
6.1.6.2 +1.5V low voltage....418
6.1.6.3 +3.3V high voltage....418
6.1.6.4 +3.3V low voltage....419
6.1.6.5 +5V high voltage....419
6.1.6.6 +5V low voltage....419
6.1.6.7 +12V high voltage....420
6.1.6.8 +12V low voltage....420
6.1.6.9 Apache/PHP not running....420
6.1.6.10 Bandwidth ethernet port 1....420
6.1.6.11 Bandwidth ethernet port 2....421
6.1.6.12 BLC not running....421
6.1.6.13 BLS not running....421
6.1.6.14 Certificate Authority Could Not Be Validated....422
6.1.6.15 Certificate Contains an Unknown Critical Extension....422
6.1.6.16 Certificate Has Been Revoked....422
6.1.6.17 Certificate is Expired....423
6.1.6.18 Certificate is Out of the Validity Period....423
6.1.6.19 Certificate Subject Could Not Be Authenticated....423
6.1.6.20 Certificate Will Expire in the Next Days....424
6.1.6.21 CDR disk space running low....424
6.1.6.22 DRHandler not running....424
6.1.6.23 CPU1 +1.8V high voltage....425
6.1.6.24 CPU1 +1.8V low voltage....425
6.1.6.25 CPU1 Vtt high voltage....425
6.1.6.26 CPU1 Vtt low voltage....425
6.1.6.27 CPU2 +1.8V high voltage....426
6.1.6.28 CPU2 +1.8V low voltage....426
6.1.6.29 Critical failure on SIP Server configuration....426
6.1.6.30 Critical failure on SIP Server core....426
6.1.6.31 CRL Could Not Be Copied From the Partner Node....427
6.1.6.32 CRL Could Not Be Downloaded....427
6.1.6.33 CRL Fails Because the Signature on the CRL is Invalid....427
6.1.6.34 CRL is Expired....428
6.1.6.35 CRL is Invalid....428
6.1.6.36 Database restored....428
6.1.6.37 DHCP Server not running....429
6.1.6.38 Disk space running low....429
6.1.6.39 Extremely high CPU usage....429
6.1.6.40 Failed to establish the minimum Backup Link bandwidth....430
6.1.6.41 Failed to establish the required Backup Link bandwidth....430
6.1.6.42 Failed update or upgrade....430
6.1.6.43 Failure to mirror phone images due to backup link mode....431
6.1.6.44 Failure to mirror phone images due to less than 25Mb available....431
6.1.6.45 Failure to mirror phone images due to survivable mode....431
6.1.6.46 Feature blocked due to license....432
6.1.6.47 File I/O error....432
6.1.6.48 Generic error code....432
6.1.6.49 Geo-redundant data transfer to remote branch failed attempts....433
6.1.6.50 Geo-redundant data not received from remote branch....433

6.1.6.51 High ambient temperature....433
6.1.6.52 High CPU usage....434
6.1.6.53 High number of active voice channels....434
6.1.6.54 High RAM usage....434
6.1.6.55 High system board temperature....435
6.1.6.56 High temperature core 0....435
6.1.6.57 High temperature core 1....435
6.1.6.58 Install: ACD install failed....435
6.1.6.59 Install: Auto Attendant install failed....436
6.1.6.60 Install: Media Server install failed....436
6.1.6.61 IP blocked due to packet flood....436
6.1.6.62 License has expired....437
6.1.6.63 License HW-Id is already in use....437
6.1.6.64 License info wrong or non existent Logical-ID....437
6.1.6.65 License using temporary grace period....438
6.1.6.66 License violation detected....438
6.1.6.67 License will expire....438
6.1.6.68 License not configured in Server....439
6.1.6.69 Loss of communication with another OSB in the branch....439
6.1.6.70 Loss of communication with billing server....439
6.1.6.71 Loss of communication with DNS server....440
6.1.6.72 Loss of communication with file server....440
6.1.6.73 Loss of communication with gateway....440
6.1.6.74 Loss of communication with Node 1 Backup OSV....441
6.1.6.75 Loss of communication with Node 1 Primary OSV....441
6.1.6.76 Loss of communication with Node2 Backup OSV....441
6.1.6.77 Loss of communication with Node2 Primary OSV....442
6.1.6.78 Loss of communication with NTP server....442
6.1.6.79 Loss of communication with Redundant System....442
6.1.6.80 Loss of communication with SIP Service Provider....443
6.1.6.81 Loss of communication with surveillance system....443
6.1.6.82 Low fan speed 1....443
6.1.6.83 Low fan speed 2....443
6.1.6.84 Low fan speed 3....444
6.1.6.85 Low fan speed 4....444
6.1.6.86 Low fan speed 5....444
6.1.6.87 Low fan speed 6....444
6.1.6.88 Low fan speed 7....445
6.1.6.89 Low fan speed 8....445
6.1.6.90 Low fan speed 9....445
6.1.6.91 Low fan speed 10....446
6.1.6.92 Low fan speed 11....446
6.1.6.93 Low fan speed 12....446
6.1.6.94 Low fan 1 speed PSU 1....446
6.1.6.95 Low fan 2 speed PSU 1....447
6.1.6.96 Low fan 1 speed PSU 2....447
6.1.6.97 Low fan 2 speed PSU 2....447
6.1.6.98 Low fan speed 1B....447
6.1.6.99 Low fan speed 2B....448
6.1.6.100 Low fan speed 3B....448
6.1.6.101 Low fan speed 4B....448
6.1.6.102 Low fan speed 5B....448
6.1.6.103 Low fan speed 6B....449
6.1.6.104 msadapter not running....449
6.1.6.105 Network failure....449
6.1.6.106 Network not running....450

6.1.6.107 No Backup Link channel can be added at all.... 450
6.1.6.108 NTP not running.... 450
6.1.6.109 Parse error for instance when parsing command-line options the '.wgetrc' or '.netcr'....451
6.1.6.110 Phone image download denied due to connections number limit.... 451
6.1.6.111 Phone image download denied due to system load over 60 percent.... 451
6.1.6.112 Port 1 failure....452
6.1.6.113 Port 2 failure....452
6.1.6.114 Power Supply 1 Failure....452
6.1.6.115 Power Supply 2 Failure....453
6.1.6.116 Process Manager not running....453
6.1.6.117 Protocol errors....453
6.1.6.118 PSU 1 failure....453
6.1.6.119 PSU 2 failure....454
6.1.6.120 Reboot requested due to license violation.... 454
6.1.6.121 Redundant system has an invalid version (sync.is disabled)....454
6.1.6.122 Redundant system has not a compatible HW (sync. is disabled).... 455
6.1.6.123 Redundant system synchronization fails.... 455
6.1.6.124 RTPProxy not running.... 455
6.1.6.125 SBC Session limit reached due to license.... 456
6.1.6.126 Server issued an error response....456
6.1.6.127 sipmgcpconv not running....456
6.1.6.128 SIP Server database not restored....457
6.1.6.129 SIP Server not running....457
6.1.6.130 SSL verification failure....457
6.1.6.131 Message Rate Control not running....458
6.1.6.132 ssdp not running....458
6.1.6.133 Standalone operation....458
6.1.6.134 SurvProcess not running.... 459
6.1.6.135 Syslog not running....459
6.1.6.136 Username/password authentication failure....459
6.1.6.137 User registration blocked due to license.... 460
6.1.6.138 VBAT high voltage.... 460
6.1.6.139 VBAT low voltage....460
6.1.6.140 Very high CPU usage....460
6.1.6.141 VRRPD not running.... 461
6.1.6.142 Wrong user ID or password entered.... 461
6.1.6.143 High number of registered users....461
6.1.6.144 Low number of registered users....462

Index.... 463

1 OpenScape SBC Assistant – Introduction

The OpenScape SBC Assistant is a network management software product that provides the configuration and administration of one or more Session Border Controllers running on Unify OpenScape SBC hardware.

The OpenScape SBC Assistant is realized as a software plug-in within the Common Management Platform (CMP).

1.1 About This Guide

This guide describes how to use the OpenScape SBC Assistant to manage and configure OpenScape Session Border Controllers. It provides instructions on how to display and enter configuration parameters in the OpenScape SBC Assistant screens, as well as descriptions of the configuration parameters.

Intended Audience

What You Need to Know

The OpenScape Session Border Controller - Configuration and Administration guide is intended for qualified service personnel responsible for configuring and maintaining the OpenScape Session Border Controller hardware.

A working knowledge of computers and client-server network architectures is necessary for executing tasks using the OpenScape SBC Assistant. In addition, has successfully completed the Unify OpenScape Voice and OpenScape Session Border Controller installation and technical training courses; and should be familiar with basic telecommunications equipment functionality and have obtained proper login permissions to use the OpenScape SBC Assistant.

OpenScape SBC Assistant Online Help

The OpenScape SBC Assistant is used to display and configure OpenScape Session Border Controllers. The online Help refers to the most current OpenScape SBC version. Therefore, if an older version OpenScape Session Border Controller is selected, some sections may describe features that are not available for these earlier version systems and some procedures may deviate from the ones described.

Release Notes

Circuit Support in Version V11

IMPORTANT:

SBC V11 does not support Circuit functionality.

We recommend that users who rely on Circuit features consider SBC V10 or explore the capabilities provided in Version V11 to meet their communication needs.

For further information or assistance, please refer to the product documentation or contact our support team.

1.2 OpenScape Session Border Controller — Overview

The OpenScape Session Border Controller (SBC) deployment in the OpenScape Voice environment is supported in a centralized location (same location as the OpenScape Unified Communication (UC) server, i.e. the customer's Data Center). There are several deployment scenarios and OpenScape SBC runs on different hardware platforms depending on the number of SBC sessions required. OpenScape SBC is a component of the OpenScape Solution Set, and is backward compatible with prior OpenScape Solution Set versions.

Functional Overview

OpenScape SBC is a software-based network border element designed to deliver superior Voice over IP (VoIP) security and cost savings for the OpenScape Enterprise Solution set. It enables OpenScape SIP-based communication and applications to be securely extended beyond the boundaries of an enterprise network.

For deployment scenarios that require a centralized SBC, OpenScape SBC performs the necessary interoperability, security, management, and control capabilities to support SIP trunking applications. It also supports the SIP endpoint registration services that are necessary to support remote user and branch office applications. OpenScape SBC performs SIP deep-packet inspection specifically tailored for the OpenScape Voice environment that is necessary to provide proper mediation between IP networks, such as the mapping of IP addresses and ports within SIP signaling and RTP/SRTP media packets that allows for NAT traversal. Media anchoring can be configured to the extent required by media control policies (for example, for NAT traversal), or set to allow direct media connections between clients.

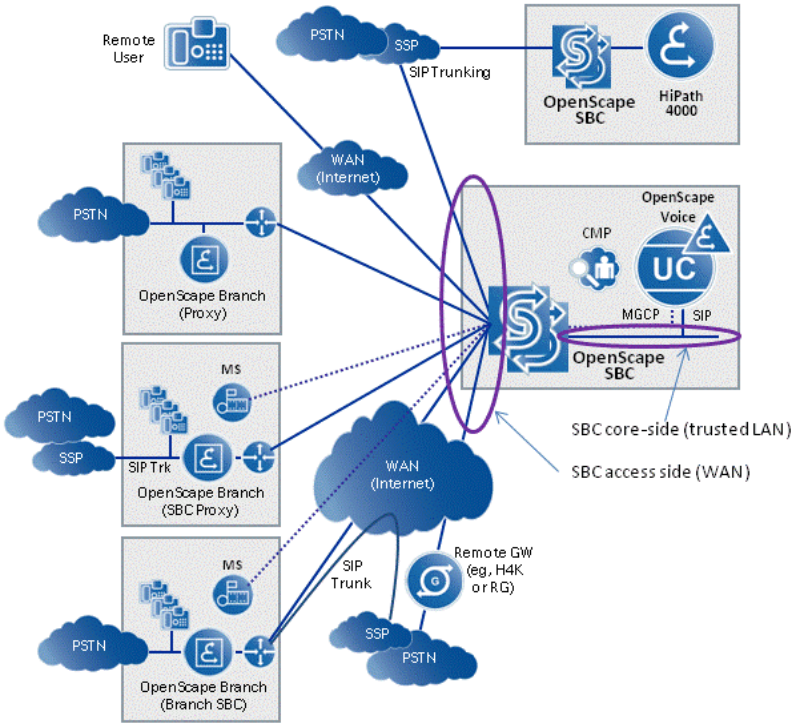
OpenScape SBC enhances customer-network security by providing SIP-aware security functionality including dynamic opening and closing of "pinholes" for media connections, stateful SIP protocol validation, Denial of Service (DoS) mitigation, and network topology hiding. It also supports TLS encryption on both the core- and access-side SIP signaling interfaces as well as SRTP media encryption for both transparent relay pass-through and termination/mediation scenarios.

OpenScape SBC facilitates SIP trunk interfaces to SIP Service Providers (SSPs), connection to remote user SIP phones, for example for home workers accessing an OpenScape Voice system over an Internet connection, and for connection to OpenScape Branch systems serving remote branch locations.

OpenScape SBC is specifically designed for use as a centralized SBC in the OpenScape solution environment. In other words, the OpenScape SBC is designed to be deployed in the same location as the OpenScape UC server, for example, in the customer's data center.

OpenScape Branch can provide SBC functionality in "non-centralized", ie, branch office, locations.

The diagram below illustrates the deployment scenarios supported by OpenScape SBC:



- The **Session Border Controller** (SBC) provides security functions such as Firewall and Virtual Private Network (VPN) while interfacing with a public network.
- The OpenScape SBC is fully manageable via a local web based Graphical User Interface (GUI) or via the **Common Management Platform** (CMP) as a single network element on the inside LAN network, making it easy to manage together with the other OpenScape solution components that comprise the Enterprise Network. OpenScape SBC also supports a local management via a web based Graphical User Interface (GUI) using HTTPS.
- The OpenScape SBC currently shares common support tools with OpenScape Branch.
- **OpenScape SBC** can be deployed within a trusted network, to untrusted networks or a mixed deployment can be used. In a trusted network all VoIP users are within the trusted Enterprise network. When interfacing to untrusted networks an Internal OpenScape SBC Firewall/NAT is used when providing VoIP service to users outside the trusted Enterprise WAN. A separate Firewall is required to support non-VoIP access, e.g., management and billing.
- A single **OpenScape SBC** can communicate to one OpenScape UC server. Multiple OpenScape SBCs can be configured to provide increased capacity as long as the SBC traffic is split e.g., a separate SBC for two different SIP Trunk Service Providers.
- The OpenScape SBC is offered on three **HW platforms** allowing a maximum SBC session capacity of up to 32,000 (32K) SBC sessions at a call rate of 105+ cps using any valid scenario.

NOTICE: Please note that number of concurrent SBC sessions required is based on many factors but not limited to

the number of remote users, SIP trunking and OpenScape Branches.

IMPORTANT: Performance and capacity vary by signaling protocol, call flow, codec, configuration and feature usage.

- An **SBC Session** is defined as an active SIP call connection that is being managed and processed by the OpenScape Session Border Controller. Each SIP call connection may be consisting of the SIP signaling packets only (when media packets are being routed between the endpoints), or when both SIP signaling and media packets being handled through the OpenScape Session Border Controller.
- **OpenScape SBC** supports several redundancy scenarios based on the deployment of OpenScape Voice and data centers in the customers network. SBC redundancy can be applied to simplex OpenScape Voice systems and Co-located Duplex OpenScape Voice systems.

NOTICE: SBC does not have the ability to block incoming calls based on the calling party number.

Software Licensing

OpenScape SBC deployment requires licensing of the product. A CAPEX licensing model and OPEX mode is used for Enterprise and hosted environments.

1) CAPEX Licensing

CAPEX licensing is used for Enterprise environments where the customer owns the licenses and does not wish to lease the licenses on a monthly basis. The following license type are associated with OpenScape SBCs:

- **OpenScape SBC Base**
- **OpenScape SBC Session License** (used for OpenScape Branch and OpenScape SBC)

2) OPEX Licensing

OPEX licensing is used for Enterprise environments where the customer wishes to lease the licenses on a monthly basis and consists of two parts:

- **Product Instance** - The Product Instance is purchased once for each product and consists of all of the licenses necessary to equip a product for its maximum capacity, including all major features. The Product Instance enables the Monthly Subscription Licenses for the OpenScape SBC.
- **Subscription License**-The Subscription License is the monthly charge for a single user to use a single product. If a single user has voice, voice mail and Unified Communications (UC), then they would pay for 3 Subscription Licenses – one for OpenScape Voice, one for OpenScape SBC and one for OpenScape UC. The Subscription Licenses are based upon the product usage that is reported monthly and the billing is calculated on actual service consumption.

3) OpenScape SBC BCF License

BFC licensing is used for Enterprise environments in order to allow Border Control Function (BCF) functionality. By applying the OpenScape SBC BCF

License, the OS-SBC will allow the following Session Licenses depending on the Platform or VM:

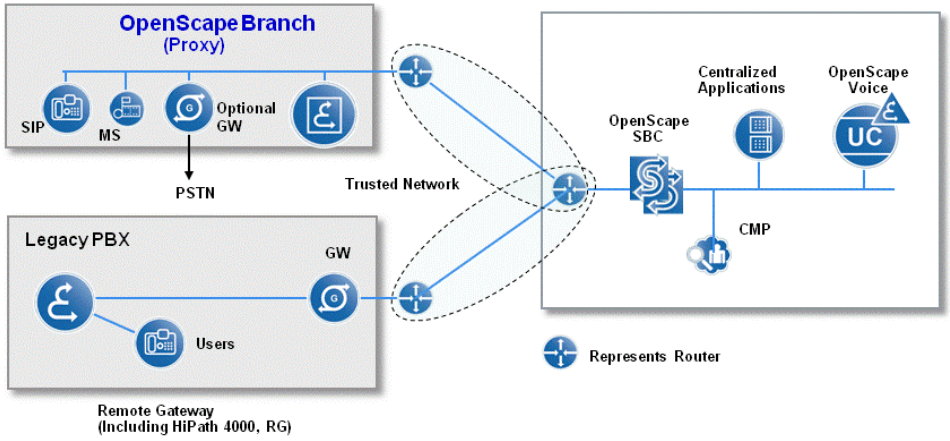
a) OS-SBC 20000 - 20000 SIP-Sessions
b) OS-SBC 6000 - 6000 SIP-Sessions

Starting with OpenScape Branch V9 and OpenScape SBC V9, new features can also be licensed in addition to those provided by the licensing model in use. The new feature may be licensed individually or based on the license version. The software version by itself no longer controls the activation of features. The activation from now on is controlled by the system base license. The system base license has some categories of licensed features:

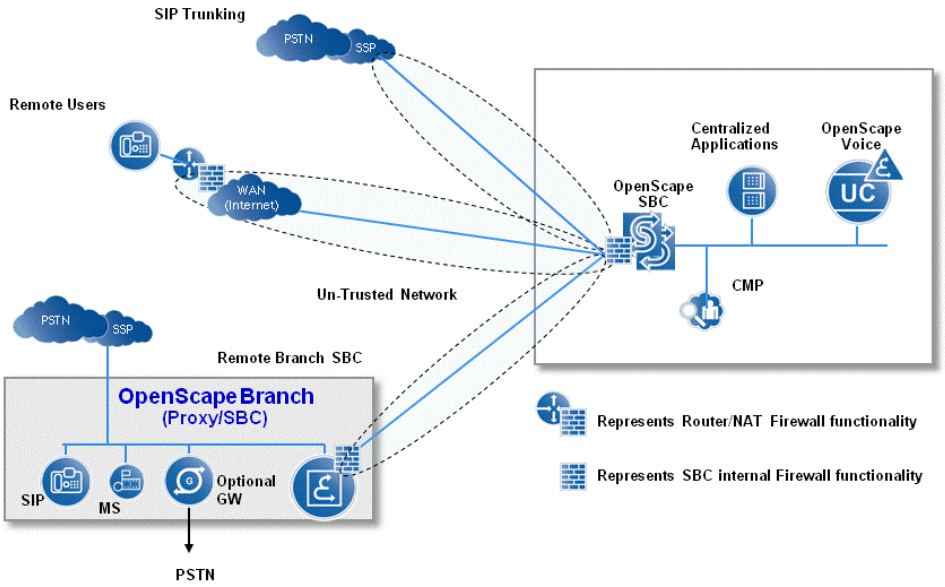
- **Base-License Version independent Features (freebies)** - A feature is available for use independently of the detected Base License Version.
- **Base-License Version dependent Feature** - The feature is available for use only for a specific Base License Version, e.g. MOH Streaming requires a V9 or higher Base-License.
- **Licensed Feature** - Features based on a special License, e.g. Voice mail requires a special Voice mail License.

OpenScape SBC in the Network

The figure below shows deployment in a trusted network with the SBC connected directly to the WAN. This deployment is possible for scenarios where all VoIP users are within a trusted Enterprise Network.



The figure below shows deployment in an untrusted network with the SBC behind an IT Firewall/NAT. This deployment is typically required by customers when providing VoIP service to users outside the trusted Enterprise WAN.



A mixed deployment can be used, with VoIP via the Internet or other service providers' networks connecting via the internal Firewall, and user within the Enterprise WAN connecting directly to the WAN side of the SBC.

OpenScape SBC Signaling Transport - Overview

OpenScape SBC supports signaling transport using TCP and transport signaling security using Mutual Authentication TLS (MTLS) and Server Authentication TLS (TLS). The following signaling transport and signaling transport security configurations are supported in the network between OpenScape and SBC networks.

Access/Peer	Core	Comments
TCP	TCP	Supported
TCP	MTLS	Supported
TLS	MTLS	Supported
TLS	TCP	Not Supported (V1)
TLS	TCP	Supported (V2)
MTLS	TLS	Supported (V2)
MTLS	MTLS	Supported (V2)

Signaling and Media Transport Protocol

OpenScape SBC - supports the following SIP signaling and media transport protocols.

Deployment Scenario	Pass-through or Termination	SIP Signaling Transport		Media Transport	
		Core	Access	Core	Access
SIP Trunking	Pass-through	TCP or UDP	TCP or UDP	RTP	RTP
		TLS *	TLS *	SRTP *	SRTP *
	Termination	TLS *	TCP * or UDP *	SRTP *	RTP *

Deployment Scenario	Pass-through or Termination	SIP Signaling Transport		Media Transport	
		Core	Access	Core	Access
		TCP	TLS	RTP	SRTP (Mikey0 or SDES)
Remote User and OpenScape Branch	Pass-through	TCP, TLS or UDP *	TCP, TLS or UDP *	RTP	RTP
		TLS	TLS	SRTP Mikey0	SRTP Mikey0
		TLS	TLS	SRTP SDES	SRTP SDES
		TLS	TLS	SRTP SDES	SRTP Mikey0
		TLS	TLS	SRTP Mikey0	SRTP SDES
	Termination	TCP *	TLS *	RTP *	SRTP (Mikey0 or SDES) *
		TLS *	TCP *, TLS* or UDP *	SRTP (Mikey0 or SDES) *	RTP *
Remote Standalone SIP-Q Gateway	Pass-through	TCP*	TCP*	RTP*	RTP*
	Termination	TCP*	TLS*	RTP*	SRTP* (Mikey0)

IMPORTANT: Use of TLS or TCP is highly recommended over UDP.

NOTICE: Best effort scenarios could be downgraded to RTP on either side.

NOTICE: Audio and video codecs are negotiated end to end.

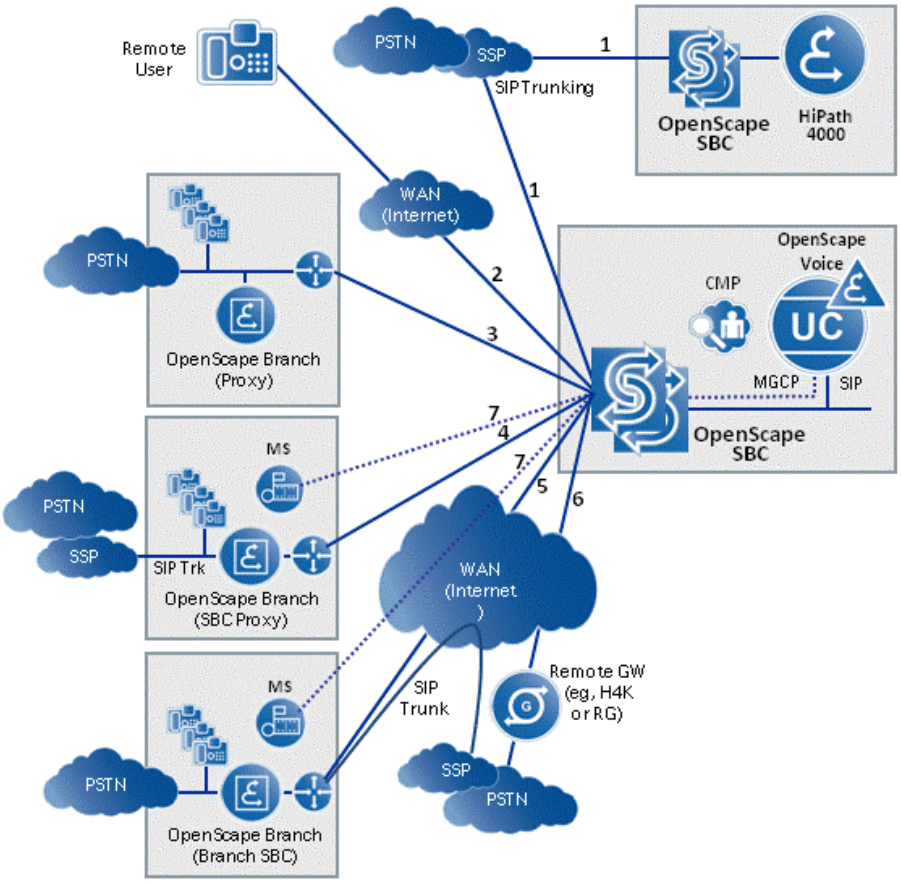
NOTICE: * Indicates not supported in OpenScape SBC V1

Media “pass-through” refers to OpenScape SBC V1 handling of the media packet payload whereby the unencrypted RTP or encrypted SRTP data that are received from the connected endpoints are relayed through the SBC without modification. OpenScape SBC does not play a role in reformatting of the actual media payload so the media format, including negotiation of codec and encryption is performed between the media endpoints. This implementation allows for SRTP media encryption to be realized across the entire end-to-end path of the media connection, assuming that the connected endpoints support SRTP using a compatible key management protocol.

Audio and video codecs are negotiated end-to-end. OpenScape SBC support of codec transcoding is planned for a future release.

Deployment Scenarios — Overview

OpenScape Session Border Controller deployment in the OpenScape Voice environment is supported in a centralized location only, that is in the same location as the OpenScape UC server (e.g., in the customer's Data Center) for the following deployment scenarios.



1) SIP Trunking to a SIP Service Provider (SSP)

- Provides secure connection of OpenScape Voice and OpenScape 4000 IP telephony solution to carrier-based SIP trunking services that provide access to the Public Switched Telephone Network (PSTN).
- OpenScape SBC also provides for compatibility with the SIP signaling variations support by various SSPs.
- Used also for private SIP trunking connections between Enterprise VoIP Networks.

2) Remote User (e.g. home worker)

- Provides secure remote user access to the IP telephony infrastructure of an OpenScape Voice system for SIP phones regardless of location.
- Supports the necessary near-end and far-end Network Address Translation (NAT) traversal functions for connection using public IP addresses via the Internet. OpenScape SBC can be installed behind an external near-end NAT/firewall, for example, inside the customer's DMZ.

OpenScape SBC can also support remote users that are installed behind a far-end NAT/firewall.

- Symmetric Response Routing is used by OpenScape SBC to dynamically detect the SIP signaling IP address/port of a remote user behind a far-end NAT which is used to send SIP responses. Symmetric RTP is used similarly for the media payload.
- All OpenScape Voice SIP subscriber features are supported by OpenScape SBC for a Remote User.

3) **Remote OpenScape Branch (Proxy)**

- Facilitates the connection of remote branch offices that use OpenScape Branch operating in proxy mode connected with the headquarters via the private enterprise network, and is therefore using the same IP address space.
- OpenScape SBC is usually optional in this configuration since there is typically no NATing to be performed; however, an OpenScape SBC may be used, for example, when the remote OpenScape Branch system that is operating in proxy mode because it is installed behind a DSL router (with a static or dynamic IP address) at the branch office. Use of OpenScape SBC may also be desired for serviceability and/or security reasons in cases when there is no NATing to be performed.

4) **Remote OpenScape Branch (SBC Proxy)**

- Facilitates the connection of remote branch offices that use OpenScape Branch operating in proxy mode connected to the central headquarters via the enterprise network, and is therefore using the same IP address space.
- OpenScape SBC is optional in this configuration since there is no NATing to be performed; however, use of OpenScape SBC may be desired for serviceability and/or security reasons.
- The Remote OpenScape Branch provides secure SBC connection to carrier-based SIP trunking services that provide access to the Public Switched Telephone Network (PSTN).
- The Remote OpenScape Branch also provides SBC functionality for compatibility with the SIP signaling variations support by various SSPs.

5) **Remote OpenScape Branch (Branch SBC)**

- Facilitates the connection of remote branch offices that use OpenScape Branch operating in SBC mode connected to the central headquarters via a WAN, such as an untrusted or public network.
- The OpenScape SBC is required for NATing and security at the data center, as is the integrated SBC in the OpenScape Branch required for NATing and security at the remote branch office. The NAT device serving a branch location must may be configured with either a static or dynamic IP address.
- The Remote OpenScape Branch can provide a secure SBC connection to carrier-based SIP trunking services that provide access to the Public Switched Telephone Network (PSTN).
- Overlapping IP Address Ranges are supported at the different branch offices.

6) **Remote Gateways (not behind OpenScape Branch)**

- Facilitates the connection of remote SIP-Q gateways, such as OpenScape Business, OpenScape 4000, or RG gateways, which are connected to the central headquarters via a WAN, such as an untrusted or public network.

- The OpenScape SBC is required for NATing and security at the data center.

7) **MGCP Signaling support for remote Media Servers**

- Facilitates the connection of a remote branch office that requires services from an external OpenScape Media Server connected to the central headquarters via the enterprise network or WAN. In this case the OpenScape SBC supports the MGCP signaling connection between the OpenScape Media Server located at the branch office and the OpenScape Voice system located at the central headquarters.
- OpenScape SBC is optional when the connection is via a trusted enterprise network and there is no NATing to be performed; however, the SBC may still be desired for serviceability and/or security reasons.

Any combination of the above supported deployment scenarios can be supported using the same OpenScape SBC provided that the IP address(es) of the WAN interface are on a common network for the deployment scenarios that are being used. In cases where the deployment scenarios interface different networks having different IP address space on the SBC's WAN interface (for example, an SSP that delivers SIP trunk services via MPLS and requires the SBC's WAN interface to be assigned a private IP address on the SSP's network together with Remote Users that require a public Internet IP address to access the SBC's WAN interface), multiple OpenScape SBCs would be required; one for each different WAN network. (Workaround: A single OpenScape SBC can be configured to logically separate the one physical OpenScape SBC access interface (eth1) into one or more VLAN 802.1q tagged private networks plus a default public network (not 802.1q VLAN tagged). IP packets on the OpenScape SBC access interface are exchanged via the local external L2 managed switch, which is configured to forward IP messages to specific L2 ports based on the VLAN tag. In the process of forwarding the IP message the VLAN tag may be removed. OpenScape SBC requires that each supported VLAN have a unique (VLAN independent) WAN IP address configured on OpenScape SBC. Each server on the respective VLAN would be required to use this WAN IP address to communicate with the OpenScape SBC).

IMPORTANT: IP packets with the used ports (configured in OSV, SBC, OSB) must be routed transparently in the IP network, meaning that the packets must not be manipulated, e.g. by a firewall. Functional problems can be the result of non-transparent routing.

Untrusted WAN networks for which an SBC is required are:

- Internet
- SIP Service Provider Network
- Extensions of corporate IP networks to remote locations or remote users which the customer's IT organization does not consider sufficiently secure, thus further security measures are necessary for VoIP deployment.

Trusted WAN networks for which an SBC is optional are:

- Virtual Private Networks (VPNs). If OpenScape SBC is used in a trusted WAN network that uses VPNs, since OpenScape SBC can support only a

signal VPN connection, a VPN concentrator must be used on the access side of the OpenScape SBC.

- Extensions of corporate IP networks to remote locations or remote users which the customer's IT organization does consider sufficiently secure, thus either no further security measures are necessary or there are limited select security considerations.

Multiple OpenScape SBCs can be deployed on a single OpenScape Voice system; however, routing of traffic to the desired SBC is static based upon the system and user configuration. Multiple OpenScape SBCs can be used in projects that have SBC capacity requirement that exceed the capacity limits of a single OpenScape SBC.

A single OpenScape SBC can serve multiple OpenScape Voice systems. Clustered Mode is also applicable to OpenScape Voice systems.

An OpenScape SBC can be deployed in a single-server configuration, or as a redundant server pair (cluster) using a VRRP-like connection for active-standby operation to achieve high availability. For OpenScape SBC redundant servers must be installed on the same subnet.

OpenScape SBC V2 supports co-located and geographically-separated duplex OpenScape Voice systems with SBCs running in either active-standby mode or active-active mode.

OpenScape SBC is designed as a border element that sits between two different IP networks and therefore requires separate interfaces be used for the access-side (WAN) and core-side (LAN) connections. Connecting OpenScape SBC using a single interface, which would require both the access-side (WAN) and core-side (LAN) to be on the same IP network, is not supported.

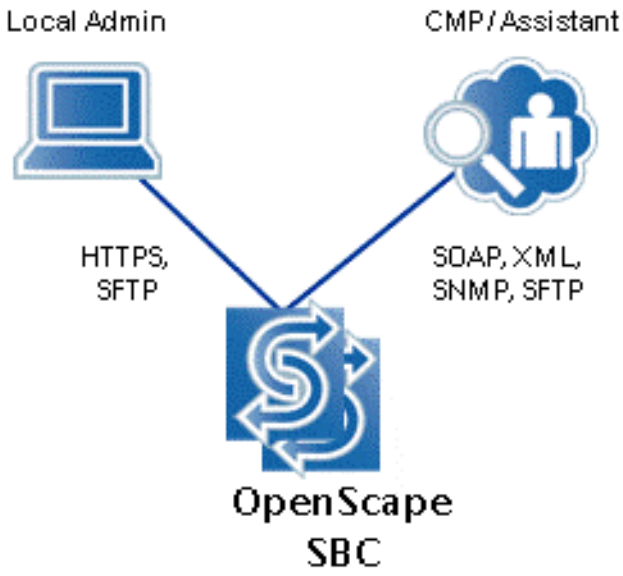
While the preferred installation approach is to use OpenScape SBC as the VoIP firewall on the WAN (access side) boundary of the data center in parallel with the customer's data firewall, OpenScape SBC can be installed (behind) the data firewall (i.e., in the customer's DMZ).

Management

OpenScape SBC can be managed centrally by the Common Management Platform (CMP) using SOAP and XML, using the OpenScape SBC Assistant. It also supports a local management via a web based Graphical User Interface (GUI) using HTTPS.

Alarms are supported via SNMP traps to the CMP / Assistant.

OpenScape SBC supports secure file handling when transferring files using the Secure File Transfer Protocol (SFTP).



NOTICE: DLS uses the customer's data network to manage OpenStage phones. For remote OpenStage phones that access OpenScape Voice via OpenScape SBC, the DLS traffic is not routed through the OpenScape SBC, but rather through the customer's data firewall. If the remote users are behind a NAT/ Firewall then the DLS/phones have to use a 'Contact Me Proxy' to allow DLS to manage the phones.

Redundancy

There are various options for deploying redundancy based on the customers network, location of data centers and number of data centers. The basic configurations for redundancy are:

- SBC Server Redundancy on the same Subnet (SBC Luster) ->(SBC Cluster)
- SBC Redundancy support for L3 geographically-separated OpenScape Voice nodes.

OpenScape Session Border Controller Redundancy Support

Redundant OpenScape SBC configurations provide VIP address failover for both LAN network and WAN addresses.

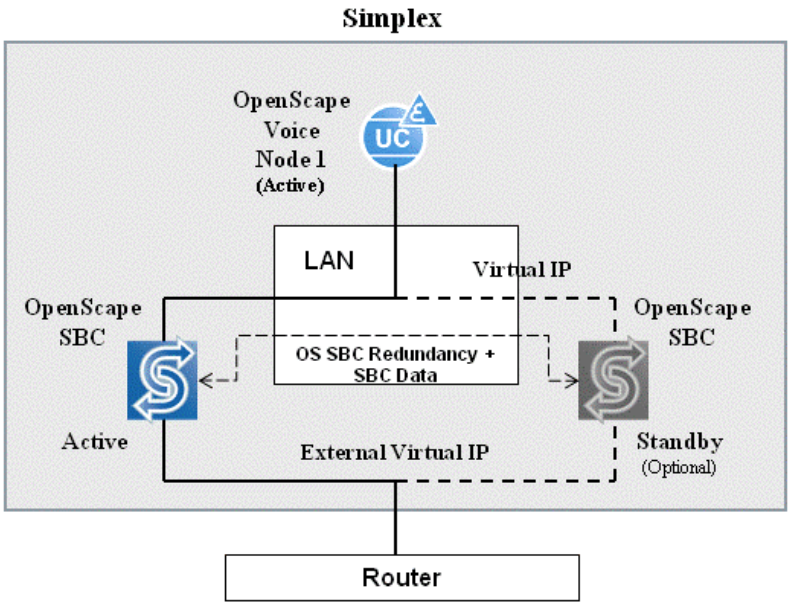
Periodic heartbeats are sent by the Standby OpenScape SBC node to detect failover conditions. Either OpenScape SBC node may assume active or standby mode at any time, however only one node shall be in an active operation mode.

When the redundant OpenScape SBC nodes share the same sub-net for the inside network additional data is synchronized in near real-time between the OpenScape SBC nodes to allow continued operation when the standby OpenScape SBC node must assume an active OpenScape SBC node status. The synchronization data includes for example:

- Configuration changes
- Media port mappings for sessions traversing the SBC.

- IP addresses and ports used for established TCP connections
- TLS session handles using TCP connections
- Updates to any current SIP registration bindings

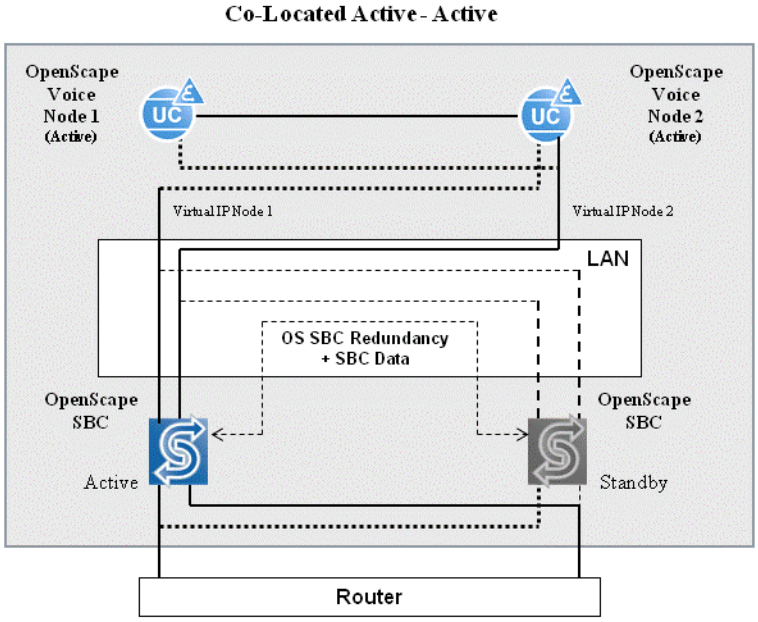
Simplex OpenScape Voice (OSV)



The OpenScape SBC does not require any special functionality to interface with a simplex OpenScape Voice (OSV). All SIP requests and responses are received at a single outside/ WAN interface of the OpenScape SBC and are relayed to a single OSV IP address. The OpenScape SBC is configured with Comm. System Type = Simplex.

An optional second OpenScape SBC can be used to provide a redundant SBC cluster if necessary although as OSV itself has no redundancy in this configuration.

Duplex co-located OpenScape Voice (OSV)



When OpenScape Voice (OSV) is operating in duplex mode, end devices communicate with both nodes of the duplex OSV configuration, requiring the OS SBC cluster support 2 Virtual IP (VIP) addresses, one for each OSV node. For each OSV, an SBC inside VIP address associated with an outside VIP address is needed. Endpoint devices must be configured with one of the outside network VIP's as their SIP Server / SIP Registrar, distributed to provide a balance OSV load.

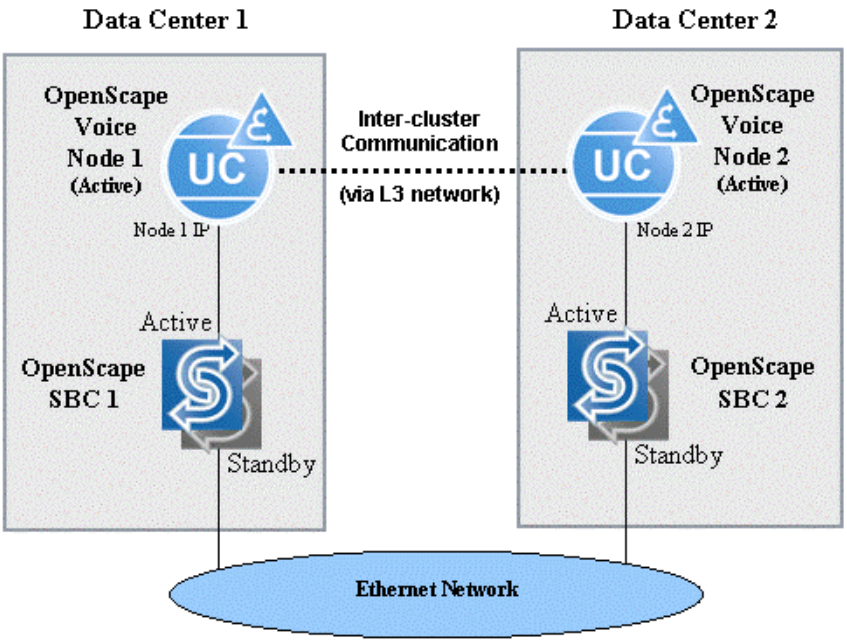
SBC redundancy is only available in an active-standby mode.

OS SBC node failover handling requires that both VIP address pairs (external and internal OSV bindings) are taken over or assumed by the OS SBC Standby Node.

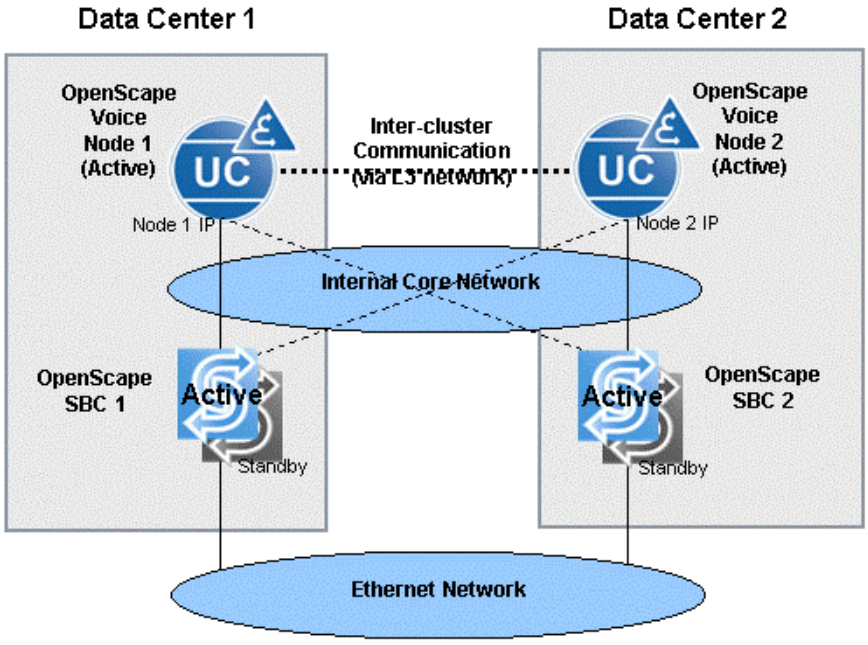
In this non-geographically separated configuration, OSV failures are transparent to the OS SBC since an OSV node failure leads to the partner OSV node taking over the internal VIP address of the failed OSV node assuming both inside network VIP addresses.

In the Active-Active OSV configuration, the OS SBC is configured with Comm. System Type = Collocated.

OpenScape Voice (OSV) L3 Geographically Separated Redundancy



OpenScape Voice Geographically Separated Redundancy (no internal core network)



OpenScape Voice Geographically Separated Redundancy (with internal core network)

In addition to the OpenScape SBC redundancy on the same subnet for support of co-located OpenScape Voice redundant nodes, this feature provides support

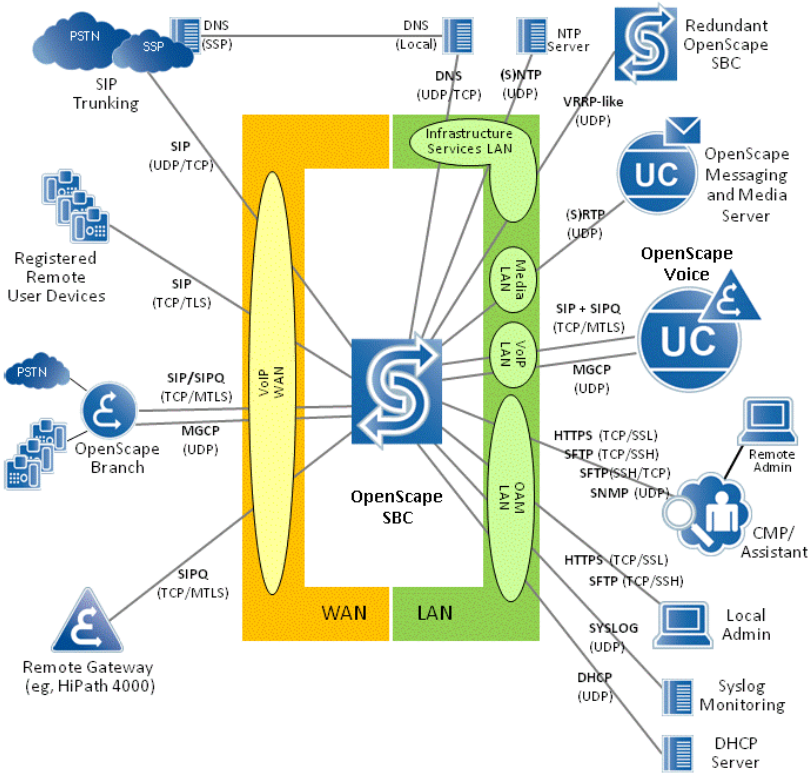
for OpenScape Voice redundancy of geographically separated nodes that are on separate subnets. A Layer 3 (L3) connection is used to exchange call state information between the geographically separated OpenScape SBCs.

At least two OpenScape SBC servers (one at each data center) are required to support OpenScape Voice geographically separated redundancy. Four OpenScape SBC servers are required (two at each data center) in case server redundancy at each data center is also required.

Unlike OpenScape SBC redundancy on the same subnet where a common set of SBC Session Licenses can be shared between the Active and Standby servers, OpenScape SBCs that are L3 geographically separated are counted as separate systems for purposes of SBC Session Licenses. In other words, a separate set of SBC Session Licenses need to be used for the OpenScape SBC system that are geographically separated.

Protocols

OpenScape SBC supports multiple protocols. The diagram below illustrates their usage in the network.



Security Certification

OpenScape SBC is rated Certified Secure by Miercom Independent Testing Labs. The Certified Secure rating is valid for a two-year period while advancements in both security countermeasures and vulnerability exploits continue to be monitored.

Certified Secure testing involves subjecting the product to a rigorous battery of vulnerability analyses and scans as well as a complex set of exploits designed by a team of experienced security professionals.

Miercom performed attacks as an outside attacker would, within the constraints of the test environment. The approach and methodology utilized in this test is based on knowledge that Miercom, in collaboration with leading security experts, has collected over several years through its work in VoIP pre- and post-deployment site surveys and security assessments, as it uses in testing other vendors SBC products.

1.3 Navigation

The OpenScape SBC administration within the Common Management Platform is used to administer OpenScape SBCs.

OpenScape Common Management Platform

The primary navigation areas in the Common Management Platform are the Function Tabs, System Bar, Navigation Bar, Navigation Tree and Work Area

OpenScape Common Management Platform Overview

- **Function Tabs**

  Located in the Common Management Platform initial window, these tabs provide access to **Configuration**, **Maintenance**, **User Management**, **Fault Management**, **Performance Management** and **Accounting** functions.
- **System Bar**

  Located in the **Configuration** function window upper most location includes access to administer products, **OpenScape Voice**, **OpenScape Branch**, **OpenScape SBC**, **RG8700**, **Unified Communications**, **CMP** and **Device Management**.
- **Navigation Bar**

  Locate just below the System Bar, contains navigation tabs which provides access to menu items and menu options base on the navigation tab selected.
- **Navigation Tree**

  Located on the left side, opens topics belonging to the selected navigation menu option in the Work Area.
- **Work Area**

  Located on the right side, lists comprehensive information and displays different activity options. Information and actions are displayed above the listed items in the Work Area.

OpenScape SBC Administration

OpenScape SBC administration is used to administer OpenScape SBCs. It presents the following items in the Navigation Bar and Tree under **OpenScape SBC**.

Administration

This section of the Navigation Tree is used for configuring OpenScape Branch Offices and OpenScape Session Border Controllers.

- **Job Management**

  Menu items to manage mass scheduled software upgrades.

- **Licensing**

  Drop-down-list to select **Licensing List** and **Licensing thresholds** information. SBCs and branch offices licensing information appear in the Work Area.
- **Communication System**

  Drop-down-list to select **All systems** or a particular communication system. SBCs servers associated with the selected communications system appear in the Work Area.
- **OpenScape SBC list**

  Select **OpenScape SBC list** to display and refresh OpenScape SBC information for the selected Communication System. SBCs servers for the preselected Communications System will appear in the Work Area.
- **Select OpenScape SBC**

  The drop-down-list is used to select a particular SBC server. The Licensing Information for the selected SBC appears in the Work Area.
- **Management**

  Used to manage a selected SBC server.
- **Configuration**

  Menu items to configure particular **OpenScape SBC** devices.

  – **Local Dashboard**
  – **System**
  – **Network/Net Services**
  – **VoIP**
  – **Features**
  – **Security**
  – **Diagnostics & Logs**
  – **Alarms**
  – **Maintenance**

2 OpenScape SBC Assistant – Primary Administration

The steps on the primary administration level deal with general administrative tasks.

General Administrative Tasks

Primary administration comprises the following tasks:

- Viewing and updating Session Border Controller Status.
- Creating or selecting a Session Border Controller.
- Saving changes.
- Changing the password in the local Assistant´s database.

NOTICE: The OpenScape SBC Assistant is used to display and configure OpenScape Session Border Controllers. The online Help system may describe features that are not available for earlier versions OpenScape Session Border Controller and some procedures may deviate from the ones described.

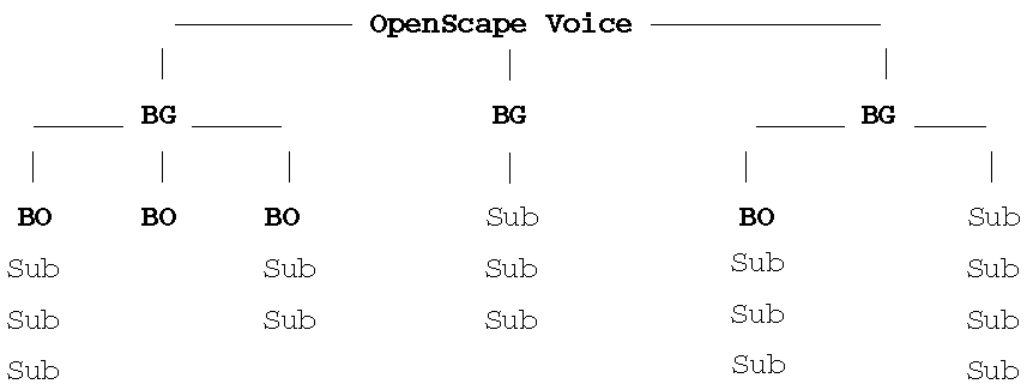
2.1 Business Groups and Branch Offices

The relationship between Business Groups (BG) and, Session Border Controllers (SBC) and Branch Offices (BO) within OpenScape Voice is characterized by the following properties:

- One BG can have zero or more BOs.
- One BO always belongs to a BG.
- A BG can have many subscribers (Sub).
- A BO can have many subscribers.

  Subscribers of a BO that belongs to a BG are still considered subscribers of the BG as well as subscribers of the BO.

  For instance, intra-BG feature transparency (such as calling name delivery) applies for subscribers belonging to different BOs of a given BG.
- Subscribers always belong to a BG.
- Subscribers do not always belong to a BO.



2.2 How to Add or Delete an OpenScape SBC to OpenScape SBC Assistant

Proceed as follows to add an OpenScape SBC to OpenScape SBC Assistant:

Prerequisites

Adequate administrative permissions.

The connection to the OpenScape Voice system is up.

Step by Step

1) Navigate to **Configuration tab** and select **OpenScape SBC** within the Navigation Bar in the Common Management Platform.

2) Select the **OpenScape SBC list** in the Navigation Tree under Administration.

The system presents the **OpenScape SBC Overview** in the Work Area with a current list of all SBCs.

3) Proceed as follows to assign a new OpenScape SBC:

a) Click the **Add...** button.

The **Add OpenScape SBC** dialog is displayed.

b) Select the associated **Comm System** by clicking the "**...**" button and selecting a Comm system from the **Comm Systems** dialog.

c) Click to **OK** key to save the Comm System.

The **Add OpenScape SBC** dialog is re-displayed and the Comm System information is shown.

d) Select the associated **Business Group** by clicking the "**...**" button and selecting a Business Group from the **Business groups** dialog.

e) Click to **OK** key to save the Business Group.

The **Add OpenScape SBC** dialog is re-displayed and the Business Group information is shown.

f) Select the associated **Endpoint** by clicking the "**...**" button and selecting a Endpoint from the **Endpoint** dialog.

The following fields are populated:

The associated OpenScape SBC Name in the **Central SBC Name** field

The associated OpenScape SBC IP Address in the **IP Address** field

g) The **Communicating over Secured channel** checkbox indicates the status of the OpenScape SBC device. When "unsecured" (unchecked) allows the OpenScape SBC (identified by logical ID) to request an authentication statement. The checkbox is set to unchecked and grayed out by default when the OpenScape SBC is first added to the OpenScape SBC Assistant. Once the OpenScape SBC requests an authorization statement and theOpenScape SBC Assistant sends the authorization statement; the checkbox is automatically checked and the OpenScape SBC is placed in Secured Mode (the **Security status** is updated to **Secured Mode**).

NOTICE: Communicating over Secured channel checkbox must be unchecked to reinstall an OpenScape

SBC using simplified installation. Unchecking the checkbox will revoke the current authentication statement and allow the OpenScape SBC to request a new authentication statement.

h) Click to **OK** key to save the Endpoint.

The **Add OpenScape SBC** dialog is re-displayed and the Endpoint information is shown.

i) Click to **OK** key to save the Endpoint.

The **Add OpenScape SBC** dialog is closed and the **OpenScape SBC Overview** is displayed with the new SBC.

The OpenScape SBC Assistant is able to administer the added OpenScape SBC.

4) Proceed as follows to remove an existing branch office from the list:

a) Select the OpenScape SBC from the **OpenScape SBC Overview** work area by checking the associated checkbox.

b) Click the **Delete** button in the work area.

The corresponding record will be deleted from the OpenScape SBC Assistant's database.

2.3 How to Display an OpenScape SBC Via OpenScape SBC Assistant

The OpenScape SBC Assistant can administer OpenScape Session Border Controllers. Thus it keeps a list of SBCs in its database. The "OpenScape SBC Overview" form displays all known SBCs and provides a search function to find a particular appliance.

Prerequisites

Adequate administrative permissions.

At least one SBC is configured and in operation.

The connection to the OpenScape Voice system is up.

Step by Step

1) To display all SBCs: Navigate to **Configuration tab** > **OpenScape SBC** within the Navigation Bar in the Common Management Platform.

2) Select **All systems** in the Communication System pull-down under **Administration** in the Navigation Tree (if not currently selected).

3) Select **OpenScape SBC list** in the **Administration** Navigation Tree area.

The system presents the **OpenScape SBC Overview** in the Work Area, with a current list of all known SBCs. If no SBCs are defined, the list is empty.

4) To view a list of SBCs configured for a specific communication system, select the desired communication system under the Communication System pull-down field under **Administration** in the Navigation Tree.

The list of SBCs for the selected **Communication System** is displayed in the **OpenScape SBC Overview** Work Area.

5) To find and select a particular SBC, use one of the following options:

- In the Work Area select the checkbox to the left of the desired SBC in the list. The following Action Menu buttons are set active in the Work Area:
  - **Manage**, **Password...**, **Refresh Selected**, **Refresh All**, Add..., **Edit...**, **Delete**

  Selecting the **Manage** button replaces the **OpenScape SBC Overview** work area with the selected SBC, and displays relevant information and data in the Work Area.
- Choose a SBC from the **OpenScape SBC** pull-down located in the Navigation Tree.

  Relevant Information and data is displayed in the Work Area for the selected SBC.
- Enter filter search criteria to filter the list of SBC.

  Filtering is possible on the following criteria in the **for** field: **OpenScape SBC**, **Business Group, IP Address, Version, Status.**

  NOTICE: Wild cards are supported (* for 0 or more characters, "?" for single characters).

  - Once the filters are set, click the **Go** button.

    The system refreshes the list of SBCs, and displays the ones matching the search criteria.
  - The system clears the filter criteria field when the **Clear** button is selected, and displays all records of the default communication system selected in the **Communication System** field. If no specific communication system was selected, all SBCs are listed in the Work Area.

The data displayed is provided by the OpenScape SBC assistant database rather than the hardware itself. This means that the data might be out of date if it was changed on the SBC without the assistant being notified.

2.4 How to Update SBC Status

The information for one particular SBC or all SBCs stored in the database can be updated.

Prerequisites

Adequate administrative permissions.

At least one SBC is configured.

The connection to the OpenScape Voice system is up.

Step by Step

1) To display all SBCs: Navigate to **Configuration tab** > **OpenScape SBC** within the Navigation Bar in the Common Management Platform.

2) Select **All systems** in the Communication System pull-down under **Administration** in the Navigation Tree (if not currently selected).
3) Select **OpenScape SBC list** in the **Administration** Navigation Tree area.

   The system displays the **OpenScape SBC Overview** in the Work Area, with a current list of all known SBCs. If no SBCs are defined, the list is empty.

   The following values are displayed in the **Status** column of the OpenScape SBC Overview work area:

   - **Inventory** - Indicates the OpenScape SBC system is configured in the Assistant but not installed.
   - **Authenticated** – Indicates the OpenScape SBC platform has contacted the OpenScape SBC Assistant with all appropriate credentials.
   - **Installation started** – Indicates that the OpenScape SBC has all the data necessary and started the installation process.
   - **File Transfer Started** - Indicates that the File Transfer has been started by the OpenScape SBC.
   - **File Transfer Successful**.
   - **File Transfer failed**: <filename>-<HttpErrorCode> - Indicates that one of the file transfers has failed (error log file only).
   - **Booting** - Indicates the Boot of the OpenScape SBC has started.
   - **Boot Failed** - Indicates that the OpenScape SBC failed to come up after the boot. No communication is possible.
   - **Normal/Survival** - The appliance has successfully been installed and ready for the call handling.
   - **Unknown** - The Operational state is not available when the SBC is a Backup Node of a Redundancy System.The Master & Redundant Nodes are in Normal or Survival state and the Backup (standby) proxy mode remains in "Unknown" state. The "Unknown" state is due to Standby mode (Redundancy SBCs) and because the Operational state is not available for the Backup Node.
   - **Unreachable** – check alarms.
4) To update all SBCs click the **Refresh All** button.

   The system contacts all SBCs that are visible or invisible in the list and refreshes its internal information.

   NOTICE: This may cause a delay time depending on the number of SBCs configured.

5) To update particular SBCs, check the respective SBC checkboxes in the list or use the filter fields to limit the number of displayed SBCs.
   a) Click The **Refresh Selected** button.

      The internal information of the SBCs checked is updated.

      NOTICE: This may cause a delay time depending on the number of SBCs configured.

2.5 How to Change the Password in the Local Assistant Database

After an update or a missed synchronization of the password, the administrator can set the SOAP (Simple Object Access Protocol) password in the assistant's database as follows:

Prerequisites

Adequate administrative permissions.

At least one SBC is configured and in operation.

The connection to the OpenScape Voice system is up.

Step by Step

1) To display all SBCs and branch offices: Navigate to **Configuration tab** > **OpenScape SBC** within the Navigation Bar in the Common Management Platform.

2) Select **All systems** in the Communication System pull-down under **Administration** in the Navigation Tree (if not currently selected).

3) Select **OpenScape SBC list** in the **Administration** Navigation Tree area.

The system presents the **OpenScape SBC Overview** in the Work Area, with a current list of all known SBCs. If no SBCs are defined, the list is empty.

4) Choose an OpenScape SBC by checking a checkbox, to the left of the particular SBC in the OpenScape SBC Office List.

5) Click the **Password...** button.

The **Password** dialog appears.

6) In the **Password** dialog panel, proceed as follows:

a) Select a user identification in the **User** selection list.

b) Enter the new password in the **New password** and **Confirm new password** fields. The password must be 8...36 characters.

NOTICE:

The users and their default passwords are referenced in OpenScape SBC Configuration Guide.

---

c) In most cases the new password change applies to both the OpenScape SBC Assistant and the SBC appliance, and the user must continue with the substeps defined below. Otherwise, when the new password is meant only for the OpenScape SBC Assistant, skip the substeps below and continue with Step 7.

d) Check the **Update password on appliance** checkbox.

e) Enter the **Current appliance password**.

NOTICE: This is the SBC appliance password, which must match the OpenScape SBC assistant password. Otherwise, the SBC assistant password must be changed to match the SBC appliance, and then both can be changed from the assistant.

---

7) Click the **Change** button to set the new password or click the **Reset** button to reset the password to default.

> **NOTICE:** The Reset applies only to the OpenScape SBC assistant, not the SBC appliance.

A confirmation message is displayed.

8) Click the **Close** button.

The password is changed in the database of the OpenScape SBC Assistant and the OpenScape SBC appliance,

Related concepts

Password Management on page 67

Related tasks

How to Change or Reset the Password on page 232

3 OpenScape SBC Assistant – Maintenance

This section provides information about system monitoring and maintenance and enables the administrator to perform various service and maintenance tasks.

OpenScape SBC Assistant Online Help

The OpenScape SBC Assistant can be used to display and configure OpenScape Session Border Controllers. The online Help system may describe features that are not available for older versions of OpenScape SBC and some procedures may deviate from the ones described.

3.1 System Information and Monitoring

Aggregated information on an OpenScape Session Border Controller can be displayed via the Common Management Platform (CMP).

3.1.1 The OpenScape SBC Dashboard via CMP

The **Dashboard** view of an OpenScape Session Border Controller can be displayed via the Common Management Platform. It provides a variety of performance and system information. Several sub-windows provide advanced information.

The dashboard view suits for the administrator as well as for the service technician to get a quick and global overview of the selected SBC.

Alarm summary:

The following information is provided:

- Number of critical alarms.
- Number of major alarms.
- Number of minor alarms.

The administrator can view a list with the current alarms. The following information is displayed:

- Alarm ID:

  ID that uniquely identifies an alarm e.g., 757, 1478 (numeric).
- 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).

- Managed Resource:

  Alarm source ID. Describes the entity that has generated the alarm. This is either a Fault Handler or an SNMP (Simple Network Management Protocol) Trap Receiver (which makes the connection to the OpenScape SBC). The entity is referenced by a GUID (Global Unique Identifier). This GUID can be used to identify the alarm source in the system management.
- Alarm Type:

  Alarm classification e.g., OpenBranchAlarm0512: Spontaneous Alarm from the managed network element.
- Last Occurred:

  Date and time when this alarm last occurred e.g., 2011/06/01 04:12:23.
- Acknowledged Status:

  This field shows whether the administrator has confirmed the alarm or not. The value is **false** if the alarm has not been acknowledged.
- User:

  Name or ID of the user associated with the alarm. If the alarm is unconfirmed the display remains empty.
- Hit Count:

  Number of times this alarm has occurred.

For each alarm a detailed description can be displayed within a sub-window.

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.
- **Disk Usage**

  This displays the percentage of disk usage - a snapshot information for a small period of time. 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".
- **Hostname**:

  This field shows the node name. The name is defined in the node.cfg file and set during a full installation.

- **Operating System**:

  The operating system and its software version used for the selected SBC or branch office of the OpenScape Branch type.
- **Hardware Type**:

  The hardware type used for OpenScape SBC or Branch.

Status

The system presents the following status information:

- **Operational Status**:

  Shows the system connectivity with the OpenScape Voice server. "Normal" indicates full connectivity to primary and/or secondary server. "Survivability" indicates no connection to the server. A transition to survivable mode goes from: "normal" mode to "transition" mode to "survivable" mode. The proxy remains in "transition" state N times "OPTIONS interval" seconds where N is the "Transition Mode threshold" (see also "Timers & Thresholds" configuration).
- **Redundancy State**:

  When Redundancy is enabled, Redundancy state shows the status.

  The state "MASTER" indicates that the system is the current active system.

  The state "BACKUP" indicates that the system is in a standby mode (all services are disabled).

  The state "FAULT" indicates that there is no network connectivity.
- **Primary** and **Backup** Server:

  These boxes present the addresses or FQDN of the central SIP Servers, the green/red box associated indicates the state of the server.
- **Penalty Box State**

  These boxes represent the state of the central SIP servers, "NotRunning" is the state reported when the survivability provider is not running, "In Penalty Box" is presented when the OpenScape SBC or Branch lost the connection with SIP server. "Active" represents full connectivity with the SIP server. "Transition" is presented when OpenScape SBC or Branch detects a connectivity problem with the SIP Server. "OK" represents the state where the binding has lower priority than the currently active binding.

Applications

The application name and the software version are displayed.

Actions

The "Actions" sections provides buttons to display advanced information or allows to start an health check. The following options appear:

- Start Rapidstat.
- Show Software Version (current or backup).
- Show Service status.
- Display log files.

3.1.1.1 How to Display the OpenScape SBC Dashboard via CMP

The OpenScape SBC Assistant displays aggregated information and data for the selected Session Border Controller in the "Dashboard View" via the Common Management Platform.

Prerequisites

Adequate administrative permissions.

At least one SBC is configured and in operation.

The connection to the OpenScape Voice system is up.

Step by Step

1) Navigate to **Maintenance** > **Inventory** > **Nodes**

The system presents the list of nodes with a current list of all known systems of all kinds.

2) Select a node of the OpenScape SBC type:

a) Select **OpenScape SBC** in the **in** Drop-down field to filter the list for OpenScape SBC nodes.

b) Click the **Search** button.

c) Click the name of the desired Open Scape SBC in the list.

The system presents the **Dashboard** view of the selected node.

3.1.1.2 How to Display Active Alarms

Perform the following steps to display active alarms of a particular OpenScape Session Border Controller.

Prerequisites

Adequate administrative permissions.

At least one SBC is configured and in operation.

Step by Step

1) Navigate to **Maintenance** > **Inventory** > **Nodes**.

The system presents the list of nodes with a current list of all known systems of all kinds.

2) Select a node of the OpenScape SBC type:

a) Select **OpenScape SBC** in the **in** Drop-down field to filter the list for OpenScape SBC nodes.

b) Click the **Search** button.

c) Click the name of the desired Open Scape SBC in the list.

The system presents the **Dashboard** view of the selected node.

3) Click the **Show Active Alarms** button in the **Alarm Summary** field area. The following information is provided:

- **Alarm ID**:

  ID that uniquely identifies an alarm e.g., 757, 1132 (numeric).
- **Severity**:

  The severity level shows, how critical an alarm is. The following severity levels can be displayed:

  - Critical (red)

  - Major (orange)

  - Minor (yellow)

  - Information (blue)

  - Warning (cyan)

  - Normal (green).
- **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 SBC). The entity is referenced by a GUID (Global Unique Identifier). This GUID can be used to identify the alarm source in the system management.
- **Alarm Type**:

  Alarm classification e.g., [License][License using temporary grace period]
- **Last Occurred**:

  Date and time when this alarm last occurred e.g., 2013/12/17 10:40:40.
- **Acknowledged Status**:

  This field shows whether the administrator has confirmed the alarm or not. The value is false if the alarm has not been acknowledged.
- **User**:

  Name or ID of the user associated with the alarm. If the alarm is unconfirmed the display remains empty.
- **Hit Count**:

  Number of times this alarm has occurred.

The **Active Alarms** window appears displaying a list of alarms for the selected SBC.

Related tasks

How to Display Alarm Details on page 41

How to Start Rapidstat to Perform a Health Check on page 42

How to Display Detailed Version Information on page 43

How to Display the Services Status of an earlier-than-V8 OpenScape SBC on page 45

How to Display, Export and Clear Log Files for an earlier-than-V8 OpenScape SBC on page 47

3.1.1.3 How to Display Alarm Details

Perform the following steps to display details of a specific alarm of a particular OpenScape Session Border Controller.

Prerequisites

Adequate administrative permissions.

At least one SBC is configured and in operation.

Step by Step

1) Navigate to **Maintenance** > **Inventory** > **Nodes**.

   The system presents the list of nodes with a current list of all known systems of all kinds.
2) Select a node of the OpenScape SBC type:
   a) Select **OpenScape SBC** in the **in** Drop-down field to filter the list for OpenScape SBC nodes.
   b) Click the **Search** button.
   c) Click the name of the desired Open Scape SBC in the list.

   The system presents the **Dashboard** view of the selected node.
3) Click the **Show Active Alarms** button in the **Alarm Summary** field area.

   The **Active Alarms** window appears displaying a list of alarms for the selected SBC.
4) Click on the Alarm ID in the list to display details for the corresponding alarm.

   The **Alarm details - <Alarm ID>** window appear with the **General** tab selected by default.
5) To view the alarm description, select the **Description** tab.

Example

Example of an alarm description:

```
neName: C-SBC-65-215
groupId: 7
eventId: 1
eventGroupName: Admin
eventName: Wrong user ID or password entered
severity: 2
eventType: 3
eventTime: 2013-12-17T10:40:40-0500
faultyObject: Authentication
monitoredValue: 1
thresholdValue: 0
neType: csbc
```

Related tasks

How to Display Active Alarms on page 39
How to Start Rapidstat to Perform a Health Check on page 42
How to Display Detailed Version Information on page 43

How to Display the Services Status of an earlier-than-V8 OpenScape SBC on page 45
How to Display, Export and Clear Log Files for an earlier-than-V8 OpenScape SBC on page 47

3.1.1.4 How to Start Rapidstat to Perform a Health Check

The Rapidstat functionality allows to perform a health check for an OpenScape Session Border Controller.

Prerequisites

Adequate administrative permissions.

At least one SBC is configured and in operation.

The connection to the OpenScape SBC is up.

Step by Step

1) Navigate to **Maintenance** > **Inventory** > **Nodes**.

The system presents the list of nodes with a current list of all known systems of all kinds.

2) Select a node of the OpenScape SBC type:

a) Select **OpenScape SBC** in the **in** Drop-down field to filter the list for OpenScape SBC nodes.
b) Click the **Search** button.
c) Click the name of the desired Open Scape SBC in the list.

The system presents the **Dashboard** view of the selected node.

3) In the **Actions** field area, click the CSBC Rapidstat **Start** button.

The **Rapid Stat** dialog appears.

4) Select a Level from the **Rapidstat info level** selection list.

- Level 1 to 5:
  - System configuration, Template files, Boot and system log, Process manager log, Installed packages, CPU (Central Processing Unit) load, Security, SNMP (Simple Network Management Protocol), Memory usage, Disk usage, process status, License Information.
  - Default setting, SIP (Session Initiation Protocol) server logs, B2BUA (Back-to-Back User Agent) logs, SP logs, CDR (Call Detail Recording) logs
  - Message Rate Control and audit logs
  - Management logs
  - Media Server logs (i.e., MS Adapter)

5) Click the **Start** button.

A compressed file is created containing the information and an information window appears. The files can be downloaded to review.

Related tasks

How to Display Active Alarms on page 39

How to Display Alarm Details on page 41
How to Display Detailed Version Information on page 43
How to Display the Services Status of an earlier-than-V8 OpenScape SBC on page 45
How to Display, Export and Clear Log Files for an earlier-than-V8 OpenScape SBC on page 47

3.1.1.5 How to Display Detailed Version Information

The OpenScape SBC Assistant provides detailed information about the software components installed on the system.

Prerequisites

Adequate administrative permissions.

At least one SBC is configured and in operation.

Step by Step

1) Navigate to **Maintenance** > **Inventory** > **Nodes**.

   The system presents the list of nodes with a current list of all known systems of all kinds.
2) Select a node of the OpenScape SBC type:
   a) Select **OpenScape SBC** in the **in** Drop-down field to filter the list for OpenScape SBC nodes.
   b) Click the **Search** button.
   c) Click the name of the desired Open Scape SBC in the list.

   The system presents the **Dashboard** view of the selected node.
3) In the **Actions** field area, click the Version **Show** button.

   The **Version** dialog appears.
4) Select **Current version** or **Backup** from the **Version** selection list in the **Version** field area.
5) Click the **Show** button in the **Version** field area.

The window is refreshed and a detailed version information is displayed.

Example

Example of a detailed version information:

```
-----------------------------------------
- OpenScape SBC version information -
-----------------------------------------
Version            = V8R0.01.00
Internal Version   = oss-08.00.01.00-43
Date               = 2013-Dec-06 11:47:38
WSDL               = Version V6.00.01
Partition          = Second
-----------------------------------------
sw=aaa_base 12.2-2.11.1
```

```
sw=alarm 08.00.01.00-43
```

Related tasks

How to Display Active Alarms on page 39
How to Display Alarm Details on page 41
How to Start Rapidstat to Perform a Health Check on page 42
How to Display the Services Status of an earlier-than-V8 OpenScape SBC on page 45
How to Display, Export and Clear Log Files for an earlier-than-V8 OpenScape SBC on page 47

3.1.1.6 How to Display System Information for OpenScape SBC

Perform the following steps to display system information for an OpenScape Session Border Controller.

Prerequisites

Adequate administrative permissions.

At least one OpenScape Session Border Controller is configured and in operation.

Step by Step

1) Navigate to **Maintenance tab** > **Inventory** > **Nodes**.

   The system presents the list of nodes with a current list of all known systems of all kinds.

2) Select a node of the OpenScape SBC type:
   a) Select **OpenScape SBC** in the **in** Drop-down field to filter the list for OpenScape SBC nodes.
   b) Click the **Search** button.
   c) Click the name of the desired Open Scape SBC in the list.

   The system presents the **Dashboard** view of the selected node.

3) View the **System Info** field area. The following information is provided:

- **CPU:**

  Percentage of CPU processing power used.
- **Memory:**

  Percentage of available memory used.
- **Disk Usage:**

  Percentage of available disk space used.
- **Date/Time:**
- **System Uptime:**

  Time in days hours and minutes the system has been active from the last restart.
- **Hostname:**

  Name given to the server/node for identification.
- **Operating System:**

  OpenScape based operating system e.g., openSUSE 13.
- **Hardware Type:**

  Physical or Virtual hardware type e.g., IBM x3250, x3550 (VM).

The **System Information** is displayed for the selected OpenScape Session Border Controller.

3.1.1.7 How to Display the Services Status of an earlier-than-V8 OpenScape SBC

The current status of the available services of the selected OpenScape Session Border Controller (SBC) can be displayed.

Prerequisites

Adequate administrative permissions.

At least one OpenScape SBC is configured and in operation.

Step by Step

1) Navigate to **Maintenance** > **Inventory** > **Nodes**

   The system presents the list of nodes with a current list of all known systems of all kinds.
2) Select a node of the OpenScape SBC type:
   a) Select **OpenScape SBC** in the **in** Drop-down field to filter the list for OpenScape SBC nodes.
   b) Click the **Search** button.
   c) Click the name of the desired Open Scape SBC in the list.

   The system presents the **Dashboard** view of the selected node.
3) In the **Actions** field area, click the **Services status:** > **Show** button.

   The **Services Status** window appears.

The current status (not running, active, running, stand-by) of available services for the selected OpenScape Session Border Controller is displayed.

The following apply to OpenScape Session Border Controller:

- Alarm Manager: Application responsible for generating and clearing the alarms.
- Audit: Application used to provide an assessment of a system's internal control.
- Continuous Tracing: Trace application that collects the system logs and traces and sends it to an external application.
- Cron: Linux open source application that provides time-based job scheduling.
- DBMS: Database Management System. This application is used to provide a secure access and control of the internal database tables.
- DHCP: The DHCP application is a Linux open source application using Dynamic Host Configuration Protocol, a network application protocol used by devices (DHCP clients) to obtain configuration information for operation in an Internet Protocol network.
- DNS: Linux open source application that handles Domain Name System distributing the responsibility of assigning domain names and mapping those names to IP addresses.
- Geo-Redundancy: Indicates status of OpenScape SBC geographically separated redundant nodes
- Interface 1: First network interface.
- Interface 2: Second network interface.
- IPsec: Linux open source application that controls the IPsec encryption/ authentication system.
- MS Adapter: Running only in SBC mode, the MS Adapter application is a Proxy for MGCP messages, which converts messages from WAN to LAN and sends it to the Media Server.
- NTP: Linux open source application that uses the Network Time Protocol for synchronizing the clocks of computer systems over packet-switched, variable-latency data networks.
- Process Manager: Controls all OpenScape Branch/SBC applications, responsible for monitoring and restart applications in case of fail or re-configuration.
- Redundancy: Indicates status of OpenScape SBC redundant nodes
- RTP Proxy: The RTP (Real-time Transport Protocol) proxy is an open source application that proxies the payload from outside to inside addresses and vice-versa (WAN to LAN and LAN to WAN). It only runs in SBC mode.
- SIP server: This application controls SIP Requests. It is a transaction full Proxy which can operate as SBC (Session Border Controller) or Proxy.
- SNMP: Linux open source application that uses Simple Network Management Protocol to monitor network-attached devices for conditions that warrant administrative attention.
- Message Rate Control: Open source Network Intrusion Prevention and Detection System (NIPS/NIDS)
- SSDP: Responsible for discovery of the OpenScape Voice system connectivity and to send the Notify messages to the phones in order to inform about the operational mode (Survivability Mode or Normal Mode).
- SSH: The SSH (Secure Shell) Linux open source application allows data to be exchanged using a secure channel between two networked devices.
- SSM: (SIP Services Module)

- Syslog: Open source application responsible for the system and application logs. It provides a rotation mechanism to store logs according to the log level set.
- VPN (Virtual Private Network):
- Web server: Application used to host and provide access to OpenScape SBC Homepage by Web Browsers.

Related tasks

How to Display Active Alarms on page 39
How to Display Alarm Details on page 41
How to Start Rapidstat to Perform a Health Check on page 42
How to Display Detailed Version Information on page 43
How to Display, Export and Clear Log Files for an earlier-than-V8 OpenScape SBC on page 47

3.1.1.8 How to Display, Export and Clear Log Files for an earlier-than-V8 OpenScape SBC

A Log file contains information on an application or component of an OpenScape SBC, for example the SIP (Session Initiation Protocol) server log. Perform the following steps to display, export or clear log files of an OpenScape SBC.

Prerequisites

Adequate administrative permissions.

At least one SBC is configured and in operation.

Step by Step

1) Navigate to **Maintenance** > **Inventory** > **Nodes**.

The system presents the list of nodes with a current list of all known systems of all kinds.

2) Select a node of the OpenScape SBC type:

a) Select **OpenScape SBC** in the **in** Drop-down field to filter the list for OpenScape SBC nodes.
b) Click the **Search** button.
c) Click the name of the desired Open Scape SBC in the list.

The system presents the **Dashboard** view of the selected node.

3) In the **Actions** field area, click the **Log files:** > **Show** button.

The **Log Viewer** window appears.

4) Select one of the following log files from the **Select log** selection list:

- Alarm History:

  Alarm history, showing all active or cleared alarms.
- Alarm Manager:

  Log of Alarm manager application.
- Boot:

  Log of last boot.
- CDR:

  Log of the Call Detail Records.
- Continuous Tracing:

  Log of the Continuous Tracing application.
- Current process:

  A list of the current processes running on OpenScape SBC.
- Install/Upgrade:

  Log from system installation, updates or upgrades. This includes also media server language installation information.
- Process Manager:

  Log of PM application.
- Redundancy:

  Log of redundancy SBC redundancy status
- RTP Proxy:

  Log of RTP Proxy application.
- SIP Server:

  SIP stateful proxy or SBC (Session Border Controller) application.
- Message Rate Control:

  Log from Message Rate Control application.
- SSM:

  Log of SIP Services Module application.
- Survivability Provider:

  Log of Survivability provider application.
- System:

  Log of system events.
- Web server:

  Log of the local web server application.

5) The following options appear:

- To show the log file of the selected type, click the **Show** button.
- To transfer the log file to a directory, click the **Export** button.
- To clear all logs, except for "Alarm History", "Boot", "Current processes" and "Web Server" logs, click the **Clear All** button
- To clear the current log file, click the **Clear** button.

  NOTICE: The "Boot", "Current processes", Alarm History" and "Web Server" logs can't be cleared.

- To return to the **Dashboard** window, click the **Close** button.

Related tasks

How to Display Active Alarms on page 39
How to Display Alarm Details on page 41
How to Start Rapidstat to Perform a Health Check on page 42
How to Display Detailed Version Information on page 43
How to Display the Services Status of an earlier-than-V8 OpenScape SBC on page 45

3.1.1.9 How to Restart the System

Proceed as follows to restart the system to the current configuration or the backup configuration.

Prerequisites

Adequate administrative permissions.

At least one SBC is configured and in operation.

The connection to the OpenScape Voice system is up.

Step by Step

1) Navigate to **Maintenance** > **Inventory** > **Nodes**.

The system presents the list of nodes with a current list of all known systems of all kinds.

2) Select a node of the OpenScape SBC type:

a) Select **OpenScape SBC** in the **in** Drop-down field to filter the list for OpenScape SBC nodes.
b) Click the **Search** button.
c) Click the name of the desired Open Scape SBC in the list.

The system presents the **Dashboard** view of the selected node.

3) In the **Actions** field area, to restart the system use one of the following options:

   - Click the **Current Version** > **Restart** button to restart to the current version.

     On redundant systems this only restarts the selected node. To restart the other node of the redundant pair, select the other node and repeat the procedure.

     NOTICE:

     When the node being restarted is acting as Master the other node might take over the Master function.

   - Click the **Backup Version** > **Restart** button to restart to the backup version.

     On redundant systems this only restarts the selected node to the backup version. It is mandatory to repeat the procedure on the other node of the redundant pair.

     NOTICE:

     When the node being restarted to backup is acting as Master the other node might take over the Master function.

     NOTICE:

     While one of the nodes has been restarted to backup and the other hasn't, an alarm stating "Redundant system has an invalid version (sync is disabled)" will be triggered until both are running the same version.

   A confirmation dialog appears.

4) Confirm the restart.

The system restarts.

3.1.2 General System Information

The "General" section in the OpenScape SBC Assistant menu provides statistics and system information on the selected OpenScape SBC.

Licensing Information

The following License File and Hardware Information is displayed:

- **First Updated**:

  When the License files were first updated.
- **Last Updated**:

  When the License files were last updated.

- **Logical ID**:

  The logical ID associated with the OpenScape SBC.
- **HW ID**:

  The hardware I ID associated with the OpenScape SBC.
- **HW ID2**:

  The hardware ID associated with the OpenScape SBC backup node, if a backup node is configured.

The following buttons are displayed:

- Refresh: Select the **Refresh** button to update the license files for the OpenScape SBC.
- Device license update: Select the **Device license update** button to update the licenses for devices associated with the OpenScape SBC.
- Configure: Select the **Configure** button to update the license files for the OpenScape SBC.

NOTICE: Refer to section "How to Configure and Clear Licensing for an OpenScape Branch Office or SBC via OpenScape Branch Assistant" for details.

The following License Configured and Usage Information is displayed in the table:

- **License Type**:

  The types of licenses configured e.g., OpenScape SBC Base, SBC Sessions.
- **Configured**:

  Number of available licenses configured in the CMP.
- **Locally Reported**:

  Number of licenses assigned in the local OpenScape SBC.
- **Usage (Peak)**:

  Peak usage of the licenses assigned in the local OpenScape SBC.

System Info

The following System Information can be displayed.

- **Registered subscribers**: Select the **Show** button to display a list of registered subscribers for the OpenScape SBC.

NOTICE: Refer to section **How to Display a List of Registered Subscribers** for details.

- **Backup link Status**: Select the **Show** button to displayed backup link status for the OpenScape SBC.
- **Dynamic IP Remote Endpoints**: Select the **Show** button to display the mapping for a remote endpoint Logical Branch Office ID to it's external IP address and SBC Access IP address.

NOTICE: Refer to section **How to Display a List of Dynamic IP Remote Endpoints** for details.

Statistics

Statistics comprise current quantities of specific values of the SIP server of an OpenScape SBC.

The following Information is displayed for the SIP Server:

- **Active dialogs**:

  The number of SIP dialogs currently active.
- **Requests In**:

  The number of SIP requests received since the SIP server is in operation.
- **Requests Out**:

  The number of SIP requests sent since the SIP server is in operation.
- **Responses In**:

  The number of SIP responses received since the SIP server is in operation.
- **Responses Out**:

  The number of SIP responses sent since the SIP server is in operation.

3.1.2.1 How to Display a List of Registered Subscribers

Perform the following steps to display a list of all subscribers e.g., remote subscribers, registered within a particular OpenScape Session Border Controller.

Prerequisites

Adequate administrative permissions.

At least one SBC is configured and in operation.

At least one subscriber is registered in the selected OpenScape SBC.

Step by Step

1) Navigate to **Configuration** > **OpenScape SBC** within the Navigation Bar in the Common Management Platform.
2) Select **All systems** in the Communication System pull-down under **Administration** in the Navigation Tree (if not currently selected).
3) Select the **OpenScape SBC list** in the Navigation Tree under **Administration**

   The system presents the **OpenScape SBC Overview** in the Work Area with a current list of all SBCs.
4) To view a list of SBCs configured at a specific communication system, select a communication system in the **Communication System** field in the navigation tree.

   The default selection for the **Communication System** field is the selection of the global settings in the system menu.

5) To select a particular OpenScape SBC use one of the following options:
   - In the Work Area select the checkbox to the left of the particular SBC in the list and select **Manage**.
   - Choose a SBC from the **Select OpenScape SBC** pull-down located in the Navigation Tree.

   The Work Area presents the **General** view with information and data for the selected SBC.
6) Navigate to **Configuration** > **Local Dashboard** in the navigation tree under **Administration**

   NOTICE: This step does not apply to earlier-than-V8 OpenScape SBC appliances

   The **General** dialog with detailed information and data for the selected SBC appears.
7) Click the **Registered subscribers** > **Show** button in the **System Info** field area.

The **Registered Subscribers** window appears. The following data of all subscribers of the selected SBC is displayed:

- Username:

  Name of the subscriber.
- Contact:

  SIP contact information (Access Network).
- OSV Expiry:

  The expiration time is based on the time remaining before the user must re-register to OSV.
- Subscriber Expiry:

  The expiration time is based on the information sent by the subscriber on registration. The time used by expiration may be shorter, if the central SIP server modifies the expiration timer.
- Mapped Port:

  Mapping from the Access Network to the inside network used for OSV processing.

3.1.2.2 How to Display a List of Dynamic IP Remote Endpoints

Perform the following steps to display a list of Dynamic IP Remote Endpoints associated a particular OpenScape Session Border Controller.

Prerequisites

Adequate administrative permissions.

At least one SBC of the OpenScape Branch type is configured and in operation.

At least one subscriber is registered in the selected OpenScape SBC.

Step by Step

1) Navigate to **Configuration** > **OpenScape SBC** within the Navigation Bar in the Common Management Platform.
2) Select **All systems** in the Communication System pull-down under **Administration** in the Navigation Tree (if not currently selected).
3) Select the **OpenScape SBC list** in the Navigation Tree under **Administration**

   The system presents the **OpenScape SBC Overview** in the Work Area with a current list of all SBCs.
4) To view a list of SBCs configured at a specific communication system, select a communication system in the **Communication System** field in the navigation tree.

   The default selection for the **Communication System** field is the selection of the global settings in the system menu.
5) To select a particular OpenScape SBC use one of the following options:

   - In the Work Area select the checkbox to the left of the particular SBC in the list and select **Manage**.
   - Choose a SBC from the **Select OpenScape SBC** pull-down located in the Navigation Tree.

   The Work Area presents the **General** view with information and data for the selected SBC.
6) Navigate to **Configuration** > **Local Dashboard** in the navigation tree under **Administration**

   NOTICE: This step does not apply to earlier-than-V8 OpenScape SBC appliances

   ---

   The **General** dialog with detailed information and data for the selected SBC appears.
7) Click the **Dynamic IP Remote Endpoints** > **Show** button in the **System Info** field area.

The **Dynamic IP Remote Endpoints** window appears. The following data of all dynamic IP remote endpoints of the selected SBC is displayed:

NOTICE: Information can be filtered by Logical ID, External IP Address or SBC Access ID.

- **Logical ID**:

  Logical ID associated remote endpoint configured as "Dynamic IP".
- **External IP Address**:

  Displays the current Dynamic IP allocated to the OpenScape SBC, otherwise a blank field is displayed.
- **SBC Access IP**:

  Displays the contact address in the appropriate IPv4/IPv6 type, otherwise a blank field is displayed.

3.1.2.3 How to Display a List of Statistics

Perform the following steps to display a list of Dynamic IP Remote Endpoints associated a particular OpenScape Session Border Controller.

Prerequisites

Adequate administrative permissions.

At least one SBC of the OpenScape Branch type is configured and in operation.

At least one subscriber is registered in the selected OpenScape SBC.

Step by Step

1) Navigate to **Configuration** > **OpenScape SBC** within the Navigation Bar in the Common Management Platform.
2) Select **All systems** in the Communication System pull-down under **Administration** in the Navigation Tree (if not currently selected).
3) Select the **OpenScape SBC list** in the Navigation Tree under **Administration**

   The system presents the **OpenScape SBC Overview** in the Work Area with a current list of all SBCs.
4) To view a list of SBCs configured at a specific communication system, select a communication system in the **Communication System** field in the navigation tree.

   The default selection for the **Communication System** field is the selection of the global settings in the system menu.
5) To select a particular OpenScape SBC use one of the following options:
   - In the Work Area select the checkbox to the left of the particular SBC in the list and select **Manage**.
   - Choose a SBC from the **Select OpenScape SBC** pull-down located in the Navigation Tree.

   The Work Area presents the **General** view with Statistics information, when the selected SBC is an earlier-than-V8 OpenScape SBC appliances.
6) Navigate to **Configuration** > **Diagnostics & Logs** > **Statistics** in the navigation tree under **Administration**

   NOTICE: This step does not apply to earlier-than-V8 OpenScape SBC appliances

   ---

   The **Diagnostics & logs** dialog with the **Statistics** for the selected SBC appears.

The following Information is displayed for the SIP Server:

- **Active dialogs**:

  The number of SIP dialogs currently active.
- **Requests In**:

  The number of SIP requests received since the SIP server is in operation.

- **Requests Out**:

  The number of SIP requests sent since the SIP server is in operation.
- **Responses In**:

  The number of SIP responses received since the SIP server is in operation.
- **Responses Out**:

  The number of SIP responses sent since the SIP server is in operation.

3.2 Serviceability

Several functions are available to easily change the system configuration and/or store system configuration files or repair the system.

Serviceability for a Particular OpenScape SBC

Serviceability for a particular OpenScape SBC comprises the following methods or tasks:

- Restarting the system to the current configuration
- Restarting the system to the backup configuration
- Import/export configuration files
- Software activation
- Debugging the system
- Continuous tracing
- On demand tracing

Mass Scheduled Software Updates and Upgrades

The administrator can create batch jobs for software transfer and software activation for a list of OpenScape SBCs. The following methods and tasks are supported:

- Display a list of available software on the CMP (Common Management Platform) for downloading to the OpenScape SBCs.
- Software transfer or activation for a list of OpenScape SBCs.
- Software transfer of new software from the software repository or USB stick or remote locations to the CMP server.
- Display a status overview of the software transfer or software activation process.
- Scheduling multiple batches.

OpenScape SBC Local Management Tool Versus Assistant

For a new installation and complete setup of an OpenScape SBC the OpenScape SBC local management tool provides all relevant configuration and service functions. When the WAN and LAN connection to the OpenScape Voice system is up, the OpenScape SBC Assistant may be used to maintain and configure the system as well.

3.2.1 OpenScape SBC File System

In the system partitions are defined for the active and backup software images. The system configuration is stored in xml configuration files.

In order to accommodate reusing components from the OpenScape Voice system and external applications, the same OpenScape Voice directory structure is preserved.

Partitioning

The compact flash is partitions are as follows:

- Partition “A” is used to hold the one copy of the uncompressed OpenScape SBC software.
- Partition “B” is used to hold a second copy of the uncompressed OpenScape SBC software.
- A Data partition is used to hold data.

The “A” and “B” partitions provide the possibility of falling back to a previous software release in the event of a problem when upgrading to a new software release.Upon initial installation, the “A” partition holds the “active” file system which is loaded into RAM whenever the OpenScape SBC is restarted. When it becomes time to perform the first upgrade after the initial installation, the new software will be stored on the “B” partition and the boot loader will be modified so that the “B” partition is designated as holding the “active” file system which will be loaded into RAM whenever the OpenScape SBC is restarted.

At this point, the software on the “A” partition becomes the backup software.If there is a problem with the new software, fallback to the software which still resides on the “A” partition is possible.

Assuming the previous upgrade was successful, a subsequent upgrade would replace the software on the “A” partition and the bootloader would be modified once again so that the software on the “A” partition is becomes the partition designated as holding the “active” file system and the software on the “B” partition would become the backup software.

The “Data” partition contains directories for XML (Extensible Markup Language) system configuration data files, syslog, alarms, manifest (list of all files and versions delivered with the images), and temporary space.

XML Configuration File Handling

Whenever the XML configuration file is changed, a new version of the XML configuration file is created (e.g. config.001, config.002) and the name of the administrator is documented providing an audit trail and fallback configurations. The XML configuration files are stored on the compact flash (max. 100).

Configuration Files and Correlation to Deployment Scripts

Additionally to each image the production includes a configuration file, deployment script and a file containing encrypted MD5 sums of the configuration file and the deployment script. The configuration file is an XML formatted data structure.The configuration files consist of the following XML elements:

- <version> Version of the complete image.
- <component> The component type e.g. rootfs.

- <startscript> Name of the deployment script.
- <md5full> MD5 sum of the full uncompressed image.
- <md5fullcompressed> MD5 sum of the full compressed image.
- <description> A short description.

The described XML tags are enclosed in a higher level tag <config>. Below is an example of such a configuration file.

This file contains the MD5-sum of the new software image, and the MD5-sum of the whole package. After verifying the installed software package has not been tampered (by using the signature file delivered separately from the image), the system checks the md5-sum of the new software image after download and applies it to the OpenScape SBC. Should the md5 checksum not match, the update will be stopped, removed and the user informed via an error message.

```
<?xml versi”n=””.0" ?>
<config>
<startscript>010_middleware.sh</startscript>
<component>middleware</component>
<imagetype>full</imagetype>
<md5full>a3cca2b2aa1e3b5b3b5aad99a8529074</md5full>
<md5fullcompressed>7e716d0e702df0505fc72e2b89467910</
md5fullcompressed>
<description>Full Root File Image</description>
</config>
```

Related concepts

Software Updates and Upgrades on page 62

3.2.1.1 How to Load and Apply New Configuration Files

Proceed as follows to change the configuration of the system using a new configuration file where all configuration settings are stored.

Prerequisites

Adequate administrative permissions.

At least one SBC is configured and in operation.

The connection to the OpenScape Voice system is up.

Step by Step

1) Navigate to **Configuration** > **OpenScape SBC** within the Navigation Bar in the Common Management Platform.
2) Select the **OpenScape SBC list** in the Navigation Tree under **Administration**

   The system presents the **OpenScape SBC Overview** in the Work Area with a current list of all SBCs.

3) To view a list of SBCs configured at a specific communication system, select a communication system in the **Communication System** field in the navigation tree.

   The default selection for the **Communication System** field is the selection of the global settings in the system menu.

4) To select a particular OpenScape SBC use one of the following options:

   - In the Work Area select the checkbox to the left of the particular SBC in the list and select **Manage**.
   - Choose the SBC from the **Select OpenScape SBC** pull-down located in the Navigation Tree.

   The Work Area presents the **General** view with information and data for the selected SBC.

5) Navigate to **Configuration > System** in the navigation tree under **Administration**

   The **System** dialog appears.

6) Select the **Import/Export** tab.

   The **File in use** field displays the name of the configuration file currently in use.

7) To select a new configuration file use one of the following options:

   - Select the configuration file in the **Use a new configuration file** field.
   - Click the **Import** button and select a configuration file to be transferred to the system.

8) Click the **Load** button.

   The system reads and stores the xml config file settings temporarily.

9) Click the **Close** button to close the **Import/Export** window.

10) Click the **Apply Changes** button in the main window to confirm the changes and start the action.

The configuration settings of the selected configuration XML (Extensible Markup Language) file is applied to the system.

Related tasks

How to Select a Configuration File for Import on page 59

3.2.1.2 How to Select a Configuration File for Import

Proceed as follows to import a new configuration file where all configuration settings are stored.

Prerequisites

Adequate administrative permissions.

At least one SBC or branch office of the OpenScape Branch type is configured and in operation.

The connection to the OpenScape Voice system is up.

Step by Step

1) Navigate to **Configuration** > **OpenScape SBC** within the Navigation Bar in the Common Management Platform.
2) Select the **OpenScape SBC list** in the Navigation Tree under **Administration**

   The system presents the **OpenScape SBC Overview** in the Work Area with a current list of all SBCs.
3) To view a list of SBCs configured at a specific communication system, select a communication system in the **Communication System** field in the navigation tree.

   The default selection for the **Communication System** field is the selection of the global settings in the system menu.
4) To select a particular OpenScape SBC use one of the following options:

   - In the Work Area select the checkbox to the left of the particular SBC in the list and select **Manage**.
   - Choose the SBC from the **Select OpenScape SBC** pull-down located in the Navigation Tree.

   The Work Area presents the **General** view with information and data for the selected SBC.
5) Navigate to **Configuration > System** in the navigation tree under **Administration**

   The **System** dialog appears.
6) Select the **Import/Export** tab.

   The **File in use** field displays the name of the configuration file currently in use.
7) Click the **Import** button.

   The **Import** window appears.
8) Click the **Browse...** button to select the file name and path of the configuration file to be transferred to the system.
9) Click the **OK** button.

   The **Import** window closes and selected configuration XML (Extensible Markup Language) is temporarily applied to the system. The **Apply Changes** button in the main menu becomes enabled and navigation in any of the configuration menu screens will indicate the temporarily imported configuration.
10) Click the **Apply Changes** button to set this configuration to the OpenScape SBC appliance.

Related tasks

How to Load and Apply New Configuration Files on page 58

3.2.1.3 How to Export Configuration Files

Proceed as follows to export a configuration file where all configuration settings are stored.

Prerequisites

Adequate administrative permissions.

At least one SBC is configured and in operation.

The connection to the OpenScape Voice system is up.

Step by Step

1) Navigate to **Configuration** > **OpenScape SBC** within the Navigation Bar in the Common Management Platform.

2) Select the **OpenScape SBC list** in the Navigation Tree under **Administration**

The system presents the **OpenScape SBC Overview** in the Work Area with a current list of all SBCs.

3) To view a list of SBCs configured at a specific communication system, select a communication system in the **Communication System** field in the navigation tree.

The default selection for the **Communication System** field is the selection of the global settings in the system menu.

4) To select a particular OpenScape SBC use one of the following options:

- In the Work Area select the checkbox to the left of the particular SBC in the list and select **Manage**.
- Choose the SBC from the **Select OpenScape SBC** pull-down located in the Navigation Tree.

The Work Area presents the **General** view with information and data for the selected SBC.

5) Navigate to **Configuration > System** in the navigation tree under **Administration**

The **System** dialog appears.

6) Select the **Import/Export** tab.

The **File in use** field displays the name of the configuration file currently in use.

7) Select a configuration file in the **Select a configuration file to export** field.

8) Click the **Export** button.

The **file Download** dialog opens.

9) Use one of the following options:

- Click the **Open** button to open and display the configuration file in the system´s XML (Extensible Markup Language) file viewer application.
- Click the **Save** button and specify the location of the configuration file to be exported. Then click the **Save** button in the **Save As** dialog.
- Click the **Cancel** button to abort the action and return to the **Export/ Import** window.

10) Click the **Export All** button (optional); a tar file is created with the latest 10 xml configuration files.

    The **file Download** dialog opens.

11) Use one of the following options:

    - Click the **Open** button to open and display the configuration file in the system´s ZIP (WinZip) file viewer application.
    - Click the **Save** button and specify the location of the configuration file to be exported. Then click the **Save** button in the **Save As** dialog.
    - Click the **Cancel** button to abort the action and return to the **Export/ Import** window.

12) Click the **Close** button to close the **Import/Export** window.

The action is completed.

3.2.2 Software Updates and Upgrades

Depending on the customer´s service concept, software updates can be performed automatically or manually.

OpenScape SBC Software Upgrades and Updates

Only one process for software delivery is supported: An entire image or a delta image that is used to rebuild a new image on the OpenScape SBC appliance.

The following functions are provided:

- Show Active version of a selected OpenScape SBC.
- List available software stored in the local file system.
- List available software in the OpenScape SBC (passive partition/USB).
- Transfer software to OpenScape SBC.
- Mass updates or upgrades via OpenScape SBC Assistant, Job Management.

> **NOTICE:** Software can be activated on an OpenScape SBC Application using the **Maintenance** tab in the Common Management Platform.

Job Management

The OpenScape SBC Assistant can be used to create, view and configure scheduled batch jobs for upgrading/updating several SBCs via the Job Management in the navigation tree.

Related concepts

OpenScape SBC File System on page 57

3.2.2.1 How to Activate Software on a Particular OpenScape SBC or Branch Device via CMP

OpenScape Voice Assistant can be used to activate software on an OpenScape SBC device. Proceed as follows activate the software. The activation process may take some time.

Prerequisites

Adequate administrative permissions.

At least one SBC is configured and in operation.

The connection to the OpenScape SBCis up.

The file to be activated has been uploaded to the CMP software repository (any other upload is not provided).

Step by Step

1) In the Common Management Platform, under **Maintenance** tab, select the **Inventory**, and then select **Applications** in the Navigation tree.

   The system presents the current list of all applications.

2) In the row of the respective OpenScape SBC application, select the **Software activation** command by clicking on the arrow (right side).

   The **Software activation** dialog appears and can then be selected.

3) Select the location of the file(s) to be activated in the **Location** selection list. The following options are available:

   - Common Repository
   - USB stick

4) Select the file version to be activated from the **Version** selection list. The Image type displayed in the **Image type** column can be **Full** (Complete file for activation) or **Delta** (update from the version before).

   NOTICE: Only applicable images are displayed in the list.

5) Click the **Activate...** button to activate the software as displayed in the list. The activation may take some time.

   The **Software activation - Current status** window appears.

   NOTICE: The **Software activation - Current status** window may not be closed until the status "completed" is displayed in the window.

6) Click the **Close** button.

The software is activated at the OpenScape SBC appliance and the Software activation window is closed.

3.2.3 Job Management

OpenScape SBC Job Management enables the administrator to view the OpenScape SBC software repository and to manage batch jobs for updating or upgrading.

Schedules

In order to create batch jobs for software transfer or software activation for several OpenScape SBC devices, the administrator displays OpenScape SBCs devices. The list of devices can be filtered for sorting on cluster name, IP address or software version installed on the devices. After the devices have been selected, the administrator selects the software to be transferred or activated and then schedules a time for the batch job or starts it immediately.

The status of all batch jobs is displayed and the administrator can display log information for each device or cancel the actions for a specific device.

Common Management Platform Software Repository

The CMP Software repository is used to store and manage upgrade files (*.spa or *.zip) for various applications of an OpenScape system. A list of available software can be retrieved using the **Maintenance** tab > **Inventory** > **Repository**.

3.2.3.1 How to View Batch Jobs

The OpenScape SBC Assistant can be used to create, view and configure batch jobs for mass upgrading/updating of OpenScape SBC devices. Proceed as follows to display a list of batch jobs and detailed information.

Prerequisites

Adequate administrative permissions.

SBCs are configured and in operation.

The connection to the OpenScape Voice system is up.

Step by Step

1) Navigate to **Configuration** > **OpenScape SBC** within the Navigation Bar in the Common Management Platform.
2) Navigate to **Job Management** in the navigation tree.

   The **List of Jobs** appears in the content pane of the Work Area.

   The **Status** (Scheduled, In progress, Completed, Failed or Cancelled), the unique **Job-ID**, the **Action** (Transfer or Activation) **Start Date** and an optional **Note** are displayed for each batch job.
3) To filter the list of jobs, enter a filter criterion in the **Filter** field and the corresponding parameter in the **for** selection list.
4) Click the **Go** button to start the filtering or click the **Clear** button to reset the filter criterion.

   The list shows the elements matching the filter criterion.

5) To view the detailed status of a particular batch job:
   a) Click the checkbox of the respective batch job.
   b) Click the **View Detailed Status...** button.

      The **View Detailed status** dialog appears displaying all information available for the selected batch job.
   c) Click the **Close** button to return to the list of jobs.

Related tasks

How to Create a New Batch Job on page 65
How to Edit or Cancel a Batch Job on page 66

3.2.3.2 How to Create a New Batch Job

The OpenScape SBC Assistant can be used to create, view and configure batch jobs for mass upgrading/updating of OpenScape SBCs devices. Proceed as follows to add a new batch job to the list of batch jobs.

Prerequisites

Adequate administrative permissions.

SBCs are configured and in operation.

The connection to the OpenScape Voice system is up.

Step by Step

1) Navigate to **Configuration** > **OpenScape SBC** within the Navigation Bar in the Common Management Platform.
2) Navigate to **Job Management** in the navigation tree under Administration.

   The **List of Jobs** appears in the content pane of the main window.
3) To create a batch job, the following options are available:
   - Click the **Add...** button to create a new batch job for software transfer or activation.
   - Select an existing batch job from the list and click the **Clone...** button to just change parameters and the scheduled time of an existing job.

   The **Add** window appears.
4) Select the type of action to be taken from the Action Field selection list (Values: **Transfer**, **Activation**, **Transfer WAV files**, **Assign profile**).
5) Enter or modify the software version to be transferred or activated in the **Target Version** field:
   a) Click the **[...]** button.

      The **Version** dialog appears displaying a list of available software versions.
   b) Select a software version from the list.
   c) Click the **OK** button to close the **Version** window.

NOTICE: To configure the list of available software please navigate to **Maintenance > Inventory > Repository**.

6) Enter or modify the comment in the **Note** field (optional).
7) Configure the start time and date:
   a) Click the **Immediate** option to start the batch job after the configuration has been finished.
   b) Enter the date and time in the respective fields to start the job in future.
8) To define the OpenScape SBCs or Branch devices for the batch job click the **Add...** button in the **List of Nodes** field area.

   The **Nodes** window appears displaying a list of all SBCs and branch offices configured on the OpenScape Voice system.
9) Select particular devices or click the checkbox in the headline of the list to select all displayed SBCs and branch offices. The column headings of the list can be used for filtering.
10) Click the **OK** button to confirm your selection and close the dialog window.

    The selected SBCs and Branch offices are displayed in the **Add** window.
11) Click the **OK** button to return to the **List of Jobs** window and initiate the CMP batch job.

The new batch job is added to the list of batch jobs.

Related tasks

How to View Batch Jobs on page 64
How to Edit or Cancel a Batch Job on page 66

3.2.3.3 How to Edit or Cancel a Batch Job

The OpenScape SBC Assistant can be used to create, view and configure batch jobs for mass upgrading/updating of OpenScape SBCs devices. Proceed as follows to edit an existing job or delete one from the list of batch jobs.

Prerequisites

Adequate administrative permissions.

SBCs are configured and in operation.

The connection to the OpenScape Voice system is up.

Step by Step

1) Navigate to **Configuration** > **OpenScape SBC** within the Navigation Bar in the Common Management Platform.
2) Navigate to **Job Management** in the navigation tree.

   The **List of Jobs** appears in the content pane of the Work Area.
3) To cancel a batch job, select the batch job in the list and click the **Cancel** button.

   The scheduled job status is updated to “**CANCEL**”.
4) To edit a batch job, select the batch job in the list and click the **Edit...** button.

   The **Edit** window appears displaying all parameters of the job.
5) Edit or modify the parameters of the batch job as required.

6) Click the **OK** button to confirm the changes and close the dialog.

The batch job is displayed in the list with its modified settings.

Related tasks

How to View Batch Jobs on page 64
How to Create a New Batch Job on page 65

3.3 Password Management

The password management is used to change or reset passwords.

OpenScape SBC Passwords

Passwords to access an OpenScape SBC appliance can be defined for several user identities depending on the access rights. Via the OpenScape SBC Assistant these passwords can be configured under **Configuration** > **OpenScape SBC** > **Administration** area in the navigation tree by selecting the SBC from the **Select OpenScape SBC** pull-down and select **Security** > **General** for current SBC versions, or **System** for earlier-than-V8 SBCs. The passwords are stored in the database of the OpenScape SBC appliance. On the OpenScape SBC Assistant´s database, only the passwords of the user ID "assistant" and "administrator" are stored.

Choose the SBC from the **Select OpenScape SBC** pull-down located in the Navigation Tree.

After an update or a missed synchronization of the password, the access to an OpenScape SBC may be denied so that the method to reset or change the password described above will fail. In this case, the administrator can change or reset the SOAP (Simple Object Access Protocol) password using the **Password...** button in the **OpenScape SBC Overview** screen.

Types of Users on the OpenScape SBCAppliance

The following users are available for login and can be configured in the **System** window:

- administrator,
- assistant,
- guest,
- redundancy,
- service,

If the user logs in as guest, configuration can not be changed.

NOTICE: The users and their default passwords are referenced in the OpenScape SBC Configuration Guide.

Types of Users on the OpenScape SBC Assistant

The following users are available for login:

- administrator, assistant, redundancy

Related tasks

How to Change the Password in the Local Assistant Database on page 34
How to Change or Reset the Password on page 232

3.4 General Installation - Overview

This chapter describes the options for installing software and hardware for OpenScape SBCs.

OpenScape SBC Assistant Configuration

"General Settings" is used to configure a secure method of transport between OpenScape SBC Assistant and the OpenScape Voice Assistant for the purpose of transferring files.

Installation Options

There are two types of installation procedures: “Simplified Installation” and “Basic Installation”.

Simplified Installation provides four options:

- **Option 1 (LAN MAC Address):**

  The OpenScape server hardware is pre-loaded with the required installation software prior to shipping to the customer. The installation does not require a USB stick. The LAN MAC address is pre-configured in the OpenScape SBC Assistant and is used to communicate from the OpenScape hardware to the OpenScape SBC Assistant to fetch software and configuration data.

  DHCP servers are used to communicate the pre-configured Common Management Platform (CMP) URL to the OpenScape server hardware. DHCP also provides a temporary IP address to the OpenScape server to be used during the download process. The OpenScape SBC Assistant must be configured with the software load required for this particular server.

  NOTICE: The OpenScape SBC is configured to run on the first network interface (LAN interface) and will accept the first DHCP Offer that contains Option 43 with a CMP FQDN or IP Address. If on the first network interface (LAN) a DHCP Offer is not returned or is returned but does not contain Option 43, then the OpenScape SBC will send a DHCP Discover message out the second network interface (WAN interface) if configured. If that DHCP offer contains Option 43 with a CMP FQDN or IP Address, the OpenScape SBC will then accept that DHCP Offer from the second network interface (WAN) and use that interface to contact the CMP. The OpenScape SBC ignores any DHCP Offers which do not contain Option 43.

- **Option 2 (Local Logical ID):**

  The OpenScape SBC server hardware requires a USB stick for installation. The USB stick is pre-loaded with required installation software including the Logical ID information for the OpenScape SBC prior to shipping to the customer. The Logical ID information is comprised of <name of the

OpenScape Voice connected to> : <business group name> : <branch name> and is used to communicate from the OpenScape hardware to the OpenScape SBC Assistant to fetch software and configuration data.

DHCP servers are used to provide the temporary IP address, as well as, to communicate the pre-configured Common Management Platform (CMP) URL to the OpenScape server hardware.

The OpenScape SBC Assistant must be configured with the software load required for this particular server.

- **Option 3 (Local CMP URL)**:

  The OpenScape SBC server hardware requires a USB stick for installation. The USB stick is pre-loaded with required installation software including the Logical ID information for the OpenScape SBC and the CMP URL prior to shipping to the customer.

  Pre-configuration of the DHCP servers is required when using this option. A temporary dynamic IP is set up for communication between the DHCP server and the OpenScape hardware.

  The OpenScape SBC Assistant must be configured with the software load required for this particular server.
- **Option 4 (Local xml Config File)**:

  The OpenScape SBC server hardware requires a USB stick for installation. The USB stick is pre-loaded with required installation software including and a xml configuration file for the OpenScape SBC prior to shipping to the customer. The xml file contains the Logical ID, Static IP address and address of the CMP to be used.

  Pre-configuration of the DHCP servers is not required when using this option. The Static IP is used to communicate between the CMP and the OpenScape hardware.

Basic Installation:

The OpenScape SBC “Basic Installation” is the pre-Version 2 OpenScape SBC installation method. Installation requires the use of a memory stick with the current software load and the assigned IP address for the system.

Refer to the **OpenScape SBC Hardware - Overview** chapter for detailed installation steps.

3.4.1 OpenScape SBC Assistant - Configuration

This chapter describes configuration for the OpenScape SBC Assistant.

General Settings

The "General Settings" option is used to configure a secure method of transport between OpenScape SBC Assistant and the OpenScape Voice Assistant for the purpose of transferring configuration.

3.4.1.1 How to Configure OpenScape SBC Assistant - General Settings

Proceed as follows to configure OpenScape SBC Assistant General Settings:

Prerequisites

Adequate administrative permissions.

The connection to the OpenScape Voice system is up.

Step by Step

1) Navigate to **Configuration** and select **OpenScape SBC** within the Navigation Bar in the Common Management Platform.
2) Select the **General Settings** in the Navigation Tree under Administration.

   The system presents the **General Settings** dialog.
3) Proceed as follows to enable secure transport between the OpenScape SBC Assistant and the OpenScape Voice Assistant:
   a) Check the **Secure transfer** checkbox.
   b) The **Security transfer** checkbox indicates the enables secure communications via SOAP between the OpenScape SBC Assistant and the OpenScape Voice Assistant. When “unsecured” (unchecked) the transport method is unsecure via HTTPS.

      NOTICE: The following transport mechanism is used to transfer files from the OpenScape SBC Assistant (certain files only apply to OpenScape SBC servers).

      - - Software Load: HTTPS only
      - - Configuration File: HTTPS or SOAP (Secure

      NOTICE: If the Transport mechanism is set to **Secure transfer** and the OpenScape Branch or OpenScape SBC load does not support the new SOAP transport method, OpenScape Branch or OpenScape SBC is booted with the newest software load and apply the default Configuration file. An alarm is generated to indicate that file transfer has failed due to the wrong transport mechanism.

   c) Click the **Save** key to complete configuration.

   When the Secure transfer is enabled, from that point the OpenScape SBC Assistant will communicate securely to the OpenScape Voice Assistant.

3.4.2 Simplified Installation Steps

This chapter describes the general steps for OpenScape SBC simplified installation of software and hardware.

General Steps Checklist

The following is a checklist of general steps. Some steps may only apply to certain installation options as indicated.

1) **Download Installation Files Into the CMP:**

   Download all installation files to the Common Management Platform (CMP). Installation files include:

   Mandatory files:

   - SPA file
   - Software load image
   - Configuration file (XML file)

   Optional files:

   The downloaded files are used to install multiple OpenScape SBC servers.

   - Required for Option 1-4

2) **Pre-configure the DHCP Server:**

   Pre-configure the URL associated with the Common Management Platform (CMP) into the DHCP server.

   - Required for Option 1-2

   The DHCP server must return a “temporary” IP address to be used for downloading the OpenScape SBC server.

   - Required for Option 1-3

   NOTICE: OpenScape SBC during DHCP server discovery sends out a DHCP Discover message with Option 60 Vendor Class Identifier automatically set to "OpenScapeSBC" (without the quotes).

   NOTICE: The DHCP Server must be configured to contain the matching Vendor Class Identifier Option 60 so that the associated Option 43 parameters specific to this vendor class can be provided to the OpenScape SBC from the DHCP Server. The Option 43 parameters returned to the OpenScape SBC in a DHCP Offer will include the Common Management Platform FQDN(s) or IP Address(es) so that the OpenScape SBC can contact it to authenticate and download the necessary files to begin the installation procedure. In order to provide the correct Option 43 Vendor Specific Information to the OpenScape SBC in a DHCP Offer, the DHCP Server must not only be provisioned with Option 60, but also be provisioned with Option 43 containing the Common Management Platform FQDN(s) or IP Address(es).

3) **Add the OpenScape Session Border Controller (SBC) to OpenScape Voice Assistant:**

   Add the OpenScape SBC into the Common Management Platform (CMP), OpenScape Voice Assistant.

   - Required for Option 1-4

4) **Add the OpenScape Session Border Controller (SBC) to OpenScape SBC Assistant:**

   Add the OpenScape SBC into the Common Management Platform (CMP), OpenScape SBC Assistant. The OpenScape SBC will automatically appear

in the OpenScape SBC Assistant when configured in the OpenScape Voice Assistant and does not need to be manually added.

- Required for Option 1-4

5) **Configure the Software Load and Hardware Type for the OpenScape SBC:**

Configure the Software Load to be downloaded to the server and the Hardware Type of the server for the OpenScape SBC in the Common Management Platform (CMP), OpenScape SBC Assistant.

NOTICE: If desired, the full configuration associated with each device, may also be downloaded to the CMP. If this is done, the download will include the “config.xml” file and the device will boot up with this configuration database.

- Required for Options 1-4

6) **Configure the Data Configuration File for the OpenScape SBC:**

A Data configuration file can be downloaded to the OpenScape SBC using the Common Management Platform (CMP), OpenScape SBC Assistant.

- Optional for Options 1-4

7) **Add the LAN MAC Address to the OpenScape SBC Assistant:**

Add the OpenScape SBC into the Common Management Platform (CMP), OpenScape SBC Assistant.

- Required for Option 1 only

8) **Connect the OpenScape Hardware to the Network:**

Install the OpenScape server onto the network. Plug in the USB stick into the OpenScape SBC server and power up the server. Upon power up installation information is exchanged between the CMP and the OpenScape SBC server. The list of installation files includes the software load, configuration file and possibly media files and config.xml file for the database. The device may boot up to three times during the process of downloading and installation.

- USB stick not required for Option 1
- USB stick required for Option 2-4

NOTICE: OpenScape SBC Access to CMP (unsecured port 4709) must be configured in the OpenScape SBC Assistant prior to powering up the server. This is required to allow authentication, configuration and licensing information.

---

9) **Troubleshooting Installation Errors and Alarming:**

The OpenScape SBC server will log errors and produce alarms when possible, if errors occur during installation. Resolve errors and re-install.

10) **Confirmation Installation is complete:**

The OpenScape SBC Assistant can be used to view the status of all the OpenScape SBC devices as they are being installed. The status will indicate the current state of the installation process including if the OpenScape SBC device was successfully installed, the failure state, and reason (when provided). Once an OpenScape SBC device has been

successfully installed the state shown in the OpenScape SBC Assistant will be “normal”.

Should the OpenScape SBC software need additional updates, the normal OpenScape SBC Batch processing functions can be used.

The OpenScape SBC server will signal that installation is complete by audible alert. Audible alarm as are also used to signal installation issues.

3.4.2.1 How to Download Installation Files Into the CMP

Proceed as follows to install files to the repository to the Common Management Platform (CMP). The downloaded files include product software loads and can be used to install multiple OpenScape SBC servers.

Prerequisites

Adequate administrative permissions.

The connection to the OpenScape Voice system is up.

Step by Step

1) Navigate to **Maintenance** > **Inventory** within the Navigation Bar in the Common Management Platform.

   The system presents the **Nodes & Application** Navigation Tree.
2) Select **Repository** from the Navigation tree.

   The **Software Repository** window appears with a list of software.
3) Click the **Add...** button, in the work area navigation bar.

   The **Add to software repository** window appears.
4) Select the **Browse...** button to search and select a file. One to ten files can be downloaded at one time. These files can be individual files or zip files. It is required to download the SPA file and software image.tar file for software updates.

   NOTICE: The SPA file for software update which contains the meta information **must be the first file** in the download list.

   The **browser** window appears, for search and selection of a file.
5) Select the file from the browser and **Open** to add the file to the list to be loaded.

   The **Add to software repository** window is updated with the selected file information.
6) Click the **Add** button next to **Add another file** to add additional files when greater than 10 files are required.

   The **Add to software repository** window appears.

7) Click the **Save** button to update the CMP software repository.

The **Add software repository** window closes and the Software repository window appears with the updated software file information.

NOTICE: Configuration files must be transferred manually to CMP in the following directories:

- **Offboard** (separate server used for CMP):

  Configuration File directory:

  `/opt/siemens/openbranch/ob_config/<Logical_ID>/Configuration_File`
- **Onboard** (aka Integrated, CMP runs in the same OpenScape Voice server):

  Configuration File directory:

  `/img/enterpriseimg/primary/openbranch/ob_config/Configuration_File`

8) The CMP repository now has the required installation software.

The software in the CMP repository can now be used to install multiple OpenScape severs.

3.4.2.2 How to Configure a Windows DHCP Servers

OpenScape device DHCP client will Broadcast a DHCP discovery Request with Option 60 Vendor Class Identifier automatically set to "OpenScapeSBC". The DHCP Server shall acknowledge with information via Option 43 containing the Common Management Platform FQDN(s) or IP Address(es). Proceed as follows to configure a Windows DHCP server with Common Management Platform (CMP) information used for Simplified Installation Options 1-2:

Prerequisites

Adequate administrative permissions.

DHCP Servers are available to the OpenScape devices in the customers network and used for temporary Dynamic IP address retrieval.

Step by Step

1) Configure Option 60: Enter the following information into the DHCP server.

a) Open the DHCP Console in Windows Server 2003/2008

b) Select (highlight) the DHCP Server in the navigation tree, right click on it and select **Define Vendor Classes**.

The **DHCP Vendor Classes** window appears.

c) Click the **Add** button.

The **New Class** window appears.

d) Enter the following Vendor Class Information: **Display Name** e.g., OSBC_VCI, **Description**e.g., OpenScape SBC Vendor Class Identifier.

e) Click the field under the **ASCII** column in the table and enter the value “OpenScapeSBC” (without quotes) in the field.

f) Click the **OK** button when finished.

The **New Class** window closes and the **DHCP Vendor Classes** window appears with the new vendor class displayed.

g) Click the **Close** button.

Option 60 is configured.

2) Configure Option 43: Enter the following information into the DHCP server.

a) Open the DHCP Console in Windows Server 2003/2008 (may be currently opened)

b) Select (highlight) the DHCP Server in the navigation tree, right click on it and select **Predefine Options**.

The **Predefined Options and Values** window appears.

c) Select the option class previously created (OSBC_VCI) from the **Option class** field list.

The **Add** button becomes active.

d) Click the **Add** button.

The **Option Type** window appears.

e) Enter the option type name in the **Name** field e.g., OSBC-Opt43-for-CMP.

f) Select data type **String** in the **Data type** field list.

g) Enter **1** for the code in the **Code** field. This will return Type 01 in Option 43 which the OpenScape SBC requires.

h) Enter description in the **Description** field (optional) e.g., OSBC Opt43 for CMP FQDN/IP.

i) Click the **OK** button when finished.

The **Option Type** window closes and the **Predefined Options and Values** window appears with the new Option name displayed.

j) Enter the IP Address of the Common Management Platform (CMP) in the **Value** field. This could also consist of a single FQDN if desired, two

FQDNs or two IP Addresses if CMP redundancy exists, which all can resolve to the Common Management Platform IP Addresses.

Example: String value is a single IP Address for CMP: 10.245.4.52

Example: String value contains two CMP IP Addresses: 10.245.4.52,10.245.4.62

Example: String value is a single FQDN for the CMP: cmp52.simpinst.com

Example: String value contains two FQDNs (comma separated): cmp52.simpinst.com,cmp52.simpinst.com62

k) Click the **OK** button.

Option 43 is configured and the **DHCP** main window appears.

3) Assign Option 43 to the DHCP Scope: Enter the following information into the DHCP server.

a) Open the DHCP Console in Windows Server 2003/2008 (may be currently opened)

b) Select (highlight) the DHCP Server in the navigation tree, right click on it and select **Configure Options**.

The **Scope Options** window appears.

c) Select the **Advanced** tab.

The **Advanced** work area appears.

d) Select the vendor class previously created (OSBC_VCI) from the **Vendor class** field list.

The **Available Options and Description** is populated in the table.

e) Checkmark the option previously created for Option 43 in the checkbox.

The **Data entry String value** is automatically updated with the CMP IP or FQDN information.

f) Click the **OK** button.

Option 43 is assigned and the **DHCP** main window appears.

4) Pre-configuration of the DHCP server is complete.

The OpenScape SBC is configured to run on the first network interface (LAN interface) and will accept the first DHCP Offer that contains Option 43 with a CMP FQDN or IP Address. If on the first network interface (LAN) a DHCP Offer is not returned or is returned but does not contain Option 43, then the OpenScape SBC will send a DHCP Discover message out the second network interface (WAN interface) if configured. If that DHCP offer contains Option 43 with a CMP FQDN or IP Address, the OpenScape SBC will then accept that DHCP Offer from the second network interface (WAN) and use that interface to contact the CMP. The OpenScape SBC ignores any DHCP Offers which do not contain Option 43.

After the DHCP server is configured additional simplified installation steps are required prior to installation of an OpenScape Session Border Controller.

3.4.2.3 How to Configure a LINUX DHCP Server

OpenScape device DHCP client will Broadcast a DHCP discovery Request with Option 60 Vendor Class Identifier automatically set to "OpenScapeSBC". The

DHCP Server shall acknowledge with information via Option 43 containing the Common Management Platform FQDN(s) or IP Address(es). Proceed as follows to configure a LINIUX DHCP server with Common Management Platform (CMP) information used for Simplified Installation Options 1-2:

Prerequisites

Adequate administrative permissions.

DHCP Servers are available to the OpenScape devices in the customers network and used for temporary Dynamic IP address retrieval.

Step by Step

1) The following details the specific configuration parameters that are required to provision a Linux DHCP Server for Simplified Installation with the OpenScape SBC. The parameters below refer to the specific settings needed for the Simplified Installation with the OpenScape SBC outside of the typical DHCP server settings already existing in the customer environment if using a Linux DHCP Server (DHCP Address Pools, Reservations, Default Gateway, DNS server addresses, etc. as this depends on the customer infrastructure)

a) Only the "option Vendor.swsupply1" line should be used and can be populated with either a single FQDN, a single IP Address, two FQDNs or two IP Addresses (separated by a comma) for representing CMP redundancy

   The "option Vendor.swsupply2" (code 2) should not be used, as the OpenScape SBC only recognizes and accept Option 43 responses with Type Code 01. The "option Vendor.swsupply2" uses Type Code 02 which the OpenScape SBC does not accept for representing a CMP address

b) If the DHCP Discover message sent by the OpenScape SBC upon bootup contains Option 60 Vendor Class Identifier equal to the value "OpenScapeSBC", the DHCP Server will return in the DHCP Offer Option 43 with one of the values not commented out in "option Vendor.swsupply1" under the "Vendor" class.

c) In the example below, the DHCP Server will return in the DHCP Offer Option 43 with 10.234.3.35, which represents the Common Management Platform IP Address

   Only one value in "option Vendor.swsupply1" can be active at a time within this dhcp.conf file. In the example below, having either of the "option Vendor.swsupply1" values active (not commented out) will return in Option 43 the associated entries (the first returns a single IP Address, the second returns a single FQDN, the third returns two IP Addresses (separated by a comma), and the fourth returns two FQDNs (separated by a comma)

Example data:

- the customer domain is simpinstall.com
- the customer is providing addresses via DHCP for network 10.20.1.0/24 GW: 10.20.1.1
- the customer's DHCP Scope is for addresses 10.20.1.10 thru 10.20.1.100
- the customer's two DNS Servers are 10.20.4.230 and 10.20.5.230

- the customer's CMP is at IP Address 10.234.3.35 based on "option Vendor.swsupply1”

DHCP Server settings in the /etc/dhcpd.conf file:

```
option domain-name "simpinstall.com";
option domain-name-servers 10.20.4.230, 10.20.5.230;
option routers 10.20.1.1;
#
class “Vendor” {
option Vendor.swsupply1 “10.234.3.35”;
# option Vendor.swsupply1 "cmp35.simpinstall.com";
# option Vendor.swsupply1 "10.234.3.35,10.234.2.206";
# option Vendor.swsupply1 "cmp35.simpinstall.com";
# option Vendor.swsupply1
 "cmp35.simpinstall.com,cmp36.simpinstall.com";
match if option vendor-class-identifier =
 “OpenScapeSBC”;
vendor-option-space Vendor:
}
subnet 10.20.1.0 netmask 255.255.255.0 {
range 10.20.1.10 10.20.1.100;
default-lease-time 86400;
max-lease-time 1800;
}
```

2) Pre-configuration of the DHCP server is complete.

The OpenScape SBC is configured to run on the first network interface (LAN interface) and will accept the first DHCP Offer that contains Option 43 with a CMP FQDN or IP Address. If on the first network interface (LAN) a DHCP Offer is not returned or is returned but does not contain Option 43, then the OpenScape SBC will send a DHCP Discover message out the second network interface (WAN interface) if configured. If that DHCP offer contains Option 43 with a CMP FQDN or IP Address, the OpenScape SBC will then accept that DHCP Offer from the second network interface (WAN) and use that interface to contact the CMP. The OpenScape SBC ignores any DHCP Offers which do not contain Option 43.

After the DHCP server is configured additional simplified installation steps are required prior to installation of an OpenScape Session Border Controller.

3.4.2.4 How to Configure a Cisco Router Utilizing the DHCP Server

OpenScape device DHCP client will Broadcast a DHCP discovery Request with Option 60 Vendor Class Identifier automatically set to "OpenScapeSBC". The DHCP Server shall acknowledge with information via Option 43 containing the Common Management Platform FQDN(s) or IP Address(es). Proceed as follows to configure a Cisco Router Utilizing the DHCP server with Common Management Platform (CMP) information used for Simplified Installation Options 1-2:

Prerequisites

Adequate administrative permissions.

DHCP Servers are available to the OpenScape devices in the customers network and used for temporary Dynamic IP address retrieval.

Step by Step

1) The steps needed to set up a Cisco Router to act as a DHCP Server can be obtained from the Cisco Web Site. The following provides the specific configuration parameters necessary for the Simplified Installation to work with the OpenScape SBC with a Cisco Router DHCP Server.
2) Configure Option 60: Enter the following information into the “ip dhcp pool”.
   - **option 60 hex 4f70.656e.5363.6170.6542.7261.6e63.68**

   NOTICE: in hex this string is equal to: OpenScapeSBC
3) Configure Option 43: Enter the following information into the “ip dhcp pool”.
   - Option 43 hex string is assembled by concatenating TLV values (Type + Length + Value)
   - For whatever string value is desired for the FQDN(s) or IP Address(s) for the Common Management Platform, the Option 43 must begin with the first byte being “01” for Type Code 01, the second byte representing the length in bytes of the actual value, followed by the representative string value bytes.

   Example 1:

   Add the following to the configured “ip dhcp pool” for a CMP IP Address of 10.234.2.206:

   option 43 hex 010c.3130.2e32.3334.2e32.2e32.3036

   Actual representation of bytes:

   ```
   01 = Type code 01
   0C = Length 12 (12 bytes make up the IP Address
    10.234.2.206)
   10.234.2.206 in hex = 31 30 2e 32 33 34 2e 32 2e 32 30
    36
   ```

   Example 2:

   Add the following to the configured “ip dhcp pool” for a CMP FQDN of cmp35.jgmb.com:

   option 43 hex 010c.3130.2e32.3334.2e32.2e32.3036

   Actual representation of bytes:

   ```
   01 = Type code 01
   0E = Length 14 (14 bytes make up the FQDN
    cmp35.jgmb.com)
   cmp35.jgmb.com in hex = 63 6d 70 33 35 2e 6a 67 6d 62 2e
    63 6f 6d
   ```
4) Pre-configuration of the DHCP server is complete.

After the DHCP server is configured additional simplified installation steps are required prior to installation of an OpenScape Session Border Controller.

3.4.2.5 How to Add an Endpoint in OpenScape Voice for OpenScape SBC

Proceed as follows create an endpoint in OpenScape Voice; required to create an OpenScape SBC for Simplified Installation Options 1-4:

Prerequisites

Adequate administrative permissions.

Endpoint Profiles must be configured prior to adding endpoints.

The connection to the OpenScape Voice system is up.

Step by Step

1) Navigate to **Configuration** > **OpenScape Voice** and select the **Business Group** icon within the Navigation Bar in the Common Management Platform.

2) Select the `<Business Group>` in the Available Business Groups pull-down associated with the SBC.

The navigation tree is associated with the Business Group selected in the Available Business Groups pull-down.

3) Select the **Members** > **Endpoints** in the Navigation Tree.

The system presents the **Endpoints** view in the Work Area with a current list of all endpoints (e.g., SBCs and branch offices) associated with the selected Business Group.

4) Proceed as follows to create a new OpenScape SBC endpoint (Central SBC):

a) Click the **Add...** button.

The **General** tab under the **Add Endpoint** dialog is displayed by default.

b) Fill in the **Name**, selecting the **Registered** checkbox indicates static registration, select an Endpoint Profile in the **Profiles** selection list and configure all other required fields under the **General** tab work area.

NOTICE: The **Registered** checkbox is grayed out by default. To enable the checkbox, in the **SIP** tab under the

SIP Signaling section the user must select the **Type**= `Static`.

The Endpoint Profile must be configured before adding an endpoint.

c) Navigate to the **SIP** tab and configure the appropriate fields in the work area.

Because OpenScape SBC is deployed as a SIP proxy and because it does not authenticate the remote subscribers that use the SBC to register with the OSV, the endpoint should not be configured as "Trusted".

d) Navigate to the **Attributes** tab and checkmark the appropriate attributes in the work area.

Example: To create an endpoint the following parameters must be configured:

- **SIP Proxy** - Checked
- **Central SBC** - Checked
- **Route via Proxy** - Checked
- **Allow Proxy Bypass** - Unchecked
- **Public/Offnet Traffic** - Checked
- **Enable Session Timer** - Checked

e) Navigate to the **Aliases tab** and configure the Alias IP address. If using OpenScape Branch with Redundancy then Alias must include redundant IP and Physical IP addresses for both OpenScape Branch nodes.

f) Continue as described in the *Managing Branch Offices* chapter in the *OpenScape Voice Assistant* documentation.

The OpenScape SBC (Central SBC) **endpoint** is now created.

The OpenScape “SBC” must now be configured in the OpenScape Voice Assistant database and further configured in the OpenScape SBC Assistant.

5) To configure the OpenScape SBC in the OpenScape Voice Assistant database, select the **Branch Office List** in the Navigation Tree.

The system presents the **Branch Office List** view in the Work Area with a current list of all SBCs and branch offices associated with the selected Business Group.

6) Proceed as follows to create a new SBC:

a) Click the **Add...** button.

The **<BG name> - Add Branch Office** dialog is displayed.

b) Fill in the **Branch Office Name** and **Representative End Point** fields.

c) Select a numbering plan for the SBC from the **Numbering Plan** selection list.

d) Select an office code from the **Office Code** selection list.

e) Select the routing area of the SBC in the **Routing Area** selection list.

f) Check the **This is a Branch Office of type OpenScape Branch** checkbox in the OpenScape Branch Type field area in the **General** tab.

g) Continue as described in the *Managing Branch Offices* chapter in the *OpenScape Voice Assistant* documentation.

The Endpoint is added to the OpenScape Voice Assistant database.

NOTICE: The OpenScape SBC must be further configured in the OpenScape SBC Assistant.

NOTICE: The OpenScape SBC Assistant Overview work area will display the endpoint for OpenScape SBC **Status** as **Inventory**

3.4.2.6 How to Add or Delete an OpenScape SBC to OpenScape SBC Assistant

Proceed as follows to add an OpenScape SBC to OpenScape SBC Assistant for Simplified Installation Options 1-4:

Prerequisites

Adequate administrative permissions.

The connection to the OpenScape Voice system is up.

Step by Step

1) Navigate to **Configuration tab** and select **OpenScape SBC** within the Navigation Bar in the Common Management Platform.

2) Select the **OpenScape SBC list** in the Navigation Tree under Administration.

The system presents the **OpenScape SBC Overview** in the Work Area with a current list of all SBC devices.

3) Proceed as follows to assign a new OpenScape SBC:

a) Click the **Add...** button.

The **Add OpenScape SBC** dialog is displayed.

b) Select the associated **Comm System** by clicking the "**...**" button and selecting a Comm system from the **Comm Systems** dialog.

c) Click the **OK** key to save the Comm System.

The **Add OpenScape SBC** dialog is re-displayed and the Comm System information is shown.

d) Select the associated **Business Group** by clicking the "**...**" button and selecting a Business Group from the **Business groups** dialog.

e) Click the **OK** key to save the Business Group.

The **Add OpenScape SBC** dialog is re-displayed and the Business Group information is shown.

f) Select the associated **Endpoint** by clicking the "**...**" button and selecting a Endpoint from the **Endpoint** dialog.

The following fields are populated:

The associated OpenScape SBC Name in the **Central SBC Name** field

The associated OpenScape SBC IP Address in the **IP Address** field

g) The **Communicating over Secured channel** checkbox indicates the status of the OpenScape SBC device. When "unsecured" (unchecked) allows the OpenScape SBC (identified by logical ID) to request an authentication statement. The checkbox is set to unchecked and grayed

out by default when the OpenScape SBC is first added to the OpenScape SBC Assistant. Once the OpenScape SBC requests an authorization statement and the OpenScape SBC Assistant sends the authorization statement; the checkbox is automatically checked and the OpenScape SBC is placed in Secured Mode (the **Security status** is updated to **Secured Mode**).

NOTICE: Communicating over Secured channel checkbox must be unchecked to reinstall an OpenScape SBC using simplified installation. Unchecking the checkbox will revoke the current authentication statement and allow the OpenScape SBC to request a new authentication statement.

---

h) Click the **OK** key to save the Endpoint.

The **Add OpenScape SBC** dialog is re-displayed and the Endpoint information is shown.

i) Click the **OK** key to save the OpenScape SBC endpoint that was created under OpenScape Voice.

The **Add OpenScape SBC** dialog is closed and the **OpenScape SBC Overview** is displayed. OpenScape SBC assigned endpoint information is shown with a **Status** = **Inventory**.

When the OpenScape SBC is added to the OpenScape SBC Assistant, from that point the OpenScape SBC Assistant will be able to administer this OpenScape SBC.

4) Proceed as follows to remove an existing SBC device from the list:

a) Select the OpenScape SBC from the **OpenScape SBC Overview** work area by checking the associated checkmark box.

b) Click the **Delete** button in the work area.

The corresponding record will be deleted from the OpenScape SBC Assistant's database.

3.4.2.7 How to Configure the Software Load and Hardware Type

Proceed as follows to configure the Software Load to be downloaded to the server and the Hardware Type of the server for the OpenScape SBC for Simplified Installation Options 1-4:

Prerequisites

The software load to be downloaded to the server, must be pre-loaded to the Common Management Platform (CMP) Software Repository.

The **Allowed to request a security Authentication Statement** parameter (**Configuration** > **OpenScape SBC** > **Administration** > **OpenScape SBC List** > Edit an existing OpenScape SBC > **Configuration Installation button**) must be enabled to allow communication between the CMP and OpenScape SBC.

Adequate administrative permissions.

The connection to the OpenScape Voice system is up.

Step by Step

1) Navigate to **Configuration tab** and select **OpenScape SBC** within the Navigation Bar in the Common Management Platform.
2) Select the **OpenScape SBC list** in the Navigation Tree under Administration.

   The system presents the **OpenScape SBC Overview** in the Work Area with a current list of all SBC devices.
3) Select the OpenScape SBC from the **OpenScape SBC Overview** in work area by checking the associated checkbox.

   The **Edit...** button becomes active in the **OpenScape SBC Overview** Work Area.
4) Click the **Edit...** button in work area.

   The **Edit OpenScape SBC** dialog becomes active.
5) Click the **Configure Installation** button.

   The **Installation Info** dialog becomes active.
6) Select the **Software load** from the pull-down menu in the general work area e.g., V2R0.02.0.
7) Select the **Hardware Type** from the pull-down menu in the general work area. Possible values are based on the current hardware supported e.g., X3250, X3550, RX330, RX200, ...
8) Checkmark the **Installation** checkbox if the simplified installation method is to be used to install Hardware. Setting of this flag is mandatory for simplified installation.

   NOTICE: The **Communicating over secured channel** checkbox in the General Tab is unchecked by default the first time. When the installation is completed, this parameter is set automatically. This parameter must be unchecked manually if the server is to be reinstalled.

   ---
9) Click the **OK** button.

   The **Installation info** dialog closes and the **Edit OpenScape SBC** dialog appears.
10) Click the **OK** button.

    The **Edit OpenScape SBC** dialog closes and the **OpenScape SBC Overview** window appears with the OpenScape SBC updated.

3.4.2.8 How to Configure the Data Configuration File

Proceed as follows to configure the data configuration file for the OpenScape SBC for Simplified Installation Options 1-4:

Prerequisites

Adequate administrative permissions.

The connection to the OpenScape Voice system is up.

Step by Step

1) Navigate to **Configuration tab** and select **OpenScape SBC** within the Navigation Bar in the Common Management Platform.
2) Select the **OpenScape SBC list** in the Navigation Tree under Administration.

   The system presents the **OpenScape SBC Overview** in the Work Area with a current list of all SBC devices.
3) Select the OpenScape SBC from the **OpenScape SBC Overview** in work area by checking the associated checkbox.

   The **Edit...** button becomes active in the **OpenScape SBC Overview** Work Area.
4) Click the **Edit...** button in work area.

   The **Edit OpenScape SBC** dialog becomes active.
5) Click the **Configure Installation** button.

   The **Installation Info** dialog becomes active.
6) Select the **Data Configuration File** tab.

   The **Data Configuration File** dialog is displayed with the current data configuration file displayed for the OpenScape SBC.
7) Click the **Browse...** button in the work area.

   The browser dialog is displayed.
8) Select the specific Data Configuration file.

   Only one data file can be used by the OpenScape SBC.

   NOTICE: Only XML files are allowed (no WAV files).
9) Click the **Add...** button in the **Data Configuration File** work area.

   The **Data Configuration File** dialog is updated with the selected Data Configuration file.
10) Click the **OK** button.

    The **Installation info** dialog closes and the **Edit OpenScape SBC** dialog appears.
11) Click the **OK** button.

    The **Edit OpenScape SBC** dialog closes and the **OpenScape SBC Overview** window appears with the OpenScape SBC now updated.

3.4.2.9 How to Configure the MAC Address

Proceed as follows to configure the MAC address to an OpenScape SBC for Simplified Installation Option 1 only:

Prerequisites

Adequate administrative permissions.

The connection to the OpenScape Voice system is up.

Step by Step

1) Navigate to **Configuration tab** and select **OpenScape SBC** within the Navigation Bar in the Common Management Platform.
2) Select the **OpenScape SBC list** in the Navigation Tree under Administration.

   The system presents the **OpenScape SBC Overview** in the Work Area with a current list of all SBC devices.
3) Select the OpenScape SBC from the **OpenScape SBC Overview** in work area by checking the associated checkbox.

   The **Edit...** button becomes active in the **OpenScape SBC Overview** Work Area.
4) Click the **Edit...** button in work area.

   The **Edit OpenScape SBC** dialog becomes active.
5) Click the **Configure Installation** button.

   The **Installation info** dialog becomes active.
6) Select the **Software load** from the pull-down menu in the general work area (if not already configured).
7) Select the **Hardware Type** from the pull-down menu in the general work area (if not already configured).
8) Enter the LAN MAC address in the **MAC address** field in the general work area is used for simplified installation and licensing. The LAN MAC address must be entered in the form of e.g., 5C:F3:FD:31:DK:52 (not case sensitive).
9) The LAN MAC address in the **MAC Address Node 2** field in the general work area is automatically populated. This address is used for redundant systems and licensing.
10) Click the **OK** button.

    The **Installation info** dialog closes and the **Edit OpenScape SBC** dialog appears.
11) Click the **OK** button.

    The **Edit OpenScape SBC** dialog closes and the **OpenScape SBC Overview** window appears with the OpenScape SBC now updated.

3.4.2.10 How to Install Hardware for Simplified Installation

Proceed as follows to install an OpenScape SBC Hardware using Simplified Installation:

Prerequisites

The OpenScape hardware is pre-loaded with all required installation software based on the installation option.

The Common Management Platform (CMP) and OpenScape SBC Assistant is pre-loaded with all required installation software and Configuration file.

The USB stick is pre-loaded with all required installation software (Options 2-4).

The URL associated with the Common Management Platform (CMP) is pre-configured into the DHCP server (Option 1-2).

The DHCP server is configured and operational (Options 1-3).

The MAC address (LAN MAC) in configured in the OpenScape SBC Assistant (Option 1 only).

The OpenScape SBC is configured in OpenScape Voice.

The simplified **Installation** parameter (checkbox) is checkmarked in the **Configure Installation> Installation Info** dialog.

The **Communicating over secured channel** checkbox in the **Edit OpenScape SBC > General Tab** is unchecked.

The OpenScape SBC is configured in OpenScape SBC Assistant with a Unique ID (MAC Address (LAN MAC) for Option 1, Logical ID is generated (not configured) for options 2-4), Software load, Hardware type.

OpenScape SBC Access to CMP (unsecured port 4709) must be configured in the OpenScape SBC Assistant prior to powering up the server. This is required to allow authentication, configuration and licensing information.

Adequate administrative permissions.

The connection to the OpenScape Voice system is up.

Step by Step

1) Connect the OpenScape Server to the customer's network.

2) Plug the USB stick into the OpenScape server. Required for Options 2-4).

3) Power up the OpenScape Server.

The following installation functions take place:

- OpenScape SBC will send a DHCP Request (Options 1-3)
- Once DHCP data is received it will reboot to apply temporary IP address and connect to the network.
- Once the temporary IP address is set, the OpenScape SBC will contact the CMP server.
- The SBC device is validated by the OpenScape SBC Assistant. For Option 1 the MAC address (LAN MAC) is used for validation and for Options 2-4, the logical ID is used for validation.
- The SBC sends a request for a list of installation files to the OpenScape SBC Assistant.
- The OpenScape SBC Assistant validates the request and returns a list of file names, paths and information about the http server (e.g., CMP) from which to retrieve the files. The file list can include file information related to sw load version, configuration file name that need to be downloaded by the OpenScape SBC device. OpenScape SBC Assistant also updates the device state in the GUI.
- The OpenScape SBC device Server installs the files using HTTP(s) based on information in the file provided by OpenScape SBC Assistant.
- A final boot is required to apply the xml file data and activate the software (SW) version download from the CMP.
- The OpenScape SBC device logs the error cases and will also send alarms if possible.

4) Monitor installation progress using the OpenScape SBC Assistant. Select the **Configuration tab** > **OpenScape SBC** > **OpenScape SBC list** in the navigation tree. Refresh the OpenScape SBC Overview work area display.
   a) Click the **Refresh All** button to update the OpenScape SBC Overview status information.
   b) Or, Select the device of interest in the work area and click the **Refresh Selected** button to update the OpenScape SBC Overview status information.

   The following values are displayed in the Status column of the OpenScape SBC Overview work area:

   - **Inventory** - Indicates the OpenScape SBC system is configured in the Assistant but not installed.
   - **Authenticated** – Indicates the OpenScape SBC platform has contacted the OpenScape SBC Assistant with all appropriate credentials.
   - **Installation started** – Indicates that the OpenScape SBC has all the data necessary and started the installation process.
   - **File Transfer Started** - Indicates that the File Transfer has been started by the OpenScape SBC.
   - **File Transfer Successful**.
   - **File Transfer failed**: <filename>-<HttpErrorCode> - Indicates that one of the file has failed to transfer.
   - **Booting** - Indicates the Boot of the OpenScape SBC has started.
   - **Boot Failed** (and reason if provided) - Indicates that the OpenScape SBC failed to come up after the boot. No communication is possible.
   - **Normal/Survival** - The appliance has successfully been installed and ready for the call handling.
   - **Unknown** - The Operational state is not available when the SBC is a Backup Node of a Redundancy System.The Master & Redundant Nodes are in Normal or Survival state and the Backup (standby) proxy mode remains in "Unknown" state. The "Unknown" state is due to Standby mode (Redundancy SBCs) and because the Operational state is not available for the Backup Node.
   - **Unreachable** – check alarms.

5) Troubleshoot and correct any errors or alarms during installation and reinstall.
6) The OpenScape SBC device alerts when the installation is complete. If the Installation is successful the OpenScape SBC device will beep once, pause, and repeat. Beeps will occur for 10 cycles.

After the process is concluded the OpenScape SBC device is installed and operational.

3.4.2.11 How to Troubleshoot Installation Errors and Alarms

The OpenScape SBC and Assistant will provide error log information locally. This information must be retrieved manually. The OpenScape SBC device will provide audible beeps, if hardware supports, to the installer so the installer can determine the nature of the problem. If the OpenScape SBC device knows the CMP URL it will also try to send alarms. Proceed as follows to troubleshoot audible alarm sequences that occur during Simplified Installation:

Prerequisites

Adequate administrative permissions.

The connection to the OpenScape Voice system is up.

Step by Step

1) Troubleshoot and correct any alarms during installation and reinstall.

> **NOTICE:** If an error condition occurs, the OpenScape SBC will abort installation and fallback to the default IP 192.168.0.1 (park state). After the issues are resolved, the OpenScape SBC can be restarted and the simplified installation process will be restarted.

2) Beeps, pause and repeat for 10 cycles represent the following alarms:

- Cannot contact DHCP
- DHCP server did not return temporary dynamic IP for the OpenScape SBC device
- DHCP server not configured to return CMP URL

3) Beeps, pause and repeat for 10 cycles represent the following alarms:

- MAC not pre-configured in CMP
- Logical ID not pre-configured in CMP
- Lack of NW connectivity
- Cannot contact CMP

> **NOTICE:** Logical ID consists of: <OpenScape Voice Name>:<Business Group Name>:<SBC Name>

4) Beeps, pause and repeat for 10 cycles represent the following alarms:

- Installation Info unavailable
- File Transfer unsuccessful
- Boot Failure
- SOAP Responses received with negative acks
- No Response to SOAP Requests sent by the OpenScape SBC device
- SOAP Requests received that have invalid data

5) Troubleshoot and correct any errors indicated on the OpenScape SBC Assistant during installation and reinstall. Select the **Configuration** > **OpenScape SBC** > **OpenScape SBC list** in the navigation tree. Refresh the OpenScape SBC Overview work area display.

a) Click the **Refresh All** button to update the OpenScape SBC Overview work area information.

b) Or, Select the device of interest in the work area and click the **Refresh Selected** button to update the OpenScape SBC Overview work area information.

The following values are displayed in the Status column of the OpenScape SBC Overview work area:

- **Inventory** - Indicates the OpenScape SBC system is configured in the Assistant but not installed.
- **Authenticated** – Indicates the OpenScape SBC platform has contacted the OpenScape SBC Assistant with all appropriate credentials.
- **Installation started** – Indicates that the OpenScape SBC has all the data necessary and started the installation process.
- **File Transfer Started** - Indicates that the File Transfer has been started by the OpenScape SBC.
- **File Transfer Successful**.
- **File Transfer failed**: <filename>-<HttpErrorCode> - Indicates that one of the file has failed to transfer (error log file only).
- **Booting** - Indicates the Boot of the OpenScape SBC has started.
- **Boot Failed** - Indicates that the OpenScape SBC failed to come up after the boot. No communication is possible.
- **Normal/Survival** - The appliance has successfully been installed and ready for the call handling.
- **Unknown** - The Operational state is not available when the SBC is a Backup Node of a Redundancy System.The Master & Redundant Nodes are in Normal or Survival state and the Backup (standby) proxy mode remains in "Unknown" state. The "Unknown" state is due to Standby

mode (Redundancy SBCs) and because the Operational state is not available for the Backup Node.

- **Unreachable** – check alarms.

Information related to file transfer failure is displayed in the error log file including the name of the file that failed and the HTTP reasons for the file transfer failure returned by SBC which can include:

- 400 Bad Request
- 401 Unauthorized
- 403 Forbidden
- 404 Not Found
- 405 Method Not Allowed
- 406 Not Acceptable
- 408 Request Timeout
- 409 Conflict
- 410 Gone
- 413 Request Entity Too Large
- 414 Request-URI Too Long
- 415 Unsupported Media Type
- 422 Unprocessable Entity
- 423 Locked
- 426 Upgrade Required
- 444 No Response
- 499 Client Closed Request
- 500 Internal Server Error
- 501 Not Implemented
- 503 Service Unavailable

Error Log File Locations:

- Common Management Platform (CMP) log file name is **symphonia.log** under the following directories

  - Offboard: **/var/siemens/common/log/**

  - Onboard: **/log/**
- OpenScape SBC log file name is **autoinstall.log** under the following directory **/opt/siemens/openbranch/var/log/openbranch/**

6) Power up the OpenScape SBC server once the errors have been corrected.

The **Communicating over Secured channel** checkbox for the OpenScape SBC configuration in the OpenScape SBC Assistant must be unchecked (Unsecured mode) to allow installation and reinstall an OpenScape SBC.

7) The OpenScape SBC device alerts when the installation is complete. If the Installation is successful the OpenScape SBC device will beep once, pause, and repeat. Beeps will occur for 10 cycles.

After the process is concluded the OpenScape SBC device is installed and operational.

3.5 OpenScape SBC Licensing Files

For OpenScape Session Border Controller and associated applications different license types and license files are available.

License File Generation

A License file can be generated in one of two ways: Generated for Centralized Licensing Management via Common Management Platform (CMP) or generated for Stand Alone Mode License Management via the local SBC administration.

- **Centralized License Management**

  The license file is generated using the MAC ID of the Common Management Platform.

  This license file can be offline activated/applied via the CMP. Optionally, a License Authorization Code (LAC) can be used to online activate/apply a license file via the CMP.
- **Stand Alone Mode License Management**

  Stand Alone Mode management is used when the OpenScape SBC is deployed at a customer who does not have a Common Management Platform (CMP) with OpenScape SBC Assistant or the CMP is not upgraded to a version that supports OpenScape SBC licensing.

  The stand alone license file must have been previously generated and supplied to the customer, using the MAC ID of the OpenScape SBC. These customers use the OpenScape SBC local GUI to manage the OpenScape SBC.

Licensing Files

The following types of license files are supported:

- **Regular License Files** (RLF) contain licenses purchased by the customer. Regular Licenses have no expiration date.

  The following types of files are contained in the OpenScape SBC License file:

  – Centralized SBC Base Licenses (maximum allowed 100)
  – OpenScape SBC Session Licenses (Maximum allowed 160K for Branches and 40K for OpenScape SBC)
- **Software Subscription License File** is a Regular License file that expires on Jan 31st and will contain the maximum values possible for each OpenScape SBC license type.

  – 100 Centralized SBC Base Licenses
  – 200,000 OpenScape SBC Session Licenses (160K for Branches and 40K for OpenScape SBC)
- **Evaluation License File** is a Regular License File with an expiration time of 180 days. The Evaluation License File shall contain the following licenses:

  – 1 OpenScape SBC Evaluation License (if evaluating SBC)
  – 100 OpenScape SBC Session Licenses (if evaluating OSB or SBC)

Redundancy

A license quantity is needed for the Redundant feature in V11 in the following cases:

- When the system is redundant with V10 Licenses and then is upgraded to V11 Licenses.
- When the Redundancy feature is initially activated in V11, either in a fresh or an upgraded system.

Only one license is needed per each redundant system since the active node populates its licensing to the backup node. No additional licenses are required for the backup node.

OS-SBC Virtualization on Vmware

- In order to install VM-OS-SBC, please refer to the OpenScape SBC Configuration Guide, section 2.1.6.
- OpenScape SBC Backup & Restore procedures are recommended to be used versus VM snapshots. VM Snapshots are not to be used in a production environment, except during initial installation process. All snapshots are to be removed once the OpenScape SBC VM is placed into production.

When snapshots of the OpenScape SBC virtual machine are taken, the two boxes presented in the **Take Virtual Machine Snapshot** window of the vSphere client should not be selected. The **Snapshot the virtual machine's memory** box is not selected to prevent stale call data if the snapshot is restored. The **Quiesce guest file system** box is not selected because this selection will pause running processes which will impact service.

- Prior to requesting a standalone license file with an **Advanced Locking ID (ALI)** for a Virtual SBC, configure the OS-SBC according to the OpenScape SBC Configuration Guide. Be sure to configure the SBC to use the default gateway and be sure to have at least one DNS server in the DNS Server list (or check/enable the DNS Server box and provide the eth0 interface IP address as the DNS server address for purposes of calculating an ALI, then, this can be disabled after applying the license file). An ALI cannot be requested if no DNS Server is configured.
- If Standalone licensing is to be used on a VM-OS-SBC, then the license file should be requested by providing the following information from the VM-OS-SBC to generate an **Advanced Locking ID (ALI)**. There is a **Calculate Locking ID** folder in CLS. For a redundant SBC cluster, this information should be taken from the master node:

- – **Hostname** of the OS-SBC: from the Local GUI of OS-SBC, from the main page, refer to the **System Info** section (right frame side), at the **Hostname** field.
  – **Primary DNS Server:** from Local GUI of OS-SBC, navigate to **Network/ NetServices** > **DNS** > **Client** tab, open the **DNS server IP Address** list box and select the **Primary DNS**.
  – **Default Gateway Address**: from the Local GUI of OS-SBC, navigate to **Network/Net Services** > **Settings** > **Routing** > **Default Gateway Address** field.
  – **Host IP Address**: from the Local GUI of OS-SBC, navigate to **Network/ Net Services** > **Settings** > **Interface Configuration** and **Access Realm Configuration** boxes, refer to the **IP Address** field of the **Main IPv4** row.

– **Timezone**: from Local GUI of OS-SBC, navigate to **Network/Net Services** > **NTP** >**Timezone** field.

This data is used to generate an **Advanced Locking ID (ALI)** and the license file will be generated with that ALI. Then apply this license file from the OS-SBC Local GUI, by navigating to **System** > **License** > **License Information** > **Standalone license file**, selecting file by pressing **Choose** button, click **Upload** then click **OK**, click **Save** & exit page. For a redundant SBC cluster, apply the license file on the master node only by logging into LOCAL GUI via the **Virtual Router Redundancy Protocol (VRRP)** address of the SBC cluster. Applying a license file/or allocating licenses to SBC from the OSB Assistant will result in a SIP Server restart on the SBC and potential loss of existing calls.

IMPORTANT: If any of the these parameters change, a new license file is required.

This method of standalone licensing of Virtual OS-SBC is not the preferred method, but may still be used. The **Advanced Locking ID** method in the previous bullet item is the recommended method to request a standalone license file for a Virtual OS-SBC.

IMPORTANT: If the customer has the invalid license due to hardware or configuration changes, the SBC will go into the grace period of 30 days to allow the fix of the license problem.

3.5.1 OpenScape SBC Regular License File

OpenScape SBC Assistant supports Regular License files. The Regular license is a customer purchased license that does not expire.

License Functionality

- The OpenScape Session Border Controller (SBC) Regular license file provides the license types and quantities necessary for a customer to use OpenScape SBC functionality, SBC base functions and SBC sessions without expiration.

License Monitoring

- OpenScape SBC Assistant is informed by the License Management service that a new RLF license file has been applied including the total number of OpenScape SBC licenses for each license type and the expiration date of the license file. OpenScape SBC Assistant will then check to ensure the number of licenses in the RLF is enough to accommodate the number of configured licenses for all devices. If not, OpenScape SBC Assistant provides a popup to inform the craft the RLF license file does not have enough licenses. In this situation OpenScape SBC Assistant will also return license values of zero to all devices requesting a license update until a license file with enough licenses is applied to the system.
- If the RLF license file has enough licenses to accommodate all the devices, OpenScape SBC Assistant will check-out the licenses for each device.
- The OpenScape SBC will display a popup at least once a day whenever any license file is within 60 days of expiration and whenever configuration is not

possible due to the inability to check-out a license. The popup will be shown when navigating to the OpenScape SBC Assistant tab.
- If OpenScape SBC Assistant is informed by the License Management service that an RLF license file has expired, the OpenScape SBC Assistant will return values of zero for all licenses whenever a device requests a license update. This will occur until a new license file is applied.

3.5.2 OpenScape SBC Software Subscription License File

OpenScape SBC Assistant supports Software Subscription License (SSL) files. Software Subscription Licensing consists of two parts – the Product Instance and the Subscription License.

Licensing Structure

- **Product Instance**: The Product Instance is purchased once for each product and consists of all of the licenses necessary to equip a product for 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.
- **Subscription License**: The Subscription License is the monthly charge for a single user to use a single product. If a single OpenScape SBC user has voice, voice mail and Unified Communications (UC), then they would pay for 4 Subscription Licenses – one for OpenScape Voice, one for Xpressions, one for OpenScape UC and one for OpenScape SBC. The Subscription Licenses are based upon the product usage that is reported monthly and the billing is calculated on actual service consumption.

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. The following SSL licensing is provided based on the Licensing Structure and type of Customer:

- **Product Instance** - The following licenses are provided via SSL Licensing:
  - OpenScape SBC version Product Instance for Service Provider Licensing
  - OpenScape SBC version Product Instance for Enterprise Licensing
- **Subscription License**- The following licenses are provided via SSL Licensing:
  - Monthly Subscription License Service Provider OpenScape SBC Session License (per session)
  - Monthly Subscription License Enterprise Provider OpenScape SBC Session License (per session)

License Functionality

- The OpenScape Session Border Controller (SBC) Software Subscription licenses provide the capability for a customer to use OpenScape SBC functionality, SBC base features and SBC sessions for the length of the software subscription.

License Monitoring

- The OpenScape SBC Assistant displays a popup at least once a day whenever any license file is within 60 days of expiration and whenever configuration is not possible due to the inability to check-out a license. The popup is displayed when navigating to the OpenScape SBC Assistant.
- If OpenScape SBC Assistant is informed by the License Management service that a Regular License File (RLF) license file has expired, the OpenScape SBC Assistant will return values of zero for all licenses whenever a device requests a license update. This will occur until a new license file is applied.

License Billing

- OpenScape SBC Assistant provides high water mark counters for the last 12 months and supports the retrieval of the current values of the high watermarks by the Common Management Platform (CMP) for each new license type.
- The billing period ID as well as the values of all high watermarks are included in the results.
- A high watermark of the values of the OpenScape SBC License usage counters are calculated on every counter change and written to OpenScape SBC Assistant database and the disk along with the billing period ID.
- On a monthly basis, the high watermarks are reset to the instant value of used Dynamic Licenses.
- The Software Subscription licensing related parameters/counters are displayed in the OpenScape Branch Assistant.

Software Subscription License Monitoring and Reporting

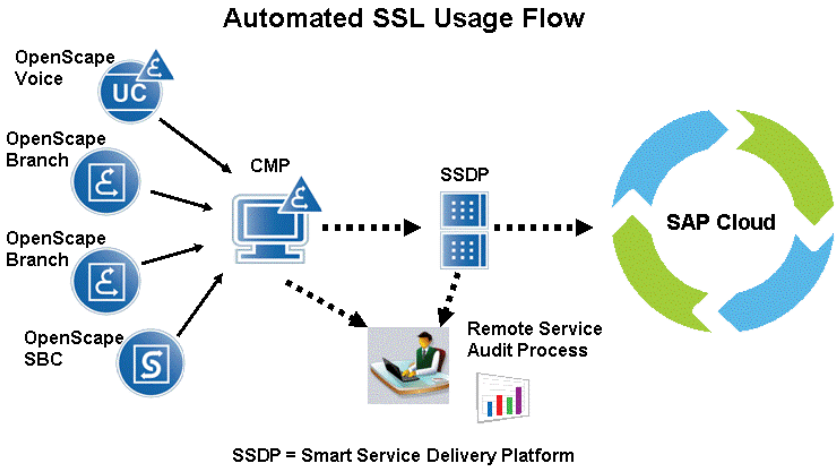
- A monitoring and reporting mechanism resides in the OpenScape SBC Assistant and CMP License Management Server for support of Software Subscription Licensing (SSL).
- OpenScape SBC Assistant provides calculation and reporting of OpenScape SBC Session license usage.

3.5.2.1 OpenScape SBC Software Subscription License (SSL) Monitoring and Reporting - Details

OpenScape SBC Assistant supports Software Subscription License (SSL) files with monitoring and reporting capabilities.

Application Scenario

All of the products in the Software Subscription Licensing Model record subscriber license usage over the course of the month and allow this usage information to be retrieved by the CMP. “Usage” is defined as license consumption, based on the product’s current licensing model, not minute-by-minute usage of any particular product. The Smart Service Delivery Platform (SSDP) service tool provides remote access to the CMP for retrieval of the usage information by Unify Service. This usage information can be retrieved by SAP. The SSDP tool has the ability to schedule the automatic retrieval of the usage information, reducing the Unify Service overhead.



Terms and Definitions

- **High Water Mark**: As high watermark is defined the maximum value which is set. Any increment which produces a current value numerically greater than the current “high watermark”, should cause the “high watermark” to increase to the current value.
- **Billing Period**: As billing periods, in the context of Software Subscription Licensing, are defined monthly time intervals. The billing period ID is the number of the month where the billing period starts. The day of the month where a billing period starts is 1 e.g. Billing Period #1 is from January 1st 0:00:00 to January 31st 23:59:99.
- **Collection**: The SSDP periodically connects to the CMP and collects the usage data for the products (pull from CMP). Remote Service Engineer can display Monthly Usage for specific customer.
- **Billing**: The information gathered by SSDP and the customer ID are retrieved by SAP to invoice the customer for the monthly usage (pull from SSDP).

Description

- **Polling**: Once per day, each product is polled by the CMP for its usage (pull from product).
- **Display**: The CMP has a “Usage” screen that shows the monthly usage from all of the products.
- **Collection**: The SSDP periodically connects to the CMP and collects the usage data for the products (pull from CMP). Remote Service Engineer can display Monthly Usage for specific customer.
- **Billing**: The information gathered by SSDP and the customer ID are retrieved by SAP to invoice the customer for the monthly usage (pull from SSDP).
- **Usage**: Each product will calculate the usage based on their existing licensing model of either statically configured license usage or concurrent usage. For example, licensing in OpenScape Voice is a concurrent model where licenses are pulled from a pool for consumption based on the number of phones and soft clients currently registered. In contrast, OpenScape UC would use a statically configured model as licenses are consumed when a user is configured in the system, whether they login to OpenScape UC or not.

- **OpenScape SBC Session Usage**:
  - A “mixed” model is followed for the usage of the OpenScape SBC and is calculated based on the concurrent license usage.
  - As OpenScape SBC Session usage is defined as the high watermark of the number of consumed OpenScape SBC Session licenses in the month.

CMP License Management Service

The CMP License Management service is aware of the OpenScape SBC related configured licenses. Thus the usage of the licenses where the statically configured model will be followed is retrieved by the CMP License Management Service.

Additionally the Product Instance ID (retrieved by the license file) is provided. The CMP License Management Service interface is called by OpenScape SBC Assistant whenever SSL usage data is reported to the SSL service.

CMP License Management service updates the a usage counter for the following:

- Whenever the Billing Period (the month) is changed. The first day of a month CMP License Management service resets the usage counter to the current value of the corresponding license counter.

NOTICE: The counter is stored encrypted to avoid unwanted modifications. Additionally, this counter is referred to the current Billing Period. The calculation of the Billing period is based on the configured system time of the application server (where CMP License Management Service is installed).

OpenScape SBC Assistant - Calculation of OpenScape SBC Session Usage

OpenScape SBC Assistant maintains one counter for the OpenScape SBC Session Usage for all the configured OpenScape Branch/SBC appliances. Usage is calculated separately on the OpenScape Branch appliances and the OpenScape SBC appliances and is combined into one count.

- Usage for OpenScape Branch (based on the statically configured model): Is the maximum of the total of the configured OpenScape SBC Sessions on all the configured OpenScape Branch appliances.
- Usage for OpenScape SBC (based on the concurrent model): Is the high watermark of the sum of the OpenScape SBC sessions simultaneously actually used for all the configured OpenScape SBC appliances.
- The final usage counter that is reported for the OpenScape SBC Session License shall is the sum of the usage on the OpenScape Branch plus the usage on the OpenScape SBC.

NOTICE: The counters are stored encrypted to avoid unwanted modifications. Additionally, those counters are referred to the current Billing Period. The calculation of the Billing period is based on the configured system time of the application server (where CMP License Management Service is installed).

The OpenScape SBC Assistant updates the a usage counter for the following:

- Whenever an update is done in the total configured OpenScape SBC sessions. If the updated number is greater than the usage counter then the usage counter is updated, otherwise the usage counter remains unchanged.
- Whenever the Billing Period (the month) is changed. The first day of a month OpenScape SBC Assistant resets the usage counter to the current value of the corresponding counter.

NOTICE: In case of redundant systems, OpenScape SBC Assistant takes into consideration only the licenses of the Master Node.

OpenScape SBC Assistant License Management Interface with the SSL Service

OpenScape SBC Assistant uses the interface of the SSL service in order to report the SSL usage data. Whenever the SSL service requests SSL usage data (e.g. once per day), OpenScape SBC Assistant performs the following:

- request license information (OpenScape SBC Session usage included) from the OpenScape SBC appliances.
- reports the SSL usage counters for OpenScape SBC session to SSL service

The OpenScape SBC Assistant reports the following parameters to the SSL service:

Parameter	Description	Length	Allowed Characters
Year	The year the license info is reported. 4-digits representing the year (e.g. 2010).	4 characters	numeric only
Month	The month the license info is reported. Integer value ranging from 1 (January) to 12 (December).	2 characters	numeric only
Product-instance-ID	The unique ID of the product instance. This ID identifies the product in the SAP	17 characters	Alpha-numeric
Product Name	The name of the product (for informational purposes only).	20 characters	Alpha-numeric
Feature –ID (= License ID)	The ID of the feature (SSL Feature ID). Possible values depend on product type.	20 characters	Alpha-numeric

Parameter	Description	Length	Allowed Characters
Used-licenses	Number of used licenses in the reported month (High Watermark). If the CMP did not receive data from the product during the month, then -1 is reported.	6 characters	numeric only
Timestamp	Time when the last license update from the product was obtained. The Timestamp is used by SAP to determine up to date data was recieved for the month. This shall be reported as a string with format: yyyy-mm-dd hh:ss	16 characters	numeric plus “-“ and “:” charters
Violation	The violation flag indicates whether the license of the affected product is violated.	1 characters	true / false

In addition, OpenScape SBC Assistant reports the following parameters necessary to process SSL usage data within the CMP SSL service:

- Node name, string -The IP address or node name
- Node type, string - OpenScape SBC Assistant
- SSL Node Group - N/A (an empty string)

The additional parameters are not needed for SAP.

3.5.3 OpenScape SBC Evaluation License File

OpenScape SBC Assistant supports Evaluation License files. The Evaluation license file is a Regular License file (RLF) that expires after 180 (calendar) days.

License Functionality

- The OpenScape Session Border Controller (SBC) Evaluation license file provides the license types and quantities necessary for a customer to evaluate OpenScape SBC functionality, SBC base functions and SBC sessions for up to 180 days.

License Monitoring

- The OpenScape SBC Assistant displays a popup at least once a day whenever any license file is within 60 days of expiration and whenever configuration is not possible due to the inability to check-out a license. The popup is displayed when navigating to the OpenScape SBC Assistant.
- If OpenScape SBC Assistant is informed by the License Management service that an Evaluation license file has expired, the OpenScape SBC

Assistant will return values of zero for all licenses whenever a device requests a license update. This will occur until a new license file is applied.

3.5.4 OpenScape SBC Base License

The OpenScape Session Border Controller (SBC) Base license provides full usage of the basic SBC software for a given version.

The OpenScape SBC Base license is not tied to a software release or hardware type. OpenScape SBC Base licenses are used to track the number of OpenScape SBC(s) in the field.

OpenScape SBC Base licenses are configured via the OpenScape SBC Assistant. The OpenScape SBC Assistant will then request the license from the Existing License Management Service. If the OpenScape SBC Base licenses are not available, the OpenScape SBC Assistant will not allow the configuration of the Base License. The OpenScape SBC Assistant keeps track of the usage counters and displays the OpenScape SBC Base licenses assigned to OpenScape SBC devices.

The maximum number of OpenScape SBC base licenses in a license file is 100.

One OpenScape SBC Base License must be allocated and assigned to each OpenScape SBC managed by the CMP

3.5.5 OpenScape SBC Session License

OpenScape SBC Session licenses are either shared between OpenScape Branch and OpenScape SBC, and control the maximum number of connections to OpenScape SBC and OpenScape Branch SBCs or are used for each trunk session or each user session connected.

OpenScape SBC Session licenses are configured via the OpenScape SBC Assistant. The OpenScape SBC Assistant will then request the licenses from the existing License Management Service. If the OpenScape SBC Session licenses are not available, the OpenScape SBC Assistant will not allow the configuration of the Session License. The OpenScape SBC Assistant keeps track of the usage counters and displays the OpenScape SBC Session licenses assigned to OpenScape Branch SBC and OpenScape SBC devices.

An OpenScape SBC Session License is required for the following:

- OpenScape SBC - Internet connections
- OpenScape SBC - SIP Trunking and Remote Subscribers
- OpenScape Branch - SBC Proxy - SIP Trunking
- OpenScape Branch - Branch SBC - SIP Trunking

The maximum number of OpenScape SBC Session licences is 200,000 (160K for OpenScape Branches and 40K for OpenScape SBCs).

3.5.6 Upgrade License - Overview

The OpenScape Upgrade Licenses are required when upgrading an OpenScape SBC version.

For SSL upgrade licenses are not required. Monthly Subscription licenses are version–independent. To upgrade from one major version to the next, a new Product Instance for the new product version is ordered (a small handling fee is charged) and the license file will deliver once again the full complement of feature and user licenses. The end user is invoiced for the monthly usage as usual and the change is transparent to the user.

Licensing Software Upgrades for the OpenScape SBC

The following applies to handling of software upgrades for OpenScape SBC:

- OpenScape SBC Assistant version upgrade:
  - OpenScape SBC license data must be maintained whenever the OpenScape SBC Assistant is upgraded.
- When performing an OpenScape SBC software upgrade to a newer V10R2 release, the upgrade is only performed if a license version V9 or later is already installed. Old V10 versions will upgrade as usual.

NOTICE: If the license file version is V8 but the license file contains the component id "EMSS_Check" (Extended Manufacturer Software Support) which is still valid, the upgrade procedure will be executed, and the license file will be accepted.

OpenScape SBC Upgrade Licenses

The following Upgrade Licenses apply to OpenScape SBC:

- OpenScape SBC Upgrade Base License
- OpenScape SBC Upgrade Session License

3.6 Managing Licenses

This chapter provides information about the following topics:

- License Management Concept
- License Information
- Activating Licenses

3.6.1 License Management Concept

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.

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 or desired 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 (offline activation).

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.

Centralized Licensing via Common Management Platform

Centralized Licensing implies that the license file is applied at the Common Management Platform (CMP). The license file must have been generated previously with the MAC ID of the CMP. This license file can be offline activated/ applied via the CMP. Optionally, a License Authorization Code (LAC) can be used to online activate/apply a license file via the CMP.

The licenses are applied/activated with Common Management Platform either offline or online. The Common Management Platform online activation transfers the License Authorization Code (LAC) to the CLS and receives the associated license file. The CMP offline activation assumes the license file was previously generated (with the CMP MAC ID).

The licenses and their related information are displayed in Common Management Platform. The total number of licenses, which licenses are assigned to which OpenScape SBC, and when these licenses expire can be viewed in the CMP. In addition, number of licenses that are still free can also be viewed.

OpenScape SBC Assistant stores licensing information encrypted on the disk.

Licensing in Stand Alone Mode

Stand Alone Mode is defined as when an OpenScape SBC is deployed at a customer who does not have a Common Management Platform (CMP) with OpenScape SBC Assistant or the CMP is not upgraded to a version that supports OpenScape SBC licensing. The standalone license file must have been previously generated and supplied to the customer, using the MAC ID of the OpenScape SBC. These customers use the OpenScape SBC local GUI to manage the OpenScape SBC.

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.

MAC address (Locking-ID)

During production, hardware is assigned a board-specific number called a MAC address which is unique world-wide. To guarantee unique licensing, the license file is linked to the hardware's MAC address (for example, network card of the system server). Every project/feature license is therefore linked to this locking ID.

3.6.2 License Information

This Common Management Platform (CMP) and the OpenScape SBC Assistant can be used to retrieve licensing information:

License Information via Common Management Platform (CMP)

The following information can be displayed using the CMP:

- **General license information**

  The general license information contains

  – the license name (feature name)
  – the name of the product for which the license is used
  – the number of licenses already used
  – the licenses validity
- **License locking IDs**

  A locking ID is a unique feature of a computer system - e. g. the MAC address of a network board. 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.
- **Software Subscription License Monitoring and Reporting**

  OpenScape SBC CMP supports display of Software Subscription License (SSL) information.

License Information via OpenScape SBC Assistant

The following information can be displayed using the OpenScape SBC Assistant:

- **General license information per SBC**

  The general license information contains

  – the node name
  – the license type
  – the number of licenses configured
  – the number of licenses locally configured
  – the peak number of licenses used during the past month
  – when the license was first updated to the SBC
  – when the license was last updated to the SBC
- **License thresholds**

  License thresholds can be set and displayed for the following license types:

  – OpenScape SBC Base
  – SBC Sessions

  The percentage threshold for each license type is used to warn the customer that more licenses may need to be purchased. When the percentage of licenses have been allocated from the license pool, a pop-up warning will be issued indicating that threshold was exceeded.

3.6.2.1 How to Display License Information via CMP

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 **Licenses** 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:

System

Displays the system for which the license information is being reported.

Product Name

Shows the name of the product for which the license information is being displayed e.g., OpenScape Branch / SBC Vx.

Feature Name

States the feature name/license type associated with the product e.g., OpenScape SBC Base.

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.

Validity

Shows the validity for the feature's licenses by expiration date. License entries that are invalid or have expired or are about to expire are marked red e.g., Grace Period 30 days, or unlimited.

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 partial letters preceded and/or followed by an asterisk (*) used for multiple character wildcard search (e. g. *SBC*).
   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 **CSV icon** in the work area to the right of the Items/Page controls.
   b) From the File Download dialog select **Save**.
   c) Enter the **Save in:** location and **File Name** and click on **Save**.
   d) The CSV file is saved and the **License Information** work area appears.

3.6.2.2 How to Display Software Subscription License Information via CMP

To display Software Subscription License (SSL) data 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 **Licenses** navigation menu item.
2) Select **Software Subscription** in the navigation tree.

   The Subscription License Usage dialog appears.

3) A list of nodes by name and type with the associated subscription licenses is displayed in the work area. This list contains for each entry the following information:

Node Name

Shows the Node IP or Hostname.

Node Type

Indicates the type of node associated with subscription license reported e.g., OpenScape Branch, OpenScape Branch/SBC.

License Type

Specifies the Monthly Subscription License type the nodes use e.g., License Type for OpenScape SBC: **osSBC**

Quantity

Shows the number of used licenses in the reported month (High Watermark). If the CMP did not receive data from the product during the month, then -1 is reported.

Product ID

The unique ID of the product instance. This ID identifies the product in the SAP.

Remaining Days

Shows the number of remaining days before expiration of the licenses. If the license is unlimited the field will hold the **N/A** value.

Collection error

The Collection error flag indicates there was an issue with collection of license data.

Last collection date

When the last license update from the product was obtained. The Timestamp is used by SAP to determine up to date data was received for the month.

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. *SBC*).

b) From the list displayed, select whether the filtering is to be applied to the **Node Type** or **Product ID** column.

c) From the year and month field list, select the year and month for which the data will be displayed.

NOTICE: Data is only valid for a rolling year.

---

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.

5) Information in the list can be sorted by Node Name, Node Type and Violation by clicking the associated column name.

3.6.2.3 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 **Licenses** navigation menu item.
2) Select **Locking IDs** in the navigation tree.
3) A list of all computer systems available in the entire system is displayed in the work area. This list contains for each entry the following information:

   NOTICE: If a Locking ID was already used for licensing, it is the only Locking ID displayed.

   Locking ID

   Shows the Locking ID (MAC address) of the system to which the licenses are registered.

   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**.

3.6.2.4 How to Display License Information via OpenScape SBC Assistant

To display license information via the OpenScape SBC Assistant, proceed as follows:

Prerequisites

Adequate administrative permissions.

Step by Step

1) Navigate to **Configuration tab** and select **OpenScape SBC** within the Navigation Bar in the Common Management Platform.
2) Select **Licensing** in the navigation tree, under Administration.
3) Select **Licensing list** in the navigation tree, under Licensing.

4) A list of all licenses available for OpenScape SBCs are displayed in the work area. This list contains for each entry the following information:

Name

Shows the name of the OpenScape SBC for which the license information is being displayed.

License Type

Type of Licenses are as follows:

- SBC sessions
- OpenScape SBC Base

Configured licenses

Specifies how many licenses are configured in the OpenScape SBC Assistant for this logical device.

- SBC sessions (values - 0-4000)
- OpenScape SBC Base (values - 0-1)

Locally Configured licenses

Specifies how many licenses are configured for this physical device, OpenScape Branch or SBC. Maximum values are the same as Configured license values.

Usage (Peak)

Shows the peak number of licenses used for the current month.

First updated

Date and time when the license information was first updated between the CMP and OpenScape SBC.

Last updated

Date and time when the license information was last updated between the CMP and OpenScape SBC.

5) The Licences list can be filtered by Name.

a) Enter the desired filter term in the field **Filter:**. You can either enter the complete term or the partial characters preceded and/or followed by the asterisk (*) wildcard (e. g. *C-SBC*).

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

c) Click on **Clear** to deactivate the filter. Filter conditions are deleted. All the list elements are displayed again.

3.6.2.5 How to Display and Manage Licensing Thresholds via OpenScape SBC Assistant

This feature allows the administrator to manage the allocation of licenses by specifying the threshold values for licenses associated with OpenScape SBC. The threshold value is used to determine when to generate a warning (pop-up) so the administrator can obtain additional licenses prior to running out of licenses. To display or manage threshold license information via the OpenScape SBC Assistant, proceed as follows:

Prerequisites

Adequate administrative permissions

Step by Step

1) Navigate to **Configuration** tab and select **OpenScape SBC** within the Navigation Bar in the Common Management Platform.
2) Select **Licensing** in the navigation tree, under Administration.
3) Select **License thresholds** in the navigation tree, under Licensing.

   The **OSB licenses thresholds** dialog opens.
4) The following Licenses and associated thresholds will be displayed

   OpenScape SBC Base (%):

   The default value is 80%, and the valid range is [0 % ...100 %].

   SBC Sessions (%):

   The default value is 90%, and the valid range is [0 % ...100 %].
5) Enter the threshold percentage of licenses used for the associated license type(s). When the license usage reaches the threshold value a warning shall be sent to the administrator.
6) Click **Save** to make the changes of the threshold values valid.

The threshold warning level for the associated license type usage is modified and set.

3.6.2.6 How to Display Licensing for an OpenScape SBC Via OpenScape SBC Assistant

The OpenScape SBC Assistant can administer OpenScape SBCs. Thus it keeps a list of SBCs in its database. The "OpenScape SBC Overview" form displays all known SBC devices and provides a search function to find a particular one. The administrator can select a single OpenScape SBC to view and configure.

Prerequisites

Adequate administrative permissions.

At least one OpenScape SBC is configured and in operation.

The connection to the OpenScape Voice system is up.

Step by Step

1) To display all SBCs: navigate to **Configuration** > **OpenScape SBC** within the Navigation Bar in the Common Management Platform.
2) Select **All systems** in the pull-down under **Administration** in the Navigation Tree (if not currently selected).
3) Select **OpenScape SBC list** in the Navigation Tree.

   The system presents the **OpenScape SBC Overview** in the Work Area, with a current list of all known SBCs. If no SBCs are defined, the list is empty.

4) To find and select a particular SBC device use one of the following options:

a) In the Work Area select the checkbox to the left of the particular SBC in the list. Select the **Manage** button.

b) Choose a SBC from the **Select OpenScape SBC** pull-down located under **Administration** in the Navigation Tree.

c) Enter filter search criteria to filter the list of SBC devices.

Filtering is possible on the following criteria in the **for** field: **OpenScape SBC**, **Business Group, IP Address, Version, Status**.

Once the filters are set, click the **Go** button.

The system refreshes the list of displayed SBC devices and displays the ones matching the search criteria.

In the Work Area select the checkbox to the left of the particular SBC in the list. Select the **Manage** button.

NOTICE: Wild cards are supported (* for 0 or more characters, "?" for single characters).

Information and data is displayed in the Work Area for the selected SBC.

5) View the work area under **Licensing Information**. The following is displayed:

   First updated:

   Date and time when the license was first updated.

   Last updated:

   Date and time when the license was last updated.

   Logical ID:

   Unique ID for the OpenScape SBC in the form of System Name:Business Group Name:OpenScape SBC Name.

   Hw ID:

   Unique Hardware ID associated with the hardware of the OpenScape SBC.

   License type

   Type of Licenses are as follows: SBC sessions and OpenScape SBC Base.

   Configured

   Specifies how many licenses are configured in the OpenScape SBC Assistant for this logical device.

   Reported locally

   Specifies how many licenses are configured for this physical device, OpenScape SBC.

   Usage(Peack)

   Shows the highest number of licenses used at any point in time during the current month.

   Refresh button

   Used to refresh the current licensing information displayed for that particular OpenScape SBC from the OpenScape SBC Assistant database.

   Device license update button

   Used to request an update of license data from the OpenScape SBC Assistant, to the OpenScape SBC device.

   Configure button

   Used to access configuration of licenses for the OpenScape SBC. In addition, provides access to clear license counters at the OpenScape SBC devices.

6) Configuration and update of licenses can be accomplished for a single OpenScape SBC.

The data displayed is provided by the OpenScape SBC assistant database and the OpenScape SBC hardware itself. This means that the data might be out of date if it was changed on the SBC without the assistant being notified. Refresh button must be used to synchronize data when changes are made.

3.6.2.7 How to Configure and Clear Licensing for an OpenScape SBC Via OpenScape SBC Assistant

The OpenScape SBC Assistant can administer licensing for a particular OpenScape SBC.

Prerequisites

Adequate administrative permissions.

At least one OpenScape SBC is configured and in operation.

The connection to the OpenScape Voice system is up.

Completed either online or offline license activation to apply the license file to the Common Management Platform (CMP).

Step by Step

1) To display all SBCs: navigate to **Configuration** > **OpenScape SBC** within the Navigation Bar in the Common Management Platform.

2) Select **All systems** in the pull-down under **Administration** in the Navigation Tree (if not currently selected).

3) Select **OpenScape SBC list** in the Navigation Tree.

The system presents the **OpenScape SBC Overview** in the Work Area, with a current list of all known SBCs. If no SBCs are defined, the list is empty.

4) To find and select a particular SBC device use one of the following options:

a) In the Work Area select the checkbox to the left of the particular SBC in the list. Select the **Manage** button.

b) Choose a SBC from the **Select OpenScape SBC** pull-down located under **Administration** in the Navigation Tree.

c) Enter filter search criteria to filter the list of SBC devices.

Filtering is possible on the following criteria in the **for** field: **OpenScape SBC**, **Business Group, IP Address, Version, Status**.

Once the filters are set, click the **Go** button.

The system refreshes the list of displayed SBC devices and displays the ones matching the search criteria.

In the Work Area select the checkbox to the left of the particular SBC in the list. Select the **Manage** button.

NOTICE: Wild cards are supported (* for 0 or more characters, "?" for single characters).

Information and data is displayed in the Work Area for the selected SBC.

5) This Step should be executed when changing out OpenScape SBC hardware.

a) Click the **Configure** button in the work area under Licensing Information.

The **Configure licenses** licenses dialog appears and the following information is displayed:

- Clear license counters
- OpenScape licenses assigned for each license type
- Number of available licenses associated with each license type

b) Checkmark the **Clear license counters** and click the **Save** button to clear out “all” licenses at the OpenScape SBC device. This will clear the link between the allocated licenses and the hardware ID.

NOTICE: This should be done prior to changing out OpenScape SBC hardware.

The licenses on the OpenScape SBC are cleared and the **General** OpenScape SBC work area appears. The allocated licenses are not returned to the license pool.

c) Uncheck the **Clear license counters** checkbox and click the **Save** button once the new hardware is installed; the **Clear license counters** checkbox should be cleared so the new hardware can receive the licenses configured in the OpenScape SBC Assistant. This will link the licenses allocated to the device with the devices’ hardware ID.

The **General** OpenScape SBC work area appears.

6) Enter the number of licenses to be assigned to the OpenScape SBC for each license type. The number of assigned licenses can not exceed the number of available licenses shown e.g., **Available:** 9790, for the associated license type. License types include the following:

- **SBC Sessions**
- **OpenScape SBC Base**

7) Click the **Save** button to complete the assignment of licenses in the OpenScape SBC Assistant for the OpenScape SBC device.

NOTICE: This action also updates OpenScape SBC licenses in the OpenScape hardware.

IMPORTANT: Applying or changing licenses assigned to an SBC will cause the SBC to restart the sip server process which will have an affect on transient (non-stable) calls.

Licenses are now allocated in the OpenScape SBC Assistant for the OpenScape SBC and the General OpenScape work area appears.

8) Click the **Device license update** button, in the Licensing Information work area to update license information in the OpenScape SBC device.

   NOTICE: This action transfers licensing information from the OpenScape SBC Assistant to the OpenScape SBC hardware.

   Licenses are now configured in the OpenScape SBC hardware.

9) Click the **Refresh** button, in the Licensing Information work area to refresh the OpenScape SBC licensing information from the OpenScape SBC Assistant.

The data displayed is provided by the OpenScape SBC assistant database rather than the hardware itself. This means that the data might be out of date if it was changed on the SBC without the assistant being notified.

3.6.2.8 How to Display Licensing Warnings for an OpenScape SBC

The OpenScape SBC Assistant automatically displays licensing warnings to notify the administrator of possible licensing issues. Warnings can occur during display and configuration of OpenScape SBCs.

Prerequisites

Adequate administrative permissions.

At least one OpenScape SBC is configured and in operation.

The connection to the OpenScape Voice system is up.

Step by Step

1) Navigate to **Configuration** > **OpenScape SBC** within the Navigation Bar in the Common Management Platform.
2) Select **All systems** in the pull-down under **Administration** in the Navigation Tree (if not currently selected).
3) Select **OpenScape SBC list** in the Navigation Tree.

   The system presents the **OpenScape SBC Overview** in the Work Area, with a current list of all known SBCs. If no SBCs are defined, the list is empty.

4) To find and select a particular SBC device use one of the following options:

a) In the Work Area select the checkbox to the left of the particular SBC in the list. Select the **Manage** button.

b) Choose a SBC from the **Select OpenScape SBC** pull-down located under **Administration** in the Navigation Tree.

c) Enter filter search criteria to filter the list of SBC devices.

Filtering is possible on the following criteria in the **for** field: **OpenScape SBC**, **Business Group, IP Address, Version, Status**.

Once the filters are set, click the **Go** button.

The system refreshes the list of displayed SBC devices and displays the ones matching the search criteria.

In the Work Area select the checkbox to the left of the particular SBC in the list. Select the **Manage** button.

NOTICE: Wild cards are supported (* for 0 or more characters, "?" for single characters).

Information and data is displayed in the Work Area for the selected SBC.

In addition, licensing pop-up warnings will appear if applicable. Warning may include but are not limited to the following:

- A license file is within 60 days of expiring. If a new license file is not added within xx days branch calls will not be possible.
- A configured threshold has been exceeded.
- license file has expired, branch calls will not be possible.
- A license file has been applied that does not have enough licenses. Add a new license file with sufficient licenses for the licenses configured in the Assistant.
- A configuration was attempted but no license was available
- Number of licenses according to the device is out of sync with the number of configured licenses (i.e. after the device responds with a status of “success” after updating its license info but the number of licenses the device reports to have is different than the number of licenses configured. Note: this can happen if the administrator assigns more User or SBC Session licenses than the OpenScape Branch or OpenScape SBC hardware can handle.

In addition, licensing pop-up warnings will appear if applicable. Warning may include but are not limited to the following:

5) Warnings can occur during display and configuration of OpenScape SBCs.

The administrator is warned about licensing issues and can then correct the pending issue.

3.6.3 Activating Licenses

After you have purchased an OpenScape product, you will have to activate the licenses supplied with it in order to enable the product and its features.

Licenses can be activated by one of the following two methods:

In order to activate licensing via the Common Management Platform (CMP); the license file must have been generated using the MAC ID of the CMP.

NOTICE: If the CMP does not support licensing or no CMP is available, OpenScape Branch or OpenScape SBC licensing can be activate via the Stand Alone Licensing mechanism using the local administration GUI.

- **Activating 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.
- **Activating 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.

Supplementary licenses can be purchased to use additional products. When additional licenses are purchased, a separate License Authorization Code (LAC) is provided which can then be used to activate the new licenses you purchased. After activation, all features for which a license is required will be available.

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, which is also called the 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 Platform checks if the MAC address saved in the license file matches the MAC address of the system server (locking ID). If the check succeeds, the licenses of the product/feature are added to the license pool of the CMP. Otherwise, the licenses are not added to the pool.
9) The customer can then create the OpenScape Branch or OpenScape SBC in the CMP and allocate licenses to the branch or sbc from the pool, to provide the functionality purchased.

3.6.3.1 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.

Common Management Platform and OpenScape SBC Assistant supports OpenScape SBC Licensing.

The license file must have been generated with the MAC ID of the Common Management Platform (CMP)

Step by Step

1) On the **Maintenance** navigation tab click on the **Licenses** navigation menu item.
2) Select **Information** in the navigation tree.

> **IMPORTANT:** OpenScape Voice license activation is 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.

> **NOTICE:** The license pool is created and licenses can then be allocated/configured to individual OpenScape SBCs.

3.6.3.2 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

The license file must have been generated with the MAC ID of the Common Management Platform (CMP)

Step by Step

1) On the **Maintenance** navigation tab click on the **Licenses** navigation menu item.
2) Select **Information** in the navigation tree.

   IMPORTANT: OpenScape Voice license activation is 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 system server's MAC address (Locking ID). If the verification is successful, the data is transferred from the file and the licenses are displayed in the Common Management Platform with the associated information.

NOTICE: The license pool is created and licenses can then be allocated/configured to individual OpenScape SBCs.

3.6.4 License Enforcement and Update

This Common Management Platform (CMP) and the OpenScape SBC Assistant can be used to retrieve licensing information:

Enforcing Licensing

Alarms, pop-ups and logging will occur when enforcing licensing limits.

The following table shows how Licensing enforcement will be handled during Installation/Upgrade and when OpenScape devices are operational:

	Install / Upgrade License Enforcement	Operation License Enforcement
Base license	No base: No enforcement	No base: No enforcement

	Install / Upgrade License Enforcement	Operation License Enforcement
SBC Session license	• If no Licenses of any type are available, operates normal but alarm daily. After 30 days of no licenses the final response to Invites will be 606 (a warning header may be included for diagnostic purposes). The same is true for gateways. • If licenses of any type are provided during the 30 day period OpenScape SBC begins to operate based on the licenses available.	Attempts to exceed license: • Established SIP Service Provider/ OpenScape SBC calls will be counted based on 2xx (ack) responses. New Invites exceeding the license limit will be rejected with response code 606 (a warning header may be included for diagnostic purposes) and a critical alarm is generated daily with text indicating SIP Service Provider calls blocked due to insufficient SBC Session licenses. The alarm must be manually cleared.

- **Additional Enforcement Scenarios and Responses**

  Scenarios::

  – OpenScape SBC prevents licensed features from working if the License Server does not respond to a request for a refresh of licenses for 30 consecutive days (OpenScape SBC has successfully received license information from OpenScape SBC Assistant at least once). This can happen when there is a communication error or when the licenses are already allocated to another hardware device.
  – If the licenses have been released for a device the OpenScape SBC Assistant will return zero as the value for all licenses for a device as a response to a license refresh request from a device. In this case licensed features shall be blocked by the device.
  – If the Evaluation license file has expired, the OpenScape SBC Assistant will return zero as the value for all licenses for a device whenever a license refresh request is sent. In this case licensed features shall be blocked by the device.

  Responses:

  – A pop-up is provided to alert the craft whenever a OpenScape SBC is created but installation data and/or licensing data has not been configured for the device.
  – If no Licenses of any type are available OpenScape SBC will operate normal for 30 days and generate a daily alarm with text indicating how many days before the OpenScape SBC will not provide any calls since no licenses are installed.

License Update

The OpenScape SBC requests licensing update for the following:

- after every reboot
- every 24 hours (based on the last reboot time)

License Validation

The OpenScape SBC validate licenses periodically with the central License Server (CMP). If validation fails, additional attempts are made to validate licenses:

- OpenScape SBC to License Server (CMP) Validation:

  The OpenScape SBC checks the License server (CMP) once a day to validate licenses.

  If the first request fails a second attempt is made 30 minutes later, a third attempt 15 minutes after that and an forth attempt 5 minutes later. In other words, 4 tries during the one hour period. After the four validation attempts; validation attempts will take place once every 24 hours.

  – If the connection from the OpenScape SBC to the License server (CMP) is restored within the grace period; the grace period operation returns to normal.
  – If the grace period expires, licensed features stop working. Periodic checking from the OpenScape SBC to the License server (CMP) continues. If the connection to the License server is restored after the grace period expires, operation returns to normal.
- Stand-alone licensing can be used at the OpenScape SBC to bring operation back to normal (Notice: The OpenScape SBC must be configured for Stand Alone license operation).

3.6.5 License Security

The Common Management Platform (CMP) and the OpenScape SBC secures licensing information in the following ways:

Securing Licensing in the OpenScape SBC

- Licensing information stored in the OpenScape SBC is secured by encryption.
- The OpenScape SBC automatically sets the SBC licensing to secure mode if it is in unsecured mode and the Licensing Information request contains a correct authentication statement. This function is performed regardless of whether the licenses are configured.
- Authentication Statements are encrypted and saved in the backup. The Authentication Statements are usable after restore.

Securing Licensing in the OpenScape SBC Assistant

- Licensing information stored in the OpenScape SBC Assistant is secured by encryption. Secured information includes the Logical-IDs, MAC addresses, Authentication Statements and License counts.
- The OpenScape SBC Assistant only allows Authentication Statement requests in unsecured mode. License Information requests are not possible in unsecured mode.
- Authentication Statements are included in the backup and are available after restore. The Authentication Statements are encrypted and persist over restarts and upgrades.

4 OpenScape SBC Assistant – Configuration

In the main navigation area of the OpenScape SBC Assistant instances of OpenScape Session Border Controllers (SBC) can be configured.

OpenScape SBC Assistant Online Help

The OpenScape SBC Assistant is used to display and configure OpenScape Session Border Controllers. The online Help refers mainly to the most current version of OpenScape SBC. Therefore, if an earlier version of OpenScape Session Border Controller is selected some sections may describe features that are not available for the system and some procedures may deviate from the ones described.

4.1 Alarm Configuration Overview

The Alarms section under Configuration allows to display and configure the alarm settings and trap destinations for the OpenScape SBC appliance.

The OpenScape SBC alarming application provides several configuration and administration functions. A configuration file defines text strings to be monitored in the syslog and HW (Hardware) sensors to be checked and the corresponding alarm attributes. The configuration file is read during the initialization of the alarming application. SOAP (Simple Object Access Protocol) attributes are defined to allow for alarming administration activities such as:

- Retrieve a list of active alarms (GroupId-Event-Id).
- Manually delete an alarm identified by GroupId-Event-Id.
- Read the status of a particular GroupId-EventId.
- Change the severity.
- Change the ReportingClass.
- Define trap destinations that alarms are sent to.

4.1.1 Alarm Settings

The Alarms section under Configuration allows to display and configure the alarms settings and trap destinations for the OpenScape SBC appliance.

The OpenScape SBC Assistant Plug-in receives SNMP (Simple Network Management Protocol) traps from one or more OpenScape SBC devices. Alarms received by OpenScape SBC devices will be stored in the Assistant database.

Alarm Settings

The OpenScape SBC Assistant provides a table displaying all types of alarms and the respective parameters. For each type it is possible to edit the alarm parameters individually.

Trap Destinations

The administrator has to define trap destinations that alarms are sent to. The trap destination is identified by “IP address or FQDN (Fully Qualified Domain Name)” and “port number”. It is possible to have more than one trap

destination for one IP address. It is possible to configure the SNMP trap specific parameters such as:

- Blocked (no traps are sent).
- ReportingClassSet (set of ReportingClass numbers of the events to be sent).

SNMP MIB (Simple Network Management Protocol Management Information Base):

The alarm traps of the OpenScape SBC are defined as traps of the following structure. All parameters with the exception of "neName" are taken from the status table.

```
openBranchAlarm0201 NOTIFICATION-TYPE
        OBJECTS {       neName,
                        eventGroupName,
                        eventName,
                        severity,
                        eventType,
                        eventTime,
                        faultyObject,
                        monitoredValue,
                        threshold
}       STATUS          current
        DESCRIPTION    "Spontaneous Alarm from the managed
                       network
                       element."
        ::= { eventGroup02 1 }
```

4.1.1.1 How to Display Alarms Settings

The alarm settings are displayed in a table view to provide an overview of the alarm settings for the different types of alarms.

Prerequisites

Adequate administrative permissions.

At least one OpenScape SBC is configured and in operation.

The connection to the OpenScape Voice system is up.

Step by Step

1) Navigate to **Configuration** tab > **OpenScape SBC** within the Navigation Bar in the Common Management Platform.
2) Select the **OpenScape SBC list** in the Navigation Tree under **Administration**.

   The system presents the **OpenScape SBC Overview** in the Work Area with a current list of all SBCs.

3) To view a list of SBCs configured at a specific communication system, select a communication system in the **Communication System** field in the navigation tree.

   The default selection for the **Communication System** field is the selection of the global settings in the system menu.

4) To find and select a particular OpenScape SBC use one of the following options:

   - In the Work Area select the checkbox to the left of the particular SBC in the list and select **Manage**.
   - Choose a SBC from the **OpenScape SBC** pull-down located in the Navigation Tree.

   General information and data for the selected SBC is displayed in the Work Area.

5) Navigate to **Configuration** > **Alarms** > **Alarm Settings** in the navigation tree under **Administration**.

   The **Alarms** window appears with the **Alarm Settings** tab selected by default.

The following information is provided for each type of alarm:

- **Group ID** and **Event ID**:

  These fields correspond to the SNMP trap OID (Object Identifier) (the last 2 numbers of the OID). An alarm trap is cleared by a trap with the same OID of severity 'cleared'.
- **Group name**:

  Name of the GroupID. It groups together system status information of similar kind (Hardware, Ethernet, Resource, Software, Communication, Usage, Admin, License).
- **Event name**:

  Event name is a character string that describers the alarm. It is closely related to the trap name as defined in the OpenScape SBC SNMP (Simple Network Management Protocol) MIB (Management Information Base).
- **Active**:

  Determines if the alarm will be generated or not.
- **Threshold**:

  Monitored value that needs to be crossed for an alarm to be generated.
- **Trigger**:

  Trigger shows the condition where the alarm will be generated. Trigger is a comparison between the current value and alarm value.
- **Severity**:

  Alarm severity assigned to that particular alarm (warning, minor, major, critical). The Severity is fixed per Fault-Id.
- **Flow timer**:

  Minimal time to wait before generating the next occurrence of the same alarm.

- **Reporting class**:

  Reporting class for Alarm Settings is a number between 0 and 7 that groups events to classes which are reported to the same trap destination. The value "0" means that the event is not reported via SNMP trap.
- **Event type**:

  Classifies the alarms into the following categories: Communications, environmental, equipment, processing error, Quality of Service.
- **Faulty object**:

  Faulty Object is a character string that defines the object that is at fault. This value may be different from SBC to SBC, but it is fixed for a particular SBC.

  Parameters are as follows:

  – HW-Sensors (e.g., Temperature, voltage)
  – Ethernet (e.g., Port failure)
  – Resource (e.g., Bandwidth, CPU usage)
  – Survivability Provider (not running)
  – Apache/PHP (not running)
  – SIP Server (not running)
  – RTP Proxy (not running)
  – Process Manager (not running)
  – network (not running)
  – DHCP server (not running)
  – NTP (not running)
  – Syslog (not running)
  – msadapter (not running)
  – SIP Server (e.g., configuration, core, database)
  – VRRP (not running)
  – Message Rate Control (not running)
  – Update or Upgrade (failure)
  – BLC (not running)
  – BLS (not running)
  – Node 1 Primary OSV link (loss of communication)
  – Node 1 Backup OSV link (loss of communication)
  – Gateway link (loss of communication)
  – DNS link (loss of communication)
  – Billing server link (loss of communication)
  – Surveillance system link (loss of communication)
  – File Server link (loss of communication)
  – Node 2Primary OSV link (loss of communication)
  – Node 2Backup OSV link (loss of communication)
  – Redundancy (e.g., fails, disabled)
  – Geosepmgr (e.g., dat failure)
  – Voice channels (e.g., high activity)
  – Active calls (e.g., high activity)
  – Authentification (e.g., wrong password)
  – phone sw repository (e.g., failure, limit warnings)
  – Install (e.g., simplified installation failure)
  – License (e.g., Expired, blocking, violations)

4.1.1.2 How to Display Alarms Settings for earlier-than-v8 OpenScape SBC devices

The alarm settings are displayed in a table view to provide an overview of the alarm settings for the different types of alarms.

Prerequisites

Adequate administrative permissions.

At least one OpenScape SBC is configured and in operation.

The connection to the OpenScape Voice system is up.

Step by Step

1) Navigate to **Configuration** tab > **OpenScape SBC** within the Navigation Bar in the Common Management Platform.
2) Select the **OpenScape SBC list** in the Navigation Tree under **Administration**.

   The system presents the **OpenScape SBC Overview** in the Work Area with a current list of all SBCs.
3) To view a list of SBCs configured at a specific communication system, select a communication system in the **Communication System** field in the navigation tree.

   The default selection for the **Communication System** field is the selection of the global settings in the system menu.
4) To find and select a particular OpenScape SBC use one of the following options:

   - In the Work Area select the checkbox to the left of the particular SBC in the list and select **Manage**.
   - Choose a SBC from the **OpenScape SBC** pull-down located in the Navigation Tree.

   General information and data for the selected SBC is displayed in the Work Area.
5) Navigate to **Configuration > Alarms** in the navigation tree under Administration.

The **Alarms** window appears with the **Settings** tab selected by default.

The following information is provided for each type of alarm:

- **Active**:

  Determines if the alarm will be generated or not.
- **Event name**:

  Event name is a character string that describers the alarm. It is closely related to the trap name as defined in the OpenScape SBC or Branch SNMP (Simple Network Management Protocol) MIB (Management Information Base).
- **Group name**:

  Name of the GroupID. It groups together system status information of similar kind (Hardware, Ethernet, Resource, Software, Communication, Usage, Admin, License).

- **Trigger**:

  Trigger shows the condition where the alarm will be generated. Trigger is a comparison between the current value and alarm value.
- **Severity**:

  Alarm severity assigned to that particular alarm (warning, minor, major, critical). The Severity is fixed per Fault-Id.
- **Reporting class**:

  Reporting class for Alarm Settings is a number between 0 and 7 that groups events to classes which are reported to the same trap destination. The value "0" means that the event is not reported via SNMP trap.

- **Faulty object**:

  Faulty Object is a character string that defines the object that is at fault. This value may be different from SBC to SBC or branch to branch, but it is fixed for a particular SBC or branch.

  Parameters are as follows:

  – HW-Sensors (e.g., Temperature, voltage)
  – Ethernet (e.g., Port failure)
  – Resource (e.g., Bandwidth, CPU usage)
  – Survivability Provider (not running)
  – Apache/PHP (not running)
  – SIP Server (not running)
  – RTP Proxy (not running)
  – Process Manager (not running)
  – network (not running)
  – DHCP server (not running)
  – NTP (not running)
  – Syslog (not running)
  – msadapter (not running)
  – SIP Server (e.g., configuration, core, database)
  – VRRP (not running)
  – Message Rate Control (not running)
  – Update or Upgrade (failure)
  – BLC (not running)
  – BLS (not running)
  – Node 1 Primary OSV link (loss of communication)
  – Node 1 Backup OSV link (loss of communication)
  – Gateway link (loss of communication)
  – DNS link (loss of communication)
  – Billing server link (loss of communication)
  – Surveillance system link (loss of communication)
  – File Server link (loss of communication)
  – Node 2Primary OSV link (loss of communication)
  – Node 2Backup OSV link (loss of communication)
  – Redundancy (e.g., fails, disabled)
  – Geosepmgr (e.g., dat failure) (V2)
  – Voice channels (e.g., high activity)
  – Active calls (e.g., high activity)
  – Authentification (e.g., wrong password)
  – phone sw repository (e.g., failure, limit warnings) (V2)
  – Install (e.g., simplified installation failure) (V2)
  – License (e.g., Expired, blocking, violations) (V2)

4.1.1.3 How to Edit Alarms Settings

The alarm settings are displayed in a table view to provide an overview of the alarm settings for the different types of alarms.

Prerequisites

Adequate administrative permissions.

At least one OpenScape SBC is configured and in operation.

The connection to the OpenScape Voice system is up.

Step by Step

1) Navigate to **Configuration** tab > **OpenScape SBC** within the Navigation Bar in the Common Management Platform.

2) Select the **OpenScape SBC list** in the Navigation Tree under **Administration**.

The system presents the **OpenScape SBC Overview** in the Work Area with a current list of all SBCs.

3) To view a list of SBCs configured at a specific communication system, select a communication system in the **Communication System** field in the navigation tree.

The default selection for the **Communication System** field is the selection of the global settings in the system menu.

4) To find and select a particular OpenScape SBC use one of the following options:

- In the Work Area select the checkbox to the left of the particular SBC in the list and select **Manage**.
- Choose a SBC from the **OpenScape SBC** pull-down located in the Navigation Tree.

General information and data for the selected SBC is displayed in the Work Area.

5) Navigate to **Configuration** > **Alarms** > **Alarm Settings** in the navigation tree under **Administration**.

The **Alarms** window appears with the **Alarm Settings** tab selected by default.

6) Scroll down to the row of alarm to be edited in the list.

NOTICE: Some fields are "display-only-fields" and can not be modified.

---

a) Check or uncheck the **Active** checkbox to determine if the alarm will be generated or not.

b) Assign an Alarm severity in the **Severity** field. Possible values are: warning, minor, major, critical. The Severity is fixed per Fault-Id.

c) Enter a threshold in the **Threshold** field. Threshold is the value that needs to be crossed by monitored-value for an alarm to be generated. If

e.g. the existence of an alarm condition is represented by True =1 then the threshold should be 0 to trigger an alarm.

d) Enter a value in seconds in the **Flow timer** field. Flow Timer indicates the minimal time to wait before to generate a next occurrence of the same alarm.

e) Enter the reporting class in the **Reporting class** field. This number between 0 and 7 groups events to classes that are reported to the same trap destination. "0" means that the event is not reported via SNMP trap.

7) Click the **OK** button to save the changes temporarily in the administrator´s login session.

8) Click the **Apply Changes** button in the main window to save the changes permanently.

The alarm setting for the selected type of alarms is completed and applied to the system.

4.1.1.4 How to Edit Alarms Settings for earlier-than-v8 OpenScape SBC devices

The alarm settings are displayed in a table view to provide an overview of the alarm settings for the different types of alarms.

Prerequisites

Adequate administrative permissions.

At least one OpenScape SBC is configured and in operation.

The connection to the OpenScape Voice system is up.

Step by Step

1) Navigate to **Configuration** tab > **OpenScape SBC** within the Navigation Bar in the Common Management Platform.

2) Select the **OpenScape SBC list** in the Navigation Tree under **Administration**.

The system presents the **OpenScape SBC Overview** in the Work Area with a current list of all SBCs.

3) To view a list of SBCs configured at a specific communication system, select a communication system in the **Communication System** field in the navigation tree.

The default selection for the **Communication System** field is the selection of the global settings in the system menu.

4) To find and select a particular OpenScape SBC use one of the following options:

- In the Work Area select the checkbox to the left of the particular SBC in the list and select **Manage**.
- Choose a SBC from the **OpenScape SBC** pull-down located in the Navigation Tree.

General information and data for the selected SBC is displayed in the Work Area.

5) Navigate to **Configuration > Alarms** in the navigation tree under Administration.

   The **Alarms** window appears with the **Settings** tab selected by default.

6) Select the type of alarm to be edited in the list.

7) Click the **Edit** button.

   The **Edit Alarms Settings** window appears.

   Fields displayed in grey color are "display-only-fields" and can not be modified:

   - **GroupID** and **EventId**:

     This fields correspond to the SNMP trap OID (Object Identifier) (the last 2 numbers of the OID). An alarm trap is cleared by a trap with the same OID of severity 'cleared'.
   - **Group name**:

     Name of the GroupID. It groups together system status information of similar kind.
   - **Event name**:

     Event name is a character string that describers the alarm. It is closely related to the trap name as defined in the OpenScape SBC SNMP (Simple Network Management Protocol) MIB (Management Information Base).
   - **Faulty object**:

     Faulty Object is a character string that defines the object that is at fault. This value may be different from SBC to SBC, but it is fixed for a particular branch.
   - **Event type**:

     Classifies the alarms into: Communications, environmental, equipment, processing error, Quality of Service.

8) Check or uncheck the **Set as active** checkbox to determine if the alarm will be generated or not.

9) Assign an Alarm severity in the **Severity** field. Possible values are: warning, minor, major, critical. The Severity is fixed per Fault-Id.

10) Enter a threshold in the **Threshold** field. Threshold is the value that needs to be crossed by monitored-value for an alarm to be generated. If e.g. the existence of an alarm condition is represented by True =1 then the threshold should be 0 to trigger an alarm.

11) Enter a value in seconds in the **Flow timer** field. Flow Timer indicates the minimal time to wait before to generate a next occurrence of the same alarm.

12) Enter the reporting class in the **Reporting class** field. This number between 0 and 7 groups events to classes that are reported to the same trap destination. "0" means that the event is not reported via SNMP trap.

13) Click the **OK** button to save the changes temporarily in the administrator´s login session.

14) Click the **Apply Changes** button in the main window to save the changes permanently.

The alarm setting for the selected type of alarms is completed and applied to the system.

4.1.1.5 How to Edit and Add Trap Destinations

Already configured trap destinations can be edited and new trap destinations can be added.

Prerequisites

Adequate administrative permissions.

At least one OpenScape SBC is configured and in operation.

The connection to the OpenScape Voice system is up.

Step by Step

1) Navigate to **Configuration** tab > **OpenScape SBC** within the Navigation Bar in the Common Management Platform.
2) Select the **OpenScape SBC list** in the Navigation Tree under **Administration**.

   The system presents the **OpenScape SBC Overview** in the Work Area with a current list of all SBCs.
3) To view a list of SBCs configured at a specific communication system, select a communication system in the **Communication System** field in the navigation tree.

   The default selection for the **Communication System** field is the selection of the global settings in the system menu.
4) To find and select a particular OpenScape SBC use one of the following options:

   - In the Work Area select the checkbox to the left of the particular SBC in the list and select **Manage**.
   - Choose a SBC from the **OpenScape SBC** pull-down located in the Navigation Tree.

   General dialogue is presented in the Work Area displaying information and data for the selected SBC.
5) Navigate to **Configuration** > **Alarms** > **Trap Destinations** in the navigation tree under **Administration**.

   The **Alarms** window appears with the **Trap Destinations** tab selected by default.

   The list with the trap destinations configured is displayed:

   - **IP Address**

     This column defines the IP address (IPv4) used for sending a trap.
   - **Port**:

     This column defines the internal port used for sending the trap.
   - **Blocked**:

     A trap will not be sent when this checkbox is checked.
   - **Reporting class set**:

     Reporting class is a number between 1 and 7 that groups events to classes which are reported to the same trap destination.

6) To edit an existing trap destination, click on the **IP Address**, **Port**, **Blocked** checkbox or **Reporting class set** field and modify to the correct value.
7) To add a new trap destination, click the **Add** button.

   A new Trap Destination row appears.

   Edit each field for the new Trap Destination.
   a) To modify or add the IP address used for sending the trap, enter the new address in the **IP Address** field.
   b) To modify or add the port number of the internal port used for sending the trap, enter the new number in the **Port** field.
   c) To modify or add the value used as reporting class, enter the new value in the range of 1...7 in the **Reporting class set** field. Multiple classes can be entered and each class can only be entered once e.g., 1;2;5;6;7 or 1;2;3;4;5.
   d) To block or unblock a trap check or uncheck the **Blocked** checkbox.
8) Click the **OK** button to save the changes temporarily in the administrator´s login session.

   The **Alarms** window disappears and the **General** window appears for the selected SBC.
9) Click the **Apply Changes** button in the main window to save the changes permanently.

This modification of the trap destination or the new trap destination entry is completed and applied to the system.

4.1.1.6 How to Edit and Add Trap Destinations for earlier-than-v8 OpenScape SBC devices

Already configured trap destinations can be edited and new trap destinations can be added.

Prerequisites

Adequate administrative permissions.

At least one OpenScape SBC is configured and in operation.

The connection to the OpenScape Voice system is up.

Step by Step

1) Navigate to **Configuration** tab > **OpenScape SBC** within the Navigation Bar in the Common Management Platform.
2) Select the **OpenScape SBC list** in the Navigation Tree under **Administration**.

   The system presents the **OpenScape SBC Overview** in the Work Area with a current list of all SBCs.

3) To view a list of SBCs configured at a specific communication system, select a communication system in the **Communication System** field in the navigation tree.

   The default selection for the **Communication System** field is the selection of the global settings in the system menu.

4) To find and select a particular OpenScape SBC use one of the following options:

   - In the Work Area select the checkbox to the left of the particular SBC in the list and select **Manage**.
   - Choose a SBC from the **OpenScape SBC** pull-down located in the Navigation Tree.

   General information and data for the selected SBC is displayed in the Work Area.

5) Navigate to **Configuration > Alarms** in the navigation tree under Administration.

   The **Alarms** window appears with the **Settings** tab selected by default.

6) Select the **Trap destinations** tab.

   The list with the trap destinations configured is displayed:

   - **IP Address**

     This column defines the IP address (IPv4) used for sending a trap.
   - **Port**:

     This column defines the internal port used for sending the trap.
   - **Blocked**:

     A trap will not be sent when this checkbox is checked.
   - **Reporting class set**:

     Reporting class is a number between 1 and 7 that groups events to classes which are reported to the same trap destination.

7) To modify an existing trap destination, select the respective trap destination in the list and click the **Edit** button.

   The **Edit trap destination SNMP** window appears.

8) To add a new trap destination, click the **Add** button.

   The **Add trap destination SNMP** window appears.

9) To modify or add the IP address used for sending the trap, enter the new address in the **IP Address** field.

10) To modify or add the port number of the internal port used for sending the trap, enter the new number in the **Port** field.

11) To modify or add the value used as reporting class, enter the new value in the range of 1...7 in the **Reporting class set** field. Multiple classes can be entered and each class can only be entered once e.g., 1;2;5;6;7 or 1;2;3;4;5.

12) To block or unblock a trap check or uncheck the **Blocked** checkbox.

13) Click the **OK** button to confirm the changes.

    The **Edit trap destination SNMP** or **Add trap destination SNMP** window disappears and the **Alarms** window appears.

14) Click the **OK** button to save the changes temporarily in the administrator´s login session.

    The **Alarms** window disappears and the **General Branch** window appears.

15) Click the **Apply Changes** button in the main window to save the changes permanently.

This modification of the trap destination or the new trap destination entry is completed and applied to the system.

4.1.1.7 How to Display and Delete Trap Destinations

The configured trap destinations can be displayed.

Prerequisites

Adequate administrative permissions.

At least one OpenScape SBC is configured and in operation.

The connection to the OpenScape Voice system is up.

Step by Step

1) Navigate to **Configuration** tab > **OpenScape SBC** within the Navigation Bar in the Common Management Platform.
2) Select the **OpenScape SBC list** in the Navigation Tree under **Administration**.

   The system presents the **OpenScape SBC Overview** in the Work Area with a current list of all SBCs.

3) To view a list of SBCs configured at a specific communication system, select a communication system in the **Communication System** field in the navigation tree.

   The default selection for the **Communication System** field is the selection of the global settings in the system menu.

4) To find and select a particular OpenScape SBC use one of the following options:

   - In the Work Area select the checkbox to the left of the particular SBC in the list and select **Manage**.
   - Choose a SBC from the **OpenScape SBC** pull-down located in the Navigation Tree.

   General dialogue is presented in the Work Area displaying information and data for the selected SBC.

5) Navigate to **Configuration** > **Alarms** > **Trap Destinations** in the navigation tree under **Administration**.

   The **Alarms** window appears with the **Trap Destinations** tab selected by default.

   The list with the trap destinations configured is displayed:

   - **IP Address**

     This column defines the IP address (IPv4) used for sending a trap.
   - **Port**:

     This column defines the internal port used for sending the trap.
   - **Blocked**:

     A trap will not be sent when this checkbox is checked.
   - **Reporting class set**:

     Reporting class is a number between 1 and 7 that groups events to classes which are reported to the same trap destination.

     NOTICE: When in BLS mode, the reporting class 6 is used to inform the Backup Link status.

6) To edit an existing trap destination, click on the **IP Address**, **Port**, **Blocked** checkbox or **Reporting class set** field and modify to the correct value.
7) To delete an existing trap destination, select the respective trap destination in the list and click the **Delete** button.

   The trap destination is removed from the list.
8) Click the **OK** button to save the changes temporarily in the administrator´s login session.
9) Click the **Apply Changes** button in the main window to save the changes permanently.

If a trap destination has been deleted, the modification is completed and applied to the system.

4.1.1.8 How to Display and Delete Trap Destinations for earlier-than-v8 OpenScape SBC devices

The configured trap destinations can be displayed.

Prerequisites

Adequate administrative permissions.

At least one OpenScape SBC is configured and in operation.

The connection to the OpenScape Voice system is up.

Step by Step

1) Navigate to **Configuration** tab > **OpenScape SBC** within the Navigation Bar in the Common Management Platform.

2) Select the **OpenScape SBC list** in the Navigation Tree under **Administration**.

   The system presents the **OpenScape SBC Overview** in the Work Area with a current list of all SBCs.

3) To view a list of SBCs configured at a specific communication system, select a communication system in the **Communication System** field in the navigation tree.

   The default selection for the **Communication System** field is the selection of the global settings in the system menu.

4) To find and select a particular OpenScape SBC use one of the following options:

   - In the Work Area select the checkbox to the left of the particular SBC in the list and select **Manage**.
   - Choose a SBC from the **OpenScape SBC** pull-down located in the Navigation Tree.

   General information and data for the selected SBC is displayed in the Work Area.

5) Navigate to **Configuration > Alarms** in the navigation tree under Administration.

   The **Alarms** window appears with the **Settings** tab selected by default.

6) Select the **Trap destinations** tab.

   The list with the trap destinations configured is displayed:

   - **IP Address:**

     This column defines the IP address used for sending a trap.
   - **Port**:

     This column defines the internal port used for sending the trap.
   - **Blocked**:

     A trap will not be sent when this checkbox is checked.
   - **Reporting class set**:

     Reporting class is a number between 1 and 7 that groups events to classes which are reported to the same trap destination.

     NOTICE: When in BLS mode, the reporting class 6 is used to inform the Backup Link status.

7) To delete an existing trap destination, select the respective trap destination in the list and click the **Delete** button.

   The trap destination is removed from the list.

8) Click the **OK** button to save the changes temporarily in the administrator´s login session.

9) Click the **Apply Changes** button in the main window to save the changes permanently.

If a trap destination has been deleted, the modification is completed and applied to the system.

4.2 Logging Configuration Overview

The logging configuration enables the administrator to modify and enter logging settings. Debugging provides tools to analyze the network components. Continuous Tracing and On Demand Trace serve for analyzing the software, network, and configuration problems for maintenance purposes.

4.2.1 Logging for OpenScape Session Border Controller

Logging allows the administrator to set log levels for OpenScape Session Border Controllers (SBC).

Log Types

The following logs are available for OpenScape Session Border Controllers:

- Alarm History (view only):

  Alarm history, showing all active or cleared alarms.
- Alarm Manager:

  Log of Alarm manager application.
- Boot (view only):

  Log of last boot.
- CDR:

  The Log for Call Detail Records.
- Continuous Tracing:

  Log of the Continuous Tracing application.
- Current processes (view only):

  A list of the current processes running on OpenScape SBC.
- EVO Database
- EVO Https
- EVO Reverse Proxy
- EVO WebSocket
- Firewall & Msg Rate Control
- Install/Update/Upgrade (view only):

  Log from system installation, updates or upgrades (also includes language installation logs).
- Media Server Adapter:

  Log of NAT transversal of the MGCP communications.
- Process Manager:

  Log of PM application.
- RTP (Real-Time Transport Protocol) Proxy:

  Log of RTP Proxy application.
- QoS Application
- QoS Monitoring
- RTP Proxy
- Registration Blacklist

- SIP Server:

  SIP stateful proxy or SBC application.
- SSM (SIP Services Module)

  Log of SIP Services
- Simplified Installation
- Survivability Provider:

  Log of Survivability provider application.
- System (view only):

  Log of system events.
- Web server (view only):

  Log of the local web server application

OpenScape SBC Applications and Functional Components

For the following OpenScape SBC log levels can be set:

- Alarm Manager
- Continuous Tracing
- MS Adapter
- Process Manager
- RTP (Real-time Transport Protocol) Proxy
- SIP (Session Initiation Protocol) Server
- SSM (SIP Services Module)
- Survivability Provider

Log Levels

The following log levels are predefined an can be assigned individually to each OpenScape SBC:

- Emergency

  Emergency is a panic condition report.
- Alert

  Alert reports a condition that should be corrected immediately, such as failure in configuration.
- Critical

  Critical is a report of device failures.
- Error

  Error is a level used for applications to report internal errors.
- Warning

  Warning is a level to be used to report application instability.
- Notice

  Notice will report conditions that are not errors, but should require some attention.
- Info

  Info is used for informational messages.
- Debug

  Debug is the level used for debugging applications. This level may affect the system performance and will generate several log files.

4.2.1.1 How to Edit Settings for Logs

Proceed as follows to assign log levels for OpenScape SBC and Branch applications or functional components and configure the fallback data.

Prerequisites

Adequate administrative permissions.

At least one OpenScape SBC is configured and in operation.

The connections to the OpenScape Voice system and to the WAN/LAN are up.

Step by Step

1) Navigate to **Configuration** tab > **OpenScape SBC** within the Navigation Bar in the Common Management Platform.

2) Select the **OpenScape SBC list** in the Navigation Tree under **Administration**.

The system presents the **OpenScape SBC Overview** in the Work Area with a current list of all SBCs.

3) To view a list of SBCs configured at a specific communication system, select a communication system in the **Communication System** field in the navigation tree.

The default selection for the **Communication System** field is the selection of the global settings in the system menu.

4) To find and select a particular OpenScape SBC use one of the following options:

- In the Work Area select the checkbox to the left of the particular SBC in the list and select **Manage**.
- Choose a SBC from the **OpenScape SBC** pull-down located in the Navigation Tree.

General dialogue is presented in the Work Area displaying information and data for the selected SBC.

5) Navigate to **Configuration** > **Diagnostics & Logs** > **Settings** in the navigation tree under **Administration**.

The **Diagnostics & logs** window appears with the **Settings** tab selected by default.

6) Select a log level from the drop-down list for each log entry. Each of the drop-down entry fields provide the following selection list entries:

   - **Emergency**

     Emergency is a panic condition report.
   - **Alert**

     Alert reports a condition that should be corrected immediately, such as failure in configuration.
   - **Critical**

     Critical is a report of device failures.
   - **Error**

     Error is a level used for applications to report internal errors.
   - **Warning**

     Warning is a level to be used to report application instability.
   - **Notice**

     Notice will report conditions that are not errors, but should require some attention.
   - **Info**

     Info is used for informational messages.
   - **Debug**

     Debug is the level used for debugging applications. This level may affect the system performance and will generate several log files.

7) Enter the maximum file size for log files in the **Log size** field. Once a log file reaches this value it is closed, renamed in a sequential number and a new log file is created.
8) Enter the IP address (IPv4) of the external Server to be used to receive syslog messages in the **Syslog server** field.
9) If the log levels shall be set to the default log level, select the **Fallback to default log level** checkbox in the **Fallback Settings** field area.
10) Enter the fallback time in the **Fallback time** fields (format hh.mm, default value 01:06). This is the time of the day when the OpenScape SBC resets the continuous tracing configuration back to default.
11) Click the **OK** button to save the changes temporarily in the administrator´s login session.
12) Click the **Apply Changes** button in the main window to save the changes permanently.

The settings for logging are completed and applied to the system.

4.2.1.2 How to Edit Settings for Logs for earlier-than-v8 OpenScape SBC devices

Proceed as follows to assign log levels for OpenScape SBC and Branch applications or functional components and configure the fallback data.

Prerequisites

Adequate administrative permissions.

At least one OpenScape SBC is configured and in operation.

The connections to the OpenScape Voice system and to the WAN/LAN are up.

Step by Step

1) Navigate to **Configuration** tab > **OpenScape SBC** within the Navigation Bar in the Common Management Platform.
2) Select the **OpenScape SBC list** in the Navigation Tree under **Administration**.

   The system presents the **OpenScape SBC Overview** in the Work Area with a current list of all SBCs.
3) To view a list of SBCs configured at a specific communication system, select a communication system in the **Communication System** field in the navigation tree.

   The default selection for the **Communication System** field is the selection of the global settings in the system menu.
4) To find and select a particular OpenScape SBC use one of the following options:

   - In the Work Area select the checkbox to the left of the particular SBC in the list and select **Manage**.
   - Choose a SBC from the **OpenScape SBC** pull-down located in the Navigation Tree.

   General dialogue is presented in the Work Area displaying information and data for the selected SBC.
5) Navigate to **Configuration** > **Logging** in the navigation tree under **Administration**.

   The **Logging** window appears with the **Settings** tab selected by default.

6) For each OpenScape SBC application or functional component the selection list provides the following entries:

- **Emergency**

  Emergency is a panic condition report.
- **Alert**

  Alert reports a condition that should be corrected immediately, such as failure in configuration.
- **Critical**

  Critical is a report of device failures.
- **Error**

  Error is a level used for applications to report internal errors.
- **Warning**

  Warning is a level to be used to report application instability.
- **Notice**

  Notice will report conditions that are not errors, but should require some attention.
- **Info**

  Info is used for informational messages.
- **Debug**

  Debug is the level used for debugging applications. This level may affect the system performance and will generate several log files.

a) Select a log level for **SIP Server** (Session Initiation Protocol).
b) Select a log level for **Process Manager**.
c) Select a log level for **Alarm Manager**.
d) Select a log level for **Continuos Tracing**.
e) Select a log level for **CDR** (Call Detail Records).
f) Select a log level for **MS Adapter**
g) Select a log level for **Survivability Provider**.
h) Select a log level for **RTP Proxy** (Real-time Transport Protocol).
i) Select a log level for **SSM** (SIP Services Module)
j) Select a log level for **Geo-Redundancy**

7) Enter the maximum file size for log files in the **Log size** field. Once a log file reaches this value it is closed, renamed in a sequential number and a new log file is created.

8) Enter the IP address (IPv4) of the external Server to be used to receive syslog messages in the **Syslog server** field.

9) If the log levels shall be set to the default log level, select the **Fallback to default log level** checkbox in the **Fallback Settings** field area.

10) Enter the fallback time in the **Fallback time** fields (format hh.mm, default value 01:06). This is the time of the day when the OpenScape Branch resets the continuous tracing configuration back to default.

11) Click the **OK** button to save the changes temporarily in the administrator´s login session.

12) Click the **Apply Changes** button in the main window to save the changes permanently.

The settings for logging are completed and applied to the system.

4.2.2 Debugging

Debugging provides tools to analyze the network components.

Debugging

The debugging functionality enables the administrator to use the following debugging tools:

- ICMP (Internet Control Message Protocol)

  This tool can be used to send a ping request to a destination in the IP network.
- Traceroute

  This tool shows the hops from the origin to the given destination in the IP network.
- Network Tracer

  This tool collects IP packages from the IP network and exports the information for decoding.

4.2.2.1 How to Use Debugging Tools

Proceed as follows to use debugging tools in order to analyze the network components.

Prerequisites

Adequate administrative permissions.

At least one OpenScape SBC is configured and in operation.

The connections to the OpenScape Voice system and to the WAN/LAN are up.

Step by Step

1) Navigate to **Configuration** tab > **OpenScape SBC** within the Navigation Bar in the Common Management Platform.

2) Select the **OpenScape SBC list** in the Navigation Tree under **Administration**.

The system presents the **OpenScape SBC Overview** in the Work Area with a current list of all SBCs.

3) To view a list of SBCs configured at a specific communication system, select a communication system in the **Communication System** field in the navigation tree.

The default selection for the **Communication System** field is the selection of the global settings in the system menu.

4) To find and select a particular OpenScape SBC use one of the following options:

   - In the Work Area select the checkbox to the left of the particular SBC in the list and select **Manage**.
   - Choose a SBC from the **OpenScape SBC** pull-down located in the Navigation Tree.

   General dialogue is presented in the Work Area displaying information and data for the selected SBC.

5) Navigate to **Configuration** > **Diagnostics & Logs** > **Debugging** in the navigation tree under **Administration**.

   The **Diagnostics & logs** window appears with the **Debugging** tab selected by default.

6) Use one of the following debugging tools from the **Tool** drop-down selection list to analyze the functionality of a network element:

   - **ICMP** (Internet Control Message Protocol)

     Select **ICMP** and enter for example the IP address (IPv4 or IPv6) of the component the PING request shall be sent to in the **Options** field.
   - **Traceroute**

     Select **Traceroute** and enter for example the IP address (IPv4 or IPv6) of the component the request shall be sent to in the **Options** field.
   - **Network Tracer**

     Select **Network Tracer** and select an option/filter from the **Interface** drop-down selection list: All interfaces, SIP/MGCP Trace, SIP/MGCP/RTP Trace.

   NOTICE: ICMP (Internet Control Message Protocol) and traceroute services are not parsed. All commands supported by ping and traceroute can be entered.

7) Click the **Start** button and wait for the **Stop** button to activate.

   The action is started and the answer of the request is stored in the selected Log data entry.

   NOTICE: The ICMP and Traceroute requests must complete and can not be aborted.

8) Click the **Stop** button to complete the request(s).

   Each of the request results can be displayed or saved to a file, one download at a time.

9) Click the **View** button to the right of **Results** to view the result of the request.

   The **Debug results viewer** window opens.

10) Click the **Export** button, and then the **Open** button to open the log file or the **Save** button to save the log file.

11) Click the **OK** button to finish the debugging session and close the **Diagnostics & logs** window.

4.2.2.2 How to Use Debugging Tools for earlier-than-v8 OpenScape SBC devices

Proceed as follows to use debugging tools in order to analyze the network components.

Prerequisites

Adequate administrative permissions.

At least one OpenScape SBC is configured and in operation.

The connections to the OpenScape Voice system and to the WAN/LAN are up.

Step by Step

1) Navigate to **Configuration** tab > **OpenScape SBC** within the Navigation Bar in the Common Management Platform.

2) Select the **OpenScape SBC list** in the Navigation Tree under **Administration**.

The system presents the **OpenScape SBC Overview** in the Work Area with a current list of all SBCs.

3) To view a list of SBCs configured at a specific communication system, select a communication system in the **Communication System** field in the navigation tree.

The default selection for the **Communication System** field is the selection of the global settings in the system menu.

4) To find and select a particular OpenScape SBC use one of the following options:

- In the Work Area select the checkbox to the left of the particular SBC in the list and select **Manage**.
- Choose a SBC from the **OpenScape SBC** pull-down located in the Navigation Tree.

General dialogue is presented in the Work Area displaying information and data for the selected SBC.

5) Navigate to **Configuration** > **Logging** in the navigation tree under **Administration**.

The **Logging** window appears with the **Settings** tab selected by default.

6) Select the **Debugging** tab in the **Logging** window

7) Use one or more of the following debugging tools to analyze the functionality of a network element:

   - **ICMP** (Internet Control Message Protocol)

     Click the **ICMP** checkbox and enter for example the IP address (IPv4 or IPv6) of the component the PING request shall be sent to in the **Parameter** field.
   - **Traceroute**

     Click the **Traceroute** checkbox and enter for example the IP address (IPv4 or IPv6) of the component the request shall be sent to in the **Parameter** field.
   - **Network Tracer**

     Click the **Network Tracer** checkbox and select an option/filter from the following entries: All interfaces, SIP server, SIP server with TLS (Transparent LAN Service).

   NOTICE: ICMP (Internet Control Message Protocol) and traceroute services are not parsed. All commands supported by ping and traceroute can be entered.

8) Click the **Start** button and wait for the **Stop** button to activate.

   The action is started and the answer of the request is displayed in the **Results display** field area for the ICMP and Traceroute request.

   NOTICE: The ICMP and Traceroute requests must complete and can not be aborted.

9) Click the **Stop** button to complete the request(s).

   The request information is displayed in the **Results display** field area for the ICMP and Traceroute request. Each of the request results can be displayed or saved to a file, one download at a time.

10) Click the **Download** button beside the **Network Tracer log file** text to view the result of the network tracer request.

    The **Save file window** opens.

11) In the **Save file window**, click the **Open** button to open the log file or click the **Save** button to save the log file.

12) To remove the results from the **Results display** fields, click the **Clear results** button.

13) Click the **OK** button to finish the debugging session and close the **Logging** window.

4.2.3 Continuous Tracing and On Demand Trace

Tracing serves for analyzing the software, network, and configuration problems for maintenance purposes.

The OpenScape Voice Trace Management provides an interface for call tracing and analysis within the network. The tracing functionality collects the detailed call data needed by field technicians, developers, system testers, and support engineers to efficiently analyze software, network, and configuration problems.

Functional Sequence

The SIP (Session Initiation Protocol) traces or MGCP (Media Gateway Control Protocol) traces can be started, stopped or restarted by the OpenScape SBC Assistant. The OpenScape Voice trace management has an SFTP (Secure File Transfer Protocol) server. An SFTP client is used to transfer the files to the Continuous Tracing tool. After being transferred, the trace file is deleted.

The file names are:
`<OpenBranchNodeName>_sipmgcp_<yyyymmddhhmmss>.cap.bz2,<OpenBranchNodeN`
`<LogType> = sip|b2b|ms|cdr|pm|sp|rtp|alm|alh|sys|boot|snt|updtrc`

When the transfer of a file or a group of files to the Continuous Trace server is finished, an empty flag file is transferred to the Continuous Trace server to indicate that a new file was copied.

Every time the Continuous Trace tool detects the flag file and collects the new received files it deletes the flag file. If due to a network problem a file transfer fails, the system keeps this information so that the file is transferred in a later opportunity.

By every file rotation the file names are changed, since the last generated file is always named nn.log.1.bz2. The branch node name and timestamp which is added to the target name contains the time when the file was created and not the time of the transfer. This is relevant when the file transfer is postponed due to network problems.

Continuous Tracing Configuration

The OpenScape Session Border Controller (SBC) must be configured to connect to the trace server in order to transfer trace files in the **Configuration** > **OpenScape SBC** > **Administration** area > **Configuration** > **Diagnostics & Logs** > **Continuous Tracing** tabsheet.

The configuration of the log levels must be configured in the **Diagnostics & Logs** > **Settings** tabsheet. The log level which is set for Continuous Tracing will also be valid for accessing the logs via Assistant or CMP. The following logs will be transferred from OpenScape SBC to OSV-TM (Trace Manager):

- Alarm History (view only),
- Alarm Manager,
- Boot (view only),
- CDR,
- Continuous Tracing
- Update/Upgrade/Install,
- Process Manager,
- RTP Proxy,
- SIP Server,
- SSM SIP Service Module,
- Survivability Provider,
- System (view only).

The log levels of the following logs can be configured:

Log	Default Level
Alarm Manager	Error
Continuous Tracing	Error

Log	Default Level
MS Adapter	Error
Process Manager	Error
RTP Proxy	Error
SIP Server	Error
SSM (SIP Services Module)	Error
Survivability Provider	Error

On Demand Trace Configuration

The On Demand Trace function allows to select a log type and log level and start or stop the tracing instantly. For OpenScape Session Border Controllers the log type can be one of the following:

- Alarm Manager,
- Continuous Tracing,
- Process Manager,
- Redundancy,
- RTP Proxy,
- SIP Server,
- SSM (SIP Services Module),
- Survivability Provider,

The following log levels are predefined an can be assigned:

- Emergency
- Alert
- Critical
- Error
- Warning
- Notice
- Info
- Debug

4.2.3.1 How to Configure Continuous Tracing

Proceed as follows to configure continuous tracing for an OpenScape SBC.

Prerequisites

Adequate administrative permissions.

At least one OpenScape SBC is configured and in operation.

The connections to the OpenScape Voice system and to the WAN/LAN are up.

The log levels have been configured in the **Diagnostics & Logs**> **Settings** tabsheet.

Step by Step

1) Navigate to **Configuration** tab > **OpenScape SBC** within the Navigation Bar in the Common Management Platform.
2) Select the **OpenScape SBC list** in the Navigation Tree under **Administration**.

   The system presents the **OpenScape SBC Overview** in the Work Area with a current list of all SBCs.
3) To view a list of SBCs configured at a specific communication system, select a communication system in the **Communication System** field in the navigation tree.

   The default selection for the **Communication System** field is the selection of the global settings in the system menu.
4) To find and select a particular OpenScape SBC use one of the following options:

   - In the Work Area select the checkbox to the left of the particular SBC in the list and select **Manage**.
   - Choose a SBC from the **OpenScape SBC** pull-down located in the Navigation Tree.

   General dialogue is presented in the Work Area displaying information and data for the selected SBC.
5) Navigate to **Configuration** > **Diagnostics & Logs** > **Settings** in the navigation tree under **Administration**.

   The **Diagnostics & logs** window appears with the **Settings** tab selected by default.
6) If the log levels shall be set to the default log level, select the **Fallback to default log level** checkbox in the **Fallback** field area.
7) Enter the fallback time in the **Fallback time** fields (format hh.mm, default value 01:06). This is the time of the day when the OpenScape SBC resets the trace configuration back to default.
8) Click on the **Continuous Tracing** tab.
9) To activate the continuous tracing function, check the **Enable** checkbox.
10) Configure the general settings as follows:
    a) Enter the IP address (IPv4) or the FQDN of the continuous tracing tool for establishing the SFTP (Secure File Transfer Protocol) session in the **Server** field.
    b) Specify the size of the file which will be used to rotate the log/trace file in the **File size threshold** field. Range: 1 – 1024 (Kbytes), default 256 KB.
    c) Specify the time interval of the file which will be used to rotate the log/trace file in the **Time interval threshold** field. Range: 1 – 60 (minutes), default: 5 minutes.
    d) Check the **SIP/Q931 trace** checkbox to control the Session Initiation Protocol status for integrated gateways.
    e) Check the **MGCP trace** checkbox to control the Media Gateway Control Protocol status.

11) Enter SFTP server data in the **SFTP** field area as follows:
    a) Enter the of the SFTP server in the **System name** field.
    b) Enter the username for identification on the SFTP server in the **Username** filed.
    c) Enter the password to identify on the SFTP server in the **Password** field.
12) Click the **OK** button to save the changes temporarily in the administrator´s login session.
13) Click the **Apply Changes** button in the main window to save the changes permanently.

The settings for continuous tracing are applied to the system.

4.2.3.2 How to Configure Continuous Tracing for earlier-than-v8 OpenScape SBC devices

Proceed as follows to configure continuous tracing for an OpenScape SBC or Branch office.

Prerequisites

Adequate administrative permissions.

At least one OpenScape SBC is configured and in operation.

The connections to the OpenScape Voice system and to the WAN/LAN are up.

The log levels have been configured in the **Logging > Settings** tabsheet.

Step by Step

1) Navigate to **Configuration** tab > **OpenScape SBC** within the Navigation Bar in the Common Management Platform.
2) Select the **OpenScape SBC list** in the Navigation Tree under **Administration**.

   The system presents the **OpenScape SBC Overview** in the Work Area with a current list of all SBCs.
3) To view a list of SBCs configured at a specific communication system, select a communication system in the **Communication System** field in the navigation tree.

   The default selection for the **Communication System** field is the selection of the global settings in the system menu.
4) To find and select a particular OpenScape SBC use one of the following options:

   - In the Work Area select the checkbox to the left of the particular SBC in the list and select **Manage**.
   - Choose a SBC from the **OpenScape SBC** pull-down located in the Navigation Tree.

   General dialogue is presented in the Work Area displaying information and data for the selected SBC.

5) Navigate to **Configuration** > **Logging** in the navigation tree under **Administration**.

   The **Logging** window appears with the **Settings** tab selected by default.

6) If the log levels shall be set to the default log level, select the **Fallback to default log level** checkbox in the **Fallback Settings** field area.

7) Enter the fallback time in the **Fallback time** fields (format hh.mm, default value 01:06). This is the time of the day when the OpenScape SBC resets the trace configuration back to default.

8) Select the **Continuous Tracing** tabsheet.

9) To activate the continuous tracing function, check the **Enable** checkbox.

10) Configure the general settings in the **General** field area as follows:
    a) Enter the IP address (IPv4) or the FQDN of the continuous tracing tool for establishing the SFTP (Secure File Transfer Protocol) session in the **Server** field.
    b) Specify the size of the file which will be used to rotate the log/trace file in the **File size threshold** field. Range: 1 – 1024 (Kbytes), default 256 KB.
    c) Specify the time interval of the file which will be used to rotate the log/trace file in the **Time interval threshold** field. Range: 1 – 60 (minutes), default: 5 minutes.
    d) Check the **SIP/Q931 trace** checkbox to control the Session Initiation Protocol status for integrated gateways.
    e) Check the **MGCP trace** checkbox to control the Media Gateway Control Protocol status.

11) Enter SFTP server data in the **SFTP** field area as follows:
    a) Enter the of the SFTP server in the **System name** field.
    b) Enter the username for identification on the SFTP server in the **Username** filed.
    c) Enter the password to identify on the SFTP server in the **Password** field.

12) Click the **OK** button to save the changes temporarily in the administrator´s login session.

13) Click the **Apply Changes** button in the main window to save the changes permanently.

The settings for continuous tracing are applied to the system.

4.2.3.3 How to Start, Stop and Configure On Demand Tracing

Proceed as follows start, stop and configure the settings for on demand tracing for an OpenScape SBC.

Prerequisites

Adequate administrative permissions.

At least one OpenScape SBC is configured and in operation.

The connections to the OpenScape Voice system and to the WAN/LAN are up.

The SFTP server has been assigned in the **Configuration > OpenScape SBC** > **Configuration** in the navigation tree **Administration** area > **Diagnostics & Logs** >**Continuous Tracing** tabsheet.

Step by Step

1) Navigate to **Configuration** tab > **OpenScape SBC** within the Navigation Bar in the Common Management Platform.

2) Select the **OpenScape SBC list** in the Navigation Tree under **Administration**.

The system presents the **OpenScape SBC Overview** in the Work Area with a current list of all SBCs.

3) To view a list of SBCs configured at a specific communication system, select a communication system in the **Communication System** field in the navigation tree.

The default selection for the **Communication System** field is the selection of the global settings in the system menu.

4) To find and select a particular OpenScape SBC use one of the following options:

- In the Work Area select the checkbox to the left of the particular SBC in the list and select **Manage**.
- Choose a SBC from the **OpenScape SBC** pull-down located in the Navigation Tree.

General dialogue is presented in the Work Area displaying information and data for the selected SBC.

5) Navigate to **Configuration** > **Diagnostics & Logs** > **On Demand Trace** in the navigation tree under **Administration**.

The **Diagnostics & logs** window appears with the **On Demand Trace** tab selected by default.

6) Select the log type to be created in the **Log Type** selection list. The following log types are listed:

- Alarm Manager,
- CDR
- Continuous Tracing,
- Media Server Adapter,
- Process Manager,
- QoS Application
- RTP Proxy,
- SIP Server,
- SSM (SIP Services Module),
- Survivability Provider.

7) Select the log level in the **Log Level** selection list.

8) Enter the duration of the tracing in the **Duration** field in minutes.

9) To activate the tracing function, click the **Start** button.

The trace function starts immediately and the data is transferred to the server assigned in the **SFTP** field area in the **Continuous Tracing** tab. A notification message appears.

NOTICE: During the on demand trace, the continuous tracing function stops automatically. After the on demand trace has been finished, the continuous tracing function continues operation again.

---

10) To deactivate the tracing function, click the **Stop** button.

The trace function stops immediately and a notification message appears.

4.2.3.4 How to Start, Stop and Configure On Demand Tracing for earlier-than-v8 OpenScape SBC devices

Proceed as follows start, stop and configure the settings for on demand tracing for an OpenScape SBC.

Prerequisites

Adequate administrative permissions.

At least one OpenScape SBC is configured and in operation.

The connections to the OpenScape Voice system and to the WAN/LAN are up.

The SFTP server has been assigned in the **Configuration > OpenScape SBC** > **Configuration** in the navigation tree **Administration** area > **Logging > Continuous Tracing** tabsheet.

Step by Step

1) Navigate to **Configuration** tab > **OpenScape SBC** within the Navigation Bar in the Common Management Platform.
2) Select the **OpenScape SBC list** in the Navigation Tree under **Administration**.

   The system presents the **OpenScape SBC Overview** in the Work Area with a current list of all SBCs.
3) To view a list of SBCs configured at a specific communication system, select a communication system in the **Communication System** field in the navigation tree.

   The default selection for the **Communication System** field is the selection of the global settings in the system menu.
4) To find and select a particular OpenScape SBC use one of the following options:

   - In the Work Area select the checkbox to the left of the particular SBC in the list and select **Manage**.
   - Choose a SBC from the **OpenScape SBC** pull-down located in the Navigation Tree.

   General dialogue is presented in the Work Area displaying information and data for the selected SBC.

5) Navigate to **Configuration** > **Logging** in the navigation tree under **Administration**.

   The **Logging** window appears with the **Settings** tab selected by default.

6) Select the **On Demand Trace** tab.

7) Select the log type to be created in the **Log Type** selection list. The following log types are listed:

   - Geo-Redundancy
   - Alarm Manager,
   - Continuous Tracing,
   - Media Server,
   - Process Manager,
   - RTP Proxy,
   - Redundancy,
   - SIP Server,
   - SSM (SIP Services Module),
   - Survivability Provider.

8) Select the log level in the **Log Level** selection list.

9) Enter the duration of the tracing in the **Duration** field in minutes.

10) To activate the tracing function, click the **Start** button.

    The trace function starts immediately and the data is transferred to the server assigned in the **SFTP** field area in the **Continuous tracing** tab. A notification message appears.

    NOTICE: During the on demand trace, the continuous tracing function stops automatically. After the on demand trace has been finished, the continuous tracing function continues operation again.

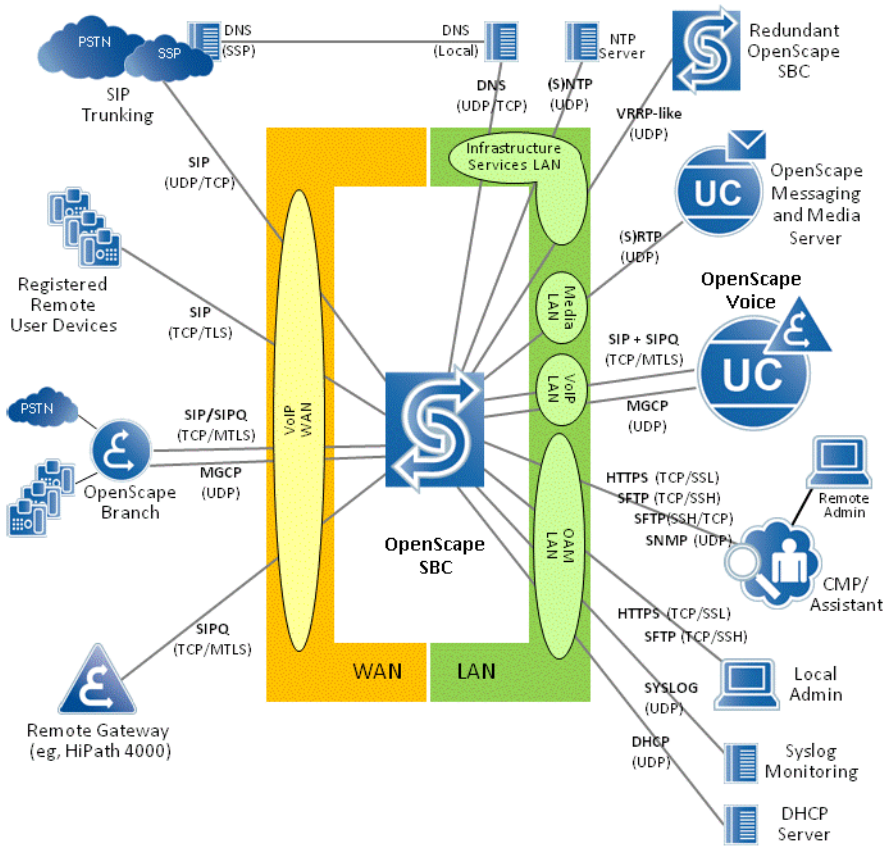
11) To deactivate the tracing function, click the **Stop** button.

    The trace function stops immediately and a notification message appears.

4.3 Network Services — Overview

Network Services comprise configuration of interfaces, routing and traffic shaping as well as NTP (Network Time Protocol) and DNS (Domain Name System) settings.

External Protocol Overview



Via network services the following data can be configured:

- **Interfaces**

  Depending on the hardware used, up to two addresses can be configured for the WAN (Wide Area Network), up to four addresses for LAN (Local Area Network). A pre-defined configuration of interfaces can be done using the USB Stick Wizard.
- **Routing**

  Routing regarding the network services comprise the configuration of the default gateway address and IP routes.
- **Redundancy**

  There are various options for redundancy used to protect connectivity through the customers network.
- **Traffic Shaping**

  Traffic shaping (also known as "packet shaping") serves for controlling computer network traffic in order to optimize or guarantee performance, low latency, and/or bandwidth by delaying packets.
- **NTP**

  Network Time Protocol is used for synchronizing the time and date of the OpenScape SBC appliance in the network.

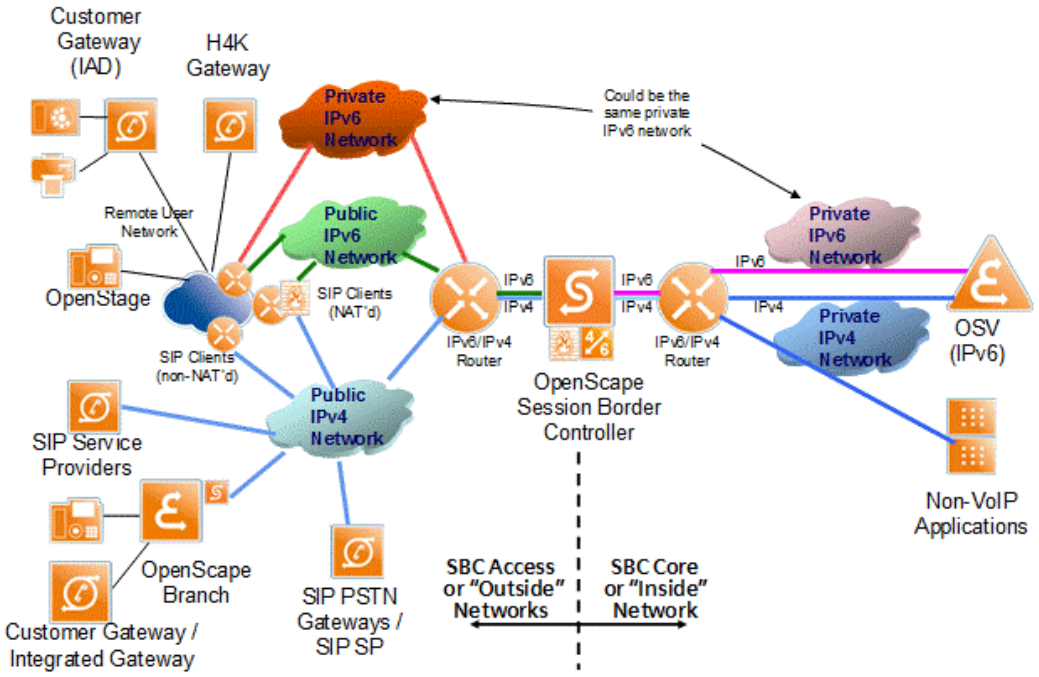
- **DNS**

  The Domain Name System client can be configured in the OpenScape SBC in order to resolve FQDNs (Fully Qualified Domain Name). The OpenScape SBC system acts as DNS client. In the server section the OpenScape SBC Domain Name can be configured. A pre-defined configuration of the gateway can be done using the USB Stick Wizard.

Support of IPv4 and IPv6 - Overview

OpenScape SBC supports IPv6 in addition to the IPv4. The figure below shows the basic network scenario for IPv4 and IPv6.

IPv4/IPv6 Dual-Stack support is available for both the OpenScape SBC Core and Access networks. However, dual-IP is not provided for VoIP communications. Each remote network must operate as an IPv4-only or IPv6-only network without any mixed operation requiring dual-IP.



The configuration supports:

OS-SBC Access or Outside Network Interface:

- Remote Subscribers which support dynamic registration as IPv4-only or IPv6-only:

  - Remote Subscribers may be in a private or public network without a NAT.

  - Remote Subscribers in a private network behind a NAT. Only private networks of the same IP version as the public NAT interface are supported.
- Remote Subscribers which are statically configured as IPv4-only or IPv6-only
- Remote Gateways (e.g., H4K) which are statically configured as IPv4-only or IPv6-only
- Session establishment between IPv4-only or IPv6-only Remote Subscribers with other SIP interfaces using the same or different IP version.
- Session establishment between IPv4-only or IPv6-only Remote Gateways with other SIP interfaces using the same or different IP version

- SRTP/RTP Media bridging between media endpoints using different IP versions
- SRTP/RTP Media session optimization between media endpoints within the same subnet

OS-SBC Core or Inside Network Interface

- For VoIP communications (SIP, SIP-Q, (s)RTP) the network interface may be configured as IPv4-only or IPv6-only. For networks supporting an OpenScape Branch proxy or proxy (SBC) with remote media server, the SBC Core network must be IPv4-only. If the VoIP communications is configured for IPv6, the network interface shall support IPv4 for non-VoIP Applications, e.g., administrative services including CMP, Trace Manager, etc.

Additional Features Supported:

1) Support for OpenScape Branch using IPv6

In OpenScape Branch operating mode Branch SBC-Proxy, the gateways are supported using IPv4 and IPv6 addresses in WAN side.In OpenScape Branch operating mode Branch SBC, the subscribers and gateways are only supported using IPv4 address.In OpenScape Branch operating mode Branch Proxy, the subscribers are supported using IPv4 and IPv6 addresses.

2) OS-SBC Core network support for IPv4/IPv6 MGCP interworking

OpenScape Branch remote media servers can only be supported when the OS-SBC Core network is configured as IPV4-only. To support OpenScape Branch remote media servers with an OS-SBC IPv6 Core network requires the OS-SBC provide MGCP IPv4/IPv6 interworking which is not yet planned. A similar interworking would be required when the OpenScape Branch is IPv6-only and the OS-SBC Core network is configured as IPv4-only.

3) NAT64/NAT46

Only SIP UA's behind a NAT using the same IP version as the public NAT address IP version are supported in the current configuration. Other configurations would require additional support such as NAT64 or NAT46 which is a future feature candidate.

4) Administrative OS-SBC Core Network Service Support for IPv6

The IPv6 feature provides support for an OS-SBC IPv6-only Core network for VoIP communications an IPv4-only network is required for administrative services such as CMP for SOAP/HTTPS, SNMP, and ssh.

Even with this IPv4-only administrative services signaling restriction, administrative services must support IPv6 addresses in the payload.

Support of IPv4 and IPv6 for External Interfaces

OpenScape SBC supports IPv6 in addition to the IPv4. The following identifies IPv4 and IPv6 usage for external interfaces:

- **SIP and SIP-Q**

  SIP messages may contain IPv6 addresses in the domain part of the URI.

  SDP bodies may contain IPv6 addresses.
- **MGCP**

  IPv4 and IPv6 addresses are supported.

- **HTTPS**

  IPv4 and IPv6 addresses are supported.
- **SNMP**

  IPv4 and IPv6 addresses are supported.
- **SFTP**

  IPv4 and IPv6 addresses are supported.
- **SSH**

  IPv4 and IPv6 addresses are supported.
- **syslog**

  IPv4 and IPv6 addresses are supported.
- **NTP**

  An external NTP server may be addressed with IPv4 or IPv6 addresses based on configuration.

  The OpenScape SBC NTP server may be addressed with IPv4 or IPv6 on the OpenScape SBC Access network based on the remote subscriber registration contact network or static remote endpoint configuration.
- **DNS**

  DNS servers may be addressed using IPv4 and IPv6. A DNS server addressed with IPv6 is expected to resolve an FQDN to IPv6 addresses, however IPv4 addresses shall also be supported.

IPv4 and IPv6 Addresses

The IPv4 address is represented as a sequence of 4 decimal numbers from 0 to 255 separated by ‘.’, as for example:

127.128.128.128

The IPv6 address is represented as a sequence of hexadecimal digits, being each four digits separated by a ‘:’, as for example:

2001:0db8:0100:f101:0210:a4ff:fee3:9566

The IPv6 localhost address is represented as:

0000:0000:0000:0000:0000:0000:0000:0001 which can be reduced to ::1.

These rules for storing IPv6 addresses shall be applied in such a way that:

- The IPv6 addresses are always sent out in the canonic format.
- The IPv6 addresses are always stored internally in the canonic format to allow the comparison of IPv6 addresses.

  Example:

  Not canonic: 2001:0db8:f101:21dc:3245:4567:0000:abcd

  Canonic: 2001:db8:f101: 21dc:3245:4567:0:abcd

Support of Multiple VLANs

Virtual Local Area Network (VLAN) Environment

OpenScape SBC supports multiple VLANs for connectivity to remote branches in customer networks where VLAN tagging is used to achieve network segmentation. In such networks, VLANs are used to differentiate between

multiple remote branch locations that use overlapping private IP addresses. The OpenScape SBC can differentiate between remote branch locations based on its VLAN tag, e.g., to properly perform NATing between multiple remote branches on the WAN (access-side) and the OSV IP address/port addresses on the LAN (core-side) of the SBC.

OpenScape SBC also supports configurable firewall rules between the multiple VLANs that are handled by the OpenScape SBC.

- **VLAN support for the SBC Core Network**

  For this feature only the WAN interface may be configured in support of VLANs, i.e., there is no network separation for the OS-SBC core network, i.e., no Admin or VoIP VLAN support
- **VLAN support using single OS-SBC IP Address**

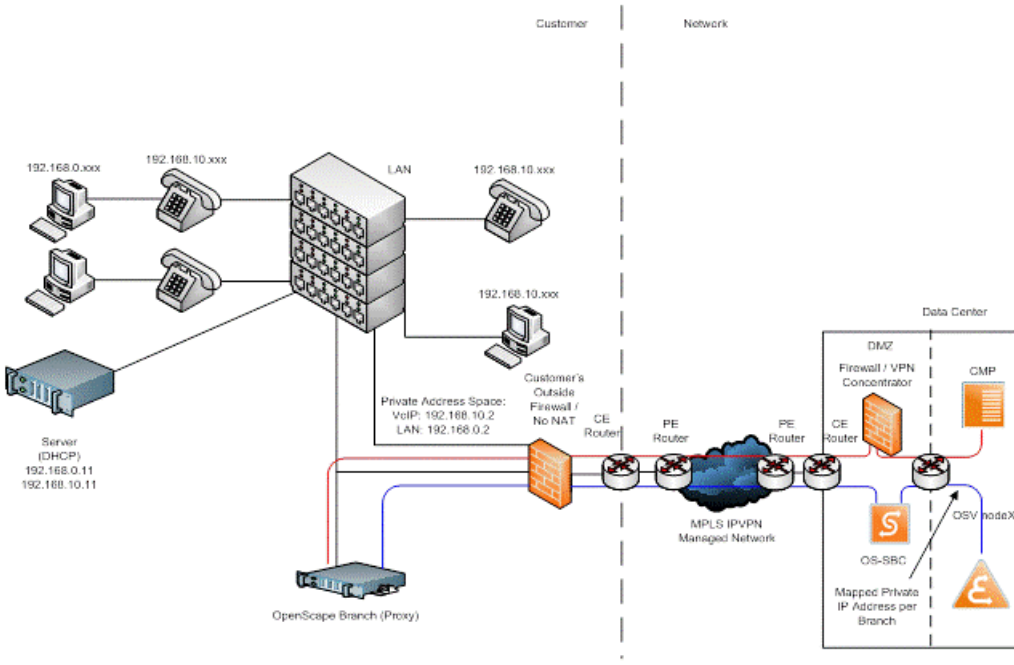
  The current feature operation utilizes one OS-SBC IP address per VLAN to support the separation at Layer-3. Binding to a logical network interface remains a future feature option.
- **Signaling and media network separation**

  Separation of signaling and media remains a topic for future study. It would be desirable to allow signaling and media be supported on different networks.
- **Installation / USB Stick / Simplified Install**

  The access network interface configuration uses the default access network configuration and does not provide any VLAN support.

A Virtual Local Area Network (VLAN) supports Layer-2 network separation as defined in 802.1q, allowing the same Layer-3 network IP addressing be used in multiple networks.

For the customer, many times the branch IP network (WAN) is supported as an extension of the data center LAN via a provider MPLS VPN network. This allows the same IP address range be used for each remote branch network. A form of NAT is required to provide address separation for data center access. Deployment of VLAN mapping on the outer edges of the MPLS VPN network helps provide the connectivity to the edge of the data center, however within the data center a unique address mapping is required to communicate with each branch office. This is where the OpenScape SBC’s role comes into play.

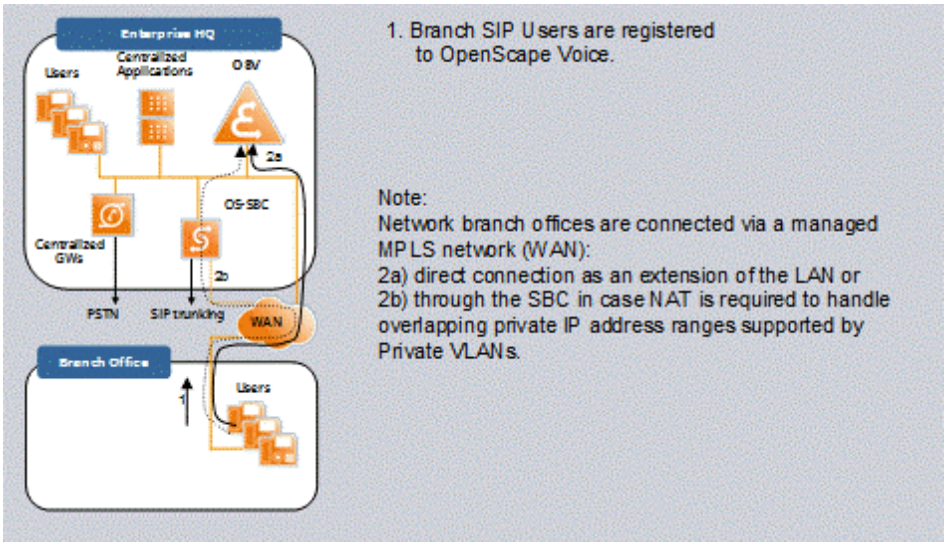


Network Application Scenario

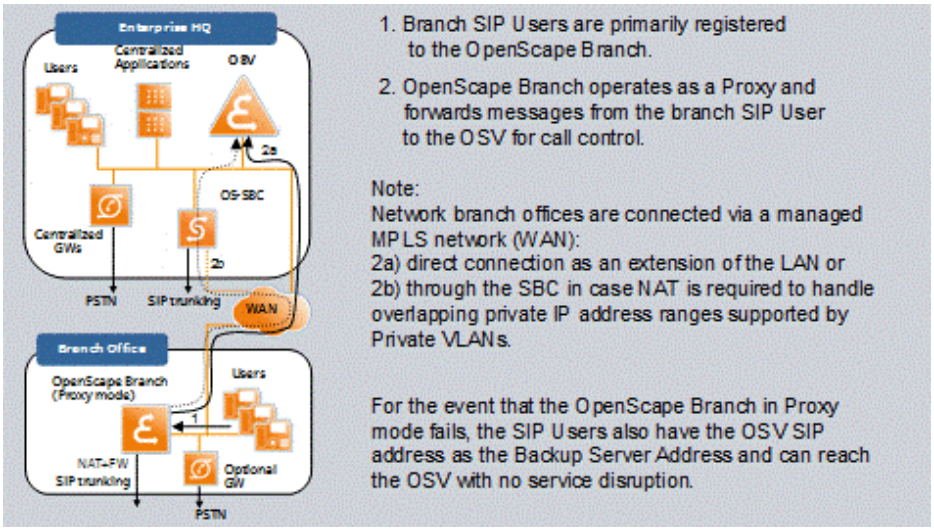
Supported Scenarios

There are two basic VLAN applications supported for OpenScape Branch.

- Branch Office
- Branch - Proxy operating mode



Branch Office Application:



Branch - Proxy Operating Mode

For the network applications shown above, Version 7 introduces VLAN support on the physical access network interface using 802.1q. The physical interface supports the existing non-VLAN network for other traffic e.g., Internet as well.

The physical access network interface is logically separated into multiple logical network interfaces. For each logical network interface, a unique IP address is assigned along with an optional VLAN ID. The main access network is also able to support VLAN or non-VLAN network interfaces. One or more remote endpoints and/or remote users may be associated with any logical network interface or the main access network. The network interface determines the network address and VLAN requirements for any IP message traffic.

The logical network interface IP address becomes an OpenScape SBC listening address for requests it receives as well as the OpenScape SBC's source IP address for requests it sends. If the logical network is associated with a VLAN ID, the 802.1q VLAN tag is inserted or processed at the network layer (Layer-2).

Up to 1000 VLANs are supported. In a collocated system this requires 2000 IP addresses be supported, each pair associated with each network. In non-VLAN deployments, up to 10 (non-collocated OSV) and 20 (collocated OSV) logical networks may be supported. Due to the number of sipserver child process created for UDP transport message listening purpose, up to two access realms of non-vlan type may be configured to use UDP.

4.3.1 How to Configure the Interfaces

Proceed as follows to configure the interfaces.

Prerequisites

Adequate administrative permissions.

At least one OpenScape SBC is configured and in operation.

The connection to the OpenScape Voice system is up.

Step by Step

1) Navigate to **Configuration** tab > **OpenScape SBC** within the Navigation Bar in the Common Management Platform.

2) Select the **OpenScape SBC list** in the Navigation Tree under **Administration**.

The system presents the **OpenScape SBC Overview** in the Work Area with a current list of all SBCs.

3) To view a list of SBCs configured at a specific communication system, select a communication system in the **Communication System** field in the navigation tree.

The default selection for the **Communication System** field is the selection of the global settings in the system menu.

4) To find and select a particular OpenScape SBC use one of the following options:

- In the Work Area select the checkbox to the left of the particular SBC in the list and select **Manage**.
- Choose a SBC from the **OpenScape SBC** pull-down located in the Navigation Tree.

General dialogue is presented in the Work Area displaying information and data for the selected SBC.

5) Navigate to **Configuration** > **Network/Net Services** > **Settings** in the navigation tree under **Administration**.

The **Network/Net Services** window appears with the **Settings** tab selected.

6) For General configuration of Core (LAN) and Access (WAN) interfaces the following parameters under the **Physical Network Interface** area must be set:

a) **Interface** - Ethernet Interface ports, numbered eth0 -> eth3

b) **Enabled** - Flag indicating the interface is enabled or disabled. To enable or disable the interface for the Core or Access interface realms, check or uncheck the checkbox for the specific interface.

c) **MTU** - Maximum Transmission Unit field defining maximum packet size The customer may set the field to any value between `300` and `1500`. The default value is "`1500`".

d) **Speed (Mbps)** - Select the interface speed to be used, from the selection list to specify a specific network speed and override auto-sensing. (Values: `Auto`, `10`, `100`, `1000`).

NOTICE: Auto indicates auto-sensing is used to identify the network speed.

---

e) **Duplex mode** - Enables the user to adjust the duplex mode (`Full` or `Half`).

NOTICE: This option is disabled if **Speed** option is set to `Auto`. If the **Speed** field is set to `1000` Mbps, then the **Duplex mode** field shall be set to `Full`.

---

7) To edit or add **Core realm configuration** settings (LAN), click on the field to edit or, click the **Add** button and then edit the fields.

a) The type of interface **Main IPv4**, **Main IPv6** or **Non-VLAN IP** options are provided under the **Type** field.

b) Enter the **Network ID** designation.

c) Enter the **IP Address** (IPv4 or IPv6) associated with the private side of the network, used to provide multiple communications paths to OpenScape Voice.

d) Enter the subnet mask (IPv4 or IPv6) of the interface in the **Subnet Mask** field. This parameter must align with the Admin IP Address field

e) Enter the unique **VLAN tag** (IPv4 or IPv6). This information is used to establish remote media server connections.

f) Enter the **SIP UDP**, **SIP TCP** and **SIP TLS** ports in their respective fields. This information is used for routing traffic into the core network. Traffic is secured using TLS over TCP.

g) Enter the MGCP port number in the **MGCP port** field.

8) To edit or add **Access IP Configuration** settings (WAN), click on the field to edit or, click the **Add** button and then edit the fields.

a) The type of interface **Main IPv4**, **Main IPv6**, **VLAN IP** or **Non-VLAN IP** options are provided under the **Type** field.

b) Enter the **Network ID**, a logical network interface identifier.

c) Enter the **Local IP Address** (IPv4 or IPv6).The Local IP address associated with the public side of the network, used to provide multiple paths for load distribution to collocated and geo-separated nodes and access to multiple networks.

d) Enter the subnet mask of the interface in the **Subnet Mask** field. This parameter must align with the Local IP Address field.

e) Enter the unique **VLAN tag** (IPv4). This information is used to establish remote media server connections.

f) Enter the **SIP UDP**, **SIP TCP** and **SIP TLS** ports in their respective fields. This information is used for routing traffic into the core network. Traffic is secured using UDP, TLS over TCP.

g) Enter the MGCP port number in the **MGCP port** field.

h) Select the node number in the **SIP Server** field list, in the General work area. Values: **Node1** and **Node 2**.

9) Click the **OK** button to store the changes temporarily in the administrator´s login session.

The **Network/Net Services** dialog disappears.

10) Click the **Apply changes** button in the main window.

NOTICE: Changes to Interface Network Settings require a system restart to apply!

4.3.2 How to Configure the Interfaces for earlier-than-v8 OpenScape SBC devices

Proceed as follows to configure the interfaces.

Prerequisites

Adequate administrative permissions.

At least one OpenScape SBC is configured and in operation.

The connection to the OpenScape Voice system is up.

Step by Step

1) Navigate to **Configuration** tab > **OpenScape SBC** within the Navigation Bar in the Common Management Platform.

2) Select the **OpenScape SBC list** in the Navigation Tree under **Administration**.

The system presents the **OpenScape SBC Overview** in the Work Area with a current list of all SBCs.

3) To view a list of SBCs configured at a specific communication system, select a communication system in the **Communication System** field in the navigation tree.

The default selection for the **Communication System** field is the selection of the global settings in the system menu.

4) To find and select a particular OpenScape SBC use one of the following options:

- In the Work Area select the checkbox to the left of the particular SBC in the list and select **Manage**.
- Choose a SBC from the **OpenScape SBC** pull-down located in the Navigation Tree.

General dialogue is presented in the Work Area displaying information and data for the selected SBC.

5) Navigate to **Configuration** > **Network Services** in the navigation tree under **Administration**.

The **Network Services** window appears with the **Interfaces** tab selected by default.

The interface configuration is displayed in the list with the following parameters:

- **IP Address** - IP address of the Interface
- **Enabled** - Flag indicating the interface is enabled or disabled
- **Interface** - Interface number 1-4
- **Type** - Type of interface LAN or WAN

6) Select the row of the interface to be configured in the list.

7) Click the **Edit...** button to modify interface settings.

The **Edit Interface 1...4** window appears, depending on your selection.

8) For General configuration of **LAN and WAN interfaces**; Select the **General** Tab

   a) To enable or disable the interface for LAN or WAN interfaces, check or uncheck the **Enable** checkbox in the **General** tab.
   b) Select the IP version from the **IP version** field list. Values: **IPv4** or **IPv6**
   c) Enter the Main IP address (IPv4 or IPv6) of the interface in the **Main IP Address** field
   d) Enter the subnet mask (IPv4 or IPv6) of the interface of the interface in the **Subnet Mask** field. This parameter must align with the Main IP Address field.
   e) Enter the Admin IP address (IPv4 or IPv6) of the interface in the **Admin IP Address** field
   f) Enter the subnet mask (IPv4 or IPv6)of the interface in the **Subnet Mask** field. This parameter must align with the Admin IP Address field
   g) Select the interface speed to be used, from the **Speed** selection list to specify a specific network speed and override auto-sensing. (Values: Auto, 10MB, 100 MB, 1000 MB).

   NOTICE: Auto indicates auto-sensing is used to identify the network speed.

9) For **LAN Interfaces**: Select the **Core IP Configuration** tab.

   The **Core IP Configuration** tab opens and the settings are displayed in the following columns:

   - **IP Address**: The IP address (IPv4 or IPv6) associated with the private side of the network, used to provide multiple communications paths to OpenScape Voice.
   - **VLAN ID**: A unique VLAN tag may be provisioned.
   - **TCP**: Indicates access via this protocol is enabled or disabled.
   - **TLS**: Indicates access via this protocol is enabled or disabled.
   - **MGCP**: Indicates access via this protocol is enabled or disabled.

10) To edit or add Core IP Configuration settings (LAN), click the **Edit..**. or **Add..**. button.

   The **Edit Core IP** or **Add Core IP** sub-window appears depending on your selection.

   a) The type of interface e.g. **Core** or **Admin** is displayed in the **Type** field, in General work area.
   b) Enter the **IP Address** (IPv4 or IPv6), in the General work area.
   c) Enter the **VLAN** unique tag (IPv4 or IPv6) in the General work area. This information is used to establish remote media server connections.
   d) Enter the **SIP TCP** port and **SIP TLS** port in the respective fields in the **Signaling ports** work area. This information is used for routing traffic into the core network. Traffic is secured using TLS over TCP.
   e) Enter the MGCP port number in the **MGCP port** field in the **Signaling ports** work area.
   f) Click the **OK** button to close the sub-window

11) For **WAN Interfaces**: Select the **Access IP Configuration** tab.

The **Core IP Configuration** tab opens and the settings are displayed in the following columns:

- **Network ID** - Logical network interface identifier.
- **Local IP Address** - IP address associated with the public side of the network
- **UDP**: Indicates the port.
- **TCP**: Indicates the port
- **TLS**: Indicates the port
- **MGCP**: Indicates the port
- **SIP Server**: Indicates the node number

12) To edit or add Access IP Configuration settings (WAN), click the **Edit..**. or **Add..**. button.

The **Edit Access IP** or **Add Access IP** sub-window appears depending on your selection.

a) The type of interface e.g. **Access** is displayed in the **Type** field, in General work area. Value: 32 characters maximum.
b) Enter the **Network ID**, a logical network interface identifier, in the General work area.
c) Enter the **Local IP Address** (IPv4 or IPv6), in the General work area.The Local IP address associated with the public side of the network, used to provide multiple paths for load distribution to collocated and geo-separated nodes and access to multiple networks.
d) Enter the subnet mask of the interface in the **Subnet Mask** field. This parameter must align with the Local IP Address field.
e) Select the node number in the **SIP Server** field list, in the General work area. Values: **Node1** and **Node 2**.
f) Enter the **VLAN** unique tag (IPv4) in the General work area. This information is used to establish remote media server connections.
g) Enter the **SIP UDP** port, **SIP TCP** port and **SIP TLS** port in the respective fields in the Signaling ports work area. This information is used for routing traffic into the core network. Traffic is secured using UDP, TLS over TCP.
h) Enter the MGCP port number in the **MGCP port** field in the Signaling ports work area.
i) Click the **OK** button to close the **Access IP Configuration** sub-window

13) Click the **OK** button to close the **Edit/Add Interface 1...4** sub-window.

14) Click the **OK** button to store the changes temporarily in the administrator´s login session.

The **Network Services** dialog disappears.

15) Click the **Apply changes** button in the main window.

NOTICE: Changes to Interface Network Settings require a system restart to apply!

4.3.3 How to Configure the Default Gateway Addresses

Proceed as follows to enter or change the default gateway addresses.

Prerequisites

Adequate administrative permissions.

At least one OpenScape SBC is configured and in operation.

The connection to the OpenScape Voice system is up.

Step by Step

1) Navigate to **Configuration** tab > **OpenScape SBC** within the Navigation Bar in the Common Management Platform.
2) Select the **OpenScape SBC list** in the Navigation Tree under **Administration**.

   The system presents the **OpenScape SBC Overview** in the Work Area with a current list of all SBCs.
3) To view a list of SBCs configured at a specific communication system, select a communication system in the **Communication System** field in the navigation tree.

   The default selection for the **Communication System** field is the selection of the global settings in the system menu.
4) To find and select a particular OpenScape SBC use one of the following options:

   - In the Work Area select the checkbox to the left of the particular SBC in the list and select **Manage**.
   - Choose a SBC from the **OpenScape SBC** pull-down located in the Navigation Tree.

   General dialogue is presented in the Work Area displaying information and data for the selected SBC.
5) Navigate to **Configuration** > **Network/Net Services** > **Settings** in the navigation tree under **Administration**.

   The **Network/Net Services** window appears with the **Settings** tab selected.
6) Scroll down to the **Routing** section under the **Settings** tab.
7) Enter or modify the default gateway IP address:

   - In the **Default gateway address** field for IPv4.
   - In the **Default gateway IPv6 address** field for IPv6.
8) Click the **OK** button to store the changes temporarily in the administrator´s login session.

   The **Network/Net Services** dialog disappears.
9) Click the **Apply changes** button in the main window to save the changes permanently.

The settings are applied to the system.

4.3.4 How to Configure the Default Gateway Addresses for earlier-than-v8 OpenScape SBC devices

Proceed as follows to enter or change the default gateway addresses.

Prerequisites

Adequate administrative permissions.

At least one OpenScape SBC is configured and in operation.

The connection to the OpenScape Voice system is up.

Step by Step

1) Navigate to **Configuration** tab > **OpenScape SBC** within the Navigation Bar in the Common Management Platform.

2) Select the **OpenScape SBC list** in the Navigation Tree under **Administration**.

The system presents the **OpenScape SBC Overview** in the Work Area with a current list of all SBCs.

3) To view a list of SBCs configured at a specific communication system, select a communication system in the **Communication System** field in the navigation tree.

The default selection for the **Communication System** field is the selection of the global settings in the system menu.

4) To find and select a particular OpenScape SBC use one of the following options:

- In the Work Area select the checkbox to the left of the particular SBC in the list and select **Manage**.
- Choose a SBC from the **OpenScape SBC** pull-down located in the Navigation Tree.

General dialogue is presented in the Work Area displaying information and data for the selected SBC.

5) Navigate to **Configuration** > **Network Services** in the navigation tree under **Administration**.

The **Network Services** window appears with the **Interfaces** tab selected by default.

6) Select the **Routing** tab.

7) Checkmark the **Enable default gateway** checkbox, in the **Gateway** work area to enable the default gateway and configuration.

The **Default Gateway Address** fields becomes active when the checkbox is selected.

8) Enter or modify the default gateway IP address (IPv4 or IPv6) for the LAN in the **Default Gateway Address LAN** field.

9) Enter or modify the default gateway IPv6 address for the LAN in the **Default Gateway IPv6 Address LAN** field.

10) Enter or modify the default gateway IP address (IPv4 or IPv6) for the WAN in the **Default Gateway Address WAN** field.

11) Enter or modify the default gateway IPv6 address for the LAN in the **Default Gateway IPv6 Address WAN** field.

12) Click the **OK** button to store the changes temporarily in the administrator´s login session.

The **Network Services** dialog disappears.

13) Click the **Apply changes** button in the main window to save the changes permanently.

The settings are applied to the system.

4.3.5 How to Add, Edit or Delete a Route

Proceed as follows to add, edit or delete a route.

Prerequisites

Adequate administrative permissions.

At least one OpenScape SBC is configured and in operation.

The connection to the OpenScape Voice system is up.

Step by Step

1) Navigate to **Configuration** tab > **OpenScape SBC** within the Navigation Bar in the Common Management Platform.
2) Select the **OpenScape SBC list** in the Navigation Tree under **Administration**.

   The system presents the **OpenScape SBC Overview** in the Work Area with a current list of all SBCs.
3) To view a list of SBCs configured at a specific communication system, select a communication system in the **Communication System** field in the navigation tree.

   The default selection for the **Communication System** field is the selection of the global settings in the system menu.
4) To find and select a particular OpenScape SBC use one of the following options:

   - In the Work Area select the checkbox to the left of the particular SBC in the list and select **Manage**.
   - Choose a SBC from the **OpenScape SBC** pull-down located in the Navigation Tree.

   General dialogue is presented in the Work Area displaying information and data for the selected SBC.
5) Navigate to **Configuration** > **Network/Net Services** > **Settings** in the navigation tree under **Administration**.

   The **Network/Net Services** window appears with the **Settings** tab selected.
6) Scroll down to the **Routing** > **Routing configuration** section under the **Settings** tab.

7) Create a route by clicking the **Add** button.

   It is then possible to configure the Destination IP address, Gateway IP address, Netmask (network) mask, and choose which interface will be used, in the **Interface** field, to route the IP packets.

8) To delete a route select the route and then click the Delete button.

9) Once the routes are created, edited, or deleted, click the **OK** button to save the changes temporarily in the administrator´s login session.

   The **Network/Net Services** window shall close.

10) Click the **Apply changes** button in the main window to save the changes permanently.

The route settings are applied to the system.

4.3.6 How to Add, Edit or Delete a Route for earlier-than-v8 OpenScape SBC devices

Proceed as follows to add, edit or delete a route.

Prerequisites

Adequate administrative permissions.

At least one OpenScape SBC is configured and in operation.

The connection to the OpenScape Voice system is up.

Step by Step

1) Navigate to **Configuration** tab > **OpenScape SBC** within the Navigation Bar in the Common Management Platform.

2) Select the **OpenScape SBC list** in the Navigation Tree under **Administration**.

   The system presents the **OpenScape SBC Overview** in the Work Area with a current list of all SBCs.

3) To view a list of SBCs configured at a specific communication system, select a communication system in the **Communication System** field in the navigation tree.

   The default selection for the **Communication System** field is the selection of the global settings in the system menu.

4) To find and select a particular OpenScape SBC use one of the following options:

   - In the Work Area select the checkbox to the left of the particular SBC in the list and select **Manage**.
   - Choose a SBC from the **OpenScape SBC** pull-down located in the Navigation Tree.

   General dialogue is presented in the Work Area displaying information and data for the selected SBC.

5) Navigate to **Configuration** > **Network Services** in the navigation tree under **Administration**.

   The **Network Services** window appears with the **Interfaces** tab selected by default.

6) Select the **Routing** tab.

   The routes are displayed in the **Routes** work area list.

7) To configure a route, select the row of the respective route in the list, in the **Routes** work area and choose one of the following option:

   - Click the **Edit...** button to edit the selected route.
   - Click the **Delete...** button to remove the selected route from the list.
   - Click the **Add...** button to add a new route to the list.

   The **Edit Network Services Routing** or the **Add Network Services Routing** subwindow appears, depending on your selection.

8) Enter or modify the IP address (IPv4 or IPv6) of the destination server in the **Destination** field.

9) Enter or modify the netmask (IPv4 or IPv6) of the destination server in the **Netmask** field.

10) Enter or modify the IP address (IPv4 or IPv6) of the gateway in the **Gateway** field.

11) Enter or modify the interface used to route the IP packets in the **Interface** field.

12) Click the **OK** button to close the sub-window.

13) Click the **OK** button to store the changes temporarily in the administrator´s login session.

    The **Network Services** dialog disappears.

14) Click the **Apply changes** button in the main window to save the changes permanently.

The route settings are applied to the system.

4.3.7 Traffic Shaping

Traffic shaping (also known as "packet shaping") serves for controlling computer network traffic in order to optimize or guarantee performance, low latency, and/or bandwidth by delaying packets.

General Configuration

In order to configure the traffic shaping, classes of traffic are defined. Using smart bandwidth shapers, which understand TCP/IP, the system can be configured to prioritize streams and modify packet tagging.

Rule Filters and Mark Filters

Rule filters serve for selecting traffic for each traffic class. Mark filters are used to set the firewall filter rules for each traffic class.

4.3.7.1 How to Configure Traffic Shaping

Proceed as follows to configure the general settings, rule filters and mark filters for traffic classes.

Prerequisites

Adequate administrative permissions.

At least one OpenScape SBC is configured and in operation.

The connection to the OpenScape Voice system is up.

Step by Step

1) Navigate to **Configuration** tab > **OpenScape SBC** within the Navigation Bar in the Common Management Platform.

2) Select the **OpenScape SBC list** in the Navigation Tree under **Administration**.

The system presents the **OpenScape SBC Overview** in the Work Area with a current list of all SBCs.

3) To view a list of SBCs configured at a specific communication system, select a communication system in the **Communication System** field in the navigation tree.

The default selection for the **Communication System** field is the selection of the global settings in the system menu.

4) To find and select a particular OpenScape SBC use one of the following options:

- In the Work Area select the checkbox to the left of the particular SBC in the list and select **Manage**.
- Choose a SBC from the **OpenScape SBC** pull-down located in the Navigation Tree.

General dialogue is presented in the Work Area displaying information and data for the selected SBC.

5) Navigate to **Configuration** > **Network/Net Services** > **Traffic Shaping** in the navigation tree under **Administration**.

The **Network/Net Services** window appears with the **Traffic Shaping** tab selected.

6) To enable traffic shaping, the user has to set the **Enable traffic shaping** checkbox.

7) Under the Traffic shaping table:

- Click the **Add** button to add a new traffic class row to the list.
- To delete a row from the table, first select the row by clicking on it, and then click the **Delete** button.

8) **Parent Class ID** - Enter or modify the ID for the traffic parent class. This is a hexadecimal number in the range 0...FFFF.

NOTICE: There should be at least one row without the Parent Class ID set, because that row is the parent for the others.

---

9) Class ID - Enter or modify the ID for the traffic class. This is a hexadecimal number in the range 0...FFFF
10) **Interface** - Enter or modify the interface the shaping is applied to.
11) **Default Class ID** - (Optional) Enter or modify the ID for the default traffic class. This is a hexadecimal number in the range 0...FFFF.
12) **Description** - Enter or modify an arbitrary string used to describe a class in a symbolic way.
13) **Rate (Kbps)** - (Mandatory) Enter or modify the rate for the traffic going through the class. This mandatory parameter defines how much bandwidth is allocated for the class. The value is defined in Kbit per second.
14) **Ceiling Rate (Kbps)** - (Optional) This optional parameter is used to set the maximum bandwidth to be used by the class. The difference with **Rate** amounts to bandwidth the class can borrow, if there is unused bandwidth. By default, ceiling rate is equal to rate so the class cannot borrow bandwidth.
15) **Burst (Kbytes)** - (Optional) This optional parameter defines how many bytes can be sent from one class at full speed before trying another class. This value is defined in Kilobytes (for example 1 Kbyte).
16) **Ceiling burst (Kbytes)** - (Optional) This optional parameter sets the maximum value of the burst. This value is defined in Kilobytes (for example 1 Kbyte).
17) **MTU (bytes)** - (Optional) Enter or modify the MTU (Maximum Transmission Unit). This optional parameter defines the maximum packet size. The default is 1600 bytes. Values are defined in bytes.
18) **Priority** - (Optional) Enter or modify this field to define the priority of class traffic. The higher the number, the lower the priority. Classes with higher priority are offered excess bandwidth first. The default value is 0.
19) **Leaf queuing** - (Optional) This is an optional parameter set by default to none. This parameter defines the leaf queue discipline to HTB (Hierarchical Token Bucket). Possible values are: None, sfq, packetFifo and byteFifo.
20) **SFQ Quantum** - (Optional) The SFQ (Stochastic Fair Queue) Quantum optional parameter defines the amount of data in bytes of a stream, which is allowed to dequeue before the next queue gets a turn. A default is set to one MTU-sized packet.

    NOTICE: Do not set this parameter below the MTU value.

21) **SFQ Perturbatic (sec) -** (Optional) This optional parameter defines how many seconds are allowed for a period of hash function perturbation. The default value is set to 10 seconds.
22) **Packet FIFO limit** - (Optional) The optional parameter Packet FIFO (First In, First Out) defines the number of packets that the queue can hold. The unit is number of packets.
23) **Byte FIFO limit** - (Optional) This optional parameter defines the number of bytes that the queue can hold. The unit is number of bytes.

24) **Rule filters** - This parameters build the "u32" filter rules that select traffic for each of the classes. The rules are separated by a comma. The syntax rule is as follows:

    RULE = [[source [/prefix]] [: port [/mask]],] [destination [/prefix]] [: port [/mask]]

    Example:

    RULE=10.1.55.0/32:8080. This rule filter selects traffic going to port 8080 in network 10.1.55.0.

25) **Mark filters** - This parameters sets the firewall filter rules that select traffic for each of the classes according to firewall "mark". Mark is a decimal number packet that is tagged, if firewall rules apply to it. The marks are separated by a semi-colon. Marks for different filter types can be combined.

26) To delete a mark filter, select the respective row in the list and click the **Delete** button.

27) Click the **OK** button to store the changes temporarily in the administrator´s login session.

    The **Network/Net Services** window is closed.

28) Click the **Apply changes** button in the main window to save the changes permanently.

The traffic shaping settings are applied to the system.

4.3.7.2 How to Configure Traffic Shaping for earlier-than-v8 OpenScape SBC devices

Proceed as follows to configure the general settings, rule filters and mark filters for traffic classes.

Prerequisites

Adequate administrative permissions.

At least one OpenScape SBC is configured and in operation.

The connection to the OpenScape Voice system is up.

Step by Step

1) Navigate to **Configuration** tab > **OpenScape SBC** within the Navigation Bar in the Common Management Platform.

2) Select the **OpenScape SBC list** in the Navigation Tree under **Administration**.

    The system presents the **OpenScape SBC Overview** in the Work Area with a current list of all SBCs.

3) To view a list of SBCs configured at a specific communication system, select a communication system in the **Communication System** field in the navigation tree.

    The default selection for the **Communication System** field is the selection of the global settings in the system menu.

4) To find and select a particular OpenScape SBC use one of the following options:

   - In the Work Area select the checkbox to the left of the particular SBC in the list and select **Manage**.
   - Choose a SBC from the **OpenScape SBC** pull-down located in the Navigation Tree.

   General dialogue is presented in the Work Area displaying information and data for the selected SBC.

5) Navigate to **Configuration** > **Network Services** in the navigation tree under **Administration**.

   The **Network Services** window appears with the **Interfaces** tab selected by default.

6) Select the **Traffic Shaping** tab.

   The traffic classes are displayed in the list.

7) To configure a traffic class, select the row of the respective route in the list.

8) Choose one of the following options:

   - Click the **Edit...** button to edit the selected traffic class.
   - Click the **Delete...** button to remove the selected traffic class from the list.
   - Click the **Add...** button to add a new traffic class to the list.

   The **Edit Traffic shaping** or the Add Traffic shaping subwindow appears, depending on your selection.

9) Enter or modify the ID for the traffic parent class in the **Parent Class ID** field. This is a hexadecimal number in the range 0...FFFF.

10) Enter or modify the interface the shaping is applied to in the **Interface** field.

11) Enter or modify the ID for the traffic class in the **Class ID** field. This is a hexadecimal number in the range 0...FFFF

12) Enter or modify the rate for the traffic going through the class in the **Rate** field. This mandatory parameter defines how much bandwidth is allocated for the class. The value is defined in Kbit per second.

13) Enter or modify the ID for the default traffic class in the **Default Class ID** field. This is a hexadecimal number in the range 0...FFFF.

14) Enter or modify the ceiling rate for the traffic class in the **Ceiling rate** field. This optional parameter is used to set the maximum bandwidth to be used by the class. The difference between **Ceiling Rate** and **Rate** amounts to bandwidth the class can borrow, if there is unused bandwidth. By default, ceiling rate is equal to rate so the class cannot borrow bandwidth. The value is defined in Kbit per second.

15) Enter or modify an arbitrary string used to describe a class in a symbolic way in the **Description** field.

16) Enter or modify the burst in the **Burst** field. This optional parameter defines how many bytes can be sent from one class at full speed before trying another class. This value is defined in Kilobytes (for example 1 Kbyte).

17) Enter or modify the MTU (Maximum Transmission Unit) in the **MTU** field. This optional parameter defines the maximum packet size. The default is 1600 bytes. Values are defined in bytes.

18) Enter or modify the Ceiling burst in the **Ceiling burst** field. This optional parameter sets the maximum value of the burst. This value is defined in Kilobytes (for example 1 Kbyte).

19) Enter or modify the priority of class traffic in the **Priority** field. The higher the number is, the lesser is the priority. Classes with higher priority are offered excess bandwidth first. The priority is an optional parameter, the default value is 0.
20) Enter or modify the SFQ (Stochastic Fair Queue) Quantum in the **SFQ Quantum** field. This is an optional parameter that defines the amount of data in bytes of a stream, which is allowed to dequeue before the next queue gets a turn. A default is set to one MTU-sized packet. Do not set this parameter below the MTU value!
21) Enter or modify the Leaf queuing value in the **Leaf queuing** field. This is an optional parameter set by default to none. This parameter defines the leaf queue discipline to HTB (Hierarchical Token Bucket). Possible values are: None, sfq, packetFifo and byteFifo.
22) Enter or modify the SFQ Perturbatic value in the **SFQ Perturbatic** field. This optional parameter defines how many seconds are allowed for a period of hash function perturbation. The default value is set to 10 seconds.
23) Enter or modify the value for the Packet FIFO (First In, First Out) limit in the **Packet FIFO limit** field. This optional parameter defines the number of packets that the queue can hold. The unit is number of packets.
24) Enter or modify the value for the Byte FIFO limit in the **Byte FIFO limit** field. This optional parameter defines the number of bytes that the queue can hold. The unit is number of bytes.
25) Select the **Rule filters** tab.

    The filters are displayed in a list. This parameters build the "u32" filter rules that select traffic for each of the classes. The rules are separated by a comma. The rule syntax is as following:

    RULE = [[source [/prefix]] [: port [/mask]],] [destination [/prefix]] [: port [/mask]]

    Example:

    RULE=10.1.55.0/32:8080. This rule filter selects traffic going to port 8080 in network 10.1.55.0.
26) To delete a rule filter, select the respective row in the list and click the **Delete** button.
27) To add a rule filter, type the new rule filter into the field above the list and click the **Add** button.

    The new rule filter is displayed in a new row in the list.
28) Select the **Mark filters** tab.

    The filters are displayed in a list. This parameters set the firewall filter rules that select traffic for each of the classes according to firewall "mark". Mark is a decimal number packet that is tagged, if firewall rules apply to. The marks are separated by a comma. Marks for different filter types can be combined.
29) To delete a mark filter, select the respective row in the list and click the **Delete** button.
30) To add a mark filter, type the new mark filter into the field above the list and click the **Add** button.

    The new mark filter is displayed in a new row in the list.
31) Click the **OK** button to close the **Traffic shaping** window.

32) Click the **OK** button to store the changes temporarily in the administrator´s login session.

The **Network Services** dialog disappears.

33) Click the **Apply changes** button in the main window to save the changes permanently.

The traffic shaping settings are applied to the system.

4.3.8 How to Configure System NTP Settings

Proceed as follows to configure the time and date settings for the OpenScape SBC or Branch appliance using a NTP (Network Time Protocol) server.

Prerequisites

Adequate administrative permissions.

At least one OpenScape SBC is configured and in operation.

The connection to the OpenScape Voice system is up.

Step by Step

1) Navigate to **Configuration** tab > **OpenScape SBC** within the Navigation Bar in the Common Management Platform.
2) Select the **OpenScape SBC list** in the Navigation Tree under **Administration**.

   The system presents the **OpenScape SBC Overview** in the Work Area with a current list of all SBCs.
3) To view a list of SBCs configured at a specific communication system, select a communication system in the **Communication System** field in the navigation tree.

   The default selection for the **Communication System** field is the selection of the global settings in the system menu.
4) To find and select a particular OpenScape SBC use one of the following options:

   - In the Work Area select the checkbox to the left of the particular SBC in the list and select **Manage**.
   - Choose a SBC from the **OpenScape SBC** pull-down located in the Navigation Tree.

   General dialogue is presented in the Work Area displaying information and data for the selected SBC.
5) Navigate to **Configuration** > **Network/Net Services** > **NTP** in the navigation tree under **Administration**.

   The **Network/Net Services** window appears with the **NTP** tab selected.
6) **Time zone** selection list. Select the time zone to be used in OpenScape SBC, e.g. GMT (Greenwich Mean Time).
7) Enable local NTP server checkbox. Used to activate the local NTP server.

8) Select one of the following options:

- **Manual configuration**

  Check this option to set the date and time manually. In this case, enter the **Date** (dd/mm/yyyy) and, the **Time** as a the 24-hour format (hh:mm). Click the **Apply** button to set it up.

  NOTICE: The timezone and the date and time are read from the system. If no timezone is configured, then is read from the system configuration file.

- **Synchronize with NTP server**

  Check and use this option to synchronize with a NTP (Network Time Protocol) server that is available. In this case the server address must be entered in the **NTP server** field. Any IP is valid, except 0.0.0.0 and 255.255.255.255.

  NOTICE: To synchronize manually with the NTP server, use the **Synchronize now** button. It must be used when the system is already using an NTP Server.

9) Check the **Enable local NTP server** checkbox to activate the local NTP server. In this case both, manual and synchronized time settings are allowed.

10) Click the **OK** button to store the changes temporarily in the administrator´s login session.

    The **Network/Net Services** dialog disappears.

11) Click the **Apply changes** button in the main window.

The settings for NTP are applied on the OpenScape SBC system.

4.3.9 How to Configure System NTP Settings for earlier-than-v8 OpenScape SBC devices

Proceed as follows to configure the time and date settings for the OpenScape SBC or Branch appliance using a NTP (Network Time Protocol) server.

Prerequisites

Adequate administrative permissions.

At least one OpenScape SBC is configured and in operation.

The connection to the OpenScape Voice system is up.

Step by Step

1) Navigate to **Configuration** tab > **OpenScape SBC** within the Navigation Bar in the Common Management Platform.

2) Select the **OpenScape SBC list** in the Navigation Tree under **Administration**.

   The system presents the **OpenScape SBC Overview** in the Work Area with a current list of all SBCs.

3) To view a list of SBCs configured at a specific communication system, select a communication system in the **Communication System** field in the navigation tree.

   The default selection for the **Communication System** field is the selection of the global settings in the system menu.

4) To find and select a particular OpenScape SBC use one of the following options:

   - In the Work Area select the checkbox to the left of the particular SBC in the list and select **Manage**.
   - Choose a SBC from the **OpenScape SBC** pull-down located in the Navigation Tree.

   General dialogue is presented in the Work Area displaying information and data for the selected SBC.

5) Navigate to **Configuration** > **Network Services** in the navigation tree under **Administration**.

   The **Network Services** window appears with the **Interfaces** tab selected by default.

6) Select the **NTP** tab.

7) Select the time zone to be used in OpenScape SBC, e.g. GMT (Greenwich Mean Time), from the **Time zone** selection list.

   NOTICE: The time zone setting will be saved only if the **Auto (via NTP server)** option is enabled (see below).

8) Select one of the following options:

   - **Auto (via NTP server):**

     Check this option to synchronize with a NTP (Network Time Protocol) server. In this case the server address must be entered in the **Server** field.

     NOTICE: To synchronize with the NTP server promptly, use the **Synch manually** button In this case the server address must be entered in the **Server** field. For the time zone field to be kept as a value, the **Auto (via NTP server)** option should be set.

   - **Manually**:

     Check this option to enter date and time manually. In this case the corresponding fields (Date and Time) have to be filled in.

     NOTICE: If the option is set to **Manually**, the time zone setting is not saved.

9) Enter the IP address (IPv4 or IPv6) of the NTP server in the **Server** field. Any IP is valid, except 0.0.0.0 and 255.255.255.255. This step is only required for the **Auto (via NTP server)** option.

NOTICE: The IP address field is IPv4/IPv6 configurable independent of the OS-SBC access or outside network VoIP configuration. A compatible WAN network interface address matching the IP version used for the remote server service must be configured.

---

10) Enter the date in the format (dd/mm/yyyy) in the **Date** field. This step is only required for the **Manually** option.
11) Enter the time in the 24-hour format (hh:mm) in the **Time** field. This step is only required for the **Manually** option.
12) Click the **Apply** button to apply updates for date and time.
13) Check the **Enable local NTP server** checkbox to activate the local NTP server. In this case both, manual and synchronized time settings are allowed.
14) Click the **OK** button to store the changes temporarily in the administrator´s login session.

    The **Network Services** dialog disappears.
15) Click the **Apply changes** button in the main window.

The settings for NTP are applied on the OpenScape SBC.

4.3.10 How to Synchronize Manually with the NTP Server

Proceed as follows to synchronize the time and date settings for the OpenScape SBC or Branch appliance manually with the NTP (Network Time Protocol) server.

Prerequisites

Adequate administrative permissions.

At least one OpenScape SBC is configured and in operation.

The connection to the OpenScape Voice system is up.

The NTP server is already configured for the OpenScape SBC.

Step by Step

1) Navigate to **Configuration** tab > **OpenScape SBC** within the Navigation Bar in the Common Management Platform.
2) Select the **OpenScape SBC list** in the Navigation Tree under **Administration**.

   The system presents the **OpenScape SBC Overview** in the Work Area with a current list of all SBCs.

3) To view a list of SBCs configured at a specific communication system, select a communication system in the **Communication System** field in the navigation tree.

   The default selection for the **Communication System** field is the selection of the global settings in the system menu.

4) To find and select a particular OpenScape SBC use one of the following options:

   - In the Work Area select the checkbox to the left of the particular SBC in the list and select **Manage**.
   - Choose a SBC from the **OpenScape SBC** pull-down located in the Navigation Tree.

   General dialogue is presented in the Work Area displaying information and data for the selected SBC.

5) Navigate to **Configuration** > **Network/Net Services** > **NTP** in the navigation tree under **Administration**.

   The **Network/Net Services** window appears with the **NTP** tab selected.

6) Click the **Synchronize now** button. The system synchronizes manually with the NTP server without using the **Apply Changes** button. The synch manually function must be used when the system already uses a NTP server.

7) Click the **OK** button to close the **Network/Net Services** window.

The date and time of the OpenScape SBC has been synchronized manually with the NTP server.

4.3.11 How to Synchronize Manually with the NTP Server for earlier-than-v8 OpenScape SBC devices

Proceed as follows to synchronize the time and date settings for the OpenScape SBC or Branch appliance manually with the NTP (Network Time Protocol) server.

Prerequisites

Adequate administrative permissions.

At least one OpenScape SBC is configured and in operation.

The connection to the OpenScape Voice system is up.

The NTP server is already configured for the OpenScape Branch system.

Step by Step

1) Navigate to **Configuration** tab > **OpenScape SBC** within the Navigation Bar in the Common Management Platform.

2) Select the **OpenScape SBC list** in the Navigation Tree under **Administration**.

   The system presents the **OpenScape SBC Overview** in the Work Area with a current list of all SBCs.

3) To view a list of SBCs configured at a specific communication system, select a communication system in the **Communication System** field in the navigation tree.

   The default selection for the **Communication System** field is the selection of the global settings in the system menu.

4) To find and select a particular OpenScape SBC use one of the following options:

   - In the Work Area select the checkbox to the left of the particular SBC in the list and select **Manage**.
   - Choose a SBC from the **OpenScape SBC** pull-down located in the Navigation Tree.

   General dialogue is presented in the Work Area displaying information and data for the selected SBC.

5) Navigate to **Configuration** > **Network Services** in the navigation tree under **Administration**.

   The **Network Services** window appears with the **Interfaces** tab selected by default.

6) Select the **NTP** tab.

7) Click the **Synch manually** button. The system synchronizes manually with the NTP server without using the **Apply Changes** button. The synch manually function must be used when the system already uses a NTP server.

8) Click the **OK** button to close the **Network Services** window.

The date and time of the OpenScape SBC has been synchronized manually with the NTP server.

4.3.12 Configuration of DNS Server

Depending on the network environment the OpenScape SBC is operating in, different configurations of the DNS (Domain Name System) server settings apply.

There are three possibilities of handling the names using OpenScape SBC DNS Server:

- DNS Server acts a slave of a master DNS outside of OpenScape SBC network; in this case the DNS Server configuration is mandatory.
- Forward DNS: DNS queries are forwarded to an external DNS server. In this case, it forwards all requests to another DNS and caches the results.
- DNS Server is acting as master solving the names in OpenScape SBC network; in this case the DNS Server configuration must be left open.

The zone configuration allows to define the type of DNS Server, the zone name, the IP address of the DNS Master or forward destination and the file name.
For the first case (slave or forwarding), the **Type** parameter defines if the DNS Server will forward the requests or act as slave.

DNS Server as Slave

In this configuration the Zone Name must contain a valid name for the zone which has to be defined in the Master DNS. The IP will contain the Masters IP

and the file name must be the name of a file corresponding to that zone. This file will be used to store the zone information that DNS Server gets from master. The DNS Server will respond as authoritative for those zones for which it is defined to be a 'slave' and for which it has a currently valid zone configuration. The zones should be added to the DNS zones list. See the example below.

Example for the zone list:

Row	Type	Zone name	IP Master/ Forward	File name
1	slave	myzone.com	1.2.3.4	myzone.com
2	slave	reverse-myzone.com	1.2.3.4	reverse-myzone.com

NOTICE: The reverse zone must also be contained in the list!

The master DNS for each zone is defined in the 'masters' zone section and allows slaves to refresh their zone record when the 'expiry' parameter of the SOA Record (Start Of Authority record) is reached. If a slave cannot reach the master DNS when the 'expiry' time has been reached it will stop responding to requests for the zone. It will NOT use time-expired data. The file parameter is optional and allows the slave to write the transferred zone to disc and hence if BIND is restarted before the 'expiry' time the server will use the saved data. In large DNS systems this can save a considerable amount of network traffic.

DNS Server as Forwarding (a.k.a Proxy) Name Servers

A forwarding (a.k.a. Proxy, Client, Remote) server is one which simply forwards all requests to another DNS and caches the results. This configuration is similar and the zones have also to be added. If the configuration doesn’t contain any zone then the forward IP list can be used to forward the DNS queries.

DNS Server as Master

For this case, no DNS Master Server is configured and only the checkbox "Enable DNS" is activated and no configurations are done in the **DNS** Configuration tab of the **Network Services** window. In this case the all zones have to be manually configured. Service must be contacted for support using this option.

NOTICE: If Redundancy is active, system will use physical IP for DNS queries. So, for slave synchronization the physical IP of both Master and Slave OpenScape SBC must be added to DNS Server firewall list.

4.3.12.1 How to Configure System DNS Settings

Proceed as follows to configure the DNS (Domain Name System) settings for the OpenScape SBC.

Prerequisites

Adequate administrative permissions.

At least one OpenScape SBC is configured and in operation.

The connection to the OpenScape Voice system is up.

Step by Step

1) Navigate to **Configuration** tab > **OpenScape SBC** within the Navigation Bar in the Common Management Platform.

2) Select the **OpenScape SBC list** in the Navigation Tree under **Administration**.

The system presents the **OpenScape SBC Overview** in the Work Area with a current list of all SBCs.

3) To view a list of SBCs configured at a specific communication system, select a communication system in the **Communication System** field in the navigation tree.

The default selection for the **Communication System** field is the selection of the global settings in the system menu.

4) To find and select a particular OpenScape SBC use one of the following options:

- In the Work Area select the checkbox to the left of the particular SBC in the list and select **Manage**.
- Choose a SBC from the **OpenScape SBC** pull-down located in the Navigation Tree.

General dialogue is presented in the Work Area displaying information and data for the selected SBC.

5) Navigate to **Configuration** > **Network/Net Services** > **DNS** in the navigation tree under **Administration**.

The **Network/Net Services** window appears with the **DNS** tab selected displaying the DNS Client and Server configuration settings.

6) To configure the DNS Client the following configuration options are provided:

- **Refresh DNS** - Allows the user to manually refresh the DNS client (restarting the service).
- **DNS server IP address** - List of DNS server IP addresses to be used by this client (maximum 3 DNS servers).

  To add a server to the list enter an IP address (IPv4 or IPv6) of a new DNS server and click the **Add** button.

NOTICE: The DNS server IP version is independent of the OpenScape SBC access or outside network VoIP configuration.The list may include both IPv4 and IPv6 addressed DNS servers. A compatible OpenScape SBC Access network interface address must be configured

on the OpenScape SBC access or outside network matching the IP version used to address the DNS server

Select an IP address in the list and click the **Delete** button to remove a server from the list.

- **Alias** - List of aliases to be used by this client.

  To add an alias to the list, enter an IP address (IPv4 or IPv6) of a new alias in the address field and click the **Add** button.

  Select an IP address in the list and click the **Delete** button to remove an entry from the list.

7) To enable the internal DNS Server service check the **Enable DNS server** checkbox and click the **DNS configuration** button.

The **DNS Server** window is displayed.

8) To configure the **Zone Configuration**:

- Add a DNS zone to the zone list, by clicking the **Add** button.

  A new zone row is added to the **Zone Configuration** table.
- To remove an entry from the **Zone Configuration** table zone list, select the respective row and click the **Delete** button. The zone is removed from the list.
- Select the zone type (Slave or Forward) from the **Type** selection list.
- Enter the zone domain name in the **Zone name** field.
- Enter the IP address (IPv4 or IPv6) or IP address list (separated by commas) for the configured zone type in the **IP master/forward** field. When the Zone type is configured as forward, the IP address should be included in the Forward IP List.
- Enter the file name to read the server data from in the **File name** field.

9) To configure the **Forward IP** list: click the **Configure** button beside the label.

- To add an IP address to the list, enter an IP address (IPv4 or IPv6) in the address field and click the **Add** button.
- Select an IP address in the list and click the **Delete** button to remove an entry from the list.

10) Click the **OK** button to confirm your updates and close the **DNS Server** dialog.

11) The **Enable Customization** checkbox allows the user to upload files to customize configuration of DNS.

- Check the **Enable DNS server** and then the **Enable Customization** checkbox.
- Click the **Administer custom files** button.

  The **Administer Custom DNS Files** window opens.
- Click **Browse** the button to find and select the DNS configuration file.
- Click the **Upload** button.
- Click the **Close** button to close the **Administer Custom DNS Files**.

12) Click the **OK** button to store the changes temporarily in the administrator´s login session.

The **Network/Net Services** window disappears.

13) Click the **Apply changes** button in the main window to save the changes permanently.

The DNS Server settings are applied on the OpenScape SBC device.

4.3.12.2 How to Configure System DNS Settings for earlier-than-v8 OpenScape SBC devices

Proceed as follows to configure the DNS (Domain Name System) settings for the OpenScape SBC.

Prerequisites

Adequate administrative permissions.

At least one OpenScape SBC is configured and in operation.

The connection to the OpenScape Voice system is up.

Step by Step

1) Navigate to **Configuration** tab > **OpenScape SBC** within the Navigation Bar in the Common Management Platform.

2) Select the **OpenScape SBC list** in the Navigation Tree under **Administration**.

The system presents the **OpenScape SBC Overview** in the Work Area with a current list of all SBCs.

3) To view a list of SBCs configured at a specific communication system, select a communication system in the **Communication System** field in the navigation tree.

The default selection for the **Communication System** field is the selection of the global settings in the system menu.

4) To find and select a particular OpenScape SBC use one of the following options:

- In the Work Area select the checkbox to the left of the particular SBC in the list and select **Manage**.
- Choose a SBC from the **OpenScape SBC** pull-down located in the Navigation Tree.

General dialogue is presented in the Work Area displaying information and data for the selected SBC.

5) Navigate to **Configuration** > **Network Services** in the navigation tree under **Administration**.

The **Network Services** window appears with the **Interfaces** tab selected by default.

6) Select the **DNS** tab.

The DNS settings are displayed for client and server including the DNS zone list with the following columns: **Type**: The zone type (slave or forward). **Zone name**: The zone domain name. **IP Master/Forward**: The IP address for the configured zone type. **File name**: The file to read the name server data from.

7) To configure the DNS server list click the **Configure** button beside the **DNS server list** label.

   The **DNS Server list** window appears. The IP addresses of the configured DNS servers are listed. A maximum of 3 DNS servers are allowed.

8) Use one of the following options:

   - To add a server to the list enter an IP address (IPv4 or IPv6) of a new DNS server in the address field and click the **Add** button.

     NOTICE: The DNS server IP version is independent of the OpenScape SBC access or outside network VoIP configuration.The list may include both IPv4 and IPv6 addressed DNS servers. A compatible OpenScape SBC Access network interface address must be configured on the OpenScape SBC access or outside network matching the IP version used to address the DNS server

   - Select an IP address in the list and click the **Delete** button to remove a server from the list.

9) Click the **Close** button to go back to the **Network Services** window.

10) To configure the alias list click the **Configure** button beside the **Alias list** label.

    The **Alias list** window appears. The aliases used by this client are listed.

11) Use one of the following options:

    - To add an alias to the list, enter an IP address (IPv4 or IPv6) of a new alias in the address field and click the **Add** button.
    - Select an IP address in the list and click the **Delete** button to remove an entry from the list.

12) Click the **Close** button to go back to the **Network Services** window.

13) Use the **Synch manually** button to synchronize with the DNS server promptly.

14) Enter the OpenScape SBC domain name in the **OpenScape Branch Domain Name** filed, e.g. `company.com`.

15) To enable the internal DNS Server service check the **Enable DNS** checkbox.

16) To configure the forward IPs list, click the **Configure** button beside the **Forward IPs** label.

    The **Forward IPs** window appears. The dialog contains a list of IP addresses for the DNS server to forward queries to.

17) Use one of the following options:

    - To add an IP address to the list, enter an IP address (IPv4 or IPv6) in the address field and click the **Add** button.
    - Select an IP address in the list and click the **Delete** button to remove an entry from the list.

18) Click the **Close** button to go back to the **Network Services** window.

19) To configure the zone list, use one of the following options:

- To remove an entry from the system zone list, select the respective row and click the **Delete** button. The zone is removed from the list.
- To edit a zone in the system zone list, click the **Edit** button.
- To add a DNS zone to the system zone list, click the **Add** button.

The **Add Zone** dialog appears.

20) Select the zone type (Slave or Forward) from the **Type** selection list.

21) Enter the zone domain name in the **Zone name** field.

22) Enter the IP address (IPv4 or IPv6) or IP address list (separated by commas) for the configured zone type in the **IP Master/Forward** field. When the Zone type is configured as forward, the IP address should be included in the Forward IP List.

23) Enter the file name to read the server data from in the **File name** field.

24) Click the **OK** button to close the **Add Zone** dialog.

25) Click the **OK** button to store the changes temporarily in the administrator´s login session.

The **Network Services** window disappears.

26) Click the **Apply changes** button in the main window to save the changes permanently.

The DNS Server settings are applied on the OpenScape SBC.

4.4 Security Configuration — Overview

Security configuration comprises general settings, configuration of Message Rate Control settings, firewall settings, port forwarding and password administration.

The OpenScape SBC provides security features according to the OpenScape Voice security strategy.

OpenScape Voice Security Strategy

The OpenScape Voice security strategy is based on a layered security approach, as follows:

- The first layer of security is the network design itself that separates bearer, signaling, and management traffic from each other and from other traffic on the network.
- The second layer of security is the support for integrated end-to-end secure interfaces within the OpenScape Voice equipment itself.
  - Open VPN (Virtual Private Network) (Currently Not Supported)

    Open VPN can be used to provide a secure link to an OpenScape Voice system in the main office.

OpenScape SBC Security Strategy

The two main goals of OpenScape SBC security are to protect the customers and to protect the network and its equipment. Protecting customers includes:

- Maintain Service Availability.

- Ensure confidentiality and integrity of customer information.

Protecting the network includes:

- Ensure non-malicious interaction between customers and the system.
- Enforce customer access only to authorized features.
- Maintain the confidentiality and integrity of system information.
- Enforce operations span of control & scope of commands.
- Ensure non-malicious interactions among system elements.
- Maintain a security audit trail.

4.4.1 TLS Certificates and Shared Secret Files

Digital certificates, which contain a public key and the identity of the owner, are used in security to insure that one entity is trusted.

The OpenScape Voice security strategy optionally supports TLS (Transport Layer Security) with mutual authentication using certificates, which are verified as being valid against a set of pre-stored root certificates.

Functional Description

Server authentication takes place when the TLS connection is established. OpenScape Voice and the interface partner authenticate each other using certificates. For this purpose, OpenScape SBC and Branch support the installation of client specific TLS certificates and Shared Secret Files.

Definitions

- CA Certificates: A certificate authority or certification authority (CA) issues digital certificates which contain a public key and the identity of the owner. This is used in security to insure that one entity is trusted.
- X.509: This is an ITU-T standard for a public key infrastructure (PKI) for single sign-on and Privilege Management Infrastructure (PMI). X.509 specifies standard formats for public key certificates, certificate revocation lists, attribute certificates, and a certification path validation algorithm.
- Key Files: A key file contains encryption or license keys and often is part of the public key infrastructure.
- Shared Secret Files: Shared secret key files are used for a VPN connection, when the type of authentication is defined as secret.

Configuration

TLS and MTLS Certificates (X.509 certificates, CA certificates, Key files) and shared secret files can be displayed, created, uploaded or deleted by the administrator.

TLS Certificates are managed through the use of certificate profiles. Additionally, security is enhanced by:

- Preventing unauthorized use of services by improved CA certificate validation.
- Periodic certificate expiration checking.
- Certificate Revocation List management.
- TLS session renegotiation.

- Configuration of TLS or MTLS separately for remote endpoints, remote subscribers, core side (OpenScape SBC) and general TLS (OpenScape Branch)
- Keep-alive

Authentication - Keep Alive - Connection Establishment

For Remote Endpoints:

OpenScape Branch, remote endpoints shall be understood as external Gateways, SIP Trunks or SIP Service Providers

- **TLS**

  The Authentication of the Remote Endpoint on the OpenScape SBC is done during the TLS connection establishment, by validating the server certificate (TLS Server Authentication Model).

  A keep-alive mechanism can be configured. The Remote Endpoint in OS SBC can be configured to always be the TLS client and will be responsible for keeping the TLS connection alive. This means that the establishment of the TLS connection shall be initiated by the OS SBC. The OS SBC will be responsible for keeping the TLS connection alive. So, it shall implement a keep-alive mechanism to detect a TLS connection failure. The keep-alive mechanism shall be executed by periodically sending a double carriage return / line feed (CRLF) to the SIP service Provider as defined by RFC5626. The SIP Service Provider shall respond with a single CRLF. If the OS SBC does not receive a response from the SIP Service Provider, it shall conclude that the TLS connection has dropped and it shall reestablish the TLS connection. Notice that any message received from the peer side counts as a keep-alive response.

  A SIP Service Provider may reuse an already established TLS connection for initiating a new SIP dialog or it can establish a new TLS connection. Since a TLS connection being initiated by a Remote Endpoint does not allow the authentication of the peer. It is possible to disable reuse if required for security reasons.

  The following scenarios are possible for TLS:

  – SIPconnect approach – OS SBC are responsible for initiating and keeping the connection alive. SIP Service Provider shall always reuse an already established TLS connection. OS SBC may only assume the role of a TLS Client and the keep-alive mechanism shall be supported.
  – TLS Dual Path – the SIP Service Provider does not reuse the established TLS connection, but by needing to initiate a SIP dialog, it establishes a new TLS connection. OS SBC shall accept a TLS connection as a TLS Server and does not need to support the keep-alive mechanism.

  For TLS with Remote Endpoints other than SIP SP, OS SBC are typically a TLS server. This means that the Remote Endpoints will be responsible for initializing TLS and for keeping TLS up and running. In this case, OS SBC must respond to a keep-alive request (double CRLF) with a single CRLF.

  If a Remote Endpoint is configured with transport type TLS, it listens to the configured TLS port (default port 5061) for a request to establish a TLS connection.

- **MTLS**

  MTLS means that the OpenScape SBC and the Remote Endpoint are mutually authenticated. Each side will send its own certificate.

  The establishment of the TLS connection can be initiated either by the OS SBC or by the Remote Endpoint depending on the side which is starting the transaction.

  It is possible to configure different certificates to be used when the OS SBC acts as TLS client or TLS server for MTLS. The client and server certificates shall contain the same public key.

  The TLS connection will be dropped if not used for a certain time.

  There are 2 methods for working with MTLS when an endpoint has a TLS connection which was established by the peer endpoint and needs to initiate a SIP dialog to the peer endpoint:

  – TLS connection reuse – the endpoint reuses the TLS connection.
  – TLS Dual Path – the endpoint creates a new TLS connection.

  OS SBC will always reuse the TLS connection if it needs to initiate a SIP dialog and there is already a TLS connection which had been established by the remote endpoint.

  However, if the OS SBC has an established TLS connection and it receives a request from the remote endpoint to create a new TLS connection, it will accept it.

4.4.1.1 How to Manage TLS Certificates

Proceed as follows to select a manage TLS (Transport Layer Security) Certificates for the OpenScape SBC.

Prerequisites

Adequate administrative permissions.

At least one OpenScape SBC is configured and in operation.

The connection to the OpenScape Voice system is up.

Step by Step

1) Navigate to **Configuration** tab > **OpenScape SBC** within the Navigation Bar in the Common Management Platform.

2) Select the **OpenScape SBC list** in the Navigation Tree under **Administration**.

The system presents the **OpenScape SBC Overview** in the Work Area with a current list of all SBCs.

3) To view a list of SBCs configured at a specific communication system, select a communication system in the **Communication System** field in the navigation tree.

The default selection for the **Communication System** field is the selection of the global settings in the system menu.

4) To find and select a particular OpenScape SBC use one of the following options:

- In the Work Area select the checkbox to the left of the particular SBC in the list and select **Manage**.
- Choose a SBC from the **OpenScape SBC** pull-down located in the Navigation Tree.

General dialogue is presented in the Work Area displaying information and data for the selected SBC.

5) Navigate to **Configuration** > **Security** > **General** in the navigation tree under **Administration**.

The **Security** window appears with the **General** tab selected.

6) Click the **Certificate Management Configure...** button.

The **Certificate Management** window appears with the **General Configuration** tab displayed as default. The General Configuration tab manages the following:

- System TLS Certificate selection
- Certificate creation
- Certificate upload
- Certificate download

7) System TLS Certificate Selection

a) Select the TLS certificate to be used on a system-wide basis from the **System TLS Certificate** field selection list.

NOTICE: The OSV solution certificate is provided by default.

---

8) Certificate Creation

a) Enter the name of the new certificate to be created in the **Name** field.

b) Select the file type to be created from the CA File field selection list. Values: **Self signed** (default), **ServerCA.pem**.

c) Click the **Create** button.

The certificate is now created and can be downloaded, and used when creating a certificate profile. The newly created certificate will appear in the associated download and certificate profiles field lists.

9) Display Certificates

a) Click the **Upload** button in the Certificate upload work area.

The **TLS Certificates** dialog appears displaying a list of certificates with the associated certificate type.

10) **Certificate Upload**
    a) Click the **Upload** button in the Certificate upload work area.

       The **TLS Certificates** dialog appears displaying a list of certificates with the associated certificate type.
    b) Click the **Add** button.

       The **Add Certificate** dialog appears.
    c) To upload a certificate, Select the type of certificate (**CA Certificate**, **Key File**, **X.509 Certificate**) from the field list and Click the **Browse** button. Locate and select the file to be uploaded.
    d) To complete the add certificate configuration click the **OK** button.

       The certificate is now uploaded and added or created and can be downloaded, and used when creating a certificate profile. The newly created certificate will appear in the associated dowload and certificate profiles field lists.
11) **Certificate Download**
    a) To download a **Certificate file**; Select the certificate from the **Certificate File** field list in the **Certificate download** work area.
    b) Click the **Download** button associated with the Certificate File Field list.

       The browser appears. Selected the location to save the certificate and select **Save**.

       The certificate is now downloaded.
    c) To download a **Key file**; Select the key file from the **Key File** field list in the **Certificate download** work area.
    d) Click the **Download** button associated with the Key File Field list.

       The browser appears. Selected the location to save the key file and select **Save**.

       The key file is now downloaded.

The changes are saved automatically.

4.4.1.2 How to Create, Edit and Delete Certificate Profiles

Proceed as follows to create, edit and delete Certificate Profiles for OpenScape SBC. A Certificate Profile can be assigned to one or more OpenScape SBC (Remote Endpoints or Remote Subscribers) allowing for faster configuration of certificates.

Prerequisites

Adequate administrative permissions.

Adequate knowledge of TLS certificate handling.

At least one OpenScape SBC is configured and in operation.

The connection to the OpenScape Voice system is up.

Step by Step

1) Navigate to **Configuration** tab > **OpenScape SBC** within the Navigation Bar in the Common Management Platform.

2) Select the **OpenScape SBC list** in the Navigation Tree under **Administration**.

The system presents the **OpenScape SBC Overview** in the Work Area with a current list of all SBCs.

3) To view a list of SBCs configured at a specific communication system, select a communication system in the **Communication System** field in the navigation tree.

The default selection for the **Communication System** field is the selection of the global settings in the system menu.

4) To find and select a particular OpenScape SBC use one of the following options:

- In the Work Area select the checkbox to the left of the particular SBC in the list and select **Manage**.
- Choose a SBC from the **OpenScape SBC** pull-down located in the Navigation Tree.

General dialogue is presented in the Work Area displaying information and data for the selected SBC.

5) Navigate to **Configuration** > **Security** > **General** in the navigation tree under **Administration**.

The **Security** window appears with the **General** tab selected.

6) Click the **Certificate Management Configure...** button.

The **Certificate Management** window appears with the **General Configuration** tab displayed as default.

7) Select the **Certificate Profiles** tab.

The **Certificate Profiles** tab work area appears with the current configured certificate profiles listed. The certificate profile display contains the following parameters for each profile:

- Profile Name
- Certificate Service
- Client Certificate File
- Server Certificate File
- Local CA File
- Remote CA File
- Local Key File
- Attach to Cfg file

8) Add a Certificate Profile

There are three basic areas of configuration when creating a certificate profile: General, Validation and Renegotiation settings.

It is possible to create up to 10 certificate profiles.

a) Click the **Add** button.

The **Certificate profile** dialog appears with the General tab selected by default.

General Settings Configuration:

b) Enter the name of the new certificate profile name to be created, in the **Certificate Profile Name** field.

c) Select the certificate service to be applied from the **Certificate service** field selection list. Values: **SIP-TLS** (default) or **VPN**.

d) Select the certificate to be used when establishing a TLS connection as a client from the **Local client certificate file** field selection list.

To display certificate attributes: Click the **Show** button. The Certificate viewer dialog appears with the certificate information for the following areas Subject, Issuer, Validity and Fingerprints.

e) Select the certificate to be used when establishing a TLS connection as a server from the **Local server certificate file** field selection list.

To display certificate attributes: Click the **Show** button. The **Certificate viewer** dialog appears with the certificate information for the following areas Subject, Issuer, Validity and Fingerprints.

Subject:

- - Common Name (CN)
- - Organization (O)
- - Organizational Unit (OU)
- - Serial Number

Issuer:

- - Common Name (CN)
- - Organization (O)
- - Organizational Unit (OU)

Validity:

- - Issued On
- - Expires On

Fingerprints:

- - SHA1 Fingerprint
- - MD5 Fingerprint

f) Select the CA file with the rootCA certificate which signed (issuer) the local certificates, from the **Local CA file** field selection list.

To display certificate attributes: Click the **Show** button. The **Certificate viewer** dialog appears with the certificate information for the following areas Subject, Issuer, Validity and Fingerprints.

g) Select the CA file to validate the certificate received from the remote endpoint, from the **Remote CA file** field selection list.

To display certificate attributes: Click the **Show** button. The **Certificate viewer** dialog appears with the certificate information for the following areas Subject, Issuer, Validity and Fingerprints.

h) The **Attach to Cfg** file field selection list, indicates the certificate file in **Remote CA file** column will be saved/restored to/from the xml configuration file.

i) Select the Key file that contains the private key from the **Local key file** field selection list.

Validation Settings Configuration:

j) Select the **Validation** tab.

The Validation tab dialog appears

k) Checkmark the **Certificate validation** checkbox, if the following validation checks are required:

Validation:

- CA chain and CA signature - will be checked
- Validity Period - the current time will be checked against the notBefore and notAfter certificate fields
- Critical Extensions - all critical extensions contained within the certificate will be verified

l) Checkmark the **Revocation Status** checkbox, if the CRL of the CA must be checked to see if the certificate has been revoked.

IMPORTANT: If this flag is checked the corresponding CRL must be configured in the **Certificate revocation**

list (tab) otherwise the TLS connection will not be established.

m) Checkmark the **Subject authentication** checkbox, if the certificate Subject CN or Subject Alternative Name CN must be validated against the configured endpoint.

Renegotiation Settings Configuration:

n) Select the **Renegotiation** tab.

The Renegotiation tab dialog appears

o) Checkmark the **Enforce TLS session renegotiation** checkbox, if renegotiation of an established TLS session is enabled for this endpoint. (default is disabled)

p) Enter the TLS renegotiation interval, in the **TLS session renegotiation interval** field to specify length of time a negotiated key is valid in a TLS connection. Valid values: 15 – 1440 minutes. Default: 60 minutes.

q) Select the TLS version supported from the **TLS version** field selection list. Values: **TLSv1.0**, **TLSv1.1**, **TLSv1.2** (default), or **TLSv1.3**

NOTICE: In V10R2, after full install, the default value for Minimum TLS version was changed to TLS V1.2 in Certificate Profile.

It is still possible to select TLS V1.0 from menu.

r) Click the **OK** button to store the general profile settings.

The **Certificate Profiles** tab dialog appears with the new certificate profile displayed in the profile list.

s) Click the **OK** button to store the new certificate profile.

The **Security** window is displayed.

9) Edit a Certificate Profile

a) From the **Certificate Profiles** tab window; Select the **Certificate Profile** to be edited.

b) Click the **Edit** button in the general work area.

The **Certificate profile** dialog appears with the General tab selected by default.

c) Refer to the sub-steps in the section **Add a Certificate Profile** above for parameter details.

10) Delete a Certificate Profile

a) From the **Certificate Profiles** tab window; Select the **Certificate Profile** to be deleted.

b) Click the **Delete** button in the general work area.

The Certificate profile is deleted and the display list is updated on the Certificate Profiles tab window.

11) Click the **OK** button when prompted to delete the certificate profile.

NOTICE: When saving a Certificate Profile, all selected certificate files shall be validated based on the following criteria: Certificate Authority Validation, Validity Period and Revocation Status. If the validation fails in any of the validation criteria, an error shall presented to the user indicating the reason of

the failure. This validation prevents the administrator from configuring an invalid certificate.

4.4.1.3 How to Configure Certificate Expiration Checking

Proceed as follows to configure certificate expiration checking for the OpenScape SBC and Branch system.

Prerequisites

Adequate administrative permissions.

At least one OpenScape SBC is configured and in operation.

The connection to the OpenScape Voice system is up.

Step by Step

1) Navigate to **Configuration** tab > **OpenScape SBC** within the Navigation Bar in the Common Management Platform.

2) Select the **OpenScape SBC list** in the Navigation Tree under **Administration**.

The system presents the **OpenScape SBC Overview** in the Work Area with a current list of all SBCs.

3) To view a list of SBCs configured at a specific communication system, select a communication system in the **Communication System** field in the navigation tree.

The default selection for the **Communication System** field is the selection of the global settings in the system menu.

4) To find and select a particular OpenScape SBC use one of the following options:

- In the Work Area select the checkbox to the left of the particular SBC in the list and select **Manage**.
- Choose a SBC from the **OpenScape SBC** pull-down located in the Navigation Tree.

General dialogue is presented in the Work Area displaying information and data for the selected SBC.

5) Navigate to **Configuration** > **Security** > **General** in the navigation tree under **Administration**.

The **Security** window appears with the **General** tab selected.

6) Click the **Certificate Management Configure...** button.

The **Certificate Management** window appears with the **General Configuration** tab displayed as default. The General Configuration tab manages the following:

- System TLS Certificate selection
- Certificate creation
- Certificate upload
- Certificate download

7) Select the **Certificate expiration checking** tab.

   The **Certificate expiration checking** tab work area appears with the default or current configured parameters displayed.

8) Enter the number of days to warn the administrator prior to the expiration of the certificate, in the **Certificate expiration warning period** field. An expiration warning alarm is generated indicating the impending expiration of the certificate.

9) Enter the number of days to repeat the certificate expiration warning alarm, in the **Certificate Expiration Warning Interval** field. An expiration warning alarm is repeated once the certificate expiration warning period is reached.

10) Enter the time of day to run the certificate expiration check, in the **Certificate expiration time of day** field lists. The format for time of day is hh:mm (hours 00-24:minutes 00-59).

11) Click the **OK** button to store the settings.

The changes are saved automatically.

4.4.1.4 How to Display and Configure the Certificate Revocation List (CRL)

Proceed as follows to display, add, edit and delete Certificate Revocation List entries for OpenScape SBC and Branch systems.

Prerequisites

Adequate administrative permissions.

At least one OpenScape SBC is configured and in operation.

The connection to the OpenScape Voice system is up.

Step by Step

1) Navigate to **Configuration** tab > **OpenScape SBC** within the Navigation Bar in the Common Management Platform.

2) Select the **OpenScape SBC list** in the Navigation Tree under **Administration**.

   The system presents the **OpenScape SBC Overview** in the Work Area with a current list of all SBCs.

3) To view a list of SBCs configured at a specific communication system, select a communication system in the **Communication System** field in the navigation tree.

   The default selection for the **Communication System** field is the selection of the global settings in the system menu.

4) To find and select a particular OpenScape SBC use one of the following options:

   - In the Work Area select the checkbox to the left of the particular SBC in the list and select **Manage**.
   - Choose a SBC from the **OpenScape SBC** pull-down located in the Navigation Tree.

   General dialogue is presented in the Work Area displaying information and data for the selected SBC.

5) Navigate to **Configuration** > **Security** > **General** in the navigation tree under **Administration**.

   The **Security** window appears with the **General** tab selected.

6) Click the **Certificate Management Configure...** button.

   The **Certificate Management** window appears with the **General Configuration** tab displayed as default.

7) Select the **Certificate revocation list** tab.

   The **Certificate revocation list** tab work area appears with the current certificate revocation (CRLs) entries listed. The certificate profile display contains the following parameters for each profile:

   - Name - Name of the root certificate authority.
   - CRL URL
   - CRL download interval
   - CRL short download interval
   - CRL time of day

8) **Add a CRL Entry**

   The following sub-steps are used to add and modify a CRL entry. The CRL file can be updated automatically based on configuration or a manual update can be initiated. Up to 10 entries can be created.

   a) Click the **Add** button.

      The **Certificate revocation configuration** dialog appears.

   b) Enter the name (Root CA) of the name of the root certificate authority, in the **Name** field. Only CRLs of certificates that are verified up to this root CA shall be downloaded. CRLs of certificates that are not issued by this CA or one of its intermediate CAs are not downloaded, and will lead to a minor alarm, that a connection was accepted without certificate revocation check.

   c) Enter the URL, provided by the CA, from which the CRL file can be downloaded, in the **CRL URL** field.

      Manual CRL File Update:

   d) Click the Manual update button to initiate a manual update of the CRL file.

      Automatic CRL File Update:

   e) Enter the maximum interval between two CRL downloads, in the **CRL download interval** field. Default value:24 hours.

      NOTICE: This value is typically less than the time difference of the current time with the time recorded in the **Next Update** field of the CRL itself. If this interval is set to 0, the **Next Update** field is used instead for the automatic CRL downloads.

   f) Enter the interval at which a CRL check shall occur in case the download of a CRL failed because the CRL could not be downloaded

e.g. CRL download server problem or network connectivity problem, in the **CRL short download interval** field. Default value:60 minutes.

g) Enter the specific time of day at which to start the CRL check, in the **CRL time of day** field. The format for time of day is hh:mm (hours 00-24:minutes 00-59).

NOTICE: This variable is only checked if the CRL download interval is 24 or a multiple of 24.

---

h) Click the **OK** button to store the certificate revocation configuration settings.

The **Certificate revocation list** tab dialog appears with the new Certificate Revocation List (CRL) entry displayed.

i) Click the **OK** button to store the new certificate profile.

The **Security** window is displayed.

9) Show a CRL Entry

a) From the **Certificate revocation list** tab window; Select the **Certificate Revocation List entry** to be shown.

b) Click the **Show CRL** button in the general work area.

The **CRL viewer** dialog appears with the following information displayed:

- CRL download URL
- CRL issuer
- Status
- This update
- Next update
- Last update

c) Click the **Close** button to return to the Certificate revocation list tab display.

10) Edit a CRL Entry

a) From the **Certificate revocation list** tab window; Select the **Certificate Revocation List entry** to be edited.

b) Click the **Edit** button in the general work area.

The **Certificate revocation configuration** dialog appears.

c) Refer to the sub-steps in the section **Add a CRL Entry** above for parameter details.

11) Delete a CRL Entry

a) From the **Certificate revocation list** tab window; Select the **Certificate Revocation List entry** to be deleted.

b) Click the **Delete** button in the general work area.

The Certificate Revocation List (CRL) is deleted and the display is updated on the Certificate Revocation List tab window.

12) Click the **OK** button to store the settings.

The changes are saved automatically.

NOTICE: A log is generated when a CRL is deleted or updated. The log can be viewed at **Maintenance > Inventory > Nodes >**

select the OpenScape SBC > Log files: Show button > in the Log Viewer select Web Server from the Select Log: field list

4.4.1.5 How to Select a Shared Secret File for Use

Proceed as follows to select a shared secret file for use in the OpenScape SBC and Branch system.

Prerequisites

Adequate administrative permissions.

At least one OpenScape SBC is configured and in operation.

The connection to the OpenScape Voice system is up.

Step by Step

1) Navigate to **Configuration** tab > **OpenScape SBC** within the Navigation Bar in the Common Management Platform.
2) Select the **OpenScape SBC list** in the Navigation Tree under **Administration**.

   The system presents the **OpenScape SBC Overview** in the Work Area with a current list of all SBCs.
3) To view a list of SBCs configured at a specific communication system, select a communication system in the **Communication System** field in the navigation tree.

   The default selection for the **Communication System** field is the selection of the global settings in the system menu.
4) To find and select a particular OpenScape SBC use one of the following options:

   - In the Work Area select the checkbox to the left of the particular SBC in the list and select **Manage**.
   - Choose a SBC from the **OpenScape SBC** pull-down located in the Navigation Tree.

   General dialogue is presented in the Work Area displaying information and data for the selected SBC.
5) Navigate to **Configuration** > **Security** > **General** in the navigation tree under **Administration**.

   The **Security** window appears with the **General** tab selected.
6) Use the **Shared Secret Files** selection list to choose a shared secret file to be used.

The changes are saved automatically.

4.4.1.6 How to Display, Add and Delete Shared Secret Files

Proceed as follows to display, add and delete Shared Secret files for OpenScape SBC and Branch systems.

Prerequisites

Adequate administrative permissions.

At least one OpenScape SBC is configured and in operation.

The connection to the OpenScape Voice system is up.

Step by Step

1) Navigate to **Configuration** tab > **OpenScape SBC** within the Navigation Bar in the Common Management Platform.

2) Select the **OpenScape SBC list** in the Navigation Tree under **Administration**.

The system presents the **OpenScape SBC Overview** in the Work Area with a current list of all SBCs.

3) To view a list of SBCs configured at a specific communication system, select a communication system in the **Communication System** field in the navigation tree.

The default selection for the **Communication System** field is the selection of the global settings in the system menu.

4) To find and select a particular OpenScape SBC use one of the following options:

- In the Work Area select the checkbox to the left of the particular SBC in the list and select **Manage**.
- Choose a SBC from the **OpenScape SBC** pull-down located in the Navigation Tree.

General dialogue is presented in the Work Area displaying information and data for the selected SBC.

5) Navigate to **Configuration** > **Security** > **General** in the navigation tree under **Administration**.

The **Security** window appears with the **General** tab selected.

6) Click the **Shared Secret Files Configure...** button.

The **Shared Secret Files** window appears with the list of Shared Secret Files displayed.

7) Add a Shared Secret File

There are two basic ways to add a shared secret file: create the file or upload the file.

a) Click the **Add** button.

The **Add Certificate** dialog appears.

b) To upload a shared secret file certificate, Click the **Upload** radio button. The type of certificate is **Shared Secret File** in the field list. Click the **Browse** button. Locate and select the file to be uploaded.

c) To create a shared secret file certificate, Click the **Create** radio button. The type of certificate is **Shared Secret File** in the field list. Enter the name of the certificate to be created in the **Name** field.

d) To complete the add certificate configuration click the **OK** button.

The **Shared Secret Files** dialog is displayed with the new shared secret file certificate in the display list.

The shared secret file certificate is now uploaded and added or created and can be used. The newly created shared secret file certificate will appear in the associated certificate field lists.

8) Display a List of Shared Secret Files

a) From the **Security** window General tab; Select the **Shared Secret Files Configure button**.

The **Shared Secret Files** window appears with the list of Shared Secret Files displayed.

9) Delete a Shared Secret File

a) From the **Share Secret Files** window; Select the **Shared Secret File** to be deleted.

b) Click the **Delete** button in the general work area.

10) Click the **OK** button when prompted to delete the file.

The Shared Secret File certificate is deleted and the display list is updated on the **Secret Shared Files** window.

NOTICE: When saving a Certificate Profile, all selected certificate files shall be validated based on the following criteria: Certificate Authority Validation, Validity Period and Revocation Status. If the validation fails in any of the validation criteria, an error shall presented to the user indicating the reason of the failure. This validation prevents the administrator from configuring an invalid certificate.

4.4.2 Network Intrusion Detection and Prevention (Message Rate Control)

Message Rate Control is a Network Intrusion prevention system (NIPS) and network intrusion detection system (NIDS).

Message Rate Control performs packet logging and real-time traffic analysis on IP networks. The OpenScape SBC uses the Message Rate Control rules only against Denial of Service Attacks based on the packet transmission rates attack.

Message Rate Control Rules

Message Rate Control rules need to be configured so that appropriate alarms are raised to alert the administrator of any possible unauthorized access or intrusion. Appropriate alarms are generated and stored in the syslog.

4.4.2.1 How to Configure Message Rate Control Rules

Proceed as follows to configure the network intrusion prevention and detection system Message Rate Control.

Prerequisites

Adequate administrative permissions.

At least one OpenScape SBC is configured and in operation.

The connection to the OpenScape Voice system is up.

Step by Step

1) Navigate to **Configuration** tab > **OpenScape SBC** within the Navigation Bar in the Common Management Platform.
2) Select the **OpenScape SBC list** in the Navigation Tree under **Administration**.

   The system presents the **OpenScape SBC Overview** in the Work Area with a current list of all SBCs.
3) To view a list of SBCs configured at a specific communication system, select a communication system in the **Communication System** field in the navigation tree.

   The default selection for the **Communication System** field is the selection of the global settings in the system menu.
4) To find and select a particular OpenScape SBC use one of the following options:

   - In the Work Area select the checkbox to the left of the particular SBC in the list and select **Manage**.
   - Choose a SBC from the **OpenScape SBC** pull-down located in the Navigation Tree.

   General dialogue is presented in the Work Area displaying information and data for the selected SBC.
5) Navigate to **Configuration** > **Security** in the navigation tree under **Administration**.

   The **Security** window appears with the **General** tab selected.
6) Select the **Message Rate Control** tab.
7) To activate Message Rate Control, check the **Enable Message Rate Control** checkbox.
8) Use the **Message rate threshold** field to define the number of kilobytes per second, which will block an IP address. The network administrator should set this parameter according to the desired bandwidth. Setting this value to a minimum could cause RTP (Real-Time Transport Protocol) packages being dropped, especially in SBC (Session Border Controller) installations. Possible values: 100... 25600.

9) Enter the blocking time of the IP address in seconds in the **Block period** field.

10) The **White List** contains all IP addresses which will not be blocked by Message Rate Control. Use one of the following options:

- To add a new IP address (IPv4 or IPv6) or Logical Branch Office ID the address in the **IP address/Logical Branch Office ID** field and click the **Add** button.

  NOTICE: The Logical Branch Office ID is supported for endpoints configured for Dynamic IP.

- Click the **Delete** button to delete an IP address from the list.

11) Click the **Close** button to go back to the **Security** window.

12) Click the **OK** button to store the changes temporarily in the administrator´s login session and close the **Security** window.

The **Security** dialog disappears.

13) Click the **Apply changes** button in the main window.

The Message Rate Control rules are applied on the OpenScape SBC or Branch system.

4.4.3 Firewall Configuration

A firewall is installed on the OpenScape SBC in order to protect access to systems behind it, limiting their exposure to the Internet.

OpenScape SBC supports near-end NAT firewall in addition to the supported firewall operating in transparent mode. Both internal and external firewalls are supported.l

The firewall configuration allows to define filter rules for incoming and outgoing WAN or network connections as well as incoming VoIP (Voice over IP) connections.

Enable masquerading

When IP Masquerading is enabled, it masks the LAN addresses in the WAN. This shall hide the entire internal address space which appears as a single IP address in another, often public address space.

Enable Port Forwarding configuration

This firewall service defines the rules for Port Forwarding.

Incoming/Outgoing WAN network connections

It is possible to allow or block access to some services (DNS, SSH, SNMP, ICMP, FTP, FTPS, Telnet, HTTP, HTTPS and NTP). These settings affect new incoming connections to OpenScape SBC and outgoing connections (Devices under OpenScape SBC trying to access WAN services).

Incoming WAN VoIP connections

TLS, RTP/sRTP and MGCP) from the WAN interface accessing the internal address space.

White List

Allow incoming and outgoing WAN network connections for a specific IP/Port. If the Port field is zero, all ports are allowed.

Black List

Block incoming and outgoing WAN network connections for a specific IP/Port. If the Port field is zero, all ports are blocked.

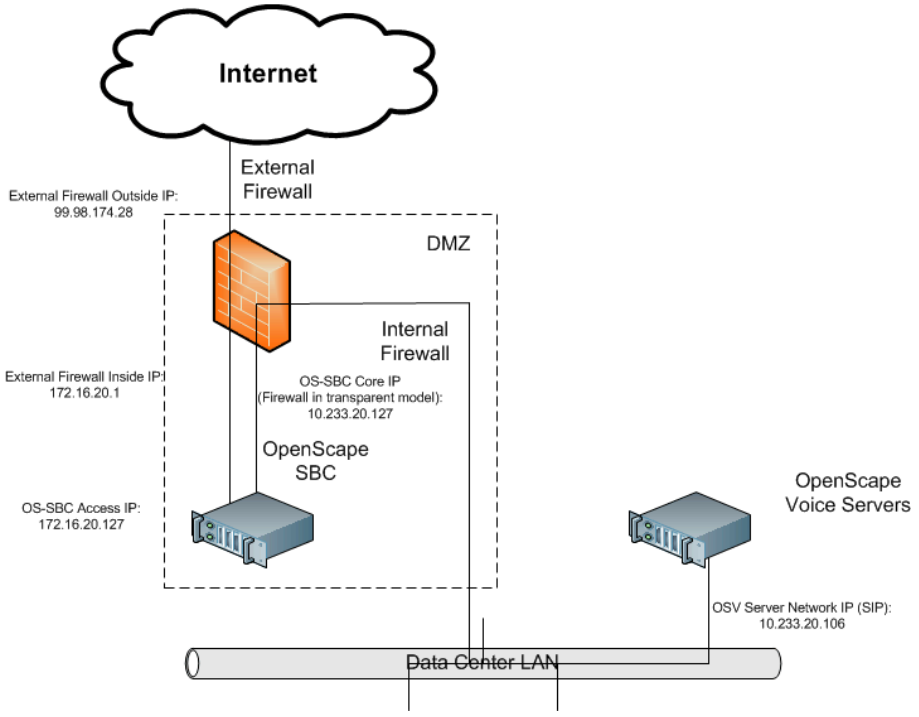
NOTICE: Message Rate Control (if enabled) will be restarted when the firewall rules are changed.

Application Overview

In a near-end NAT firewall all external networks interface with the firewall external network interface instead of the OpenScape SBC. The OpenScape SBC accommodates the near-end NAT support for the firewall by supporting the external firewall IP address for all SIP messages and SDP.

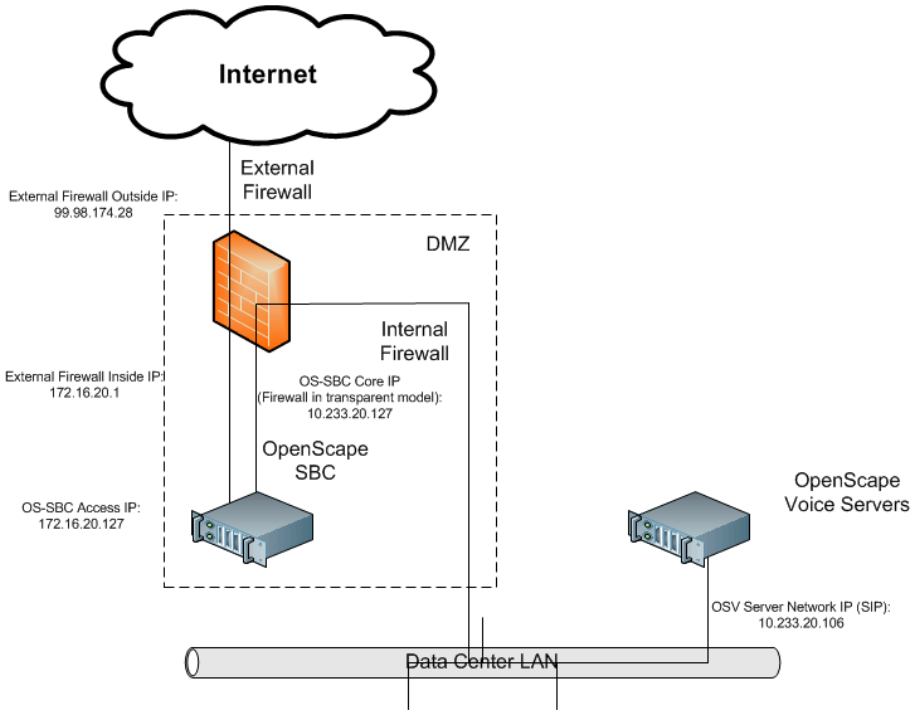
External Only Firewall Deployment

The figure below is an example of an external firewall deployment.



External and Internal (DMZ) Firewall Deployment

The figure below is an example of deploying both internal and external firewalls.



Deployment Scenarios

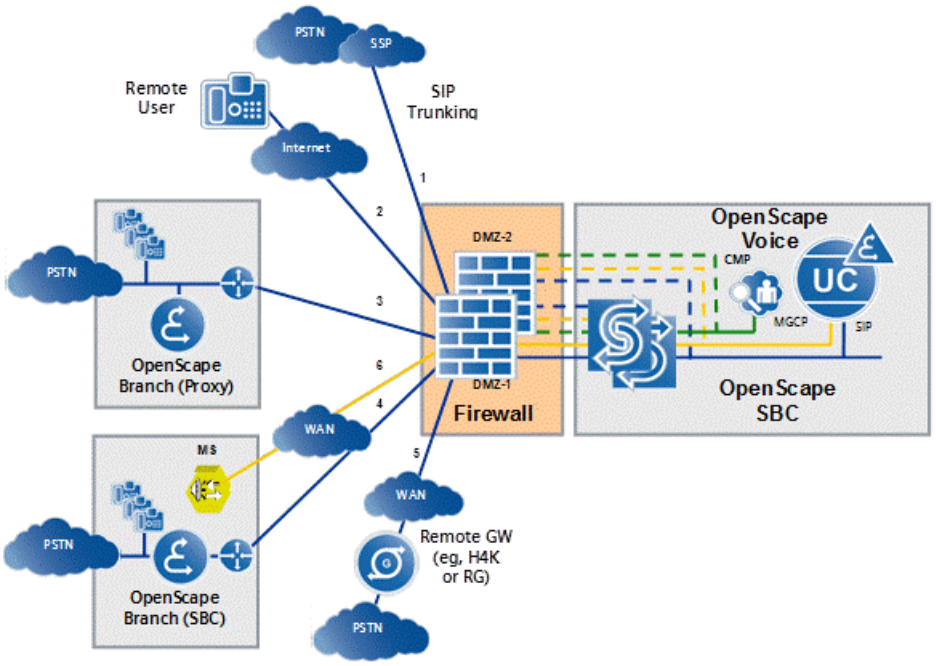
The OpenScape SBC is able to support firewalls operating in “transparent mode”.

Two firewall deployment options are considered dependant on the customer's Demilitarized Zone (DMZ) requirements.

- External-only firewall (DMZ-1): Servers deployed in the DMZ interfacing with external networks may be considered trusted, able to directly access other services inside the customer network.
- Internal firewall (DMZ-2) – The customer may deploy servers interfacing with outside networks in a DMZ to restrict their access due to security policy, requiring other parts of the network be accessed through an internal firewall.

NOTICE: The firewall may perform Network Address Translation (NAT), a.k.a., near-end NAT, however the internal network firewall shall always operate in “transparent mode”. If the firewall supports SIP ALG it must be disabled.

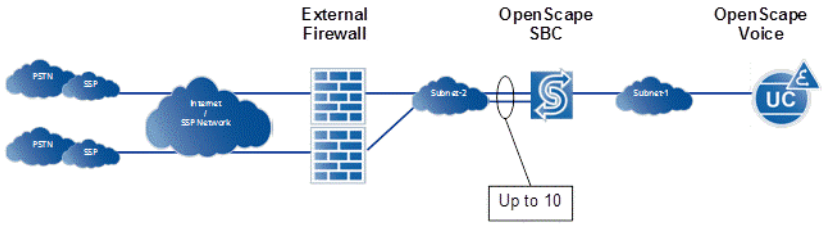
Application Scenario - Overview



The external firewall implications are summarized below for each application scenario:

1. SIP Trunking to a SIP Service Provider (SSP)

Provides secure connection of IP telephony solution (OpenScape Voice) to carrier-based SIP trunking services that provide access to the Public Switched Telephone Network (PSTN).



Firewall implications:

For this scenario the firewall may operate in “transparent mode” where the internal and external firewall network interfaces are in the same subnet. The OpenScape SBC continues to support the remote network interface as is done today.

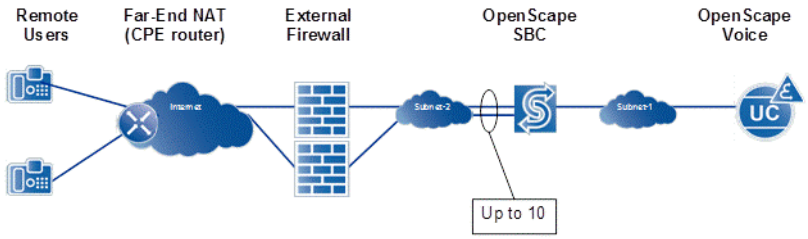
If firewall “transparent mode” operation is not possible, it may still be possible to perform the near-end NAT only in the OpenScape SBC. In this configuration the firewall supports two subnets for the enterprise external and internal networks however the OpenScape SBC is configured with the SIP information needed to communicate in the external network (WAN) and is thus able to perform all application layer NAT on behalf of the firewall.

If TLS is used the firewall supports the TLS connection with the remote interface on the firewall external network interface. TLS may be used for the firewall internal network interface with the OpenScape SBC.

For RTP media streams the firewall becomes a gateway for the OpenScape SBC. The firewall must be configured with the same RTP media ports as the OpenScape SBC with static port forwarding. When RTP media packets arrive from the remote network interfaces, the firewall establishes a pinhole for both subnets to enable sending RTP media packets to the other.

2. Remote User (e.g., home worker)

Provides secure remote user access to the IP telephony infrastructure of an OpenScape Voice system for SIP phones regardless of location. Since far-end Network Address Translation (NAT) traversal (namely NAPT) functions for connection via the Internet require Hosted NAT traversal (HNT).



Firewall implications:

Mixing far-end NAT requiring Hosted NAPT traversal (HNT) and a near-end NAT firewall requires special firewall support since the OpenScape SBC must route packets to the NAT.

For SIP registrations, the firewall establishes pinholes for the signaling channel and passes the public Far-End-NAT (FE-NAT) IP address and source port to the OpenScape SBC or alternatively establish a unique SIP contact binding address pinhole for the remote network device when passing the registration to OpenScape SBC. The firewall's signaling pinhole remains open until the FE-NAT device stops communication using the IP address and port or SIP contact expires.

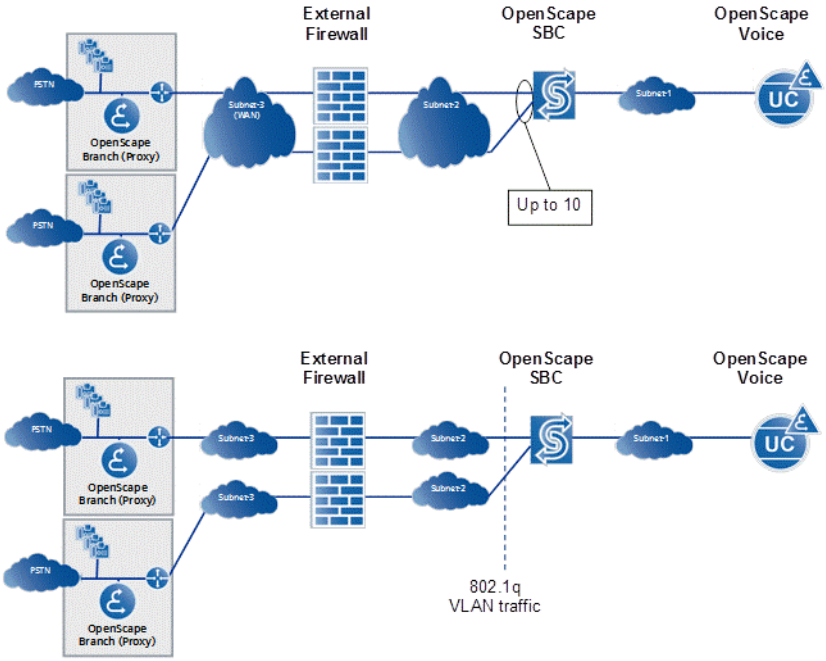
The external firewall is configured to route IP messages between external network interfaces and the OpenScape SBC Access IP. The OpenScape SBC performs all SIP/SDP NAT using the firewall external IP address.

If TLS connections are used the firewall supports the TLS connection with the remote interface on the firewall external network interface. TLS may be used for the firewall internal network interface with the OpenScape SBC.

For RTP media streams the firewall becomes a gateway for the OpenScape SBC. The firewall must be configured with the same RTP media ports as the OpenScape SBC with static port forwarding. When RTP media packets arrive from HNT devices, the firewall updates its pinhole with the FE-NAT IP address and port for the HNT media stream. It passes the RTP media packets unchanged to the OpenScape SBC to allow updating its RTP destination IP address and port.

3. Remote OpenScape Branch (Proxy)

The OpenScape Branch is connected via the enterprise network using the same IP address space, so the OpenScape SBC is optional. If 802.1q VLAN tagging is used the OpenScape SBC is required due to the possibility of the same subnet being replicated for each VLAN, with the possibility of overlapping IP addresses.



Firewall implications:

Without 8021q VLAN Tagging:

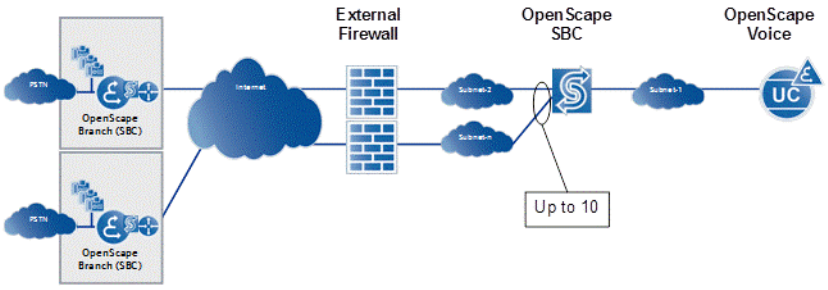
- If an OpenScape SBC is included without 802.1q VLAN tagging the firewall may be configured to operate in a “pseudo-transparency mode” where it does not perform any application layer NAT (SIP, SDP). The application layer NAT is instead performed by the OpenScape SBC. The NE-NAT firewall supports two subnets for the enterprise external network however the OpenScape SBC is configured with the SIP information needed to communicate in the external network (WAN) and is thus able to perform all application layer NAT on behalf of the firewall.
- The OpenScape SBC is configured to communicate with the OpenScape Branch (Proxy) through the firewall however there are multiple NAT’s involved, i.e., Subnet1-Subnet2, Subnet2-Subnet3 which are not really needed.
- The external firewall is configured to route IP messages between external network interfaces and the OpenScape SBC Access IP. The OpenScape SBC performs all SIP/SDP NAT using the firewall external IP address.
- For RTP media streams the firewall becomes a gateway for the OpenScape SBC. The firewall must be configured with the same RTP media ports as the OpenScape SBC with static port forwarding. When RTP media packets arrive from the remote network interfaces, the firewall establishes a pinhole for both subnets to enable sending RTP media packets to the other.

With 8021q VLAN Tagging:

- When 802.1q VLAN tagging is used the firewall may be configured to operate in a “pseudo-transparency mode” where it does not perform any application layer NAT (SIP, SDP). The application layer NAT is instead performed by the OpenScape SBC. The NE-NAT firewall supports two subnets for each external VLAN 802.1q tagged network however the OpenScape SBC is configured with the SIP information needed to communicate in the external network (WAN) and is thus able to perform all application layer NAT on behalf of the firewall.
- The OpenScape SBC is configured to communicate with the OpenScape Branch (Proxy) through the firewall however there are multiple NAT’s involved, i.e., Subnet1-Subnet2, Subnet2-Subnet3 which are not really needed.
- The external firewall is configured to route IP messages between external network interfaces and the OpenScape SBC Access IP for the VLAN. The OpenScape SBC performs all SIP/SDP NAT using the firewall external IP address corresponding to the VLAN.
- For RTP media streams the firewall becomes a gateway for the OpenScape SBC. The firewall must be configured with the same RTP media ports as the OpenScape SBC with static port forwarding. When RTP media packets arrive from the remote network interfaces, the firewall establishes a pinhole for both subnets to enable sending RTP media packets to the other.

4. Hosted OpenScape Branch (SBC)

This scenario is similar to the remote user scenario except that the dynamic NAT must be considered for the OpenScape Branch SBC and other OpenScape Branch VoIP devices.



Firewall implications:

Mixing far-end NAT requiring Hosted NAPT traversal (HNT) and near-end NAT for the firewall requires special consideration since the OpenScape SBC must route packets to the NAT device for all interfaces.

For registrations, the firewall must either establish a SIP contact address pinhole, or SIP signaling address pinhole for the registering device. The signaling pinhole remains until the HNT device stops communication using the SRC-IP:Port and the pinhole times out and is closed. This could occur when the device behind the HNT interface is being powered off, re-initializing establishing a new SIP contact binding, or the HNT device establishing a new SRC-IP.

For SIP OPTIONS exchange, the firewall must establish a SIP signaling address pinhole for the OpenScape Branch. The signaling pinhole remains until the HNT device stops communication using the SRC-IP:Port and the pinhole

times out and is closed. This could occur when the HNT device is establishing a new SRC-IP.

The external firewall is configured to route IP messages between external network interfaces and the OpenScape SBC Access IP. The OpenScape SBC performs all SIP/SDP NAT using the firewall external IP address.

NOTICE: (Currently not supported) In the future it may be desirable or required than the near-end NAT requirements be supported by the external firewall. When this capability is available the following would apply.

For RTP media streams the firewall becomes a gateway for the OpenScape SBC. The firewall must be configured with the same RTP media ports as the OpenScape SBC with static port forwarding. When RTP media packets arrive from the remote network interfaces, the firewall establishes a pinhole for both subnets to enable sending RTP media packets to the other.

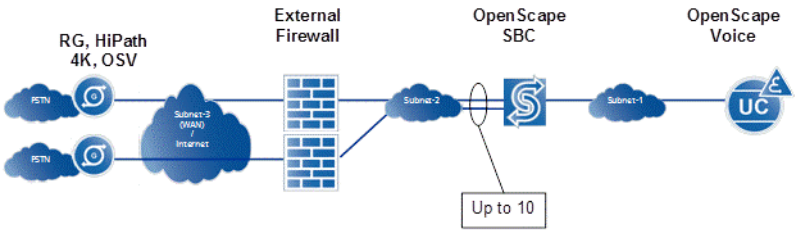
For RTP media streams the firewall becomes a gateway for the OpenScape SBC. The firewall must be configured with the same RTP media ports as the OpenScape SBC with static port forwarding. When RTP media packets arrive from HNT devices, the firewall updates its pinhole with the FE-NAT IP address and port for the HNT media stream. It passes the RTP media packets unchanged to the OpenScape SBC to allow updating its RTP destination IP address and port.

---

5. Standalone SIP-Q Gateways (not behind OpenScape Branch)

Facilitates the connection of remote SIP-Q gateways, such as OpenScape Business, OpenScape 4000, or RG gateways, which are connected to the central headquarters via a WAN, such as an untrusted or public network.

The OpenScape SBC is required for NATing and security at the data center.



Firewall implications:

There is no HNT, however the firewall support for this scenario is similar to the one for OpenScape Branch (Proxy). The SIP message SIP-Q body is transparently sent between the firewall network interfaces without any NAT performed in the firewall.

The firewall may be configured to operate in a “pseudo-transparency mode” where it does not perform any application layer NAT (SIP, SDP), which is instead performed by the OpenScape SBC. The firewall supports two subnets for the enterprise external network however the OpenScape SBC is configured

with the SIP information needed to communicate in the external network (WAN) and is thus able to perform all application layer NAT on behalf of the firewall.

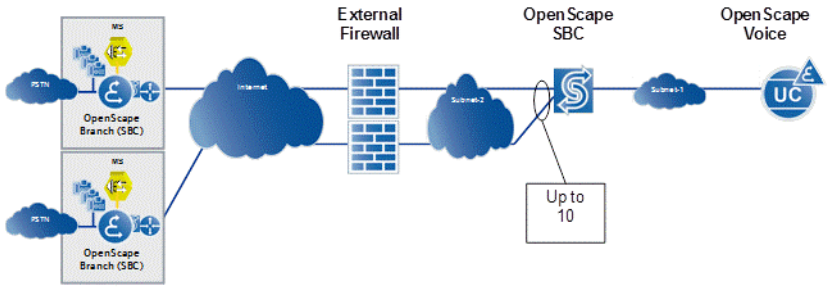
The OpenScape SBC is configured to communicate with the gateway through the firewall however there are multiple NAT's involved, i.e., Subnet2-Subnet3.

For RTP media streams the firewall becomes a gateway for the OpenScape SBC. The firewall must be configured with the same RTP media ports as the OpenScape SBC with static port forwarding. When RTP media packets arrive from the remote network interfaces, the firewall establishes a pinhole for both subnets to enable sending RTP media packets to the other.

6. MGCP Signaling Support for Remote Media Servers

Facilitates the connection of a remote branch office that requires the use of an external OpenScape Media Server connected to the central headquarters via the enterprise network or WAN. In this case the OpenScape SBC supports the MGCP signaling connection between the OpenScape Media Server located at the brand office and the OpenScape Voice system located at the central headquarters.

The OpenScape SBC is optional when the connection is via a trusted enterprise network and there is no NATing to be performed; however, the OpenScape SBC may still be desired for serviceability and/or security reasons.



4.4.3.1 How to Configure the Firewall

Proceed as follows to configure the firewall rules.

Prerequisites

Adequate administrative permissions.

At least one OpenScape SBC is configured and in operation.

The connection to the OpenScape Voice system is up.

Step by Step

1) Navigate to **Configuration** tab > **OpenScape SBC** within the Navigation Bar in the Common Management Platform.

2) Select the **OpenScape SBC list** in the Navigation Tree under **Administration**.

   The system presents the **OpenScape SBC Overview** in the Work Area with a current list of all SBCs.

3) To view a list of SBCs configured at a specific communication system, select a communication system in the **Communication System** field in the navigation tree.

   The default selection for the **Communication System** field is the selection of the global settings in the system menu.

4) To find and select a particular OpenScape SBC use one of the following options:

   - In the Work Area select the checkbox to the left of the particular SBC in the list and select **Manage**.
   - Choose a SBC from the **OpenScape SBC** pull-down located in the Navigation Tree.

   General dialogue is presented in the Work Area displaying information and data for the selected SBC.

5) Navigate to **Configuration** > **Security** > **General** in the navigation tree under **Administration**.

   The **Security** window appears with the **General** tab selected.

6) Select the **Firewall** tab.

   The **Firewall** tab window appears with the following displayed.

   - **Network ID** - Name
   - **Access IP** - Address
   - **External Firewall** - indication
   - **DNS** - indication
   - **FTP** - indication
   - **SSH** - indication
   - **TELNET** - indication
   - **SNMP** - indication
   - **ICMP** - indication
   - **NTP** - indication
   - **SIPP** - indication
   - **RTP/sRTP** - indication
   - **TLS** - indication
   - **MGCP** - indication

7) Click the **Add...** button.

   The **Add Firewall** window appears.

   NOTICE: For editing a firewall click the **Edit** button. The **Edit Firewall** window will be displayed. Refer to the Add Firewall steps for associated information.

   ---

8) Select the Network ID from the **Network ID** field list, to provide a default access IP association to the Remote Endpoint.

   The location of the Remote Endpoint is also identified dynamically based on the access IP which its communicating to, however if a message is not received from the Remote Endpoint, then the assigned access IP is used

to reach the Remote Endpoint. Any changes in Remote Endpoint to access IP association based on the actual IP used by Remote Endpoint is not reflected in the configuration.

9) To enable external firewall configuration, check the **External Firewall** checkbox. Saving the configuration with “External Firewall” checked, without entering any external firewall configuration parameters identifies that the external firewall will be operating in “transparent mode”.

NOTICE: If “transparent mode” external firewall operation is to be used the external firewall configuration fields “SIP ALG” (currently non-selectable) and “Firewall External IP Address” must be reset to their default values. If the initial configuration selection is “External Firewall” these fields are automatically reset to their defaults.

Selecting “External Firewall” does not disable the internal OpenScape SBC firewall for that Network ID. The external firewall may be configured to provide its own filtering rules to block specific traffic.

For each Network ID with “External Firewall” checked, both the OpenScape SBC and external firewall configuration must be coordinated to support a common security profile, otherwise communication with external network interfaces will not be possible.

---

10) (Currently not supported) To enable the firewall external firewall to perform NAT on all SIP and SDP address fields, check the **SIP ALG** checkbox, in the External Firewall work area. If **SIP ALG** is selected the **Firewall Profile** selected from the field list identifies the behavior of the external firewall when it is performing SIP ALG. Currently there are no selectable firewall profiles.

NOTICE: The **Firewall External IP Address** configuration parameter not applicable when **SIP ALG** is selected. The **Firewall Profile** field list is currently not supported.

---

11) (Currently not supported) Select the Firewall Profile from the **Firewall Profile** field list, in the External Firewall work area, to identify the behavior of the external firewall when performing SIP ALG.

12) Enter the IP address (IPv4 or IPv6), for the External Firewall, in the **Firewall External IP Address** field, in the External Firewall work area. The OpenScape SBC will use this address to perform SIP/SDP NAT for all IP address fields in the SIP message or SDP.

13) (Currently not supported) Enter the IP address (IPv4 or IPv6), for the Internal Firewall, in the External Firewall work area, in the **Firewall Internal IP Address** field.

14) To activate masquerading, check the **Enable masquerading** checkbox, in the general work area. The masquerading will mask the LAN (Local Area Network) addresses in WAN (Wide Area Network). This will hide the entire internal address space which will appear as a single IP address in another, (public) address space.

NOTICE: The activation of masquerading is only possible for Session Border Controllers (e.g., the OpenScape

Branch system is configured in SBC (Session Border Controller) mode). This mode is configured via the **Mode** field in the **Voice over IP** window

15) Use the checkboxes in the **Incoming/Outgoing WAN network connections** field area to enable some protocols to access the WAN interface. If the **Allow all WAN network connections** checkbox is checked, the firewall for the protocols checked above is disabled.

16) Use the checkboxes in the **Incoming WAN VoIP connections** field area to enable protocols of the incoming VoIP connections.

17) To block Incoming/Outgoing WAN network connections for a specific IP/Port, click the **Black List - Configure** button. This option is only available for OpenScape Branch V1R3 and later versions, and OpenScape SBC V1 and later versions.

    The **Black List** window appears. The list shows the IPaddresses/subnets and Ports which are blocked.

18) To configure the list, the following options appear:

    - Select an entry from the list and click the **Delete** button to remove an entry from the list.
    - Select an entry from the list and click the **Edit..**. button to edit the entry.
    - Click the **Add** button to add a new rule to the list.

    The **Add Black List** window appears.

19) Enter the IP address (IPv4 or IPv6), Subnet or Logical Branch Office ID to be blocked in the **IP address/Subnet/Logical Branch Office ID** field.

    The Logical Branch Office ID is supported for endpoints configured for Dynamic IP.

    NOTICE: Please note that an IP address can either belong to the white list OR the black list.

20) Enter the port number to be blocked in the **Port** field. If the **Port** field is empty, all ports will be blocked.

21) Click the **OK** button to close the **Add Black List** window.

22) Click the **OK** button to close the **Black List** window.

23) To allow Incoming/Outgoing WAN network connections for a specific IP/Port, click the **White List - Configure** button. This option is only available for OpenScape Branch V1R3 and later versions, and OpenScape SBC V1 and later versions.

    The **White List** window appears. The list shows the IPaddresses/subnets and Ports which are blocked.

24) To configure the list, the following options appear:

    - Select an entry from the list and click the **Delete** button to remove an entry from the list.
    - Select an entry from the list and click the **Edit..**. button to edit the entry.
    - Click the **Add** button to add a new rule to the list.

    The **Add White List** window appears.

25) Enter the IP address (IPv4 or IPv6), Subnet or Logical Branch Office ID to be blocked in the **IP address/Subnet/Logical Branch Office ID** field.

    The Logical Branch Office ID is supported for endpoints configured for Dynamic IP.

    NOTICE: Please note that an IP address can either belong to the white list OR the black list.

26) Enter the port number to be blocked in the **Port** field. If the **Port** field is empty, all ports will be blocked.
27) Click the **OK** button to close the **Add White List** window.
28) Click the **OK** button to close the **White List** window.
29) Click the **OK** button to store the changes temporarily in the administrator´s login session.

    The **Security** dialog disappears.
30) Click the **Apply changes** button in the main window.

The firewall settings are applied on the OpenScape SBC or Branch system.

NOTICE: Message Rate Control (if enabled) will be restarted if the firewall rules are changed.

4.4.3.2 How to Configure Port Forwarding

Proceed as follows to configure the port forwarding settings.

Prerequisites

Adequate administrative permissions.

At least one OpenScape SBC is configured and in operation.

The connection to the OpenScape Voice system is up.

Step by Step

1) Navigate to **Configuration** tab > **OpenScape SBC** within the Navigation Bar in the Common Management Platform.
2) Select the **OpenScape SBC list** in the Navigation Tree under **Administration**.

   The system presents the **OpenScape SBC Overview** in the Work Area with a current list of all SBCs.
3) To view a list of SBCs configured at a specific communication system, select a communication system in the **Communication System** field in the navigation tree.

   The default selection for the **Communication System** field is the selection of the global settings in the system menu.

4) To find and select a particular OpenScape SBC use one of the following options:

   - In the Work Area select the checkbox to the left of the particular SBC in the list and select **Manage**.
   - Choose a SBC from the **OpenScape SBC** pull-down located in the Navigation Tree.

   General dialogue is presented in the Work Area displaying information and data for the selected SBC.

5) Navigate to **Configuration** > **Security** > **General** in the navigation tree under **Administration**.

   The **Security** window appears with the **General** tab selected.

6) Select the **Firewall** tab.

7) Click the **Add...** or **Edit** button.

   The **Add Firewall** or the **Edit Firewall** window shall be displayed.

8) To activate port forwarding, check the **Enable port forwarding** checkbox, in the **Port FW** work area.

   NOTICE: The activation of port forwarding is only possible for Session Border Controllers (e.g., the OpenScape Branch system is configured in SBC (Session Border Controller) mode). This mode is configured via the **Mode** field in the **Voice over IP** window

   ---

9) Click the **Configure...** button.

   The **Port FW** window appears with a list of port forwarding information (IP addresses/Logical Endpoint IDs., In port, Out port and associated protocol.

   - To delete a rule, select the entry in the list and click the **Delete** button.
   - To edit a rule, select the entry in the list and click the **Edit** button.
   - To add a rule, click the **Add** button.

   NOTICE: For editing a Port Forwarding click the **Edit** button. The **Edit Port FW** window will be displayed. Refer to the Add Port Forwarding steps for associated information.

   ---

10) Click the **Add...** button.

    The **Add Port FW** window appears.

11) Enter a name associated with the port forwarding in the **Name** field.

12) Enter the incoming IP address (IPv4 or IPv6) in the **Source IP** field.

13) Enter the outgoing IP address (IPv4 or IPv6) in the **IP Address/Logical Branch Office ID** field.

14) Enter the incoming port number in the **In port** field.

15) Enter the outgoing port number in the **Out port** field.

16) Select the protocol in the **Protocol** selection list.The following values are possible: **TCP** (Transmission Control Protocol), **UDP** (User Datagram Protocol), **All**.

17) Click the **OK** button.

    The **Add Port FW** window disappears and a new row is created in the Port FW list. The changes are stored temporarily.

18) Click the **OK** button to store the changes temporarily in the administrator´s login session and close the **Port FW** window.

    The **Port FW** dialog disappears and the **Add Firewall** window appears.

19) Click the **OK** button to store the changes temporarily in the administrator´s login session and close the **Add Firewall** window.

    The **Add Firewall** window disappears and the **Firewall** tab appears in the **Security** window.

20) Click the **OK** button to store the changes temporarily in the administrator´s login session and close the **Security** window.

    The **Security** window disappears.

21) Click the **Apply changes** button in the main window, work area.

The port forwarding rules are applied on the OpenScape Session Border Controller system.

NOTICE: Message Rate Control (if enabled) will be restarted if the firewall rules are changed.

4.4.4 Configuration of Administrative Access Control

Administration Access Control can be used to create an access control list of hosts LAN IP addresses and associated secure protocols allowed to administer an OpenScape Session Border Controller. Administration shall be possible from any host when no IP address is provided.

4.4.4.1 How to Configure Administrative Access Control Settings

Proceed as follows to configure an access control list of LAN IP addresses and associated secure protocols allowed to administer an OpenScape Session Border Controller. Administration shall be possible from any host when no IP address is provided.

Prerequisites

Adequate administrative permissions.

At least one OpenScape SBC is configured and in operation.

The connection to the OpenScape Voice system is up.

Step by Step

1) Navigate to **Configuration** tab > **OpenScape SBC** within the Navigation Bar in the Common Management Platform.

2) Select the **OpenScape SBC list** in the Navigation Tree under **Administration**.

   The system presents the **OpenScape SBC Overview** in the Work Area with a current list of all SBCs.

3) To view a list of SBCs configured at a specific communication system, select a communication system in the **Communication System** field in the navigation tree.

   The default selection for the **Communication System** field is the selection of the global settings in the system menu.

4) To find and select a particular OpenScape SBC use one of the following options:

   - In the Work Area select the checkbox to the left of the particular SBC in the list and select **Manage**.
   - Choose a SBC from the **OpenScape SBC** pull-down located in the Navigation Tree.

   General dialogue is presented in the Work Area displaying information and data for the selected SBC.

5) Navigate to **Configuration** > **Security** > **General** in the navigation tree under **Administration**.

   The **Security** window appears with the **General** tab selected.

6) Select the **Firewall** tab.

7) Click the **Configure...** button.

   The Access Control Security settings are displayed in a list with the following columns: **IP address**: Defines the host IP address allowed to administer the OpenScape Session Border Controller. **SSH**: Indicates access via this protocol is enabled or disabled. **HTTPS**: Indicates access via this protocol is enabled or disabled. **FTP**: Indicates access via this protocol is enabled or disabled.

8) To configure Administrative Access connections, use one of the following options:

   - To remove an entry from the Access Control connections list, select the respective row and click the **Delete** button. The Access Control list entry is removed from the list.
   - To edit an Access Control entry in the list, select the respective row and click the **Edit** button.
   - To add an Access Control entry to the list, click the **Add** button.

   The **Add/Edit Administrative Access Control** window appears.

9) Enter the IP address (IPv4 or IPv6) allowed for Administration access in the **IP address** field.

10) Checkmark the **SSH** check box if SSH protocol is to allowed to be used for this IP address.

11) Checkmark the **HTTPS** check box if HTTPS protocol is allowed to be used for this IP address.

12) Checkmark the **FTP** check box if FTP protocol is allowed to be used for this IP address.

13) Click the **OK** button to go back to the Administrative Access Control window.

    The **Administrative Access Control** window appears and the list is updated.

14) Click the **OK** button to store the changes temporarily in the administrator´s login session and close the **Administrative Access Control** dialog.

    The **Administrative Access Control** dialog disappears and the **Add Firewall** dialog appears.

15) Click the **OK** button to store the changes temporarily in the administrator´s login session and close the **Add Firewall** dialog.

    The **Add Firewall** dialog disappears and the **Firewall** tab, on the **Security** window appears.

16) Click the **OK** button to go back to the **Security** window.

    The **Access Control** dialog is updated.

17) Click the **OK** button to store the changes temporarily in the administrator´s login session and close the **Security** window.

    The **Security** dialog disappears.

18) Click the **Apply changes** button in the main window, work area, to save the changes permanently.

The Administrative Access List Security settings are applied on the OpenScape SBC.

NOTICE: Message Rate Control (if enabled) will be restarted if the firewall rules are changed.

4.4.5 RADIUS Support - Overview

RADIUS-enabled network support (Authentication, Authorization, and Accounting - AAA) functionality (RFCs 2865ff) is available in the OpenScape SBC.

Radius Support

RADIUS servers utilize the free RADIUS software application. This application comes with a PAM plug-in module that will be deployed as part of the OpenScape SBC solution.

OpenScape SBC provides the ability to connect to two different RADIUS servers.

NOTICE: SNMP or SIP authentication or accounting is not supported.

NOTICE: RADIUS challenge/response capabilities are not supported.

IMPORTANT: The customer must not configure the ‘assistant’ or ‘redundancy’ users on the RADIUS server. These are internal accounts that are only used by software components.

4.4.5.1 How to Configure Radius

Proceed as follows to configure RADIUS-enabled network support.

Prerequisites

Adequate administrative permissions.

At least one OpenScape SBC is configured and in operation.

The connection to the OpenScape Voice system is up.

Step by Step

1) Navigate to **Configuration** tab > **OpenScape SBC** within the Navigation Bar in the Common Management Platform.
2) Select the **OpenScape SBC list** in the Navigation Tree under **Administration**.

   The system presents the **OpenScape SBC Overview** in the Work Area with a current list of all SBCs.
3) To view a list of SBCs configured at a specific communication system, select a communication system in the **Communication System** field in the navigation tree.

   The default selection for the **Communication System** field is the selection of the global settings in the system menu.
4) To find and select a particular OpenScape SBC use one of the following options:

   - In the Work Area select the checkbox to the left of the particular SBC in the list and select **Manage**.
   - Choose a SBC from the **OpenScape SBC** pull-down located in the Navigation Tree.

   General dialogue is presented in the Work Area displaying information and data for the selected SBC.
5) Navigate to **Configuration** > **Security** > **RADIUS** in the navigation tree under **Administration**.

   The **Security** window appears with the **RADIUS** tab selected.
6) Checkmark the **Enable RADIUS** checkbox to enable configuration of RADIUS servers, authentication and accounting.

7) To configure **Server 1** and/or **Server 2**, proceed as follows:

NOTICE: Server 2 is optional.

---

a) **Address** - Enter the IP Address/FQDN.

NOTICE: The use of an IP address is preferred over an FQDN.

---

b) **Port** - This field is optional.A number in the range 0-65535 or "radius" (1812/1813) can be used to indicate the port number for RADIUS authentication.

NOTICE: The port number for accounting is hard-coded to be the next value up from the authentication port number. If the user does not provide the port number for authentication, the RADIUS feature looks up the 'radius' and 'radius-acct' entries in /etc/services and uses those values.

---

c) **Secret** - This entry is mandatory and identifies the shared secret that the RADIUS server and the OpenScape SBC share. A string with 16 characters is mandatory. It can consist of upper or lower case letters, digits, or special characters.

Special characters can be any of the following set:

NOTICE: The secret is a text string that is used to obfuscate some components of the RADIUS protocol. It is never passed in any messages between the client and the server.

---

d) **Timeout** - Enter the Time-out in number of minutes. Allowed values in the range: 1-10. (default = 3).

8) To configure RADIUS Authentication and/or RADIUS Accounting, proceed as follows:

NOTICE: When **Enable RADIUS** is selected, the Authentication service or Accounting service (or both) must be selected and, for each selected service, at least one application must be enabled.

---

a) **Enable RADIUS Authenication** - Checkmark to enable configuration of RADIUS authentication.

b) **Enable RADIUS Accounting** - Checkmark to enable configuration of RADIUS accounting.

c) Checkmark the appropriate checkboxes to select which application will use RADIUS for user Authentication and Accounting.

CLI - controls the users connected directly to a terminal.

SSH - controls the users using a Secure Shell or a Secure FTP connection.

Web - controls the users using an Internet Browser (Local GUI).

9) Click the **OK** button to store the changes temporarily in the administrator´s login session.

The **System** dialog disappears.

10) Click the **Apply changes** button in the main window.

The password is changed or set to default in the OpenScape Branch system.

NOTICE: Changing the password stored in the assistant's local database is possible via the **Local Password** button in the **Overview** window. This it is not applied to the OpenScape SBC appliance. Please refer to the "OpenScape SBC Assistant – Primary Administration" chapter of this documentation for more information.

4.5 Survivability and Redundancy — Overview

Survivability is the capability of a network to maintain service continuity in the presence of faults within the network. Redundancy provides for better survivability.

Survivability Mechanisms within OpenScape Voice

In the OpenScape Voice environment, survivability mechanisms such as protection and restoration have been implemented either on a per-link basis, on a per-path basis, or throughout an entire network to alleviate service disruption. This environment also provides managed redundant IP Voice systems that take advantage of IP's inherent survivability/rerouting capabilities. Plus, the VoIP's ability to make call routing decisions contingent on the IP network's status, makes for a robust and survivable voice communications system. The OpenScape Voice landscape network can terminate calls in one of two places; to another IP telephony device/endpoint or a VoIP gateway that interfaces to the local PSTN (Public Service Telephony Network). Call routing redundancy schemes provide that outbound calls make it to the PSTN even if the preferred local gateway or PSTN service is down. Redundant OpenScape Session Border Controllers provide additional network survivability with OpenScape Voice.

There are various options for deploying OpenScape SBC redundancy based on the customers network, location of data centers and number of data centers. The basic configurations for OpenScape Voice are:

- Simplex OpenScape Voice (OSV)
- Duplex collocated OSV
- Geo-separated OSV with OpenScape SBCs

SBC Redundancy

OpenScape SBC supports unit redundancy using two OpenScape SBC units side-by-side, with the same database and connected to the LAN with Virtual IP addresses. They operate on a Active and Stand-by mode. If the Active unit fails, the Stand-by unit becomes the Active and takes over the functionality.

NOTICE: Redundancy is also supported on the WAN interface, provided that the **Enable Redundancy** & **Enable access link consistency check** flags are enabled.

Enabling Redundancy

It is recommended to change the default redundancy password on each node separately before enabling the Redundancy; otherwise the system will fail to replicate the configuration to the other node. Both nodes must use the same redundancy password. Data synchronization will also fail if different software versions run in the system. After configuring the redundant system, the passwords are included in the data synchronization. When changing the redundancy password in the master node, the previous password is used in the backup node until data synchronization. After the synchronization, the redundancy password is updated.

To enable Redundancy, it is necessary to configure the IP address of Nodes 1 and 2 and configure the redundant virtual IP address. This operation requires a system restart. After restarting the system, configuration of Node 1 is automatically replicated to Node 2 (redundancy is automatically enabled on Node 2). Once Redundancy is enabled, configuration is allowed only on the master node.

Disabling Redundancy

To disable the Redundancy it is required to configure Node 1 and Node 2 separately as the following. First configure a temporary IP in the Master node and uncheck the Redundancy Enable checkbox, so the system will restart with Redundancy disabled and the other system will unable to take the control (unable to reach the system as the IP address was changed). The other node will remain in Backup state for about 9 minutes and then will become the Master node. Now it is possible to change the configuration on this node, so configure a temporary IP and uncheck the Redundancy Enable checkbox (system will restart). Now both systems are operating with Redundancy disabled and it is possible to restore the IP configuration.

Upgrading a Redundant System

The upgrade process is started in the Master node. Once the upgrade in the Master node is finished the system will reboot (after the user confirmation or via scheduled upgrade) and the Backup node will become the Master node. When the previous Master node is running again, after 5 minutes the SW image will be uploaded to the former Backup node (now Master). After the upload is finished the Master node will start the upgrade, once the upgrade is complete this system reboots. The Backup node will become the Master node again, once the Backup node is running again both nodes now have been upgraded and the process is finished.

The Local GUI/CMP shows the upgrade progress only while upgrading the Master node. The upgrade completion on the other node must be further verified by checking the software information (version).

OpenScape SBC — Redundancy Configuration

The OpenScape SBC infrastructure must be configured according to the redundancy model used.

- Collocated
- Geo-separated

4.5.1 How to Configure Redundancy Settings

Proceed as follows to configure the redundancy settings for OpenScape SBC.

Prerequisites

It is recommended to change the default redundancy password on each node separately before enabling the Redundancy; otherwise the system will fail to replicate the configuration to the other node. Both nodes must use the same redundancy password. Data synchronization will also fail if different software versions run in the system. After configuring the redundant system, the passwords are included in the data synchronization. When changing the redundancy password in the master node, the previous password is used in the backup node until data synchronization. After the synchronization, the redundancy password is updated.

Adequate administrative permissions.

At least one OpenScape SBC is configured and in operation.

The connection to the OpenScape Voice system is up.

Step by Step

1) Navigate to **Configuration** tab > **OpenScape SBC** within the Navigation Bar in the Common Management Platform.

2) Select the **OpenScape SBC list** in the Navigation Tree under **Administration**.

The system presents the **OpenScape SBC Overview** in the Work Area with a current list of all SBCs.

3) To view a list of SBCs configured at a specific communication system, select a communication system in the **Communication System** field in the navigation tree.

The default selection for the **Communication System** field is the selection of the global settings in the system menu.

4) To find and select a particular OpenScape SBC use one of the following options:

- In the Work Area select the checkbox to the left of the particular SBC in the list and select **Manage**.
- Choose a SBC from the **OpenScape SBC** pull-down located in the Navigation Tree.

General dialogue is presented in the Work Area displaying information and data for the selected SBC.

5) Navigate to **Configuration > Network Services** in the navigation tree under Administration.

The **Network Services** window appears with the **Interfaces** tab selected by default.

6) Select the **Redundancy** tab.

7) To enable the Redundancy, check the **Enable Redundancy** checkbox.

8) Select the SBC redundancy mode system´s type in the **Mode** selection list. The mode determines where OpenScape SBC is located in relationship to the redundant OpenScape SBC in the network. Possible values:
   - **Collocated**: In this mode redundant SBCs are located in the same data network.
   - **Geo-Separated**: (Supported in Version 2) This mode means that the two nodes are located in different data networks.
9) For a Geo-Separated configuration, Enter the Geo Separated IP address (IPv4 or IPv6) in the **Geo Separated OSB IP Address** field in the General work area. (Supported in Version 2)
10) For a Geo-Separated configuration, Enter the Data transfer interval in the **Data transfer interval** field, in the General work area. (Supported in Version 2).
11) Enter the data transfer interval in the **Data transfer interval** field, in the General work area.
12) Enter the backup LAN IP address (IPv4 or IPv6) in the **Backup IP address** field under the LAN section. This is the backup IP address used by the redundant OpenScape SBCs.
13) Enter the virtual LAN IP address (IPv4 or IPv6) in the **Virtual IP address** field under the LAN section. This is the virtual IP address used by the redundant OpenScape SBCs.
14) Enter the backup WAN IP address (IPv4 or IPv6) in the **Backup IP address** field under the WAN section. This is the backup IP address used by the redundant OpenScape SBCs.
15) Enter the virtual WAN IP address (IPv4 or IPv6) in the **Virtual IP address** field under the WAN section. This is the virtual IP address used by the redundant OpenScape SBCs.

    The Virtual Addresses for the LAN and WAN must be the same value for the LAN and the WAN.
16) Click the **OK** button to close the **System** window.
17) Click the **OK** button to store the changes temporarily in the administrator´s login session and close the **Network Services** window.

    The **Network Services** dialog disappears.
18) Click the **Apply changes** button in the main window, work area.

The settings for redundancy are applied on the OpenScape SBC system.

NOTICE: To enable Redundancy, it is necessary to configure the IP address of Nodes 1 and 2 and configure the redundant virtual IP address. This operation requires a system restart. After restarting the system, configuration of Node 1 is automatically replicated to Node 2 (redundancy is automatically enabled on Node 2). Once Redundancy is enabled, configuration is allowed only on the master node.

4.6 System Settings — Overview

The system settings mainly serve to configure the protocols and password settings of the OpenScape Session Border Controller (SBC) system and enables the administrator to perform some service tasks.

General Settings

Via OpenScape SBC Assistant the following protocols, interfaces or system parameters have to be configured using the system settings section:

- **Licensing Information**:

  The License Server and Backup Server information is located in the general settings area.

  – OpenScape SBC will be provisioned with a License Server URI.
  – The OpenScape SBC devices will be provisioned with an optional Backup Management Server URI. If configured, OpenScape SBC devices will register with the Backup Management Server URI for tasks other than licensing (e.g. for a Geo-separated deployment where the nodes are unable to communicate and a CMP is co-located with each OpenScape Voice node). Note: licenses are only kept on one CMP.

  NOTICE: The values in the Licensing section are pre-configured via the USB stick installation of the OpenScape SBC.

Password

To access an OpenScape SBC system, the administrator has to login via OpenScape Voice Assistant. Access to the https management interface is protected by a user name and password that must be validated using PAM (Pluggable Authentication Module) authentication. Currently a single administrator login is required. This implies that every log-in has full access to all the data on the OpenScape SBC device.

There is one (common) default password for all OpenScape SBC devices in order to ease the access of CMP (Common Management Platform) to different OpenScape SBCs devices. Changing the default password at any time is possible. It is also possible to reset the password to the default value at any time. The password is stored in encrypted format in the OpenScape SBC device and has no expiration time.

NOTICE: Changing the password stored in the assistant's local database is possible via the **Local Password** button in the **Overview** window. This it is not applied to the OpenScape SBC appliance. Please refer to the "OpenScape Session Border Controller – Primary Administration" chapter of this document for more information.

Import / Export

The system settings provide serviceability functions such as loading configuration files in order to change the configuration of the system or exporting configuration files. The administrator can restart the system to

the current configuration or to the backup configuration. Please refer to the Maintenance - chapter, Serviceability section of this document for more information.

4.6.1 How to Display and Change License Server Location

Proceed as follows to display or change the license server or backup management server location.

Prerequisites

Adequate administrative permissions.

At least one OpenScape SBC type is configured and in operation.

The connection to the OpenScape Voice system is up.

Step by Step

1) Navigate to **Configuration** tab > **OpenScape SBC** within the Navigation Bar in the Common Management Platform.
2) Select the **OpenScape SBC list** in the Navigation Tree under **Administration**.

   The system presents the **OpenScape SBC Overview** in the Work Area with a current list of all SBCs.
3) To view a list of SBCs configured at a specific communication system, select a communication system in the **Communication System** field in the navigation tree.

   The default selection for the **Communication System** field is the selection of the global settings in the system menu.
4) To find and select a particular OpenScape SBC use one of the following options:

   - In the Work Area select the checkbox to the left of the particular SBC in the list and select **Manage**.
   - Choose a SBC from the **OpenScape SBC** pull-down located in the Navigation Tree.

   General dialogue is presented in the Work Area displaying information and data for the selected SBC.
5) Navigate to **Configuration** > **System** in the navigation tree under **Administration**

   The **System** window appears with the **General** tab selected by default and the following server information is displayed:

   - **License Server and Associated Port:**

     The URI is provisioned with the OpenScape SBC Assistant IP and port 4709 for access by the OpenScape SBC server. However, in the future the license server may be off a different server.
   - **Backup management server and associated port**:

     OpenScape SBC devices may be provisioned with an optional Backup Management Server URI. If configured, OpenScape SBC devices will register with the Backup Management Server URI for tasks other than

licensing (e.g. for a Geo-separated deployment where the nodes are unable to communicate and a CMP is co-located with each OpenScape Voice node).

NOTICE: Licenses are kept only in one CMP. The values in the Licensing section are pre-configured via the USB stick installation of the OpenScape SBC.

6) To change a licensing and backup management locations, proceed as follows: (Currently not supported):
   a) Enter the new license server location URL in the **License server** field.
   b) Enter the associated port number of the license server in the **Port** field.
   c) Enter the new backup management server location URL in the **Backup management server** field.
   d) Enter the associated port number of the backup management server in the **Port** field.
   e) Click the **OK** button to store the changes temporarily in the administrator's login session.

   The **System** dialog disappears and the main work window is displayed.
7) Click the **Apply changes** button in the main window.

The server information is changed in the OpenScape SBC.

4.6.2 How to Change or Reset the Password

Proceed as follows to change or reset the login password for the access to the OpenScape Session Border Controller (SBC) or Branch system.

Prerequisites

Adequate administrative permissions.

At least one SBC or branch office of the OpenScape Branch type is configured and in operation.

The connection to the OpenScape Voice system is up.

Step by Step

1) Navigate to **Configuration** tab > **OpenScape SBC** within the Navigation Bar in the Common Management Platform.
2) Select the **OpenScape SBC list** in the Navigation Tree under **Administration**.

   The system presents the **OpenScape SBC Overview** in the Work Area with a current list of all SBCs.
3) To view a list of SBCs configured at a specific communication system, select a communication system in the **Communication System** field in the navigation tree.

   The default selection for the **Communication System** field is the selection of the global settings in the system menu.

4) To find and select a particular OpenScape SBC use one of the following options:
   - In the Work Area select the checkbox to the left of the particular SBC in the list and select **Manage**.
   - Choose a SBC from the **OpenScape SBC** pull-down located in the Navigation Tree.

   General dialogue is presented in the Work Area displaying information and data for the selected SBC.
5) Navigate to **Configuration** > **System** in the navigation tree under **Administration**

   The **System** window appears with the **General** tab selected by default.
6) Select the **Password** tab.
7) To reset a password, proceed as follows:
   a) Select the user for whom the password shall be reset in the **Select user** selection list. Possible users: administrator, assistant, guest, redundancy, service.
   b) Click the **Reset** button.

   The password will be set to default for the selected user.

   NOTICE: The users and their default passwords are referenced in OpenScape SBC Configuration Guide.
8) To change a password, proceed as follows:
   a) Select the user for whom the password shall be changed in the **Select user** selection list. Possible users: administrator, service, guest, redundancy, assistant, redundancy user.
   b) Enter the old password in the **Old Password** field.
   c) Enter the new password of the OpenScape SBC appliance in the **New Password** field.

      Password requirements:
      - The password must be 12...36 characters, with at least one upper case letter, one lower case, one digit and one special character.
      - User cannot use passwords similar to its username, as well as common passwords like "password", "qwerty", "abcdefgh", "user".
      - User cannot reuse any of their **last five passwords** when changing their password.

   d) Enter the new local password of the OpenScape SBC appliance again in the **Confirm** new password field.
   e) Click the **Change** button.

   The password will be changed and a confirmation message is displayed.

The password is changed or set to default in the OpenScape SBC.

NOTICE: Changing the password stored in the assistant's local database is possible via the **Local Password** button in the **Overview** window. This it is not applied to the OpenScape SBC. Please refer to the "OpenScape SBC Assistant – Primary Administration" chapter of this documentation for more information.

Related concepts

Password Management on page 67

Related tasks

How to Change the Password in the Local Assistant Database on page 34

4.6.3 How to Import/Export and Select Configuration Files via OpenScape SBC Assistant

Proceed as follows to import/export and select configuration files using OpenScape SBC Assistant.

Prerequisites

Adequate administrative permissions.

At least one OpenScape SBC is configured and in operation.

The connection to the OpenScape Voice system is up.

Step by Step

1) Navigate to **Configuration** tab > **OpenScape SBC** within the Navigation Bar in the Common Management Platform.
2) Select the **OpenScape SBC list** in the Navigation Tree under **Administration**.

   The system presents the **OpenScape SBC Overview** in the Work Area with a current list of all SBCs.
3) To view a list of SBCs configured at a specific communication system, select a communication system in the **Communication System** field in the navigation tree.

   The default selection for the **Communication System** field is the selection of the global settings in the system menu.
4) To find and select a particular OpenScape SBC use one of the following options:

   - In the Work Area select the checkbox to the left of the particular SBC in the list and select **Manage**.
   - Choose a SBC from the **OpenScape SBC** pull-down located in the Navigation Tree.

   General dialogue is presented in the Work Area displaying information and data for the selected SBC.
5) Navigate to **Configuration** > **System** in the navigation tree under **Administration**

   The **System** window appears with the **General** tab selected by default.
6) Select the **Import/Export** tab to import or export a configuration file.

   The **File in use** field displays the name of the configuration file currently in use.

7) Click the **Import** button to import a new configuration file.

The **Import** window appears.

a) Click the **Browse...** button to select the file name and path of the configuration file to be transferred to the system

b) Click the **OK** button

The **Import** window closes and selected configuration XML (Extensible Markup Language) is temporarily applied to the system. The **Apply Changes** button in the main menu becomes enabled and navigation in any of the configuration menu screens will indicate the temporarily imported configuration.

8) Click the **Export** button to export a single configuration file.

The **file Download** dialog opens.

a) Use one of the following options:

Click the **Open** button to open and display the configuration file in the system´s XML (Extensible Markup Language) file viewer application.

Click the **Save** button and specify the location of the configuration file to be exported. Then click the **Save** button in the **Save As** dialog.

Click the **Cancel** button to abort the action and return to the **Export/ Import** tab window.

b) Remember to **Apply Changes** in the main window.

9) Click the **Export All** button (optional) to export all configuration files.

The **file Download** dialog opens.

a) Use one of the following options:

Click the **Open** button to open and display the configuration file in the system´s XML (Extensible Markup Language) file viewer application.

Click the **Save** button and specify the location of the configuration file to be exported. Then click the **Save** button in the **Save As** dialog.

Click the **Cancel** button to abort the action and return to the **Export/ Import** window.

b) Remember to **Apply Changes** in the main window.

10) To select (load) a new configuration file for use:

a) Select the configuration file in the **Use a new configuration file** field list.

b) Click the **Load** button

The system reads and stores the xml config file settings temporarily.

11) Click the **OK** button to store the changes temporarily in the administrator´s login session.

The **System** dialog disappears.

12) Click the **Apply changes** button in the main window.

The configuration files are stored to the OpenScape SBC.

4.7 Voice over Internet Protocol Configuration — Overview

VoIP (Voice over Internet Protocol) is a transmission technology for delivery of voice communications over IP networks such as the Internet.

OpenScape SBC Assistant allows to configure the settings for "Voice over IP" telephony, the communication system and periphery for both OpenScape Session Border Controllers (SBC).

General Configuration

Functionality and configuration specific to OpenScape SBC.

- Supported deployment modes: Central SBC (OpenScape SBC), Proxy, SBC Proxy, bSBC, Proxy ATA.
- SIP Header Manipulation (applies in survivability mode)
- SIP Routing
- Error Codes
- Core Side Media Configuration
- Listening Ports
- Port Mapping
- Backup Data Channel (this feature is available for OSB V1R3 and later versions)
- Remote Endpoints and Gateways
- SIP Service Provider Profiles (this feature is available for OSB V1R3 and later versions)
- Quality of Service
- Media Servers
- Ms Profiles

Communication System Configuration

- Comm System Type
- Outbound SIP Server
- Trusted IP Addresses
- Node 1 settings
- Node 2 settings

Timers and Thresholds

Several timers and thresholds can be configured to control the system performance of the OpenScape SBC or Branch appliance.

Throttling, Registration Expiry and Remote Subscribers

Throttling and registration expiry can be configured for an OpenScape SBC or Branch appliance. Remote Subscriber firewall, domain and emergency service settings can also be configured.

Configuration Restrictions

Some configurations such as gateway configuration, binding address, emergency services, ACD (Automatic Call Distribution), MLHG (Multiline Hunt Group), digit manipulation, and SIP routing require the automatic restart of SIP server. Therefore the active calls may be dropped.

4.7.1 SIP VoIP Port Configuration and Display

SIP (Session Initiation Protocol) VoIP port configuration is required to specify the ports in the LAN (Local Area Network) where OpenScape SBC will be listening for messages during normal SBC operation, as well as, media configuration.

Requirements

SIP port configuration and displays are as follows:

- Configure VoIP setting for listening ports on the OpenScape SBC.
- Core Side Media Configuration for media security (supported in Version 2)
- Port Mapping Configuration
- Display registered subscriber port map settings for an OpenScape SBC.
- Display of Backup Port Mapping

4.7.1.1 How to Configure VoIP SIP Settings

Proceed as follows to configure the ports in LAN (Local Area Network) where OpenScape Session Border Controller (SBC) will be listening, and the port mapping parameters.

Prerequisites

Adequate administrative permissions.

At least one OpenScape SBC is configured and in operation.

The connection to the OpenScape Voice system is up.

Step by Step

1) Navigate to **Configuration** tab > **OpenScape SBC** within the Navigation Bar in the Common Management Platform.

2) Select the **OpenScape SBC list** in the Navigation Tree under **Administration**.

The system presents the **OpenScape SBC Overview** in the Work Area with a current list of all SBCs.

3) To view a list of SBCs configured at a specific communication system, select a communication system in the **Communication System** field in the navigation tree.

The default selection for the **Communication System** field is the selection of the global settings in the system menu.

4) To find and select a particular OpenScape SBC use one of the following options:

- In the Work Area select the checkbox to the left of the particular SBC in the list and select **Manage**.
- Choose a SBC from the **OpenScape SBC** pull-down located in the Navigation Tree.

General dialogue is presented in the Work Area displaying information and data for the selected SBC.

5) Navigate to **Configuration** > **VoIP** in the navigation tree under **Administration**

   The **Voice over IP** window appears with the **General** tab selected by default.

6) Enter the port number for each protocol **TCP** (Transmission Control Protocol), **UDP** (User Datagram Protocol), **TLS** (Transparent LAN Service) under the **Listening ports** section.

   TCP:5060, UDP:5060, TLS:5061

7) Configure **Core Side Media** as follows:

   a) Select the media security in the **Media security** selection list, in the **Core Side Media Configuration** area.

      - **Pass-Thru** (default) – If both originating and terminating side support the SRTP encryption mechanism then SRTP media is setup end to end in pass-thru mode and OS-SBC is not involved in the SRTP encryption and decryption. SRTP Key coming in from the originating device is being passed as is to the terminating device in addition to the RTP and the other SRTP key giving the option to the terminating side to choose the SRTP/RTP mechanism based on its configuration. For example, if the originating side sends SDES only offer then the terminating side would get RTP, SRTP (Mikey) and SRTP (SDES from the originating side. This allows for additional flexibility in terms of setting up the call. If both parties support the same SRTP mechanism then SRTP media is setup end to end in pass-thru mode and OS-SBC is not involved in the SRTP encryption and decryption.
      - **SRTP +RTP** - Terminating network is enforced with the configured SRTP Mikey or SDES best effort offer. If the Terminating side in OS-SBC is configured with SDES and the originating sides send SDES offer then the SDES is negotiated end to end. However, if the originating side offers Mikey and the terminating side in OS-SBC is configured for SDES then Mikey to SDES RTP is performed.
      - **RTP**

   b) Select the security key exchange method in the **Media security key negotiation** selection list. Values: **SDES**, **MIKEY**, **None**.

      NOTICE: If the Media Protocol is RTP or Pass-Thru no selection is possible. The entry should be **None**.

   c) Checkmark the **Mark SRTP call leg as secure** checkbox, if calls require secure media. When active, this parameter identifies the network as secure if TLS and SRTP are not used, i.e., TCP or UDP for the signaling transport or RTP is used for the media protocol.

   d) Checkmark the **Single m-line SRTP** checkbox, if the Media Protocol single m-line is to be used towards the Core Network. If unchecked a

dual m-line is to be used towards the Core Network. The crypto tokens will be passed through transparently.

The following table shows the possible combinations between Media Protocol, Media Security Key Negotiation and the single m-line parameters for Core-side Media configuration:

Media Protocol (Media security)	Media Security Key	Single m-line checkbox	Description
SRTP + RTP	SDES	Checked	OS SBC offers and accepts RTP and SRTP in a single m-line SDES offer/ answer. OS SBC also accepts SRTP only offers.
		Unchecked (default)	OS SBC offers and accepts RTP and SRTP in a dual m-line SDES offer/ answer. OS SBC also accepts SRTP only offers.
SRTP + RTP	MIKEY	Checked	OS SBC offers and accepts RTP and SRTP in a single m-line MIKEY offer/ answer. OS SBC also accepts SRTP only offers.
		Unchecked (default)	OS SBC offers and accepts RTP and SRTP in a dual m-line MIKEY offer/ answer. OS SBC also accepts SRTP only offers.
RTP	None	Disabled and Unchecked	OS SBC offers and accepts only RTP

Media Protocol (Media security)	Media Security Key	Single m-line checkbox	Description
Pass-Thru	None	Checked	• SRTP + RTP offers (received as single or dual) will be sent out as single m-line SRTP + RTP offers. The master keys will be passed transparently • RTP only offers will be passed through • SRTP only offers will by passed through
		Unchecked	• SRTP + RTP offers (received as single or dual) will be sent out as dual m-line SRTP + RTP offers. The master keys will be passed transparently • RTP only offers will be passed through • SRTP only offers will by passed through

8) Configure **Port Mapping** as follows:

a) Enter the RTP (Real-time Transport Protocol) port range to be used in RTP traffic in the **RTP ports min/max** fields, under **Port Mapping**. The fields are only enabled in SBC (Session Border Controller) mode.

b) Enter the disconnection timer for non RTP activity in the **Time to live** field, under **Port Mapping**. The field is only enabled in SBC mode.

c) Enter the SIP port range to be used in SIP messages in the **Subscriber Dynamic SIP ports min/max** fields, under **Port Mapping**. The fields are only enabled in SBC mode.

d) Enter the SIP endpoint port range to be used in SIP endpoints messages in the **Remote Endpoints Static SIP Ports min/max** fields, under **Port Mapping**. The fields are only enabled in SBC mode

9) Click the **OK** button to store the changes temporarily in the administrator´s login session.

The **Voice over IP** dialog disappears.

10) Click the **Apply changes** button in the main window, work area.

The configuration of the SIP settings is applied on the OpenScape SBC.

4.7.1.2 How to Display Registered Subscribers Port Mapping Settings

Perform the following steps to display a list of port mapping for registered subscribers.

Prerequisites

Adequate administrative permissions.

At least one SBC or branch office of the OpenScape Branch type is configured and in operation.

The connection to the OpenScape Voice system is up.

Step by Step

1) Navigate to **Configuration** tab > **OpenScape SBC** within the Navigation Bar in the Common Management Platform.
2) Select the **OpenScape SBC list** in the Navigation Tree under **Administration**.

   The system presents the **OpenScape SBC Overview** in the Work Area with a current list of all SBCs.
3) To view a list of SBCs configured at a specific communication system, select a communication system in the **Communication System** field in the navigation tree.

   The default selection for the **Communication System** field is the selection of the global settings in the system menu.
4) To find and select a particular OpenScape SBC use one of the following options:

   - In the Work Area select the checkbox to the left of the particular SBC in the list and select **Manage**.
   - Choose a SBC from the **OpenScape SBC** pull-down located in the Navigation Tree.

   General dialogue is presented in the Work Area displaying information and data for the selected SBC.
5) Navigate to **Configuration** > **VoIP** in the navigation tree under **Administration**

   The **Voice over IP** window appears with the **General** tab selected by default.

6) Click the **Port Mapping Show...** button in the **Port mapping** field area, to display registered subscribers.

   The **Registered Subscribers Port Mapping** window appears displaying the settings in a list. The following data of all subscribers of the selected SBC or branch office is displayed:

   - **Contact**: Contact information of the subscriber.
   - **External IP**: External IP Address of the subscriber.
   - **External port**: External port number of the subscriber.
   - **SBC Access IP**: Address phones use to communicate with the SBC.
   - **SBC Core Port**: Listening port for the SBC.
   - **Expire time from Server**: Amount of time for the for expiry for the subscriber.
   - **Map time**: Amount of time the subscriber registration has been active.

   One or more subscriber registrations can then be cleared.

7) To clear a subscriber registration; Check one or more subscriber checkboxes in the **Registered Subscribers Port Mapping window**.
8) Click the **Clear** button to clear the subscriber registration. The subscriber will then re-register if active.
9) Click the **Close** button to go back to the **Voice over IP** window.

4.7.1.3 How to Display Backup Port Mapping Settings

Perform the following steps to display a list of port mapping for Backup Ports.

Prerequisites

Adequate administrative permissions.

At least one SBC is configured and in operation.

The connection to the OpenScape Voice system is up.

Step by Step

1) Navigate to **Configuration** tab > **OpenScape SBC** within the Navigation Bar in the Common Management Platform.
2) Select the **OpenScape SBC list** in the Navigation Tree under **Administration**.

   The system presents the **OpenScape SBC Overview** in the Work Area with a current list of all SBCs.

3) To view a list of SBCs configured at a specific communication system, select a communication system in the **Communication System** field in the navigation tree.

   The default selection for the **Communication System** field is the selection of the global settings in the system menu.

4) To find and select a particular OpenScape SBC use one of the following options:

   - In the Work Area select the checkbox to the left of the particular SBC in the list and select **Manage**.
   - Choose a SBC from the **OpenScape SBC** pull-down located in the Navigation Tree.

   General dialogue is presented in the Work Area displaying information and data for the selected SBC.

5) Navigate to **Configuration** > **VoIP** in the navigation tree under **Administration**

   The **Voice over IP** window appears with the **General** tab selected by default.

6) Click the **Backup Port Mapping Show...** button in the **Port mapping** field area to display registered subscriber information for the associated Geo-separated OpenScape SBC.

   The **Backup Port Mapping** window appears displaying the settings in a list for the associated Geo-separated OpenScape SBC. The following data of all subscribers of the selected SBC is displayed:

   - **Contact**: Contact information of the subscriber.
   - **External IP**: External IP Address of the subscriber.
   - **External port**: External port number of the subscriber.
   - **SBC Access IP**: Address phones use to communicate with the SBC.
   - **SBC Core Port**: Listening port for the SBC.
   - **Expire time from Server**: Amount of time for the for expiry for the subscriber.
   - **Map time**: Amount of time the subscriber registration has been active.

   One or more subscriber registrations can then be cleared.

7) Click the **Close** button to go back to the **Voice over IP** window.

4.7.2 Configuration of Remote Endpoints and SIP Service Providers - Overview

The OpenScape Session Border Controller (SBC) supports interface to SIP Service Providers and Remote Endpoints e.g., OpenScape branches. Configuration of these Remote Endpoints and SIP Service Providers is required.

The following issues appear for Remote Endpoints:

- In the OpenScape Voice system the endpoint must be configured with an IP-address or FQDN (Fully Qualified Domain Name).
- Firewall settings can be configured if required.
- Emergency Services such as LIN (Line Identification Number), Emergency number and Callback number can be configured.
- A Black List and White List of blocked or allowed addresses can be configured.
- Configuration of endpoint Domain information and Media anchoring.

The following issues appear for SIP Service Providers:

- In the OpenScape Voice system a service provider profile must be configured.

- Configuration of Privacy support.
- Indication of Registration requirements. Will the OpenScape SBC be responsible for performing registration.
- Protocol settings, options and flag for exchange of information between OpenScape SBC and the Service Provider.
- TLS Certificates configuration

The following table shows an example for the configuration of remote endpoints of an OpenScape SBC:

Ro	Name	Type	Profile	IP Address / FQDN	Routing Prefix	Number of active sessions	Message rate threshold
1	proxy-0-20	Proxy	Default Proxy	10.234.0.20		0	20000
2	Vrzn-Public	SSP	Vrz-US	10.234.20.2		0	20000
3	HG3500	Gate way	Gate way	10.191.2.23		0	20000
4	ms-prxy-0-22	Media Server		10.180.2.2		0	20000
5	b-sbc-20-2	Branch SBC	Default SBC	10.234.20.2		0	20000

The following table describes the function of each configured endpoints (row by row) for the above example table:

Row	Description
1	Type = Proxy: Is used to specify addressing when the OpenScape SBC is connected to an OpenScape Branch configured in Proxy mode.
2	Type = SSP: Is used to specify addressing when the OpenScape SBC is connected to a SIP Service Provider.
3	Type = Gateway: Is used to specify addressing when the OpenScape SBC is connected to a gateway via a proxy or directly connected.
4	**Currently Not Supported:** Type = Branch SBC: Is used to specify addressing when the OpenScape SBC is connected to an OpenScape Branch configured in Branch SBC mode.
5	**Currently Not Supported:** Type = Media Server SBC: Is used to specify addressing when the OpenScape SBC is connected to an OpenScape Branch configured an integrated media server.

Reference information on the Routing Prefix parameter

When the Dial Number matches the user part of Request-URI, the corresponding gateway will be connected. Regular expressions may be used for matching. The most important regular expression patterns are the following:

- % - matches any string of zero or more characters - If you want to match a Prefix, you should always end the pattern with %. One situation where % would not be used is when you want to match specifically one number.

- _ - matches any single character
- [<list-of-characters>] - matches a single character that is contained within the brackets.
- + - denotes repetition of the previous item one or more times
- * - denotes repetition of the previous item zero or more times
- | - denotes alternation (either of two alternatives).

NOTICE: The Regular Expressions available do not necessarily comply with POSIX Regular Expression rules. Nevertheless, POSIX Regular Expressions are a good reference to build matching patterns according to your needs.

---

[09]% - A number starting with 0 or 9 and followed by any other digits.

[0][3-6][18]% - A number that starts with 0, followed by one digit in the range 3-6 followed by a digit 1 or 8 and followed by any other digits.

%[5][5][5]% - Any number that has a sequence of 555 within it.

SIP Service Provider Profiles

SIP Service Providers can be displayed and configured. A SIP Service Provider is identified by information fields such as **Name** and **Default Home DN**. Among others.

Additional configuration can be applied to a profile such as SIP Service Address use, Registration Interval, Business Identity, Digest Authentication and SIP manipulation functions.

The following flags can be assigned to a profile:

- **FQDN to header SSP:** - If assigned, the FQDN header field will be sent to the SIP Service Provider. This attribute is only valid if the entry in the SIP Service Provider's Profile is configured with FQDN.
- **Spare Flag 1-10** - To be used for future Service Provider support.

Remote Endpoint TLS Modes for SIP Service Providers

OpenScape SBC supports the connection of remote endpoints via TLS.

It is possible to configure a specific certificate for a remote endpoint. By default, the remote endpoint will use the system wide certificates.

Therefore, it is possible to restrict the transport type to TLS only since the transport type is being defined by the remote endpoints. For security reasons, configuration can restrict the remote endpoint access to the OS SBC via TLS.

- **SIP over TLS**

  The RFC3261 deprecated the use of “transport=tls” and recommends the use of SIPS scheme.

  SIPconnect 1.1 recommends that the use of TLS is based on configuration:

  – Registration mode – if the registration is performed through a TLS connection, SIP SP shall conclude that the transport type shall be TLS.
  – Static mode – both sides shall be configured to use transport type TLS.

  It also recommends that a SIP-PBX accepts the parameter “transport=tls” but does not send it.However the use of “transport=tls” is adopted by the market.

  OpenScape Branch / OpenScape SBC support the following approaches:

  – **Transport=TLS**

    When performing the registration on the SIP SP, the Request URI and Contact header shall indicate transport=tls.

    By passing other SIP requests to the SIP SP, OSB / OS SBC shall add a Record-Route and a Via header with transport=tls.

    When interworking two different transport types, OSB / OS SBC shall add 2 Record-Routes being one for each transport type as defined in the RFC5658.

    SIPS URIs will not be accepted in this case. On receipt of a request with the Request-URI or the next route element containing a SIPS URI OSB / OS SBC will return a 416 (Unsupported URI scheme). SIPS URIs in other SIP headers shall be handled as SIP URI.

  – **Endpoint Config**

    Uses the remote endpoint configuration to determine the transport and does not use "transport=tls" nor SIPS URI in the SIP Message.

    SIPConnect V1.1 [1] states the following:

    The SIP-PBX and SP-SSE MUST support Transport Layer Security (TLS) v1.0 as described in [RFC 2246] and [RFC 3261]. While SIPconnect 1.1 continues to require TLS support at MUST strength, it should be noted that using TLS for signaling does not require the use of the SIPS URI scheme.

    [RFC 3261] deprecates the "transport=TLS" URI parameter. SIP-PBXes and SP-SSEs MUST ignore this parameter.

    When using TLS (as a result of being configured to require use of TLS, or as a result of discovering the availability of TLS from DNS), the SIP-PBX MUST establish a TLS connection (if not already established) prior to registration and MUST use that connection to deliver the REGISTER request and all subsequent SIP messages to the SP-SSE. The SP-SSE MUST authenticate the SIP-PBX using SIP digest authentication, and reject the REGISTER request if authentication fails. Following successful registration, the SP-SSE MUST use a TLS connection that is

authenticated as a connection to this SIP-PBX to deliver all SIP requests to the SIP-PBX.

If the registration is performed through a TLS connection, SIP SP shall conclude that the transport type shall be TLS.

Every SIP message sent to the Remote Endpoint is checked to determine if a TLS connection is established. If so, the SIP message shall be sent on TLS. If a TLS connection is not established and transport type to this SIP SP is configured as TLS or MTLS, OSB / OS SBC shall establish a TLS /MTLS connection.

The indication transport=tls shall not be sent.

No SIPS URI shall be used. As specified in the SIPconnect spec, SIP requests with Request URI with SIPS shall be rejected with a 416 (Unsupported URI scheme) response. Other headers with a SIPS URI shall be handled as if they were a SIP URI.

– **SIPS Scheme**

  When performing the registration, no SIPS URI shall be used in Request-URI, in the To header and in the Contact header. The Remote Endpoint shall conclude that the transport type is TLS because the registration has been performed on a TLS connection.

  On non-REGISTER requests towards the Remote Endpoint, a Record-Route header with SIPS URI shall be added by OSB / OS SBC.

  When interworking two different transport types, OSB / OS SBC shall add 2 Record-Routes being one for each transport type as defined in the RFC5658.

– **Pass-thru**

  The parameter transport=tls is sent to indicate TLS protocol. SIPS in the SIP Message will not be sent. SIPS will be accepted and passed through.

4.7.2.1 How to Configure Remote Endpoints - General

Proceed as follows to add a remote endpoint to the Voice over IP Remote Endpoints list. Endpoints include SIP Service Providers (SSP), OpenScape Branches and Gateways.

Prerequisites

Adequate administrative permissions.

At least one OpenScape SBC is configured and in operation.

The connection to the OpenScape Voice system is up.

Step by Step

1) Navigate to **Configuration** tab > **OpenScape SBC** within the Navigation Bar in the Common Management Platform.

2) Select the **OpenScape SBC list** in the Navigation Tree under **Administration**.

The system presents the **OpenScape SBC Overview** in the Work Area with a current list of all SBCs.

3) To view a list of SBCs configured at a specific communication system, select a communication system in the **Communication System** field in the navigation tree.

   The default selection for the **Communication System** field is the selection of the global settings in the system menu.

4) To find and select a particular OpenScape SBC use one of the following options:

   - In the Work Area select the checkbox to the left of the particular SBC in the list and select **Manage**.
   - Choose a SBC from the **OpenScape SBC** pull-down located in the Navigation Tree.

   General dialogue is presented in the Work Area displaying information and data for the selected SBC.

5) Navigate to **Configuration** > **VoIP** in the navigation tree under **Administration**

   The **Voice over IP** window appears with the **General** tab selected by default.

6) Click the **Enable** field in the **Remote Endpoints** field area.

   The **Remote Endpoints...** button becomes active.

7) Enter the DNS refresh interval time (minutes) in the **DNS Refresh Interval** field in the **Remote Endpoints** field area. This timing is used only for gateways/trunks configured using FQDNs.

8) Checkmark the **Allow Register from SERVER** checkbox, if the remote endpoint is allowed registration via the server.

9) Click the **Remote Endpoints...** button in the **Remote Endpoints** field area.

   The **Remote Endpoints** window appears displaying the endpoints configured for the OpenScape SBC selected.

   The following information is displayed:

   - **Name** - of the remote endpoint
   - **Type** - of endpoint e.g., Proxy, BranchSBC
   - **Profile** - assigned to the endpoint
   - **IP Address/FQDN/DNS SRV/Logical Branch Office ID** - static or dynamic IP address, DNS SRV, FDQN or Logical Branch Office ID

     NOTICE: "D" in the **IP Address/FQDN** is field next to the IP address indicates Dynamic IP address.

   - **Routing Prefix**
   - **Message rate threshold** - for the endpoint

10) Click the **Add...** button.

    The **Add Remote Endpoints** window appears the General tab displayed.

    NOTICE: For editing a remote endpoint click the **Edit** button. The **Edit Remote Endpoint** window will be displayed. Refer to the Add Remote Endpoint steps for associated information.

11) Enter the endpoints Name in the **Name** field in the Settings area.

12) Select the Network ID from the **Network ID** field list, to provide a default access IP association to the Remote Endpoint.

    The location of the Remote Endpoint is also identified dynamically based on the access IP which its communicating to, however if a message is not received from the Remote Endpoint, then the assigned access IP is used to reach the Remote Endpoint. Any changes in Remote Endpoint to access IP association based on the actual IP used by Remote Endpoint is not reflected in the configuration.

13) Select a particular type of endpoint in the **Type** selection list in the Settings area. Endpoint types area as follows:

    - **SSP** (SIP Service Provider)
    - **Branch SBC**
    - **Proxy**
    - **Gateway**
    - **Media Server**

14) Select the specific SIP Service Profile in the **Profile** selection list in the Settings area. This end user assigned profile name is the one assigned in Section How to Configure OpenScape SBC SIP Service Provider Profiles. The end user assigned profile name(s) appears in the SIP Service Profile in the Profile Selection List. This field is enabled when configuring a **SSP** (SIP Service Provider) endpoint. When configuring other endpoint types the profile is set to the associated default profile values e.g. **Default SBC**, **Default proxy**, **Gateway**.

    When configuring a Media Server endpoint pre-configure the MSprofile (media server profile) prior to configuring the endpoint.

15) Select the signaling address type in the **Signaling Address Type** selection list in the Remote Location Information area. Signaling Address types area as follows:

    - **IP Address or FQDN**
    - **DNS SRV**
    - **Dynamic IP**

    NOTICE: Dynamic IP requires the Remote Endpoint **Type** = **Branch SBC**.

16) Click the **Remote Location Configure button** in the **Remote Location Information** work area, to Add, Edit or Delete remote location configurations.

    a) Click the **Add** button to add a remote location configuration

    b) Enter the endpoint‘s IP address (IPv4 or IPv6) or FQDN in the **IP Address / FQDN/DNS SRV/Logical Branch Office ID** field under Remote Location Information. The Logical Branch Office ID is supported when the Signaling Type = Dynamic IP.

    NOTICE: The Logical Branch Office ID is used to identify the branch endpoint and is associated with the dynamic IP address. The field supports entry of a character string of maximum length 128 characters. The Logical Branch ID must be unique within the OpenScape SBC. The Logical Branch ID must match the name assigned to the Branch in the CMP.

c) Enter the endpoint‘s SIP/MGCP port information e.g., 5061 for TLS and 5060 for TCP and UDP, in the **Remote port** field.

d) Select a particular transport protocol to be used in communication with the endpoint (Remote port) in the **Transport** selection list, under **Remote Location Information**. Possible values are TCP. UDP, TLS.

e) Select the media security under the **Media protocol** selection list.

- **Pass-Thru** (default) – If both originating and terminating side support the SRTP encryption mechanism then SRTP media is setup end to end in pass-thru mode and OS-SBC is not involved in the SRTP encryption and decryption. SRTP Key coming in from the originating device is being passed as is to the terminating device in addition to the RTP and the other SRTP key giving the option to the terminating side to choose the SRTP/RTP mechanism based on its configuration. For example, if the originating side sends SDES only offer then the terminating side would get RTP, SRTP (Mikey) and SRTP (SDES from the originating side. This allows for additional flexibility in terms of setting up the call. If both parties support the same SRTP mechanism then SRTP media is setup end to end in pass-thru mode and OS-SBC is not involved in the SRTP encryption and decryption.
- **SRTP +RTP** - Terminating network is enforced with the configured SRTP Mikey or SDES best effort offer. If the Terminating side in OS-SBC is configured with SDES and the originating sides send SDES offer then the SDES is negotiated end to end. However, if the originating side offers Mikey and the terminating side in OS-SBC is configured for SDES then Mikey to SDES RTP is performed.
- **RTP**

f) Select the security key exchange method in the **Key Exchange Method** selection list. Values: **SDES**, **MIKEY**, **None**.

NOTICE: If the Media Protocol is RTP or Pass-Thru no selection is possible. The entry provided shall be **None**.

---

g) Checkmark the **Mark SRTP call leg as secure** checkbox, if the call requires secure media. When active, this parameter identifies the network as secure if TLS and SRTP are not used, i.e., TCP or UDP for the signaling transport or RTP is used for the media protocol. The indication does not apply to SIP-Q endpoints since security is managed end-to-end.

h) Checkmark the **Single m-line SRTP** checkbox, if the remote endpoint uses single m-line or dual m-line when the Media Protocol is configured as STRP +RTP. If unchecked a dual m-line is to be used.

The following table shows the possible combinations between Media Protocol, Media Security Key Negotiation and the single m-line parameters for a remote endpoint with SSP type Lync Mediation Server:

Media Protocol (Media security)	Media Security Key	Single m-line checkbox	Description
SRTP + RTP	SDES	Checked (default)	OS SBC offers and accepts RTP and SRTP in a single m-line SDES offer/ answer. OS SBC also accepts SRTP only offers.
		Unchecked	OS SBC offers and accepts RTP and SRTP in a dual m-line SDES offer/ answer. OS SBC also accepts SRTP only offers.
RTP	None	Disabled and Unchecked	OS SBC offers and accepts only RTP

i) Select the Certificate profile from the **Certificate profile** field list. The certificate profile contains TLS certificates (CA File, Certification File and Certification Key) for the connection.

j) Select the TLS mode profile from the **TLS mode** field list. Values: **Server authentication**, **Mutual authentication**, **Client mode only**. Client mode prevents the establishment of a TLS connection with the remote endpoint as a client and is only valid if the transport type is configured as TLS.

k) Checkmark the **TLS keep-alive** checkbox, to enable the keep-alive mechanism if the connection was established by the OpenScape Branch or OpenScape SBC as TLS client.

l) Enter the TLS keep-alive interval in the **Keep-alive interval**: field to specify the interval between sending the keep-alive requests. Range 60 – 3600 seconds. Default is 120 seconds.

m) Enter the TLS keep-alive timeout in the **Keep-alive timeout**: field to specify how long the TLS client shall wait for the keep-alive response before considering the TLS connection to be broken. Range 5 – 120 seconds. Default is 10 seconds.

n) Click the **OK** button to close the **Add Remote Location** dialog.

The **Add Remote Location** dialog dis appears and a new row is created in the **Remote Locations** table. The changes are stored temporarily.

o) Click the **OK** button to go back to the **Add Remote Endpoints** window, **General Tab**.

17) Click the **Media Realm Configure button** in the **Remote Location Information** work area, to Add, Edit or Delete media realm configurations.

a) Click the **Add** button to add a,media realm configuration

b) Enter the Subnet IP Address (IPv4 or IPv6), in the **Subnet IP Address** field.

Not applicable if the **Remote Location Information**, **Signaling Address Type** = **Dynamic IP**.

c) Enter the Subnet mask address (IPv4 or IPv6 - must align with the **Subnet IP Address** parameter), in the **Subnet mask** field e.g., 255.255.255.0.

Not applicable if the **Remote Location Information**, **Signaling Address Type** = **Dynamic IP**.

d) Select a particular type of media anchoring **Auto** or **Forced** in the **Anchoring Media** selection list, in the Location Domain work area. Does not apply to Dynamic IP addresses.

e) Click the **OK** button to close the **Add Media Realm** dialog.

The **Add Media Realm** dialog disappears and a new row is created in the **Media Realm** table. The changes are stored temporarily.

f) Click the **OK** button to go back to the **Add Remote Endpoints** window, **General Tab**.

18) To configure **Remote Location Information and Routing**

a) Enter the Core location domain name, in the **Core location domain name** field, under Remote Location Identification / Routing work area.

b) Enter the Core Side IP Address (IPv4 or IPv6) or FQDN associated with the internal data center side of the network, in the **Core Side IP Address / FQDN**: field, under Remote Location Identification / Routing work area.

c) Enter the routing prefix in the **Routing Prefix**: field. This parameter defines a valid Dial Number to be used in search for the endpoint/ service provider. The match is done on outgoing calls only and the best match is always used.

d) Enter the Core Side Port e.g., 50001, in the **Core Side Port**: field, under Remote Location Identification.

e) Enter the Core Side TLS Port e.g., 51001, in the **Core Side TLS Port**: field, under Remote Location Identification.

19) To configure **Firewall Settings**

a) Click the **Enable** field in the **Firewall Settings** field area.

Additional configuration for firewall setting becomes active.

b) Enter the Message rate threshold for the firewall in the **Message rate threshold**: field, under Firewall Settings. Default: 20,000.

c) Click allowed types of transport for the firewall in the **Firewall Settings** field area. Transport types are **SIP UDP**, **SIP TCP**, **SIP TLS**, **MGCP** and **DNS**.

d) Click the Black List or White List **Configure...** button to configure firewall screening.

The **Black List** (blocking list) or **White List** (allowed list) dialog appears displaying a list of blocked or allowed addresses and associated ports.

e) Click the **Add...** button.

The **Add Black List** or **Add White List** dialog appears.

f) Enter the IP address (IPv4 or IPv6), Subnet or Logical Branch Office ID to be blocked or allowed in the **IP address/Subnet/Logical Branch Office ID**: field.

The Logical Branch Office ID is supported for endpoints configured for Dynamic IP.

g) Enter the port number to be blocked or allowed in the **Port**: field.

h) Click the **OK** button to close the **Add Black List** or **Add White List** dialog.

The **Add Black List** or **Add White List** window disappears and a new row is created in the Black List or White List table. The changes are stored temporarily.

i) Click the **OK** button to go back to the **Add Remote Endpoints** window.

20) Click the **OK** button to store the changes temporarily in the administrator´s login session.

The **Add remote Endpoints** dialog disappears and the **Remote Endpoints** window appears.

21) Click the **OK** button to store the changes temporarily in the administrator´s login session.

The **Remote Endpoints** dialog disappears and the **Voice over IP** window appears.

22) Click the **OK** button to store the changes temporarily in the administrator´s login session.

The **Voice over IP** dialog disappears and the **General endpoint** windows appears.

23) Click the **Apply changes** button in the main window, work area.

The configuration of the endpoint or service provider is applied on the OpenScape SBC.

4.7.2.2 How to Configure Remote Endpoints - Emergency Services

Proceed as follows to add a remote endpoint emergency number and emergency calling routing information to the Voice over IP Remote Endpoint.

Prerequisites

Adequate administrative permissions.

Endpoint general information located on the **General** tab must be configured prior to configuration of the emergency services.

At least one OpenScape SBC is configured and in operation.

The connection to the OpenScape Voice system is up.

Step by Step

1) Navigate to **Configuration** tab > **OpenScape SBC** within the Navigation Bar in the Common Management Platform.

2) Select the **OpenScape SBC list** in the Navigation Tree under **Administration**.

The system presents the **OpenScape SBC Overview** in the Work Area with a current list of all SBCs.

3) To view a list of SBCs configured at a specific communication system, select a communication system in the **Communication System** field in the navigation tree.

The default selection for the **Communication System** field is the selection of the global settings in the system menu.

4) To find and select a particular OpenScape SBC use one of the following options:

- In the Work Area select the checkbox to the left of the particular SBC in the list and select **Manage**.
- Choose a SBC from the **OpenScape SBC** pull-down located in the Navigation Tree.

General dialogue is presented in the Work Area displaying information and data for the selected SBC.

5) Navigate to **Configuration** > **VoIP** in the navigation tree under **Administration**

The **Voice over IP** window appears with the **General** tab selected by default.

6) Click the **Enable** field in the **Remote Endpoints** field area.

The **Remote Endpoints...** button becomes active.

7) Click the **Remote Endpoints...** button in the **Remote Endpoints** field area.

The **Remote Endpoints** window appears displaying the endpoints configured for the OpenScape SBC selected.

8) Click the **Add...** button. Or select an existing endpoint to edit.

The **Add Remote Endpoints** window appears the General tab displayed.

9) Click the **Emergency Calling** tab.

The **Emergency Calling** window appears displaying the **Emergency calling subnets** list.

10) Click the **Add...** button.

    The **Add emergency calling** window appears the General tab displayed.

11) Enter the calling party endpoints IP address (IPv4 or IPv6)(or range of IP addresses) of the subscriber(s) in the **IP Address/Logical Branch Office ID** field. The field supports entry of a character string of maximum length 128 characters.

    The Logical Branch Office ID is supported when the Signaling Type = Dynamic IP.

12) Enter the IP subnet (IPv4 or IPv6 - must align with the **IP Address** parameter) of the range of subscribers defined by the IP address configuration in the **Subnet mask** field. If a single subscriber is configured use mask 255.255.255.255.

    Default subnet: The entries IP=255.255.255.255 and Mask=255.255.255.254 create a Default Subnet, which will be used for all phones not comprised in any subnet. The usage of Routing Prefix is exactly like normal subnets.

13) Select a routing prefix, if applicable, from the **Routing Prefix** selection list e.g., 911999. If not applicable select None.

14) Click the **Send LIN instead of CPN** field. This option is used to avoid the adding of the CPN (Calling Party Number) in MIME (Multipurpose Internet Mail Extensions) and use the LIN (Location Identification Number) instead. Use this option if the Gateway does not accept the emergency calls using MIME.

15) Click the **LIN** tab.

    The **LIN** window appears displaying the **LIN** list.

16) Click the **Add...** button.

    The **Add LIN** window appears.

17) Enter the LIN (Location Identification Number) in the **LIN** field. The LIN is used to associate a subscriber with its physical location.

18) Click the **OK** button to close the **Add LIN List** dialog.

    The **Add LIN** window dis appears and a new row is created in the LIN List table. The changes are stored temporarily.

19) Click the **OK** button to go back to the **Add Remote Endpoints** window, **Emergency Calling** Tab.

20) Click the **Emergency Number** tab.

    The **Emergency Number** window appears displaying the **Emergency Number** list.

21) Enter the Emergency Number of the emergency center in the **Emergency Number** field.

22) Click the **Add** button.

    The Emergency Number is added to the **Emergency Number** list. If these numbers are dialed the OpenScape SBC or Branch identifies the number as an “Emergency Call” (for the USA this represents the 911 emergency calls). This will trigger the server to try to establish an outgoing call to an available gateway (highest priority).

23) Click the **OK** button to store the changes temporarily in the administrator´s login session.

    The **Emergency number** dialog disappears and the **Remote Endpoints** window appears.

24) Click the **OK** button to store the changes temporarily in the administrator´s login session.

    The **Remote Endpoints** dialog disappears and the **Voice over IP** window appears.

25) Click the **OK** button to store the changes temporarily in the administrator´s login session.

    The **Voice over IP** dialog disappears and the **General endpoint** windows appears.

26) Click the **Apply changes** button in the main window, work area.

The configuration of the endpoint emergency services is applied on the OpenScape SBC.

4.7.2.3 How to Configure OpenScape SBC SIP Service Provider Profiles

Proceed as follows to configure SIP Service Provider Profiles. A SIP Service Profile must be created prior to configuring a SIP Service Provider (SSP).

Prerequisites

Adequate administrative permissions.

At least one OpenScape SBC is configured and in operation.

The connection to the OpenScape Voice system is up.

SIP Service Providers are allowed in WAN only.

Step by Step

1) Navigate to **Configuration** tab > **OpenScape SBC** within the Navigation Bar in the Common Management Platform.
2) Select the **OpenScape SBC list** in the Navigation Tree under **Administration**.

   The system presents the **OpenScape SBC Overview** in the Work Area with a current list of all SBCs.
3) To view a list of SBCs configured at a specific communication system, select a communication system in the **Communication System** field in the navigation tree.

   The default selection for the **Communication System** field is the selection of the global settings in the system menu.

4) To find and select a particular OpenScape SBC use one of the following options:

   - In the Work Area select the checkbox to the left of the particular SBC in the list and select **Manage**.
   - Choose a SBC from the **OpenScape SBC** pull-down located in the Navigation Tree.

   General dialogue is presented in the Work Area displaying information and data for the selected SBC.

5) Navigate to **Configuration** > **Features** in the navigation tree under **Administration**

   The **Features** window appears with the list of features under the **Features configuration** tab.

6) Select the **Enable** checkbox in the **Remote Endpoints** field area.

   The **SIP Service Provider Profiles...** button becomes active.

7) Click the **SIP Service Provider Profiles...** button in the **Remote Endpoints** field area.

   The SIP Service Provider Profiles window appears displaying the SIP Service Provider Profiles configured for the OpenScape Session Border Controller system in a list.

8) Click the **Add...** button.

   The **Add SIP Service Provider Profiles** window appears with the **Basic** tabsheet selected.

9) Enter the name of the SIP Service Provider in the **Name** field, in the **Information** area. (Value:1-20 characters).

10) Choose a Default SIP Service Provider Profile from the **Default SSP Profile:** field Pull-down, in the **Information** area. Possible values are (and will expand as needed):

    - AT&T Flex Reach
    - AT&T Flex Toll-Free
    - BT
    - COLT Telecom
    - DTAG/T-Systems (Sonus)
    - Level 3 Communications (Global Crossing)
    - Lync Mediation Server
    - Orange
    - Qwest
    - Skype-IP Auth
    - Telefonica
    - Vodaphone/Arcor
    - Verizon-EAME IP Trunking
    - Verizon-IPCC Trunking
    - Verizon-US IP Trunking
    - Sip Connect
    - DTAG/NGN Registration Mode

NOTICE: It is highly recommended to not disable/uncheck fields that are automatically set when a "Default SIP Service Provider Profile" is chosen.

---

11) Check the **Use SIP Service Address for all identity headers** checkbox, in the Use SIP Service Address field area, if the SIP service address is to be sent by the OpenScape SBC. If not checked, the IP Address of the OpenScape SBC is sent.

12) Enter the **SIP Service Address** to be used by the OpenScape SBC. This setting will be used by the system only if the **Use SIP Service Address for all identity headers** option is selected.

13) Check the **Required** checkbox, in the Registration required field area. The OpenScape SBC will send a registration request to the SIP Service Provider.

    If the **Signaling Address Type** is **DNS SRV** and a DNS SRV Service Signaling Address is provisioned, the registration is sent to the resolved SIP DNS SRV Service address since the Trunk FQDN does not apply.

    NOTICE: It is not recommended to disable/uncheck fields that are automatically set when a "Default SIP Service Provider" is chosen.

    ---

14) Enter the **Interval**, in the Registration required area (Value: 60-7200 seconds). This configures the interval in which the registration will be renewed. This setting will be used by the system only if the **Registration Required** option is selected.

15) Enable **Business Identity** support by checking the **Required** checkbox, in the Business Identity Required work area if required by the Service Provider (Supported in Version 2).

    For certain Service Providers (SP), Business users must establish a funded Service Providers account to be able to make or receive calls. Calls which traverse the Service Providers IP network that do not originate or terminate within the Service Providers network are charged against the account. All outgoing calls must include the identity of the Service Provider Business account in the From: header field and may include a Caller-ID the P-Asserted-Identity header field.

16) Enter the **Business Identity Number** (Directory Number) to be used by the OpenScape SBC (Supported in Version 2). (Value: string with 30 digits including optional + sign) This setting will be used by the system only if the **Required** option is selected.

17) Enable digest authentication support by checking the **Supported** checkbox, in the Digest Authentication supported field area (Supported in Version 2).

18) Enter the values for Digest Authentication **Realm**, **User ID** and **Password** if Digest Authentication support is available, in the **Digest Authentication supported** work area (Values: Realm: 0-128 characters, User ID: 6-64 characters, Password: 6-20 characters) (Supported in Version 2).

    - Realm - Protection domain for authentication, is configured as a hostname or domain name or IP Address (IPv4 or IPv6).
    - User ID - Username required for an authenticated registration.
    - Password - required for an authenticated registration.

    By providing a User ID and a Password which match with a corresponding account on the SIP registrar, the phone authenticates itself. Optionally, a Realm can be added. This parameter specifies the protection domain wherein the SIP authentication is meaningful. The protection domain

is globally unique, so that each protection domain has its own arbitrary usernames and passwords.

If Digest Authentication fails, an alarm shall be generated.

19) Select the **Options** tab.

The **Options** tab window is displayed.

20) Choose a TLS signaling mode from the **TLS signaling:** field Pull-down, in the **TLS Certificate** work area. Possible values are:

- Transport=TLS
- Pass-thru (default)
- Endpoint Config
- SIPS Scheme

NOTICE: Refer to the chapter on "Configuration of Remote Endpoints and SIP Service Providers - Overview" for detailed descriptions of TLS modes.

---

21) Select the **Flags** tab.

The **Flags** tab window is displayed.

22) Select flags for the Service Provider Profile by checking the checkboxes in the **Flags** area.

NOTICE: Please refer to SIP Service Provider on page 345 to see the description of the respective flags.

---

23) Select the **SIP manipulation** tab to configure SIP Manipulation rules.

The **SIP manipulation** tab window appears. The rules are displayed in a list.

24) Check the **Insert Anonymous Caller-ID for blocked Caller-ID** checkbox, in the SIP manipulation work area, if the Service Provider requires that the blocked callers_ID be identified in the P-Asserted-Identity header field URI.

25) To configure the rules, the following options appear:

- Select an entry from the list and click the **Delete** button to remove an entry from the list.
- Select an entry from the list and click the **Edit...** button to edit the entry.
- Click the **Add** button to add a new rule to the list.

The **Add VoIP SIP Manipulation** window appears.

26) Enter the rule for the match digits in the **Match digits** field. This parameter defines the matching digits. Only numerical digits or the character "+" are supported.

27) Enter the rule for the match position in the **Match Position** field. This parameter defines from which digit position the matching is performed on the header. The first position is 0.

28) Enter the rule for the match length in the **Match Length** field (format x, x/, or x/y).

29) Select the SIP header the rule applies for in the **Header** selection list. Options are as follows:
    - **R-URI**
    - **From**
    - **P-Asserted Identity**
    - **P-Preferred identity**
    - **Diversion**
30) Enter the delete/insert position in the **Delete/insert position** field. This parameter defines from which digit position on the header the fields "Number of digits to delete" and "Insert digits at position" are applied. If the value of this parameter does not correspond to an effective position on the header digits, the related operations will be ignored. The first position is "0".
31) Enter the number of digits to be deleted from the defined position in the **Number of digits to delete** field. If there are not enough digits to be deleted from the defined position on the header, this operation will be ignored.
32) Enter the digits to be inserted at the defined position in the **Insert digits** field.
33) Enter the prefix to be added to the digits on the header in the **Add prefix** field.
34) Enter the digits to replace all header digits with in the **Replace all with** field.
35) Select the Call Type that digit manipulation applies for in the **Call Type** selection list. Options are as follows:
    - **SIP-Provider**
36) Click the **OK** button to store the changes temporarily.

    The **SIP Manipulation** window appears and the SIP Manipulation list is updated with the new entry.
37) Click the **OK** button.

    The **SIP Service Provider Profiles** window dis appears and a new row is created in the SIP Service Provider Profiles table. The changes are stored temporarily.
38) Click the **OK** button to go back to the **Voice over IP** dialog.
39) Click the **OK** button to return to the OpenScape Branch General work area window.

    The **Voice over IP** dialog disappears.
40) Click the **Apply changes** button in the General - main window, work area.

The configuration of SIP Service Provider Profile is created for use when configuring a SIP Service Provider on the OpenScape SBC.

4.7.3 Media Server Profile Configuration — Overview

The OpenScape Session Border Controller supports Media Server Adapter used for NAT traversal of MGCP (Media Gateway Control Protocol) communication between the local media server and the Call Agent. To provide this capability a media server type remote endpoint with an associated Media Server Profile must be created. OpenScape Session Border Controller does

not support an integrated Media Server and therefore integrated Media Server configuration is not required.

4.7.3.1 How to Configure a Media Server Profile

The Media Server Profile is required prior to configuring a Media Server type remote endpoint. Proceed as follows to create a Media Server Profile.

Prerequisites

Adequate administrative permissions.

At least one OpenScape SBC is configured and in operation.

The connection to the OpenScape Voice system is up.

Step by Step

1) Navigate to **Configuration** tab > **OpenScape SBC** within the Navigation Bar in the Common Management Platform.

2) Select the **OpenScape SBC list** in the Navigation Tree under **Administration**.

The system presents the **OpenScape SBC Overview** in the Work Area with a current list of all SBCs.

3) To view a list of SBCs configured at a specific communication system, select a communication system in the **Communication System** field in the navigation tree.

The default selection for the **Communication System** field is the selection of the global settings in the system menu.

4) To find and select a particular OpenScape SBC use one of the following options:

- In the Work Area select the checkbox to the left of the particular SBC in the list and select **Manage**.
- Choose a SBC from the **OpenScape SBC** pull-down located in the Navigation Tree.

General dialogue is presented in the Work Area displaying information and data for the selected SBC.

5) Navigate to **Configuration** > **Diagnostics & Logs** > **On Demand Trace** in the navigation tree under **Administration**.

The **Diagnostics & logs** window appears with the **On Demand Trace** tab selected by default.

6) Navigate to **Configuration** > **VoIP** > **Media** in the navigation tree under Administration.

The **VOIP** window appears with the **Media** tab selected by default.

7) Check the **Enable** field in the **Remote Endpoints** field area to enable the Media Server Profiles functionality.

8) Click the **Ms Profiles...** button in the **General** field area, under **Remote Endpoints**.

The **Media Server Profiles** window appears displaying the profiles configured for the OpenScape SBC.

9) Click the **Add...** button.

   The **Add Media Server Profile** window appears.

10) Enter the name of the Media Server Profile in the **Name** field.

11) Enter the maximum duration of a MGCP transaction in SBC mode in seconds in the **Time to Live** field. Default value: 30 seconds.

12) Enter the maximum time a conference is allowed to be active in the **Maximum conference time** field. Default value: 18000 seconds.

13) Check the **Unlimited** field, disable a timed **Maximum conference time** and to enable unlimited conference time.

    Unlimited time is set and Maximum conference time value is removed.

14) Enter the maximum time a conference is allowed to be active in the **Maximum announcement time** field. Default value: 1800 seconds.

15) Check the **Unlimited** field, to disable timed **Maximum announcement time** and to enable unlimited announcement time.

    Unlimited time is set and Maximum announcement time value is removed.

16) Click the **OK** button.

    The **Add Media Server Profile** dialog disappears. The **Media Server Profiles dialog appears and displays the added profile**.

17) Click the **OK** button to store the changes temporarily in the administrator´s login session.

    The **Media Server Profiles** dialog disappears and returns to **General** window for the selected SBC in the work area.

18) Click the **Apply changes** button in the main window, in the work area, to save the changes permanently.

The settings are applied to the system.

4.7.3.2 How to Configure a Media Server Profile for earlier-than-v8 OpenScape SBC devices

The Media Server Profile is required prior to configuring a Media Server type remote endpoint. Proceed as follows to create a Media Server Profile.

Prerequisites

Adequate administrative permissions.

At least one OpenScape SBC is configured and in operation.

The connection to the OpenScape Voice system is up.

Step by Step

1) Navigate to **Configuration** tab > **OpenScape SBC** within the Navigation Bar in the Common Management Platform.

2) Select the **OpenScape SBC list** in the Navigation Tree under **Administration**.

   The system presents the **OpenScape SBC Overview** in the Work Area with a current list of all SBCs.

3) To view a list of SBCs configured at a specific communication system, select a communication system in the **Communication System** field in the navigation tree.

   The default selection for the **Communication System** field is the selection of the global settings in the system menu.

4) To find and select a particular OpenScape SBC use one of the following options:

   - In the Work Area select the checkbox to the left of the particular SBC in the list and select **Manage**.
   - Choose a SBC from the **OpenScape SBC** pull-down located in the Navigation Tree.

   General dialogue is presented in the Work Area displaying information and data for the selected SBC.

5) Navigate to **Configuration > VoIP** in the navigation tree under Administration.

   The **Voice over IP** window appears with the **General** tab selected by default.

6) Check the **Enable** field in the **Remote Endpoints** field area to enable the Media Server Profiles functionality.

7) Click the **Ms Profiles...** button in the **General** field area, under **Remote Endpoints**.

   The **Media Server Profiles** window appears displaying the profiles configured for the OpenScape SBC.

8) Click the **Add...** button.

   The **Add Media Server Profile** window appears.

9) Enter the name of the Media Server Profile in the **Name** field.

10) Enter the maximum duration of a MGCP transaction in SBC mode in seconds in the **Time to Live** field. Default value: 30 seconds.

11) Enter the maximum time a conference is allowed to be active in the **Maximum conference time** field. Default value: 18000 seconds.

12) Check the **Unlimited** field, disable a timed **Maximum conference time** and to enable unlimited conference time.

    Unlimited time is set and Maximum conference time value is removed.

13) Enter the maximum time a conference is allowed to be active in the **Maximum announcement time** field. Default value: 1800 seconds.

14) Check the **Unlimited** field, to disable timed **Maximum announcement time** and to enable unlimited announcement time.

    Unlimited time is set and Maximum announcement time value is removed.

15) Click the **OK** button.

    The **Add Media Server Profile** dialog disappears. The **Media Server Profiles dialog appears and displays the added profile**.

16) Click the **OK** button to store the changes temporarily in the administrator´s login session.

    The **Media Server Profiles** dialog disappears.

17) Click the **Apply changes** button in the main window, in the work area, to save the changes permanently.

The settings are applied to the system.

4.7.4 Quality of Service Configuration

QoS (Quality of Service) is the ability to guarantee a certain level of performance to the Voice over IP data flow in converged voice/data IP networks.

One common source of voice quality problems is data traffic peaks that consume too much of the available bandwidth, resulting in voice packet loss, or unacceptable packet delays. SIP (Session Initiation Protocol) telephones and many SIP gateways can be configured to support QoS mechanisms such as traffic segregation or traffic shaping. Therefore, compatible support with the network switches and routers is required.

4.7.4.1 How to Configure VoIP QoS Rules

Proceed as follows to display, delete, edit or add a Quality of Service rule in the Voice over IP settings for the OpenScape SBC and Branch system.

Prerequisites

Adequate administrative permissions.

At least one SBC is configured and in operation.

The connection to the OpenScape Voice system is up.

Step by Step

1) Navigate to **Configuration** tab > **OpenScape SBC** within the Navigation Bar in the Common Management Platform.

2) Select the **OpenScape SBC list** in the Navigation Tree under **Administration**.

The system presents the **OpenScape SBC Overview** in the Work Area with a current list of all SBCs.

3) To view a list of SBCs configured at a specific communication system, select a communication system in the **Communication System** field in the navigation tree.

The default selection for the **Communication System** field is the selection of the global settings in the system menu.

4) To find and select a particular OpenScape SBC use one of the following options:

- In the Work Area select the checkbox to the left of the particular SBC in the list and select **Manage**.
- Choose a SBC from the **OpenScape SBC** pull-down located in the Navigation Tree.

General dialogue is presented in the Work Area displaying information and data for the selected SBC.

5) Navigate to **Configuration** > **VoIP** in the navigation tree under **Administration**

   The **Voice over IP** window appears with the **General** tab selected by default.

6) Check the **Enable** field in the **QoS** field area to enable the QoS functionality.

7) Click the **Configure...** button in the **QoS** field area.

   The **VoIP QoS** window appears. The QoS rules are displayed in a list.

8) Enter a DSCP (Differentiated Services Codepoint) value for SIP signaling to be set in the IP packets for the QoS rule in the **DSCP for SIP** field (Value 1-63). If there are not enough digits to be deleted from the defined position on the header, this operation will be ignored.

9) Enter a DSCP (Differentiated Services Codepoint) value for RTP signaling to be set in the IP packets for the QoS rule in the **DSCP for RTP** field (Value 1-63). If there are not enough digits to be deleted from the defined position on the header, this operation will be ignored.

10) To configure the rules, the following options appear:

    - Select an entry from the list and click the **Delete** button to remove an entry from the list.
    - Select an entry from the list and click the **Edit..**. button to edit the entry.
    - Click the **Add** button to add a new rule to the list.

    The **Add VoIP QoS** window appears.

11) Select the protocol for the QoS rule in the **Protocol** selection list. Possible values: All, TCP (Transmission Control Protocol), UDP (User Datagram Protocol), ICMP (Internet Control Message Protocol).

12) Select the incoming interface for the QoS rule in the **In Interface** selection list. The possible values depend on the interfaces supported by the system (Possible values: all, Interface1, Interface2).

13) Select the outgoing interface for the QoS rule in the **Out Interface** selection list. The possible values depend on the interfaces supported by the system (Possible values: all, Interface1, Interface2).

14) Enter the port number for the QoS rule in the **Port** field.

15) Enter a DSCP (Differentiated Services Codepoint) value to be set in the IP packets for the QoS rule in the **DSCP** field. If there are not enough digits to be deleted from the defined position on the header, this operation will be ignored.

16) Enter a mark for the QoS rule in order to use with traffic shaping in the **Mark** field.

17) Click the **OK** button to store the settings temporarily.

    The **Add VoIP QoS** window disappears, a new line is displayed in the list in the **VoIP QoS** window.

18) Click the **OK** button to go back to the **Voice over IP** window.

19) Click the **OK** button to store the changes temporarily in the administrator´s login session.

    The **Voice over IP** dialog disappears.

20) Click the **Apply changes** button in the main window, work area.

The configuration of the QoS is applied on the OpenScape SBC.

4.7.5 Communication System Settings

The OpenScape SBC is connected to the OpenScape Voice communication system.

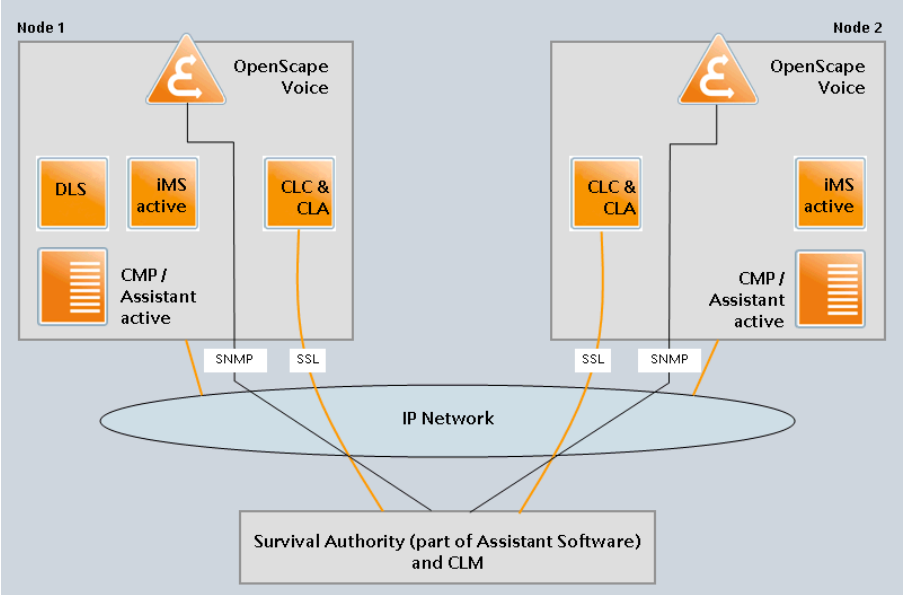
Redundancy

There are various options for deploying redundancy based on the customers network, location of data centers and number of data centers. The basic configurations for OpenScape Voice redundancy are:

- Single Node (Simplex)

  A nonredundant OpenScape Voice system running on a single server machine.
- Node redundancy (Duplex)

  Node 1 and node 2 built an OpenScape Voice communication system which can be co-located (in one location) or geo-separated (in different locations). Each node is the redundant backup for its partner.



- Geo-Separated redundancy

  Geographically-separated OpenScape SBC nodes.

OpenScape Session Border Controller Redundancy Support

Redundant OpenScape SBC configurations provide VIP address failover for both LAN network and WAN addresses.

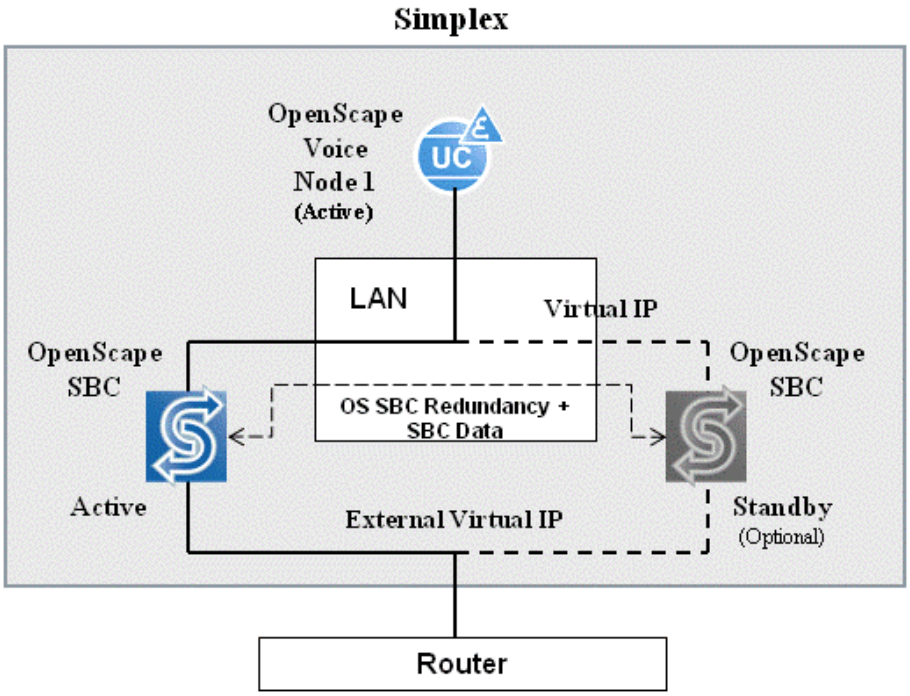
Periodic heartbeats are sent by the Standby OpenScape SBC node to detect failover conditions. Either OpenScape SBC node may assume active or standby mode at any time, however only one node shall be in an active operation mode.

When the redundant OpenScape SBC nodes share the same sub-net for the inside network additional data is synchronized in near real-time between the OpenScape SBC nodes to allow continued operation when the standby OpenScape SBC node must assume an active OpenScape SBC node status. The synchronization data includes for example:

- Configuration changes

- Media port mappings for sessions traversing the SBC.
- IP addresses and ports used for established TCP connections
- TLS session handles using TCP connections
- Updates to any current SIP registration bindings

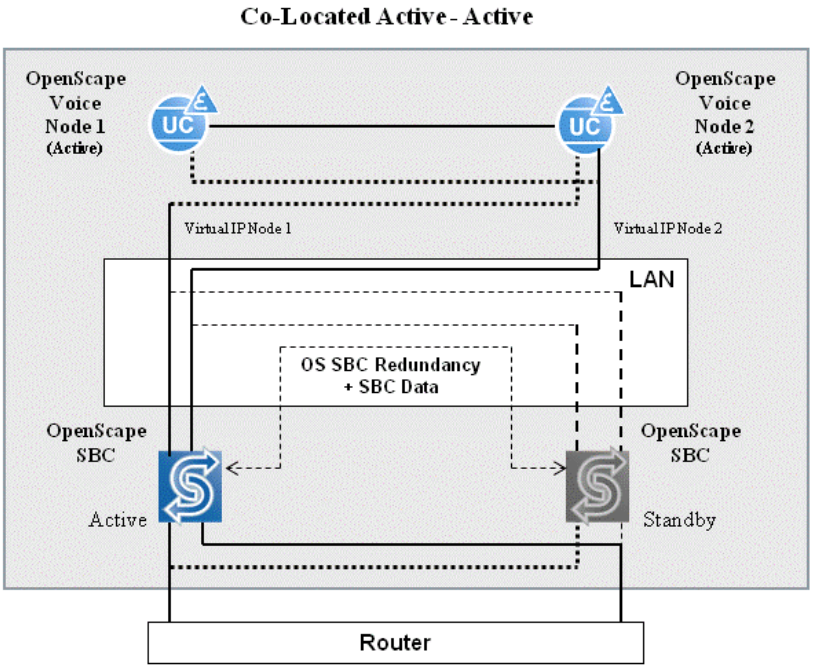
Simplex OpenScape Voice (OSV)



The OpenScape SBC does not require any special functionality to interface with a simplex OpenScape Voice (OSV). All SIP requests and responses are received at a single outside/ WAN interface of the OpenScape SBC and are relayed to a single OSV IP address. The OpenScape SBC is configured with Comm. System Type = Simplex.

An optional second OpenScape SBC can be used to provide a redundant SBC cluster if necessary although as OSV itself has no redundancy in this configuration.

Duplex co-located OpenScape Voice (OSV)



When OpeScape Voice (OSV) is operating in duplex mode, end devices communicate with both nodes of the duplex OSV configuration, requiring the OS SBC cluster support 2 Virtual IP (VIP) addresses, one for each OSV node. For each OSV, an SBC inside VIP address associated with an outside VIP address is needed. Endpoint devices must be configured with one of the outside network VIP's as their SIP Server / SIP Registrar, distributed to provide a balance OSV load.

SBC redundancy is only available in an active-standby mode.

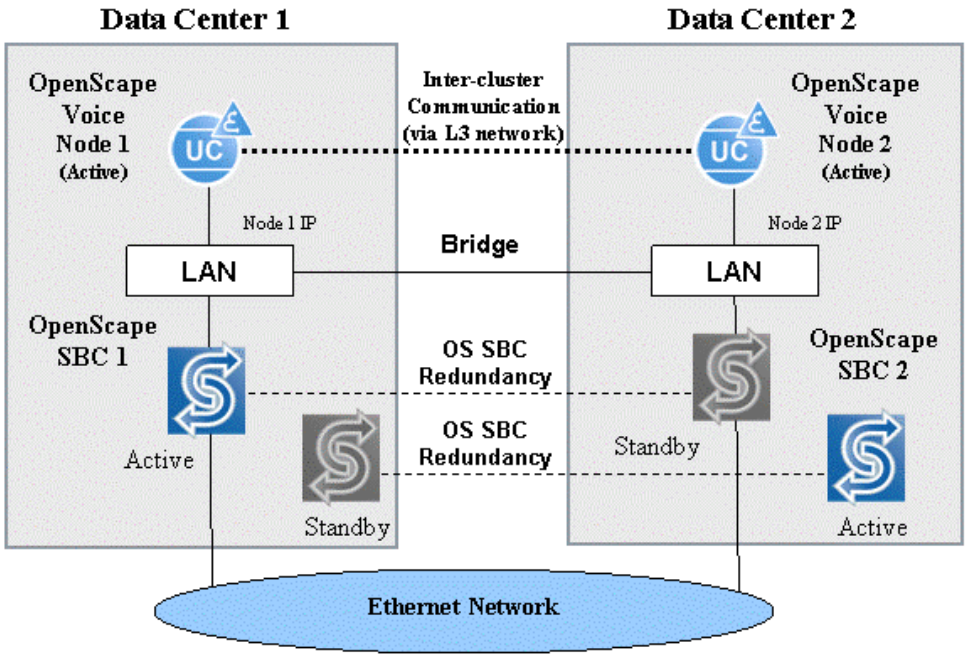
OS SBC node failover handling requires that both VIP address pairs (external and internal OSV bindings) are taken over or assumed by the OS SBC Standby Node.

In this non-geographically separated configuration, OSV failures are transparent to the OS SBC since an OSV node failure leads to the partner OSV node taking over the internal VIP address of the failed OSV node assuming both inside network VIP addresses.

In the Active-Active OSV configuration, the OS SBC is configured with Comm. System Type = Collocated.

OpenScape Voice (OSV) L3 Geographically Separated Redundancy

Redundancy across geographically-separated nodes is supported in OpenScape SBC version 2.



In addition to the OpenScape SBC redundancy on the same subnet for support of co-located OpenScape redundant nodes, this feature provides support for OpenScape Voice redundancy of geographically separated nodes that are on separate subnets. A Layer 3 (L3) connection is used to exchange call state information between the geographically separated OpenScape SBCs.

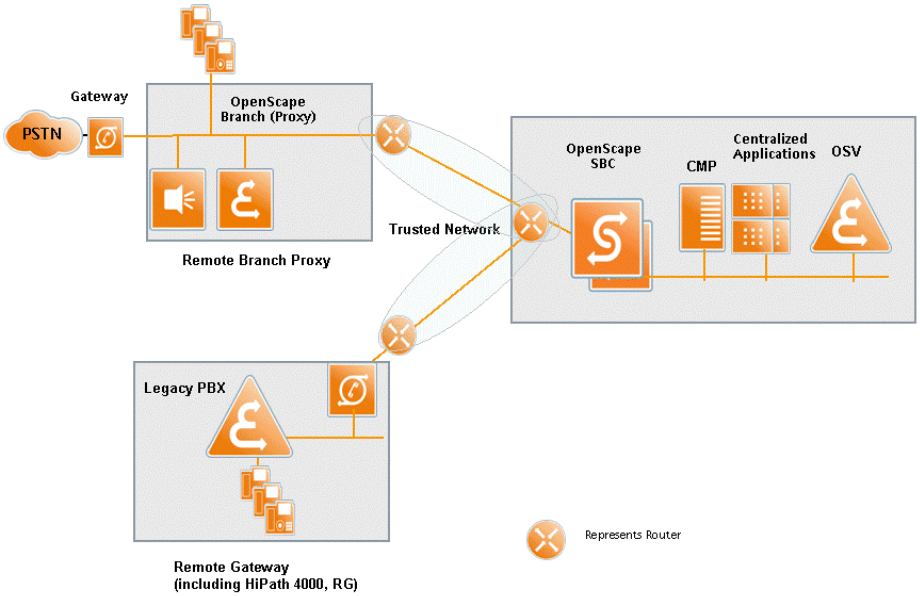
At least two OpenScape SBC servers (one at each data center) are required to support OpenScape Voice geographically separated redundancy. Four OpenScape SBC servers are required (two at each data center) in case server redundancy at each data center is also required.

Unlike OpenScape SBC redundancy on the same subnet where a common set of SBC Session Licenses can be shared between the Active and Standby servers, OpenScape SBCs that are L3 geographically separated are counted as separate systems for purposes of SBC Session Licenses. In other words, a separate set of SBC Session Licenses need to be used for the OpenScape SBC system that are geographically separated.

Trusted Addresses

The list of Voice over IP trusted addresses is used for installations of the OpenScape Voice communication system and shows trusted SIP Servers, from which requests can be accepted.

The figure below shows OpenScape SBC deployment in a trusted network with the SBC connected directly to the WAN. This deployment is possible where all VoIP users are within a trusted Enterprise Network.



4.7.5.1 How to Configure the Communication System for OpenScape SBC

Proceed as follows to display and configure the settings for the connected OpenScape Voice communication system.

Prerequisites

Adequate administrative permissions.

At least one OpenScape SBC is configured and in operation.

The connection to the OpenScape Voice system is up.

Step by Step

1) Navigate to **Configuration** tab > **OpenScape SBC** within the Navigation Bar in the Common Management Platform.
2) Select the **OpenScape SBC list** in the Navigation Tree under **Administration**.

   The system presents the **OpenScape SBC Overview** in the Work Area with a current list of all SBCs.
3) To view a list of SBCs configured at a specific communication system, select a communication system in the **Communication System** field in the navigation tree.

   The default selection for the **Communication System** field is the selection of the global settings in the system menu.

4) To find and select a particular OpenScape SBC use one of the following options:

   - In the Work Area select the checkbox to the left of the particular SBC in the list and select **Manage**.
   - Choose a SBC from the **OpenScape SBC** pull-down located in the Navigation Tree.

   General dialogue is presented in the Work Area displaying information and data for the selected SBC.

5) Navigate to **Configuration** > **VoIP** in the navigation tree under **Administration**

   The **Voice over IP** window appears with the **General** tab selected by default.

6) Select the **Comm System** tab.

7) Select the communications system´s type in the **Comm System Type** selection list. The type determines how OpenScape SBC is connected to the OpenScape Voice network. Possible values:

   - **Simplex**: Single node configuration.
   - **Collocated**: In this mode redundant SBCs are configured with both SBCs in active mode.
   - **Geo-Separated**: This mode means that the two nodes are at different locations.

   NOTICE: If the configuration is set to "Geo-Separated", the Secondary server fields for Node 1 and Node 2 will be enabled.

   ---

8) Click the **Trusted Addresses**, **Configure...** button in the **General** field area.

   The **Trusted Addresses** window appears. The trusted addresses list is used for Geo-separated installations. The addresses are displayed in a list.

9) To configure the list of trusted addresses, the following options appear:

   - Select an entry from the list and click the **Delete** button to remove an entry from the list.
   - Select an entry from the list and click the **Edit..**. button to edit the entry.
   - Click the **Add** button to add a new rule to the list.

   The **Add/Edit trusted address** window appears.

10) Enter or modify the trusted server IP address or FQDN (Fully Qualified Domain Name) in the **IP Address/FQDN** field.

11) Enter / modify the SIP port of the trusted server in the **Port** field.

12) Select the SIP transport protocol to be used in communication with the trusted server in the **Transport** selection list. Possible values: TCP (Transmission Control Protocol), UDP (User Datagram Protocol), TLS (Transparent LAN Service).

13) Click the **OK** button to store the settings temporarily.

    The **Add/Edit trusted address** window disappears, a new line is displayed in the list of trusted addresses.

14) Enter the settings for Node 1 in the **Node 1** field area:

    a) **Target type** field: The target type determines how OpenScape Branch will use the WAN outage server address. If the configuration

is "**Binding**" then the address will be either IPs or FQDNs. While configuration is "**SRV record**" a DNS-SRV query will search the address automatically. In this case OpenScape Branch uses the DNS-SRV response record to determine the priority of servers. The network administrator shall configure the priority of the SIP Server according to the network configuration.

b) **Primary server** field: The IP address (IPv4 or IPv6) of the primary server.
c) **Transport** field: Select a SIP protocol used to communicate with the primary server.
d) **Port** field: Used SIP port for the primary server.
e) **Secondary server** field: The IP address (IPv4 or IPv6) of the secondary server.
f) **Transport** field: SIP protocol used to communicate with the secondary server.
g) **Port** field: Used SIP port for the secondary server.
h) **SRV Record** field: IP address to retrieve the SRV (Service) record from.
i) **Transport** field: SIP protocol used to communicate with the server.
j) **Access IP Address/FQDN** field: (Currently not supported).

15) Enter the settings for Node 2 in the **Node 2** field area, in the **Comm System** tab:

a) **Target type** field: The target type determines how OpenScape SBC will use the WAN outage server address. If the configuration is "**Binding**" then the address will be either IPs or FQDNs. While configuration is "**SRV record**" a DNS-SRV query will search the address automatically. In this case OpenScape SBC uses the DNS-SRV response record to determine the priority of servers. The network administrator shall configure the priority of the SIP Server according to the network configuration.
b) **Primary server** field: The IP address (IPv4 or IPv6) of the primary server.
c) **Transport** field: Select a SIP protocol used to communicate with the primary server.
d) **Port** field: Used SIP port for the primary server.
e) **Secondary server** field: The IP address (ipv4 or IPv6) of the secondary server.
f) **Transport** field: SIP protocol used to communicate with the secondary server.
g) **Port** field: Used SIP port for the secondary server.
h) **SRV Record** field: IP address to retrieve the SRV (Service) record from.
i) **Transport** field: SIP protocol used to communicate with the server.
j) **Access IP Address/FQDN** field: (Currently not supported).

16) Click the **OK** button to go back to the **Voice over IP** window.

17) Click the **OK** button to store the changes temporarily in the administrator´s login session.

The **Voice over IP** dialog disappears.

18) Click the **Apply changes** button in the main window, work area.

The configuration of the communication system is applied on the OpenScape Session Border Controller.

4.7.6 How to Configure Timers and Thresholds

Proceed as follows to configure the timers and thresholds to control the system performance of the OpenScape SBC.

Prerequisites

Adequate administrative permissions.

At least one SBC is configured and in operation.

The connection to the OpenScape Voice system is up.

Step by Step

1) Navigate to **Configuration** tab > **OpenScape SBC** within the Navigation Bar in the Common Management Platform.

2) Select the **OpenScape SBC list** in the Navigation Tree under **Administration**.

The system presents the **OpenScape SBC Overview** in the Work Area with a current list of all SBCs.

3) To view a list of SBCs configured at a specific communication system, select a communication system in the **Communication System** field in the navigation tree.

The default selection for the **Communication System** field is the selection of the global settings in the system menu.

4) To find and select a particular OpenScape SBC use one of the following options:

- In the Work Area select the checkbox to the left of the particular SBC in the list and select **Manage**.
- Choose a SBC from the **OpenScape SBC** pull-down located in the Navigation Tree.

General dialogue is presented in the Work Area displaying information and data for the selected SBC.

5) Navigate to **Configuration** > **VoIP** in the navigation tree under **Administration**

The **Voice over IP** window appears with the **General** tab selected by default.

6) Select the **Timers and Thresholds** tab.

The settings for the timers and thresholds are displayed.

7) Enter the number of failure attempts that OpenScape SBC will count until a node failure is considered in the **Failure threshold (pings)** field.

8) Enter the number of positive responses to wait until node activation can be considered in the **Success threshold (pings)** field.

9) Enter the number of failure attempts during transition mode that OpenScape SBC counts until it switches to survivable mode in the **Transition Mode threshold (pings)** field.

10) Enter the time interval to send OPTIONS to the server in the **OPTIONS interval (sec)** field.

11) Enter the timeout when waiting for 200OK from SIP server in the **OPTIONS request timeout (sec)** field.

12) Enter the number of notifications per second sent to phones after state transition in the **Notification Rate** field. This field is disabled when OpenScape Branch operates in Proxy ACD mode.

13) Click the **OK** button to store the changes temporarily in the administrator´s login session.

    The **Timers and Thresholds** dialog disappears.

14) Click the **Apply changes** button in the main window.

The settings for timers and thresholds are applied on the associated OpenScape SBC server.

4.7.7 Configuration of Remote Subscribers - Overview

The OpenScape Session Border Controller (SBC) supports interface to Remote Subscribers. Configuration of these Remote Subscribers attributes is provided.

The following issues appear for one or more Remote Subscribers:

- The name associated with the remote subscriber or group of remote subscribers.
- Firewall settings can be configured if required.
- Emergency Services such as LIN (Line Identification Number), Emergency number and Callback number can be configured.
- A Black List and White List of blocked or allowed addresses can be configured.
- Configuration of endpoint Domain information and Media anchoring.

4.7.7.1 How to Configure Remote Subscribers - General

Proceed as follows to add a remote subscribers to the Voice over IP Remote Subscribers list.

Prerequisites

Adequate administrative permissions.

At least one OpenScape SBC is configured and in operation.

The connection to the OpenScape Voice system is up.

Step by Step

1) Navigate to **Configuration** tab > **OpenScape SBC** within the Navigation Bar in the Common Management Platform.

2) Select the **OpenScape SBC list** in the Navigation Tree under **Administration**.

   The system presents the **OpenScape SBC Overview** in the Work Area with a current list of all SBCs.

3) To view a list of SBCs configured at a specific communication system, select a communication system in the **Communication System** field in the navigation tree.

   The default selection for the **Communication System** field is the selection of the global settings in the system menu.

4) To find and select a particular OpenScape SBC use one of the following options:

   - In the Work Area select the checkbox to the left of the particular SBC in the list and select **Manage**.
   - Choose a SBC from the **OpenScape SBC** pull-down located in the Navigation Tree.

   General dialogue is presented in the Work Area displaying information and data for the selected SBC.

5) Navigate to **Configuration** > **VoIP** in the navigation tree under **Administration**

   The **Voice over IP** window appears with the **General** tab selected by default.

6) Click the **Remote Subscriber** tab.

   The **Remote Subscriber** window appears displaying the **Remote Subscribers** section.

7) Click the **Configure...** button in the **Remote Subscribers** field area.

   The **Remote Subscribers** window appears displaying a list of remote subscriber and subscriber group.

8) Click the **Add...** button. Or select an existing Remote Subscriber to edit.

   The **Add Remote Subscribers** window appears the General tab displayed.

9) Enter the remote subscriber Name in the **Name** field in the **Settings** field area.

   Domain configuration is mandatory to add remote subscribers. Firewall and emergency configuration can be done at a later time.

10) Click the **Symmetric Media** field in the **Settings** field area if symmetric media is to be sent between the Remote Subscriber and the OpenScape Voice system.

    Domain configuration is mandatory to add remote subscribers. Firewall and emergency configuration can be done at a later time.

11) Click the **Enable** field in the **Firewall Settings** field area.

    Additional configuration for firewall setting becomes active.

12) Enter the Message rate threshold for the firewall in the **Message rate threshold**: field, under Firewall Settings. Default: 20,000.

13) Enter the Number of active sessions allowed for this firewall in the **Number of active session**: field, under Firewall Settings.

14) Click allowed types of transport for the firewall in the **Firewall Settings** field area. Transport types are **SIP UDP**, **SIP TCP**, **SIP TLS**, **MGCP** and **DNS**.

15) Click the Black List or White List **Configure...** button to configure firewall screening.

    The **Black List** (blocking list) or **White List** (allowed list) dialog appears displaying a list of blocked or allowed addresses and associated ports.

16) Click the **Add...** button.

    The **Add Black List** or **Add White List** dialog appears.

17) Enter the IP address (IPv4 or IPv6) or Subnet to be blocked or allowed in the **IP address/Subnet**: field.

18) Enter the port number to be blocked or allowed in the **Port**: field.

19) Click the **OK** button to close the **Add Black List** dialog.

    The **Add Black List** window dis appears and a new row is created in the Black List table. The changes are stored temporarily.

20) Click the **OK** button to go back to the **Add Remote Subscribers** window.

21) Configure the **Location Domain** as follows:

    a) Click the **Domain & Media** tab.

       The **Domain & Media** window appears.

    b) Enter the Location Domain Name in the **Location Domain Name** field.

    c) Enter the Subnet IP Address (IPv4 or IPv6) in the **Subnet IP Address** field.

    d) Enter the Subnet mask address (IPv4 or IPv6) in the **Subnet mask** field e.g., 255.255.255.0.

    e) Select a particular type of media anchoring **Auto** or **Forced** in the **Anchoring Media** selection list, in the Location Domain work area.

22) Configure the **Media** as follows:

    a) Select the media protocol in the **Media protocol** list field, in the Media field area (in the Domain & Media tab). Options are **Pass-thru**, **STRP - Best effort** and **RTP**.

       Pass-thru (default) – If both originating and terminating side support the SRTP encryption mechanism then SRTP media is setup end to end in pass-thru mode and OS-SBC is not involved in the SRTP encryption and decryption. SRTP Key coming in from the originating device is being passed AS-IS to the terminating device in addition to the RTP and the other SRTP key giving the option to the terminating side to choose the SRTP/RTP mechanism based on its configuration. For example, if the originating side sends SDES only offer then the terminating side would get RTP, SRTP (Mikey) and SRTP (SDES from the originating side. This allows for additional flexibility in terms of setting up the call. If both parties support the same SRTP mechanism then SRTP media is setup end to end in pass-thru mode and OS-SBC is not involved in the SRTP encryption and decryption.

       Best effort SRTP Mikey or SDES configuration: Terminating network is enforced with the configured SRTP Mikey or SDES best effort offer. If the Terminating side in OS-SBC is configured with SDES and the originating sides send SDES offer then the SDES is negotiated end to end. However, if the originating side offers Mikey and the terminating

side in OS-SBC is configured for SDES then Mikey to SDES RTP is performed.

If SRTP-Best effort is selected, one of the following media security key negotiation protocols must be selected: SDES or MIKEY

If the Media Protocol is RTP or Pass-Thru no selection is possible. The entry should be grayed out with “none” shown.

b) Select the Key exchange method in the **Key Exchange Method** list field. Values: **SDES**, **MIKEY**, **None**. Select **None** if this method does not apply.

c) Checkmark the **Mark SRTP call leg as secure** checkbox, if the call requires secure media. When active, this parameter identifies the network as secure if TLS and SRTP are not used, i.e., TCP or UDP for the signaling transport or RTP is used for the media protocol.

d) Select the Certificate profile from the **Certificate profile** field list. The certificate profile contains TLS certificates (CA File, Certification File and Certification Key) for the connection.

23) Click the **OK** button to store the changes temporarily in the administrator´s login session.

The **Add Remote Subscribers** window disappears and the **Remote Subscriber** window appears with the General tab displayed.

24) Click the **OK** button to store the changes temporarily in the administrator´s login session.

The **Remote Subscribers** dialog disappears and the **Voice over IP** window appears.

25) Click the **OK** button to store the changes temporarily in the administrator´s login session.

The **Voice over IP** dialog disappears and the **General endpoint** windows appears.

26) Click the **Apply changes** button in the main window, work area.

The configuration of the Remote Subscribers is applied on the OpenScape SBC.

4.7.7.2 How to Configure Remote Subscribers - Emergency Services

Proceed as follows to add Remote Subscribers emergency number and emergency calling routing information.

Prerequisites

Adequate administrative permissions.

Remote Subscriber general information located on the **General** tab must be configured prior to configuration of the emergency services.

At least one OpenScape SBC is configured and in operation.

The connection to the OpenScape Voice system is up.

Step by Step

1) Navigate to **Configuration** tab > **OpenScape SBC** within the Navigation Bar in the Common Management Platform.
2) Select the **OpenScape SBC list** in the Navigation Tree under **Administration**.

   The system presents the **OpenScape SBC Overview** in the Work Area with a current list of all SBCs.
3) To view a list of SBCs configured at a specific communication system, select a communication system in the **Communication System** field in the navigation tree.

   The default selection for the **Communication System** field is the selection of the global settings in the system menu.
4) To find and select a particular OpenScape SBC use one of the following options:

   - In the Work Area select the checkbox to the left of the particular SBC in the list and select **Manage**.
   - Choose a SBC from the **OpenScape SBC** pull-down located in the Navigation Tree.

   General dialogue is presented in the Work Area displaying information and data for the selected SBC.
5) Navigate to **Configuration** > **VoIP** in the navigation tree under **Administration**

   The **Voice over IP** window appears with the **General** tab selected by default.
6) Click the **Remote Subscribers** tab.

   The **Remote Subscribers** window appears displaying the **Remote Subscribers** section.
7) Click the **Configure...** button in the **Remote Subscribers** field area.

   The **Remote Subscribers** window appears displaying a list of remote subscriber and subscriber group.
8) Click the **Add...** button. Or select an existing Remote Subscriber to edit.

   The **Add Remote Subscribers** window appears the General tab displayed.
9) Click the **Emergency Calling** tab.

   The **Emergency Calling** window appears displaying the **Emergency calling subnets** list.
10) Click the **Add...** button.

    The **Add emergency calling** window appears the General tab displayed.
11) Enter the calling party endpoints IP address (IPv4 or IPv6)(or range of IP addresses) of the subscriber(s) in the **IP Address** field.
12) Enter the IP subnet of the range of subscribers defined by the IP address (IPv4 or IPv6) configuration in the **Subnet mask** field. If a single subscriber is configured use mask 255.255.255.255.

    Default subnet: The entries IP=255.255.255.255 and Mask=255.255.255.254 create a Default Subnet, which will be used for all phones not comprised in any subnet. The usage of Routing Prefix is exactly like normal subnets.

13) Select a routing prefix, if applicable, from the **Routing Prefix** selection list e.g., 911999. If not applicable select None.

14) Click the **Send LIN instead of CPN** field. This option is used to avoid the adding of the CPN (Calling Party Number) in MIME (Multipurpose Internet Mail Extensions) and use the LIN (Location Identification Number) instead. Use this option if the Gateway does not accept the emergency calls using MIME.

15) Click the **LIN** tab.

    The **LIN** window appears displaying the **LIN** list.

16) Click the **Add...** button.

    The **Add LIN** window appears.

17) Enter the LIN (Location Identification Number) in the **LIN** field. The LIN is used to associate a subscriber with its physical location.

18) Click the **OK** button to close the **Add LIN List** dialog.

    The **Add LIN** window dis appears and a new row is created in the LIN List table. The changes are stored temporarily.

19) Click the **OK** button to go back to the **Add Remote Endpoints** window, **Emergency Calling** Tab.

20) Click the **Emergency Number** tab.

    The **Emergency Number** window appears displaying the **Emergency Number** list.

21) Enter the Emergency Number of the emergency center in the **Emergency Number** field.

22) Click the **Add** button.

    The Emergency Number is added to the **Emergency Number** list. If these numbers are dialed the OpenScape SBC or Branch identifies the number as an “Emergency Call” (for the USA this represents the 911emergency calls). This will trigger the server to try to establish an outgoing call to an available gateway (highest priority).

23) Click the **OK** button to store the changes temporarily in the administrator´s login session.

    The **Emergency number** dialog disappears and the **Add Remote Subscriber** window appears.

24) Click the **OK** button to store the changes temporarily in the administrator´s login session.

    The **Add Remote Subscribers** dialog disappears and the **Remote Subscribers** window appears.

25) Click the **OK** button to store the changes temporarily in the administrator´s login session.

    The **Remote Subscribers** dialog disappears and the **Voice over IP** window appears.

26) Click the **OK** button to store the changes temporarily in the administrator´s login session.

    The **Voice over IP** dialog disappears and the **General branch** windows appears.

27) Click the **Apply changes** button in the main window, work area.

The configuration of the subscriber emergency services is applied on the OpenScape SBC.

4.7.7.3 How to Configure Remote Subscribers - Domain

Remote Subscribers domain location information must be configured with the subscribers general information when adding a Remote Subscriber. Domain location information is sent from the OpenScape SBC to the OpenScape Voice for processing calls. For details refer to:

How to Configure Remote Subscribers - General

4.7.7.4 How to Configure Throttling and Registration Expiry

Proceed as follows to configure TLS throttling and subscriber registration timers associated with a OpenScape SBC.

Prerequisites

Adequate administrative permissions.

At least one SBC is configured and in operation.

The connection to the OpenScape Voice system is up.

Step by Step

1) Navigate to **Configuration** tab > **OpenScape SBC** within the Navigation Bar in the Common Management Platform.
2) Select the **OpenScape SBC list** in the Navigation Tree under **Administration**.

   The system presents the **OpenScape SBC Overview** in the Work Area with a current list of all SBCs.
3) To view a list of SBCs configured at a specific communication system, select a communication system in the **Communication System** field in the navigation tree.

   The default selection for the **Communication System** field is the selection of the global settings in the system menu.
4) To find and select a particular OpenScape SBC use one of the following options:

   - In the Work Area select the checkbox to the left of the particular SBC in the list and select **Manage**.
   - Choose a SBC from the **OpenScape SBC** pull-down located in the Navigation Tree.

   General dialogue is presented in the Work Area displaying information and data for the selected SBC.
5) Navigate to **Configuration** > **VoIP** in the navigation tree under **Administration**

   The **Voice over IP** window appears with the **General** tab selected by default.

6) Select the **Remote Subscriber** tab.

   The settings for TLS throttling and subscriber registration are displayed.

7) Click the **Enable** field.

   The **Remote Subscriber** screen becomes active.

8) Click the **Enable Throttling for non TLS** field in the **Registration Expiry Timer** field area to enable throttling for non TLS connections.

9) Click the **Enable Throttling for TLS** field in the **Registration Expiry Timer** field area to enable throttling for TLS connections.

10) Enter the timer interval in the **Timer time towards subscriber** field timer value towards subscriber behind a NAT. For subscribers behind NAT, the smaller value of either the **Timer time towards subscriber** or the expiry interval received from the subscriber is sent to subscribers in order to allow the NAT pinhole to remain open. Default: 60 seconds.

11) Enter the timer interval in the **Max throttling timer threshold** field for throttling towards OpenScape Voice for subscribers behind NAT. For subscribers behind NAT, the smaller value of either **Max throttling timer threshold** or the expiry interval received from the subscriber is sent to Register to OpenScape Voice. Default: 1800 seconds.

12) Enter the maximum registration expiry time allowed from the subscriber in the **Maximum registration expiry time** field. A registration received from a subscriber with expiry greater than the **Maximum registration expiry time** is rejected. Default: 5000 seconds.

13) Enter the TTL timer interval in the **TTL timer** field. Default: 2 hours.

14) Click the **OK** button to store the changes temporarily in the administrator´s login session.

    The **Voice over IP** dialog disappears and the General SBC main window appears.

15) Click the **Apply changes** button in the main window, work area.

The settings for throttling and registration expiry are applied on the associated OpenScape SBC.

5 OpenScape SBC Local Management Platform Overview

IMPORTANT: The **OpenScape Session Border Controller** platform is also available in the following languages: English, German and French (starting from V10R2.2.0). You may choose the language of your preference (English, German or French) before login.

This application is used to configure OpenScape V9 Session Border Controllers via their own / local graphical user interface (GUI).

In upper right corner of the web page the logged user is presented. Help and Logout links are also offered in same position.

There are four available users for login: administrator, service, guest and root. If the user logs in as guest, configuration can not be changed.

To save a configuration, the user should click on **Apply Changes** button. All configuration is then saved and applied to the system. Depending on the changes some process or even the entire system will restart. See below the impacts of each process restart.

- SipServer Restart: New and ongoing calls will fail. New feature requests such as Hold, Consult, Blind Transfer may fail. Active calls may be disconnected.
- SSM Restart: New and ongoing calls will fail. New feature requests such as Hold, Consult, Blind Transfer may fail. Active calls may be disconnected.
- RTP Proxy Restart: All calls that utilize sRTP, G.729, WAN-LAN, and LAN-WAN will fail. New and ongoing may fail and active calls will have no speech.

If the **Cancel Changes** button is used, all changes are lost and the last committed configuration is loaded to the page.

All configuration fields are validated using a regular expression for each field type available. When one or more fields do not match the validation criteria, a message is shown to the user: "There are invalid field values: [field]; Enter a valid [field type].". The available types are:

- **Number** – Allows numeric characters [0-9] (in some numeric fields, there is also a range validation)
- **Port** – Is a numeric field between 0 and 65535
- **Port range** – A port range written as start_port:end_port
- **IP address** – Written in dot-decimal notation, which consists of the four octets of the address expressed in decimal and separated by periods
- **Hostname** (FQDN or IP address) – These fields allow IP addresses or FQDN. Each FQDN must contain only letters, numbers or hyphen ("-") characters. The characters are not case-sensitive.
- **Netmask** – Written in dot-decimal notation
- **Digits** – Allows numeric characters and the + digit (used for dial numbers)
- **Routing prefix** – Allows numeric characters and the characters used to write regular expressions: [ ] _ % | + * - ^

5.1 Dashboard

This top level screen presents the most important system information and gives quick access to system status and alarm details.

5.1.1 Alarms

Alarm summary:

The **Alarm summary** shows the number of **Critical**, **Major** and **Minor** alarms. The information presented is cumulative. Alarms can be cleared manually by the user or by the system, when the cause of the alarm is solved. The number of alarms displayed will increase until the user or the system clear the alarms.

Show alarm details:

Show alarm details button opens the **Alarm Details** window with the following information:

- **Group ID** and **Event ID** correspond to the SNMP trap OID (the last 2 numbers of the OID). An alarm trap is cleared by a trap with the same OID of severity 'cleared'.
- **Group name** is the name of the GroupID. It groups together system status information of similar kind.
- **Event name** is a character string that describers the alarm. It is closely related to the trap name as defined in the Branch SNMP MIB.
- **Monitored value** shows the current condition of the system relevant for that particular alarm, e.g. temperature or just True/False. An empty ('blank') value means no-alarm.
- **Time** is the time when the alarm occurred.
- **Threshold** is the value that needs to be crossed by monitored-value for an alarm to be generated. If e.g. if the existence of an alarm condition is represented by True =1 then the threshold should be 0 to trigger an alarm.
- **Trigger** shows the condition where the alarm will be generated. Trigger is a comparison with alarm value.
- **Severity** is the alarm severity assigned to that particular alarm (warning, minor, major, critical). The Severity is fixed per Fault-Id.
- **Flow timer** indicates the minimum time to wait before generating a next occurrence of the same alarm.
- **Reporting class** is a number between 0 and 7 that groups events to classes that are reported to the same trap destination. 0 means that the event is not reported via SNMP trap.
- **Faulty object** is a character string that defines the object that is at fault. This value may be different from branch to branch, but it is fixed for a particular branch.
- **Event type** classifies the alarms into:
  - **Communications**
  - **Environmental**
  - **Equipment**
  - **processingError**
  - **qualityOfService**

An alarm can be cleared individually or by group. The alarms can be sorted based on any of the information category bullet items presented above.

Once an alarm is cleared, it will only appear in Alarm History log.

5.1.2 System Status

Mode:

Mode of the Session Border Controller (SBC), e.g. Centralized SBC.

Auto refresh timer:

Using this combo box an auto refresh timer can be set, after the timer expiration the Status, System Info and Alarm information is refreshed automatically. When setting the auto refresh to never the user has to refresh each tab individually using the refresh icon.

Operational state:

Operational state shows the system connectivity with the central SIP Server.

- **normal** indicates full connectivity to primary and/or backup server.
- **survivable** indicates no connection to server and the system operating in "limited mode". A transition to survivable mode goes from: **normal** mode to **transition** mode to **survivable** mode.
- **transition** state is the transition interval between states. The proxy remains in **transition** state N times "OPTIONS interval" seconds where N is the "Transition Mode threshold" (see also "Comm System" configuration).
- **Standalone** state is set when the **Enable Standalone** flag is enabled under **Features**.

IMPORTANT: Once the flag is enabled and the configuration is applied, the dashboard will show **Standalone** in Operational mode. The Primary server is set to **127.0.0.1** (loopback) and the state should be green. This is accomplished by Survivability Provider sending OPTIONS message to the loopback interface.

Redundancy state:

When Redundancy is enabled, the state shows the status of Redundancy system.

- **MASTER** indicates that the system is the current active system.
- **BACKUP** indicates that the system is in a standby mode (all services are disabled).
- **FAULT** indicates no network connectivity.

NOTICE: When entering the Local GUI using the Virtual IP address, instead of 'Redundancy state', a field 'Master IP address' is displayed with the IP address of the master node.

Primary and Backup server:

These boxes present the addresses or FQDN of the central SIP Servers, the green/red box associated indicates the state of the server.

Displayed for both **Com Node 1** and **Com Node 2**.

Penalty box state:

These boxes represent the state of the central SIP servers; displayed for both **Com Node 1** and **Com Node 2**.

- **NotRunning** is the state reported when survivability provider is not running,
- **In Penalty Box** is presented when the SBC loses connection with the SIP server.
- **Active** represents full connectivity with SIP server.
- **Transition** is presented when SBC detects a connectivity problem with the SIP Server.
- **OK** represents the state where the binding has lower priority than the currently active binding.

5.1.3 Services Status

Show the status of the following items:

- **Alarm Manager** – Application responsible for generating and clearing alarms.
- **Audit** – Application used to provide an assessment of a system's internal control.
- **B2B Controller**- Application responsible to manager B2B calls, routing, and rerouting for the mode "Standalone with internal SIP Stack".
- **B2BUA** (Not Applicable, status = "not running") – Back to Back SIP User Agent, this application is responsible for MLHG/ACD/Integrated Gateway and Auto Attendant call handling.
- **Continuous Symptom Collector**-A process used to send normal log messagesfrom one server to another server via a network connection. The logswill be saved locally and remotely.
- **Continuous Tracing** – Trace application that collects the system logs and traces and send to an external application.
- **Cron** – Linux open source application that provides time-based job scheduling.
- **DBMS** – Database Management System application.
- **DHCP** – Linux open source application using Dynamic Host Configuration Protocol, a network application protocol used by devices (DHCP clients) to obtain configuration information for operation in an Internet Protocol network.
- **DNS** – Linux open source application that handles Domain Name System, distributing the responsibility of assigning domain names and mapping those names to IP addresses.
- **eth0** – First network interface.
- **eth1** – Second network interface.
- **IPsec**-(Internet Protocol security) provides a secure tunnel between hosts.
- **Kernel Console Collector**-A kernel feature that allows kernel log messagesto be sent via an express network connection (ethernet protocol) to becaptured by another server.
- **MS Adapter** – Runs in Branch SBC, SBC-Proxy and Centralized SBC modes. It is a Proxy for MGCP messages which converts messages from WAN to LAN and sends them to Media Server.
- **Media Server** – Internal proprietary application responsible for the announcements and large conferences.

- **NTP** – Linux open source application that uses the Network Time Protocol for synchronizing the clocks of computer systems over packet-switched, variable-latency data networks.
- **Process Manager** – Controls all SBC applications. Responsible for monitoring and restarting applications in case of failure or re-configuration.
- **Push Notification**-It supports sending Notifications to an Apple Push Notification Server and Firebase Cloud Messaging Server.
- **QoS Application** – Responsible for monitoring Quality of Service media statistics calculations.
- **Redis** - Database based on memory for some applications.
- **Redundancy** – Application which provides redundancy.
- **Reverse Proxy**-Currently Not Used. Reserved for future (TBD).
- **RTP Proxy** – Open source application that proxies payload from outside to inside address and vice-versa (WAN to LAN and LAN to WAN). It runs in Branch SBC, SBC-Proxy and Centralized SBC modes.
- **SIP Loadbalancer** -The SIP Load Balancer distributes the SIP Signaling traffic among a Telephony connector cluster.
- **SIP Server** – Application that controls SIP Requests. It can operate as SBC or Proxy. It's based on open source SIP Server.
- **SNMP** – Linux open source application that uses Simple Network Management Protocol to monitor network-attached devices for conditions that warrant administrative attention.
- **SSH** – Linux open source application that allows data to be exchanged using a secure channel between two networked devices.
- **SSM** – SIP Services Module, this application controls some services used in survivable mode for instance MOH.
- **Service**-The component implements a REST API to configure some internalcomponents and allow retrieving logs and other information useful fortroubleshooting.
- **Survivability Provider** – The SP is responsible for checking the Operational State and send Notifications to subscribers.
- **Syslog** – Open source application responsible for system and application logs. It provides a rotation mechanism to store logs according to the log level set.
- **Web server** – Application used to host and provide access to SBC Homepages by Web Browsers.
- **Peer Monitoring** - The application is responsible for monitoring peers using OPTIONS messages. It is utilized for the SBA, the endpoint connectivity checks in the "Standalone with internal SIP Stack" mode, and in OPTIONS with alias port on the core side.

NOTICE: This option is only available in V11R1.01.00 or higher.

Overall applications can have status **running** or **not running**. Status **running** means the application is enabled and running, while **not running** can either identifies the application as disabled or that an error occurred and the application has stopped.

The **Continuous Tracing** and the **Redundancy** applications are kept running even though when disabled. While running, these two applications can have status **active** when enabled or, **stand-by** when disabled. The ethernet interfaces eth2, eth3, eth4 and eth5 will be shown if they are configured on system.

5.1.4 Registered Subscribers

This button opens a new window or tab to show the subscribers that are registered internally on SBC. The presented expiration time is based on the information sent by the subscriber on registration, therefore the time used by expiration may be shorter if the central SIP server modifies the expiration timer.

The total amount of registered subscribers depends on the hardware type:

- VM250 - maximum of 250 subscribers.
- IBM x3250 - maximum of 6000 subscribers.
- x3550, Fujitsu RX330 and Fujitsu RX200 - maximum of 50000 subscribers.

5.1.5 SSP Connectivity Status

SSP Connectivity Status

This page shows the connectivity status of all SSP endpoints and it is also possible to trigger REGISTER requests for the SSP that are configured to do it so.The following information is shown:

- **Status** - icon that represents the current state
- **SSP Trunk Name** - configured SSP's name
- **Default Home DN -** configured SSP's Default Home DN
- **URI** - configured SSP's URI
- **SSP Connectivity Check** - SBC monitors the OPTIONS requests and the respective responses that pass through it towards the SSPs. The possible values are:
  - **Not Available**: No OPTIONS request has passed through SBC towards this SSP
  - **Connected**: SSP responded successfully the last OPTIONS request
  - **Not Connected**: SSP responded with an error or did not respond the last OPTIONS request
- **SSP Registration Status**- for the SSPs that the registration is required, SBC monitors the REGISTER requests and the respective responses. The possible values are:
  - **Not Available**: The registration is not required for this SSP
  - **Registered**: SSP responded successfully the last REGISTER request
  - **Not Registered**: SSP responded with an error or did not respond the last REGISTER request
  - **Suspended**: Automatic registration suspended by the user (unregister).
- **Register/Unregister**- This column is used to trigger a REGISTER or UNREGISTER (expires=0) request to the SSPs that the registration is required. When enabling the checkbox, the user can trigger the request to the SSP by clicking on the **Register** or **Unregister** button. More than one SSP can be selected at once.

  NOTICE:

  The automatic registration will be suspended when triggering an unregister to the SSP. To enable it again, it is necessary to either

trigger a register to the SSP or apply any configuration on the system.

IMPORTANT: It is not possible to trigger a REGISTER request to the SSPs that the **Registration Status** is marked as '**Not Available**'. This status represents that the SSP is not configured to send REGISTER requests.

The Auto refresh timer can be set to periodically reload the status. This refreshment is not enabled by default.

5.1.6 Dynamic Port Mapping

Dynamic Port mapping

The **Dynamic port mapping** button opens the **Port Mapping** window to show the subscribers port mapping, with their core and access IP address and ports.

- **Contact** is set by the received Contact of SIP message and is the same Contact field presented in the Registered Subscribers table.
- **External IP** is the IP Address of the SIP phone
- **SBC core Port** is the port where SBC is listening to the SIP messages from the SIP phone.
- **External Port** is the external port allocated according to the configured SIP port range.
- **SBC access IP** is the Access (WAN) IP address.
- **Map time** - Amount of time the subscriber registration has been active.
- **Expire time from server** - Time allocated to a subscriber before new registration is required.

5.1.7 CloudLink panel

CloudLink panel

The **Show** button next to **Cloudlink panel** opens the CloudLink Daemon pop-up window. By default, CloudLink is disconnected.

- **Link to CloudLink**: Allows you to connect to the CloudLink server.

  Once connected, the CloudLink Daemon window displays the connection details.

  For more information, refer to Integrating SBC with CloudLink Daemon on page 289.

CloudLink Daemon window

- **About**: This section displays the general CloudLink connection information (version, Mitel Cloud Services Terms and Conditions and Licenses).
- **CloudLink registration**: Displays the Account name, Account ID and the option to disconnect from CloudLink.
- **Inentory Report Submission**: Upon a successful connection, an inventory report is generated and refreshed approximately every 30 minutes.

- **CloudLink Daemon update**: Allows you to schedule and manage CloudLink Daemon update.
- **Tunnels**: Allows you to enable the SBC UI within CloudLink, by clicking **Start**.

  Once connected, the **Launch** button becomes active under **System Inventory** > **Applications** and you can perform a remote SBC server configuration.

5.1.7.1 Integrating SBC with CloudLink Daemon

If your communication system is OpenScape Voice or OpenScape 4000, the OpenScape SBC must be properly configured to establish a connection with CloudLink. This configuration enables the routing of calls from the communication system to Zoom Phone.

To facilitate this connection, the OpenScape SBC administrator is required to complete specific tasks using the OpenScape SBC Assistant (version V10R2.4.0 or later).

Prerequisites

Adequate administrative permissions.

The CloudLink Daemon RPM is installed. 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.

CMP is connected to CloudLink Daemon. For more information, refer to OpenScape Common Management Platform V10, Administrator Guide and OpenScape Solution V11, Zoom with OpenScape Voice and OpenScape SBC, Phone System Integration Solution Guide.

To connect OpenScape SBC to CloudLink Daemon:

Step by Step

1) Log in to the OpenScape SBC Assistant.
2) Navigate to the **System** > **Settings** tab.
3) Locate the **CloudLink** section.
4) To enable the SBC-CloudLink connection, check the **Enable Cloudlink Service** checkbox.
5) Click **OK**.

   You are redirected to the main page, where the SBC Dashboard displays the **CloudLink status**.
6) To activate the SBC-CloudLink connection information, click **Show** next to the **Cloudlink panel** item.

   The CloudLink Daemon window pops up. By default, CloudLink is disconnected.
7) Click **Link to CloudLink** to connect to the CloudLink server.
8) Enter your credentials in the CloudLink sign-in pop-up window and click **Next**.
   The CloudLink Daemon window displays the connection details.

9) To configure tunnels and enable the SBC UI within CloudLink:
   a) In the **Tunnels** section of the CloudLink Daemon, click **Start** next to the OpenScape SBC component.
   b) Click **Yes** to confirm.
   c) Log in to CloudLink Daemon.
10) Optionally, you can view system information and launch a remote SBC configuration:
   a) From the left-hand menu, click the **System Inventory** drop-down to expand it.
   b) To view the SBC(s) connected to CloudLink, select **Platforms**.
   c) To perform a remote SBC server configuration, select **Applications**, then click **Launch**.

   NOTICE: The **Launch** button becomes active only after the tunnel has been successfully established.

11) To disconnect from CloudLink, click **Disconnect from CloudLink** in the main CloudLink window.

5.1.8 Dynamic IP Remote Endpoints

The Dashboard's Dynamic IP remote endpoints **Show** button opens the **Dynamic IP Remote Endpoints** window to show a list of "Dynamic IP" remote endpoints including their Logical-Endpoint-ID and current contact address is displayed in the appropriate IP field. If no contact address is currently assigned the field is blanked out.

5.1.9 Denial of Service Mitigation

The following parameters are displayed on the **Denial of Service Mitigation** screen.

- **IP** - Source IP of the device that violated the message rate limit
- **Quarantine TTL** - Time to Live – remaining time (in seconds) that the source IP has left in quarantine. This value will decrement to zero, at which point, the source IP is no longer quarantined.
- **Network ID** - name of the SBC access interface where the violation was observed.
- **Unblock** - the administrator may select a row from the Quarantine Grid and unblock (un-quarantine) the source IP. Select an entry and click **Unblock** button to free the source IP from quarantine. The TTL will go immediately to zero, but the entry will NOT be deleted from the table.

The Quarantine Grid will hold a maximum of 100 entries, with the most recently quarantined Source IPs are listed at the top.

Quarantine Grid for Unauthorized/Unknown Users

- **IP:Port** - Source IP and Port of the device that is on the Unauthorized/ Unknown Users quarantine list.
- **Expire** - The time that the source IP will leave the quarantine list.

5.1.10 SIP Load Balancer status

The default Load Balancer mechanism is the Round-Robin. In this mechanism, each connection is forwarded to one of the active servers, and the entries stay in the table (Cluster or ClusterTLS) until the end of the expiration timer (Session Persistence timeout). If the entry already exists in the table, the connection will use it.

The following parameters are displayed on the SIP Load Balancer status screen for each configured SIP Cluster:

- **IP**
- **Port**
- **Enabled**
- **Status**
- **Conn**

NOTICE: The Conn (connection counter) field calculates any new incoming connection attempts, in the transport layer, regardless of whether the SIP connection was Successful, Failed or Dropped.

5.1.11 System Info

CPU:

This box gives the percentage of the usage of CPU; this is snapshot information for a small period of time. Depending on the system load it will indicate from 0% to 100% of usage. If the Hardware type is Virtual, it will also display the number of CPUs and the CPU speed.

Memory:

This box gives the percentage of the usage of RAM memory; this is snapshot information for a small period of time. Depending on the system load it will indicate from 0% to 100% of usage. If the Hardware type is Virtual, it will also display the total memory available.

Disk:

This box gives the percentage of disk usage; this is snapshot information for a small period of time. Depending on the system load it will indicate from 0% to 100% of usage. If the Hardware type is Virtual, it will also display the disk size.

System uptime:

This box shows how long the system has been running. 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".

Hardware Type:

This box shows the hardware type (CPU) used for SBC.

Hostname:

This box shows the node name. The name is defined in node.cfg file and set during a full installation.

NOTICE:

From V10R3.1.1 onwards, the VMware reservation settings (Reserved CPU and Memory for VM) have been added in the system information of Dashboard.

Information about these settings has also been added in vmsettings.txt file which is in the info.tar file of rapidstat functionality.

5.1.12 Software Info

Software version:

This box indicates the software version running on the system. Detailed information is available by selecting on the **Software Partition information** buttons.

Software Partition information:

- **Active** - Using this button the user can see detailed information of the installed packages on the active partition, a new window or tab will be opened to show the information.
- **Backup** - Using this button the user can see detailed information of the installed packages on the backup partition, a new window or tab will be opened to show the information.

IMPORTANT: For **Hosted OpenScape SBC** (hSBC) on **OS4K** Deployments, **Backup** is disabled.

5.2 System

This administrative area contains settings for SBC such as the mode, host name, domain name, licenses, and branding info.

5.2.1 Settings

General

The following sections concern details for the system settings tab for the SBC.

- **SBC Mode**

  Available options: **Centralized SBC**, **Load Balance**
- **Hostname**

  This field shows the node name. The name is defined in node.cfg and set during a full installation.

- **Domain Name**

  This field shows the domain within which the node resides.

Administration

- **Session expiry timer**

  It is used to extend the https session timeout. The timers are:

  – 1 hour
  – 2 hours
  – 3 hours

Watchdog configuration

> **IMPORTANT:** For **Hosted OpenScape SBC** (hSBC) on **OS4K** Deployments, **Watchdog** configuration is disabled

- **Enable** - If checked, this field enables Hardware Watchdog. It is recommended that it is enabled for redundant systems.
- **Watchdog information** - By clicking on this button a new window appears with information about Watchdog's activity (**Status**, **Expiry Timer**, **Refresh, Preset**, **Watchdog options**)
- **Watchdog expiry timer** - This field is used to extend the expiry timer. By default is set to 1 minute. The possible timer values are:

  – 1 minute
  – 2 minutes
  – 3 minutes
  – 4minutes
  – 5 minutes

Open VM Tools

- **Enable Open VM Tools**

  If checked, this field enables the Open Virtual Machine Tools (open-vm-tools)

CloudLink

- **Enable CloudLink service**

  Check this checkbox to enable the SBC-CloudLink connection. Once enabled, you are redirected to the main page, where the SBC Dashboard displays the CloudLink status and CloudLink panel.

  For more information, refer to Integrating SBC with CloudLink Daemon on page 289.

5.2.2 Licenses

General

- **License server** - This is the IP address of the license server.

  – **Port** - This is the SOAP port of the license server.

- **Backup management server** - This is the IP address of the backup management server used on Branch installations when the primary server is not available. Read only field.
  - **Port** - This is the SOAP port of the backup management server. Read only field.
- **Logical ID** - This is the unique identifier used on the SBC Assistant for authentication purposes.
- **Hardware ID** - This is MAC address of the SBC Core Access realm (LAN) interface used to identify the SBC on Assistant. It is a read only field and is greyed out.
- **Advanced Locking ID** - This is the unique identifier used to generate a Standalone license file. It must be refreshed in case of changes in: hostname, IP addresses, default gateway, DNS or Time Zone. It must be cleared before uploading a standalone license file.

NOTICE: DNS Server must be enabled.

License Information

- **License type** - This is the type of the SBC license. Possible values are:
  - **None** - If no licenses were assigned to the Branch.
  - **Floating** - If the licenses were retrieved from a license server.
  - **Stand Alone** - If the licenses were provided in the USB Stick during the SBC installation or manually uploaded.
- **Days till license expires** - This field shows the number of days until the configured license expires. If the system is running without license this will show how many days still available in grace period.
- **License Version** - Indicates the version associated with the license obtained from the Central License Server (CLS).
- **SIEL ID** - This field shows the Standardized Integrated Equipment Life-cycle (SIEL) that is delivered to each network element with licenses file from the Central License Server (CLS). The SIEL ID is also retrievable over a specific SNMP get request.

  Depending on the Licence type (CMP assigned or local Licence) the SIEL ID will read:

  - for CMP assigned Licences:

    CMP will provide the SIEL ID thru the WSDL interface along with the Licence Version (V9, V10 etc.)

    SIEL ID is received from CMP: SID: received siel ID

    SIEL ID is NOT received from CMP: SID: CMP assigned
  - for locally applied License

    SID: SIEL ID retrieved from CLS

NOTICE: The IP address of the node that will execute the snmpget commands needs to be included under **Alarms** >**SNMP Configuration** > **SNMP v2c Read-Only IP**

- **Stand alone license file** - Using the **Choose File** browser button the user can select one valid license file (.lic). The **Upload** button will be used to upload the selected license file, validate it and activate the licenses.

- The "Refresh" button is used to request licenses to the configured license server. After a request is done, the screen is updated with the new values.
- The license counters are presented in table where the first column shows the **License type**, the second column shows the number of **Licenses configured** on the system and third one shows the **Licenses usage (peak)** (watermark value reset monthly). Below is a brief description of each license type.
  - **Base** - This is the SBC base license used to track the number of SBC in the field.
  - **SBC Sessions** - This license determines the maximum number of system wide SBC Sessions.

Open Source Software License

Using the drop down list is possible to select the open source application and then using the **Show** button get the license used for this application.

EULA

- **EULA** - The user can select an end-user license agreement (EULA) or software license agreement from the drop-down list and then click the **Show** button. A new window will open to display the agreement.

5.2.2.1 Open source software license

Shows the open source software license information of the selected application.

5.2.3 Branding

Branding Settings

- **Company Name**

  Allow changing the Company Name that is presented on Local Management. This name can be made up of upper or lower case letters, digits, or special characters. Special characters can be any of the following set: !@#%&()_-+{}|:;'?/=,^$.*[]™©äÄüÜöÖ€µß and the white space.
- **Product Name**

  Allow changing the Product Name that is presented on Local Management. This name can be made up of upper or lower case letters, digits, or special characters. Special characters can be any of the following set: !@#%&()_-+{}|:;'?/=,^$.*[]™©äÄüÜöÖ€µß and the white space.
- **TLA**

  Allow changing the Trademark License Agreement that is presented on Local Management. This name can be made up of upper or lower case letters, digits, or special characters. Special characters can be any of the following set: !@#%&()_-+{}|:;'?/=,^$.*[]™©äÄüÜöÖ€µß and the white space.

- **Logo Picture**

  Allows changing the Logo Picture that is presented on Local Management for the login screen and title bar. The file must be a valid image (png, jpg, gif) and should use the recommended dimension (160x40) for proper display.

  IMPORTANT: It is recommended for the file size is to be smaller than 5Kb.

  The **Import** button is used for uploading a new picture file, which becomes afterwards visible at the Logo Picture combo box.

  The **Delete** button is used for deleting the selected picture file.

  The option "default" is used to select the original logo picture.

  NOTICE: regarding browser cache: Any changing user interface element may not be immediately visible on all versions of supported browsers. Browser reload discarding cache (usually Ctrl-F5) may be needed for updating the pages accordingly. Even the clear of browsing history may be needed.

IMPORTANT: For Hosted OpenScape SBC (hSBC) on OS4K Deployments, Branding is disabled.

5.3 Network / Net Services

In this administrative area the user can configure the network services.

Network Services comprise configuration of interfaces, routing and traffic shaping as well as NTP (Network Time Protocol), DNS (Domain Name System) and QoS (Quality of Service) settings.

5.3.1 Settings

Configuration of interfaces for the Core (LAN) and Access (WAN) realms, routing and, Redundancy is done under the **Settings** folder.

5.3.1.1 Physical Network Interface

Most of the hardware models have only two network interfaces. In some models four network interfaces are available. Additional interfaces are not configurable by Management Portal.

The user must configure the necessary physical interface characteristics and enable each physical Ethernet network interface controller (NIC) to be supported in the system.

Interface

Identifies the hardware platform physical interfaces available for configuration, eth0, eth1, eth2, eth3, corresponding to the external port configuration.

Enabled

This check box allows the user to enable/disable the interface. The eth0 and eth1 NIC'S are enabled by default, while eth2-eth3 SHALL be available for user configuration. The first interface can't be disabled.

IMPORTANT: Enabling/Disabling the interfaces reboots the system. Active and ongoing calls may fail.

MTU

Enables user to adjust the MTU Size.

The customer may set the field to any value between `300` and `1500`. The default value is "`1500`".

Speed (Mbps)

The interface speed can be configured under this cell. Options are `Auto`, `10` Mbps, `100` Mbps and `1000` Mbps. If the `Auto` option is selected, auto negotiation is used. Otherwise, the interface speed is set to the configured value.

Duplex Mode

Enables the user to adjust the duplex mode (`Full` or `Half`). This option is disabled if **Speed** option is set to `Auto`.

NOTICE: If the **Speed** field is set to `1000` Mbps, then the **Duplex mode** field option is disabled and shall only show `Full`.

Interface bonding

This enables ethernet NIC 'Teaming' or 'Bonding', as an optional capability to be used for load-sharing or redundancy, available for "Single Armed" or "Multi-Armed" OpenScape SBC configurations.

IMPORTANT:

In case ALL available eth interfaces are bonded the respective **Realm Network IDs** cannot be added under Firewall Settings.

IMPORTANT: For **Hosted OpenScape SBC** (hSBC) on **OS4K** Deployments, **Interface Bonding** is disabled

---

If **Single armed** is enabled, only a single bonding interface, identified as 'bond0', is used. The 'bond0' interface consists of at least the two physical interfaces eth0 and eth1. If additional NIC interfaces exist in the hardware configuration they may be included in 'bond0'. Once 'bond0' is configured all logical network interface definitions, routes and firewall references previously

referencing Ethernet NIC eth0 or eth1 are promoted to use the ‘bond0’ interface.

For “Multi-Armed” OpenScape SBC configurations the user must ensure that at least one interface, either a bond or Ethernet NIC interface exists within the core and access network realms, and that all logical network interfaces reference the appropriate interface.

NOTICE: Each Ethernet NIC may be a member of only one bond interface.

NOTICE: Converting an existing “Multi-Armed” SBC to “Single-Armed” is not supported since IP routing must be disrupted for a network conversion using the same IP subnet. If such a configuration change is required it must be performed within a maintenance interval.

IMPORTANT: For IPv4 or IPV6, the CIDR format for subnets is valid only for the settings whit no separated fields for subnets, i.e white/black list IPs.

IMPORTANT: **Single armed** is disabled.

5.3.1.2 Interface Configuration

A realm is a network interface definition for the OS-SBC to allow addressing one or more external network interfaces.

Realms are identified and organized according to their application to support customer local network communications in the core realm or in the access realm, a few examples are peer network interfaces, SSP’s, branch offices, or remote endpoints.

The user must select the **Add** button to add a new network interface to the desired realm. The user may edit the new or existing network interface for the access or core realm by first selecting the row entry followed by the cell.

To delete an existing network interface select the row entry followed by the **Delete** button.

NOTICE: If the user attempts to remove a network interface, a cross check is performed to ensure all realm profile references to the network interface being deleted have been removed before it is allowed to save the configuration.

Configuring the OS-SBC for Dual-IP version support, i.e., both IPv4 and IPv6, is performed by configuring a row entry for each IP address version using a unique Network-ID. The IP address version for the entry is determined by the format of the provisioned IP Address field.

In the following steps physical interfaces are associated with logical network interfaces which are associated with the access or core realm.

NOTICE: For new install or upgrade, the default configuration is the following:Core Realm network interfaces are associated with eth0.

Access Realm network interfaces are associated with eth1.

Core realm configuration

IMPORTANT: For **Hosted OpenScape SBC** (hSBC) on **OS4K** Deployments, **Core realm** is not configurable.

- **Type**

  The drop down tab is used to identify the network interface usage. The selectable values are:

  – **Main IPv4**
  – **Main IPv6**
  – **Non-VLAN IP**
- **Network ID**

  A a network interface is referenced by its Network-ID which includes a physical network interface association. Each network interface is identified by its type.
- **Interface**

  Only eth0 physical network can be configured for Core realm network interface associations.
- **IP Address**

  The IP address (IPv4 or IPv6) associated with the private side of the network, used to provide multiple communication paths to OpenScape Voice.

  IMPORTANT: IPs 198.18.0.0/15 cannot be used for LAN (Core) IP address - they are reserved for Network Interconnect Device Benchmark Testing [RFC3330].
- **Subnet mask**

  The subnet mask (IPv4 or IPv6) of the interface.
- **VLAN tag**

  This information is used to establish remote media server connections.
- **Signaling** and **Media**

  All core realm network interfaces SHALL support both signaling and media by default as there is no separation of signaling and media. Both ‘Signaling’ and ‘Media’ selections are shown as preselected and grayed out indicating no change is possible.

- The Signaling ports for access realm network interfaces provisioned to support signaling, are configurable. This information is used for routing traffic into the core network. Traffic is secured using UDP, TLS over TCP.
  - **SIP UDP**
  - **SIP TCP**
  - **SIP TLS**
  - **SIP MTLS**
  - **MGCP** - The access realm MGCP port (client) MUST be configured to 2727.

- **External Alias IP**

  Packets sent to Alias IP will be forwarded to Core Main IP, Packets sent from Core Main IP to OSV (Node1 or Node2) will be sent with source as Alias IP. This configuration is only relevant for Trunk SBC.

Access and Admin realm configuration

- **Type**

  The drop down tab is used to identify the network interface usage.

  When **Single armed** is not set, the selectable values are:

  - **Main IPv4**
  - **VLAN IP**
  - **Main IPv6**
  - **Non-VLAN IP**
  - **Main admin IPv4**

  When **Single armed** is set (enabled), the selectable values are:

  - **SA Main IPv4**
  - **SA Main IPv6**
  - **Non-VLAN IP**
  - **VLAN IP**
  - **Forward Main -** The IP address field is populated with the IP address of Main_IP and can't be changed.**VLAN tag** is set to 0, Signaling and Media checkboxes are unchecked and cannot be checked. A port must be set in at least one of the columns reserved to protocol.
  - **Forward Non VLAN -** The IP address field must be entered, **VLAN tag** is set to 0, Signaling and Media checkboxes are unchecked and cannot be checked. A port must be set in at least one of the columns reserved to protocol.
  - **Forward VLAN -** The IP address field must be entered, the **VLAN tag** must be entered with a value different to 0,Signaling and Media checkboxes are unchecked and cannot be checked. A port must be set in at least one of the columns reserved to protocol.

    IMPORTANT: Only two non Main Access realms can be used with UDP Port.

- **Network ID**

  Each network interface is identified by its type. Up to 10 network-ID’s are supported and hence unique IP addresses for the default non-VLAN tagged network **(VLAN=0**). These entries can be included within the ‘Main-Access-

IPvX' network and thus share the same IP address. Their membership in the 'Main-Access' network is identified by being provisioned with Network-ID = 'Main-Access-IPvX', same 'IP Address', however all signaling ports must be unique between entries of the same IP version.

- **Interface**

  Physical Network Interface, eth0, eth1, eth2, eth3, assigned to the network interface. The realm association to a physical interface is chosen whenever an initial network interface is assigned. The exception to this rule is eth0 since it can only be used for the core realm.

  NOTICE: Once a NIC <-> OS-SBC realm association is established, it SHALL not be possible to associate with another realm.

- **IP Address**

  The Local IP address (IPv4 or IPv6) associated with the public side of the network, used to provide multiple paths for load distribution to collocated and geo-separated nodes and access to multiple networks.

  IMPORTANT: IPs 198.18.0.0/15 cannot be used for WAN (Access) IP address - they are reserved for Network Interconnect Device Benchmark Testing [RFC3330].

- **Subnet**

  The subnet mask (IPv4 or IPv6) of the interface.

- **VLAN tag**

  This information is used to establish remote media server connections.

- **Signaling** and **Media**

  By default, all network interfaces are configured to support Signaling and Media. Signaling and media separation is allowed by removing the selection from the checkbox.

- The Signaling ports for access realm network interfaces provisioned to support signaling, are configurable. This information is used for routing traffic into the core network. Traffic is secured using UDP, TLS over TCP.
  - **SIP UDP**
  - **SIP TCP**
  - **SIP TLS**
  - **MGCP** - The access realm MGCP port (client) MUST be configured to 2727.

- **SIP Server**

  SIP Server Node (OSV) in the core realm.

- **Message rate limit**

  Message rate limit per second. Allowed values are 5,10, 25,50,75 and 100. Default is 100.

- **Trust Level**

  Statically configured remote endpoints have a higher level of trust as compared to dynamic registration remote subscribers. The available options are:

  – **N/A** (default)
  – **Medium**
  – **Minimal**
- **Signaling Restriction**

  It SHALL be possible to optionally configure signaling restrictions for access realm network interfaces provisioned to support signaling. The available options are:

  – **Unrestricted** (default) – Signaling SHALL be allowed without any restrictions as to what type of OS-SBC routing or identity object.
  – **Remote Subscriber** – Only dynamic registration SIP devices SHALL use this network interface.
  – **Remote Endpoint** – Only statically configured remote endpoints SHALL use this network interface.

  NOTICE: A cross check SHALL be performed when modifying signaling restrictions. The cross check is performed to ensure all OS-SBC routing and identity objects associated with the same network interface have the same restrictions.

Realm Profile

5.3.1.3 Realm Profile

Realm profiles associate signaling and media network interfaces with network realms to support multimedia sessions. Once a realm profile is defined, routing and identify objects may be configured to identify their realm association to support signaling and media flows between the OS-SBC access and core realm network interfaces.

The user may add a new realm profile, edit an existing realm profile in-line or delete a realm profile row entry. The user follows the same in-line edit options as used in other network services configuration sections.

Each realm profile section row has the following fields:

- **Realm Profile** - A unique identity to identify the realm profile.**Network ID** must be associated to a new realm profile that will be used in the remote endpoint configuration.

  Available options:

  – **Main-Core-Realm-ipv4**
  – **Main-Access-Realm-ipv4**
  – **Second_Access**
  – **Third_Access**
- **Realm** - Identifies the realm the realm profile is associated; either Access or Core may be selected, e.g., from a pull-down list.

- **Signaling Network-ID** - The user is presented a list of signaling capable Network-ID's for selection. Alternatively the user may be provided a list of Network-ID's filtered by the chosen association.
- **Media Network ID** - By default, selecting a signaling and media capable network interface in the **Signaling Network-ID** provisioning step shall automatically show the same Network-ID as a preferred selection for this field.
- **Forward Network ID** - Forward network ID ties a Realm profile to an existent Forward VLAN.Tt is mandatory to have an entry in Realm Profile for each configured Forward VLAN.

NOTICE: Before a realm profile deletion Is allowed to proceed, a crosscheck SHALL be performed to ensure that there are no existing associations or relationships with routing or identify objects.

NOTICE: When creating a Realm Profile: if a forward non-vlan Network is to be used (even if different network interfaces are used) such network must be configured only as the **Forward network id** and the Signaling network ID must be **Main Access network ID**.

5.3.1.4 Routing

Default gateway address

This defines the IPv4 address to be used as Gateway

Default gateway IPv6 address

This defines the IPv6 address to be used as Gateway

Routing configuration

A new route is added using the **Add** button. In this case a new row in the routing table is created and is possible to configure the **Destination** IP address, **Gateway** IP address, network mask (ie. **Netmask**) and choose which **Interface** will be used to route the IP packets.

To delete a route select the route and then use the **Delete** button.

Once the routes are entered or deleted the **OK** button will save the configuration and the window will close. To apply this configuration the user must click on **Apply Changes** button.

5.3.1.5 Redundancy

Redundancy uses a non-proprietary protocol which is used to increase the availability of the SBC. This is based on a virtual IP address in the same subnet of the SBC used for redundancy. The check box enables the Redundancy protocol.

IMPORTANT: For **Hosted OpenScape SBC** (hSBC) on **OS4K** Deployments, **Redundancy** is disabled.

Enabling/Disabling Redundancy

It is recommended to change the default redundancy password on each node separately before enabling the Redundancy; otherwise the system will fail to replicate the configuration to the other node. Both nodes must use the same redundancy password. Data synchronization will also fail if different software versions run in the system. After configuring the redundant system, the passwords are included in the data synchronization. When changing the redundancy password in the master node, the previous password is used in the backup node until data synchronization. After the synchronization, the redundancy password is updated.

To enable Redundancy, it is necessary to configure the IP address of Nodes 1 and 2 and configure the redundant virtual IP address.This operation requires a system restart. After restaring the system, configuration of Node 1 is automatically replicated to Node 2 (redundancy is automatically enabled on Node 2). Once Redundancy is enabled, configuration is allowed only on the master node.

To disable the Redundancy is required to configure Node 1 and Node 2 separately as the following. First configure a temporary IP in the Master node and uncheck the Redundancy Enable check box, so the system will restart with Redundancy disabled and the other system will unable to take the control (unable to reach the system as the IP address was changed). The other node will remain in Backup state for about 9 minutes and then will become the Master node. Now it is possible to change the configuration on this node, so configure a temporary IP and uncheck the Redundancy Enable check box (system will restart). Now both systems are operating with Redundancy disabled and it is possible to return back the IP configuration.

Upgrading a redundant system

The Local GUI/CMP shows the upgrade progress only while upgrading the Master node. The upgrade completion on the other node must be further verified by checking the software information (version).

The upgrade process is started in the Master node. Once the upgrade in the Master node is finished the system will reboot (after the user confirmation or via scheduled upgrade) and the Backup node will become the Master. When the previous Master node is running again, it will become Master and will validate the software. An alarm of invalid SW version will be raised. Then after about 5 minutes the SW image will be uploaded to the former Backup node. After the upload is finished the Backup node will start the upgrade, once the upgrade is complete this system reboots. When the Backup node is running again both nodes now have been upgraded and the process is finished.

The estimated time for the redundancy system to be stable is about 20 minutes.

Settings that require a reboot on a redundant system

Once the change that requires a reboot (hostname, NTP, etc) is applied on the Master node, it will reboot and the Backup node stays in Backup waiting for the Master node to reboot and validate the database. After that, the Master node will copy the database to the Backup node, which will reboot.

The estimated time for the redundancy system to be stable is about 5 minutes.

Unbalanced Redundancy

In order for two nodes to be a redundant OS-SBC system, both nodes must have the same hardware configuration. However, in versions after V11R0.02.00-1, it is possible to create a new type of redundancy, called **Unbalanced Redundancy**. In this type of redundancy, the user can pair two different types of hardware, given it's one of the combinations that are listed below:

x3250	sr250
x3550	sr530
x3550	sr630
sr530	sr630

5.3.1.6 Core Link Connectivity Check

Core Link Connectivity Check

This tab is used to setup specific IPs to check in case there is a connectivity issue, in order to initiate switch from an active to a backup node.

- **Core link connectivity check IP address** - This field is used by the Redundancy Manager to check the LAN access of the Node. It will ping this server and if it is down then it can be used to change the state from active to backup node.

  It must be set to an IP that is always active in the network. Normally, it is set to the **Default Gateway**.
- **Enable access link connectivity check** - This check box allows the address in the field **Access link connectivity check IP address** to be used to check the WAN state by the Redundancy Manager. As with the field **Core link connectivity check IP address**, this IP address can be used to trigger a change from master to backup node if the link is down.
- **Enforce call context mirroring based on LAN MTU size** - This is only enabled after Support Team request, to avoid fragmentation of packages during the synchronization of data between two Redundant Nodes. It must be left disabled.

5.3.1.7 External Health Check

External Health Check

This tab controls the external visibility of the Health Check server as well as the http port that will be used.

- **Enable External Health Check** - When enabled, an external agent (already allowed in the firewall rules) can check the server state and take actions based on the answer (e.g.: a Load Balance server can divert the traffic to this server).This checkbox makes the server available in the LAN and WAN interfaces
- **Listening Port** - The http port of the Health Check Server

5.3.2 DNS

Client

This box configures the DNS client functionality.

- **Refresh DNS** - Allows the user to manually refresh the DNS client (restarting the service).
- **DNS server IP address** - List of DNS server IP addresses to be used by this client (maximum of 3 DNS servers).
- **Alias list** - List of aliases to be used by this client.

Server

- **Enable DNS server**

  This check box enables the internal DNS Server service.
- **DNS configuration**

  This button opens a window to configure DNS Server parameters (Refer to: DNS Configuration > DNS Server).
- **Enable Customization**

  checkbox allows the user to upload files to customize configuration of DNS under the **Administer Custom files** (refer to: DNS > Administer Custom DNS Files). Depending on the custom configuration several files may require upload e.g. zones configuration.

IMPORTANT: The syntax and the contents of the file(s) will not be checked, so wrong configuration may cause the DNS service to not start. When the Customization is enabled, the DNS server configuration through the local management will be disabled. The custom files configuration will be preserved in case of upgrades.

IMPORTANT: The DNS custom file must be backed up to survive a re-installation of the SBC. Backup of the custom file will be included in the "Export all" function. After a re-installation of the SBC, the custom files must be restored to the SBC in a similar manner to how the XML configuration file is restored. The files must then be manually uploaded back into the custom files list.

5.3.2.1 DNS Configuration > DNS Server

This window allows the configuration of the DNS parameters to enable the DNS Server service.

Zone Configuration

- **Type** - The zone type (slave or forward) to be configured.
- **Zone name** - The zone domain name.
- **IP masters/forwards** - The IP address or IP address list (separated by commas) for the configured zone type. When the Zone type is configured as forward, the IP address should be included in the Forward IP List.

- **File name** - The file to read the name server from (required field when zone type is slave).

Forward IP

- **Forward IP address list** - List of IP addresses for the DNS server to forward queries to. It's not necessary to configure the DNS Client if the Forward IP is configured. It doesn't necessarily query the forwarders in the order listed; it chooses which one to query first based on roundtrip time.

5.3.2.2 DNS > Administer Custom DNS Files

This window allows custom configuration of the DNS via uploading and deletion of custom DNS.

5.3.3 NTP > NTP Settings

The **Timezone** drop list defines which timezone will be used in Branch.You are able to choose timezones by region (e.g. Europe, Africa, Asia, etc.),provided by the **Region** drop list. The **Timezone** drop list provides the list of timezones in a selected region.

NOTICE: The **Timezone** shows the current offset. If the current date is inside the DST period it will show the DST (Daylight Saving Time) offset.

Enable local NTP server check box is used to activate the local NTP server. In this case both: manual or synchronized time settings are allowed.

Manual configuration is used to set the Date and Time manually. Click in the Apply button to set it up. This button is visible only if Manual configuration is checked. The timezone as well as date and time are read from the system. In case of no timezone is configured, then it is read from the xml database.

Synchronize with NTP server is the option used when a NTP server is available. In this case the server address must be entered in the NTP server box. Any IP is valid, except 0.0.0.0 and 255.255.255.255

The **Synchronize now** button is used to Synchronize manually with the NTP Server without doing **Apply Changes**. It must be used when the system is already using a NTP Server (It does not set up anything, just uses the current ntp.conf).

When in "Manual configuration" mode, timezone changes are applied when clicking in "Apply" button and then confirming it.

When in "Synchronize with NTP server" mode, timezone changes are applied when clicking in "Apply Changes" button and then confirming it.

Due to issues in Apache Session Timeout and Postgres database a reboot happens in case of changes that apply a new configuration manually or modify the NTP Server/timezone.

NOTICE: Beginning with V8 Pkg1 it is possible to configure up to 3 NTP servers all with IPV4 or IPV6 (It is not possible to mix IPV4 and IPV6 addresses). Additionally,

-"Synchronize now" executes the command "ntpq" for all configured NTP servers.

-If flag "Enable Local NTP Server" is checked and DHCP server is enabled then all configured NTP servers will be sent to all DHCP clients. #

IMPORTANT: For **Hosted OpenScape SBC** (hSBC) on **OS4K** Deployments, **NTP** is disabled

NOTICE: If Redundancy is active, system will use physical IP for NTP queries. So, for slave synchronization the physical IP of both Master and Slave OpenScape SBC must be added to NTP Server firewall list.

5.3.4 Traffic Shaping

Enable traffic shaping

To enable the traffic shaping the user has to check the selection box.

Traffic shaping configuration (Add)

This button opens a new window/tab where is possible to configure traffic shaping. A new class of traffic is added using the add button. In this case a new row in table is created and the parameters can be configured in this new row.

The meaning of the parameters is defined as following:

- Parent class ID: Is a hexadecimal number in range 0-FFFF, representing the ID for the traffic parent class.

  Please note that should be at least one row without the Parent Class ID set, because that row is the parent for others.
- Class ID: Is a hexadecimal number in range 0-FFFF, representing the ID for the traffic class.

  Please note that the Parent Class ID and the Class ID cannot be equal.
- Interface: Select the interface to apply the shaping.
- Default: This (optional) parameter sets the default class ID where the unclassified packets will go. The default class ID 0 is used as an internal fifo queue that passes packets at full speed.
- Description: An arbitrary string used to describe a class in symbolic way.
- Rate: This mandatory parameter defines how much bandwidth will be allocated for the class. Traffic going through the class will be shaped according to the specified rate. Values are defined in Kbit, Mbit or bps.
- Ceiling rate: This is an optional parameter used to set the maximum bandwidth to be used by the class. The difference between Ceiling Rate and RATE amounts to bandwidth the class can borrow, if there is unused bandwidth. By default, Ceiling Rate is equal to Rate so the class can't borrow bandwidth.

- Burst: Optional parameter used to define how many bytes can be sent from one class at full speed before trying another class. Values are defined in Kbytes (Example 1Kb).
- Ceiling burst: Also an optional parameter, that sets the maximum value of the burst. Values are defined in Kbytes (Example 1Kb).
- MTU: is an optional parameter that defines the maximum packet size. The default is 1600 bytes. Values are defined in bytes.
- Priority: This numeric parameter is used to define the priority of class traffic. The higher is the number, the lesser the priority. Classes with higher priority are offered excess bandwidth first. The priority is optional, the default value is 0.
- Leaf queuing: Optional parameter set by default to none, this parameter defines the leaf queue discipline to HTB. Possible values are: None, Sfq, Pfifo and Bfifo
- SFQ quantum: This is an optional parameter that defines the amount of data in bytes a stream which is allowed to dequeue before next queue gets a turn. A default is set to one MTU-sized packet. Do not set this parameter below the MTU!
- SFQ perturbation: This optional parameter defines how many seconds are allowed for a period of hash function perturbation. The default value is set to 10.
- Packet Fifo limit: This is an optional parameter which defines the number of packets that the queue can hold. The unit is number of packets.
- Byte Fifo limit: This is an optional parameter which defines the number of bytes that the queue can hold. The unit is number of bytes.
- Rule filters: These parameters build the "u32" filter rules that select traffic for each of the classes. The rules are separated by a semi-colon. The rule syntax is as following:

  RULE = [[source [/prefix]] [: port [/mask]],] [destination [/prefix]] [: port [/mask]]

  Examples:

  RULE=10.1.1.0/24:80

  Selects traffic going to port 80 in network 10.1.1.0
- Mark filters: These parameters set the firewall filter rules that select traffic for each of the classes according to firewall "mark". Mark is a decimal number packet that is tagged if firewall rules apply to. The marks are separated by a semi-colon. Marks for different filter types can be combined.

5.3.5 QoS Settings

Enable QoS Configuration

The QoS is enabled by using this check box.

IMPORTANT: If the Border Control Function (BCF) feature is enabled, this check box is by default enabled and the values for SIP/MGCP/Audio RTP and VideoRTP are fixed. Other rules can be added in the grid.

DSCP for SIP

DSCP value to be set in the IP packets of SIP protocol sent by the SBC SIP Server.

DSCP for MGCP

DSCP value to be set in the IP packets of SIP protocol sent by the SBC SIP Server.

DSCP for RTP (Audio)

DSCP value to be set in the IP packets of RTP protocol sent by all traffic except Circuit.

DSCP for RTP (Video)

DSCP value to be set in the IP packets of RTP protocol sent by the SBC Media Services.

QoS configuration table

A new line in QoS table is created using **Add** button, in this case a new QoS rule can be configured. It can set the DSCP value for IP packets filtered according to the configured parameters and/or set the mark for traffic shaping. The QoS rule is deleted from table using **Delete** button.

- **Protocol** - This box defines the protocol for the QoS rule.
- **In interface** - This box defines the incoming interface for the QoS rule.
- **Out interface** - This box is used to configure the outgoing interface for the QoS rule.
- **Port** - This box defines the port or a port range (start_port:end_port) for the QoS rule (input or output).
- **DSCP** - This box defines the DSCP value to be set in the IP packets for the QoS rule.
- **Mark** - This box defines the mark for the QoS rule in order to use with traffic shaping.

NOTICE: DSCP values of QoS configuration table rule can overwrite the values set by SIP and RTP protocols when conflicting rules are set.

The DSCP field is a 6-bit field which is defined in RFC2474. Should use values in the range from 0 to 64. For information, the current association is as follows:

Name	Space	Reference	Decimal
CS0	000000	[RFC2474]	0
CS1	001000	[RFC2474]	8
CS2	010000	[RFC2474]	16
CS3	011000	[RFC2474]	24
CS4	100000	[RFC2474]	32
CS5	101000	[RFC2474]	40

Name	Space	Reference	Decimal
CS6	110000	[RFC2474]	48
CS7	111000	[RFC2474]	56
AF11	001010	[RFC2597]	10
AF12	001100	[RFC2597]	12
AF13	001110	[RFC2597]	14
AF21	010010	[RFC2597]	18
AF22	010100	[RFC2597]	20
AF23	010110	[RFC2597]	22
AF31	011010	[RFC2597]	26
AF32	011100	[RFC2597]	28
AF33	011110	[RFC2597]	30
AF41	100010	[RFC2597]	34
AF42	100100	[RFC2597]	36
AF43	100110	[RFC2597]	38
EF PHB	101110	[RFC3246]	46

As stated by the current IANA assignment, the DSCP is divided in three pools:

Pool	Codepoint Space	Registration Procedure	Note
1	xxxxx0	Standards Action	
2	xxxx11	Experimental or Local Use	Reserved for experimental or Local Use
3	xxxx01	Experimental or Local Use	May be utilized for future Standards Action allocations as necessary

5.4 VOIP

In this administrative area the user can configure the VOIP parameters.

Some configuration here will cause the SIP Server restart, active and ongoing calls may fail.

5.4.1 SIP Server Settings

General

- **Comm System Type**

  The Comm System Type (mode) determines how SBC is connected to the Comm System network.

  – **Simplex** is a single node configuration.
  – **Active-Active**(formerly Collocated) mode in SBC means Active-Active load balancing configuration of Comm System i.e. traffic coming in on Access IP 1 goes to Comm System node 1 and traffic on Access IP 2 goes to Comm System node 2.

  NOTICE: When in **Active-Active** mode, additional Access IP configuration is a must for load balancing. If load balancing is not needed, then **Simplex** or**Active-Standby** mode for Comm System must be used.

  NOTICE: UDP between Clustered Server Node (OS4000 or OSV) and SBC is not allowed when Remote Endpoint is configured due to performance issues and memory usage, so this configuration shall be restricted to TCP (TLS) for cluster same as for non-cluster configurations.

  IMPORTANT: For **Hosted OpenScape SBC** (hSBC) on **OS4K** Deployments,**Active-Active** is disabled.

  – **Active-Standby** mode means that two nodes are in different locations. If the configuration is other than Simplex the secondary server will be enabled.

  NOTICE: If the configuration is set to **Active-Active** or**Active-Standby**, the **Primary server** field for Node 2 will be enabled.

  IMPORTANT: For **Hosted OpenScape SBC** (hSBC) on **OS4K** Deployments,**Active-Standby** is disabled.

  – **Clustered** mode means it is possible to define groups of SIP server nodes on the core side. Each group (cluster) may contain one or more SIP servers. The SBC routes incoming requests from the access side to one of the defined clusters on the core side based on either the access

interface that the request was received or based on the best match of the request URI user part, prefix codes and priority configured per group.

For **Clustered** mode, the Routing prefix does not use regular expression. It just checks the prefix and uses the best match criteria.

The validation is described in RFC3986 for userinfo:

```
userinfo = *( unreserved / pct-encoded / sub-delims)

unreserved = ALPHA / DIGIT / "-" / "." / "_" / "~"

ALPHA = A-Z | a-z

DIGIT = 0-9

pct-encoded = "%" HEXDIG HEXDIG

sub-delims = "!" / "$" / "&" / "'" / "(" / ")" / "*" /
"+" / "," / ";" / "="
```

The SBC performs **Load Balancing** between the nodes if a specific configuration happens. **Load Balancing** will happen only between the nodes that have the same routing prefix, same priority and are in the same group name (if in a group there is nodes with same prefix and priority and nodes with different prefix & priority the load will not happen).

NOTICE: Clustered mode is useful in the case of supporting multiple HG3500 gateways / OpenScape 4000s via SIP.

IMPORTANT: Under**Network/Net Services** >**Settings** > **Access and Admin realm configuration** > **Sip Server**, if**Any** is configured, then the system will ignore the group name from the cluster screen configuration, meaning that all the nodes will be part of the same group even with different group names.

– **Standalone with internal SIP Stack**: In this mode, the B2B-Controller can function as a B2BUA and support the BYOT (Bring Your Own Trunk) feature. BYOT enables the SBC to route and establish calls between endpoints without requiring an external SIP server. In this mode, the server configuration is disabled, and Direct Routing Configuration is enabled.

- **Allow Register from SERVER**

  Select the checkbox, if the remote endpoint is allowed registration via the server.

- **Use RURI to Route to Comm System**

  Select this checkbox to route the calls to the Communication System server nodes based on RURI.

NOTICE: Note that, when this flag is set, the SIP messages containing a RURI with FQDN will be only routed to the Communication System if the FQDN matches the clustered servers FDQN.

- **Bond TCP connections to SLB**

  Select this checkbox in order to reuse the TCP connections.
- **Clustered Servers**

  Press the **Clustered Servers** button to open the Clustered Servers configuration window.
- **Other Trusted Servers**

  This configuration edits the list of trusted SIP Servers from which Requests can be accepted.

Node 1

- **Target type**

  The target type determines how OpenScape SBC will use the WAN outage server address.
- – **Binding** the address will be either IPs or FQDNs.
  – **SRV record** DNS-SRV Record query will search the address automatically (SRV Record field) using the respective Transport (Transport field). The network administrator shall configure the priority of the SIP Server according to the network configuration.

  NOTICE: If the configuration is Binding then the **SRV record** field will be grayed-out and the user has to enter in the Primary and Backup (depending on Comm System mode) the IP or FQDN, the Transport and the Port (the last fields are mandatory).

- **Primary server**

  The IP address (IPv4 or IPv6) of the Node 1 server.
- **Transport**

  Select a SIP protocol used to communicate with the Node 1 server.
- **Port**

  Used SIP port for the Node 1 server.
- **SRV record**

  IP address to retrieve the SRV (Service) record from.

Node 2

- **Target type**

  The target type determines how OpenScape SBC will use the WAN outage server address.
- – **Binding** the address will be either IPs or FQDNs.
  – **SRV record** DNS-SRV Record query will search the address automatically (SRV Record field) using the respective Transport (Transport field). The network administrator shall configure the priority of the SIP Server according to the network configuration.

  NOTICE: If the configuration is Binding then the **SRV record** field will be grayed-out and the user has to enter in the Primary and Backup (depending on Comm System mode)

the IP or FQDN, the Transport and the Port (the last fields are mandatory).

- **Primary server**

  The IP address (IPv4 or IPv6) of the Node 2 server.
- **Transport**

  Select a SIP protocol used to communicate with the Node 2 server.
- **Port**

  Used SIP port for the Node 2 server.
- **SRV record**

  IP address to retrieve the SRV (Service) record from.

Clustered Nodes settings

- **Ping Method**

  Available options: OPTIONS, INFO, REGISTER, NOTIFY, UPDATE.
- **Failure threshold (pings)**

  This is the number of failure attempts that SBC counts until it is considered a node failure.
- **Success threshold (pings)**

  This defines the number of positive responses to wait until consider a node active again.
- **Transition mode threshold (pings)**

  This is the number of failure attempts during Transition Mode that SBC will count until switch to Survivable Mode.
- **OPTIONS interval (sec)**

  This box defines the time interval to send OPTIONS to the server.
- **OPTIONS timeout (sec)**

  This box defines the timeout when waiting for 200OK from SIP server.
- **Notification rate (per sec)**

  This is the number of notifications per second sent to phones after state transition.
- **No Destination Error Code**

  Select which error response will be sent in case no destination is available when in Clustered Server mode. Available values are:

  – 403 Forbidden (Default option)
  – 480 Temporarily Unavailable
  – 503 Service Unavailable

5.4.1.1 Clustered Servers

Clustered mode means it is possible to define groups of SIP server nodes on the core side. Each group (cluster) may contain one or more SIP servers. The SBC routes incoming requests from the access side to one of the defined clusters on the core side based on either the access interface that the request was received or based on the best match of the request URI user part, prefix codes and priority configured per group.

For **Clustered** mode, the Routing prefix does not use regular expression. It just checks the prefix and uses the best match criteria.

The validation is described in RFC3986 for userinfo:

```
userinfo = *( unreserved / pct-encoded / sub-delims)

unreserved = ALPHA / DIGIT / "-" / "." / "_" / "~"

ALPHA = A-Z | a-z

DIGIT = 0-9

pct-encoded = "%" HEXDIG HEXDIG

sub-delims = "!" / "$" / "&" / "'" / "(" / ")" / "*" /
"+" / "," / ";" / "="
```

The SBC performs **Load Balancing** between the nodes if a specific configuration happens. **Load Balancing** will happen only between the nodes that have the same routing prefix, same priority and are in the same group name.Each node is possible to configure with **Group Name**, **Prefix Codes**, **Node Name**, **IP/FQDN**, **Port**, **Transport Protocol**, **Stick with CommServer** and **Priority**.

IMPORTANT: Under **Network/Net Services** > **Settings** > **Access and Admin realm configuration** > **Sip Server**, if **Any** is configured, then the system will ignore the group name from the cluster screen configuration, meaning that all the nodes will be part of the same group even with different group names.

NOTICE:

The transport type must be the same for all clustered servers.

5.4.1.2 Other Trusted Servers

This configuration edits the list of trusted SIP Servers from which Requests can be accepted.

The list should include only IPs from trusted servers, not gateways, phones and others.

- **IP address or FQDN** - This is the configuration of the IP address or Fully Qualified Domain Name of the trusted server.
- **Port** - This box is used to configure the SIP port of the trusted server.
- **Transport** - This combo defines the SIP transport protocol to be used in communication with the trusted server.

NOTICE: The sipsm1 address should not be added to trusted servers if sipsm3 (MTLS) address is used.

5.4.1.3 Direct Routing Configuration

Routing groups

In this session it is possible to configure all remote endpoints groups with routing rules and link them.

Group settings

- **Group name**

  Configures the remote endpoints group name to be added using the "Add group" button.
- **Group selected**

  Select the group to be configured or deleted. Use the "Delete group" button to delete the group.
- **Group for endpoints**

  Define the endpoints group type (MS Teams, SSPs, Gateway, and Proxy) to be listed in the endpoints list. "MS Teams" refers to endpoints of type SSP and MS Teams profile. "SSPs" refer to endpoints of type SSP without the profile MS Teams.
- **Relates to group**

  Links the group to another group. You can add the association to the routing table by using the "Add to routing table" button.

NOTICE: The following combination of types are allowed for group association:

– MS Teams with SSP, and vice-versa.
– Gateway with SSP, and vice-versa.
– Proxy with SSP, and vice versa.

Routing table

Table with all remote endpoints' groups association. Use the "Delete routing" button to delete the selected associations from the routing table.

- **Endpoints for group**

  Configure the remote endpoints for the selected group and add routing rules to the endpoints.

  The **Endpoints list** allows selecting the endpoints to be added to the group using the "Add" button. Use the "Delete" button to remove the selected endpoints.

  For each endpoint it is presented the name, address, port, and transport. The priority, FQDN Routing, and Regex can be configured to reach the endpoint. The priority field defines the order of endpoints that will be selected when more than one rule matches the rule. FQDN Routing indicates the R-URI domain that should match to reach the endpoint. Regex is the regular expression in ES6 pattern for the user part of the R-URI that should match to

reach the endpoint. The FQDN Routing and Regex are optional, and empty values indicate that they will not be checked.

Examples:

INVITE URI is
`sip:98765432@abc.msteams.com:5061;transport=tls`

- FQDN is set to `abc.msteams.com`, and Regex is empty - Endpoint is selected because FQDN matches
- FQDN is set to `def.msteams.com`, and Regex is set to `^9876` - Endpoint is not selected because FQDN does not match.
- FQDN is empty, and Regex is set to `^9876` - Endpoint is selected because Regex matches.
- FQDN is empty, and Regex is set to `^4567` - Endpoint is not selected because Regex does not match.
- FQDN is set to `abc.msteams.com`, and Regex is set to `^9876` - Endpoint is selected because FQDN and Regex match.
- FQDN and Regex are empty - Endpoint is selected because FQDN and Regex are not checked.

More than one endpoint can be selected and, in that case, the priority will define the routing order. Lower values have higher priority. Additionally, rerouting can occur if the endpoint or endpoints with higher priority fail.

When more than one endpoint with the same priority is selected, b2b-controller will sort the endpoints by the endpoint with the longest unused time.

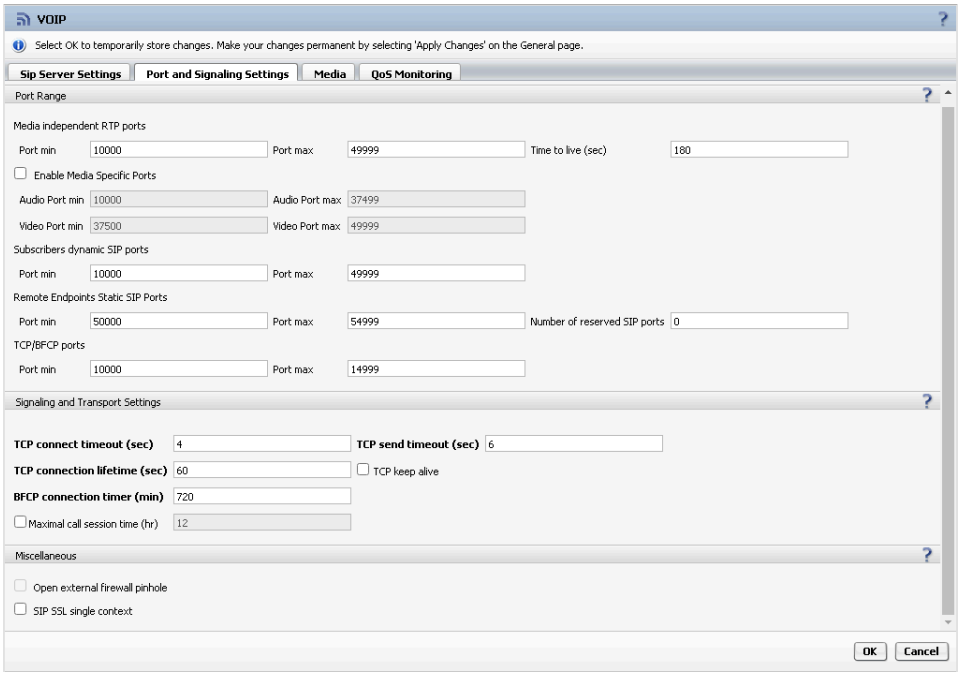
Unavailable endpoints (Failed by SSP OPTIONS connectivity check) are not included in the selection of endpoints for routing.

Timers and Thresholds

SSP OPTIONS timeout (ms): the duration after which a SSP server will drop a SIP session if it remains inactive.

5.4.2 Port and Signaling Settings

Configuration of the Core and Access Port Range, Signaling and Transport, and Miscellaneous items.



5.4.2.1 Port and Signaling Settings > Port Range

Port Range Core Side/Port Range Access Side

For Single Armed operation, the ranges will be configured separately for Core and Access side, following the same range rules.

- **Port min** - define the minimum RTP (Real-time Transport Protocol) port threshold to be used in RTP traffic. Valid values for Min and Max are between 10000 and 65000. A port range with only 2 ports is not allowed.

  IMPORTANT: For Single Armed operation, the ranges will be configured separately for Core and Access side. **Port Range Core Side**: from `10.000` to `19.999` and **Port Range Access Side**: from `20.000` to `49.999`.

- **Port max** - define the maximum RTP (Real-time Transport Protocol) port threshold to be used in RTP traffic.

  IMPORTANT: For Single Armed operation, the ranges will be configured separately for Core and Access side.**Port Range Core Side**: from `10.000` to `19.999` and **Port Range Access Side**: from `20.000` to `49.999`.

- **Time to live (sec)** - the disconnection timer for non RTP activity. It can range between `180` and `1200` seconds, default is set at `180`. This field is valid for the Proxy, when G729/sRTP is enabled.
- **enable Media Specific Ports** - You may optionally specify media specific RTP port ranges by selecting **Enable Media Specific Ports**. Once checked, the media specific Audio / Video RTP port ranges (**Audio Port min**, Audio Port max, Video Port min, **Video Port max**) are enabled, and the existing media independent RTP port range fields are disabled (grayed out). These fields allow entry of the port range to be supported for Audio and Video

media streams. Default for Audio at Core side is from 10.000 to 23.749 and for Audio at Access side is from 23750 to 37499. For Video, the default for Core side is from 37500 to 43749 and for Access side is from 43750 to 49999.

If the **Enable Media Specific Ports** is disabled, the Audio and Video min and max RTP port ranges are disabled (grayed out).

Subscriber dynamic SIP ports

These boxes defines the SIP port range to be used in SIP messages. The valid value for Min and Max is between 10000 and 65000.

NOTICE: Port range must be higher than or equal to 500 ports.

IMPORTANT: If the range has been changed, the port mapping will be cleared and active calls will be affected. All subscribers must register again.

Remote EndpointsStatic SIP ports

These boxes define the SIP port range to be used as core port of remote endpoints. The valid value for Min and Max is between 50000 and 54999.

NOTICE: Port range must not overlap other ranges for instance subscribers dynamic SIP ports.

- **Number of reserved SIP ports** - This field defines the pool of remote ports for endpoints that is created previously avoiding the restart of SIP Server in case the new endpoints are created/removed or changed. The maximum number allowed to reserve sip remote endpoint static ports is 1000.

  If an endpoint configuration is changed, added or deleted and the Core realm port of this endpoint is within the range of Port min (remote Endpoints Static SIP Port) plus the number of reserved SIP ports configured, then the restart of SIP Server is not executed and the already established calls will not be tear down.

TCP/BFCP ports

The text boxes contain the minimum and maximum destination ports that are allowed to allocate a TCP/BFCP connection. The OSS shall set the following default ranges:

- **Port min =** 1000
- **Port max =** 14999

5.4.2.2 Port and Signaling Settings > Signaling and Transport Settings

TCP connect timeout (sec)

Time in seconds before an outgoing attempt to connect will be stopped.

TCP send timeout (sec)

Time in seconds after a TCP connection will be closed if it is not available.

TCP connection lifetime (sec)

Lifetime in seconds for TCP connections, any TCP connection which is inactive for the lifetime will be automatically closed.

TCP keep alive

TCP keep alive is based on RFC 1122. Even with the flag disabled the server will respond to endpoint keep alive. When the flag is enabled the server will start sending TCP keep alive probes after 30 seconds of idle connection. The probes will be periodically sent every 240 seconds in case of two consecutives ones fails the TCP connection will be terminated. Flag should only be enabled if all endpoints using TCP are compatible with TCP keep alive.

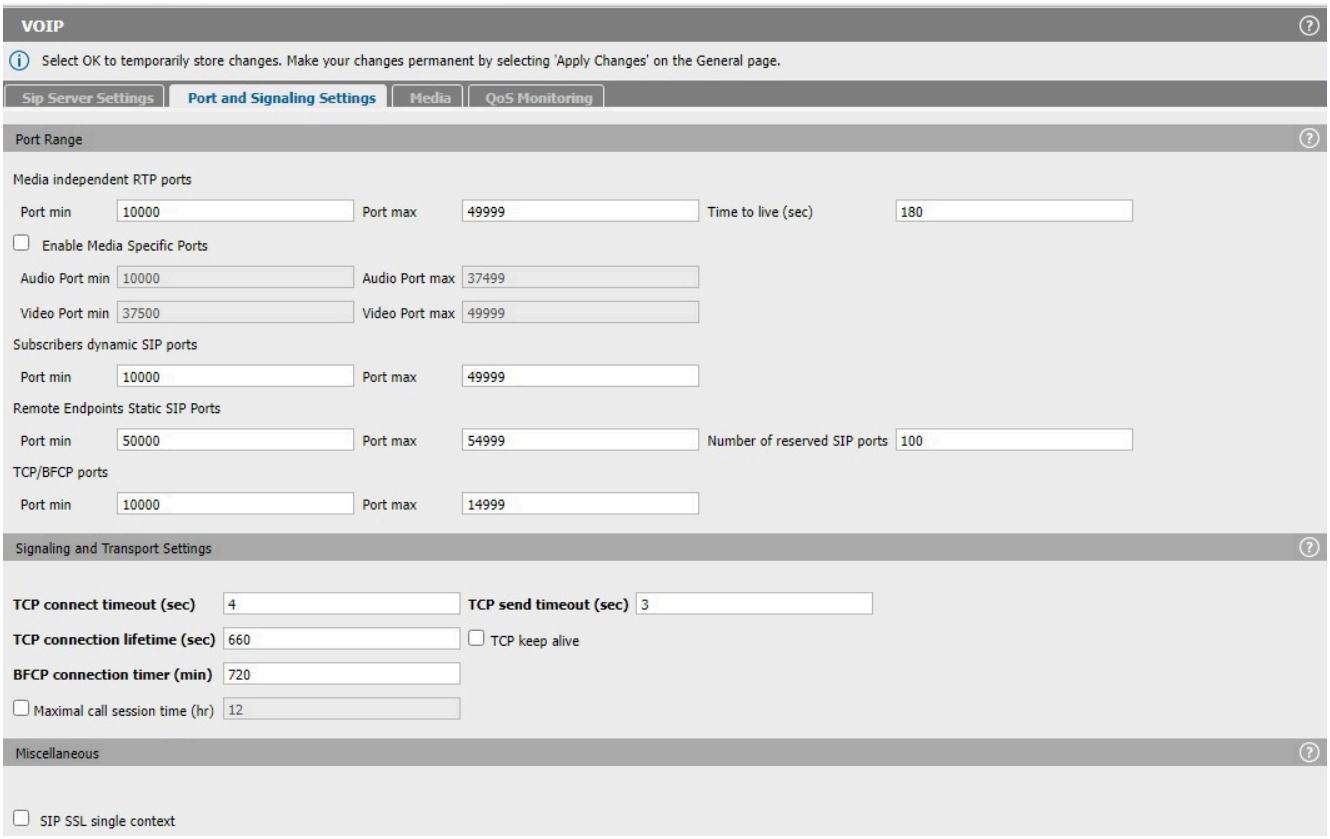
BFCP connection timer (min)

Long time duration timer for a BFCP connection that is established over TCP or TLS. The value is entered in minutes. The range must be between 60 to 1440 minutes, with the default value of 720 minutes (12 hours).

Maximal call session time (hr)

If enabled, the configured time will indicate the length, in hours, that the call will remain active in SBC. After this time, the SIP dialog and the anchored media session are released.

5.4.2.3 Port and Signaling Settings > Miscellaneous



SIP SSL single context

It is used to share the same SSL context among the SIP Server child processes in order to save SIP Server shared memory.

If the flag is disabled, there is an increase in memory usage by the SIP server compared to if it is enabled. It may increase up to 1% of total system memory usage.

If the system has memory enough for multiple TLS processing or has multiple local addresses pointing to the same remote address using TLS protocol, it is recommended to disable it.

The default value is disabled.

5.4.3 Media

It is possible to define one ore more media profiles under the Media tab.

An administrator shall be able to create a media profile or edit an existing media profile and select the –common- packetization interval, add or remove codecs from a list of available codecs and also to prioritize the codecs.

Media Handling

- **Allow multiple media lines for the same media type** - This flag allows SIP messages with multiple media lines for audio and video.If the flag is not set,

SSM will adjust multiple media lines with non zero port keeping only one non zero port for each media type.

- **Replace the SDP Origin (o) field** - This flag enables the replacement of SDP Origin (o) field with the SBC addresses and username OSSBC.
- **Reset SRTP context upon key change**- when enabled, the SRTP context (for Mikey and SDES) will be recreated upon a cryptographic key change. Otherwise, the SRTP context will be just updated with the new key. The configuration is enabled by default to avoid breaking flows with already supported SSPs.

  IMPORTANT: According to the RFCs, the context must not be recreated if only the key has changed. Despite being enabled by default, the flag implies a non-RFC behavior.

- **Use single bridge/port for audio media**- when enabled, a single bridge will be used for audio m-lines. The consequence is that all audio m-lines will use a single port.

  This flag avoids a speech problem in cases where multiple audio m-lines, i.g. RTP and SRTP, were offered, and a provisional SDP response with only one audio m-line was received. The configuration is disabled by default.

  IMPORTANT: The single bridge usage gives the possibility to maintain the same SRTP context even after changing the media negotiation with the other peer. For example, if peer A has an active SRTP context with SBC and on a reINVITE peer B changes from a secure m-line to a non-secure, the formerly used bridge will be replaced by a new one, losing/ recreating the SRTP context with peer A. This can eventually affect the speech between peers.

Core Side Media Configuration

- **Media profile** - the administrator shall be able to select the Media Profile from a drop-down list containing the media profiles configured in the system to the LAN Core Side interface.

User Agent

The administrator is able to **Add** a new user-agent header and assign it a media profile from a drop-down list. The administrator can also select an existing user agent header and **Edit** it, or select one or more existing user agent headers and **Delete** them.

Media Profiles

The administrator is presented with the option to create a new media profile by clicking on the **Add** button. Existing media profiles can be selected for **Edit** or **Delete**.

Upon clicking the **Add** or **Edit** buttons, the Media Profile window is open where the user shall be able to create or modify, the media profile.

If a media profile is deleted and this media profile is assigned to an endpoint type/user-agent header then all associations with this media profile shall be removed. A warning shall be presented and the administrator shall be given

the option to verify and proceed with the removal of the media profile and all existing associations.

The default media profiles are:

- **default** - Remote subscribers and remote endpoints use this Media Profile by default. This can be changed via configuration.
- **webrtc_default** - Recommended configuration for WebRTC endpoints (Circuit).
- **WE_Phone_default** - Recommended configuration for CP Phones and ICE aware devices.
- **Unify_Phone_default**- Recommended configuration for NGTC (Next Generation Telephony Connector) endpoints.

Media Realm Groups

The **Media Realm Groups** allow the customer to have some control over media connectivity between network media domains (or network segments) without L3 NAT. To support the needed flexibility, the customer is required to identify network segments (media realms) in a group (**Media Realm Groups**), identifying the media anchoring requirements for the media realm group. Additionally each media realm has its own intra-realm media anchoring requirements. Media connections outside the media realm group are automatically anchored by the OpenScape SBC.

- **Distributed Media Realm Groups**

  The Distributed Media Realm Group is used when more than one SBC is in the media path and the media can be anchored in only one SBC. Depending on media capabilities on peers, the media can even not be anchored at all meaning the direct media will be used.

A new **Media Realm Group** is created by clicking on the **Add** button. Existing media profiles can be selected for **Edit** or **Delete**.

Upon clicking the **Add** or **Edit** buttons, the Media Realm Group Configuration window is open where the user shall be able to create or modify, the media realm group. A maximum of 1024 Media Realm Groups can be defined.

Session Recording Client (SRC)

Starting from V11R2.2.0, the **Session Recording Client** (SRC) tab allows the configuration of SIP Recording Server, which records RTP streams using the SipRec protocol.

NOTICE:

SipRec restrictions: Only audio will be recorded.

- **Enable recording**

  This flag enables or disables the Session Recording Server.
- **Record Early Media Session**

  If enabled, the SBC will start the Recording Session when a 180 or 183 with SDP is received.

  The default value is **Disabled**.

- **Hold 200 OK until Recording Session is established**

  When enabled, the SBC will delay sending the 200 OK response to the caller until the recording session is established. If disabled, the SBC will forward the response as soon as possible, which may result in media loss in the recording.

  The default is disabled.
- **Record calls from**

  Specifies the call direction from which the SBC will record calls. The available options are:

  Access

  Core

  Core and Access

  The default is **Core and Access**.
- **Priority**

  Defines the recorder's priority.

  NOTICE: This setting has no effect on the SBC, as it supports only one recorder.

- **Server address**

  The IP address or FQDN of the recording server.
- **Server port**

  The port on which the recorder listens for SIP messages.
- **Protocol**

  The protocol used to communicate with the recording server. Options: **UDP**, **TCP**, or **TLS**.
- **Realm**

  The SIP realm associated with the recording server.

5.4.3.1 Media Profile

This is where media profiles for the Core (LAN) interface, User-Agent Headers, Remote Subscribers Location Domain and Remote Endpoints may be administered.

A media profile is a list of prioritized codecs to be used when sending an SDP offer to the side of the call which is assigned the media profile, overriding the list of codecs in the original SDP offer, when the receiver has a different media profile than the sender.

General

- **Name** - Media Profile name must be unique

- **Media protocol** - drop-down selection list
  - **Strict Pass-Thru** - Incoming SDP received from the originating side would be sent out as is with the exception of doing the NAT on the IP addresses and Port i.e. number of m lines remains the same.
  - **Best Effort SRTP** - Incoming SDP would be converted to the Best Effort SRTP SDP based on the SRTP configuration.

    NOTICE: 1. If the incoming SDP offer is Best Effort (SRTP+RTP) with the matching key negotiation protocol (Mikey or SDES) then media encryption and decryption is end to end i.e. no SRTP termination is performed.

    2. If the incoming SDP offer is Best Effort (SRTP+RTP) with non matching key negotiation protocol (Mikey or SDES) then SRTP interworking is performed.

    3. If the incoming SDP offer is RTP only then SRTP interworking is performed if need be based on the terminating side's answer.

  - **Single m-line Best Effort SRTP** - Incoming SDP would be converted to the Best Effort SRTP SDP based on the SRTP configuration with a Single m-line.

    NOTICE: Same behavior as Best Effort SRTP but with a Single m-line SRTP.

  - **SRTP only** - Incoming SDP would be converted to the SRTP only SDP based on the SRTP configuration.
  - **RTP only** - Incoming SDP would be converted to the RTP only SDP

    NOTICE: If the incoming SDP offer is Best Effort (SRTP +RTP) then end to end call is established using RTP

    If the incoming SDP offer is SRTP only then SRTP to RTP interworking is performed.

- **Direct Media Support** - When both source Media Profile and destination Media Profile have this flag enabled, SBC will forward rtcp-mux and ICE related attributes from one peer to another. If both peers support ICE and have the same behavior regarding rtcp-mux (with or without), the media path will be optimized. If the remote peer does not support either of these attributes it can ignore them and the call will be completed in the traditional way.
- **Support ICE** - Adds ICE support to outgoing SDP. If the remote peer does not support ICE, it can ignore the ICE attributes and the call will be completed in the traditional way.

  The ICE-Lite attribute **SHALL NOT** be used in the context of **RTSP** (Real-Time Streaming Protocol). The **ICE** specification describes the following two implementations of ICE:

  - **Full**
  - **Lite**

  Hosts that are not behind a **NAT** (Network Address Translator) are allowed to implement only **Lite**. For **RTSP**, the Lite implementation is insufficient

because it does not cause the media server to send a connectivity check, which is used to protect against making the **RTSP** server a denial-of-service tool.

Network Address Translation (**NAT**) is a method by which IP addresses are mapped from one address realm to another, providing transparent routing to end hosts. There are many variations of address translation that lend themselves to different applications. However, all flavors of NAT devices should share the following characteristics:

– Transparent Address assignment.
– Transparent routing through address translation. (routing here refers to forwarding packets, not exchanging routing information)
– ICMP error packet payload translation

The need for IP Address translation arises when a network's internal IP addresses cannot be used outside the network, either because they are invalid for use outside, or because the internal addressing must be kept private from the external network.

Full: An ICE implementation that performs the complete set of functionality defined by this specification.

Lite: An ICE implementation that omits certain functions, implementing only what is necessary for a peer with a Full implementation to gain the benefits of ICE.

Lite implementations do not maintain any of the state machines and do not generate connectivity checks. For each IP address, independent of an IP address family, there **MUST** be zero or one candidate. With the Lite implementation, ICE cannot be used to dynamically choose amongst candidates. Therefore, including more than one candidate from a particular IP address family is **NOT RECOMMENDED**, since only a connectivity check can truly determine whether to use one address or the other. Instead, it is **RECOMMENDED** that agents that have multiple public IP addresses run **Full ICE** implementations to ensure the best usage of its addresses.

NOTICE: For more information, refer to RFC 7604, RFC 8445, RFC 5245, RFC 2663.

IMPORTANT: If **Direct Media Support** is enabled, this flag will enforce the use of **ICE**.

- **Support NGTC Trickle ICE**- Adds NGTC Trickle ICE support to outgoing SDP.
- **Enable NGTC WebRTC Compatibility** - This flag changes the SDP for NGTC WebRTC compatibility.

IMPORTANT: This flag must be used only for NGTC WebRTC remote subscribers.

- **RTP/RTCP Multiplex in offer**- Adds rtcp-mux support to outgoing SDP. If the remote peer does not support rtcp-mux it can ignore the attribute and the call will be completed in the traditional way.

  IMPORTANT: If **Direct Media Support** is enabled, this flag will enforce the use of rtcp-mux.

- **SDP Compatibility Mode**- Some SIP Service Providers do not accept certain codecs or unknown attributes in the SDP. Use this flag to remove extra fields from the SDP. If this flag is enabled, the codec list of the respective Media Profile cannot be empty and the **Allow unconfigured codecs** flag must be disabled.

  If this flag is enabled only the attributes related to the codec list of this Media Profile will be passed through. If there is more than one telephone-event payload type in the SDP offer, they will be removed, and only the first telephone-event with rate equal to 8000 will be used and, the additional parameters will be removed. The list of removed attributes include: **candidate**, **ice-ufrag**, **ice-pwd**, **rtcp-fb**, **end-of-candidates**, **msid**, **bside_ml**, **label**.

  NOTICE: The **SDP Compatibility Mode** flag is disabled by default.

- **Support Mid Attribute** - This flag sets the attribute **mid** in the media lines of SDP. When enabled, the same mid attributes received in the SDP offer will be included in the SDP answer. If the flag **Support Mid Attribute** is disabled, the attribute **mid** is removed from the SDP towards the endpoint/ subscribe associated to the respective media profile.

  IMPORTANT: For media profiles associated to remote endpoints of type GTC, the flag is required to be enabled.

- **Do not set port to zero on session timer answer SDP** - This flag will avoid setting the SDP media port to zero on SDP answer of session timer when no SDP change is verified. Although the last port is kept with a no-zero port, SBC will not listen to the respective port.
- **Keep sendonly attribute on NAT** - This flag ensures that the received `sendonly` attribute is sent to the destination associated with the media profile, even if NAT is detected. Naturally, when NAT is detected, the `sendonly` attribute is converted to the `sendrcv` attribute.

  NOTICE: Keep sendonly attribute on NAT is available starting from V11R2.

SRTP configuration

- **SRTP crypto context negotiation** following the option selected between the three flags for the **Media protocol** selected, except for "Strict Pass-Thru"
  - **MIKEY** - Multimedia Internet KEYing
  - **SDES** - Security Descriptions Mark

    (ciphers supported: AES 128, AES 256, both)
  - **DTLS** - Datagram Transport Layer Security

- **Mark sRTP Call-leg as Secure**

  Checkmark the checkbox, if calls require secure media. When active, this parameter identifies the network as secure if TLS and SRTP are not used, i.e., TCP or UDP for the signaling transport or RTP is used for the media protocol.
- **Crypto change mode**: This option can be configured in any of the following ways:
  - **Default**: The crypto key on media renegotiation is preserved when associated with the core side and changed when associated with the access side.
  - **Steady**: This mode preserves the crypto key on media renegotiation when associated with either the core or access side.

> **NOTICE:** The behavior described is also influenced by the SSP profile— for the MS Teams default profile, the behavior of Steady mode operates independently of the configured crypto change mode.

RTCP Configuration

Some peers may need to receive RTCP packets. This configuration allows the application handling media to generate RTCP when not being sent to it.

- **RTCP Mode**
  - **Bypass**: This is the default behavior. The media application does not generate any RTCP, it forwards them. When the QoS is disabled, the packets are transparently forwarded
  - **Generate Always**: The media application generates RTCP packets, regardless if the media (RTP) is active (for example, call on hold).
  - **Generate only When RTP is active**: The media application generates RTCP packets only when the media (RTP) is active.
- **RTCP generation timeout**: The time (in seconds) that the media application must wait for an RTCP on the same direction before it starts generating them.

> **NOTICE:**
>
> When configured to generate RTCP, the media application collects all the QoS statistics (process all incoming/outgoing RTP/RTCP packets) to fill the generated RTCPs.

> **NOTICE:**
>
> When configured to generate RTCP, there is no SRTP pass-through, since the media application needs to encrypt the generated RTCP.

Codec configuration

- **Allow unconfigured codecs**

  Enabled by default.

  When enabled, codecs received in the SDP Offer that are not configured in the profile are presented to the called Party in addition to the configured codecs.

  When the flag **Allow unconfigured codecs** is unmarked in the media profile, the SBC will add in the outgoing SDP only the codecs assigned in the codec list, except for CLEARMODE, CN and Telephone-event codecs.

  NOTICE: It is possible to change this behavior from XML configuration items by using the following flags: **removeClearmode**, **removeCN** and **removeTelephoneEvent**. These flags could be added in the XML configuration, to remove these codecs respectively. These parameters must be configured in the **mediaData** session and will apply to all profiles without the **Allow unconfigured codecs** flag set.

- **Enforce codec priority in profile**

  If this flag is enabled and codec transcoding is applied for the destination, the codec order in the media profile is enforced with this option regardless of the codec preference in the SDP offer.

  If the flag is not enabled, the codec order of the received SDP is kept and the additional codecs of media profile that are not included in the original SDP are appended at the end of the original sdp.

  NOTICE: If no transcoding is applied, the flag does not take effect.

- **Send Telephony Event in Invite without SDP**

  When this profile is used by SIP Service Provider configured with **Do not send Invite without SDP** flag, enabling this checkbox allows sending the INVITE with RFC2833 telephone-event indication in the SDP built by the OS-SBC.

- **Use payload type 101 for telephony event/8000**

  Disabled by default. This flag allows SBC to convert the payload type for telephone-event rate 8000 to 101 in the SDP offer and restore the original payload type when sending the SDP answer. Some SIP Service Providers send the payload type 101 for the telephone-event/8000 in the SDP, even if another payload type was used in the SDP offer to negotiate the telephone-event payload type. As a result, the DTMF tones between the parties may not be recognized. This flag should be enabled in the Media Profile of the destination endpoint. This Media profile's codec list CANNOT be empty.

  This flag should be used to prevent conflicts in the SDP m-line if the codecs iLBC (PT 97), iSAC (PT 103) or OPUS (PT 96) are present in the codec list and there is a telephone-event using a conflicting payload type (PT) in the same SDP m-line.

- **Enforce Packetization interval**

  Disabled by default.It is necessary at least one codec configured to enable this feature. When this flag is enabled, all codecs must have the same Packetization interval and it cannot be set as Auto.

  As 'Allow unconfigured codecs' requires that 'Packetization Interval' be set to Auto, the two features can not be activated at the same time.

  Each codec has its own packetization interval that can be selected from adrop down list with the following available options: 10ms, 20ms, 30ms, 40ms,50ms 60ms, and pass-through (auto) with default value auto. Up to 3 different packetization interval values are allowed per Media Profile.

  IMPORTANT: If the Allow unconfigured codecs checkbox is selected, then the Packetization interval can only be auto for each and every codec. If it is not selected, then other options are allowed, as long as the codec is compatible with the assigned time value.

- **Codec**

  The user is able to select a codec from a drop-down list and click **Add** to add it to the bottom of the list of codecs for this media profile.

  NOTICE: If a codec is already in the list of codecs for this media profile, then it does not appear in the drop-down list for adding codecs.

  The user can also select a codec from the list and click **Move up** or **Move down** to move it up or down the list in terms of priority or click **Delete** to delete it. In these cases the priority numbering should be updated.

At the bottom of the Media Profile window the following options are offered:

- **OK**- to save all media profile changes.
- **Cancel**- to cancel changes and exit the Media Profile window.

Transcoding in SBC

In SBC transcoding occurs when the negotiated codecs between SBC and the call parties are not equal or not explicitly common.

In such case, one of the parties might send RTP with payload that is not supported by the other side. SBC transcodes RTP packets to ensure that the media can be properly received by the receiver. To understand better how transcoding works, see the examples below.

Scenario cases

- **In the following scenario case transcoding takes place:**

1) A-Side supports Codec1 and Codec2 and B-Side supports Codec1 and Codec3.
2) Due to the media profile, SBC sends Codec4 towards B-side. B-side accepts Codec1 and Codec 4.

- **In the following scenario case transcoding does not take place:**

1) A-Side supports Codec1 and Codec2 and B-side supports only Codec1.

2) Due to the media profile, SBC sends only Codec1 and Codec2 towards B-side. B-side is forced not to use Codec3 since it is not offered.

- **In the following scenario case transcoding will occur only if Codec1 is added in the Media profile for A-side:**

1) A-Side supports Codec1 and B-Side supports Codec2 & Codec3.
2) Media profile for B-side is configured to support Codec2 & Codec3.

   If Codec1 is not added in the Media profile for A-side, SBC won't accept the INVITE request, even if the "Allow unconfigured codecs" is enabled for A-side.

5.4.3.2 Media Realm Group Configuration

Media Realm Optimization Settings

It is a period of time in milliseconds between rtcp reports.

- **Name** - Name of the Media Realm Group.
- **Anchoring Media** - Drop down list with the following values:
  - **auto** - when selected and both legs of the call are in the current subnet then the local Media is setup between the endpoints. Otherwise, Media is anchored through the SBC.
  - **forced** - when selected Media is always anchored through the SBC.
- **Force media anchoring on transcoding** - If checked, then when the OS-SBC determines that transcoding is required for the media session it shall anchor the media session.
- **Enable Multi-SBC support** - If checked, different SBCs will try to optimize the path of subscribers residing in the same subnet. In order to do that this flag must be enabled and the media realm correctly configured in all SBCs participating in the optimization. When selected, and both legs of the call are in the same subnet, then optimization will occur. Otherwise, Media is anchored through the SBCs.

Media Optimization Subnets

It is set to enable/disable strict RTP protection.

- **Physical Interface** -
- **VLAN** - VLAN tag in all rows must match. If the VLAN tag is non 0, then the **Physical Interface** in all rows must match.
- **IP address, Subnet or Logical Endpoint ID** - IP address/FQDN of the domain subnet.
- **Subnet** - Domain subnet mask. Maximum of 1024 subnets can be defined. A given subnet cannot appear in more than 8 Media Realm Group Profiles.
- **Anchor Media** - Drop down list with the following values:
  - **auto** - when selected and both legs of the call are in the current subnet then the local Media is setup between the endpoints else Media is anchored through the SBC.
  - **forced** - when selected Media is always anchored through the SBC.
- **Allow Force Anchoring on Transcoding** - If checked, then when OS-SBC determines transcoding is required for the media session it shall anchor the media session.

5.4.4 QoS Monitoring

The OpenScape SBC is traversed by calls from Remote Subscribers (teleworkers), SIP Service Providers and Remote Branches. In case of network problems the speech quality may be severely impacted. Since the OS SBC is separating very distinct networks, namely the access and the core network, it is important to get the QOS measurements of both sides separately.

- **Enable QoS Monitoring**

  This flag must be enabled in order to perform media statistic calculations.

  NOTICE: If this flag is disabled no statistics calculation for media is performed in the SBC.

- **Send traps**

  This flag shall enable / disable the generation of traps to the QDC server. The QDC trap shall be generated at the end of the media session with QoS statistics report for the Access Side, the Core Side and the Remote Endpoint.

  Default status: unchecked.
- **Report Mechanism**

  This parameter is hardcoded to **Collection of each call session**. The parameter is not configurable and shall be grayed out.
- **QCU IP address**

  IP address of QCU servers.
- **QCU Port**

  Port to which the QDC traps shall be sent on the QCU server.

5.4.5 VoIP > SIP Headers Manipulation Rules (HMR)

The Header Manipulation Rules (HMR) feature provides extensive flexibility for customizing SIP headers, ensuring that all phone systems can understand and accept them.

It allows you to add, modify, or remove headers through Lua plugins written as short scripts, enabling compatibility with various SSPs.

For more information on Lua, see https://www.lua.org/.

IMPORTANT:

The Header Manipulation Rules (HMR) feature is available starting with V11R3.

Some examples of how HMR rules can be used are listed below:

- Remove or correct broken or incompatible headers
- Force or alter SIP functionality
- Add info based on SIP trunk
- Create in-house scripts to improve client experience

When selecting **VoiP** > **SIP HMR**, the **SIP Header Manipulation Rules** page is displayed, with the following columns:

- **Index** - Order of the HMR profile.
- **Name** - The name of the HMR profile.
- **Control** - The options to edit or delete a HMR profile are available.
  - To edit a Header Manipulation Rules (HMR) profile, click ✎ next to the profile you want to edit.
  - To delete a Header Manipulation Rules (HMR) profile, click **X** next to the profile you want to delete.

To add a new Header Manipulation Rules (HMR) profile, click **Add new profile**.

The **SIP HMR Profile** window opens, allowing you to configure a new HMR Profile (see VoIP > SIP Headers Manipulation Rules (HMR) > SIP HMR Profile on page 334).

5.4.5.1 VoIP > SIP Headers Manipulation Rules (HMR) > SIP HMR Profile

Profile information

- **Profile Name** - Enter a new Header Manipulation rule profile name.

Configuring Incoming and Outgoing messages

Incoming messages

Incoming messages refer to messages processed within the system.

When a script is selected, it is applied before the message is sent to the SSP and remains effective until the message reaches the SSP.

For example, a script can add a new header to an INVITE message as it passes through the system, and this header will persist until the message arrives at the SSP.

Outgoing messages

Outgoing messages differ from incoming messages only in that they take effect at the end.

They are applied when the messages reach the SSP, not while they pass through the system.

Scripts

Scripts can be used in multiple profiles, **for both incoming and outgoing messages**.

In both cases, the order of execution matters: scripts are applied from top to bottom.

When manipulating multiple parameters on the same header, you must use a single Lua script to avoid duplicate headers.

Removing and then re-adding the same header in the same direction (incoming or outgoing) is not a valid use case.

NOTICE:

This feature can work alongside others, such as the SIP Service Address. When scripts are selected for *Outgoing Messages*, they take priority over the SIP Service Address, whereas for *Incoming Messages*, the SIP Service Address takes priority.

- **Upload** - Click to select and upload a .lua script to the system.

  NOTICE:

  Only .lua scripts can be uploaded.

  Uploaded scripts are not checked for Lua syntax. It is the administrator's responsibility to verify both the syntax and functionality of the scripts.

  The list of available scripts uploaded to the system are displayed under the **Available scripts** section on the left-hand side.

  – To select a script, click on it and then click ➔ to move it to the **Selected Scripts** section.

  – To unselect it, click ←.

    The script will be moved back to **Available scripts**.

  If you upload a script with the same name as an existing script in the system, you are alerted that completing the upload will overwrite the existing script. In this case, it is recommended to proceed with caution, as this action may indirectly affect other profiles.

  The scripts are stored in a pool with 300 available positions. If you attempt to add more than 300 scripts, a warning message is displayed to inform you that the limit of available script positions has been reached.

  NOTICE:

  The pool is common for all HMRs, which means that one script can be used for multiple HMRs. If a script has a different behavior for a specific rule, it must be renamed and attached to that rule only; otherwise, it will affect all rules.

- **Download** - Download any script already uploaded on the system.
- **Delete** - Delete a script on the system.

  NOTICE:

  It is possible to delete a script only if it is not being used in another profile.

- **See templates** - When clicked, the **SIP HMR Templates** window opens, displaying the available default .lua templates for download. The displayed columns are:
  - **Name** - The name of the SIP HMR template, such as **Add header**.
  - **Download** - Download the SIP HMR template.
  - **Description** - A brief description of the SIP HMR template.

  All displayed SIP HMR templates can be downloaded and used as a base for creating other scripts.

  NOTICE:

  It is recommended to proceed with caution when modifying a selected template. Uploaded scripts are not checked for Lua syntax. It is the administrator's responsibility to verify both the syntax and functionality of the scripts.

  Some HMRs cannot be removed, or it is recommended NOT to remove them. These are listed below:

  Table 1: HMRs that cannot or should not be removed

HMR	Restriction
Via header	Cannot be removed
Call id	Cannot be removed
From	Cannot be removed
To	Cannot be removed
Record-route	Do not remove (recommended)

Saving a SIP HMR Profile

To temporarily save your changes, select **OK** on the **SIP HMR Profile** page.

To permanently save your changes, select **Apply changes** on the **General** page.

Once a new HMR is available, it can be configured on SIP Service Provider Profile and Remote Subscribers: see section **SIP Headers Manipulation Rules** in General on page 345 and Remote Subscribers on page 338.

5.4.5.2 Troubleshooting SIP Headers Manipulation Rules (HMR)

When using scripts with Kamailio, most issues can be identified and resolved by checking logs, traces, and script behavior.

In most cases, Kamailio will recover automatically and the scripts will have no effect.

If Kamailio cannot salvage the situation, it will revert to the last known good configuration.

Procedure

- **Check HMR logs**: all logs related to the HMR are stored in the **SIP Server** log. To view them, set the **SIP Server** log level to **Debug**.
- **Verify functionality**: capture SIP traces to confirm that traffic is flowing as intended.
- If needed, re-upload the correct scripts and apply the changes.

  If neither recovery nor fallback resolves the issue, it is likely that a script was applied that modified a SIP header incorrectly.

  Review the last script changes for:

  – Header manipulations (e.g., From, To, Contact).
  – Incorrect syntax or missing values.

  Correct the script and re-apply.

5.5 Features

In this administrative area the user can configure remote subscribers, remote endpoints and codec support of transcoding.

Remote Subscribers Overview:

- The **Remote Subscribers configuration** is enabled using the **Enable Remote Subscribers** check box.
- To configure Remote Subscriber settings click the **Remote Subscribers configuration** button.
- The **Remote Subscribers** provisioning window is displayed.

Remote Endpoints Overview

- The **Remote Endpoints configuration** is enabled using the **Enable Remote Endpoints** check box.
- Clicking on the **Remote Endpoints configuration** button launches the **Remote Endpoints** window.

NOTICE: SBC does not have the ability to block incoming calls based on the calling party number.

Codec Support for Transcoding Overview

- The Codec Support for Transcoding is enabled using the **Enable Codec Support for Transcoding** check box.
- Clicking on the **Configure** button launches the **Codecs** window where various Codecs (e.g. OPUS) may be enabled/disabled via checkboxes.

  The selected codecs can be then used in the media profiles in the Codec configuration session. In that session the codec priority and packetization interval can be defined. Once media profile is set it can be associated to endpoints and/or remote subscribers. The core side of SBC is always associated to the default media profile.

THIG (Topology Hiding Interworking Gateway)

IMPORTANT: This flag is only available to the V11R1.0.0 or higher versions.

When THIG is enabled, the way that OSSBC handles NAT is changed to provide the THIG functionality. Instead of changing the source IP to its own IP, THIG will bypass the IP and just change the port according to port forwarding rules.

This way, network elements will point to OSSBC WAN address as the destination, and the package will be forwarded to the LAN while preserving the original source IP address. All network packages on the LAN interface with destinations not belonging to the subnet of the originating address will see SBC THIG as the destination since it is the network gateway.

OSSBC THIG will forward the packet to the WAN using its own WAN address, making the network elements on the WAN unaware that they are not directly communicating with the intended destination.

IMPORTANT:

For Hosted OpenScape SBC (hSBC) on OS4K Deployments, THIG is disabled.

SBC Standalone mode feature

By enabling the **Standalone mode** SBC should operate without connection to a PBX at core side.SBC will send OPTIONS to the loopback interface that gets responded by itself.That way it stays in "normal mode" and the access side interfaces are not locked.

In order to use the **SBC Standalone mode** feature it is necessary to configure pairs of Associated **Remote Endpoints** - such configuration is only made available with the activation of the feature.

Once the **Enable Standalone** flag is set, the following buttons become grayed out: **Enable Remote Subscribers**, or **Enable Sip Load Balancer** and **Enabled Border Control Function**. In the same way the **Enable Standalone** Flag is grayed out if one of the previous mentioned flags is enabled.

Push Notification Service Feature

The Push Notification Service feature supports sending VoIP Notifications to an Apple Push Notification Server.

5.5.1 Remote Subscribers

The **Remote Subscribers** provisioning window is displayed with the following configuration options.

General Settings

In this section the throttling parameters can be configured.

NOTICE: Throttling only applies to Subscribers behind NAT device. Direct Subscribers not behind NAT device are not impacted by these settings.

- **Enable register throttling** - this option allows the user to enable and configure the register throttling timers for UDP and TCP.

  Usually remote subscribers tend, as a standard procedure, to request a Register for a long period of time to establish a connection. Although, when the subscriber is behind a NAT/Firewall, the Register time cannot take too long otherwise the pinhole from NAT would close. So, to make the subscriber ask constantly for a Register and avoid the main server (OSV) answering every request made by the remote subscriber, an interface device (OSS) is configured to do these tasks.The interface device initially will receive a request from the remote subscriber (for a Register with comparatively long period of time), it will forward to the main server that will register the subscriber for that period of time. The server will answer to the interface device about the time the subscriber was registered and, knowing that, the interface will divide this time in blocks of time configured by the parameter **Timer value towards subscriber**. It means that the interface only will give the subscriber a Register for the time configured and before that period ends, the subscriber needs to send another Register request to keep itself registered.The procedure will continue as described above until the time registered in the main server is about to expire or the time is about to reach the value configured in **Maximum throttling timer threshold**. When the smallest of those values is about to be achieved, the OSS will forward the Register request to the main server for the registration to be renewed.

  – **Timer value towards subscriber - UDP (sec)** - Enables register throttling timers for UDP Timer value towards the subscriber (sec).

    The value will correspond to the maximum interval of time in which the subscriber (using **UDP-User Datagram Protocol**) is registered in OSS. Before this time expires, the remote subscriber needs to request a new Register in order to keep the NAT's pinhole open.

    NOTICE: The value of this parameter should be the amount of time that it takes for the NAT's pinhole to close.

  – **Enable register throttling for TLS** - Enables register throttling timers for TLS Timer value towards the subscriber.

  – **Timer value towards subscriber TCP/TLS (sec)** - Configured when register throttling for TLS is enabled.

    The value will correspond to the maximum interval of time in which the subscriber (using Transmission Control Protocol/Transport Layer Security) is registered in OSS. Before this time expires, the remote

subscriber needs to request a new Register in order to keep the NAT's pinhole open.

Possible values: **30** sec – **1800** sec.

Default value: **60** sec.

NOTICE: The value of this parameter should be the amount of time that it takes for the NAT's pinhole to close.

– **Maximum throttling timer threshold (sec)** - Throttling timer towards Comm System for subscribers.

The value is the maximum interval of time that OSS will respond the solicited Registers made by the remote subscriber. Before this time expire, instead of renewing the Register itself, the OSS will forward the request to the main server (OSV) to the register to be renewed.

Possible values: **300** sec – **3000** sec.

Default value: **1800** sec.

- **Maximum registration expiry time (sec)** - It is the maximum acceptable expiry time for a Register request. Maximum registration expiry allowed from the subscriber. Registration received from subscriber with expiry greater than this value would be rejected. Possible values are in range 3600 to 86400.
- **Minimum registration interval (sec)** - This timer minimizes ineffective registration attempts with OSV. The OS-SBC will not accept a registration expiration value less that the provisioned value. Any attempt to do so will be responded to by a "423 Interval Too Brief" response which includes a Min-Expires header field containing the provisioned value. This value should be coordinated with the setting of OpenScape Voice Srx/Sip/Min_Register_Time. The value should be provisioned with the same or greater time value with a default of 300 seconds. Repeated violations may subject the SIP interface to being quarantined due to DoS IP (Message Rate Control) or SIP message threshold detection.
- **Quarantine registration interval violators** - Users which violate the minimum allowed registration rate may have their IP address quarantined for the "minimum registration interval". During this interval OS-SBC will ignore any SIP message from the IP address.
- **Throttling Bypass Based on UA (Regex)** - This feature allows specific User-Agents (UA) to bypass standard throttling limits by using regular expression (Regex) pattern matching.

  By default, the bypass is enabled for User-Agents that match the string **Zoom** (case-insensitive).

  This is useful for allowing trusted or high-priority applications (such as Zoom) to avoid throttling limitations that apply to general traffic, ensuring uninterrupted service performance for these clients.

  The field accepts a regular expression for flexible matching (for example, `Zoom|Skype|Teams` allows bypass for multiple applications).
- **Port Mapping TTL timer (hours)** - It is the timer for Port Mapping TTL. Possible values are within the range 1 to 48 hours or never (meaning port mappings persist once they occur).
- **Disable External Port Mapping** - When this flag is set, the subscriber mapped port is not included in the core side SIP messages.

- **Core realm profile** - For the core realm, the “Main-Core-Realm” profile is always selected by the system and cannot be modified by the user (grayed out).
- **Access realm profile** - For the access realm, the “Main-Access-Realm” profile is always selected by the system and cannot be modified by the user (grayed out).
- **INVITE No Answer timeout (msec)** - Final response timeout (in milliseconds) to an INVITE request that has not received a final reply. Range is 120000 to 600000 milliseconds. Default is 360000 msec.
- **INVITE No Reply timeout (msec)** - Timeout (in milliseconds) for an INVITE request or a non-INVITE transaction that has not received a provisional response. Range is 1000 to 32000 milliseconds. Default is 3000 msec.

  NOTICE: When a provisional response is received, this timer is stopped and the **INVITE No Answer Timeout (msec)** is set.

- **Enable remap internal error code** - Available options: **408**,**504**
- **Open external firewall pinhole** - When the SBC is under an external firewall, dummy UDP packets are sent towards the endpoint media destination (connection address and port in the SDP) in order to dynamically open the firewall for the incoming media streaming.

  This feature avoids several rules to be added to the firewall in order to keep open all possible addresses and ports used by the SBC for the media connection values. This configuration applies to all remote subscribers under the SBC.

  NOTICE: This feature only applies for the addresses and ports used for the media streaming. It is not applicable to the SIP or MGCP protocols.

- **Send RTP dummy packets** - As some providers were having issues with the dummy UDP packets a new flag "Send RTP dummy packets" is added to send RPT packets instead.

  Similar to the "Open External Firewall Pinhole" method, dummy RTP packets are sent toward the endpoint media destination (the connection address and port specified in the SDP) to dynamically open the firewall for the incoming media streaming. The dummy RTP packet is sent with payload type of the first codec listed in the SDP answer message.

  NOTICE: This feature is applicable only to the addresses and ports used for the media streaming. It is not applicable to the SIP or MGCP protocols. The RTP dummy packets will have the payload type negotiated by the SDP protocol, taking the first Codec listed on the Answer of the SDP.

- **Insert Location Header** - When enabled, SBC will add the **X-Siemens-Location** header towards OSV. By default, this is not enabled.

  IMPORTANT: The configuration options listed below are only available for the V11R1.01.00 or higher.

- **Drop received RTP**- Drop RTP packets received while sending dummy packets.

- **Dummy RTP to Core side**- Send packets to the core side as well. If the current system uses Standalone with internal SIP stack, this flag is greyed out.
  - The minimum time for both fields below is: 10 ms
  - The maximum time for both below is: 3000 ms
- **Stream Delay (ms)**- The amount of time, from ACK, before starting to send the dummy packets. The default value is 60 ms.

  Stream Duration (ms)- The amount of time the dummy stream will last. The default value is 80 ms.
- **Observation**- It is possible to set the value of **Stream Delay** and **Stream Duration** as 0.
  - – **Stream Delay set as 0** - The dummy packets will be sent right after ACK, with no delay.
  - **Stream Duration set as 0**- Only 1 dummy packet will be sent.

External Load Balancer

NOTICE: This tab is grayed out if the flag for SLB on SipServer settings is not enabled

---

- **IP Address or FQDN** - IP Address or FQDN of the External Load Balancer.
- **TCP Port** - TCP Port of the External Load Balancer.
- **TLS Port** - TLS Port of the External Load Balancer.

Remote Subscribers configuration

Clicking on the **Add** or **Edit** button launches the Remote Subscriber Configuration window.

SIP Headers Manipulation Rules

IMPORTANT:

The Header Manipulation Rules (HMR) feature is available starting with V11R3.

- **HMR for messages to the core side**:

  This dropdown configures the Header Manipulation Rules feature.

  When a profile is selected, all associated Lua scripts and configurations within that profile are applied.

  This setting affects messages directed to the CORE side.

  The default value is: No Manipulation

- **HMR for messages to the access side**:

  This dropdown configures the Header Manipulation Rules feature.

  When a profile is selected, all associated Lua scripts and configurations within that profile are applied.

  This setting affects messages directed to the ACCESS side.

  The default value is: No Manipulation

  NOTICE: When SBC is in **Standalone With Internal SIP stack (BYOT – Bring your own trunk)** mode, the feature will apply to Core Side.

5.5.1.1 Remote Subscriber Configuration

Remote Subscriber Settings

- **Name** - Enter the remote subscriber Name in this field.

Remote Subscriber Location Domain

In this section it is possible to configure a location domain for the remote subscriber.

- **Location Domain Name** - The domain name

  NOTICE: The Fallback TLS option, when used with Mutual Authentication, will allow TLS clients to connect, otherwise only MTLS will be allowed.

Subnet

- **Subnet** - Selected by default. Subnet configuration items are editable and Subnet configuration is used for Location Domain.

  NOTICE: When selected, **DN List** items are grayed out. See more information under **DN list**.

- **Subnet IP Address** - IP address of the domain subnet.
- **Subnet Mask** - Domain subnet mask.
- **Certificate profile** - Select the TLS certificate profile. Default value is **None**.
- **Media profile**- Select a Media Profile which is configured with the Media protocol, codecs, and packetization interval suited for the remote subscriber.
- **TLS Mode**- Available options: Server Authentication, Client Authentication and Mutual Authentication.

DN List

- **DN list**- Disabled by default. When selected, the items "Media profile", "TLS mode" and "Fallback TLS" are available for configuration. The **Subnet** items are grayed out.
- **Media profile** - Select a Media Profile which is configured with the Media protocol, codecs, and packetization interval suited for the remote subscriber.

- **TLS Mode** - Available options: Server Authentication, Client Authentication and Mutual Authentication.
- **Contact Header** - Checked by default when DN List is enabled. DN check will be based on **Contact Header** DN.
- **FROM Header** - If selected, DN check will be based on **FROM Header** DN.
- **DN list box** - Entries are limited to max 50 DNs. All items will be stored in the XML config file.

Access Side Firewall Settings

The Firewall Settings are enabled using the **Enable Firewall Settings** check box. The **Firewall Settings** button is used to open the Firewall Settings configuration window. Management of White Lists and Black Lists of IP address and port combinations is supported as well and enable/disable control over SIP, MGCP and DNS protocols.

Emergency configuration

Configuration of Emergency Calling requires administration of the following areas:

- **Emergency Calling Subnets**

  This button opens the Emergency Calling window where it is possible to configure the emergency calling subnets.
- **Emergency Calling Numbers**

  This is the list of Emergency numbers, that when dialed will allow the SBC to identify an Emergency Call. For USA, this is the 911 emergency numbers.

  A call to a number in this list will trigger the server to try to establish an outgoing call to a available gateway (highest priority).

  The search for a emergency destination is done as follows:

  – Try a gateway configured with emergency.
  – If no emergency gateway is available try to use lowest priority gateway looking at priority 1 gateways.
  – If the first and second searches fail then try a default gateway (priority 0).
  – If still no gateway is available then try to reach local attendant configured in LIN table.

NOTICE: An association between the Emergency Number and the Emergency Calling Subnets is done by means of the routing prefix. Any number which is configured as an Emergency Number and matches to the first digits of the Routing Prefix will be associated to that subnet. For example, both 9 and 911 match the beginning of the Routing Prefix 911222, that means both are associated to that subnet. Due to this reason, you will not be allowed to delete the 9 neither 911.

5.5.2 Remote Endpoints

SIP Service Provider Profile

- **SFTP Server** - External SFTP (Secure File Transfer Protocol) Server.

- **Port** -Is a numeric field between **0** and **65535**.This box is used to configure the SFTP Server port.
- **Remote directory** - Remote directory
- **User name** - User name.Default value: `administrator`
- **Password** - Up to 8 numerical characters are allowed.
- **Download New Profile List** - Download new default profile list from an external SFTP server. The files will be downloaded in **.csv** format.The list must be synchronized with SW deliverable, so as long as a new provider is certified, the internal and external list are updated.

A new SIP Service Provider is configured using **Add** button under the **Service Provider Profiles** section. An existing SIP Service Provider can be changed using **Edit** button and deleted using **Delete** button.

Clicking on the **Add** or **Edit** button launches the SIP Service Provider window.

Remote Endpoints configuration

A new Remote Endpoint can be configured by using the **Add** button under the **Remote Endpoints configuration** section. An existing Remote Endpoint can be changed by using the **Edit** button and deleted by using the **Delete** button.

Clicking on the **Add** or **Edit** button launches the **Remote Endpoints Configuration** window.

The **Export Logical IDs** button is used to download a CSV file containing all the Endpoints using Logical ID with the Row Index of Remote Endpoint table, Logical IDs, the Logical ID hash code and the Access Network Realm.

Media Server Profiles

A new Media Server profile is configured using the **Add** button under the **Media Server Profiles** section. An existing Media Server profile can be changed using **Edit** button and deleted using **Delete** button.

Clicking on the **Add** or **Edit** button launches the Media Server Profile window.

5.5.2.1 SIP Service Provider

5.5.2.1.1 General

- **Name** - SIP Service Provider name, a string with up to 20 alphanumeric characters. For Skype profiles the length of the name is limited to 14 characters.

- **Default SSP profile** - A dropdown list of the available default SSP profiles. If one is selected, certain options or flags are automatically enabled, checked, or made required.

  Field is optional.

  NOTICE:

  Starting from V11R3, the profile **Workflow Studio** is available in the **Default SSP profile** list.

  DTAG/Company Flex default SSP profile:

  When the default SSP profile **DTAG/Company Flex** is selected, the parameter for specification 1TR119 is automatically selected. It requires that the associated SSP uses media profile with SRTP/SDES and includes the following SIP headers in the methods REGISTER, INVITE and UPDATE:

  – Proxy-Require: mediasec
  – Require: mediasec
  – Security-Verify: msrp-tls; mediasec
  – Security-Verify: sdes-srtp;mediasec
  – Security-Verify: dtls-srtp;mediasec

    The header **Security-Verify** is included in the method REGISTER only when the authorization is sent after the challenge.

    For the method REGISTER, the following SIP header is included:

    – Security-Client: sdes-srtp;mediasec

      In addition, the attribute **3ge2ae: requested** is included in the SDP offering to the SSP.
- **Enable SSP Privacy and Complementary Flags** - This flag enables configuration and behavior of the general flags below it, and the SIP Privacy – Privacy Support field. If disabled, behavior will be the same as of previous releases (V10).

  NOTICE: This flag is only available for the **V11R1.01.00** or higher versions.

- **Allow sending of insecure Referred-By header** - When enabled, a **Referred-By header** field will be sent for calls transferred to the SIP Service Provider. Otherwise, the header will be removed from messages sent to SSP. The **Referred-By header** field is only sent for Blind Transfer scenarios. For these scenarios, the initial SIP INVITE request sent to the endpoint contains the transferred party identity as the calling party (From and P-Asserted-Identity header-fields). The transferring party identity is in the Referred-By header field.
- **Send P-Preferred-Identity rather than P-Asserted-Identity** - When enabled, a **P-Preferred-Identity header** field will be sent whenever a P-Asserted-Identity header field would be normally sent. This attribute is primarily intended for use when connecting to a SIP Service Provider that does not accept a P-Asserted-Identity SIP header field.
- **Do not send Diversion header** - When enabled, a **SIP Diversion header** field will not be sent to the SSP. This attribute is primarily intended for use when connecting to a SIP Service Provider that does not understand the Diversion header field.

- **Send URI in telephone-subscriber format** - When enabled, "+" is inserted only in front of the 'R-URI' and 'TO' headers (not the FROM, PAI, or Diversion headers).
- **Send authentication number in Diversion header** - When enabled, the authentication DN will be included in the Diversion header. The authentication number can be the Authentication user ID, Default Home DN or Business Identity DN, depending on the SSP profile configuration. For calls that are redirected to the SSP, the calling party number may not be a subscriber that belongs in that SSP. In this case, the SSP needs to authenticate the call based on the number of the redirecting subscriber, i.e., the number contained in the Diversion header.
- **Send authentication number in P-Asserted-Identity header** - When enabled, the authentication DN will be included in the PAI or PPI header. The authentication number can be the Authentication user ID, Default Home DN or Business Identity DN, depending on the SSP profile configuration. Most SSPs authenticate all incoming calls to assert that the call has been originated by a subscriber (DID Number) that belongs to that provider. For some SSPs the authentication is done with the calling party number provided in the P-Asserted-Identity header field.
- **Send authentication number in From header** - When enabled, the authentication DN will be included in the **From header**. The authentication number can be the Authentication user ID, Default Home DN or Business Identity DN, depending on the SSP profile. Most SSPs authenticate all incoming calls to assert that the call has been originated by a subscriber (DID Number) that belongs to that SSP. For some SSPs the authentication is done with the calling party number provided in the **From header** field.
- **Include restricted numbers in From header** - When enabled, the authentication number present in PAI, PPI or Diversion headers will be present in From header in situations where it should be restricted (i.e., in the presence of "Privacy:id" header).
- **Do not validate second Via header**: When enabled, the SIP server skips verification of the second Via header. This validation is typically performed when an SSP is located behind the outbound proxy. When this option is enabled, only the outbound proxy address is validated.

IMPORTANT:

This setting is available starting with V11R3.

- **SIP Headers Manipulation Rules**

  IMPORTANT:

  The Header Manipulation Rules (HMR) feature is available starting with V11R3.

  – **HMR for messages to the core side**:

    This dropdown configures the Header Manipulation Rules feature.

    When a profile is selected, all associated Lua scripts and configurations within that profile are applied.

    This setting affects messages directed to the CORE side.

    The default value is: No Manipulation

  – **HMR for messages to the access side**:

    This dropdown configures the Header Manipulation Rules feature.

    When a profile is selected, all associated Lua scripts and configurations within that profile are applied.

    This setting affects messages directed to the ACCESS side.

    The default value is: No Manipulation

    NOTICE: When SBC is in **Standalone With Internal SIP stack (BYOT – Bring your own trunk)** mode, the feature will apply to Core Side.

5.5.2.1.2 SIP Privacy

- Define Session Border Control behavior in respect to receiving/sending/ignoring PAI (or PPI) header.
  – If Privacy Support is set to **Basic**, the OpenScape Session Border Control SHALL NOT send a P-Asserted-Identity header field in the messages (requests or responses) to the endpoint. The OpenScape Session Border Control SHALL also ignore any received P-Asserted-Identity header fields.
  – If Privacy Support is set to **Full**, the OpenScape Session Border Control SHALL send a P-Asserted-Identity (or a P-Preferred-Identity) header field in the messages (requests and responses) to the endpoint. The OpenScape Session Border Control SHALL also accept any received P-Asserted-Identity header fields. If the caller ID is restricted, the "Privacy: id" header will be sent to the SSP.
  – If Privacy Support is set to **Full-Send**, the OpenScape Session Border Control SHALL send a P-Asserted-Identity (or a P-Preferred-Identity) header field in the messages to the endpoint. However, the OpenScape Session Border Control SHALL ignore any received P-Asserted-Identity header fields. If the caller Id is restricted, the "Privacy: id" header will be sent to the SSP.
  – If Privacy Support is set to **Full-Receive**, the OpenScape Session Border Control SHALL NOT send a P-Asserted-Identity header field in the messages (requests and responses) to the endpoint. However, the OpenScape Session Border Control SHALL accept any received P-Asserted-Identity header fields.

5.5.2.1.3 SIP Service Address

- **Use SIP Service Address for identity headers** - When enabled, for both normal and survivability modes, identity header fields are modified to include the SIP Service Address network domain field.
- **SIP service address** - FQDN or IP address identifying the network domain for the SIP Service Provider.
- **Use SIP Service Address in Request-URI header** - Modifies Request-URI header to include the SIP Service Address network domain.
- **Use SIP Service Address in From header** - Modifies From header to include the SIP Service Address network domain.
- **Use SIP Service Address in To header** - Modifies To header to include the SIP Service Address network domain.
- **Use SIP Service Address in P-Asserted-Identity header** - Modifies P-Asserted-Identity header to include the SIP Service Address network domain
- **Use SIP Service Address in Diversion header** - Modifies Diversion header to include the SIP Service Address network domain
- **Use SIP Service Address in Contact header** - Modifies Contact header to include the SIP Service Address network domain
- **Use SIP Service Address in Via header** - Modifies Via header to include the SIP Service Address network domain
- **Use SIP Service Address in P-Preferred-Identity header**- Modifies P-Preferred-Identity header to include the SIP Service Address network domain

5.5.2.1.4 SIP User Agent

- **SIP User Agent towards SSP** - Default value is `Passthru` for all SSP profiles. Available options:
  - **Passthru** - the **SIP User Agent** configuration box is grayed out.If no **SIP User Agent** is received from the LAN side, nothing will be added.
  - **Add if non received** - the received User Agent from the LAN side is passed on unchanged.
  - **Add or Replace** - the received User Agent from the LAN side will be replaced with the configured User Agent.

  IMPORTANT: If no User Agent is received from the LAN side, the configured User Agent will be added

- **SIP User Agent** - Configurable SIP User Agent able to recognize a SIP soft switch and apply dynamically a profile to this SIP soft switch and monitor it. Up to 32 alphanumeric characters allowed, e.g `OSBC-test-24`

5.5.2.1.5 Registration

- **Registration required** - If selected (enabled), the Branch will send registrations to SSP (60-7200 seconds).
- **Registration interval (sec)** - Registration interval in seconds.

  NOTICE: The Registration interval displayed in the list of configured SIP Service Providers Profiles is applicable only if Registration required is selected (enabled) for that SIP Service Provider.

5.5.2.1.6 Business Identity

- **Business identity required** - if enabled, requires the caller identified in the From header field contain the Business Identity DN.
- **Business identity DN** - Contains the Business DN. Parameter takes precedence over Default Home DN if both are configured for the From Header.

5.5.2.1.7 Outgoing SIP manipulation

- **Insert anonymous caller ID for blocked Caller-ID** -If enabled, blocked Caller-ID's will be updated by adding Anonymous to message headers.
- **Manipulation** - Opens the Manipulation configuration window allowing creation/modification/deletion of specific SIP manipulation rules.

5.5.2.1.7.1 Manipulation

SIP Service Provider (window) > Outgoing SIP Manipulation (section)

Under this window it is possible to perform digit manipulation for the outgoing SIP message on the following SIP Headers:

- **R-URI**
- **From**
- **P-PI**
- **P-AI**
- **Diversion**
- **P-AI (or FROM if no P-AI exists)** - manipulates the digits in the P-Asserted Identity Header or, the digits in the From Header when no PAI header is present

A new digit manipulation rule is added using the **Add** button. In this case a new row is created in the table.

- **Match digits-** This parameter defines the matching digits. Only numerical digits or the character "+" are supported
- **Match Position-** This parameter defines from which digit position the matching is performed on the header. The first position is 0.
- **Match Length**- Enter a valid value (format x, x/, or x/y) for field Match length.
- **Header-** The legal SIP Header values are listed at the top of this section.
- **Delete/insert position-** This parameter defines from which digit position on the header the fields "Number of digits to delete" and "Insert digits at position" are applied. If the value of this parameter does not correspond to an effective position on the header digits, the related operations will be ignored. The first position is "0".
- **Number of digits to delete-** the number of digits to be deleted from the defined position. If there are not enough digits to be deleted from the defined position on the header, this operation will be ignored.
- **Insert digits-** The digits to be inserted at the defined position
- **Add prefix-** The prefix to be added to the digits on the header.
- **Replace all with-** The digits to replace all header digits.
- **Call Type-** The Call Type that digit manipulation applies. The current option is 'SIP-Provider'.

To delete a digit manipulation rule select the row and then use the **Delete** button.

Once the rules are entered or deleted the and the window will close. To apply this configuration the user must click on **Changes**

5.5.2.1.8 Incoming SIP Manipulation

- **Calling Party Number** - Most of SSPs send the calling party number only in the user party of From or P-Asserted-Identity headers. However, some provides send the user and display name parts of those headers as described in RFC2161. This configuration item allows to configuration which information shall be used.

  The possible options are:

  – **From header user and display name part** - Preserves the user and display name parts of From header. Default value.
  – **From header user part** - Uses the From user part as the Calling Party Number. If present, the display name is removed from this header.
  – **From header display name part** - Uses the display name part of the From header as the Calling Party Number. If present, the display name replaces the user part in From header. Otherwise, no manipulation is done.
  – **P-Asserted-Identity user part** - Uses the P-Asserted-Identity user part as the Calling Party Number. If present, the display name is removed from this header.
  – **P-Asserted-Identity display name part** - Uses the display name part of the P-Asserted-Identity header as the Calling Party Number. If present, the display name replaces the user part in P-Asserted-Identity header. Otherwise, no manipulation is done.

  NOTICE: This configuration applies to both Normal and Survivability modes of OSB. When in Survivability mode, the SIP Manipulation configured in the OSB may apply to From and P-Asserted-Identity headers. However, the SIP Manipulation is applied only after the SSP Calling Party Number manipulation.

- **SIP User Info header and Regex**: Available only for SIP Service Provider Profile with "MS Teams" as the Default SSP profile. It allows the

manipulation of the user part of incoming From or/and P-Asserted-Identity headers using a regular expression.

It is possible to select the following options:

1) None
2) From header
3) P-Asserted-Identity header
4) From and P-Asserted-Identity headers

The first item disables the feature and is the default value. The other options modify the respective header and require the configuration of Regex, which is a regular expression based on POSIX regex substitutions.

Regex format

The regex format is the following: /{ME}/{RE}/{F}

See below the description for each item:

– {ME}: Match expression (Posix regular expression)
– {RE}: Replacement expression is substitution expression with back references to matched tokes: \1, \2, ..., \9
– {F}: flags (optional):
  – i - match ignore case
  – s - match within multi-lines strings
  – g - replace all matches

Some characters are not allowed by configuration ("|", "@", "<", and ">") and the limit is 64 characters in length.

If the match expression has no match, the replacement is not performed. The same occurs if the regular expression does not result in a valid URI user part.

Example:

– Received From header URI: sip: +441291222222;ext=6963333@sip.pstnhub.microsoft.com:5061;user=phone
– Received User part of From header URI: +441291222222;ext=6963333
– Regular expression configured for From header: /^.*;ext=(.*)$/\1/
– New user part of From header URI: 6963333

IMPORTANT: The configuration options listed below are only available in V11R1.01.00 or higher.

- **Change tel URI to sip URI in PAI header** - If enabled, the incoming call converts a PAI header with TEL URI to a PAI header with SIP URI. In that case, the parameter "user=phone" is included in the SIP URI.
- **Remove email from PAI header** - If enabled, the incoming call with e-mail (alphanumeric user and domain) in the PAI header is removed.

5.5.2.1.9 Flags

- **FQDN in TO header to SSP** - If selected (enabled), To header is modified for the in-dialog SIP Requests sent to SSP with FQDN configured for SSP.
- **Use To DN to populate the R-URI** - Enable if the SIP Service Provider is sending the Account information in the Request URI and the destination information in the To header. Disabled by default.

- **Send Default Home DN in Contact for Call messages** - If enabled, the configured default home DN is used to set the Contact header only for call messages.It is not applicable for REGISTER message. Disabled by default.
- **Allow SDP changes from SSP without session version update** - Flag to take care of SSP which are incorrectly keeping the same session id and session version but changing the contents of the SDP.
- **Do not send INVITE with sendonly media attribute** - Do not send INVITE with send only media attribute to SSP
- **Do not send INVITE with inactive media attribute** - Change ‘inactive’ media attribute to ‘sendrecv’ in the OFFER SDP
- **Do not send ANSWER SDP with inactive media attribute** - Change ‘inactive’ media attribute to ‘sendrecv’ in the ANSWER SDP
- **Do not send INVITE with video media line** - Do not send INVITE with video media line to SSP
- **Do not send Invite without SDP** - Do not send INVITE without SDP to SSP. When enabled, the SBC interworks an INVITE without SDP to an INVITE with SDP towards the SSP, which does not support INVITE requests without SDP. All re-invites originating from the core side that include SDP, will be delivered to the access side using normal processing procedures such as transcoding and m-line type modifications. However, if a re-invite without SDP is sent from the core side to the access side, SSM will retrieve the most recent SDP sent to the access side, remove the media attribute (sendrecv, inactive, sendonly, or recvonly) and send the re-invite to the access side.

NOTICE: The "Do not send re-Invite" flag precedes the "Do not send Invite without SDP" flag. When using the "Do not send Re-Invite" flag, it is recommended not to use the endpoint attribute "Enable Session Timer" in the corresponding endpoint (OSV).

WARNING: When this flag is being used, there is a restriction to use Mikey and DTLS in Media Profile (core and access side). If Mikey or DTLS are configured in the media profile, GUI displays an error message during **Apply Changes**. The recommended migration path is to move the configuration from MIKEY or DTLS to SDES.

WARNING: When the "Do not send Invite without SDP" flag is enabled, the session timer refresh (INVITE message) is allowed to pass through. If the "Do not send Re-Invite" flag is enabled, the session timer refresh (INVITE Message) is blocked.

NOTICE: Starting from V10R3.03.00.

- **Renew core side crypto keys**: Starting from V10R3.1.3, with this feature every answer generated by the system is assigned a new crypto key on the core side.

  IMPORTANT: This flag is used only when the flag **Do not send invite without SDP** is activated. If not, this flag is grayed out.

  If a new crypto context is necessary, it is recommended to activate the flag **Reset SRTP context upon key change** in folder VOIP/Media for long calls with SRTP.

  When the flags **Renew core side crypto keys** and **Reset SRTP context upon key change** are enabled, after each re-invite with SDP, the crypto context is recreated. This implies a new sequence number and a reset of the Roll-Over Counter. This flag only changes the crypto in the SDP. If the endpoint does not support a crypto refresh, do not use this flag.

  NOTICE: The combination of the flags **Renew core side crypto keys** and **Reset SRTP context upon key change** implies non-RFC behavior.

- **Do not send Re-Invite when no media type change** - Do not send re invite to SSP if there is no change in the media type characteristics towards SSP (e.g. audio to audio re-invite).

  NOTICE: Old Codecs from the SSP would be reused towards the core and hence requires that at least one common codec should exist between all endpoints including SSP.

- **Do not send Re-Invite** - Do not send re invite at all to the SSP.

WARNING: The "Do not send re-Invite" flag precedes the "Do not send Invite without SDP" flag. When using the "Do not send Re-Invite" flag, it is recommended not to use the endpoint attribute "Enable Session Timer" in the corresponding endpoint (OSV).

WARNING: When any of the flags are enabled, T38 fax negotiation is not possible. If a Re-Invite with T38 is received, a **488 Not Acceptable here** message is displayed.

WARNING: When these flags are being used, there is a restriction to use Mikey and DTLS in Media Profile (core and access side). If Mikey or DTLS are configured in media profile, the Gui displays an error message is during **Apply Changes**. The recommended migration path is to move the configuration from MIKEY to SDES.

NOTICE: When the "Do not send Invite without SDP" flag is enabled, following implementation linked to Support

for Session Refresh, the session timer refresh (INVITE message) is allowed to pass through. However, if the "Do not send Re-Invite" flag is enabled, the session timer refresh (INVITE Message) is blocked, maintaining the feature's original functioning.

- **Remove Silence Suppression parameter from SDP** - Remove the attribute for silence suppression and related codecs coming from and going to the SIP Service Provider. Disabled by default.
- **Enable pass-through of Optional parameters**- When enabled, you may configure up to 10 optional SIP - Header parameters pass-through for Call handling to / from SIP Service Providers (SSPs). You only need to add the parameter name (e.g. "alias").Disabled by default.
- **Force direction attribute to sendrcv**- This flag indicates if the SDP Media Attribute will be maintained, added or changed to sendrecv. This configuration is recommended for providers that do not accept to receive SDP without direction attribute.

  IMPORTANT: This configuration only applies for SIP responses.

- **Send default Home DN in PAI** - When enabled, the respective configured Home DN is replaced in the user part of the P-Asserted-Identity header if available for the message to the SSP.
- **Send default Home DN in PPI** - When enabled, the respective configured Home DN is replaced in the user part of the P-Preferred-Identity header if available for the message to the SSP.
- **Preserve To and From headers per RFC2543** - When set the To and From header to the SSP would match the URI received from the SSP in order to meet the RFC2543 dialog matching requirements.
- **Disable FQDN pass-through in FROM header**-When FQDN is received in FROM header if this flag is enabled the appropriate IP interface address will be used in the core to access side mapping. If the flag is disabled the FQDN received will be passed transparently to the other side.

  NOTICE: When "Disable FQDN Passthrough in FROM header" is enabled and FQDN is received in FROM header the "SIP Service Address" is not used in FROM header even if "Use SIP Service Address for all identity headers" is enabled.

- **Keep Digest Authentication Header** - after receiving the first challenge, SBC will keep sending the authentication header, incrementing the nonce count each time. The SSP must challenge again if the registration fails at some point.
- **Send Contact header in OPTIONS**- This flag modifies the OPTIONS messages to include the Contact header when it is not present.

  When the option **Use SIP Service Address in Contact header** is set, the SIP service Address will be used in the Contact header. Otherwise, the external firewall, when enabled, or the endpoint IP will be used.

- **Do not send Privacy header in response messages**- This flag removes Privacy header from SIP response messages 183 and 200.

  When the option **Do not send Privacy header in response messages** is set, the responses to original INVITE sent with Privacy header will have this header removed.
- **Remove bandwidth (b) lines from SDP**- This flag removes the bandwidth parameters from the SDP session and media lines present in the messages sent to the SSP.
- **Keep P-Asserted-Identify from access side**-This flag keeps the original P-Asserted-Identity (PAI) header received from the access side. This flag prevents the PAI header to be changed by OS-SBC.

  NOTICE: This flag is not directly associated with emergency calls and can be used in other situation.

- **Avoid sending 183 messages**- When this flag is set, the SBC does not forward the 183 Session Progress response messages received by the SSP to the core side.
- **Avoid sending 180 message (for 60s)**- In scenarios concerning outgoing calls from SBC, this flag prevents the multiple 180 Ringing informational messages sent from SSP to be forwarded to the SBC core side, for 60 seconds, after the last 180 Ringing message.

  NOTICE: The flags **Avoid sending 183 messages** and **Avoid sending 180 messages (for 60s)** have been created for MS Teams but can also be used by other SSPs.

- **Remove SDP from received 180**- If set, the SBC will remove the SDP from received 180 Ringing messages
- **Remove SDP from received 183**- If set, the SBC will remove the SDP from received 183 Session Progress messages
- **Send supported P-Early-Media header in initial INVITE**- If set, the SBC adds the "P-Early-Media: supported" header in the initial INVITE
- **Do not clean resolved IP's from Remote Endpoints FQDNs**- If set, the SBC will retain the resolved IP addresses of the associated Remote Endpoint FQDNs. This option is useful in scenarios where the FQDN IP addresses change frequently.

5.5.2.1.10 TLS

- **TLS Signaling** - This box is used to configure how TLS as a transport type will be signaled in the SIP messages of remote endpoint calls. Possible values are:
  - **Transport=tls** - Uses parameter "transport=tls" in SIP messages and does not accept SIPS URI.
  - **SIPS Scheme** - Uses the TLS connection to identify the transport type of registration, uses SIPS URI in Record-Route header of remote endpoint requests.
  - **Endpoint Config** - Uses the remote endpoint configuration to determine the transport and does not use "transport=tls" nor SIPS URI in the SIP Message.
  - **Pass-Thru** - Accept or Send transport=tls or SIPS in SIP Message.

5.5.2.1.11 SIP Connect

- **Use Tel URI** - When the SSP requires the use of tel URIs the user must check this box. In this case the SBC converts all SIP URIs to Tel URIs towards the SSP and vice versa. The following SIP Headers could be modified: **Contact**, **To**, **From**, **Referred-By**, **Refer-To**, **P-Preferred-Identity (PPI)**, and **P-Asserted-Identity (PAI)**.
- **Send user=phone in SIP URI** - When checked, the SBC adds “user=phone” in SIP URIs towards SIP-SP.This flag is applicable when user part in SIP URIs is **GNF** (**Global Number Format**). The endpoint for SSP should be configured on OSV with the following attribute: “**Send International Numbers in Global Number Format (GNF)**“

  NOTICE: In order to be SIP Connect 1.1 compliant the certificates presented by the OS SBC shall use a SIP URI in the subject AltName and Common Name fields, in accordance with [RFC 5280]. The OSV Solution recommended way to create certificates is to use OpenSSL where it shall be possible to specify the above fields using a SIP URI.

- **Registration Mode** - When Registration Mode flag is enabled, SBC will be sending Register message with **Registration Mode** format of SIP Connect 1.1 that will add the following headers:
  - Proxy-Require: gin
  - Require: gin
  - Supported: path
  - Allow-Events: vq-rtcpx
- **Bulk registration required** - When checked, then the Registration AOR must also be configured. In this case the OSB/SBC shall use the configured Registration AOR in the FROM and TO headers of the REGISTER request towards the SSP.
- **Registration AOR** - The SIP-PBX must be capable of provisioning any format of SIP-URI as the Registration AOR, in order to accommodate SP-SSE requirements.

5.5.2.1.12 Survivable Branch Appliance (SBA)

This flag enables the MS Teams Survivable Branch Appliance (SBA) for Direct Routing. When the SBA is activated, the SBC will fork Public Switched Telephone Network (PSTN) calls to the Microsoft Phone System and the SBA. This configuration ensures that Microsoft Clients can sustain the ability to initiate and receive PSTN calls even when communication with the Microsoft Cloud is disrupted.

- **Enable SBA for MSTEAMS**

  If the checkbox is enabled, the SBA service is enabled and the fields must be set up.
- **Certificate profile**

  The certificate must be the same as the one added on the SBA Server. It is recommended to use a specific certificate for the SBA.
- **FQDN**

  The SBA Server FQDN.

- **Port**

  By default, SBA uses port 5061.

5.5.2.1.13 Emergency call configuration

In the SSP profile, a new flag enables the PSAP capabilities, identifying the emergency call by the Priority header on the origin endpoint. Once the **Enable PSAP capabilities** flag is set, new configuration options become available:

- **Geolocation forward**: This flag enables the RFC-6442 (geolocation header) to be sent to the next hop. The default option is enabled.
- **Map ELIN to PAI header**: This flag is used to move the ELIN string to PAI header. The default option is disabled.
- **Enable callback based on ELIN**: A flag to allow callback calls from the original B-side to be forwarded to the original caller.
  - **Callback binding timeout**: It defines the maximal time for a callback after the end of the emergency call, which is identified by the ELIN association to the caller. After this time the biding/association is removed. It is configurable from 30 to 300 minutes. The default value is 30 minutes.

New emergency calls with the same ELIN will overwrite the previous callback binding. This means that callbacks to that ELIN will connect to the most recent caller from an emergency call if it takes place during the callback binding period.

Other emergency parameters i.e. ELIN as part of the From/PAI header will be automatically bypassed when the flag “Enable PSAP capabilities” is set.

5.5.2.1.14 Source Based Routing table

IMPORTANT: This configuration is only available in V11R1.01.00 or higher.

- **Source Based Routing table** - In the table it is possible to add a prefix and alias core port. The prefix can have up to 20 characters and can contain digits and the characters "[", "]", ",", "+", "-", "X", and "#".

  The character "+" can be used in the initial prefix.

  The character "X" means any digit that can be included in any position.

  The character "#" can be used in the last position to indicate that no more digit is expected after a prefix.

  Ranges of digits can be configured as in the following example:

  – "[23-34,55-58]" means two ranges: one from 23 to 34 and another from 55 to 58.

  A list of numbers can also be configured using brackets:

  – For example, the list of numbers 234, 345, and 678 can be configured as "[234,345,678]".

  When multiple prefixes match the configured header for source base routing, the following priority sequence will be used:

  1) The Specific Prefix (complete digits)
  2) Prefix with wildcards "X"
  3) Ranges of digits in multiple prefixes

  The Alias core port column should contain one alias core port within the range of remote endpoint core ports. This port can be duplicated in one or

more rows in the table and can be included in other profiles tables. However, it should not be configured as a core port of a remote endpoint.

- **Routing mode** - This item allows enabling the source base routing using the user part of PAI or From header. The options are:
  - **Disabled** - Disable the source base routing.
  - **Based on PAI header user part** - Use the PAI header user part to match a prefix for an alias port.
  - **Based on From header user part** - Use the From header user part to match a prefix for an alias port.
- **Send OPTIONS to Alias ports** - This flag allows sending SIP OPTIONS messages periodically with 60s intervals to all configured alias ports from the profile prefix table.

5.5.2.2 Remote Endpoints Configuration

Remote Endpoint Settings

In this section Routing objects and Identity objects are associated with realms to allow signaling and media flows through the OS-SBC.

Remote endpoints considered routing objects are configured to form a static association between the core and access realms.

Once a realm association is formed, an internal route is established within the OS-SBC between the access and core realm network interfaces. This route is used to support signaling and media flows between remote network interfaces in the access realm and the SIP server in the core realm.

- **Name** - Remote endpoint name
- **Type** - This box defines the remote endpoint type, options are: `Gateway`, `Proxy`, `Branch SBC`, `Media Server`, `SSP`, `SBC`, `OSBIZ`.
- **Profile** - In this box it is possible to choose a profile according to the remote endpoint **Type** assigned. Possible options: `Gateway`, `Proxy`, `Branch SBC`, `Media Server`, `SSP`, `SBC`, `OSBIZ`
  - For types **Gateway**, **OSBIZ**, **Proxy** and **Branch SBC**, a default profile is assigned.
  - For types **Media Server** and **SSP**, pre-configured profiles can be chosen.
- **Access realm profile** - The default "`Main-Access-Realm`" is shown by default when adding a new remote endpoint to the configuration, otherwise the configured realm profile is shown. The user may select an alternative access realm profile from the pull-down list which includes all access realm profiles. The Access Realm provides a default access IP association to the Remote Endpoint. Location of the Remote Endpoint is also learnt dynamically based on the access IP. However, if there is no message received from the Remote Endpoint then the assigned access IP is used to reach the Remote Endpoint.

NOTICE: The drop-down list shall not offer a profile that is already in use for a dynamic remote endpoint with disabled access control. For endpoints with **Support Peer Domain** checked and **Enable access control** unchecked, the drop down list shall not offer a profile that is already in use by another endpoint or subscriber.

- **Core realm profile** - The default "`Main-Core-Realm`" is shown by default when adding a new remote endpoint to the configuration, otherwise the configured realm profile is shown. The user may select an alternative core realm profile from the pull-down list which includes all core realm profiles.

  NOTICE: Once a realm profile selection is made the system SHALL perform a cross check to ensure that the selected realm profile belongs to the appropriate realm type being configured before being allowed to proceed.

- **Associated Endpoint** - This pull-down box is enabled when the remote endpoint Type is `Media Server`, `SSP` or `Gateway`. The user is then given the opportunity to associate the remote endpoint with another remote endpoint.

  IMPORTANT: A remote endpoint can be associated to any type except `Media Server` if the **Standalone** mode is enabled.

- **Linked Endpoint** - This field is used to identify that the endpoint is linked to another endpoint as the final destination, i.e.,SSP linked to a gateway behind a branch will have the branch as associated endpoint and the gateway as a linked endpoint.
- **Enable Call Limits** - Enable/Disable limit sessions for this specific endpoint based on the values configured.
- **Maximum Permitted Calls** - Maximum allowed number of simultaneous calls for this endpoint. When checking for session limits, the total sessions take precedence of endpoint session limits. So if total session limit has been reached, a call to/from and endpoint would be rejected if the endpoint session limit has not been reached.

  Default value set at 0.
- **Reserved Calls** - Number of calls guaranteed for this endpoint at any time. This number must be lower than the overall licensed sessions and the sum of all reservations across multiple endpoints MUST not exceed the overall sessions limit.

  Default value set at 0.

  NOTICE: Emergency calls are not subjected to rejection even after limit is reached.

SSP OPTIONS

IMPORTANT:

This session is available only for endpoints of type SSP when the **Comm System type** is configured with "Standalone with internal SIP Stack" or when the feature standalone is enabled. For more information see SIP Server Settings on page 312.

The **Enable SSP connectivity check** flag can be enabled for the endpoint. It is also possible to configure the **OPTIONS interval (sec)**. When enabled, the flag will affect the **SSP connectivity status** in the field SSP Connectivity check, and in the routing selection.

Remote Location Information

- **Support Peers Domains**: Enables the usage of URI based routing, which means that the OSS routes the call based on the Request URI that is contained in the INVITE received from the OSV. When this box is not checked, the OSS routes the call based on the static remote endpoint configuration.

  NOTICE:

  When a connection with a Foreign Peer Domain is established, if the Sip Server is restarted, the connection information is lost and in-dialog requests will not be routed correctly.

  NOTICE:

  When an external firewall is used, the firewall port must be the same as the SBC access interface port. Otherwise some problems can occur with the ports inside the sip message

- **Support Foreign Peer Domains**: Enables the usage of URI based routing without having the remote URL configured in Remote Location domain list. For incoming calls from the Access side (WAN), the call will be accepted when the destination in the request URI matches any entry in the whitelist. When the white list is empty, only outgoing calls coming from the Core side are allowed. This configuration is available only when remote endpoint type is set to `Gateway`.

  NOTICE:

  Foreign Peers Domains use the Default media profile

  NOTICE:

  By default, only calls with video m-line are accepted for **Support Peers Domains** and **Support Foreign Peer Domains** endpoints. You can change this configuration by disabling the attribute **Accept only Video Calls from Peer Domains** in **Security > General** tab

  NOTICE:

  You can configure only one remote endpoint with the attribute **Support Foreign Peer Domains** enabled in the system.

- **Whitelist**: Enables the configuration of allowed URLs in the destination R-URI for the incoming calls, when the attribute **Support Foreign Peer Domains** is enabled.

  The possible items added to the whitelist to match the destination are:

  – only exact match: sip:user@domain or sip:user@IPAddress
  – wildcard match *@video.unify.com or *.video.unify.com for all video devices in video.unify.com realm
  – regular expression e.g. sip\:sub\d\d\d\d\d@video\.unify\.com to match string sip:sub12345@video.unify.com
  – the wildcard on both user and domain part is not allowed for complete fields, meaning *@*
  – The entry must begin with "*", "sip\:" or "sips\:"
  – IPv6 entries are allowed, use [and] to indicate IPv6 entry.
  – Allowed characters: A-Z a-z 0-9 . - _ + \ [ ] : @ ? & = ( ) +
  – Ending character must match $? + * A-Z a-z 0-9)]
- **Enable Access Control**: You can activate this check box only when the **Support Peers Domains** check box is checked. Otherwise, this field is deactivated. When you check this box is, the access control functionality is enabled by allowing multiple entries in the Remote Location Domain list. Calls are only possible when the source or the destination remote URL is configured. Incoming calls from the Access side are authenticated by source IP address authentication. When you disable the **Enable access control** flag and the remote endpoint is configured with the flag **Support Peer Domains**, incoming calls are accepted from unknown peers if the MTLS negotiations are successful. The Remote Location Domain list contains exactly one entry with a blank remote URL in this case. Otherwise, multiple entries are allowed.

  When he incoming call, in this case, is not (M)TLS, then a search for a remote endpoint with a whitelist match is executed.

  IMPORTANT:

  URI based routing and Allow Open Alphanumeric Access are deprecated.

- **Signaling address type** - Identifies how the "IP address/FQDN" parameter shall be used for addressing the Remote Endpoint. The following options are available based on their configuration criteria:

  – `IP address or FQDN` - **Type** is: `Gateway`, `Proxy`, `Branch SBC`, `Media Server` or `SSP`.
  – `DNS SRV` - **Type** is: `Gateway`, `Proxy`, `Branch SBC`, `Media Server` or `SSP`.
  – `DNS NAPTR` - **Type** is: `SSP`.

  NOTICE: DNS NAPTR is available starting from V11R2. For more infromation on configuring DNS NAPTR, see the SBC V11 Configuration Guide.

  NOTICE: The Signalling address types **DNS SRV** and **DNS NAPTR** are allowed only if the Gateway is a SIP Trunk.

Remote Location domain list

Click **Add** to add a new Remote Location Domain to the Remote Endpoint.You may edit the new or existing Remote Location domain by pressing the **Edit** button.

Multiple entries (up to 255 entries) are only allowed for the remote endpoint **Type** `Gateway` and when the **Support Peer Domain** and **Enable access control** fields are checked. Multiple peers can be configured which can be source or destination of a call.Two or more remote endpoints may share the same SSP. In case of incoming calls, the remote endpoint will be determined based on either on Default home DN or Business Identity provided in from header.

To delete an existing Remote Location domain, select the row entry followed by the **Delete** button.

Remote Location Identification/Routing

- **Core FQDN** - (optional) Only an FQDN is supported, not an IP address, since the Core IP can be obtained from the Core Realm signaling interface identified in the configured core realm profile.
- **Core realm port** - For remote endpoints which are not of Type = Media Server, the port value must be assigned from the system-wide static port range. For each remote endpoint the Core Realm IP address and Core Realm Port must be unique. For a Type = Media Server this port MUST match the value 2427.
- **Default core realm location domain name** - In the absence of a Location Domain identifier from the remote server a default value can be signaled into the core realm network.
- **Default Home DN** - This configuration applies when the endpoint is a SSP. This configuration parameter was moved from the SSP Profile.

  In outgoing calls to the SSP, the Default Home DN is used to populate headers such as Contact, PAI and PPI according to the SSP profile configuration.

  A maximum 30 character string of alphanumeric characters as well as the supported set of symbols ("-" "_" "." "~" "*" "(" ")" "=" "+" "$" ";" "?" "/").
- **Enable routing based on domain** - This configuration applies when the endpoint is an SSP. It allows the incoming calls to be routed according to the destination FQDN present in the To header. When enabled, a unique FQDN can be assigned to the SSP, which will be used as selection criteria when more than one SSP is associated with the same SIP Service Provider.

  NOTICE: This configuration disables the incoming routing by prefixes.

  IMPORTANT: This configuration is available only from V10R2.
- **Incoming Route Prefixes** - In incoming calls from SSP, some providers use the R-URI as the Default Home DN or specific range of numbers. It is used to identify the remote source endpoint when there is more than one endpoint

associated to the same Sip Service Provider. It only shows if the gateway/ trunk type is set to SIP Trunk.

This table stores up to 10 prefixes associated to a remote endpoint, the query for the endpoint is then based on a best match of configured prefixes. Any configured prefixes must not overlap another previously configured prefix, thus avoiding any duplication.

A maximum 30 character string of alphanumeric characters as well as the supported set of symbols ("-" "_" "." "~" "*" "(" ")" "=" "+" "$" ";" "?" "/").

Access Side Firewall Settings

- **Enable Firewall Settings** - The Firewall Settings are enabled by using this check box.
- **Firewall Settings** - This button is used to open the Firewall Settings configuration window.These firewall settings are specifically for this remote endpoint regardless of the system wide firewall settings. The remote endpoint firewall does not currently function if the remote endpoint is behind a dynamic NAT. (Defined with a logical-ID rather then an IP address).

Emergency configuration

Configuration of Emergency Calling requires administration of the following areas:

- **Emergency Calling Subnets** - This button opens the Emergency Calling window where it is possible to configure the emergency calling subnets.
- **Emergency Calling Numbers** - This is the list of Emergency numbers, that when dialed will allow the SBC to identify an Emergency Call. For USA, this is the 911 emergency numbers.

  A call to a number in this list will trigger the server to try to establish an outgoing call to a available gateway (highest priority).

  The search for a emergency destination is done as follows:

  – Try a gateway configured with emergency.
  – If no emergency gateway is available try to use lowest priority gateway looking at priority 1 gateways.
  – If the first and second searches fail then try a default gateway (priority 0).
  – If still no gateway is available then try to reach local attendant configured in LIN table.

  NOTICE: An association between the Emergency Number and the Emergency Calling Subnets is done by means of the routing prefix. Any number which is configured as an Emergency Number and matches to the first digits of the Routing Prefix will be associated to that subnet. For example, both 9 and 911 match the beginning of the Routing Prefix 911222, that means both are associated to that subnet. Due to this reason, you will not be allowed to delete the 9 neither 911.

Miscellaneous

- **Open external firewall pinhole** - When the SBC is under an external firewall, dummy UDP packets are sent towards the endpoint media

destination (connection address and port in the SDP) in order to dynamically open the firewall for the incoming media streaming.

This feature avoids several rules to be added to the firewall in order to keep open all possible addresses and ports used by the SBC for the media connection values.

NOTICE: This feature only applies for the addresses and ports used for the media streaming. It is not applicable to the SIP or MGCP protocols.

- **Send RTP dummy packets** - To address issues encountered by some providers with dummy UDP packets, a new **Send RTP Dummy Packets** configuration flag has been introduced.

  This feature allows the system to send RTP packets instead of dummy UDP packets, dynamically opening the firewall for incoming media streaming. These packets are sent to the endpoint's media destination (the connection address and port specified in the SDP).

  IMPORTANT: This configuration option is only available for systems running V11R1.01.00 or higher.

  NOTICE:

  If the current system uses **Standalone with internal SIP stack**, the **Send RTP dummy packets** flag is greyed out.

  The feature is only applicable to addresses and ports used for media streaming and does not apply to SIP or MGCP protocols. RTP dummy packets will have the payload type

negotiated by the SDP protocol, using the first codec listed in the SDP answer.

When **Send RTP dummy packets** is enabled, the following configurations are available:

- **Drop received RTP**- Drops incoming RTP packets before the SDP offer-answer process is completed.
- **Dummy RTP to Core side**- Sends dummy RTP packets to the core side, following the same configuration logic as the access side.

  Dummy RTP packets start is based on a timer:

  - **Stream Delay (ms)**- The amount of time, from ACK, to the start of dummy packets. The default value is 60 ms.

    If set to 0, the dummy packets will be sent right after ACK, with no delay.
  - **Stream Duration (ms)**- Duration of the dummy packet stream. The default value is 80 ms.

    If set to 0, only 1 dummy packet will be sent.

    - The minimum time for both fields is: 10 ms
    - The maximum time for both fields is: 3000 ms

NOTICE: Dummy stream will stop after receiving a RTP packet from provider.

IMPORTANT: These options are applicable for the locally connected SSP (as configured in the corresponding "Remote endpoint configuration").

5.5.2.3 Remote Location Domain

Each Remote Location domain has the following field.

General

- **Remote URL** - URL of the remote endpoint or domain. The URL can be entered as IP address (IPv4/IPv6), as domain (FQDN or domain name) or as Logical-Endpoint-ID.
- **Remote SIP/MGCP port** - Defines the port to be used in communication with the endpoint.
- **Remote transport**- Defines the transport protocol to be used in communication with the endpoint. For a Media Server endpoint, Transport must be UDP.

- **Logical ID Code** (only visible if the **Signaling address type** is set to **Dynamic IP**)- Previews the Logical ID hash code for the Remote URL.

  To display and copy the Logical ID Code, click **Show**.

  To export the logical IDs along with the hashes in a csv format, click **Export Logical IDs** under the **Remote endpoint configuration** area (see Remote Endpoints Overview).

  NOTICE:

  When **DNS SRV** domain name is enabled, the remote port is automatically set to 0. The port configuration is received through DNS SRV.

  When **DNS NAPTR** domain name is enabled (available starting from V11R2), the **Remote port** and **Remote transport** fields are grayed out. DNS NAPTR dynamically configures the transport protocol.

  For more information on configuring the **DNS SRV** and **DNS NATPR** records, refer to the SBC Configuration Guide.

Signaling

- **INVITE No Answer Timeout (msec)** - Final response timeout (in milliseconds) to an INVITE request that has not received a final reply. Range is 120000 to 600000 milliseconds. Default is 360000.
- **INVITE No Reply Timeout (msec)** - Timeout (in milliseconds) for an INVITE request or a non-INVITE transaction that has not received a provisional response. Range is 1000 to 32000 milliseconds. Default is 3000 msec.

  NOTICE: When a provisional response is received, this timer is stopped and the **INVITE No Answer Timeout (msec)** is set.

TLS

- **TLS mode** - Allow the selection between Server Authentication, Mutual Authentication and Client Mode (valid only if transport type is TLS).
  - Server Authentication - In this case only server being authenticated by client.
  - Mutual Authentication - In this case server and client authenticate each other
  - Client Mode only - Prevent the establishment of a TLS connection with the remote endpoint as a client.
- **Certificate profile** - Select the TLS certificate profile.
- **TLS Keep-Alive** - Enable the keep-alive mechanism if the connection was established by the SBC as TLS client.

  The Remote Endpoint in OS SBC can be configured to always be the TLS client and will be responsible for keeping the TLS connection alive. This means that the establishment of the TLS connection shall be initiated by the OS SBC, which will be responsible for keeping the TLS connection alive. The keep-alive mechanism is used to detect a TLS connection failure and. is executed by periodically sending a double carriage return / line feed (CRLF) to the other party. The other party shall respond with a single

CRLF. If the OS SBC do not receive a response from the other party, it shall conclude that the TLS connection has dropped and it shall reestablish the TLS connection. Notice that any message received from the peer side counts as a keep-alive response.

For TLS with Remote Endpoints other than SIP SP, OS SBC are typically a TLS server. This means that the Remote Endpoints will be responsible for initializing TLS and for keeping TLS up and running. In this case, OS SBC must respond to a keep-alive request (double CRLF) with a single CRLF.

If a Remote Endpoint is configured with transport type TLS, it listens to the configured TLS/MTLS port from Access Signaling network associated to respective Access Realm Profile of the Remote Endpoint (default port 5061/5161) for a request to establish a TLS connection.

- **Keep-Alive interval (sec)** - Determines the interval between sending the keep-alive requests. Valid values: 60 - 3600 seconds, default: 120.
- **Keep-Alive timeout (sec)** - Determines how long the TLS client shall wait for the keep-alive response before considering the TLS connection to be broken. Valid values: 5 - 120 seconds, default: 10.

Media Configuration

- **Media profile** - Select a Media Profile which is configured with the Media protocol, codecs, and packetization interval suited for the remote subscriber.
- **Media realm subnet IP address** - Some endpoints don’t use the same address for SIP and media (RTP) and can also use different subnet and network interfaces. This parameter is optional and is used to identify the endpoint in terms of media address.

  This parameter is accepted only for remote EP of types SSP, SBC, Gateway, and OSBIZ. It is configured in the remote_ep table for sipserver which informs ssm about the remote EP media address of the identified endpoint.

Digest Authentication

- **Digest authentication supported** - Enables Digest Authentication support.
- **Digest authentication realm** - Configures Digest Authentication realm. A realm can be specified with an IP address, a FQDN or in format user@domain.
- **Digest authentication user ID** - Configures Digest Authentication user.
- **Digest authentication password** - Configures Digest Authentication password.

Outbound Proxy Configuration

- **Outbound Proxy** - URL of the outbound proxy. The URL can be entered as IP address (IPv4/IPv6), as domain (FQDN or domain name). If configured, the SIP messages are sent via outbound proxy to the remote endpoint.
- **Outbound Proxy Port** - Defines the port to be used in communication with the outbound proxy.

NOTICE: The remote endpoint address type applies to Outbound Proxy address, i.e, if remote endpoint is configured in terms of DNS SRV, the same shall apply to the Outbound Proxy.

NOTICE: The Outbound Proxy settings are grayed out if the endpoint is not a SIP Trunk.

Registrar Server Configuration

NOTICE: The Registrar settings are grayed out if the profile is not using Registration

- **Registrar Server** - URL of the registrar server. The URL can be entered as IP address (IPv4/IPv6), as domain (FQDN or domain name). If configured, this address is used to populate the SIP Request-URI and other header fields of the REGISTER request.
- **Registrar Server Port** - Defines the port to be used in communication with the registrar server.

5.5.2.4 Firewall Settings

Firewall Settings

- **enable SIP UDP** - If selected allows SIP through UDP.
- **enable SIP TCP** - If selected allows SIP through TCP.
- **enable SIP TLS** - If selected allows SIP through TLS.
- **enable MGCP** - If selected allows exchanging messages through MGCP protocol.
- **enable DNS** - If selected allows exchanging messages through DNS protocol.
- **Message rate threshold** - Defines the number of kilobytes per second which will block an IP address.
- **White list** - Allow Incoming WAN network connections for a specific IP or Logical-Endpoint-ID/Port. If the Port field is empty, all ports will be allowed.
- **Black list** - Block Incoming WAN network connections for a specific IP or Logical-Endpoint-ID/Port. If the Port field is empty, all ports will be blocked.

5.5.2.5 Emergency Calling

Emergency Calling Subnets

A new Emergency Calling Subnet is created clicking the **Add** button. An existing Emergency Calling Subnet can be changed using **Edit** button and deleted using **Delete** button.

Clicking on the **Add** or **Edit** button launches the Emergency Calling Subnet window.

5.5.2.6 Emergency Calling Subnet

General

- **IP address or subnet** - This configures the IP address (or range of IP addresses) of the subscriber(s).

  NOTICE: Default Subnet: the entries IP=255.255.255.255 and Mask=255.255.255.254 create a Default Subnet, which will be used for all phones not comprised in any configured subnet. The usage of Routing Prefix is exactly like the normal subnets.

- **Subnet mask** - This configures the IP subnet of the range of subscribers defined by the IP Address configuration. If a single subscriber is configured use mask 255.255.255.255.
- **Routing prefix** - This configures a preferred gateway to be used by this emergency subnet. The first digits of each prefix also links the current Subnet to a dialed Emergency Number. For example, prefixes like "91122" or "91133" restrict the Subnet to be used with a configured "911" Emergency Number.
- **Description** - T
- **Default destination** - T
- **Send LIN instead of CPN** - This option, when checked, is used to avoid the adding of the Calling Party Number in MIME and use the Location Identification Number instead (Configured in Emergency Calling Subnets Table). Use this option if your Gateway does not accept the emergency calls using MIME.

  NOTICE: Default Subnet: the entries IP=255.255.255.255 and Mask=255.255.255.254 create a Default Subnet, which will be used for all phones not comprised in any configured subnet. The usage of Routing Prefix is exactly like the normal subnets.

LIN

LIN table: This is where a list on LIN numbers is constructed or edited, only visible after clicking on **Add** or **Edit** buttons. One LIN number may be used to identify an outgoing emergency call. Different LINs are necessary to allow multiple emergency calls to take place in parallel. Please note that this table must provide enough LINs so the emergency services are not constrained.

- **LIN** - It is the Location Identification Number used to associate a subscriber to its physical location. Only numerical digits or the character + are supported.

  NOTICE: Emergency calling numbers is not allowed for Proxy ATA mode.

Please note that when LIN should be sent out on emergency calls, the LIN table should be provisioned with enough LIN numbers for allowing multiple emergency callbacks to happen. If somehow all LINs are occupied at the time an emergency call is made, this call is redirected to the Default Destination, since no callback would be possible without a valid LIN. Please also note that

allocated LINs may get reassigned to new calls after 15min, so a callback for the former call may not be possible after this time.

IMPORTANT: Emergency callback calls which cannot be routed to the original caller will be routed to the Emergency Default Destination.

Location Information

OpenScape SBC supports transparent conveyance of location information (i.e. the GeoLocation header field and the PIDF-LO) from the phone towards the OpenScape Voice.

The location information will be added to an INVITE if all the following conditions are met:

1) The INVITE request was received from a SIP subscriber
2) The DN part of the R-URI corresponds to the routing prefix of an emergency call
3) The flag Enable Geo-Location Support is checked

- **Country** - Country is available through a drop down menu with 2 uppercase characters.The field is mandatory and the maximum length is set at 2 characters, e.g. US
- **State of region or province** - it is used for the top-level subdivision within a country.The field is mandatory and the maximum length is set at 3 characters e.g. TX.
- **County or parish or district** - The field is mandatory. Any string can be used, maximum length set at 150 characters, e.g. GRIMES COUNTY.
- **City** - Mandatory field, maximum length set at 150 characters.
- **Street** - Mandatory field, maximum length set at 150 characters.
- Leading street direction - Street field value.The field is optional, maximum length set at 150 characters.
- Street type suffix - e.g. ST
- Address number - e.g. 1411
- Postal code - e.g. 77868
- Postal Community name - e.g. NAVACOSTA
- Building - The field is optional, maximum length set at 150 characters.
- Floor - e.g. 1st
- Room - The field is optional, maximum length set at 150 characters

IMPORTANT: The Location information is included if SBC is operating in normal or survivable mode.

5.5.2.7 Media Server Profile

Name - Media Server profile name.

Time to live (sec) - The maximum time, in seconds, a transaction waits for response.

Maximum conference time (sec) - The maximum time, in seconds, a conference is allowed to be inactive.

The unlimited check box will disable this configuration.

Maximum announcement time (sec) - The maximum time, in seconds, an announcement session is allowed to be inactive. The **Unlimited** check box will disable this configuration.

MGCP over SIP - If selected, allows remote media server communication using MGCP encapsulation over SIP protocol.

5.5.3 SIP Load Balancer

The SIP Load Balancer (SIP-LB) distributes the SIP traffic among a set of SBCs based on establishing a TCP / TLS connection (Round-Robin mechanism).The SIP-Load Balancer is used as Cloud Telephony (OSV based) deployments. Once the Load Balancer is activated, the other SBC functionalities are disabled. Also the core realm settings are obsolete.

The SIP Load Balancer is checking the SBC availability in the cluster based on a background script sending ICMP pings to each of the configured SBC in the cluster. The pings will be send to all as "active" marked SBCs, whereas manually marked "in-active" (down) will not be pinged. If the ping is not responded the SBC will be marked as "down" in the Cluster configuration and the configuration file will be reloaded without influencing the existing connections.

IMPORTANT: For **Hosted OpenScape SBC** (hSBC) on **OS4K** Deployments, **SIP Load Balancer** is disabled

---

The **HAProxy** Open Source is used as the main application for SIP-LB, providing a high availability Load Balancer and proxy server for TCP and HTTP-based applications.

For an SBC Server Cluster entry, the entry port is the port configurable as SIP-TCP under **Network / Net Services** > **Settings** > I**nterface Configuration** > **Access realm configuration**. Requests coming in this port will be distributed to the IPs / FQDNs and ports configured in the Cluster settings.

NOTICE: The SBC port is used to check the SBC connectivity. SIP Load Balancer will send periodically iCMP messages to each pair address: port configured in the cluster.

The **SIP Load Balancer** provisioning window is displayed with the following configuration options:

General Settings

Cluster Connectivity check

- **Status Check interval** - Range: 5sec - 60sec.Default value:10sec.
- **Ignored missed responses for "down"** - Range: 1- 4. Default value:1
- **Needed responses for "up"**- Range: 1- 4. Default value:1
- **Client inactivity timeout (min)** - Set the value of the timeout for inactivity of the TCP connection at the client side (**HAProxy**).

  Range: 1- 60 min.

- **Server Client inactivity timeout (min)** - Set the value of the timeout for inactivity of the TCP connection at the server side (**HAProxy)**.

  Range: 1- 60 min.
- **Session Persistence timeout (min)** - Set the time that the data related to the connection between clients (Front-end) and the SBCs (Back-end) remains on the Load Balance table.

  Range: 0 - 33120 min. When set to zero, the connection entry on the table remains until the application is restarted.

  IMPORTANT: After the timeout, if no activity at TCP level was performed for the existing connections, **HAProxy** will tear down the connection.

SBC Server Cluster

NOTICE: You can add a total up to 100 servers.

NOTICE: (only for SBC V9R4): Additional port for TLS (TCP port + 1) will be added for each Cluster IP.

- **Name** - 24 alpha numeric characters
- **FQDN/IP** - 24 alpha numeric characters
- **Port** - 10 numeric characters
- **Enabled** - Default value: unchecked

5.5.4 Push Notification Service

The Push Notification Service feature supports sending VoIP Notifications to a Push Notification Server.

An IOS Application in background mode, using IOS 10 SDK, cannot maintain any longer connections to the outside world only to the Apple Push Notification Server. All notifications targeted for an IOS Application (OSMO) need to be sent to an Apple IOS Notification Server who than locates the Device and sends the notification to it. The application either switches to foreground or stays in background and is able to establish the HTTP or TCP connections in order to process the content of the notification (call, …).

The **Push Notification Service** provisioning window is displayed with the following configuration options:

Registration

The Registration module will only be utilized if the OS-SBC received the contact header parameter **+UC=SIP only** or **+UC=SIP/UC dual mode**

- **Register expire time (secs)** - Available options: 600-3600sec. Default value: 3600sec.
- **Register Hold time (days)** - Default value: 1. Available options: 1-7 days

Outbound calls

- **Call hold time (secs)** - When an INVITE is sent from OSV to OSMO client passing through SBC, this INVITE will be held and SBC will send a push notification to OSMO client in an IOS device (in order to wake it up). After receiving the push notification at IOS device, OSMO client sends an OPTIONS message to SBC which says that it is ready to receive VoIP calls, then the SBC releases the INVITE towards OSMO client.

  Default value:5sec. Available options:3-15sec
- **Send Session Progress (183) during hold time** - During the hold time between the push notification which is sent to Apple Servers and received by IOS device, an **183 Session Progress** can be backwards sent to OSV in order to warn OSV that the call is ongoing and therefore avoid a call **CANCEL timeout** at OSV. A push notification sent from SBC can take up to more than 20 seconds to arrive to the IOS destination device, so this value has maximum timeout of 30 seconds and it is recommended to be set to the maximum.Enabled by default.
- **Send Session Progress (183) after: (secs)** - This is a timeout to wait for the OSMO message OPTIONS to arrive before sending backwards the **183 Session Progress** to OSV.

  Default value:5 sec. Available options: 1-10sec.

  IMPORTANT: Set to a value less than the value set in the OSV.

Notification Server (iOS)

- **Enable Sandbox Push Server** - Disabled by default. When enabled, push notification will be sent to DEVELOPMENT APN servers.
- **Push Certificate Passphrase** - It is the .p12 certificate key file, or the .p8 token key file password.
- **Account Team Id** - When using a .p8 token key file, an Apple Account **Team ID** is required.
- **Mobile Application Bundle Id** - The Mobile Application bundle ID to be used on push notifications (if voIP Is not used, suffix will add it on voIP notifications). e.g. `com.unify.iOSMO`

Notification Server (Android)

- **Firebase Database URL** - Must be filled with the client Firebase Database URL in case of user certificate upload. Otherwise, there is no need to change, because it already has a default value.

  NOTICE: APN Push Notification API uses Push Server Port 443 by default.

Security

- **Disable certificate validation**- When this flag is set, the Push certificate validation is ignored.

Response Codes for Push timeout

- **Response Code/Message for Push timeout** - Select the error code that will be sent to the PBX in case of **Push Notification** failures.

  The available options are:

  – 408 - Request Timeout
  – 480 - Temporarily Unavailable
  – 500- Internal Server Error *(default)*
  – 503 - Service Unavailable
  – 504 - Gateway Timeout

  The default value is **500 Internal Server Error**.

5.6 Security

In this administrative area the user can configure the security parameters.

5.6.1 General

Certificates

- **Certificate Management** - This button opens a new **Certificate Management** window to choose and manage the TLS Certificates. Refer to Certificate Management

Secure Web Management

- If **Security web management** flag is enabled the Apache web server will only accept TLS connections. If the flag is disabled, Apache will also accept TLSv1.2.

Passwords

- To change a password, select a **User name**, enter the **Current password**, enter the **New password**, **Confirm new password** and press the **Change** button.
- To reset a password, select a **User name** then press the **Reset** button. A confirmation window will commit the changes.

NOTICE:

Changing the password is only allowed for the **root** and **administrator** users.

The **Reset password** option is available only for default accounts (e.g., administrator, guest, assistant, service, redundancy).

User Accounts

This window presents the **User Accounts**. User Accounts can be created by clicking the **Add** button. Existing accounts can be edited or deleted using the **Edit** and **Delete** buttons. Selecting **Add** or **Edit** will open the User Account configuration window.

NOTICE: For versions prior to V11R2, **User Accounts** are presented as **Administrator Accounts**.

Starting from V11R2, root access via GUI is blocked by default. To enable it, you must create the file "rootAccess" using the following command: `./sbin/usercontrol --enable`.

To perform all user-related functions, typically available to the root user, run the following script: `/sbin/usercontrol --exec`.

This script allows you to reset passwords, change passwords, change expiration time, enable/disable SSH login and enable or disable root privileges.

Active sessions can be managed by pressing the **Active Sessions Management** button. The **Active Sessions Management** console provides an overview of all currently logged-in sessions, allowing you to review associated devices and timestamps, and to proactively terminate any session.

SIP/SDP Information Filtering

- **Warning Info on Error Responses removal** - will remove Warings 399 and 488 Header from SIP messages.
- **Internal names and additional headers removal** - will remove the UA names, server names and X-Siemens headers from SIP messages

Accept only Video Calls from Peer Domains

When this flag is enabled, only INVITE messages containing a video m-line in the SDP is accepted from calls coming from the Access side (WAN) if **Support Peer Domains** or **Support Foreign Peer Domains** is the endpoint to be used. When no video m-line is received in the INVITE message, the call is rejected. You can change this behavior by disabling this flag. This flag is enabled by default

Open SSH

- **Enable advanced Ciphers**- Allows administrators to manually configure custom cipher suites for SSH connections. When enabled, you can define your preferred cipher suites to meet your security requirements.

INFO: Enabling custom cipher suites can pose significant security risks if weak or deprecated algorithms are selected.

– When enabled, all accepted SSH ciphers are displayed.
– At least one valid cipher suite must be specified.
– Use colons (:) to specify multiple cipher suites. For example, `CIPHER1:CIPHER2`.

5.6.1.1 Certificate Management

System Certificate

- **System TLS certificate profile** - Select the certificate profile to be used for TLS connections.

  Default certificate profile: OSV Solution.

- **HTTPS certificate profile** - Select the certificate profile to be used for HTTPS connections.

  Default certificate profile: HTTPS System Default.
- **Media DTLS certificate profile** - Select the certificate profile to be used for Media DTLS connections. Not configured.
- **IOS Push certificate profile** - Select the cetificate profile to be used for IOS Push service.

  Default certificate profile: IOS Push Default.
- **Android Push certificate profile** - Select the certificate profile to be used for Android Push service.

  Default certificate profile: Android Push Default.
- **Service API certificate profile**- Select the certificate profile to be used for Service API.

  Default certificate profile: Service API Default.

Certificate Profiles

- This is the list of certificate profiles. A new certificate profile can be created pressing the **Add** button and the existing ones can be edited or deleted using **Edit** and **Delete** buttons. Adding or editing a certificate profile launches the **Certificate Profile** window. Refer to Certificate Management > Certificate Profile.

  NOTICE: The following systems: IBM 3250, 3550, Fujitsu RX200, and Fujitsu R300 have a limit of 10 for the maximum allowed Certificate Profiles.

  NOTICE: Logs will be written for creating, modifying and deleting certificate profiles. These logs are available in the System Log on the local Gui and written to /var/log/warn file.

Certificate Creation

A new TLS certificate can be created after filling out the two fields and then clicking the "Create" button.

- **Name** - Indicates the name of the certificate which will be created.
- **CA file** - Allows the selection of a CA file used to sign the certificate that is being created. If CA file option 'Self Signed' is chosen, all 3 files are created: CA Certificate file, X.509 Certificate file and Key file.

  NOTICE: Certificate files can only be created based on a CA file with certificate and key.

Log entries will be written when creating certificates. These logs are available in the System Log, on the local GUI, and written to the `/var/log/warn` file.

NOTICE:

The generated certificates are **SHA-1** only.

Certificates Upload

CA Certificates

A certificate authority or certification authority (CA) issues digital certificates which contain a public key and the identity of the owner. This is used in security to ensure that one entity is trusted.

In this section it is possible to configure CA Certificates.

- **Upload CA certificate file** - A new certificate can be added by browsing to the certificate file and then clicking the "Upload" button.
- **CA certificates** - This field lists all CA certificates loaded in the system. To delete a certificate first click on it to select it and then click the "Delete" button.

Logs will be written for uploading and deleting certificates. These logs are available in the System Log on the local GUI and written to the /var/log/warn file.

X.509 Certificates

X.509 is an ITU-T standard for a public key infrastructure (PKI) for single sign-on and Privilege Management Infrastructure (PMI). X.509 specifies standard formats for public key certificates, certificate revocation lists, attribute certificates, and a certification path validation algorithm.

In this section it is possible to configure the X.509 Certificates.

- **Upload X.509 certificate file** - A new certificate can be added by browsing to the certificate file and then clicking the "Upload" button.
- **X.509 Certificates** - This field lists all X.509 certificates loaded in the system. To delete a certificate first click on it to select it and then click the "Delete" button.

Logs will be written for uploading and deleting certificates. These logs are available in the System Log on the local GUI and written to the /var/log/warn file.

Key Files

In this section it is possible to configure the Key files.

- **Upload key file** - A new key can be added by browsing to the key file and then clicking the "Upload" button.
- **Key files** - This field lists all key files loaded in the system. To delete a key first click on it to select it and then click the "Delete" button.

Logs will be written for uploading and deleting certificates. These logs are available in the System Log on the local GUI and written to the /var/log/warn file.

Certificate Download

- **Certificate file** - A certificate file (CA or X.509) can be downloaded by selecting an entry in the Certificate file list and then clicking the **Download** button.
- **Attach certificate to configuration** - When this flag is enabled the remote certificates are attached to xml. If disabled, the attached certificates shall be removed from xml.

  When importing a xml, delta or not, you should check if the flag is set and the certificates are present in xml.If so, then the import procedures should evaluate using the md5sum field if the certificates locally stored are the

same as in the xml.If they are different, then they have to be stored locally as the import certificate procedures already available.

- **Key file** - A key file can be downloaded by selecting an entry in the Key file list and then clicking the **Download** button.

Certificate Expiration Checking

- **Certificate expiration warning period (days)** - The number of days before a certificate expires, at which time an alarm is generated to warn the administrator about the impending expiration of the certificate. Valid values: 0 - 300 days, default: 60.
- **Certificate expiration warning interval (days)** - The number of days after which to repeat the Certificate expiration warning alarm. Valid values: 0 - 60 days, default: 7.
- **Certificate expiration time of day (hh:mm)** - The time of day at which to run the certificate expiration check. Valid values: 00:00 - 23:59, default: 00:00.

Certificate Revocation List

A new Certificate Revocation List (CRL) entry can be created by clicking the "Add" button, and an existing CRL entry can be edited or deleted by first clicking it to select it and then clicking the "Edit" or "Delete" button as appropriate. The "Show CRL" button can be clicked to show a new screen with the CRL download status.

The table presents a summary of the certificate revocation list. The "Add" and "Edit" buttons bring up a new screen that contains the same fields as are shown in the summary table. The "Manual update" button is not available in the summary table.

- **Name** - Internal name for reference to the root CA.
- **CRL URL** - URL from which the CRL file can be downloaded.
- **Manual update** - Clicking this button causes the CRL to be downloaded from the configured URL and uploads the CRL to the system. A manual update can be performed only after the CRL configuration is applied to the system.
- **CRL download interval** - Maximum interval between 2 CRL uploads. If this interval is set to 0, the Next Update field is used instead for the automatic CRL downloads. Valid values: 0 - 168 hours, default: 24.
- **CRL short download interval** - This is the interval at which a CRL check will occur in case the download of a CRL failed because the CRL could not be downloaded. Valid values: 15 - 1440 minutes, default: 60.
- **CRL time of day** - Time of day at which to start the CRL check. This variable is only checked if the CRL download interval is 24 or a multiple of 24. Valid values: 00:00 - 23:59, default: 00:00.

5.6.1.2 Certificate Management > Certificate Profile

Certificate Profile Configuration

- **Certificate profile name** - Name of certificate profile.

- **Certificate service** - Parameter used to indicate if the certificate profile service is SIP-TLS, HTTPS, VPN, Media DTLS and IOS Push

  NOTICE: For the default profile, only SIP-TLS is allowed.In addition, this field cannot be changed once the profile is created.

- **Client certificate file** - Local client certificate file is an optional field. This is used when establishing a TLS connection as TLS client (only for Mutual Authentication). If the Local client certificate is not configured, the Local server certificate shall be used.
- **Server certificate file** - Certificate file to be used when establishing a TLS connection as TLS server.
- **Local CA file** - CA file with the rootCA certificate which signed the local certificates.
- **Remote CA file** - CA file for path validation of the certificate received from the remote endpoint. This is required only when a remote endpoint uses a different certificate issuer.
- **Local key file** - File containing the private key.
- **EC param** - parameter used in order to allow the configuration of the Elliptical Curve which is used with ECDH and ECDHE cipher suites. For now, this parameter will be kept grayed out with the hardcoded value secp256r1.
- **Attach to Config file** - If set, the certificate file defined in **Remote CA file** will be saved/restored to/from the xml configuration file. Available only if **Remote CA file** is filled up.

  When this flag is enabled the remote certificates are attached to xml. If the flag is disabled, the attached certificates shall be removed from xml. When importing a xml, delta or not, the persistent manager should check if the flag is set and the certificates are present in xml. If so, then the import procedures should evaluate using the md5sum field if the certificates locally stored are the same as in the xml. If not, they are different then they have to be stored locally as the import certificate procedures already available.

Pressing the **Show** button near each certificate/CA file opens a screen with a view of the certificate parameters.

Validation

- **Certificate Verification** - Controls the level of validation of the CA chain, CA signature, and Validity Period.
  - **None** - No authentication of the remote entity performed.
  - **Trusted** - This means (1) The chain of trust for the digital signature provided by the remote entity ends up in one of the (root) CA-certificates which are preconfigured for that interface on the product, (2) No certificates in the chain are expired, and (3) No certificate in the chain is revoked.
  - **Full** - Includes the Trusted checks plus: (1) Correct end entity identity (according to settings in SubjectAlternativeName (SAN) and/or the common name (CN) in the Subject). The SAN is checked first and only check the CN if the identity was not verified through the SAN.# (2) Correct use of all critical extensions (e.g. Basic constraints, Key Usage, Extended Key Usage). If an extension is marked critical and is not recognized, the certificate must be rejected. #(3) Correct use of known

extensions not marked as critical (e.g. Basic constraints, Key Usage, Extended Key Usage).

- **Revocation status** - Enables the verification of revoked certificates according to CRL of the CA.
- **Indentity check**- Enables the validation of certificate Subject CN or Subject Alternative Name according to the configured gateway/trunk FQDN or IP Address.

Renegotiation

- **Enforce TLS session renegotiation** - Indicates if renegotiation of an established TLS session is enabled for the endpoint.
- **TLS session renegotiation interval (minutes)** - Indicates how long a negotiated key is valid in a TLS connection. Valid values: 15 - 1440 minutes.

TLS version

- **Minimum TLS version** - Select the supported TLS version. The options are: **TLS V1.0**, **TLS V1.1**, **TLS V1.2** and **TLS V1.3**.

  IMPORTANT:

  The TLS V1.3 option is only available in V11R1.00.00 or higher versions.

  NOTICE: In V10R2, after full install, the default value for Minimum TLS version was changed to TLS V1.2 in Certificate Profile.

  It is still possible to select TLS V1.0 from menu.

- **Enable force TLS** - When enabled, this option enforces the use of a specific TLS version for the connection. After enabling the flag, you can select the desired TLS version in the adjacent field.

  NOTICE:

  This option is currently available only for SIP-TLS certificates.

DTLS version

IMPORTANT: If the option Media DTLS certificate profile was chosen under Certificate service, the supported DTLS version is configurable.

- **Minimum DTLS version** - Select the supported DTLS version. The options are: **DTLS V1.0** and **DTLS V1.2**

  Default value**: DTLS V1.0**:

  IMPORTANT: An invalid DTLS certificate can cause rtpproxy failure. Additional certificate validation protection is planned to next release. If not setting Media DTLS configuration, rtpproxy uses the default internal certificate.

Chiper Suites

- **Perfect Forward Secrecy** - The priority of the ephemeral Diffie-Hellman ciphers suites. The options are: Preferred PFS (default), Without PFS.
- **Encryption** - The encryption cipher. Currently AES-128 is the most recommended option.The options are: Preferred AES-128 (default), Required AES-256.
- **Mode of Operation** - The encryption cipher mode of operation: CBC or GCM (TLS V1.2 only). The options are: Preferred GCM (default), CBC Only and GCM Only.
- **Enable advanced Ciphers**- Allows administrators to manually configure custom cipher suites for HTTPS and SIP-TLS connections. When enabled, you can define your preferred cipher suites based on your security requirements.

NOTICE: For SIP-TLS profiles, only ciphers **below TLS 1.3** can be configured. **TLS 1.3** ciphers are always accepted by default.

INFO: Enabling custom cipher suites can pose significant security risks if weak or deprecated algorithms are selected.

– The system uses OpenSSL-standard cipher suite naming conventions.
– You must specify at least one valid cipher suite.
– If no TLS 1.3 cipher suite is provided, TLS 1.3 support will be automatically disabled.
– Recommended default cipher suites will be displayed when activated.
– Use colons (:) to specify multiple cipher suites. For example, `CIPHER1:CIPHER2`.

5.6.1.3 Certificate Management > Generate CSR File

Generate CSR File

This feature permits creation of certificates for use in the system's profiles, with the option to choose and customize their parameters for use with the HTTPS system, push notifications, and more. These fields are defined by the **RFC 5280 - Internet X.509** *Public Key Infrastructure Certificate* and *Certificate Revocation List (CRL) Profile.*

The created `.csr` file will be automatically downloaded upon creation, and its corresponding key will be stored in the system. If the user wishes to download them again, the `.csr` file will be stored in the CA certificates field, while the key file will be stored in the **Key files** section.

NOTICE:

Only the **Name** and **Type** fields are required. However, to ensure optimal certificate performance, the necessary fields for each application must be provided as specified in the standard mentioned above.

For lists of elements, separate them with a comma.

- **Name for the csr file**- Indicates the name of the certificate which will be created. It must be at least 8 characters long.
- **Type**- Specifies the type of key generated for signing the certificate. The available types are RSA and ECC.
- **Country Code (C)**- A field containing one or more country codes. **Example**: US.
- **State or province name (ST)**- A field containing one or more locality names. **Example**: Florida.
- **Locality name (L)**- A field containing one or more locality names. **Example**: Boca Raton.
- **Organization name (O)** - A field containing one or more organization names. **Example**: Mitel Networks Corporation.
- **Common name (CN)** - The server name protected by the certificate. It does not include any protocol or path, as it is not a URL. **Example**: `mitel.com`, `*.another.example.com`.
- **Subject alt name** - The **Subject Alternative Name (SAN)** should follow the same format as the **Common Name (CN)**, with no strict limitation on the number of hostnames that can be included.

  However, it is highly recommended to avoid using arbitrary wildcard names. Instead, specify exact names for each domain.

  Additionally, names are not required to belong to the same domain. At this time, only **Fully Qualified Domain Name (FQDN)** SANs are supported, using the following format:
  Example:

  `mitel.net,*example1.com,another.net,example2.com`.

  Values must be separated by a comma, with no spaces before or after each entry.

NOTICE:

Due to the wide range of use cases for certificates, this certificate creator allows flexibility in the number and content of fields. If you encounter errors during the generation process, please review the content of each field.

The created certificate will be downloaded automatically and available in its respective sections (X509, CA, Key). It can then be signed by a Certificate Authority (CA) and imported into the system on this page for use in a certificate profile.

5.6.1.4 Certificate Management > Certificates Upload

CA Certificates

A certificate authority or certification authority (CA) issues digital certificates which contain a public key and the identity of the owner. This is used in security to insure that one entity is trusted.

In this section is possible to configure the CA Certificates.

- **Upload CA certificate file** - A new certificate can be added by browsing for the certificate file under the **Choose File** button and clicking on the **Upload** button.
- **CA Certificates** - This box lists all certificates loaded in the system. To delete a certificate select the certificate and click the **Delete** button.

NOTICE: Logs will be written for uploading and deleting certificates. These logs are available in the System Log on the local Gui and written to /var/log/warn file.

X.509 Certificates

X.509 is an ITU-T standard for a public key infrastructure (PKI) for single sign-on and Privilege Management Infrastructure (PMI). X.509 specifies standard formats for public key certificates, certificate revocation lists, attribute certificates, and a certification path validation algorithm.

In this section is possible to configure the X.509 Certificates.

- **Upload X.509 certificate file** - A new certificate can be added by browsing for the certificate file under the **Choose File** button and clicking on the **Upload** button.
- **X.509 Certificates** - This box list all X.509 certificates loaded in the system. To delete a certificate select the certificate and click on the **Delete** button.

NOTICE: Logs will be written for uploading and deleting certificates. These logs are available in the System Log on the local Gui and written to /var/log/warn file.

Key Files

In this section is possible to configure the Key files.

- **Upload key file** - A new key can be added by browsing for the key file under the **Choose File** button and clicking on the **Upload** button.
- **Key files** - This box lists all key files loaded in the system. To delete a key select the certificate and click the **Delete** button.

NOTICE: Logs will be written for uploading and deleting certificates. These logs are available in the System Log on the local Gui and written to /var/log/warn file.

5.6.1.5 Certificate Management > Certificate Revocation

Certificate Revocation Configuration

This window presents a view of the certificate parameters.

- **Name** - Internal name for reference of root CA.
- **CRL URL** - URL from which the CRL file can be downloaded.
- **Manual update** - Downloads the CRL from configured URL and uploads the CRL to the system. A manual update can be performed only after the CRL configuration is applied to the system.
- **CRL download interval (hours)** - Maximum interval between 2 CRL uploads. If this interval is set to 0, the Next Update field is used instead for the automatic CRL downloads. Valid values: 0 - 168 hours, default: 24.
- **CRL short download interval (minutes)** - This is the interval at which a CRL check will occur in case the download of a CRL failed because the CRL could not be downloaded. Valid values: 15 - 1440 minutes, default: 60.
- **CRL time of day (hh:mm)** - Time of day at which to start the CRL check. This variable is only checked if the CRL download interval is 24 or a multiple of 24. Valid values: 00:00 - 23:59, default: 00:00.

5.6.1.6 User Accounts

This section outlines User Accounts configuration for the firewall /routing settings for the SBC.

NOTICE: For versions prior to V11R2, **User Accounts** are presented as **Administrator Accounts**.

The only settings that can be modified for default users (e.g., administrator, guest, assistant, service, redundancy) are **Password** and **Configured expires**.

All other settings are restricted.

Administrator Profile

- **Account enabled** - This flag is used to grant login rights (**SSH** and **Management Porta**l) to users.Enabled by default.

  IMPORTANT: The flag is disabled & grayed out for assistant & redundancy users.

- **User Name** - User name of the User Account.

- **Password** - The password for the User Account user name.

  Password requirements

  – The password must be 12...36 characters, with at least one upper case letter, one lower case, one digit and one special character.
  – User cannot use passwords similar to its username, as well as common passwords like "password", "qwerty", "abcdefgh", "user".
  – User cannot reuse any of their **last five passwords** when changing their password.

  During password creation or change, a visual password strength meter is displayed, providing real-time feedback on password complexity.

  A rating of "Strong" indicates the password meets the minimum security requirements.
- **Confirm Password** - Confirm & verify the User Account user name password.
- **Privilege** - Administrative privileges. Possible values: `Administrator, Network Administrator, Security Administrator, Network and Security Administrator, Read Only`.
- **Configured expires (days)** - This option sets the password expiration policy by defining the timeslot (in days) after which the password will expire. Possible values: 7 - 99999.

  NOTICE:

  Configured expires (days) configuration defines the policy for password expiration. For example, if set to 30 days, the password will expire after a 30-day timeslot from the last password change.

  This option does not reset or alter the days that have already passed since the last password change; it only sets the expiration timeslot moving forward.

  It is intended to define the password expiration policy and should not be used to extend a user's expiration time. If the password has already expired, the administrator can only modify this option after the user has changed their password.

  – **Lock account for inactivity (days)** - Specifies the number of consecutive days without login activity after which a user account is automatically locked.

    When an account is locked, it appears as disabled in the Admin panel and the **Time to lock for inactivity** column will display **Expired**.

    To reactivate a locked account, an administrator must activate the account and provide the user with new credentials.
  – **Remove account (days)** - Specifies how many days after an inactivity lockout the account will be permanently deleted.
- **SSH login** - Login to the Linux open source application that allows data to be exchanged using a secure channel between two networked devices.Disabled by default.

- **Root privileges** - This flag can only be enabled by the root user. The default accounts (administrator, guest, assistant, service, redundancy) do not have this privilege.

  IMPORTANT: This flag is only available in V11R1.00.00 or higher versions.

  NOTICE:

  Starting from V11R2, root access via GUI is blocked by default.

  To enable it, you must create the file "rootAccess" using the following command as the root user over ssh: `./sbin/usercontrol --enable`.

  To disable it, use the following command: `./sbin/usercontrol --disable`.

  To perform user-related functions run the following script: `/sbin/usercontrol --exec`.

  This script allows you to perform any of the following actions:

  – Reset password
  – Change password
  – Change expiration time (mentioned as 'Change expires')
  – Change privilege
  – Enable/disable SSH login
  – Enable/disable privilege escalations

    NOTICE: To enable/disable privilege escalations, you must first enable SSH login.

  To perform an action, select the user, choose the desired option, and save the changes.

- **Change password in first login** - When adding a new user, the **Change password in first login** is enabled by default, and the **Expires** parameter is set to **99999**, meaning the password will not expire.

  NOTICE:

  Only user root has the privilege to change the password of other users without knowing the current password.

  Users with privileges “Administrator”, “Security Administrator” and “Network and Security Administrator” are able to define the password of other users only when adding the user.

  After that, only the user itself can change the password providing the current and new password.

5.6.1.7 Certificate Management > CRL Viewer

In this screen it's possible to check the CRL download status.

- **CRL download URL** - URL from which the CRL file was downloaded.
- **Status of the CRL** - Status of the CRL list (Removed, Installed, Expired, Downloading).
- **This update** - Date and time of the CRL update (loaded from CRL).
- **Next update** - Date and time of next CRL update (loaded from CRL).
- **Last CRL update** - Date and time of the last update.

5.6.1.8 Security > General > PKI Configuration

SSH PKI Configuration Table

The table shows you which external users have been granted the ability to log into the Branch via one of the internal usernames, without the need for entering a password. To create a new entry in the table, click the "Add" button. A new screen opens. To delete an entry in the table, first click on the entry to select it and then click the "Delete" button. To update an entry in the table, first click on the entry to select it and then click the "Update" button.

For both Add and Update, the Add/Update Public Key screen appears that has the following fields.

- **Associated internal username** - when adding a new entry, the drop-down field allows the user to select between 'administrator' and 'service'. This field cannot be changed when an entry is being updated.
- **Choose file** - Clicking this button causes the standard file open dialog to appear. The user can navigate to the applicable public key file on their local computer. The file must have the '.ppk' extension and the content must adhere to certificate content standards.
- **Import** - Once the key file has been located, clicking the "Import" button will cause the key to be uploaded and stored on the Branch.

5.6.2 Firewall Overview

Firewall Settings

This window presents the Firewall Settings. Firewall Settings can be created pressing the **Add** button and the existing ones can be edited or deleted using **Edit** and **Delete** buttons. Adding or editing launches the **Firewall Configuration** window.

Firewall Configuration

- **Network ID**

  This configuration is allowed when WAN interface is enabled.
- **Enable IP masquerading**

  This check box allows the enable of IP masquerading. The IP masquerading will mask the LAN addresses in WAN, this will hide the entire internal

address space which will appear as a single IP address in another, often public address space.

This configuration is allowed when WAN interface is enabled.

> **IMPORTANT:** Masquerading works only if **Port Forwarding** is enabled.

- **Enable port forwarding**

  This check box allows the enable of port forwarding. The configuration is done using the **Configure** button and shall launch the Port Forward window.

  This configuration is allowed when WAN interface is enabled.

  > **IMPORTANT:** **Port Forwarding** will send packets from WAN side to LAN side.It is necessary to configure **IP Masquerading** so SBC will properly mask the incoming IP to the destination.This will allow the destination to return the packet to the source, which is on SBC's WAN side.

- **Incoming network connections**

  These settings are used to allow or block access to some services (**DNS**, **SSH**, **SNMP**, **ICMP**, **FTP**, **Telnet**, **HTTPS** and **NTP**). These settings affect new incoming connections (Devices under SBC trying to access WAN services). The **Allow all network connections** flag will disable the firewall for these protocols.
- **Incoming VOIP connections**

  These settings are used to disable VoIP protocols from accessing the WAN interface.
- **White List**

  Allow Incoming WAN network connections for a specific IP/Port. If the Port field is zero, all ports will be allowed.
- **Black List**

  Block Incoming WAN network connections for a specific IP/Port. If the Port field is zero, all ports will be blocked.

  > **NOTICE:** Message Rate Control (if enabled) will be restarted if the firewall rules are changed.

- **Administrative access control**

  List of LAN IP addresses of hosts to administrate the Central SBC. Format is ip address or ip address/maskbits. Configuring this will block the FTP, SSH and HTTPS connections for IP address not in this list. The administration shall be possible from any host when no IP address is provided.When provisioned, only the protocols with the checked checkboxes would be allowed for administration from that ip or subnet.
- **External Firewall**

  When enabled, the IP address of firewall shall be used in the SIP headers and SDP towards access side instead of the SBC access IP.
- **Add WAN IP in ICE Candidates**

  This flag allows the inclusion of the WAN IP address as a ICE candidate in SDP. This flag has no effect if **Circuit Only** flag is enabled.

- **Enable Seperate Firewall IP Signaling / Media**

  When this flag is enabled, the separate settings will be used: **Firewall external IP for Signalin**g in the signaling portion of the message and **Firewall external IP for Media** in the Media (SDP). This flag cannot be used if **Circuit Only** flag is enabled.
- **Profilel**

  For future use.
- **Firewall external IP**

  The public IP address of external near end firewall.
- **Firewall external IP Signaling**

  Firewall to be used for signaling (SIP content).
- **Firewall external IP Media**

  Firewall to be used for media (SDP content).
- **Firewall internal IP**

  The internal IP address of external near end firewall towards SBC (for future use).
- **Network ID**

  This configuration is allowed when WAN interface is enabled.

NOTICE: The Network ID named Main is related to Main-Access-IPV4 and the ip address is shown in Firewall settings.

5.6.2.1 Port Forward

Port forward provisioning

Under this window it is possible to configure the port forwarding. A new rule is added using the **Add** button. In this case a new row is created in the table and is possible to configure the Incoming Port number, the outgoing IP to be used, the outgoing port number and the protocol, including **SNAT**, a flag indicating that SBC will act as network gateway for the specified rule.

To delete a rule select the route and then use the **Delete** button.

Once the rules are entered or deleted the **OK** button will save the configuration and the window will close. To apply this configuration the user must click on **Apply Changes** button.

5.6.3 Message Rate Control

Message Rate Control Settings

- **Enable Message Rate Control**

  This check box enables Message Rate Control.

- **Message rate threshold**

  This box defines the number of kilobytes per second which will block an IP address.

  The network administrator should set this parameter according to desired bandwidth.

  NOTICE: Setting the Message Rate Threshold to the minimum value could cause RTP packages to be dropped.

- **Block period (sec)**

  This box defines the blocking time of the IP address in seconds.

  NOTICE: If Block period is changed (or even if Message Rate Control is disabled) by the user, previously blocked IPs are not affected by new configuration, they remain blocked until the block period is over.

- **White list**

  This window lists all IPs which will not be blocked by Message Rate Control.

  NOTICE: FQDNs (Fully Qualified Domain Names) are supported in the whitelist when a valid DNS server is properly configured.

5.6.4 RADIUS

RADIUS Settings

- **Enable RADIUS**

  This check box enables the RADIUS Server feature.
- **Server 1** and **Server 2**
  - **Address** - Two RADIUS Server IP addresses or FQDNs can be configured in the fields.

    NOTICE: Server 2 is not required. The use of an IP address is preferred over a FQDN.

  - **Port** - Port numbers in the range 0-65535 or "radius" (1812/1813) can be used to indicate the port number for RADIUS authentication. "Radius" is recommended.

    NOTICE: The port number for accounting is hard-coded to be the next value up from the authentication port number. For example, if the authentication port number is 2115, then the accounting port number will be 2116. If the user does not provide the port number for authentication, the RADIUS feature looks up the 'radius' and 'radius-acct' entries in /etc/services and uses those values

  - **Secret** - string must be supplied by the RADIUS administrator. It will be used to authenticate the password requests and to encrypt the messages exchanged.

    A string with 16 characters is mandatory. It can consist of upper or lower case letters, digits, or special characters. Special characters can be any of the following set: ~!@#$%^&*()_+|\=-'{}[]:"';<>?/.,
  - **Timeout (sec)** - length of time in seconds the SBC shall wait for a response from a Radius Server (1 - 10 seconds, 3s recommended).

    NOTICE: A timeout of 1 or 2 seconds must be avoided in networks with high delays. In case of a timeout or other network problems then, local authentication will be used.

- **Enable RADIUS Authentication** and **Enable RADIUS Accounting**

  These check boxes together with the check boxes **WEB**, **CLI** and **SSH** are used to select the services that RADIUS will use for user Authentication and Accounting.

  - **CLI** - controls the users connected directly to a terminal.
  - **SSH** - controls the users using a Secure Shell or a Secure FTP connection.
  - **WEB** - controls the users using an Internet Browser (Local GUI).

    NOTICE: When RADIUS is enabled Authentication service or Accounting service (or both) must be selected and for each selected service at least one application must be enabled.

5.6.5 Security > Tunnel Connections

IPSec

To create a new IPSec tunnel, click the **Add** button. To delete an IPSec tunnel, first click it in the table to select it and then click the **Delete** button.

This configuration is allowed in Branch SBC, SBC-Proxy and Centralized SBC modes. Redundancy is not supported.

- **Connection name** - This box defines the IPsec connection name. A unique name should be used for each connection.
- **Partner** - This box defines the public IP address of the partner VPN device. It cannot be a valid IP in the LAN subnet and it should be different from any Admin IP address.
- **Partner network** - This box defines the subnet protected by the partner VPN device.
- **Partner network mask** - This box defines the network mask of the subnet protected by the partner VPN device.
- **Side** - This box defines if the local host will be the left or right VPN device.
- **Local** - This box defines the public IP address used for the VPN.
- **Local network** - This box defines the subnet protected by the local VPN device.
- **Local network mask** - This box defines the network mask of the subnet protected by the local VPN device.

- **Compression** - This check box enables or disables the compression.
- **PFS** - This check box enables Perfect Forward Secrecy in order to avoid derived IPsec Keys.
- **Auth type** - This box defines the type of authentication.
- **Certificate profile** - This box defines the certificate profile for the connection. It must be configured only when X.509 certificates are used.
- **Secret key** - This box defines the secret key for the connection when the authentication type is defined as secret.

IPsec configuration applies only when the WAN interface is enabled.

5.6.6 Denial of Service Mitigation

Denial of Service Mitigation provides the customer protection from potential DoS attackers attempting to gain access to steal services.

SIP remote subscribers providing invalid user digest authentication credentials for successive attempts or have unknown OSV SIP server identities may be quarantined for a provisioned time interval.

For legitimate users which are unfortunately classified as a DoS attacker, the occurrences should be rare. Regardless, each detection shall be logged with sufficient user identify information to allow support personnel to remedy the situation.

Dynamic Blacklist

- **Block unauthorized users**

  If the checkbox is enabled, upon receiving a “401 unauthorized” response from the OSV, the response is forwarded to the SIP UA. The OS-SBC must supervise subsequent SIP REGISTER messages from the same SIP UA’s Source IP. If three (fixed) successive failure attempts occur, it is flagged as “User Authentication Violation” which leads to quarantining the violating Source IP for the **Unauthorized user quarantine interval**. A “403 Forbidden” response is returned to the offending endpoint instead of forwarding the “401 unauthorized” response.
- **Block unknown users**

  If the checkbox is enabled, upon receiving a “404 Not Found” response from the OSV to a SIP REGISTER message, a “403 Forbidden” response with a Warning is returned to the offending endpoint instead of forwarding the “404 Not Found” response.

  The OS-SBC shall flag the occurrence as an “Unauthorized User Violation” which leads to quarantining the violating Source IP for the **Unknown user quarantine interval**.
- **Process initial registration**

  If the checkbox is enabled, the initial SIP REGISTER message received from a SIP UA without a valid OS-SBC contact address binding is allowed to proceed as normal towards the SIP server. Otherwise, if not checked, a 503 Server unavailable is returned.
- **Unauthorized user quarantine interval**

  Quarantine interval for unauthorized users.

  Valid range: 60 to 36,000 seconds (default: 300 sec.)

- **Unknown user quarantine interval**

  Quarantine interval for unknown users.

  Valid range: 60 to 90,000 seconds (default: 300 sec.)
- **Enable gateway message rate limit**

  By default the checkbox is unchecked. When checked (feature enabled) the system applies message rate limiting and quarantining according to the configuration of the OS-SBC Access SIP listening IP:Port address

Trust Level Quarantine Intervals

An array of quarantine interval settings is administered under this section

- **Minimal** - default is 60 seconds; integer of range 60-3600.
- **Medium** - default is 10 seconds; integer of range 10-3600.

NOTICE: The default system-wide quarantine interval is variable (0-2 seconds) and is not shown since it is not configurable.

User Agent Allowed List

- **User Agent**

  If any User Agent(s) is/are added to the list, requests will only be honored from that/those User Agents. SIP requests from any other User Agents will not be honored.

Same IP SIP TCP Connections

- Specifies the number of allowed TCP connections from the same source IP address. Default value is **1024**.

5.7 Diagnostics and Logs

This section provides access to the Log Settngs, Debugging, Tracing and Statistics management areas.

5.7.1 Settings

In the **Settings** tab the user can configure the log settings.

Log Settings

- **Log size (kbytes)**

  This box defines the maximum size of each individual log file.
- **Syslog server**

  This box defines the IP address of an external server to be used to receive syslog messages. The external server must be any RFC 3164 (The BSD Syslog Protocol) compliant syslog facility server.

- **Log Levels**

  Each application can set the log level individually. The levels are defined as following:

  – **Emergency** is a panic condition report.
  – **Alert** reports a condition that should be corrected immediately, such as failure in configuration.
  – **Critical** is a report of device failures.
  – **Error** is a level used for applications to report internal errors.
  – **Warning** is a level to be used to report application instability.
  – **Notice** will report conditions that are not errors, but should require some attention.
  – **Info** is used for informational messages.
  – **Debug** is the level used for debugging applications.

  IMPORTANT: Warning: Setting the log level to Debug, Info, Notice or Warning may affect the system performance and will generate several log files. Besides, some features may not work properly, such as Media Server conference and announcements.

- **Signature on Log Files** - This flag is used to provide an MD5 signature to the compressed log files that are exported or internally stored. That way, you can check if the files were changed after they are created by the system.

  The MD5 is based on a signature key. This key is used to check if the signature plus the content of the file is trusted.In order to check the signature, proceed with the following:

  – Add a start line with the text of the **Signature Key** box.
  – Remove the last line with the MD5 result.
  – Calculate the MD5 of the result file: it must be equal to the last line removed.

Fallback

- **Fallback to default log level**

  Flag used to enable the Fallback to default log level feature.
- **Fallback time (hh:mm)**

  Time of the day when the SBC resets trace configuration back to default.

Call Log Settings

This setting upgrades the log level to DEBUG for applications SIP Server, SSM and RTP Proxy, based on the criteria selected:

- Log call started from number.
- Log call to the destination number.
- Log call initiated from remote address.
- Log call received on host address.
- Log for SIP methods.

All others settings will remain as configured.

5.7.2 Debugging

Log Viewer

- **Log data**
  - **Alarm History** – Alarm history shows details about alarms triggered in the system. These details include information of date, time and threshold when the alarm was activated or cleared.
  - **Alarm Manager** – Log of the Alarm manager application. Useful when an alarm is not being triggered, a false alarm is being activated or not cleared accordingly.
  - **B2B Controller**- Log of the B2B Controller.
  - **Boot** – Log of the last system boot. It is useful to debug problems of processes or driver modules not being correctly installed and, to identify hardware failure indications. Additionally, it provides system capabilities are correctly detected and configured.
  - **Continuous Tracing** – Continuous trace is the application that collects the logs from the applications does the log rotation, compression and aging.
  - **Current processes** – A list of the current processes running on the SBC.
  - **Denial of service**- The log will show hosts that sent DoS messages and are blocked by the system.
  - **Firewall & Msg Rate Control**

    This log contains the details of packets that are blocked by the Firewall and Msg Rate control.
  - **Install/Update/Upgrade** – Logs provided by the software installation tools that are responsible for system upgrades or updates via local file, ssh or sftp. Same tool also provides logs for the initial installation via usb stick or software image.
  - **Media Server Adapter** – Log of Media server, MGCP Adapter and SIPMGCP converter applications
  - **Process Manager** – Log of the Process Manager application responsible for the system sanity monitoring and also for license management. It includes processes status checking and starting or stopping them if applicable. It is also responsible for the configuration deployment, it includes the fallback to previous system partition when there is an

upgrade issue, the configuration is not valid, or the current system partition is corrupted.

- **Push Notification** - The logs related to notifications to an Apple Push Notification Server and Firebase Cloud Messaging Server.
- **QoS Application** - This is the log of QoS send TRAP application that sends over SNMP the QoS information to the QDC server that monitors the quality of voice calls.
- **QoS Monitoring** - This is the QoS data that was collected for the voice calls.
- **Redis Database**- Log of Redis Database.
- **Redundancy** – This log show details about the redundancy manager application. It is useful to debug issues related to redundancy process functionalities, like switchover failures.
- **Registration Blacklist**

  This table stores the subscribers that try to register but fails due not configured or wrong credentials.
- **RTP Proxy**

  The RTP Proxy is the component responsible to relay RTP packets between different interfaces and some VoIP features interworking like transcoding, transrating, SRTP, ICE, STUN, etc. RTP Proxy logs are useful debugging issues involving these features, specially voice quality issues, DTMF, FAX T.38, rtcp-mux, etc.
- **SIP Server** – SIP Server is a Kamalio application running in the system. It provides the SIP signaling, being always the system external SIP interface. This log is useful to debug call processing issues, SIP connection issues and many other problems in registration, port mapping, number modification, DNS, NAT, Options Heartbeat, etc.
- **SIP Service Provider** – This log shows details about the SSPs Registration process.
- **SSM** – SSM works together with SIPserver, it's used to provide some SIP functionalities and interworking with SIP Service providers. Usually their logs are needed for call failures related to SSPs, MoH for subscribers on SM, SipRec, call using anchored SBC sessions i.e. codec transcoding of SSM.
- **Simplified Installation** – The log of simplified installation is similar to the installation tool logs but in this case the installation procedure uses the easy install concept where the software and the system configuration is done almost with no intervention from the user.
- **Sip Load Balancer**- The logs related to Sip Load Balancer issue.
- **Survivability Provider** – Log of the Survivability provider application. This application is responsible for the OPTIONs heartbeat functionality,

that indicates the system's operational mode (SM, NM, etc). This application is also responsible for SSP registration.
  - **Symptom Collector** -This log contains the logs of the process used to send high priority logs direct to another server in the network. Useful onlywhen kernel logs and very low level errors must be checked.
  - **System** – This log contains the Kernel logs. Useful to debug operational system and device drivers (sensors, ethernet, etc) related issues.
  - **Web Server** – Log of the local web server application. Useful to debug the local management, GUI interface and XML issues.
  - **Peer Monitoring** - Log of the Peer Monitoring application, which monitors certain peers using OPTIONS messages.

NOTICE: This option is only available in V11R1.01.00 or higher.

- **Show** button opens the **Alarm History log** window to present the log information.
  - **Alarm History Log**

    This window presents the log information. It is possible to **Clear** the current log file, **Export** it to a local file or **Close** the window.

NOTICE: Alarm History, **Boot** and **Current processes** logs can't be cleared.

- **Clear** button clears the selected log file.

NOTICE: Alarm History, **Boot** and **Current processes** logs can't be cleared.

- **Clear All Logs** button clears all logs, except for **Alarm History**, **Boot** and **Current processes** logs.

Debugging Tools

- **Tool** - This drop down list selects the tool to be used:
  - **ICMP** - will start pinging
  - **Traceroute** - shows the hops from origin to the given destination
  - **Network Tracer** - gets and decodes IP packages on network.
- **Options**

  ICMP and Traceroute can have its own options entered in "Options" box. In this case the minimum option is one IP address. The given options are not parsed, because the user may want to configure some specific ping or traceroute options.

- **Interface**

  For the Network Tracer, there is a drop down list where the user selects the interface:

  – **All Interfaces**
  – **SIP/MGCP Trace**
  – **SIP/MGCP/RTP Trace**

  > **NOTICE: All Interfaces** - The network trace capture (wireshark) may not be able to capture all network packets over traffic load conditions, this is a limitation on this application.

  The original protocol information is stored in the TTL field (time to live) of the IP header. The new meanings of TTL field are:

  – UDP = 101 (decimal number)
  – TCP = 102
  – TLS = 103

  > **NOTICE:** This trace option limits the amount of data captured to 1MB. SIP messages exceeding the limit of 2048 bytes are truncated.

- **Output File Size**

  For the Network Tracer, there is a input field where the user enters the capture maximum file size. In case the maximum size is reached, the file will start to rewrite itself starting from the first entries. The range for this field is from 1MB to 100MB. This field is only applicable to the option "All".

- **Debug tool buttons**

  The **Start** button is used to execute the tool operation. The operation is stopped using **Stop** button then for **ICMP** and **Traceroute** the results can be seen in a new window by clicking on the **View** button or exported using the **Export** button. To get the **Network Tracer** results use the **Export** button.

- **Debug Results Viewer**

  Show the debug results of the selected tool.

Rapid Stat

Rapid stat is a tool that collects the system information in order to allow the system debugging.

- **Info level:**

  Up to five levels of information can be retrieved, based on the user selection the result will be a compressed file containing the information. By default the info level is set to 2.

  According to the level the following information will be stored in the compressed file:

  – Level 1 to 4 – System configuration, Template files, Boot and system log, Process manager log, Installed packages, CPU (Central Processing Unit) load, Security, SNMP (Simple Network Management Protocol), Memory usage, Disk usage, process status, License Information. Default

settings, SIP (Session Initiation Protocol) server logs, B2BUA (Back-to-Back User Agent) logs, SP logs, CDR (Call Detail Recording) logs, audit logs, Management logs, Media Server logs.

– Level 5 – adds the B2BUA channel usage and interface information for IGW HW types.

NOTICE: In level 5 due the amount of information collected, the Rapid stat can take several minutes.

5.7.3 Continuous Tracing

Enable

Flag used to enable Continuous Tracing.

Server

IP address of the Comm System-TM server.

System name

Comm System name configured on the Comm System-TM server.

NOTICE: Log/trace files are stored in the Comm System-TM server "\Tracedata\<System Hostname>\OpenBranch" directory on the Comm System-TM server. The "\Tracedata\" directory must be the home directory of the SFTP user.

File size threshold (kbytes) / Time interval threshold (min)

The log/trace files are sent to Comm System-TM server when one of the following conditions occurs:

- The file size reaches the File size threshold (valid values are between 1 and 1024kb);
- The Time interval threshold is elapsed (valid values are between 1 and 60 minutes).

The polling time is about 10 seconds so file sizes may vary if the amount of log data is increasing too fast.

SFTP username / SFTP password

Login information used to connect to the SFTP server on Comm System-TM.

SIP/Q931 trace

Flag used to enable the SIP/Q931 trace capture.

MGCP trace

Flag used to enable the MGCP trace capture.

5.7.4 On Demand Trace

The **On Demand Trace** overwrites the log level configuration for a specified interval of time. After that the log level configuration goes back to the configured one. The Continuous Tracing file size and time parameters still control when files are sent (via SFTP).

- **Log type**

  Selects the application to get the log.
- **Log level**

  Selects the log level. By default the log level is set to Error.
- **Duration**

  Specifies the duration time of an **On Demand Trace**. Ranges from 1 to 1440 minutes, default is 5 minutes.
- **Start** - button is used to execute the tool operation.
- **Stop** - button is used to stop an **On Demand Trace** operation.

5.7.5 Statistics

SIP

- **Active dialogs** - shows how many SIP dialogs are currently active.
- **Requests in** - represents the number of SIP requests received since SIP Server started.
- **Requests out** - represents the number of SIP requests sent since SIP Server started.
- **Responses in** - represents the number of SIP responses received since SIP Server started.
- **Responses out** - represents the number of SIP responses sent since SIP Server started.

Remote Endpoints Sessions

Remote Endpoint Sessions Table contains the call counters for remote endpoints.

The current used represent the number of concurrent session current used for each endpoint. The max used represents the maximal number of concurrent sessions used in the current day.

- **Overall current used** - the sum of concurrent sessions for all non circuit type endpoints.
- **Overall peak** - the sum of sessions peak for all non circuit type endpoints in the current day.
- **Requests out** - represents the number of SIP requests sent since SIP Server started.

5.7.6 Serviceability

Rest API Server

- **Enable**- enable the Rest API feature

- **Server Port** - The default Server Port is **8000**. You may change the Server Port from **8000** to another Port number and verify it.
- **Client Credentials**- Authentication is necessary for accessing the API routes. You can gain access by providing a valid ClientID / Client Password. The ClientID/Client password is sent on Authorization Header or into the Body of the request and then the Service API provides an access token to be used in each next request. The received token must be sent in Authorization Header.
- **Client ID**- Unique ID with at least 10 characters.
- **Client Password**- Password with at least 10 characters.

IMPORTANT: The Rest API will be available only on the SBC LAN side (for dual-armed configuration) in the port specified in the configuration.This is the server address that will listen for requests: `https://<SBC-LAN-IP>:<port>`

5.8 Alarms

In this administration area the user can configure the alarms and SNMP.

5.8.1 Alarms > Alarm Settings

The Alarms are presented in a table where the grayed fields can't be changed.

- **Group ID and Event ID** - These fields correspond to the last two components of the SNMP trap object ID (OID). An alarm trap is cleared by a trap with the same OID of severity 'cleared'.
- **Group name** - This field groups together different system status information of a similar type.
- **Event name** - This field is a character string that describers the alarm. It is closely related to the trap name, as defined in the Branch SNMP MIB.
- **Active** - This field determines if the alarm will be generated or not. If a particular alarm is not desired, or is not applicable to a particular system, it can be turned off by unchecking the checkbox.
- **Threshold** - This field defines the value that needs to be exceeded for an alarm to be generated. If, for example, the existence of an alarm condition is represented by True (= 1) then the threshold should be set to 0 to trigger an alarm.
- **Trigger** - This field shows the condition where the alarm will be generated. An alarm is triggered by comparing the Monitored value with the Threshold, using the Trigger as the comparison operator.
- **Severity** - This field is the alarm severity assigned to that particular alarm (warning, minor, major, critical). The Severity is fixed per Event ID.
- **Flow timer** - This field indicates the minimum time to wait before generating the next occurrence of the same alarm.
- **Reporting class** - This field is set to a number between 0 and 7 that groups events into classes that are reported to the same trap destination. 0 means that the event is not reported via SNMP trap.

- **Faulty object** - This field is a character string that defines the object that is at fault. This value may be different from Branch to Branch, but it is fixed for a particular Branch.
- **Event type** - This field classifies the alarms into:
  - Communications
  - Environmental
  - Equipment
  - Processing error
  - Quality of service

An alarm can be cleared either individually or by group.

Once an alarm is cleared, it will only appear in the **Alarm History** log.

The following alarms are disabled by default:

- **Malformed SIP Message**: To activate the alarm, simply check the **Active** checkbox of the Group Id / Event Id - 9/20 related to **Malformed SIP Message** in the **Alarm Settings** screen, and then apply the changes.
- **Low number of registered users**: To activate the alarm, simply check the **Active** checkbox of the Group Id / Event Id - 6/2 related to **Low number of registered users** in the **Alarm Settings** screen, and then apply the changes.

5.8.2 Alarms > SNMP Configuration

General

- **SNMP v2c Read-Only Community Name** - The user must enter the community name. Its length must be minimum 1 character and not exceed 32 characters.
- **SNMP v2c Read-Only IP** -

SNMP v2c Trap Destinations

The maximum number of rows permitted in the table is 5 for SBC and 5 for OSB.

- **IP address** - The user is able to enter the same IP address on multiple rows, but with different port numbers.
- **Port** -
- **Community name** - Minimum length of 6 and maximum of 32 characters. This is a required field when an IP address and port have been entered. The content of this parameter is not presented for users which are not in the same group as the root user.
- **Blocked** - When this field is checked, no traps will be sent to this destination. The default value is unchecked. This field can be used to block all three types of trap destination.
- **Reporting class set** -
- **Type** - The default for this field when a new row is added to the table is "Alarm". This field is not editable.

SNMP v3 EngineId Configuration

- **Current SNMP Engine ID** - This field is for display only to indicate what the current Engine ID is set to.

Only one of the following checkboxes can be checked at any time:

- **Generate from IP address** - Net-Snmp will choose the first IP address that it finds. Whether it is IPv4 or IPv6 is dependent on how the system has been configured. This should be checked by default when the system first starts up..
- **Generate from MAC address** - When this checkbox is selected then the drop-down list next to it is enabled and provides the list of all available NIC ports on the system. The default value is "eth0". Only the active NIC ports are displayed.
- **Text entry (max 27 chars)** - When this checkbox is selected then the field next to it is enabled. The user may enter a regular text string, up to a maximum of 27 characters, including spaces. The default for this field is an empty string.
- **Hex string entry (max 27 bytes)** - When this checkbox is selected then the field next to it is enabled. The user may enter a regular hex string, up to a maximum of 27 bytes. The default for this field is an empty string. The user can enter up to 54 hexadecimal characters. When the letters A through F are entered, either upper case or lower case is acceptable. Characters that are not 0-9 or A-F (or a-f) are not be acceptable.

SNMP v3 GET Configuration

- **Enable SNMP Get** - This checkbox allows the snmp v3 gets of linux default MIB.It is disabled by default.
- **Readonly user** - Default value: snmpv3user

  (min: 6 characters and max: 32 characters)
- **Authentication level** - Default value: authPriv
- **Authentication method** - Default value: SHA1
- **Encryption method** - Default value: AES
- **Authentication pass** - Default value: snmpv3authPass

  (min: 8 characters and max: 32 characters)
- **Encryption pass** - Default value: snmpv3encPass

  (min: 8 characters and max: 32 characters)

SNMP v3 Trap Destinations

The maximum number of rows permitted in the table is 5 for SBC and 5 for OSB.

- **IP address** - This field identifies the IP address of the far-end system to which traps are to be sent.
- **Port** - This field identifies the port number of the far-end system to which traps are to be sent. This is a required field when an IP address has been entered.
- **Security name** - Minimum length of 6 and maximum of 32 characters. This is a required field when an IP address and port have been entered. The content of this parameter is not presented for users which are not in the same group as the root user.

- **Security Level** - This is a required field when an IP address and port has been entered. This field is a drop-down list offering 3 choices:
  - None - Selecting this option provides no security at all and is essentially equivalent to what is offered now with SNMP v2c. This choice is not recommended.
  - Auth only- Selecting this option will result in the security name and password being validated before the trap is accepted at the trap receiver. The data content of the trap is in clear text. When this option is selected, "Auth Protocol" and "Auth Password" are required fields.
  - Auth + Priv- Selecting this option will result in the security name and password being validated before the trap is accepted at the trap receiver. The data content of the trap is encrypted according to the setting of "Priv Protocol". When this option is selected, "Auth Protocol", "Auth Password", "Priv Protocol", and "Priv Password" are required fields.
- Auth Protocol - This field is a drop-down list offering 2 choices: "SHA-1" or "MD5". The default value for a new record in the table is an empty string. The user must select "SHA-1" or "MD5" when "Security Level" is set to "Auth Only" or "Auth+Priv". If the user selects "MD5", a pop-up message will be displayed that says: "Note that the MD5 protocol has been deprecated and is not recommended for use.". Click "OK" to dismiss the message.
- Auth Password - At least 8 characters must be entered, with a maximum of 32. This is a required field when "Security Level" is set to "Auth Only" or "Auth+Priv".
- **Priv Protocol** - This field is a drop-down list offering 2 choices: "AES" or "DES". The default value for a new record in the table is an empty string. The user must select "AES" or "DES" when "Security Level" is set to "Auth +Priv". If the user selects "DES", a pop-up message must be presented to the user that says: "Note that the DES protocol has been deprecated and is not recommended for use.". Click "OK" button to dismiss the message.
- **Priv Password** - At least 8 characters must be entered, with a maximum of 32. This is a required field when "Security Level" is set to "Auth+Priv"..
- Blocked - When checked, no traps will be sent to this destination. Default value is unchecked. This field can be used to block all three types of trap destination.
- **Reporting Class Set** - If reporting classes have been defined in the alarm definition screen, they can be entered here. The same rules apply to this field as are currently used in the field of the same name for SNMP v2c trap destinations. There is no default value for this field.
- Type - The default for this field when a new row is added to the table is "Alarm". This field is not editable.

The user must click **OK** and then **Apply Changes** for the changes to take effect.

5.9 Maintenance

In this administrative area the user can change system configuration by loading or importing a xml config file, backup system configuration by exporting a single xml config file or exporting all xml config files as a tar file (latest 10 files), and install the system using install, upgrade or update procedures.

IMPORTANT: For **Hosted OpenScape SBC** (hSBC) on **OS4K** Deployments, **Backup** is disabled.

5.9.1 Import/Export

To backup a xml config file go to the **Maintenance** > **Import/Export** tab. There will be a list of configuration files stored in the SBC and 4 action buttons: **Load**, **Upload**, **Export** and **Export all**. These action buttons can be used in the selected xml config file.

Load

- **Select a configuration file** - Select from the drop-down list the configuration file stored in the SBC that can be loaded.
- **Load** - reads, stores and applies xml config files settings in the SBC.

Import

- **Select a file to upload** - drop-down lists the configuration files stored in the SBC that can be loaded.
- **Upload** - uploads and stores the XML file selected by the user under **Choose File** and applies xml config files settings in the SBC.

Export

- **Select a configuration file**- Select from the drop-down list the configuration file stored in the SBC to be exported.
- **Export** - Shows the options **Save** or **Open** for the selected xml config file.
- **Export all** - creates a tar file with the latest 10 xml config files and shows the following options: **Save**, **Open** and **Cancel**.

Change History

The user can see the last time that the system configuration has been changed, as well as the **User** who made the change(s) and what **User IP address** they logged in from. By clicking the **Show last changes** button, the user can see a file to file comparison between the current system configuration file and the one prior to it. Differences in the configuration that are detected in the **XML diff** window are highlighted in yellow.

Since the SBC stores a number of prior system configuration files, it is possible to compare two adjacent files. Select the file to be compared from the **Compare with previous version** drop-down box and then click **Compare**. A new screen opens showing the comparison between the selected file and the one immediately preceding it. Differences in the configuration are highlighted in yellow.

5.9.2 Install/Upgrade

This section describes GUI access to the Installation and Upgrade functions. For a full description of the entire process and the associated steps, please see the *OpenScape SBC, Installation and Upgrade* document.

Installation

Using this option, the user can perform a full installation. The Installation erases both backup and active partitions and overwrites with existent SW in USB. The database can be preserved if it is previously stored in a USB stick.

NOTICE: This option is available only if the USB stick is plugged and the system is booting from the USB stick.

Upgrade

The Upgrade means a full version is installed on the backup partition and the active partition is preserved in case of failure.

Upgrade is possible by using USB stick, local files stored in PC, HTTPS or SFTP.

The version stored in the USB stick will be used. The user chooses which local files to upload, depending on the desired version. In other methods (HTTPS and SFTP), the user has to use the **List Version** button and then select from the Software version combo box which version will be used. The List is retrieved from the server of SW supplier.

IMPORTANT: For **Hosted OpenScape SBC** (hSBC) on **OS4K** Deployments, **Upgrade** is disabled.

Activation

After the upgrade process is completed, the new code must be activated. The activation can be requested for a specific date or immediately. It is also possible to request the system to wait for running calls before rebooting to activate the new code. The **Abandon** button can be used to remove the new flag but will leave the new software available to be used in the partition. The **Remove** button will clear the partition and set it as empty.

IMPORTANT:

The use of the option to wait calls will also reject new calls. It is important to know that the system will keep blocking new calls until the entire upgrade/activation process is completed. In case of redundant systems, this also includes the upgrade of the backup node. If the rejected calls cannot be diverted to other servers, they get lost.

Activation/ Restart Information

This area shows if a reboot process is running. It is possible to cancel the process by clicking **Activation/Restart cancel** and **Schedule Cancel**.

NOTICE: This information is also available on the Restart tab.

Redundant Systems

When redundancy is enabled, the upgrade takes place first in active node and then automatically in backup node. The backup node upgrade starts once the active node reboots with the upgraded version and becomes stable (7 minutes after the reboot).

If the upgrade fails, an alarm **Redundant system has an invalid version (sync. is disabled)** is generated to indicate that the backup node still has a non upgraded version. Once this occurs, the master node tries 9 times to upgrade the backup node. The time it takes to complete the 10 attempts is up to 50 min., after the master node is considered stabilized. If after an hour the alarm still remains, the backup node has to be manually upgraded.

New Code Activation

Blocking Calls Information

For redundant system, when the flag **Reboot only when all calls are disconnected** is selected and the upgrade is activated, the calls will be blocked until the end of the upgrade process in both nodes (master and backup).

When activating the upgrade, a warning message is displayed. During this period, for instance, it is not possible to receive or generate calls and register subscribers. However, it is possible to unlock the calls when the master node has already performed the upgrade and the backup node is not finished yet. For this, it is necessary to use the **Cancel wait for backup upgrade** button. The **Cancel wait for backup upgrade** button is only available when calls are being blocked on the system by the **pmc block** command.

5.9.3 Bulk Configuration (Delta XML)

The Delta XML Feature targets the support of bulk configurations of SBCs.

The user is able to use the same set of GUI's residing locally in the SBC either for individual configurations of SBCs or for bulk configuration.

One SBC system, preferably the same type (e.g.x3250 M5, x3550 M5 or virtual OSS 6000), is chosen to play the Master role of taking the configurations and creating a Delta file having the changes against the Master base file. The receiving SBCs will take the Delta file and merge, after checking the Version, SBC type, with the current configuration file.

IMPORTANT: The maximum number of XML configuration files stored on your system is 100. In case this amount exceeds 100, the older files are deleted until the compact flash is full with 100 files.

The Delta configuration process is a two step process and needs to be performed on the chosen SBC as Master.

1) Mark the fields to be changed in the regular GUI against the currently used XML file, either with the already valid entry or just mark it. After clicking

Create Diff the diff between the currently used XML file and the changes are presented in the GUI.

2) The deltas can be fine tuned. If accepted, the changes are verified and the Delta file is created. By clicking **Upload**, the Delta file is uploaded via sFTP to the Server on the CMP.

> **NOTICE:** Prior to start the creation of Delta XML file it is necessary to change all the data included. Changes are detected by differing the not applied changes with the last saved `config xml` file.

Delta XML file can be applied using the **Import/Export** tab. Select the Delta XML file via **Browse** and click **Upload**. **Apply Changes** is used to activate the changes.

> **NOTICE:** Before **Apply Changes**, it is possible to see the changes by accessing the **Bulk Configuration (Delta XML)** tab.

> **NOTICE:** Before **Apply Changes**, it is possible to upload several Delta XML files. All changes are merged to the current configuration. It is possible to have delta XML files with different purposes applied all at once.

Edit Delta XML

- **Please Validate Configuration Before Edition**- Clicking this button validates the selected configuration file.

  If successful, the new configuration is kept and a positive response file is sent to the SFTP server to complete the process.

  If applying is not successful, the SBC falls back to the previous configuration and a negative response file is sent to the SFTP server to complete the process.

  > **NOTICE:** Changes done on configuration after validating are only detected when reloading the **Bulk Configuration (Delta XML)** tab.

- **Skip Accepted**- When setting the buttons **<<Prev diff** and **Next diff>>**, skip the changes already accepted (background in green).
- **Prev diff**- The differences between the current configuration and the prior configuration are highlighted in yellow and they can be quickly located and navigated by clicking **<<Prev diff**, **Current diff** and **Next diff >>**.
- **Current diff** - Focuses on the diff area on the current selected change.
- **Next diff**- The differences between the current configuration and the prior configuration are highlighted in yellow and they can be quickly located and navigated by clicking **<<Prev diff**, **Current diff** and **Next diff >>**.
- **XML Path**- XML Path indicates, on the xml structure, the position of the currently selected change.

- **Replace Whole Table**- When checked, all "item" elements in the same level turn green. The exported Delta XML, when applied, replaces the whole previous configured table content by the one in green.

  The complete table (all "item" blocks) background should turn green when marked and return to original color when unmarked. The table navigation buttons **Prev** and **Next** should be greyed out when the check box is unmarked.
- **Full Hierarchy**- It extends the selection done by **Replace Whole Table** (background in green) to futher tables if they exist.
- **Table Index** - Informs the position of the "item" element (starts with 0).

  Prev and **Next** navigate inside the table selecting "item" elements individually.

  Accept and **Drop** apply to them.
- **Accept** - The color of selection should turn green when accepting.
- **Drop** - The color of selection should turn back to original color when dropping the change.
- **All** - When checked, **Accept** and **Drop** act over all the changes.

  When checked for the first time, the message **Accept / Drop operation** will be applied to all diffs. Please review the accepted changes before exporting is shown.
- **Validate Accepted Changes** - When pressed, **Validate Accepted Changes** is replaced by an **Export** button and an SFTP check box.

  Delta XML file can be exported through the browser or SFTP.

IMPORTANT: If local GUI is accessed through CMP, changing **Delta XML Name** is not possible. CMP demands `deltaXml.xml` as the name of the Delta XML file, any other name is ignored.

5.9.4 Restart

- **Restart**

  This button is used to reboot the system and use the software stored in the active partition.

  The user will be prompted to confirm the system's restart.

  On redundant systems this only restarts the selected node. To restart the other node of the redundant pair, select the other node and repeat the procedure.

NOTICE:

When the node being restarted is acting as Master the other node might take over the Master function.

- **Restart to backup**

  This button is used to reboot the system and use the software stored in backup partition.

  On redundant systems this only restarts the selected node to backup version. It is mandatory to repeat the procedure on the other node of the redundant pair.

  NOTICE:

  When the node being restarted to backup is acting as Master the other node might take over the Master function.

  NOTICE:

  In case one of the nodes has been restarted to backup and the other has not, an alarm stating **Redundant system has an invalid version (sync. is disabled)** is triggered until both are running the same version.

- **File system repair**

  This button calls the check and repair tool for all Branch disks. All problems found are automatically fixed.

  NOTICE: This option is only available if the USB stick is plugged and the system is booting from the USB stick.

  IMPORTANT: For **Hosted OpenScape SBC** (hSBC) on **OS4K** Deployments, **Restart** is disabled.

- **Redundancy**

  IMPORTANT: This button is only available in V11R1.0.0 or higher versions. For non-redundant systems, the button is disabled.

  – **Switchover to Master**: This button is used to switch the backup node to the master node, and the user will be logged off. The user will be prompted to confirm the switchover.
  – **Switchover to Backup**: This button is used to switch the master node to the backup node, and the user will be logged off. The user will be prompted to confirm the switchover.

- **Code partitions**

  The available code partitions are listed in a table with buttons to control them.

  The State column informs the following states:

  1) Blocked – the partition cannot be used by an upgrade process.
  2) Ready – the partition is available for an upgrade and has a valid software.
  3) Empty - the partition is avail but has no valid software.

- **Activation / Restart Information**

  This area shows if a reboot process is running. If the process has not be completed yet, it is possible to cancel it using the buttons **Activation/Restart cancel** and **Schedule Cancel**.

  NOTICE: This information is also available on the Install / Upgrade tab.

5.9.5 Scheduled Maintenance

This section shows the server's Scheduled Maintenance state. When in a maintenance state a server does not accept any calls and must be ready for administration procedures like updates and configurations. It is expected that another server takes care of the traffic during the maintenance state.

The following points apply for the Maintenance functionality:

- Maintenance mode in SBC is a way to set the SBC call processing in an out of service state, so the traffic can be handled by another server, without shutting down the server. In that way, the upgrade and configuration functionalities can still be done.
- In case of scheduled Maintenance administrators are responsible to redirect traffic to another SBC (in case the topology of the network does not support rerouting automatically) during the maintenance window. After this new implementation, there is the possibility of scheduling automatically the maintenance mode only when there are no active calls in the system.
- In case of scheduled Maintenance mode if flag **In Maintenance only after all calls are disconnected** is set, active calls are not affected at any way before **Time to wait for all calls be disconnected (between 1 to 72 hours)** is reached. Although, all new calls are rejected, until Maintenance mode is activated. Statistics work in maintenance mode and ongoing calls can still be monitored in the **Management Portal** in **Diagnostics & Logs Menu** and in the **Statistics** Tab.

The server can enter in a maintenance state either by a user or by internal conditions. The user can decide to put a server in maintenance in a defined time or immediately. The following fields are available:

Maintenance Schedule Options

- **Maintenance State**

  It is the current state of the server and the text inside the () describes how the server enters in this state. Available options:

  – **out of service (auto)**: when the server enters in maintenance by itself (normally associated with software or hardware problems).
  – **forced**: when requested by an users administrator.
  – **schedule**: when requested by an administrator using a specific date and time period.

- **System in maintenance**

  Select what type of maintenance state will be applied when **Apply** is pressed. Available options:

  – **Auto**: The **Auto** mode uses only the server software decisions to control if the server is in maintenance.
  – **Now**: The **Now** option forces the server to enter in maintenance immediately
  – **Schedule**: the **Schedule** option uses the time in the boxes below to select when the server enters in maintenance.

  NOTICE: The server can enter the maintenance state even before the date and time defined by the user in case it is needed.

- **Start and End Data / Time**

  These fields are used to define the period when the server enters in maintenance if the **Schedule** option is used. The timers here are always related to the server date and time not the user date and time (be careful when working in different time zones).
- **In maintenance only after all calls are disconnected**

  It is also possible to request the system to wait for running calls before starts the maintenance.

  The use of the option to wait calls also rejects new calls. It is important to know that the system keeps blocking new calls until the entire maintenance process is completed.
- **Response Codes sent when in Maintenance, Upgrading or Restarting**

  These are the selected codes and messages sent to the rejected new calls when **In maintenance only after all calls are disconnected** or **Reboot only when all calls are disconnected** (in Install / Upgrade or Restart tabs) is selected.

The Maintenance state can also be checked externally by an http request. This server can be enabled under Network / Net Services.

6 Appendix - Overview

The information in this section provides additional information for Maintenance and Configuration.

6.1 Alarm Information - Overview

The Alarms Information details section provides addtional information on specifc alarms for OpenScape Branch and OpenScape SBC.

Alarm information includes but is not limited to the following:

- Alarm List
- Descriptions
- Maintenance Procedure
- Alarm Group
- Severity

6.1.1 Concept of the Alarms and Fault Messages

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 Voice Fault Management via SNMP traps.

6.1.2 Alarm Information

An Alarm entry contains information to troubleshoot the fault. Each entry contains the following information:

- **Alarm ID:** ID that uniquely identifies an alarm e.g., 757, 1132 (numeric).
- **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).
- **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 Branch). The entity is referenced by a GUID (Global Unique Identifier). This GUID can be used to identify the alarm source in the system management.

- **Alarm Type:** "Alarm Group" and "Alarm Name" e.g., [Ethernet][Port 2 failure].
- **Last Occurred:** Date and time when this alarm last occurred e.g., 2011/06/01 04:12:23.
- **Acknowledged Status:** This field shows whether the administrator has confirmed the alarm or not. The value is false if the alarm has not been acknowledged.
- **User:** Name or ID of the user associated with the alarm. If the alarm is unconfirmed the display remains empty.
- **Hit Count:** Number of times this alarm has occurred.

6.1.3 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

Normal

- Alarm clearance event

6.1.4 Alarm Type

The Alarm Type information includes the Alarm Group and Alarm Name. Both group and name are used to identify where the fault occurred and what the fault entailed.

6.1.5 Alarm Groups

Each alarm is mapped to an alarm group T.he Alarm Group information indicates the general area of the fault, e.g., Hardware, Licensing, etc.

The alarm groups used and supported by the OpenScape Branch and OpenScape SBC are:

- Admin
- Communication
- Ethernet
- Hardware
- License
- Resource
- Software
- Usage

6.1.5.1 Alarm Group: Admin

An Admin alarm is generated when the OpenScape Branch or OpenScape SBC detects a data failure.

Admin alarms report issues related to:

- Password and Usernames
- Image failure (phone)
- Security verfication
- Installation failure (media, ACD, Attendant servers)

6.1.5.2 Alarm Group: Communication

A failed communication link with another network element is reported as a communication alarm.

Communication alarms examples area as follows:

- Authentication Server
- Media Gateway (SIP)
- Billing Server (CDR)
- Loss of communication failure (primary node of OSV)

6.1.5.3 Alarm Group: Ethernet

An Ethernet port becomes unavailable is reported as an Ethernet alarm.

6.1.5.4 Alarm Group: Hardware

A Hardware alarm is generated when the OpenScape Branch or OpenScape SBC detects a hardware failure.

Hardware alarms report problems related to:

- Power Supply (voltage)
- Fan (speed)
- Card and Port (failure)
- Card and Port (loss of signal)

6.1.5.5 Alarm Group: License

A License alarm is generated when the license violations are detected or licensing resources are at risk.

License alarms report issues related to:

- Violations
- Expirations
- Blocking
- Lack of Licenses
- Licenses already in use

6.1.5.6 Alarm Group: Resource

A Resource alarm is generated when low availability of resource is detected.

Resource report issues related to:

- Bandwidth
- CPU usage
- Disk space
- RAM

6.1.5.7 Alarm Group: Software

A Software alarm is generated when the software features and servers that should be running are not running when required.

Software report issues related to:

- Applications
- Backup Links
- Survivability
- Servers
- Upgrade failure

6.1.5.8 Alarm Group: Usage

A Usage alarm is generated when critical normal usage of critical resources is greatly exceeded or critical procedures can not complete due to high usage of a resource.

Usage report issues related to:

- Active Voice Channels
- CDR Billing file errors

6.1.6 Alarm List

The Alarm List information provides additional information on specific alarms for OpenScape Branch and OpenScape SBC The Alarm list that follows is based on the Alarm Name.

6.1.6.1 +1.5V high voltage

+1.5V high voltage.

Associated Device: OSB, SBC

Group Name: Hardware:

Severity: critical

Default Threshold: x3250: 1.650; d945: 1.650;

Faulty Object: HW-Sensors

Maintenance Procedure:

6.1.6.2 +1.5V low voltage

+1.5V low voltage.

Associated Device: OSB, SBC

Group Name: Hardware:

Severity: critical

Default Threshold: x3250: 1.350; d945: 1.350;

Faulty Object: HW-Sensors

Maintenance Procedure:

6.1.6.3 +3.3V high voltage

+3.3V high voltage.

Associated Device: OSB, SBC

Group Name: Hardware:

Severity: critical

Default Threshold: rx200: 3.646; rx330: 3.646; x3250: 3.6; x3550: 3.564; d945: 3.6;

Faulty Object: HW-Sensors

Maintenance Procedure:

6.1.6.4 +3.3V low voltage

+3.3V low voltage.

Associated Device: OSB, SBC

Group Name: Hardware:

Severity: critical

Default Threshold: rx200: 3.058; rx330: 3.058; x3250: 3.1; x3550: 3.039; d945: 3.1;

Faulty Object: HW-Sensors

Maintenance Procedure:

6.1.6.5 +5V high voltage

+5V high voltage.

Associated Device: OSB, SBC

Group Name: Hardware:

Severity: critical

Default Threshold: rx200: 5.436; rx330: 5.436; x3250: 5.49; x3550: 5.582; d945: 5.49;

Faulty Object: HW-Sensors

Maintenance Procedure:

6.1.6.6 +5V low voltage

+5V low voltage.

Associated Device: OSB, SBC

Group Name: Hardware:

Severity: critical

Default Threshold: rx200: 4.659; rx330: 4.659; x3250: 4.5; x3550: 4.475; d945: 4.5;

Faulty Object: HW-Sensors

Maintenance Procedure:

6.1.6.7 +12V high voltage

+12V high voltage.

Associated Device: OSB, SBC

Group Name: Hardware:

Severity: critical

Default Threshold: rx200: 13.008; rx330: 13.008; x3250: 13.135; x3550: 13.446; d945: 13.135;

Faulty Object: HW-Sensors

Maintenance Procedure:

6.1.6.8 +12V low voltage

+12V low voltage.

Associated Device: OSB, SBC

Group Name: Hardware:

Severity: critical

Default Threshold: rx200: 11.055; rx330: 11.055; x3250: 10.792; x3550: 10.692; d945: 10.792;

Faulty Object: HW-Sensors

Maintenance Procedure:

6.1.6.9 Apache/PHP not running

Apache/PHP not running

Associated Device: OSB, SBC

Group Name: Software

Severity: major

Default Threshold: rx200: 0; rx330: 0; advantech250: 0; advantech50i: 0; advantech500i: 0; x3250: 0; x3550: 0; d945: 0;

Faulty Object: Apache/PHP

Maintenance Procedure: Process Manager has a mechanism to restart automatically the applications that are not running. If the Web Server is still not running after several restarts by PM check the web server log to see the root cause. As last resource proceed to a restart to backup.

6.1.6.10 Bandwidth ethernet port 1

Bandwidth ethernet port 1

Associated Device: OSB, SBC

Group Name: Resource

Severity: major

Default Threshold: rx200: 90; rx330: 90; advantech250: 90; advantech50i: 90; advantech500i: 90; x3250: 90; x3550: 90; d945: 90;

Faulty Object: Resource

Maintenance Procedure: Flooding TCP/IP packages on Ethernet port 1, this could indicate an excessive traffic of SIP/MGCP messages or an attack. If a kind of attack is being observer then Message Rate Control functionality should be enabled. Otherwise a network assessment is recommended.

6.1.6.11 Bandwidth ethernet port 2

Bandwidth ethernet port 2

Associated Device: OSB, SBC

Group Name: Resource

Severity: major

Default Threshold: rx200: 90; rx330: 90; advantech250: 90; advantech50i: 90; advantech500i: 90; x3250: 90; x3550: 90; d945: 90;

Faulty Object: Resource

Maintenance Procedure: Flooding TCP/IP packages on Ethernet port 1, this could indicate an excessive traffic of SIP/MGCP messages or an attack. If a kind of attack is being observer then Message Rate Control functionality should be enabled. Otherwise a network assessment is recommended.

6.1.6.12 BLC not running

BLC not running

Associated Device: OSB,SBC

Group Name: Software

Severity: critical

Default Threshold: rx200: 0; rx330: 0; advantech250: 0; advantech50i: 0; advantech500i: 0; x3250: 0; x3550: 0; d945: 0;

Faulty Object: BLC

Maintenance Procedure: Process Manager has a mechanism to restart automatically the applications that are not running. If BLC is still not running after several restarts by PM check the BLC logs to see the root cause. As last resource proceed to a restart to backup.

6.1.6.13 BLS not running

BLS not running

Associated Device: OSB,SBC

Group Name: Software

Severity: critical

Default Threshold: rx200: 0; rx330: 0; advantech250: 0; advantech50i: 0; advantech500i: 0; x3250: 0; x3550: 0; d945: 0;

Faulty Object: BLS

Maintenance Procedure: Process Manager has a mechanism to restart automatically the applications that are not running. If BLS is still not running after several restarts by PM check the BLS logs to see the root cause. As last resource proceed to a restart to backup.

6.1.6.14 Certificate Authority Could Not Be Validated

The certificate could not be validated against certificate authority chain.

Associated Device: OSB, SBC

Group Name: Security

Severity: major

Default Threshold: rx200: 0; rx330: 0; advantech250: 0; advantech50i: 0; advantech500i: 0; x3250: 0; x3550: 0; d945: 0;

Faulty Object: TLS Certificate

Maintenance Procedure: Verify the validity of the CA file. It can be that the certificate is expired or the root CA is missing.

6.1.6.15 Certificate Contains an Unknown Critical Extension

The certificate contains a critical extension which can not be handled

Associated Device: OSB, SBC

Group Name: Security

Severity: major

Default Threshold: rx200: 0; rx330: 0; advantech250: 0; advantech50i: 0; advantech500i: 0; x3250: 0; x3550: 0; d945: 0;

Faulty Object: TLS Certificate

Maintenance Procedure: The certificate and CA certificate shall only contain critical extensions which can be interpreted and handled by the system.

6.1.6.16 Certificate Has Been Revoked

The certificate has been revoked by the issuer and is not valid anymore.

Associated Device: OSB, SBC

Group Name: Security

Severity: major

Default Threshold: rx200: 0; rx330: 0; advantech250: 0; advantech50i: 0; advantech500i: 0; x3250: 0; x3550: 0; d945: 0;

Faulty Object: TLS Certificate

Maintenance Procedure: A new certificate shall be generated.

6.1.6.17 Certificate is Expired

The certificate installed on OpenScape Voice is expired.

Associated Device: OSB, SBC

Group Name: Security

Severity: major

Default Threshold: rx200: 0; rx330: 0; advantech250: 0; advantech50i: 0; advantech500i: 0; x3250: 0; x3550: 0; d945: 0;

Faulty Object: TLS Certificate

Maintenance Procedure: Update the certificate immediately.

6.1.6.18 Certificate is Out of the Validity Period

The certificate is not valid yet or is expired.

Associated Device: OSB, SBC

Group Name: Security

Severity: major

Default Threshold: rx200: 0; rx330: 0; advantech250: 0; advantech50i: 0; advantech500i: 0; x3250: 0; x3550: 0; d945: 0;

Faulty Object: TLS Certificate

Maintenance Procedure: A new certificate shall be generated.

6.1.6.19 Certificate Subject Could Not Be Authenticated

The certificate subject or alternative subject could not be authenticated against the configured FQDN of the certificate owner.

Associated Device: OSB, SBC

Group Name: Security

Severity: major

Default Threshold: rx200: 0; rx330: 0; advantech250: 0; advantech50i: 0; advantech500i: 0; x3250: 0; x3550: 0; d945: 0;

Faulty Object: TLS Certificate

Maintenance Procedure: The FQDN / IP address which is configured for the endpoint must match the FQDN which is indicated in the Subject field or in the Alternative Subject. Configure the correct FQDN or generate a new certificate with the correct FQDN.

6.1.6.20 Certificate Will Expire in the Next Days

A certificate installed on OpenScape Branch / OpenScape SBC will expire soon.

Associated Device: OSB, SBC

Group Name: Security

Severity: warning

Default Threshold: rx200: 0; rx330: 0; advantech250: 0; advantech50i: 0; advantech500i: 0; x3250: 0; x3550: 0; d945: 0;

Faulty Object: TLS Certificate

Maintenance Procedure: Update the certificate as soon as possible.

6.1.6.21 CDR disk space running low

CDR disk space running low

Associated Device: OSB, SBC

Group Name: Resource

Severity: major

Default Threshold: rx200: 90; rx330: 90; advantech250: 90; advantech50i: 90; advantech500i: 90; x3250: 90; x3550: 90; d945: 90;

Faulty Object: Resource

Maintenance Procedure:

6.1.6.22 DRHandler not running

CDRHandler not running

Associated Device: OSB

Group Name: Software

Severity: major

Default Threshold: rx200: 0; rx330: 0; advantech250: 0; advantech50i: 0; advantech500i: 0; x3250: 0; x3550: 0; d945: 0;

Faulty Object: CDR Handler

Maintenance Procedure: Process Manager has a mechanism to restart automatically the applications that are not running. If the CDR is still not running after several restarts by PM check the cdr logs to see the root cause. As last resource proceed to a restart to backup.

6.1.6.23 CPU1 +1.8V high voltage

CPU1 +1.8V high voltage.

Associated Device: OSB, SBC
Group Name: Hardware:
Severity: critical
Default Threshold: rx200: 2.03; rx330: 2.03; x3250: 1.980; d945: 1.980;
Faulty Object: HW-Sensors
Maintenance Procedure:

6.1.6.24 CPU1 +1.8V low voltage

CPU1 +1.8V low voltage.

Associated Device: OSB, SBC
Group Name: Hardware:
Severity: critical
Default Threshold: rx200: 1.58; rx330: 1.58; x3250: 1.620; d945: 1.620;
Faulty Object: HW-Sensors
Maintenance Procedure:

6.1.6.25 CPU1 Vtt high voltage

CPU1 Vtt high voltage.

Associated Device: OSB, SBC
Group Name: Hardware
Severity: critical
Default Threshold: rx330: 1.000; x3250: 1.380;
Faulty Object: HW-Sensors
Maintenance Procedure:

6.1.6.26 CPU1 Vtt low voltage

CPU1 Vtt low voltage.

Associated Device: OSB, SBC
Group Name: Hardware
Severity: critical
Default Threshold: rx330: 0.790; x3250: 1.120;
Faulty Object: HW-Sensors

Maintenance Procedure:

6.1.6.27 CPU2 +1.8V high voltage

CPU2 +1.8V high voltage.

Associated Device: OSB, SBC

Group Name: Hardware:

Severity: critical

Default Threshold: rx200: 2.03; rx330: 2.03;

Faulty Object: HW-Sensors

Maintenance Procedure:

6.1.6.28 CPU2 +1.8V low voltage

CPU2 +1.8V low voltage.

Associated Device: OSB, SBC

Group Name: Hardware:

Severity: critical

Default Threshold: rx200: 1.58; rx330: 1.58;

Faulty Object: HW-Sensors

Maintenance Procedure:

6.1.6.29 Critical failure on SIP Server configuration

Critical failure on SIP Server configuration

Associated Device: OSB,SBC

Group Name: Software

Severity: critical

Default Threshold: rx200: 0; rx330: 0; advantech250: 0; advantech50i: 0; advantech500i: 0; x3250: 0; x3550: 0; d945: 0;

Faulty Object: SIP Server

Maintenance Procedure: The sipserver configuration file is not acceptable. Check in the rapid stat file in osb.tar the error path, this will indicate which xml is causing trouble. To workaround this return to the previous xml where the sipserver was running.

6.1.6.30 Critical failure on SIP Server core

Critical failure on SIP Server core

Associated Device: OSB,SBC

Group Name: Software

Severity: critical

Default Threshold: rx200: 0; rx330: 0; advantech250: 0; advantech50i: 0; advantech500i: 0; x3250: 0; x3550: 0; d945: 0;

Faulty Object: SIP Server

Maintenance Procedure:Some internal function of sipserver is not being processed properly; most of the failures will not cause sipserver outage but to check the severity look on the sipserver logs.

6.1.6.31 CRL Could Not Be Copied From the Partner Node

A CRL issued by a Certification Authority could not be copied from the partner node.

Associated Device: OSB, SBC

Group Name: Security

Severity: warning

Default Threshold: rx200: 0; rx330: 0; advantech250: 0; advantech50i: 0; advantech500i: 0; x3250: 0; x3550: 0; d945: 0;

Faulty Object: TLS Certificate

Maintenance Procedure: Verify if there is enough disk space to store the CRL file.

6.1.6.32 CRL Could Not Be Downloaded

A CRL issued by a Certification Authority could not be downloaded due to network problems or problems at the download server.

Associated Device: OSB, SBC

Group Name: Security

Severity: warning

Default Threshold: rx200: 0; rx330: 0; advantech250: 0; advantech50i: 0; advantech500i: 0; x3250: 0; x3550: 0; d945: 0;

Faulty Object: TLS Certificate

Maintenance Procedure: Resolve the network problem that prevented the CRL download.

6.1.6.33 CRL Fails Because the Signature on the CRL is Invalid

CRL download request fails because the signature on the CRL is invalid.

Associated Device: OSB, SBC

Group Name: Security

Severity: major

Default Threshold: rx200: 0; rx330: 0; advantech250: 0; advantech50i: 0; advantech500i: 0; x3250: 0; x3550: 0; d945: 0;

Faulty Object: TLS Certificate

Maintenance Procedure: Contact the Certification Authority that issued the CRL to resolve the invalid CRL.

6.1.6.34 CRL is Expired

A CRL issued by a Certification Authority is expired.

Associated Device: OSB, SBC

Group Name: Security

Severity: warning

Default Threshold: rx200: 0; rx330: 0; advantech250: 0; advantech50i: 0; advantech500i: 0; x3250: 0; x3550: 0; d945: 0;

Faulty Object: TLS Certificate

Maintenance Procedure: Update the expired CRL.

6.1.6.35 CRL is Invalid

A CRL issued by a Certification Authority is invalid.

Associated Device: OSB, SBC

Group Name: Security

Severity: warning

Default Threshold: rx200: 0; rx330: 0; advantech250: 0; advantech50i: 0; advantech500i: 0; x3250: 0; x3550: 0; d945: 0;

Faulty Object: TLS Certificate

Maintenance Procedure: Contact the Certification Authority that issued the CRL to resolve the invalid CRL.

6.1.6.36 Database restored

Database restored

Associated Device: OSB,SBC

Group Name: Software

Severity: major

Default Threshold: rx200: 0; rx330: 0; advantech250: 0; advantech50i: 0; advantech500i: 0; x3250: 0; x3550: 0; d945: 0;

Faulty Object: Database

Maintenance Procedure: This alarm is only to indicate that dynamic database has been restored after a reboot/upgrade or switchover. The dynamic database stores the registered subscribers, port mapping and other information.

6.1.6.37 DHCP Server not running

DHCP Server not running

Associated Device: OSB,SBC

Group Name: Software

Severity: major

Default Threshold: rx200: 0; rx330: 0; advantech250: 0; advantech50i: 0; advantech500i: 0; x3250: 0; x3550: 0; d945: 0;

Faulty Object: DHCP Server

Maintenance Procedure: Process Manager has a mechanism to restart automatically the applications that are not running. If the DHCP is still not running after several restarts by PM check the DHCP configuration and system logs. As last resource proceed to a restart to backup.

6.1.6.38 Disk space running low

Disk space running low

Associated Device: OSB, SBC

Group Name: Resource

Severity: major

Default Threshold: rx200: 94; rx330: 94; advantech250: 94; advantech50i: 94; advantech500i: 94; x3250: 94; x3550: 94; d945: 94;

Faulty Object: Resource

Maintenance Procedure: There is no much space left on disk. Check for big files stored in the system, maybe some files were uploaded to the system using ssh connection and this is causing trouble. Check the in the rapid stat file the df.txt file, it will tell the disk usage. Check also messages.log to see if the big files are deleted automatically.

6.1.6.39 Extremely high CPU usage

Extremely high CPU usage

Associated Device: OSB, SBC

Group Name: Resource

Severity: critical

Default Threshold: rx200: 95; rx330: 95; advantech250: 95; advantech50i: 95; advantech500i: 95; x3250: 95; x3550: 95; d945: 95;

Faulty Object: Resource

Maintenance Procedure: This alarm is in general associated to high call rates or because due some failure one application is consuming excessive CPU. Check the in the rapid stat file the top.txt to see why the CPU is so busy. If the CPU usage is not decreasing even in a low call rates then the system must be restarted.

6.1.6.40 Failed to establish the minimum Backup Link bandwidth

Failed to establish the minimum Backup Link bandwidth

Associated Device: OSB,SBC

Group Name: Communication

Severity: critical

Default Threshold: rx200: 0; rx330: 0; advantech250: 0; advantech50i: 0; advantech500i: 0; x3250: 0; x3550: 0; d945: 0;

Faulty Object: BLC

Maintenance Procedure: Check why BackupLink calls are failing or taking too much to complete.

6.1.6.41 Failed to establish the required Backup Link bandwidth

Failed to establish the required Backup Link bandwidth)

Associated Device: OSB,SBC

Group Name: Communication

Severity: major

Default Threshold: rx200: 0; rx330: 0; advantech250: 0; advantech50i: 0; advantech500i: 0; x3250: 0; x3550: 0; d945: 0;

Faulty Object: BLC

Maintenance Procedure: BackupLink calls are failing or taking too much to complete. Check if enough channels are configured on BLS and/or why BackupLink calls are failing.

6.1.6.42 Failed update or upgrade

If upgrade failed, check the SW image file, system free memory and disk space. Check the install/upgrade log for further details.

Associated Device: OSB,SBC

Group Name: Software

Severity: critical

Default Threshold: rx200: 0; rx330: 0; advantech250: 0; advantech50i: 0; advantech500i: 0; x3250: 0; x3550: 0; d945: 0;

Faulty Object: VRRPD

Maintenance Procedure: Check the image's md5 to verify if the image isn't corrupt. If there is not disk space you may disable some system features, like Phone SW load, to free some disk space. If running on low memory you may try to reboot the system before the upgrade.

6.1.6.43 Failure to mirror phone images due to backup link mode

Failure to mirror phone images because system is in backup link mode.

Associated Device: OSB, SBC

Group Name: Admin

Severity: minor

Default Threshold: rx200: 0; rx330: 0; advantech250: 0; advantech50i: 0; advantech500i: 0; x3250: 0; x3550: 0; d945: 0;

Faulty Object: phone sw repository

Maintenance Procedure: The system is in backup link mode, see alarm (groupId='5' eventId='14').

6.1.6.44 Failure to mirror phone images due to less than 25Mb available

Failure to mirror phone images because less than 25Mb available, the phone sw repository is configured to has maximum 250Mb on disk.

Associated Device: OSB, SBC

Group Name: Admin

Severity: major

Default Threshold: rx200: 0; rx330: 0; advantech250: 0; advantech50i: 0; advantech500i: 0; x3250: 0; x3550: 0; d945: 0;

Faulty Object: phone sw repository

Maintenance Procedure: The system has a low space to store images, try remove these images to get available space. Go to tab 'Network Services' then click on button 'Phone software management' and delete one or more images.

6.1.6.45 Failure to mirror phone images due to survivable mode

Failure to mirror phone images because the system is in survivable mode.

Associated Device: OSB, SBC

Group Name: Admin

Severity: minor

Default Threshold: rx200: 0; rx330: 0; advantech250: 0; advantech50i: 0; advantech500i: 0; x3250: 0; x3550: 0; d945: 0;

Faulty Object: phone sw repository

Maintenance Procedure: The system is in survivable mode, see alarm (groupId='5' eventId='4').

6.1.6.46 Feature blocked due to license

Feature blocked due to license

Associated Device: OSB, SBC

Group Name: License

Severity: minor

Default Threshold: rx200: 0; rx330: 0; advantech250: 0; advantech50i: 0; advantech500i: 0; x3250: 0; x3550: 0; d945: 0;

Faulty Object: License

Maintenance Procedure: One feature was previously enabled and the license for this feature was no longer available. In this case the feature will be automatically blocked. If the feature is required then the license for the feature must be acquired. The alarm must be manually cleared.

6.1.6.47 File I/O error

The system get an error about read or write in disk.

Associated Device: OSB, SBC

Group Name: Admin

Severity: major

Default Threshold: rx200: 0; rx330: 0; advantech250: 0; advantech50i: 0; advantech500i: 0; x3250: 0; x3550: 0;

Faulty Object: phone sw repository

Maintenance Procedure:

6.1.6.48 Generic error code

Generic error code

Associated Device: OSB, SBC

Group Name: Admin

Severity: major

Default Threshold: rx200: 0; rx330: 0; advantech250: 0; advantech50i: 0; advantech500i: 0; x3250: 0; x3550: 0;

Faulty Object: phone sw repository

Maintenance Procedure: The system get a unknow error.

6.1.6.49 Geo-redundant data transfer to remote branch failed attempts

The system tries to export port_map information and ftp it to the geo-redundant system. It tries to do this at pre-configured interval (default 60s). System will try transfer 10 times, If all tries failed the alarm will be triggered.

Associated Device: SBC

Group Name: Communication

Severity: critical

Default Threshold: rx200: 0; x3250: 0; x3550: 0;

Faulty Object: Geosepmgr

Maintenance Procedure: To repair this problem verify connection between systems, if the communication go back the alarm will be automatic cleared.

6.1.6.50 Geo-redundant data not received from remote branch

The system repeatedly looks for port_map information that is sent to it 'from' the remote system. If it does not get any information (if this file is not available - /opt/siemens/openbranch/var/geosepmgr/partner_pm_data.csv), then alarm will be triggered.

Associated Device: SBC

Group Name: Communication

Severity: critical

Default Threshold: rx200: 0; x3250: 0; x3550: 0;

Faulty Object: Geosepmgr

Maintenance Procedure: To repair this problem verify connection between systems, if the communication go back the alarm will be automatic cleared.

6.1.6.51 High ambient temperature

High ambient temperature.

Associated Device: OSB, SBC

Group Name: Hardware:

Severity: critical

Default Threshold: rx200: 42; rx330: 42; advantech250: 58; advantech50i: 58; advantech500i: 58; x3250: 58; x3550: 41;

Faulty Object: HW-Sensors

Maintenance Procedure: TBD

6.1.6.52 High CPU usage

High CPU usage

Associated Device: OSB, SBC

Group Name: Resource

Severity: minor

Default Threshold: rx200: 80; rx330: 80; advantech250: 80; advantech50i: 80; advantech500i: 80; x3250: 80; x3550: 80; d945: 80;

Faulty Object: Resource

Maintenance Procedure: This alarm is in general associated to high call rates or because due some failure one application is consuming excessive CPU. Check the in the rapid stat file the top.txt to see why the CPU is so busy. If the CPU usage is not decreasing even in a low call rates then the system must be restarted.

6.1.6.53 High number of active voice channels

High number of active voice channels

Associated Device: OSB, SBC

Group Name: Usage

Severity: major

Default Threshold: rx200: 0; rx330: 0; advantech250: 0; advantech50i: 0; advantech500i: 0; x3250: 0; x3550: 0; d945: 0;

Faulty Object: Voice channels

Maintenance Procedure:

6.1.6.54 High RAM usage

High RAM usage

Associated Device: OSB, SBC

Group Name: Resource

Severity: major

Default Threshold: rx200: 80; rx330: 80; advantech250: 80; advantech50i: 80; advantech500i: 80; x3250: 80; x3550: 80; d945: 80;

Faulty Object: Resource

Maintenance Procedure: This alarm is in general associated to one application consuming excessive memory due some leak. Check the in the rapid stat file the top.txt and free.txt to see why the memory usage is so high. If the memory usage is not decreasing even in a low call rates then the system must be restarted.

6.1.6.55 High system board temperature

High system board temperature.

Associated Device: OSB, SBC

Group Name: Hardware:

Severity: critical

Default Threshold: rx200: 65; rx330: 65; d945: 80;

Faulty Object: HW-Sensors

Maintenance Procedure:

6.1.6.56 High temperature core 0

High temperature core 0.

Associated Device: OSB, SBC

Group Name: Hardware:

Severity: critical

Default Threshold: rx200: 72; rx330: 72; advantech250: 70; advantech50i: 70; advantech500i: 70; x3250: 70; x3550: 70; d945: 90;

Faulty Object: HW-Sensors

Maintenance Procedure:

6.1.6.57 High temperature core 1

High temperature core 1.

Associated Device: OSB, SBC

Group Name: Hardware:

Severity: critical

Default Threshold: rx200: 72; rx330: 72; advantech250: 70; advantech50i: 70; advantech500i: 70; x3250: 70; x3550: 70;

Faulty Object: HW-Sensors

Maintenance Procedure:

6.1.6.58 Install: ACD install failed

Install: ACD install failed.

Associated Device: OSB, SBC

Group Name: Admin

Severity: critical

Default Threshold: rx200: 0; rx330: 0; advantech250: 0; advantech50i: 0; advantech500i: 0; x3250: 0; x3550: 0; d945: 0;

Faulty Object: Install

Maintenance Procedure: During the simplified installation process the ACD files were not downloaded and therefore not installed. Check if the files are available at CMP and the path informed by CMP is correct and see the reason for this on simplified install logs. As last resource the workaround will be upload the files manually.

6.1.6.59 Install: Auto Attendant install failed

Install: Auto Attendant install failed.

Associated Device: OSB, SBC

Group Name: Admin

Severity: critical

Default Threshold: rx200: 0; rx330: 0; advantech250: 0; advantech50i: 0; advantech500i: 0; x3250: 0; x3550: 0; d945: 0;

Faulty Object: Install

Maintenance Procedure: During the simplified installation process the Auto Attendant files were not downloaded and therefore not installed. Check if the files are available at CMP and the path informed by CMP is correct and see the reason for this on simplified install logs. As last resource the workaround will be upload the files manually.

6.1.6.60 Install: Media Server install failed

Install: Media Server install failed.

Associated Device: OSB, SBC

Group Name: Admin

Severity: critical

Default Threshold: rx200: 0; rx330: 0; advantech250: 0; advantech50i: 0; advantech500i: 0; x3250: 0; x3550: 0;

Faulty Object: Install

Maintenance Procedure: During the simplified installation process the Media Server files were not downloaded and therefore not installed. Check if the files are available at CMP and the path informed by CMP is correct and see the reason for this on simplified install logs. As last resource the workaround will be upload the files manually.

6.1.6.61 IP blocked due to packet flood

IP blocked due to packet flood

Associated Device: OSB, SBC

Group Name: Usage

Severity: major

Default Threshold: rx200: 0; rx330: 0; advantech250: 0; advantech50i: 0; advantech500i: 0; x3250: 0; x3550: 0; d945: 0;

Faulty Object: Message Rate Control

Maintenance Procedure: The flooding mechanism of Message Rate Control blocked one IP because the number of the packages sent by this IP is higher that the configured. If this is not consider an attack the Message rate threshold can be increased or the IP can be added to the white list.

6.1.6.62 License has expired

License has expired

Associated Device: OSB, SBC

Group Name: License

Severity: major

Default Threshold: rx200: 0; rx330: 0; advantech250: 0; advantech50i: 0; advantech500i: 0; x3250: 0; x3550: 0; d945: 0;

Faulty Object: License

Maintenance Procedure: The system is running without license. To solve this enter a valid license.

6.1.6.63 License HW-Id is already in use

License HW-Id already in use

Associated Device: OSB, SBC

Group Name: License

Severity: major

Default Threshold: rx200: 0; rx330: 0; advantech250: 0; advantech50i: 0; advantech500i: 0; x3250: 0; x3550: 0; d945: 0;

Faulty Object: License

Maintenance Procedure: The Hardware ID stored in the license server is already used and the system is trying to get the license using this ID. If the Hardware ID is no longer used in license server it must be deleted.

6.1.6.64 License info wrong or non existent Logical-ID

License info with wrong or non existent Logical-ID

Associated Device: OSB, SBC

Group Name: License

Severity: major

Default Threshold: rx200: 0; rx330: 0; advantech250: 0; advantech50i: 0; advantech500i: 0; x3250: 0; x3550: 0; d945: 0;

Faulty Object: License

Maintenance Procedure: The Logical-ID does not match with the one stored in the license server. To solve this change the logical ID on local GUI. The alarm must be manually cleared.

6.1.6.65 License using temporary grace period

License using temporary grace period

Associated Device: OSB, SBC

Group Name: License

Severity: major

Default Threshold: rx200: 0; rx330: 0; advantech250: 0; advantech50i: 0; advantech500i: 0; x3250: 0; x3550: 0; d945: 0;

Faulty Object: License

Maintenance Procedure: The system is running either without license or can not contact the license server to check if the license is still valid. In this case a grace period is provided. To solve this enter a valid license and check the license server connectivity.

6.1.6.66 License violation detected

License violation detected

Associated Device: OSB, SBC

Group Name: License

Severity: major

Default Threshold: rx200: 0; rx330: 0; advantech250: 0; advantech50i: 0; advantech500i: 0; x3250: 0; x3550: 0; d945: 0;

Faulty Object: License

Maintenance Procedure:

6.1.6.67 License will expire

License will expire

Associated Device: OSB, SBC

Group Name: License

Severity: critical

Default Threshold: rx200: 0; rx330: 0; advantech250: 0; advantech50i: 0; advantech500i: 0; x3250: 0; x3550: 0; d945: 0;

Faulty Object: License

Maintenance Procedure: The system is running with valid licenses and the license will expire in less than 60 days. To solve this renew the licenses until the expiration date.

6.1.6.68 License not configured in Server

License not configured in Server

Associated Device: OSB, SBC

Group Name: License

Severity: major

Default Threshold: rx200: 0; rx330: 0; advantech250: 0; advantech50i: 0; advantech500i: 0; x3250: 0; x3550: 0; d945: 0;

Faulty Object: License

Maintenance Procedure: There is no license available for the branch on the license server. In the license server move or add licenses for the branch. The alarm will be automatically cleared when the licenses is applied.

6.1.6.69 Loss of communication with another OSB in the branch

Loss of communication with another OSB in the branch

Associated Device: OSB,SBC

Group Name: Communication

Severity: major

Default Threshold: rx200: 0; rx330: 0; advantech250: 0; advantech50i: 0; advantech500i: 0; x3250: 0; x3550: 0; d945: 0;

Faulty Object: SIP Link Server

Maintenance Procedure: The Peer OSB is not reachable the network connection as well if the Peer system is up and running.

6.1.6.70 Loss of communication with billing server

Loss of communication with billing serer

Associated Device: OSB,SBC

Group Name: Communication

Severity: major

Default Threshold: rx200: 0; rx330: 0; advantech250: 0; advantech50i: 0; advantech500i: 0; x3250: 0; x3550: 0; d945: 0;

Faulty Object: Billing server link

Maintenance Procedure: This happens when CDR was not able to contact the remote billing server, in this case check the IP address of billing server and CDR passwords. If the network connections of billing server are working, check if the billing server is properly configured at remote machine.

6.1.6.71 Loss of communication with DNS server

Loss of communication with DNS server

Associated Device: OSB,SBC

Group Name: Communication

Severity: major

Default Threshold: rx200: 0; rx330: 0; advantech250: 0; advantech50i: 0; advantech500i: 0; x3250: 0; x3550: 0; d945: 0;

Faulty Object: DNS link

Maintenance Procedure: This alarm indicates a network problem. The DNS server is either not available or the network connection to the DNS is broken. Check the network and DNS settings.

6.1.6.72 Loss of communication with file server

Loss of communication with file server

Associated Device: OSB,SBC

Group Name: Communication

Severity: major

Default Threshold: rx200: 0; rx330: 0; advantech250: 0; advantech50i: 0; advantech500i: 0; x3250: 0; x3550: 0; d945: 0;

Faulty Object: File server link

Maintenance Procedure:

6.1.6.73 Loss of communication with gateway

Loss of communication with gateway

Associated Device: OSB,SBC

Group Name: Communication

Severity: critical

Default Threshold: rx200: 0; rx330: 0; advantech250: 0; advantech50i: 0; advantech500i: 0; x3250: 0; x3550: 0; d945: 0;

Faulty Object: GATEWAY link

Maintenance Procedure: This alarm indicates that the network gateway is not reachable. Check the network gateway configuration and network connections.

6.1.6.74 Loss of communication with Node 1 Backup OSV

Loss of communication with Node 1 Backup OSV

Associated Device: OSB,SBC

Group Name: Communication

Severity: major

Default Threshold: rx200: 0; rx330: 0; advantech250: 0; advantech50i: 0; advantech500i: 0; x3250: 0; x3550: 0; d945: 0;

Faulty Object: Node 1 BackupOSV link

Maintenance Procedure: The OSV Node 1 Backup system is not responding to the OPTIONS messages and therefore is consider not reachable. Check OSV addresses, network connections and switches and if the OSV is up and running on Node 1 backup server.

6.1.6.75 Loss of communication with Node 1 Primary OSV

Loss of communication with Node 1 Primary OSV

Associated Device: OSB,SBC

Group Name: Communication

Severity: major

Default Threshold: rx200: 0; rx330: 0; advantech250: 0; advantech50i: 0; advantech500i: 0; x3250: 0; x3550: 0; d945: 0;

Faulty Object: Node 1 Primary OSV link

Maintenance Procedure: The OSV Node 1 Primary system is not responding to the OPTIONS messages and therefore is consider not reachable. Check OSV addresses, network connections and switches and if the OSV is up and running on Node 1 Primary server.

6.1.6.76 Loss of communication with Node2 Backup OSV

Loss of communication with SIP Service Provider

Associated Device: OSB,SBC

Group Name: Communication

Severity: major

Default Threshold: rx200: 0; rx330: 0; advantech250: 0; advantech50i: 0; advantech500i: 0; x3250: 0; x3550: 0; d945: 0;

Faulty Object: Node2 Backup OSV link

Maintenance Procedure: The OSV Node 2 Backup system is not responding to the OPTIONS messages and therefore is consider not reachable. Check OSV addresses, network connections and switches and if the OSV is up and running on Node 2 Backup server.

6.1.6.77 Loss of communication with Node2 Primary OSV

Loss of communication with Node2 Primary OSV

Associated Device: OSB,SBC

Group Name: Communication

Severity: major

Default Threshold: rx200: 0; rx330: 0; advantech250: 0; advantech50i: 0; advantech500i: 0; x3250: 0; x3550: 0; d945: 0;

Faulty Object: Node2 Primary OSV link

Maintenance Procedure:

6.1.6.78 Loss of communication with NTP server

Loss of communication with NTP server

Associated Device: OSB,SBC

Group Name: Communication

Severity: major

Default Threshold: rx200: 0; rx330: 0; advantech250: 0; advantech50i: 0; advantech500i: 0; x3250: 0; x3550: 0; d945: 0;

Faulty Object: NTP server link

Maintenance Procedure: The external NTP server is not responding to the NTP requests and therefore is consider not reachable. Check the NTP addresses, network connections and switches and if the NTP service is up and running on server.

6.1.6.79 Loss of communication with Redundant System

Loss of communication with Redundant System

Associated Device: OSB,SBC

Group Name: Communication

Severity: major

Default Threshold: rx200: 0; rx330: 0; advantech250: 0; advantech50i: 0; advantech500i: 0; x3250: 0; x3550: 0; d945: 0;

Faulty Object: Redundancy

Maintenance Procedure:

6.1.6.80 Loss of communication with SIP Service Provider

Loss of communication with SIP Service Provider

Associated Device: OSB,SBC

Group Name: Communication

Severity: major

Default Threshold: rx200: 0; rx330: 0; advantech250: 0; advantech50i: 0; advantech500i: 0; x3250: 0; x3550: 0; d945: 0;

Faulty Object: SIP Service Provider

Maintenance Procedure: One of the configured SIP service providers is not reachable, in this case check the SSP addresses, network connectivity and if the availability of the SSP account.

6.1.6.81 Loss of communication with surveillance system

Loss of communication with sureillance system

Associated Device: OSB,SBC

Group Name: Communication

Severity: major

Default Threshold: rx200: 0; rx330: 0; advantech250: 0; advantech50i: 0; advantech500i: 0; x3250: 0; x3550: 0; d945: 0;

Faulty Object: Surveillance system link

Maintenance Procedure:

6.1.6.82 Low fan speed 1

Low fan speed 1.

Associated Device: OSB, SBC

Group Name: Hardware:

Severity: major

Default Threshold: rx200: 1920; rx330: 1020; x3250: 4000; x3550: 530;

Faulty Object: HW-Sensors

Maintenance Procedure:

6.1.6.83 Low fan speed 2

Low fan speed 2.

Associated Device: OSB, SBC

Group Name: Hardware:

Severity: major
Default Threshold: rx200: 1920; rx330: 1020; x3250: 4000; x3550: 530;
Faulty Object: HW-Sensors
Maintenance Procedure:

6.1.6.84 Low fan speed 3

Low fan speed 3.

Associated Device: OSB, SBC
Group Name: Hardware:
Severity: major
Default Threshold: rx200: 1920; rx330: 1020; x3250: 4000; x3550: 530;
Faulty Object: HW-Sensors
Maintenance Procedure:

6.1.6.85 Low fan speed 4

Low fan speed 4.

Associated Device: OSB, SBC
Group Name: Hardware:
Severity: major
Default Threshold: rx200: 1920; rx330: 1020; x3250: 4000; x3550: 530;
Faulty Object: HW-Sensors
Maintenance Procedure:

6.1.6.86 Low fan speed 5

Low fan speed 5.

Associated Device: OSB, SBC
Group Name: Hardware:
Severity: major
Default Threshold: rx200: 1920; x3250: 4000; x3550: 530;
Faulty Object: HW-Sensors
Maintenance Procedure:

6.1.6.87 Low fan speed 6

Low fan speed 6.

Associated Device: OSB, SBC

Group Name: Hardware:

Severity: major

Default Threshold: rx200: 1920; x3550: 530;

Faulty Object: HW-Sensors

Maintenance Procedure:

6.1.6.88 Low fan speed 7

Low fan speed 7.

Associated Device: OSB, SBC

Group Name: Hardware:

Severity: major

Default Threshold: rx200: 1920;

Faulty Object: HW-Sensors

Maintenance Procedure:

6.1.6.89 Low fan speed 8

Low fan speed 8.

Associated Device: OSB, SBC

Group Name: Hardware:

Severity: major

Default Threshold: rx200: 1920;

Faulty Object: HW-Sensors

Maintenance Procedure:

6.1.6.90 Low fan speed 9

Low fan speed 9.

Associated Device: OSB, SBC

Group Name: Hardware:

Severity: major

Default Threshold: rx200: 1920;

Faulty Object: HW-Sensors

Maintenance Procedure:

6.1.6.91 Low fan speed 10

Low fan speed 10.

Associated Device: OSB, SBC
Group Name: Hardware:
Severity: major
Default Threshold: rx200: 1920;
Faulty Object: HW-Sensors
Maintenance Procedure:

6.1.6.92 Low fan speed 11

Low fan speed 11.

Associated Device: OSB, SBC
Group Name: Hardware:
Severity: major
Default Threshold: rx200: 1920;
Faulty Object: HW-Sensors
Maintenance Procedure:

6.1.6.93 Low fan speed 12

Low fan speed 12.

Associated Device: OSB, SBC
Group Name: Hardware:
Severity: major
Default Threshold: rx200: 1920;
Faulty Object: HW-Sensors
Maintenance Procedure:

6.1.6.94 Low fan 1 speed PSU 1

Low fan 1 speed PSU 1

Associated Device: OSB, SBC
Group Name: Hardware:
Severity: major
Default Threshold: rx200: 2880;
Faulty Object: HW-Sensors

Maintenance Procedure:

6.1.6.95 Low fan 2 speed PSU 1

Low fan 2 speed PSU 1

Associated Device: OSB, SBC
Group Name: Hardware:
Severity: major
Default Threshold: rx200: 2880;
Faulty Object: HW-Sensors
Maintenance Procedure:

6.1.6.96 Low fan 1 speed PSU 2

Low fan 1 speed PSU 2

Associated Device: OSB, SBC
Group Name: Hardware
Severity: major
Default Threshold: rx200: 2880;
Faulty Object: HW-Sensors
Maintenance Procedure:

6.1.6.97 Low fan 2 speed PSU 2

Low fan 2 speed PSU 2

Associated Device: OSB, SBC
Group Name: Hardware
Severity: major
Default Threshold: rx200: 2880;
Faulty Object: HW-Sensors
Maintenance Procedure:

6.1.6.98 Low fan speed 1B

Low fan speed 1B

Associated Device: OSB, SBC
Group Name: Hardware:
Severity: major

Default Threshold: x3550: 480;
Faulty Object: HW-Sensors
Maintenance Procedure:

6.1.6.99 Low fan speed 2B

Low fan speed 2B

Associated Device: OSB, SBC
Group Name: Hardware:
Severity: major
Default Threshold: x3550: 480;
Faulty Object: HW-Sensors
Maintenance Procedure:

6.1.6.100 Low fan speed 3B

Low fan speed 3B

Associated Device: OSB, SBC
Group Name: Hardware:
Severity: major
Default Threshold: x3550: 480;
Faulty Object: HW-Sensors
Maintenance Procedure:

6.1.6.101 Low fan speed 4B

Low fan speed 4B

Associated Device: OSB, SBC
Group Name: Hardware:
Severity: major
Default Threshold: x3550: 480;
Faulty Object: HW-Sensors
Maintenance Procedure:

6.1.6.102 Low fan speed 5B

Low fan speed 5B

Associated Device: OSB, SBC

Group Name: Hardware:

Severity: major

Default Threshold: x3550: 480;

Faulty Object: HW-Sensors

Maintenance Procedure:

6.1.6.103 Low fan speed 6B

Low fan speed 6B

Associated Device: OSB, SBC

Group Name: Hardware:

Severity: major

Default Threshold: x3550: 480;

Faulty Object: HW-Sensors

Maintenance Procedure:

6.1.6.104 msadapter not running

msadapter not running

Associated Device: OSB,SBC

Group Name: Software

Severity: critical

Default Threshold: rx200: 0; rx330: 0; advantech250: 0; advantech50i: 0; advantech500i: 0; x3250: 0; x3550: 0; d945: 0;

Faulty Object: msadapter

Maintenance Procedure: Process Manager has a mechanism to restart automatically the applications that are not running. If the Ms Adapter is still not running after several restarts by PM check the media server logs to see the root cause. As last resource proceed to a restart to backup.

6.1.6.105 Network failure

An error about network is generate.

Associated Device: OSB, SBC

Group Name: Admin

Severity: major

Default Threshold: rx200: 0; rx330: 0; advantech250: 0; advantech50i: 0; advantech500i: 0; x3250: 0; x3550: 0;

Faulty Object: phone sw repository

Maintenance Procedure: See link with HTTPS server is not broken.

6.1.6.106 Network not running

Network not running

Associated Device: OSB,SBC

Group Name: Software

Severity: critical

Default Threshold: rx200: 0; rx330: 0; advantech250: 0; advantech50i: 0; advantech500i: 0; x3250: 0; x3550: 0; d945: 0;

Faulty Object: Network

Maintenance Procedure: Process Manager has a mechanism to restart automatically the applications that are not running. If the network is still not running after several restarts by PM check the system logs to see the root cause. As last resource proceed to a restart to backup.

6.1.6.107 No Backup Link channel can be added at all

No Backup Link channel can be added at all

Associated Device: OSB,SBC

Group Name: Communication

Severity: critical

Default Threshold: rx200: 0; rx330: 0; advantech250: 0; advantech50i: 0; advantech500i: 0; x3250: 0; x3550: 0; d945: 0;

Faulty Object: BLC

Maintenance Procedure: Check why no BackupLink call is completing.

6.1.6.108 NTP not running

NTP not running

Associated Device: OSB,SBC

Group Name: Software

Severity: major

Default Threshold: rx200: 0; rx330: 0; advantech250: 0; advantech50i: 0; advantech500i: 0; x3250: 0; x3550: 0; d945: 0;

Faulty Object: NTP

Maintenance Procedure: Process Manager has a mechanism to restart automatically the applications that are not running. If the NTP is still not running after several restarts by PM check the system log to see the root cause. As last resource proceed to a restart to backup.

6.1.6.109 Parse error for instance when parsing command-line options the ’.wgetrc’ or ’.netcr’

Parse error for instance when parsing command-line options the ’.wgetrc’ or ’.netcr’

Associated Device: OSB, SBC

Group Name: Admin

Severity: major

Default Threshold: rx200: 0; rx330: 0; advantech250: 0; advantech50i: 0; advantech500i: 0; x3250: 0; x3550: 0;

Faulty Object: phone sw repository

Maintenance Procedure:

6.1.6.110 Phone image download denied due to connections number limit

Phone image download denied because the maximum connections number limit.

Associated Device: OSB, SBC

Group Name: Admin

Severity: minor

Default Threshold: rx200: 0; rx330: 0; advantech250: 0; advantech50i: 0; advantech500i: 0; x3250: 0; x3550: 0; d945: 0;

Faulty Object: phone sw repository

Maintenance Procedure: The system provide maximum number concurrent images, try increase that number on tab 'Network Services' then click on button 'Phone software management' and increase number 'Maximum Parallel Access'.

6.1.6.111 Phone image download denied due to system load over 60 percent

Phone image download denied because the maximum connections number limit.

Associated Device: OSB, SBC

Group Name: Admin

Severity: minor

Default Threshold: rx200: 0; rx330: 0; advantech250: 0; advantech50i: 0; advantech500i: 0; x3250: 0; x3550: 0;

Faulty Object: phone sw repository

Maintenance Procedure: Phone image download denied because system load over 60 percent.

6.1.6.112 Port 1 failure

Port 1 failure

Associated Device: OSB, SBC

Group Name: Ethernet

Severity: major

Default Threshold: rx200: 0; rx330: 0; advantech250: 0; advantech50i: 0; advantech500i: 0; x3250: 0; x3550: 0; d945: 0;

Faulty Object: Ethernet

Maintenance Procedure: The Ethernet port is not available. Process manager will try to restart the network several times if this problem persist the network cards must be replaced. In case of systems with on board interface the system must be replaced.

6.1.6.113 Port 2 failure

Port 2 failure

Associated Device: OSB, SBC

Group Name: Ethernet

Severity: major

Default Threshold: rx200: 0; rx330: 0; advantech250: 0; advantech50i: 0; advantech500i: 0; x3250: 0; x3550: 0; d945: 0;

Faulty Object: Ethernet

Maintenance Procedure: The Ethernet port is not available. Process manager will try to restart the network several times if this problem persist the network cards must be replaced. In case of systems with on board interface the system must be replaced.

6.1.6.114 Power Supply 1 Failure

Power Supply 1 Failure

Associated Device: OSB, SBC

Group Name: Hardware

Severity: major

Default Threshold: x3550: 1;

Faulty Object: HW-Sensors

Maintenance Procedure:

6.1.6.115 Power Supply 2 Failure

Power Supply 2 Failure

Associated Device: OSB, SBC

Group Name: Hardware

Severity: major

Default Threshold: x3550: 1;

Faulty Object: HW-Sensors

Maintenance Procedure:

6.1.6.116 Process Manager not running

Process Manager not running

Associated Device: OSB, SBC

Group Name: Software

Severity: critical

Default Threshold: rx200: 0; rx330: 0; advantech250: 0; advantech50i: 0; advantech500i: 0; x3250: 0; x3550: 0; d945: 0;

Faulty Object: Process manager

Maintenance Procedure: Process manager will be automatically restarted by Crom, once it restarts the alarm is generated. In this case check the core files and pm logs to determine the root cause. As last resource proceed to a restart to backup.

6.1.6.117 Protocol errors

The system get a error with HTTP Protocol.

Associated Device: OSB, SBC

Group Name: Admin

Severity: major

Default Threshold: rx200: 0; rx330: 0; advantech250: 0; advantech50i: 0; advantech500i: 0; x3250: 0; x3550: 0;

Faulty Object: phone sw repository

Maintenance Procedure: Try upgrade the HTTPS server.

6.1.6.118 PSU 1 failure

PSU 1 failure.

Associated Device: OSB, SBC

Group Name: Hardware:

Severity: major

Default Threshold: rx200: 20; rx330: 1020;

Faulty Object: HW-Sensors

Maintenance Procedure:

6.1.6.119 PSU 2 failure

PSU 2 failure.

Associated Device: OSB, SBC

Group Name: Hardware:

Severity: major

Default Threshold: rx200: 20; rx330: 1020;

Faulty Object: HW-Sensors

Maintenance Procedure:

6.1.6.120 Reboot requested due to license violation

Reboot requested due to license violation

Associated Device: OSB, SBC

Group Name: License

Severity: critical

Default Threshold: rx200: 0; rx330: 0; advantech250: 0; advantech50i: 0; advantech500i: 0; x3250: 0; x3550: 0; d945: 0;

Faulty Object: License

Maintenance Procedure: One or more system file was tampered and the License Controller detected the violation and decided to reboot the system. The action that leads to this must be investigated. The alarm will be cleared automatically after system restart.

6.1.6.121 Redundant system has an invalid version (sync.is disabled)

Redundant system has an invalid version (sync.is disabled)

Associated Device: OSB,SBC

Group Name: Communication

Severity: major

Default Threshold: rx200: 0; rx330: 0; advantech250: 0; advantech50i: 0; advantech500i: 0; x3250: 0; x3550: 0; d945: 0;

Faulty Object: Redundancy

Maintenance Procedure: The redundancy is enabled but the other node has an incompatible SW version. To solve this disable the redundancy on both systems and upgrade both systems to the same SW version.

6.1.6.122 Redundant system has not a compatible HW (sync. is disabled)

Redundant system has not a compatible HW (sync. is disabled)

Associated Device: OSB,SBC

Group Name: Communication

Severity: major

Default Threshold: rx200: 0; rx330: 0; advantech250: 0; advantech50i: 0; advantech500i: 0; x3250: 0; x3550: 0; d945: 0;

Faulty Object: Redundancy

Maintenance Procedure: The redundancy is enabled but the hardware models of the nodes are different, therefore redundancy can not be activated. The only possible solution is the replacement of one of the nodes to a compatible hardware model.

6.1.6.123 Redundant system synchronization fails

Redundant system synchronization fails

Associated Device: OSB,SBC

Group Name: Communication

Severity: major

Default Threshold: rx200: 0; rx330: 0; advantech250: 0; advantech50i: 0; advantech500i: 0; x3250: 0; x3550: 0; d945: 0;

Faulty Object: Redundancy

Maintenance Procedure: The database synchronization from master node to backup failed. This failure is associated in general with network failures or if the backup node is not up and running. Check network connections and backup node server.

6.1.6.124 RTPProxy not running

RTPProxy not running

Associated Device: OSB, SBC

Group Name: Software

Severity: critical

Default Threshold: rx200: 0; rx330: 0; advantech250: 0; advantech50i: 0; advantech500i: 0; x3250: 0; x3550: 0; d945: 0;

Faulty Object: RTPProxy

Maintenance Procedure: One or more instances of RTPProxy is not running. Process Manager has a mechanism to restart automatically the applications that are not running. If the RTP Proxy is still not running after several restarts by PM check the RTP Proxy log to see the root cause. As last resource proceed to a restart to backup.

6.1.6.125 SBC Session limit reached due to license

SBC Session limit reached due to license

Associated Device: OSB, SBC

Group Name: License

Severity: critical

Default Threshold: rx200: 0; rx330: 0; advantech250: 0; advantech50i: 0; advantech500i: 0; x3250: 0; x3550: 0; d945: 0;

Faulty Object: License

Maintenance Procedure: During a SBC session establishment the number of maximum allowed sessions was reached and the License Controller prevents the creation of this session If more sessions are required then the number of licensed must be increased by applying new licenses. The alarm must be manually cleared.

6.1.6.126 Server issued an error response

The HTTPS server send error 500 when system try synchronize with server.

Associated Device: OSB, SBC

Group Name: Admin

Severity: major

Default Threshold: rx200: 0; rx330: 0; advantech250: 0; advantech50i: 0; advantech500i: 0; x3250: 0; x3550: 0;

Faulty Object: phone sw repository

Maintenance Procedure: The system get family error 500 from HTTPS server.

6.1.6.127 sipmgcpconv not running

sipmgcpconv not running

Associated Device: OSB

Group Name: Software

Severity: critical

Default Threshold: rx200: 0; rx330: 0; advantech250: 0; advantech50i: 0; advantech500i: 0; x3250: 0; x3550: 0; d945: 0;

Faulty Object: sipmgcpconvSyslog

Maintenance Procedure: Process Manager has a mechanism to restart automatically the applications that are not running. If the SIP MGCP converter is still not running after several restarts by PM proceed to a restart to backup.

6.1.6.128 SIP Server database not restored

SIP Server database not restored

Associated Device: OSB,SBC

Group Name: Software

Severity: minor

Default Threshold: rx200: 0; rx330: 0; advantech250: 0; advantech50i: 0; advantech500i: 0; x3250: 0; x3550: 0; d945: 0;

Faulty Object: msadapter

Maintenance Procedure: This alarm indicates the dynamic database of sipserver was not restored after an upgrade. This is caused by upgrading from an incompatible database, this is not critical if the system is upgraded during maintenance window. And once the system is rebooting or restarted the alarm will be automatically cleared since the database will be recovered.

6.1.6.129 SIP Server not running

SIP Server not running

Associated Device: OSB, SBC

Group Name: Software

Severity: critical

Default Threshold: rx200: 0; rx330: 0; advantech250: 0; advantech50i: 0; advantech500i: 0; x3250: 0; x3550: 0; d945: 0;

Faulty Object: SIP Serverr

Maintenance Procedure: The SIP Server is not running. Process Manager has a mechanism to restart automatically the applications that are not running. If the Sip server is still not running after several restarts by PM check the sipserver logs to see the root cause. Another possible cause is wrong configuration, so reload the previous xml file using GUI. As last resource proceed to a restart to backup.

6.1.6.130 SSL verification failure

The system get a failure SSL verification.

Associated Device: OSB, SBC

Group Name: Admin

Severity: major

Default Threshold: rx200: 0; rx330: 0; advantech250: 0; advantech50i: 0; advantech500i: 0; x3250: 0; x3550: 0;

Faulty Object: phone sw repository

Maintenance Procedure: See certificate on HTTPS server, verify if that certificate is correct.

6.1.6.131 Message Rate Control not running

Message Rate Control not running

Associated Device: OSB,SBC

Group Name: Software

Severity: critical

Default Threshold: rx200: 0; rx330: 0; advantech250: 0; advantech50i: 0; advantech500i: 0; x3250: 0; x3550: 0; d945: 0;

Faulty Object: Message Rate Control

Maintenance Procedure: Process Manager has a mechanism to restart automatically the applications that are not running. If the Message Rate Control is still not running after several restarts by PM check the Message Rate Control logs to see the root cause. As last resource proceed to a restart to backup.

6.1.6.132 ssdp not running

ssdp not running

Associated Device: OSB,SBC

Group Name: Software

Severity: critical

Default Threshold: rx200: 0; rx330: 0; advantech250: 0; advantech50i: 0; advantech500i: 0; x3250: 0; x3550: 0; d945: 0;

Faulty Object: ssdp

Maintenance Procedure: The deployment plug-in is not running. To restart it run the following command as root in ssh: /etc/init.d/service-plugin restart.

6.1.6.133 Standalone operation

Standalone operation

Associated Device: OSB

Group Name: Communication

Severity: critical

Default Threshold: rx200: 0; rx330: 0; advantech250: 0; advantech50i: 0; advantech500i: 0; x3250: 0; x3550: 0; d945: 0;

Faulty Object: OSV link

Maintenance Procedure: Connection to OSV is broken. Check OSV address settings, network, switches and if the OSV is up and running on the server.

6.1.6.134 SurvProcess not running

SurvProcess not running

Associated Device: OSB, SBC

Group Name: Software

Severity: critical

Default Threshold: advantech250: 0; advantech50i: 0; advantech500i: 0; x3250: 0; x3550: 0; d945: 0;

Faulty Object: Survivability Provider

Maintenance Procedure: Process Manager has a mechanism to restart automatically the applications that are not running. If the Survivability Provider is still not running after several restarts by PM check the survivability provider log to see the root cause. As last resource proceed to a restart to backup.

6.1.6.135 Syslog not running

Syslog not running

Associated Device: OSB,SBC

Group Name: Software

Severity: critical

Default Threshold: rx200: 0; rx330: 0; advantech250: 0; advantech50i: 0; advantech500i: 0; x3250: 0; x3550: 0; d945: 0;

Faulty Object: Syslog

Maintenance Procedure: Process Manager has a mechanism to restart automatically the applications that are not running. If the Syslog is still not running after several restarts by PM check the system logs to see the root cause. As last resource proceed to a restart to backup.

6.1.6.136 Username/password authentication failure

Username/password authentication failure

Associated Device: OSB, SBC

Group Name: Admin

Severity: major

Default Threshold: rx200: 0; rx330: 0; advantech250: 0; advantech50i: 0; advantech500i: 0; x3250: 0; x3550: 0;

Faulty Object: phone sw repository

Maintenance Procedure:

6.1.6.137 User registration blocked due to license

User registration blocked due to license

Associated Device: OSB, SBC

Group Name: License

Severity: critical

Default Threshold: rx200: 0; rx330: 0; advantech250: 0; advantech50i: 0; advantech500i: 0; x3250: 0; x3550: 0; d945: 0;

Faulty Object: License

Maintenance Procedure: The number of the registered users is the maximum allowed for the current license, so new registrations will not be allowed. If more users are required then the number of licensed must be increased by applying new licenses. The alarm must be manually cleared.

6.1.6.138 VBAT high voltage

VBAT high voltage

Associated Device: OSB, SBC

Group Name: Hardware:

Severity: critical

Default Threshold: x3550: 3.248;

Faulty Object: HW-Sensors

Maintenance Procedure:

6.1.6.139 VBAT low voltage

VBAT low voltage

Associated Device: OSB, SBC

Group Name: Hardware:

Severity: critical

Default Threshold: x3550: 2.095;

Faulty Object: HW-Sensors

Maintenance Procedure:

6.1.6.140 Very high CPU usage

Very high CPU usage

Associated Device: OSB, SBC

Group Name: Resource

Severity: major

Default Threshold: rx200: 90; rx330: 90; advantech250: 90; advantech50i: 90; advantech500i: 90; x3250: 90; x3550: 90; d945: 90;

Faulty Object: Resource

Maintenance Procedure: This alarm is in general associated to high call rates or because due some failure one application is consuming excessive CPU. Check the in the rapid stat file the top.txt to see why the CPU is so busy. If the CPU usage is not decreasing even in a low call rates then the system must be restarted.

6.1.6.141 VRRPD not running

VRRPD not running

Associated Device: OSB,SBC

Group Name: Software

Severity: critical

Default Threshold: rx200: 0; rx330: 0; advantech250: 0; advantech50i: 0; advantech500i: 0; x3250: 0; x3550: 0; d945: 0;

Faulty Object: VRRPD

Maintenance Procedure:

6.1.6.142 Wrong user ID or password entered

Wrong user ID or password entered

Associated Device: OSB, SBC

Group Name: Admin

Severity: major

Default Threshold: rx200: 0; rx330: 0; advantech250: 0; advantech50i: 0; advantech500i: 0; x3250: 0; x3550: 0; d945: 0;

Faulty Object: Authentication

Maintenance Procedure: A wrong password was entered in a ssh session or system administration. Check the given password against the one configured. The passwords must be set accord to security policies.

6.1.6.143 High number of registered users

Associated Device: SBC

Group Name: Usage

Severity: critical

Default Threshold: advantech250: 250; x3250: 6000; x3550: 32000; sr530: 32000; sr630: 32000; kontron550: 6000;

Faulty Object: SIP Server

Maintenance Procedure: The server capacity has been exceeded. Consider changing the server type or using a new server. If the user configured this limit, the number of registered subscribers has exceeded it.

6.1.6.144 Low number of registered users

Associated Device: SBC

Group Name: Usage

Severity: critical

Default Threshold: advantech250: 25; x3250: 600; x3550: 3200; sr530: 3200; sr630: 3200; kontron550: 600;

Faulty Object: SIP Server

Maintenance Procedure: The number of registered subscribers is below the configured limit.

Index

A

Access IP 162, 165
Activate software 63
Administrative Access Control 221
Alarm Details 41
Alarm settings 122
Alarms 39, 122, 414, 418, 418, 418, 419, 419, 419, 420, 420, 420, 420, 421, 421, 421, 422, 422, 422, 423, 423, 423, 424, 424, 424, 425, 425, 425, 425, 426, 426, 426, 426, 427, 427, 427, 428, 428, 428, 429, 429, 429, 430, 430, 430, 431, 431, 431, 432, 432, 432, 433, 433, 433, 434, 434, 434, 435, 435, 435, 435, 436, 436, 436, 437, 437, 437, 438, 438, 438, 439, 439, 439, 440, 440, 440, 441, 441, 441, 442, 442, 442, 443, 443, 443, 443, 444, 444, 444, 444, 445, 445, 445, 446, 446, 446, 446, 447, 447, 447, 447, 448, 448, 448, 448, 449, 449, 449, 450, 450, 450, 451, 451, 451, 452, 452, 452, 453, 453, 453, 453, 454, 454, 454, 455, 455, 455, 456, 456, 456, 457, 457, 457, 458, 458, 458, 459, 459, 459, 460, 460, 460, 460, 461, 461, 461, 462
Alarms settings 123, 126, 129, 130
Audience 11

B

Backup 242
Batch job 64, 65, 66
Batch jobs 64
Black List 215
Branch office 29
Branch office:Create and Delete 30, 80, 82
Branch office:Display 31
Business group 29

C

Certificates 190
Communication system 266, 270
Configuration file 59
Configuration File 58, 61
Continuous tracing 147
Continuous Tracing 149, 151

D

Dashboard 36
Debugging 144
Debugging:Tools 144, 146
Default gateway address 168, 169
Deployment 12
DNS server 183
DNS:Forward IPs 185, 187
DNS:Server list 185, 187
DNS:Settings 185, 187
DNS:Zone 185, 187

F

File system 57
Firewall 207, 215

G

General 50

H

Hardware platforms 12

I

Interface 155, 156, 159, 162, 165
Interfaces and Protocols 12
Introduction 11
IP Security 221

L

License Server Location 231
License type:base license 101
License type:evaluation license 101
License type:OpenScape SBC Session license 101
License type:regular license 95
License type:SBC base license 101
License type:software subscription license 96, 97
License type:upgrade license 102
Licensing 12
List of jobs 64
Log files 47
Logging 138
Logging:Settings 140, 142

M

Management 12
Mark filters 173, 175
Media server:Adapter 261, 262
Menu 27

N

Navigation 27
Network services 156
Node 270
Node redundancy 266

NTP settings 178, 179, 181, 182

O

On demand trace 147, 153, 154
OpenScape Branch Assistant 69

P

Packet shaping 172
Password 34, 232, 234
Password management 67
Port forwarding 207
Port fowarding 219
Port mapping 241, 242

Q

QoS 264

R

Redundancy 12
Registered subscribers 52, 53, 55, 241
Remote Endpoint 243, 247, 254
Remote Subscribers 274, 274, 277
Restart 49
Routing 156, 170, 171
Routing rules 237
Rule filters 173, 175

S

Schedule 64, 65, 66
Schedules 64
Security 12, 189
Serviceability 56
Services status 45
Shared secret files 190
Signaling Transport 12
Simplified Installation 68, 68, 70, 73, 74, 77, 79, 87, 89
SIP routing rules 237
SIP Service Provider Profiles 256
SIP settings 237
SNORT 205, 206
Software 62
Software acitvation 64
Software Information 43
Status 32
Subscribers 241
Survivability 226
System settings 230

T

Threshold 273, 280
Timer 273, 280
TLS settings 192, 194, 199, 200, 203, 204
Tracing 147, 149, 151, 153, 154
Traffic class 173, 175
Traffic shaping 172, 173, 175
Transport Layer Security 190
Trap destinations 122, 132, 133, 135, 136
Troubleshooting 89
Trusted addresses 266

U

Update 62
Update OSB status 32
Upgrade 62
Upgrade manager 64
Upgrade Manager 56

V

VLAN settings 162, 165
VoIP configuration 236
VRRP settings 228

W

White List 215

© 2025 Mitel Networks Corporation. All Rights Reserved. Mitel and the Mitel logo are trademark(s) of Mitel Networks Corporation. Unify and associated marks are trademarks of Unify Software and Solutions GmbH & Co. KG. All other trademarks herein are the property of their respective owners.