



A MITEL
PRODUCT
GUIDE

Unify OpenScape Branch

OpenScape Branch V10

Administration Guide

11/2024

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 2024, Mitel Networks Corporation

All rights reserved

Contents

1 OpenScape Branch Assistant – Introduction.....	18
1.1 About This Guide.....	18
1.2 OpenScape Branch — Overview.....	19
1.2.1 Models and Hardware Platforms.....	32
1.3 Navigation.....	34
2 OpenScape Branch Assistant – Primary Administration	37
2.1 Business Groups and Branch Offices.....	37
2.2 How to Create and Delete a Branch Office of the OpenScape Branch Type.....	38
2.3 How to Display a Branch Office Via OpenScape Branch Assistant.....	39
2.4 How to Edit an OpenScape Branch via OpenScape Branch Assistant	41
2.5 How to Update Branch Offices Status.....	42
2.6 How to Change the Password in the Local Assistant Database	44
3 OpenScape Branch Assistant – Maintenance.....	46
3.1 System Information and Monitoring.....	46
3.1.1 The OpenScape Branch Dashboard via CMP.....	46
3.1.1.1 How to Display the OpenScape Branch Dashboard via CMP.....	49
3.1.1.2 How to Display Active Alarms	49
3.1.1.3 How to Display Alarm Details	51
3.1.1.4 How to Start Rapidstat to Perform a Health Check	52
3.1.1.5 How to Display Detailed Version Information	53
3.1.1.6 How to Display System Information for an OpenScape Branch Office	54
3.1.1.7 How to Display the Services Status of a V8 OpenScape Branch System	55
3.1.1.8 How to Display the Services Status of a V8 OpenScape Branch System	57
3.1.1.9 How to Display, Export and Clear Log Files for a V8 OSB	60
3.1.1.10 How to Display, Export and Clear Log Files for a V8 OSB	62
3.1.2 General System Information	64
3.1.2.1 How to Display a List of Registered Subscribers	67
3.1.2.2 How to Display the Backup Link Status	68
3.1.2.3 How to Perform PRI Channel Maintenance	70
3.2 Serviceability.....	73
3.2.1 OpenScape Branch File System	74
3.2.1.1 How to Restart the System.....	76
3.2.1.2 How to Load and Apply New Configuration Files.....	77
3.2.1.3 How to Select a Configuration File for Import.....	78
3.2.1.4 How to Export Configuration Files.....	79
3.2.2 Software Updates and Upgrades	81
3.2.2.1 How to Activate Software on a Particular OpenScape Branch Device via CMP.....	81
3.2.3 Job Management	82
3.2.3.1 How to View Batch Jobs.....	83
3.2.3.2 How to Create a New Batch Job.....	84
3.2.3.3 How to Edit or Cancel a Batch Job.....	85
3.2.4 Hardware Upgrades.....	86
3.3 Password Management	87
3.4 General Installation - Overview.....	88
3.4.1 OpenScape Branch Assistant - Configuration	90
3.4.1.1 How to Configure OpenScape Branch Assistant - General Settings.....	91
3.4.2 Simplified Installation Steps	92
3.4.2.1 How to Download Installation Files Into the CMP.....	95
3.4.2.2 How to Configure a Windows DHCP Server.....	97

3.4.2.3 How to Configure a LINUX DHCP Server.....	99
3.4.2.4 How to Configure a Cisco Router Utilizing the DHCP Server.....	101
3.4.2.5 How to Add an OpenScape Branch Office to OpenScape Voice.....	103
3.4.2.6 How to Configure the Software Load and Hardware Type.....	105
3.4.2.7 How to Add Media Server Language Files to the CMP Repository.....	106
3.4.2.8 How to Configure Media Server Language Files for an OpenScape Branch.....	107
3.4.2.9 How to Configure ACD Announcement Files.....	108
3.4.2.10 How to Configure ACD Music on Hold Files.....	109
3.4.2.11 How to Configure Auto Attendant Announcement Files.....	111
3.4.2.12 How to Configure the Data Configuration File.....	112
3.4.2.13 How to Configure the MAC Address.....	113
3.4.2.14 How to Install Hardware for Simplified Installation.....	114
3.4.2.15 How to Troubleshoot Installation Errors and Alarms.....	116
3.5 Storage of Phone Software Loads - Overview.....	119
3.5.1 How to Configure Phone Software Storage in the OpenScape Branch	120
3.6 OpenScape Branch and OpenScape SBC Licensing Files.....	123
3.6.1 OpenScape Regular License File (OSB and SBC).....	124
3.6.2 OpenScape Software Subscription License File (OSB and SBC).....	125
3.6.2.1 OpenScape Software Subscription License (SSL) Monitoring and Reporting - Details (OSB and SBC).....	127
3.6.3 OpenScape Evaluation License File (OSB and SBC).....	131
3.6.4 OpenScape Branch Base License Type (OSB only).....	132
3.6.5 OpenScape Branch Registered Line License Type (OSB only).....	132
3.6.6 OpenScape Branch Auto Attendant License (OSB only).....	134
3.6.7 OpenScape Branch Backup ACD (Automatic Call Distribution) License (OSB only).....	134
3.6.8 OpenScape Session Border Controller (SBC) Base License (SBC only).....	134
3.6.9 OpenScape SBC Session License (OSB and SBC).....	135
3.6.10 Upgrade License - Overview.....	135
3.7 Managing Licenses	136
3.7.1 License Management Concept	137
3.7.2 License Information	138
3.7.2.1 How to Display License Information via CMP.....	139
3.7.2.2 How to Display Software Subscription License Information via CMP.....	140
3.7.2.3 How to Display License Locking IDs via CMP.....	142
3.7.2.4 How to Display License Information via OpenScape Branch Assistant.....	142
3.7.2.5 How to Display and Manage Licensing Thresholds via OpenScape Branch Assistant	144
3.7.2.6 How to Display Licensing for an OpenScape Branch Office or SBC Via OpenScape Branch Assistant.....	144
3.7.2.7 How to Configure and Clear Licensing for an OpenScape Branch Office (or SBC Via SBC Assistant).....	147
3.7.2.8 How to Display Licensing Warnings for an OpenScape Branch Office or SBC.....	150
3.7.3 Activating Licenses	151
3.7.3.1 How to Activate License - Online.....	152
3.7.3.2 How to Activate License - Offline.....	153
3.7.4 License Enforcement and Update	154
3.7.5 License Security	157
4 OpenScape Branch Assistant – Configuration.....	158
4.1 Alarm Configuration Overview.....	158
4.1.1 Alarm Settings	158
4.1.1.1 How to Display Alarm Settings.....	159
4.1.1.2 How to Edit Alarm Settings.....	162
4.1.1.3 How to Edit and Add Trap Destinations.....	164
4.1.1.4 How to Display and Delete Trap Destinations.....	165
4.2 Logging Configuration Overview	166
4.2.1 Logging.....	167

4.2.1.1 How to Edit Settings for Logs.....	170
4.2.2 Debugging.....	172
4.2.2.1 How to Use Debugging Tools.....	173
4.2.3 Continuous Tracing and On Demand Trace.....	174
4.2.3.1 How to Configure Continuous Tracing.....	177
4.2.3.2 How to Start, Stop and Configure On Demand Tracing.....	178
4.3 Media Server Configuration — Overview.....	180
4.3.1 Media Server for OpenScape Branch	180
4.3.1.1 How to Enable the Media Server.....	182
4.3.1.2 How to Configure Connectivity Settings of the Media Server.....	183
4.3.1.3 How to Configure the Conference Settings.....	184
4.3.1.4 How to Configure Announcement Settings.....	185
4.3.1.5 How to Configure the Media Server Adapter.....	187
4.3.1.6 How to Configure the Media Server Converter.....	188
4.3.1.7 How to Assign a Language File.....	188
4.4 Network Services — Overview	189
4.4.1 How to Configure the Interfaces.....	191
4.4.2 How to Configure the Default Gateway Address.....	193
4.4.3 How to Add, Edit or Delete a Route.....	194
4.4.4 How to Configure, Enable and Disable Redundancy.....	196
4.4.5 Traffic Shaping	199
4.4.5.1 How to Configure Traffic Shaping.....	199
4.4.6 How to Configure System NTP Settings.....	202
4.4.7 How to Synchronize Manually with the NTP Server.....	203
4.4.8 Configuration of DNS Server	204
4.4.8.1 How to Configure System DNS Settings	206
4.4.9 Configuration of DHCP	209
4.4.9.1 How to Configure DHCP Settings	210
4.5 Security Configuration — Overview	214
4.5.1 TLS Certificates and Shared Secret Files	215
4.5.1.1 How to Manage TLS Certificates.....	217
4.5.1.2 How to Create, Edit and Delete Certificate Profiles	219
4.5.1.3 How to Configure Certificate Expiration Checking.....	223
4.5.1.4 How to Display and Configure the Certificate Revocation List (CRL)	225
4.5.1.5 How to Select a Shared Secret File for Use.....	228
4.5.1.6 How to Create Shared Secret Files.....	229
4.5.2 SSH with Public Key Infrastructure (PKI) Configuration - Overview	230
4.5.2.1 How to Configure PKI Capability	231
4.5.3 Network Intrusion Detection and Prevention (Message Rate Control).....	233
4.5.3.1 How to Configure Message Rate Control Rules.....	234
4.5.4 Firewall Configuration	235
4.5.4.1 How to Configure the Firewall.....	236
4.5.4.2 How to Configure Port Forwarding.....	238
4.5.5 Configuration of IP Security	240
4.5.5.1 How to Configure the IP Security Settings.....	241
4.5.6 RADIUS Support - Overview.....	243
4.5.6.1 How to Configure Radius.....	243
4.6 Survivability — Overview.....	246
4.6.1 How to Configure Multiline Hunt Groups for Survivability.....	250
4.6.2 How to Configure Emergency Calling for Survivability.....	252
4.6.3 How to Configure CDR Handling for Survivability	258
4.6.4 How to Configure Music on Hold Handling for Survivability.....	260
4.7 System Settings — Overview	261
4.7.1 How to Display and Change License Server Location.....	263
4.7.2 How to Change or Reset Passwords.....	264
4.7.3 How to Import/Export and Select Configuration Files via OpenScape Branch Assistant.....	266

4.7.4 How to access & apply Delta XML to an OSB via OpenScope Branch Assistant.....	268
4.8 Voice over Internet Protocol Configuration — Overview	269
4.8.1 Country Configuration - Overview.....	272
4.8.1.1 How to Display Country Configuration Information.....	272
4.8.1.2 How to Configure Country Specific Information.....	274
4.8.2 Branch Deployment Modes.....	275
4.8.2.1 How to Set the Deployment Mode.....	279
4.8.3 SIP Header Manipulation	281
4.8.3.1 How to Configure the SIP Header Manipulation Rules.....	283
4.8.4 Office Code Mapping - Overview	285
4.8.4.1 How to Configure Office Code Mapping.....	289
4.8.5 SIP Routing Rules	293
4.8.5.1 How to Configure SIP Routing Rules.....	295
4.8.5.2 How to Configure SIP Error Codes.....	297
4.8.5.3 How to Configure VoIP SIP Settings.....	298
4.8.5.4 How to Display Registered Subscribers Port Mapping Settings.....	300
4.8.6 Call Forwarding in Survivable Mode.....	301
4.8.6.1 How to Configure Call Forwarding for Survivable Mode	301
4.8.7 Configuration of Backup Data Channel	304
4.8.7.1 How to Configure OSB as Backup Link Client.....	310
4.8.7.2 How to Configure OSB as Backup Link Server.....	313
4.8.8 Configuration of Gateways	315
4.8.8.1 How to Configure Gateways.....	318
4.8.8.2 How to Configure SIP Service Provider Profiles	322
4.8.9 Quality of Service Configuration	331
4.8.9.1 How to Configure VoIP QoS Rules.....	331
4.8.10 Endpoint Service Profiles Configuration	333
4.8.10.1 How to Configure Endpoint Service Profiles.....	333
4.8.11 Communication System Settings.....	336
4.8.11.1 How to Configure the Communication System.....	337
4.9 How to Configure Timers and Thresholds.....	340
4.10 How to Configure the VoIP Codec Priority List.....	342
4.11 How to Configure RTP Settings.....	343
4.12 How to Configure Signaling and Transport Settings.....	344
4.13 Automatic Call Distribution — Overview.....	346
4.13.1 Automatic Call Distribution and Survivability.....	348
4.13.2 Automatic Call Distribution Configuration	352
4.13.2.1 How to Configure General ACD Agent Settings.....	354
4.13.2.2 How to Show the Status of ACD Agents.....	357
4.13.2.3 How to Display the ACD Log Files.....	358
4.13.2.4 How to Add, Edit, Delete Queues for ACD.....	359
4.13.2.5 How to Display Agents Assigned to a Queue for ACD.....	362
4.13.2.6 How to Add, Edit, Delete Profiles for ACD.....	363
4.13.2.7 How to Add, Edit, Delete Agents for ACD.....	365
4.14 OpenScope Voice Call Recording Solution Based on SIPREC — Overview.....	366
4.15 Integrated Gateways — Overview	368
4.15.1 How to Configure General Settings for an Integrated Gateway	370
4.15.2 How to Configure QoS Monitoring for an Integrated Gateway.....	371
4.15.3 How to Configure Media for an Integrated Gateway.....	372
4.15.4 How to Configure Codecs for an Integrated Gateway.....	374
4.15.5 How to Configure the FXS Card of an Integrated Gateway	375
4.15.6 How to Configure the FXO Card of an Integrated Gateway.....	380
4.15.7 How to Configure the BRI/S0 Card of an Integrated Gateway.....	382
4.15.8 How to Configure the T1 PRI Card/E1 PRI Card of an Integrated Gateway for OpenScope Branch 50i.....	387

4.15.9 How to Configure the T1 PRI Card/E1 PRI Card of an Integrated Gateway for OpenScape Branch 500i.....	396
4.15.9.1 How to Configure Clock Source for T1 PRI Card/E1 PRI Card.....	406
4.15.10 How to Configure Trunk Groups for the OpenScape Branch 50i	408
4.15.11 How to Configure Trunk Groups for the OpenScape Branch 500i	413
4.15.12 Configuration in OSV V8 when configuring MTLS in OSB V9	418
4.16 Auto Attendant — Overview	419
4.16.1 How to Configure Basic Auto Attendant Settings.....	422
4.16.2 How to Configure Announcements for Auto Attendant.....	423
4.16.3 How to Configure Routing for Auto Attendant.....	424
4.16.4 How to Configure Auto Attendant Menus.....	426
5 OpenScape Branch Assistant – Profile Configuration.....	430
5.1 Profiles Configuration - Overview.....	430
5.1.1 Branch Deployment Modes	430
5.1.1.1 How to Edit, Clone and Add Profiles	435
5.1.1.2 How to Display and Delete Profiles.....	436
5.1.1.3 How to Assign a Profile to an OpenScape Branch.....	437
5.2 Alarm Profile Configuration - Overview.....	438
5.2.1 Alarm Settings	438
5.2.1.1 How to Edit and Add Profile Trap Destinations.....	439
5.2.1.2 How to Display and Delete Profile Trap Destinations.....	440
5.3 Logging Profile Configuration - Overview	441
5.3.1 Logging Profile for OpenScape Branch.....	441
5.3.1.1 How to Edit Settings for Logs Associated with a Profile.....	444
5.3.2 Profiles with Continuous Tracing.....	446
5.3.2.1 How to Configure a Profile for Continuous Tracing.....	448
5.4 Media Server Profile Configuration - Overview.....	449
5.4.1 How to Configure a Profile for Media Server	449
5.5 Network Services Profile Configuration - Overview	450
5.5.1 How to Configure System NTP Profile Settings.....	451
5.5.2 Profile Configuration of DNS Server	452
5.5.2.1 How to Configure a Profile for System DNS Settings.....	453
5.6 Security Profile Configuration - Overview	455
5.6.1 Network Intrusion Detection and Prevention (Message Rate Control).....	456
5.6.1.1 How to Configure a Profile for Message Rate Control Rules.....	456
5.6.2 Firewall Profile Configuration	457
5.6.2.1 How to Configure a Profile for a Firewall.....	458
5.6.3 Radius.....	460
5.6.3.1 How to Enable RADIUS User Authentication.....	460
5.6.4 Custom.....	461
5.6.4.1 How to Configure Custom Security Settings.....	461
5.7 Survivability Profile Configuration - Overview	462
5.7.1 How to Configure Profiles for CDR Handling in Survivability.....	463
5.7.2 How to Configure Profiles for Music on Hold Handling in Survivability.....	464
5.8 System Profile Settings - Overview	465
5.9 Voice over Internet Protocol Profile Configuration - Overview	465
5.9.1 SIP Header Manipulation	466
5.9.1.1 How to Configure Profile SIP Header Manipulation Rules.....	468
5.9.2 SIP Routing Rules	469
5.9.2.1 How to Configure Profile SIP Routing Rules.....	472
5.9.2.2 How to View and Configure Profile SIP Error Codes.....	473
5.9.3 SIP VoIP Port Profile Configuration and Display	474
5.9.3.1 How to Configure Profile VoIP SIP Settings.....	475
5.9.4 Gateways Profile Configuration and Display	476
5.9.4.1 How to Configure a Profile with Gateway General Settings.....	476

5.9.4.2 How to Configure a Profile with Gateway SIP Service Provider Profiles.....	477
5.9.5 Quality of Service Profile Configuration	482
5.9.5.1 How to Configure a Profile with VoIP QoS Rules.....	482
5.9.6 How to Configure a Profile for Timers and Thresholds.....	483
6 OpenScape Branch - Local Management.....	485
6.1 Dashboard.....	485
6.1.1 Dashboard > Alarm Details.....	487
6.1.2 Dashboard > Services Status.....	488
6.1.3 Dashboard > Link Status.....	490
6.1.3.1 Dashboard > Link Status > Channel Maintenance.....	491
6.1.4 Dashboard > Backup Link Status.....	492
6.1.4.1 Dashboard > Backup Link Status Target Statistics.....	493
6.1.4.2 Dashboard > Backup Link Status PPP Connection Statistics.....	493
6.1.4.3 Dashboard > Backup Link Status IP Statistics.....	494
6.1.4.4 Dashboard > Backup Link Status RTP Statistics.....	495
6.1.5 Dashboard > Registered Subscribers.....	496
6.1.6 Dashboard > Dynamic Port Mapping.....	496
6.1.7 Dashboard > Subscriber Data.....	497
6.1.8 Dashboard > Denial of Service Mitigation.....	497
6.1.9 Dashboard > Software Info.....	497
6.2 System.....	498
6.2.1 System > Settings.....	498
6.2.1.1 System > Settings > Country Configuration Viewer.....	500
6.2.2 System > Licenses.....	500
6.2.3 System > Branding > Branding Settings.....	502
6.3 Network/Net Services.....	503
6.3.1 Network/Net Services > Settings.....	503
6.3.2 Network/Net Services > DNS.....	509
6.3.2.1 Network/Net Services > DNS Configuration.....	509
6.3.2.2 Network/Net Services > DNS > Administer Custom Files.....	510
6.3.3 Network/Net Services > NTP > NTP Settings.....	511
6.3.4 Network/Net Services > DHCP > General.....	512
6.3.4.1 Network/Net Services > DHCP > Administer Custom Files.....	513
6.3.4.2 Network/Net Services > DHCP > Static IP Addresses.....	514
6.3.5 Network/Net Services > Traffic Shaping.....	514
6.3.6 Network/Net Services > QoS Settings.....	515
6.4 VoIP.....	517
6.4.1 VoIP > SIP Server Settings.....	517
6.4.1.1 VoIP > SIP Server Settings > Other Trusted Servers.....	521
6.4.1.2 VoIP > SIP Server Settings > Load Balance Mapping Table.....	521
6.4.2 VoIP > Port and Signaling Settings.....	522
6.4.3 VoIP > Manipulation and Routing.....	525
6.4.4 VoIP > Error Codes.....	529
6.4.5 VoIP > Media.....	530
6.4.5.1 VoIP > Media > Media Profile.....	534
6.5 Features.....	537
6.5.1 Features > Gateways/Trunks Provisioning.....	540
6.5.2 Features > Integrated Gateway.....	547
6.5.2.1 Features > Integrated Gateway > BRI Configuration.....	548
6.5.2.2 Features > Integrated Gateway > FXO Configuration.....	551
6.5.2.3 Features > Integrated Gateway > FXS Configuration.....	554
6.5.2.4 Features > Integrated Gateway > FXS Configuration > Endpoint Service Profiles.....	556
6.5.2.5 Features > Integrated Gateway > PRI Configuration.....	557
6.5.2.6 Features > Integrated Gateway > PRI Configuration > PRI Interface > CAS Profiles.....	558

6.5.2.7 Features > Integrated Gateway > PRI Configuration > PRI Interface > CAS Advanced Settings.....	559
6.5.2.8 Features > Integrated Gateway > PRI Configuration > PRI Interface.....	560
6.5.2.9 Features > Integrated Gateway > Trunk Group Configuration.....	566
6.5.2.10 Features > Integrated Gateway > Trunk Group Configuration > General.....	566
6.5.2.11 Features > Integrated Gateway > Trunk Group Configuration > Channels List.....	570
6.5.2.12 Features > Integrated Gateway > Trunk Group Configuration > Network Specific Facilities (T1 only).....	570
6.5.2.13 Features > Integrated Gateway > Trunk Group Configuration > Number Modification.....	571
6.5.2.14 Features > Integrated Gateway > QoS Monitoring.....	578
6.5.2.15 Features > Integrated Gateway > Local Toll Table Configuration.....	578
6.5.2.16 Features > Integrated Gateway > Local Toll Tables Configuration > Upload Local Toll Table.....	579
6.5.3 Features > SIP Service Provider Configuration.....	580
6.5.3.1 Features > SIP Service Providers Profiles.....	593
6.5.4 Features > Auto Attendant.....	594
6.5.4.1 Features > Auto Attendant Menu.....	597
6.5.5 Features > Voice Mail Service.....	598
6.5.6 Features > Phone Software Management.....	600
6.5.7 Features > Media Server/Streaming.....	601
6.5.7.1 Features > Media Server Advanced Configuration.....	603
6.5.8 Features > Backup Link Client Configuration.....	603
6.5.9 Features > Backup Link Server Configuration.....	605
6.5.10 Features > Multi Line Hunt Groups.....	606
6.5.11 Features > Automatic Call Distribution (ACD).....	608
6.5.11.1 Features > ACD > Queues.....	611
6.5.11.2 Features > ACD > Agents.....	614
6.5.12 Features > Emergency Calling.....	615
6.5.12.1 Features > Emergency Call Routing.....	616
6.5.13 Features > Call Forwarding.....	619
6.5.14 Features > Call Detail Records.....	620
6.6 Security.....	621
6.6.1 Security > General.....	621
6.6.1.1 Security > General > Shared Secret Files.....	622
6.6.1.2 Security > General > Certificate Management.....	623
6.6.1.3 Security > General > Certificate Management > Certificate Profile.....	625
6.6.1.4 Security > General > Certificate Management > CRL Viewer.....	627
6.6.1.5 Administrator Account.....	627
6.6.1.6 Security > General > PKI Configuration.....	628
6.6.2 Security > Firewall Overview.....	629
6.6.2.1 Security > Firewall > Firewall Configuration.....	629
6.6.3 Security > Message Rate Control.....	631
6.6.4 Security > RADIUS.....	632
6.6.5 Security > Tunnel Connections.....	632
6.6.6 Security > Denial of Service Mitigation.....	634
6.7 Diagnostics and Logs.....	635
6.7.1 Diagnostics and Logs > Logs.....	635
6.7.2 Diagnostics and Logs > Debugging.....	639
6.7.3 Diagnostics and Logs > Trace.....	640
6.7.4 Diagnostics and Logs > Statistics.....	641
6.8 Alarms.....	642
6.8.1 Alarms > Alarm Settings.....	642
6.8.2 Alarms > SNMP Configuration.....	643
6.9 Maintenance.....	646
6.9.1 Maintenance > Import/Export.....	646
6.9.2 Maintenance > Install/Upgrade.....	649
6.9.3 Maintenance > Bulk Configuration (Delta XML).....	650

6.9.4 Maintenance > Restart.....	653
6.9.5 Scheduled Maintenance.....	653
7 OpenScape Branch CDR Overview.....	655
7.1 OSB CDR File Structure.....	655
7.2 OSB CDR Record Structure.....	656
7.3 OSB CDR Field Structure.....	658
8 Appendix - Overview.....	661
8.1 Alarm Information - Overview.....	661
8.1.1 Concept of the Alarms and Fault Messages.....	661
8.1.2 Alarm Information.....	661
8.1.3 Alarm Severities.....	662
8.1.4 Alarm Type.....	663
8.1.5 Alarm Groups.....	663
8.1.5.1 Alarm Group: Admin.....	663
8.1.5.2 Alarm Group: Communication.....	663
8.1.5.3 Alarm Group: Ethernet.....	664
8.1.5.4 Alarm Group: Hardware.....	664
8.1.5.5 Alarm Group: License.....	664
8.1.5.6 Alarm Group: Resource.....	664
8.1.5.7 Alarm Group: Software.....	664
8.1.5.8 Alarm Group: Usage.....	665
8.1.6 Alarm List.....	665
8.1.6.1 +1.5V high voltage.....	665
8.1.6.2 +1.5V low voltage.....	665
8.1.6.3 +3.3V high voltage.....	665
8.1.6.4 +3.3V low voltage.....	666
8.1.6.5 +5V high voltage.....	666
8.1.6.6 +5V low voltage.....	666
8.1.6.7 +12V high voltage.....	666
8.1.6.8 +12V low voltage.....	667
8.1.6.9 Apache/PHP not running.....	667
8.1.6.10 B2BUA not running.....	667
8.1.6.11 Bandwidth ethernet port 1.....	668
8.1.6.12 Bandwidth ethernet port 2.....	668
8.1.6.13 Bandwidth ethernet port 3.....	668
8.1.6.14 Bandwidth ethernet port 4.....	669
8.1.6.15 BLC not running.....	669
8.1.6.16 BLS not running.....	669
8.1.6.17 Snort not running.....	670
8.1.6.18 IPsec not running.....	670
8.1.6.19 Unsupported Hardware Platform.....	670
8.1.6.20 Branch is operating in Backup Link Mode.....	671
8.1.6.21 Card 1 failure.....	671
8.1.6.22 Card 1 port 1 failure.....	671
8.1.6.23 Card 1 port 2 failure.....	672
8.1.6.24 Card 1 port 3 failure.....	672
8.1.6.25 Card 1 port 4 failure.....	672
8.1.6.26 Card 1 port 5 failure.....	672
8.1.6.27 Card 1 port 6 failure.....	673
8.1.6.28 Card 1 port 7 failure.....	673
8.1.6.29 Card 1 port 8 failure.....	673
8.1.6.30 Card 1 port 9 failure.....	673
8.1.6.31 Card 1 port 10 failure.....	674
8.1.6.32 Card 1 port 11 failure.....	674

8.1.6.33 Card 1 port 12 failure.....	674
8.1.6.34 Card 1 port 13 failure.....	674
8.1.6.35 Card 1 port 14 failure.....	675
8.1.6.36 Card 1 port 15 failure.....	675
8.1.6.37 Card 1 port 16 failure.....	675
8.1.6.38 Card 1 port 17 failure.....	676
8.1.6.39 Card 1 port 18 failure.....	676
8.1.6.40 Card 1 port 19 failure.....	676
8.1.6.41 Card 1 port 20 failure.....	676
8.1.6.42 Card 1 port 21 failure.....	677
8.1.6.43 Card 1 port 22 failure.....	677
8.1.6.44 Card 1 port 23 failure.....	677
8.1.6.45 Card 1 port 24 failure.....	677
8.1.6.46 Card 1 port 1 recovering.....	678
8.1.6.47 Card 1 port 2 recovering.....	678
8.1.6.48 Card 1 port 3 recovering.....	678
8.1.6.49 Card 1 port 4 recovering.....	678
8.1.6.50 Card 1 port 5 recovering.....	679
8.1.6.51 Card 1 port 6 recovering.....	679
8.1.6.52 Card 1 port 7 recovering.....	679
8.1.6.53 Card 1 port 8 recovering.....	680
8.1.6.54 Card 2 failure.....	680
8.1.6.55 Card 2 port 1 failure.....	680
8.1.6.56 Card 2 port 2 failure.....	680
8.1.6.57 Card 2 port 3 failure.....	681
8.1.6.58 Card 2 port 4 failure.....	681
8.1.6.59 Card 2 port 5 failure.....	681
8.1.6.60 Card 2 port 6 failure.....	681
8.1.6.61 Card 2 port 7 failure.....	682
8.1.6.62 Card 2 port 8 failure.....	682
8.1.6.63 Card 2 port 9 failure.....	682
8.1.6.64 Card 2 port 10 failure.....	682
8.1.6.65 Card 2 port 11 failure.....	683
8.1.6.66 Card 2 port 12 failure.....	683
8.1.6.67 Card 2 port 13 failure.....	683
8.1.6.68 Card 2 port 14 failure.....	684
8.1.6.69 Card 2 port 15 failure.....	684
8.1.6.70 Card 2 port 16 failure.....	684
8.1.6.71 Card 2 port 17 failure.....	684
8.1.6.72 Card 2 port 18 failure.....	685
8.1.6.73 Card 2 port 19 failure.....	685
8.1.6.74 Card 2 port 20 failure.....	685
8.1.6.75 Card 2 port 21 failure.....	685
8.1.6.76 Card 2 port 22 failure.....	686
8.1.6.77 Card 2 port 23 failure.....	686
8.1.6.78 Card 2 port 24 failure.....	686
8.1.6.79 Card 2 port 1 recovering.....	686
8.1.6.80 Card 2 port 2 recovering.....	687
8.1.6.81 Card 2 port 3 recovering.....	687
8.1.6.82 Card 2 port 4 recovering.....	687
8.1.6.83 Card 2 port 5 recovering.....	688
8.1.6.84 Card 2 port 6 recovering.....	688
8.1.6.85 Card 2 port 7 recovering.....	688
8.1.6.86 Card 2 port 8 recovering.....	688
8.1.6.87 D-channel down on Card 1 port 1.....	689
8.1.6.88 D-channel down on Card 1 port 2.....	689

8.1.6.89 D-channel down on Card 1 port 3.....	689
8.1.6.90 D-channel down on Card 1 port 4.....	690
8.1.6.91 D-channel down on Card 2 port 1.....	690
8.1.6.92 D-channel down on Card 2 port 2.....	690
8.1.6.93 D-channel down on Card 2 port 3.....	691
8.1.6.94 D-channel down on Card 2 port 4.....	691
8.1.6.95 CDR disk space running low.....	691
8.1.6.96 CDRHandler not running.....	692
8.1.6.97 Certificate Authority Could Not Be Validated.....	692
8.1.6.98 Certificate Contains an Unknown Critical Extension.....	692
8.1.6.99 Certificate Has Been Revoked.....	693
8.1.6.100 Certificate is Expired.....	693
8.1.6.101 Certificate is Out of the Validity Period.....	693
8.1.6.102 Certificate Subject Could Not Be Authenticated.....	694
8.1.6.103 Certificate Will Expire in the Next Days.....	694
8.1.6.104 CRL Fails Because the Signature on the CRL is Invalid.....	694
8.1.6.105 Subscriber synchronization failure.....	695
8.1.6.106 Event Name Wrong Digest Authentication exchange key.....	695
8.1.6.107 CPU Vcore HT high voltage.....	695
8.1.6.108 CPU Vcore HT low voltage.....	696
8.1.6.109 CPU VDD HT high voltage.....	696
8.1.6.110 CPU VDD HT low voltage.....	696
8.1.6.111 CPU VLDT HT 1.2V high voltage.....	696
8.1.6.112 CPU VLDT HT 1.2V low voltage.....	697
8.1.6.113 CPU1 +1.8V high voltage.....	697
8.1.6.114 CPU1 +1.8V low voltage.....	697
8.1.6.115 CPU1 +2.5V high voltage.....	697
8.1.6.116 CPU1 +2.5V low voltage.....	698
8.1.6.117 CPU1 VRM CPU1 high voltage.....	698
8.1.6.118 CPU1 VRM CPU1 low voltage.....	698
8.1.6.119 CPU1 Vtt high voltage.....	698
8.1.6.120 CPU1 Vtt low voltage.....	699
8.1.6.121 CPU2 +1.8V high voltage.....	699
8.1.6.122 CPU2 +1.8V low voltage.....	699
8.1.6.123 CPU2 +2.5V high voltage.....	700
8.1.6.124 CPU2 +2.5V low voltage.....	700
8.1.6.125 CPU2 Vtt high voltage.....	700
8.1.6.126 CPU2 Vtt low voltage.....	700
8.1.6.127 CPU2 VRM CPU2 high voltage.....	701
8.1.6.128 CPU2 VRM CPU2 low voltage.....	701
8.1.6.129 Critical failure on SIP Server configuration.....	701
8.1.6.130 Critical failure on SIP Server core.....	701
8.1.6.131 CRL Could Not Be Copied From the Partner Node.....	702
8.1.6.132 CRL Could Not Be Downloaded.....	702
8.1.6.133 CRL is Expired.....	702
8.1.6.134 CRL is Invalid.....	703
8.1.6.135 Database restored.....	703
8.1.6.136 DHCP Server not running.....	703
8.1.6.137 Disk space running low.....	704
8.1.6.138 Error writing a CDR billing file.....	704
8.1.6.139 Extremely high CPU usage.....	704
8.1.6.140 Failed to add Backup Link channel.....	705
8.1.6.141 Failed to establish the minimum Backup Link bandwidth.....	705
8.1.6.142 Failed to establish the required Backup Link bandwidth.....	705
8.1.6.143 Failed update or upgrade.....	706
8.1.6.144 Failure to mirror phone images due to backup link mode.....	706

8.1.6.145 Failure to mirror phone images due to less than 25Mb available.....	706
8.1.6.146 Failure to mirror phone images due to survivable mode.....	707
8.1.6.147 Far End Alarm on Card 1 port 1: AIS signal received.....	707
8.1.6.148 Far End Alarm on Card 1 port 2: AIS signal received.....	707
8.1.6.149 Far End Alarm on Card 1 port 3: AIS signal received.....	708
8.1.6.150 Far End Alarm on Card 1 port 4: AIS signal received.....	708
8.1.6.151 Far End Alarm on Card 1 port 5: AIS signal received.....	708
8.1.6.152 Far End Alarm on Card 1 port 6: AIS signal received.....	709
8.1.6.153 Far End Alarm on Card 1 port 7: AIS signal received.....	709
8.1.6.154 Far End Alarm on Card 1 port 8: AIS signal received.....	709
8.1.6.155 Far End Alarm on Card 1 port 1: RAI signal received.....	710
8.1.6.156 Far End Alarm on Card 1 port 2: RAI signal received.....	710
8.1.6.157 Far End Alarm on Card 1 port 3: RAI signal received.....	710
8.1.6.158 Far End Alarm on Card 1 port 4: RAI signal received.....	711
8.1.6.159 Far End Alarm on Card 1 port 5: RAI signal received.....	711
8.1.6.160 Far End Alarm on Card 1 port 6: RAI signal received.....	712
8.1.6.161 Far End Alarm on Card 1 port 7: RAI signal received.....	712
8.1.6.162 Far End Alarm on Card 1 port 8: RAI signal received.....	712
8.1.6.163 Far End Alarm on Card 2 port 1: AIS signal received.....	713
8.1.6.164 Far End Alarm on Card 2 port 2: AIS signal received.....	713
8.1.6.165 Far End Alarm on Card 2 port 3: AIS signal received.....	713
8.1.6.166 Far End Alarm on Card 2 port 4: AIS signal received.....	714
8.1.6.167 Far End Alarm on Card 2 port 5: AIS signal received.....	714
8.1.6.168 Far End Alarm on Card 2 port 6: AIS signal received.....	714
8.1.6.169 Far End Alarm on Card 2 port 7: AIS signal received.....	715
8.1.6.170 Far End Alarm on Card 2 port 8: AIS signal received.....	715
8.1.6.171 Far End Alarm on Card 2 port 1: RAI signal received.....	715
8.1.6.172 Far End Alarm on Card 2 port 2: RAI signal received.....	716
8.1.6.173 Far End Alarm on Card 2 port 3: RAI signal received.....	716
8.1.6.174 Far End Alarm on Card 2 port 4: RAI signal received.....	716
8.1.6.175 Far End Alarm on Card 2 port 5: RAI signal received.....	717
8.1.6.176 Far End Alarm on Card 2 port 6: RAI signal received.....	717
8.1.6.177 Far End Alarm on Card 2 port 7: RAI signal received.....	718
8.1.6.178 Far End Alarm on Card 2 port 8: RAI signal received.....	718
8.1.6.179 Far End Loopback Activated on Card 1 port 1.....	718
8.1.6.180 Far End Loopback Activated on Card 1 port 2.....	719
8.1.6.181 Far End Loopback Activated on Card 1 port 3.....	719
8.1.6.182 Far End Loopback Activated on Card 1 port 4.....	719
8.1.6.183 Far End Loopback Activated on Card 1 port 5.....	719
8.1.6.184 Far End Loopback Activated on Card 1 port 6.....	720
8.1.6.185 Far End Loopback Activated on Card 1 port 7.....	720
8.1.6.186 Far End Loopback Activated on Card 1 port 8.....	720
8.1.6.187 Far End Loopback Activated on Card 2 port 1.....	721
8.1.6.188 Far End Loopback Activated on Card 2 port 2.....	721
8.1.6.189 Far End Loopback Activated on Card 2 port 3.....	721
8.1.6.190 Far End Loopback Activated on Card 2 port 4.....	721
8.1.6.191 Far End Loopback Activated on Card 2 port 5.....	722
8.1.6.192 Far End Loopback Activated on Card 2 port 6.....	722
8.1.6.193 Far End Loopback Activated on Card 2 port 7.....	722
8.1.6.194 Far End Loopback Activated on Card 2 port 8.....	723
8.1.6.195 Feature blocked due to license.....	723
8.1.6.196 File I/O error.....	723
8.1.6.197 FXS Ring Voltage Lost on Card 1.....	723
8.1.6.198 FXS Ring Voltage Lost on Card 2.....	724
8.1.6.199 Generic error code.....	724
8.1.6.200 Geo-redundant data transfer to remote branch failed attempts.....	724

8.1.6.201 Geo-redundant data not received from remote branch.....	725
8.1.6.202 High ambient temperature.....	725
8.1.6.203 High CPU usage.....	725
8.1.6.204 High CPU temperature.....	726
8.1.6.205 High number of active voice channels.....	726
8.1.6.206 High RAM usage.....	726
8.1.6.207 High system board temperature.....	727
8.1.6.208 High temperature core 0.....	727
8.1.6.209 High temperature core 1.....	727
8.1.6.210 Install: ACD install failed.....	727
8.1.6.211 Install: Auto Attendant install failed.....	728
8.1.6.212 Install: Media Server install failed.....	728
8.1.6.213 IP blocked due to packet flood.....	728
8.1.6.214 License has expired.....	729
8.1.6.215 License HW-Id is already in use.....	729
8.1.6.216 Could not contact license server.....	729
8.1.6.217 License info wrong or non existent Logical-ID.....	730
8.1.6.218 License using temporary grace period.....	730
8.1.6.219 License violation detected.....	730
8.1.6.220 License will expire.....	731
8.1.6.221 License not configured in Server.....	731
8.1.6.222 Loss of Clock on Card 1 port 1.....	731
8.1.6.223 Loss of Clock on Card 1 port 2.....	732
8.1.6.224 Loss of Clock on Card 1 port 3.....	732
8.1.6.225 Loss of Clock on Card 1 port 4.....	732
8.1.6.226 Loss of Clock on Card 2 port 1.....	733
8.1.6.227 Loss of Clock on Card 2 port 2.....	733
8.1.6.228 Loss of Clock on Card 2 port 3.....	733
8.1.6.229 Loss of Clock on Card 2 port 4.....	733
8.1.6.230 Redundant system not reachable via alternate interface.....	734
8.1.6.231 Switchover due to PRI threshold.....	734
8.1.6.232 Loss of communication with another OSB in the branch.....	734
8.1.6.233 Loss of communication with billing server.....	735
8.1.6.234 Loss of communication with DNS server.....	735
8.1.6.235 Loss of communication with file server.....	735
8.1.6.236 Loss of communication with gateway.....	736
8.1.6.237 Loss of communication with Node 1 Backup OSV.....	736
8.1.6.238 Loss of communication with Node 1 Primary OSV.....	736
8.1.6.239 Loss of communication with Node2 Backup OSV.....	737
8.1.6.240 Loss of communication with Node2 Primary OSV.....	737
8.1.6.241 Loss of communication with NTP server.....	737
8.1.6.242 Loss of communication with Redundant System.....	738
8.1.6.243 Loss of communication with SIP Service Provider.....	738
8.1.6.244 Loss of communication with surveillance system.....	738
8.1.6.245 Loss of Signal on Card 1 port 1.....	738
8.1.6.246 Loss of Signal on Card 1 port 2.....	739
8.1.6.247 Loss of Signal on Card 1 port 3.....	739
8.1.6.248 Loss of Signal on Card 1 port 4.....	740
8.1.6.249 Loss of Signal on Card 1 port 5.....	740
8.1.6.250 Loss of Signal on Card 1 port 6.....	740
8.1.6.251 Loss of Signal on Card 1 port 7.....	741
8.1.6.252 Loss of Signal on Card 1 port 8.....	741
8.1.6.253 Loss of Signal on Card 2 port 1.....	741
8.1.6.254 Loss of Signal on Card 2 port 2.....	742
8.1.6.255 Loss of Signal on Card 2 port 3.....	742
8.1.6.256 Loss of Signal on Card 2 port 4.....	743

8.1.6.257 Loss of Signal on Card 2 port 5.....	743
8.1.6.258 Loss of Signal on Card 2 port 6.....	743
8.1.6.259 Loss of Signal on Card 2 port 7.....	744
8.1.6.260 Loss of Signal on Card 2 port 8.....	744
8.1.6.261 Low fan speed 1.....	744
8.1.6.262 Low fan speed 2.....	745
8.1.6.263 Low fan speed 3.....	745
8.1.6.264 Low fan speed 4.....	745
8.1.6.265 Low fan speed 5.....	745
8.1.6.266 Low fan speed 6.....	746
8.1.6.267 Low fan speed 7.....	746
8.1.6.268 Low fan speed 8.....	746
8.1.6.269 Low fan speed 9.....	747
8.1.6.270 Low fan speed 10.....	747
8.1.6.271 Low fan speed 11.....	747
8.1.6.272 Low fan speed 12.....	747
8.1.6.273 Low fan 1 speed PSU 1.....	748
8.1.6.274 Low fan 2 speed PSU 1.....	748
8.1.6.275 Low fan 1 speed PSU 2.....	748
8.1.6.276 Low fan 2 speed PSU 2.....	748
8.1.6.277 Low fan speed PSU 1(S7).....	749
8.1.6.278 Low fan speed PSU 2(S7).....	749
8.1.6.279 Low fan speed 1B.....	749
8.1.6.280 Low fan speed 2B.....	749
8.1.6.281 Low fan speed 3B.....	750
8.1.6.282 Low fan speed 4B.....	750
8.1.6.283 Low fan speed 5B.....	750
8.1.6.284 Low fan speed 6B.....	751
8.1.6.285 Media Server not running.....	751
8.1.6.286 msadapter not running.....	751
8.1.6.287 Near End Alarm on Card 1 port 1: LOF/LFA.....	752
8.1.6.288 Near End Alarm on Card 1 port 2: LOF/LFA.....	752
8.1.6.289 Near End Alarm on Card 1 port 3: LOF/LFA.....	752
8.1.6.290 Near End Alarm on Card 1 port 4: LOF/LFA.....	752
8.1.6.291 Near End Alarm on Card 1 port 5: LOF/LFA.....	753
8.1.6.292 Near End Alarm on Card 1 port 6: LOF/LFA.....	753
8.1.6.293 Near End Alarm on Card 1 port 7: LOF/LFA.....	753
8.1.6.294 Near End Alarm on Card 1 port 8: LOF/LFA.....	754
8.1.6.295 Near End Loopback activated on Card 1 port 1.....	754
8.1.6.296 Near End Loopback activated on Card 1 port 2.....	754
8.1.6.297 Near End Loopback activated on Card 1 port 3.....	754
8.1.6.298 Near End Loopback activated on Card 1 port 4.....	755
8.1.6.299 Near End Loopback activated on Card 1 port 5.....	755
8.1.6.300 Near End Loopback activated on Card 1 port 6.....	755
8.1.6.301 Near End Loopback activated on Card 1 port 7.....	756
8.1.6.302 Near End Loopback activated on Card 1 port 8.....	756
8.1.6.303 Near End Alarm on Card 2 port 1: LOF/LFA.....	756
8.1.6.304 Near End Alarm on Card 2 port 2: LOF/LFA.....	756
8.1.6.305 Near End Alarm on Card 2 port 3: LOF/LFA.....	757
8.1.6.306 Near End Alarm on Card 2 port 4: LOF/LFA.....	757
8.1.6.307 Near End Alarm on Card 2 port 5: LOF/LFA.....	757
8.1.6.308 Near End Alarm on Card 2 port 6: LOF/LFA.....	758
8.1.6.309 Near End Alarm on Card 2 port 7: LOF/LFA.....	758
8.1.6.310 Near End Alarm on Card 2 port 8: LOF/LFA.....	758
8.1.6.311 Near End Loopback activated on Card 2 port 1.....	758
8.1.6.312 Near End Loopback activated on Card 2 port 2.....	759

8.1.6.313 Near End Loopback activated on Card 2 port 3.....	759
8.1.6.314 Near End Loopback activated on Card 2 port 4.....	759
8.1.6.315 Near End Loopback activated on Card 2 port 5.....	760
8.1.6.316 Near End Loopback activated on Card 2 port 6.....	760
8.1.6.317 Near End Loopback activated on Card 2 port 7.....	760
8.1.6.318 Near End Loopback activated on Card 2 port 8.....	760
8.1.6.319 Network failure.....	761
8.1.6.320 Network not running.....	761
8.1.6.321 No Backup Link channel can be added at all.....	761
8.1.6.322 NTP not running.....	762
8.1.6.323 Parse error for instance when parsing command-line options the 'wgetrc' or 'netcr'.....	762
8.1.6.324 Phone image download denied due to connections number limit.....	762
8.1.6.325 Phone image download denied due to system load over 60 percent.....	763
8.1.6.326 Port 1 failure.....	763
8.1.6.327 Port 2 failure.....	763
8.1.6.328 Port 3 failure.....	764
8.1.6.329 Port 4 failure.....	764
8.1.6.330 Power Supply 1 Failure.....	764
8.1.6.331 Power Supply 2 Failure.....	764
8.1.6.332 Process Manager not running.....	765
8.1.6.333 Protocol errors.....	765
8.1.6.334 PSU 1 failure.....	765
8.1.6.335 PSU 2 failure.....	766
8.1.6.336 Reboot requested due to license violation.....	766
8.1.6.337 Redundant system has an invalid version (sync.is disabled).....	766
8.1.6.338 Redundant system has not a compatible HW (sync. is disabled).....	767
8.1.6.339 Redundant system synchronization fails.....	767
8.1.6.340 Rejected to add Backup Link channel.....	767
8.1.6.341 RTPProxy not running.....	768
8.1.6.342 SBC Session denied due to license.....	768
8.1.6.343 Server issued an error response.....	768
8.1.6.344 sipmgcpconv not running.....	769
8.1.6.345 SIP Server database not restored.....	769
8.1.6.346 SIP Server not running.....	769
8.1.6.347 SSL verification failure.....	770
8.1.6.348 ssdp not running.....	770
8.1.6.349 Standalone operation.....	770
8.1.6.350 SurvProcess not running.....	771
8.1.6.351 Syslog not running.....	771
8.1.6.352 Username/password authentication failure.....	771
8.1.6.353 User registration blocked due to license.....	772
8.1.6.354 VBAT high voltage.....	772
8.1.6.355 VBAT low voltage.....	772
8.1.6.356 Very high CPU usage.....	772
8.1.6.357 VRRPD not running.....	773
8.1.6.358 Wrong user ID or password entered.....	773
8.2 Replacing OSB Voice Prompts.....	773
8.2.1 Language Files.....	774
8.2.2 Directory Structure.....	774
8.2.3 General Purpose Voice Prompts.....	774
8.2.4 ACD Announcements.....	775
8.2.5 Auto Attendant Announcements.....	776
8.2.6 VoiceMail Announcements.....	776
8.2.7 Replacing Files.....	777
8.2.8 V9 Backup/Restore Custom Files.....	777

Index..... 779

1 OpenScape Branch Assistant – Introduction

The OpenScape Branch Assistant is a network management software product that provides the configuration and administration of one or more branch offices running on OpenScape Branch hardware.

The OpenScape Branch Assistant is realized as a software plugin within the OpenScape Voice Assistant.

1.1 About This Guide

This guide describes how to use the OpenScape Branch Assistant to manage and configure one or more branch offices of the OpenScape Branch type. It provides instructions on how to display and enter configuration parameters in the OpenScape Branch Assistant screens, as well as descriptions of the configuration parameters.

Intended Audience

What You Need to Know

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

A working knowledge of computers and client-server network architectures is necessary for executing tasks using the OpenScape Branch Assistant. In addition, you should be familiar with basic telecommunications equipment functionality and have obtained proper login permissions to use the OpenScape Branch Assistant.

OpenScape Branch Assistant Online Help

The OpenScape Branch Assistant can be used to display and configure branch offices of the OpenScape Branch V1R3, V1R4, V2, V7,V8 and V9 types. Therefore, if an OpenScape Branch V1R3, V1R4 or V2 system is selected, some sections may describe features that are not available for V1R3, V1R4, V2 or V7 systems and some procedures may deviate from the ones described.

NOTICE:

The V8 GUI has been refactored. As a consequence the presentation of the GUI appears different for a V8 OpenScape Branch than when configuring OpenScape Branches of earlier versions. This is most evident in the Navigation Tree items. As a consequence many administrative tasks for V8 OSBs must be performed via different navigation paths, menus, and buttons. Details are pointed out where differences exist between V8 functions and pre-V8 functions.

OpenScape SBC Assistant Administration

In earlier versions this product was managed from the OpenScape Branch Assistant. As part of the V8 GUI refactoring initiative, a new SBC Assistant has been introduced as can be seen to the immediate right of the OpenScape

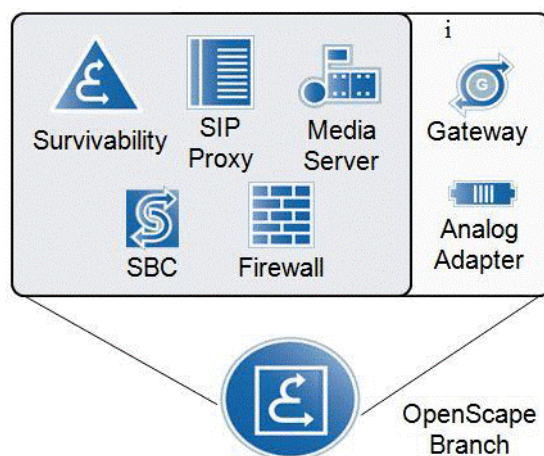
Branch Assistant on the GUI. As a consequence of the refactoring, the SBCs are no longer managed via the OpenScape Branch Assistant, but by the new SBC Assistant.

1.2 OpenScape Branch — Overview

The OpenScape Branch appliance operates in several deployment modes and runs on different hardware platforms depending on the number of users. OpenScape Branch Assistant is a tool to manage functions specific to the OpenScape Branch platform.

Functional Overview

The OpenScape Branch is a Unify developed SIP based Voice over IP appliance that empowers the remote branch offices on an OpenScape Voice network by leveraging the benefits of an open architecture VoIP enterprise environment. The main objective of the OpenScape Branch is to assure continued communications services to the branch with a rich feature set of survivability capabilities at the remote branch location during the loss or degradation of service between the remote branch and the main office.



In addition to survivability, all OpenScape Branch models include Proxy, Media Server, Branch Session Border Controller (SBC), and Branch SIP Trunking functionality. The OpenScape Branch 500i available in V1 R3 and later also provides the additional functionality of integrated Analog Adapter and PSTN Gateway (GW). All of these functions that are now also available locally at the branch increase the value of the branch and at the same time reduces the bandwidth requirement to the central location.

- The **OpenScape Branch 500i** (OpenScape Branch V2 and later) supports up to 4 or 8 E1/T1 PRI/CAS interfaces without the need of an external gateway unit. The OSB 500i also supports SIP registered lines, Integrated Media Server and Auto Attendant features; and does not support FXS or FXO interfaces.
- The local **Media Server** supports tones, announcements and conferencing which reduces the bandwidth needed to provide the same resources from a central location, hence yielding direct operational cost savings.

- The **Session Border Controller (SBC)** provides security functions like Firewall and Virtual Private Network (VPN) while interfacing with a public network. It also provides the functional templates of Branch SBC for a secure remote branch and central location communication. Additionally the support of SIP Trunking provides direct interface to SIP Service Providers (SSP) from the remote branch.
- The **OpenScape Branch 50i** has the additional functionality of integrated Gateway that provides the efficient inter-connectivity of the OpenScape Branch 50 to the public network via BRI S0, Analog or PRI (OpenScape Branch V1R4 and later) trunk interfaces without the need of an external gateway unit.

It also supports the **integrated Analog Adapter** to interconnect to analog phones or FAX machines without the need of an additional external unit. Thus being a very attractive solution for the small branch with up to 80 registered lines.

- The OpenScape Branch 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.
- The OpenScape Branch currently shares common support tools with OpenScape Session Border Controller.
- The OpenScape Branch is offered on several **HW platforms** allowing a wide range of maximum user capacities of 80, 250, 1000 and 6000 registered lines.

NOTICE: Please note that primary lines, secondary call appearances and phantom lines need to be included in the total count.

- Up to **3000 OpenScape Branch** units can be supported in an OpenScape Voice network. The OpenScape Voice network will support a maximum of 100,000 lines. The total number of users can not exceed the number of users supported by an OpenScape voice system.

Software Licensing

OpenScape Session Branch deployment requires licensing of the product. A CAPEX licensing model and OPEX model (OpenScape Branch V2 and later) 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 Branches:

- **OpenScape Branch Base**
- **OpenScape Branch User**
- **Auto Attendant feature**
- **Backup ACD feature**
- **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:

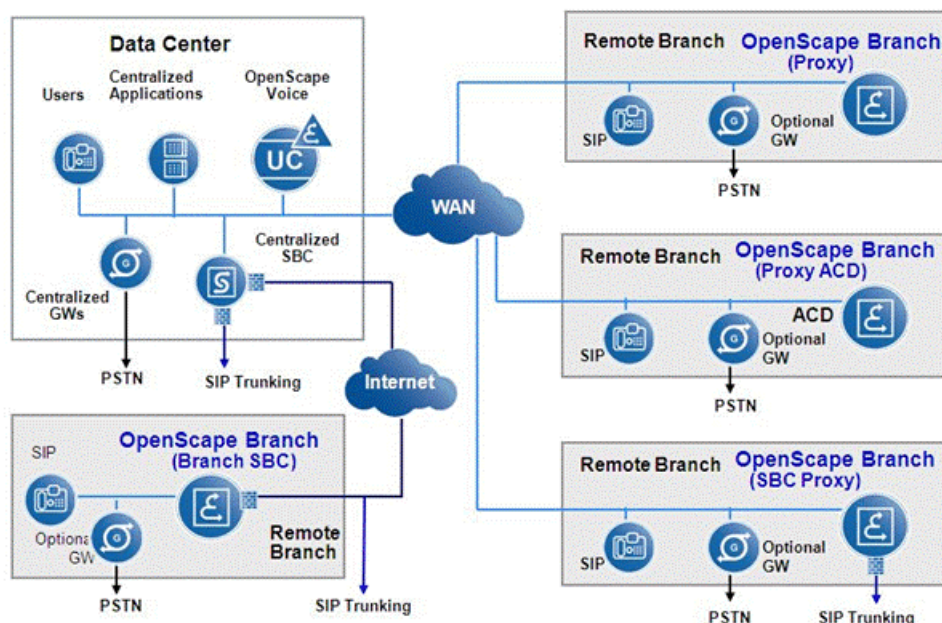
- **Product Instance** - The Product Instance is purchased once for each product and consists of all of the licenses necessary to equip a product for its maximum capacity, including all major features. The Product Instance enables the Monthly Subscription Licenses for the OpenScape Branch and applications.
- **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 Branch 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.

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 Branch in the Network

The following overview shows networking scenarios for OpenScape Branches. In addition, OpenScape Branch V1R4 and later supports the capability to configure multiple OpenScape Branch 50i servers in a single branch/remote branch. This allows support of a greater number of analog trunks to meet the customers' required capacity.



Operating Modes — Overview

The OpenScape Branch has the flexibility to support, depending on the network topology, four different operating modes:

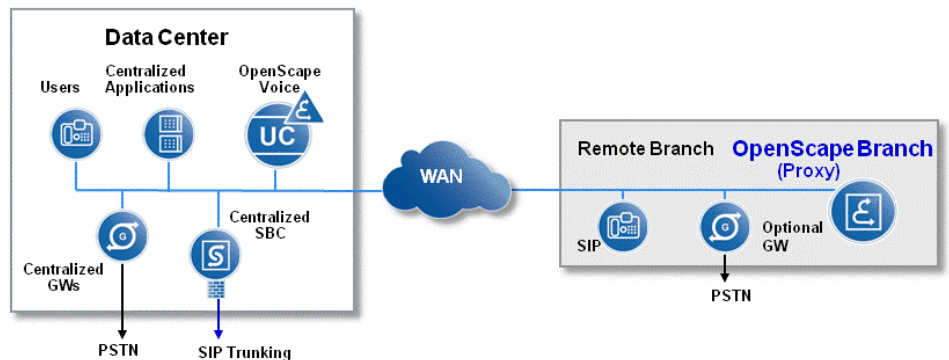
- **Proxy**
- **Proxy ATA**
- **Proxy ACD**
- **SBC Proxy**
- **Branch SBC**

The OpenScape Branch can be configured via the configuration interface (CMP or local GUI) to work in one of the above mentioned modes.

The OpenScape Session Border Controller V1 R1 requires mode "Central SBC" defined under OpenScape Branch configuration. Refer to OpenScape Session Border Controller documentation for details.

- **Central SBC**

Proxy Operating Mode



The Proxy mode is for regular proxy usage when the branch is connected via a private network.

Proxy ATA Operating Mode

There are several OpenScape 50i Proxy ATA applications (Version 2).

OpenScape 50i Proxy ATA Connected via a Proxy OpenScape Branch:

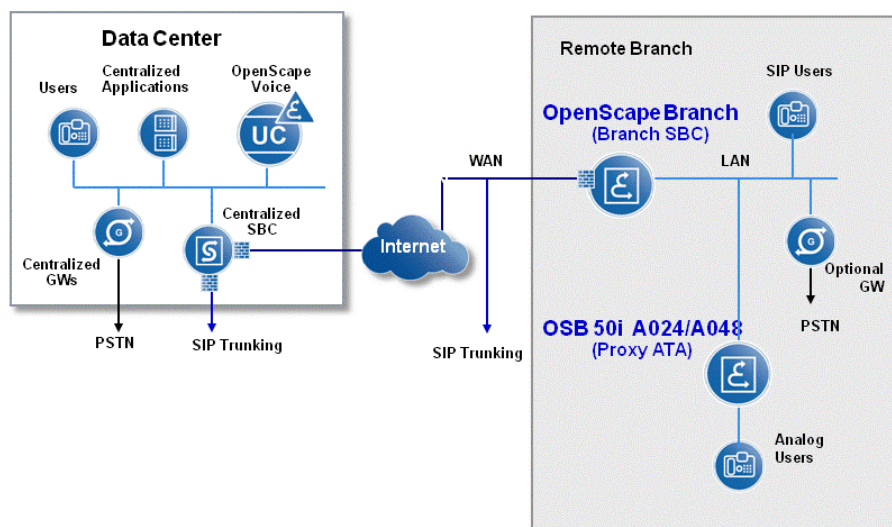
In the figure below, the upstream device is shown as an OpenScape Branch with an external gateway. An alternative to this arrangement would be to use an OpenScape Branch 50i with an internal gateway. The OpenScape Branch is connected to the OpenScape Voice over a corporate WAN, but it could also be connected over a LAN if the Remote Branch is co-located with the OpenScape Voice.

The Proxy ATA registers with only one OpenScape Branch. The Proxy ATA will not support SIP Service Provider trunks.

In this application, the OpenScape Voice can be either in simplex node, or a pair of nodes operating as a cluster (co-located).

If Survivability is required for the OpenScape Branch 50i A024/A048, it will require another upstream device to provide its connectivity to the PSTN. In this configuration, it is required that the upstream device be in the same physical location as the OpenScape Branch 50i A024/A048.

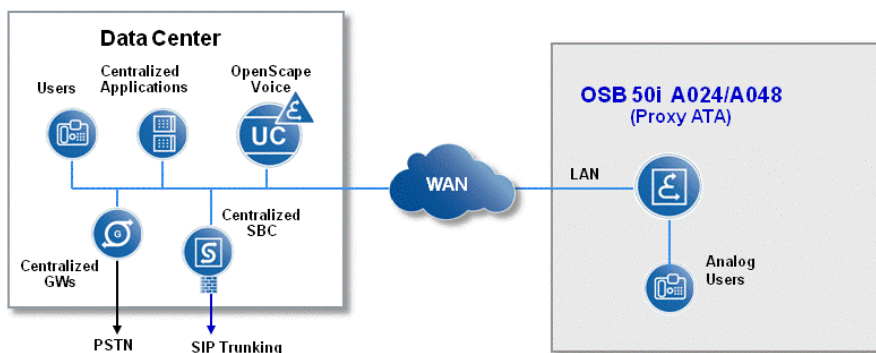
Connected via a Proxy OpenScape Branch



OpenScape 50i Proxy ATA Connected Directly to OpenScape Voice:

The OpenScape Branch 50i A024/A048 can also be utilized as an Analog Terminal Adapter (ATA) connected directly to an OpenScape Voice. The figure below, shows the configuration where the connection to the OpenScape Voice is across a WAN.

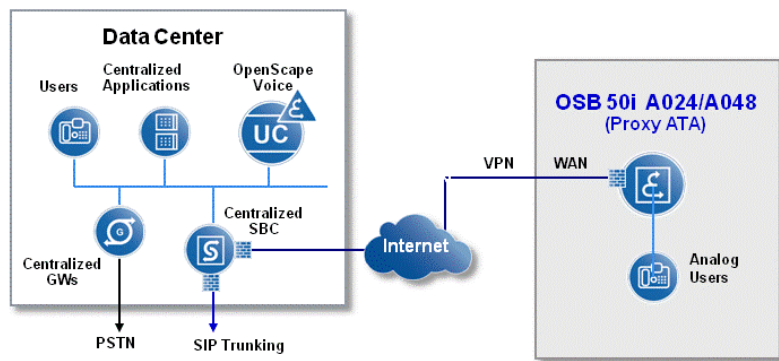
Connected Directly to OpenScape Voice



OpenScape 50i Proxy ATA Connected OpenScape Voice Across the Public Network:

The application, as shown in the figure below, has the OpenScape Branch 50i A024/A048 connected to the OpenScape Voice across a public network. In this configuration, the OpenScape SBC is used. The VPN connection is established at the NAT device.

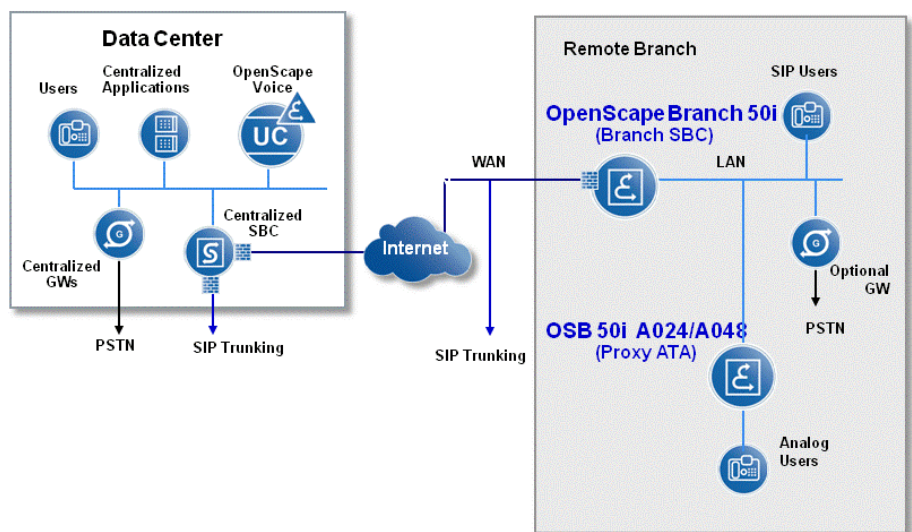
Connected to OpenScape Voice Across Public Network



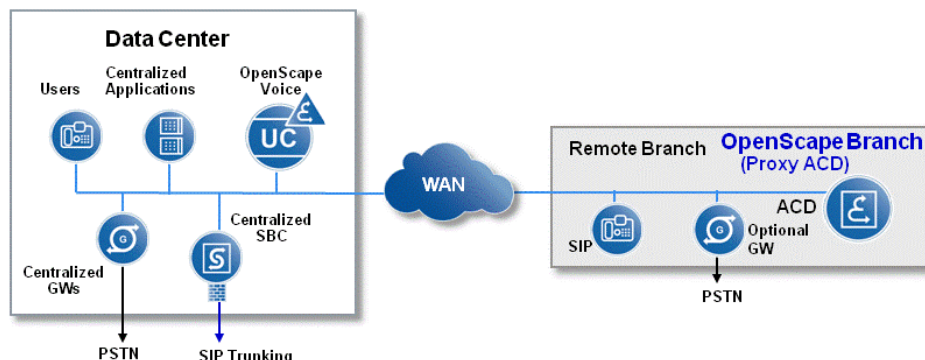
OpenScape 50i Proxy ATA Connected to OpenScape Branch 50i in Branch SBC Mode:

This application shows the OpenScape Branch 50i A024/A048 connected to a OpenScape SBC via another OpenScape Branch running in Branch SBC mode.

Connected to OpenScape Branch 50i in Branch SBC Mode



Proxy ACD Operating Mode



The Proxy ACD (Automatic Call Distribution) mode is for regular proxy connected via a private network and the capability to provide ACD functionality during survivability.

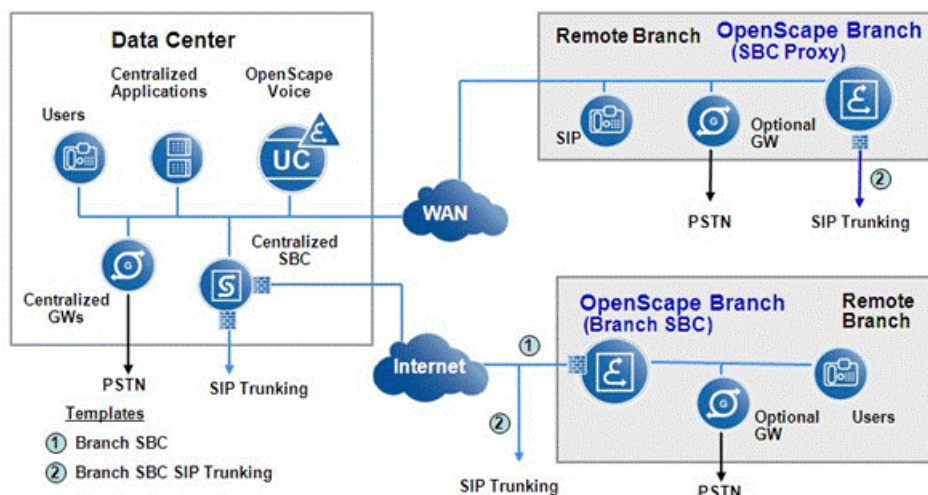
Session Border Controller (SBC)

- Supported Templates

The OpenScape Branch currently supports 2 Session Border Controller (SBC) templates.

- Branch SBC
- Branch SBC SIP Trunking

The diagram below illustrates the two supported templates. Please note that Branch SBC is only supported at the Branch SBC operating mode while the Branch SBC SIP trunking is supported at Branch SBC and SBC Proxy operating modes.



Please note that the OpenScale Branch does not support the Remote Worker template. This function is normally supported by a centralized SBC.

- Supported Capacities

The SIP Trunking capacity varies per OpenScape Branch model. The table below illustrates the maximum number of SIP Trunks and SIP Trunking sessions per OpenScape Branch model.

	50i	50i Axxx	50/250	500i	1000	6000
Max. number of SIP Trunks	1	0	1	1	10	10
Max. number of SIP Service Provider Profiles	1	0	1	1	10	10
Max. number of SIP Trunking Sessions	20	0	60	60	120	400

Please note that SBC Session licenses are required for each SIP Trunking session that is supported by the OpenScape Branch.

- Supported SIP Service Provider (SSP)

The table below lists the currently tested SIP Service Providers with which the OpenScape Branch has been tested with.

SIP Service Providers	Comments
BT HUICS	Tested
BT 21CN	Tested
Gamma (UK)	Tested - minor exceptions
Global Crossing	Tested
Skype Connect	Certified
Verizon	Verizon does not require Global Certification, however for each installation it needs to be go through the Verizon Field Trial process prior the cut-over.

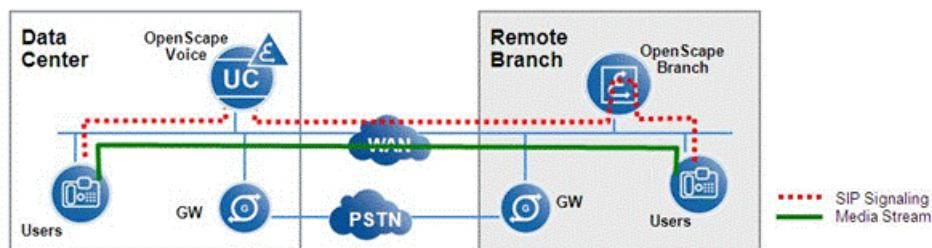
Please note that, despite the effort to keep the document current, this list may become obsolete as new SIP Service Providers are tested. There is a Published Wiki page (at http://wiki.dev.global-intra.net/publishwiki/index.php/Collaboration_with_VoIP_Providers) where all the SIP Testing status is maintain. Please consult there if there is already an activity with the SSP that you are looking for.

The interconnection of the OpenScape Branch to other not listed SIP Service Provides needs to be first tested and verified for any interoperability issue. Please start the process with the submission of an OSIRIS Project Specific Request (PSR) including the project and SSP name for development support on this activity.

Survivability

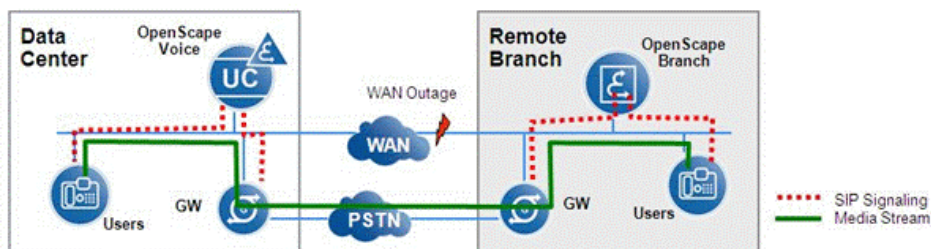
Depending on the network operating state, the OpenScape Branch can be in either one of these three Operational states:

- **Normal**



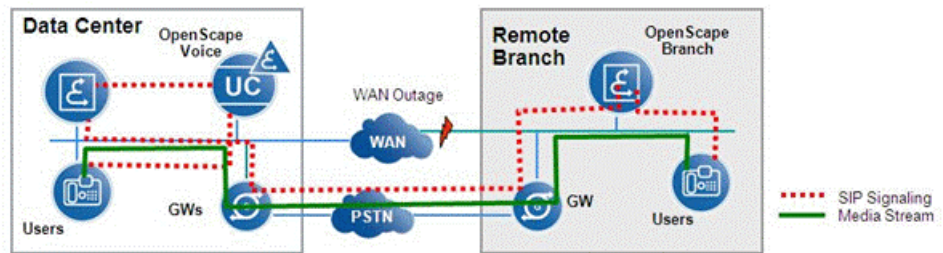
In this state the OpenScape Branch has full access to the OpenScape Voice and Applications. The OpenScape Branch relays all the messages to the OpenScape Voice, which provides all the features to the remote SIP users. Certain features e.g., basic call, consult, transfer, call waiting for analog subscribers are provided by the Asterisk application within the OpenScape Branch. The payload for inter-branch calls goes through the WAN. In the diagram above we see the signaling and media stream path for a call from a user in the branch to a user in the data center.

- **Survivable**



The OpenScape Branch enters in this operational state when there is a partial or complete WAN failure. This state can be reached when a certain number of messages between the OSB and OSV get lost or are not replied to, indicating a WAN failure. At this point the OpenScape Branch continues the service to the remote users by its own survivability features, but having a limited feature set compared to the OpenScape Voice features. In addition, for OpenScape Branch V1R4 and later, music on hold over the survivable gateway/PSTN is supported. All inter-branch calls go through the PSTN. The diagram above shows the signaling and media stream path for a call from a user in the branch to a user in the data center.

- **Backup**



In this state, when the network is configured to support the Backup Signalling Link, the remote OpenScape Branch establishes a new path via the PSTN for signalling traffic to the OpenScape Voice to continue to provide the OpenScape Voice feature set to the remote users. This functionality is currently available to the OpenScape Branch 50 and 50i models. To support this operational state, an OpenScape Branch unit also needs to be deployed at the Data Center to interconnect with the OpenScape Voice. The diagram above shows the signalling and media stream path for a call from a user in the branch to a user in the data center.

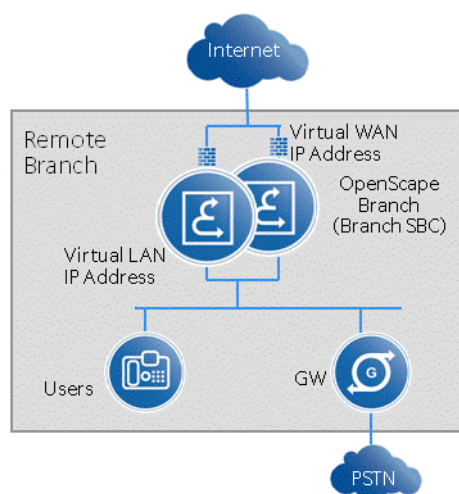
OpenScape Branch V1R4 and later versions, provides for multiple backup links. This allows a larger number of connections to be supported via backup links in case of a WAN failure.

NOTICE:

To support Backup mode, the gateway channels must be ISDN B channels as clear channel signaling is used. The Data Center Access Router must support a VPN/GRE Tunnel to the branch for supervision of the link status on the WAN. Upon a WAN failure the Access Router sends a SNMP trap to the OpenScape Voice system, which in turn sets the CAC policy for that branch to zero. The Access Router must also support failover route set, meaning VPN OK, routing through the WAN and on VPN failure, routing to the BLS (Backup Link Server). The OpenScape Branch by detecting options not being responded via the WAN link, establishes the backup link to the Data Center.

Redundancy

OpenScape Branch Redundancy allows redundancy of an OpenScape Branch unit by having a second unit located on the same subnet having exactly the same database. A communication channel between the two OSB units is used to keep call state information synchronized between the active and standby unit, in order to provide failover with minimal impact on active calls. Some calls may be lost depending on the timing of the failover relative to the calls' SIP signaling activity, particularly when a connection oriented protocol (TCP or TLS) is used for the SIP signaling transport.



OpenScape Branch can be managed via the Virtual IP address; active node synchronizes the DB/XML to the standby node. In OpenScape Branch V1R3 the standby node of OSB is not synchronized immediately during administration of the active node. Therefore, switch over from the active node to the standby node may result in loss of functionality, if the standby node was not updated prior to switch over.

In OpenScape Branch V1R4 and later releases, the standby node of OSB will be synchronized after the changes are applied to the active node and the active node is stable. Therefore, switch over from the active node to the standby node shall result in little to no loss of functionality. Alarms will be handled appropriately with two physical nodes reporting separately.

OpenScape Branch Management and Monitoring

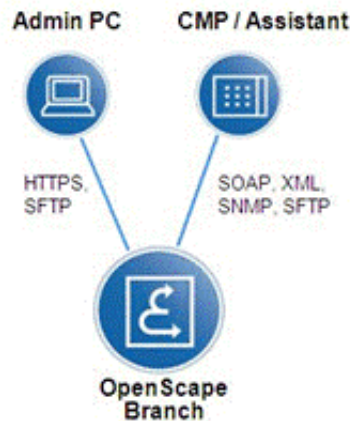
Management Access to Hosted OpenScape Branch via VPN

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

NOTICE: As pointed out earlier, the GUI presentation for a V8 OpenScape Branch is different than in earlier releases. As a consequence, the user will see differences in areas such as: Configuration / Administration Navigation Tree choices. GUI layouts: The V8 OSB Assistant GUI and V8 OSB Local GUI are aligned. This is not the case for earlier OSB versions. Access to Help (V8 has more help '?'s per screen for more granular help access). Help Text for V8 OSBs is different from earlier versions. This is a reflection of the refactoring of the OSB Local GUI as well as its redirection to the Assistant GUI so that users of both the OSB local and Assistant GUIs are afforded a common look and feel. In fact, major parts of the GUI presented on the V8 OSB Assistant are in fact a "cut-through" access to the V8 OSB Local GUI (i.e., they are one and the same).

Alarms are supported via SNMP traps to the CMP/ Assistant and to a Network Management Server.

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

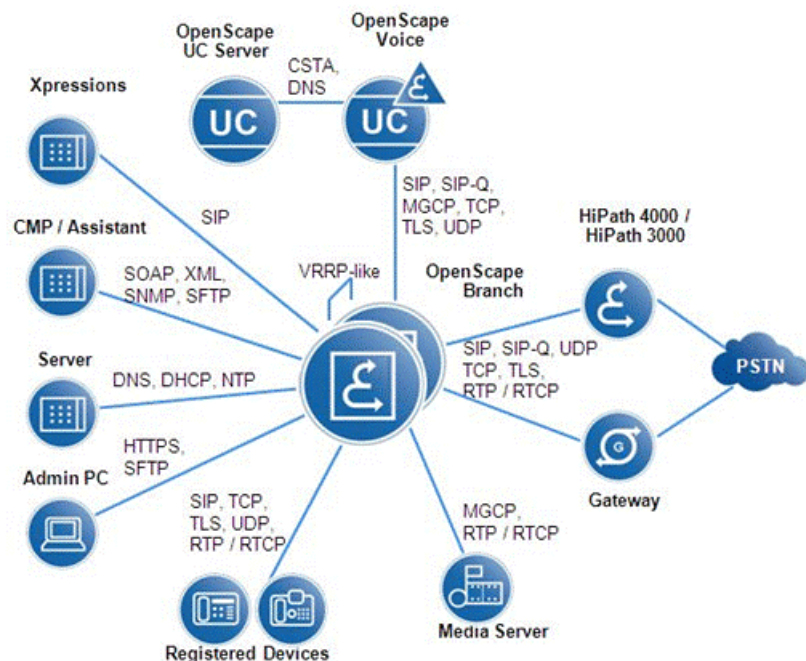


OpenScape Branch V7 introduces secure OpenScape Branch management application access within a hosted OpenScape Voice solution.

To ensure secure management access within an insecure hosted network environment, VPNs are used while VoIP communications continues to utilize the existing SIP and RTP transport security protocols.

Protocols

The OpenScape Branch supports multiple interfaces and protocols. The diagram below illustrates their usage in the network.



1.2.1 Models and Hardware Platforms

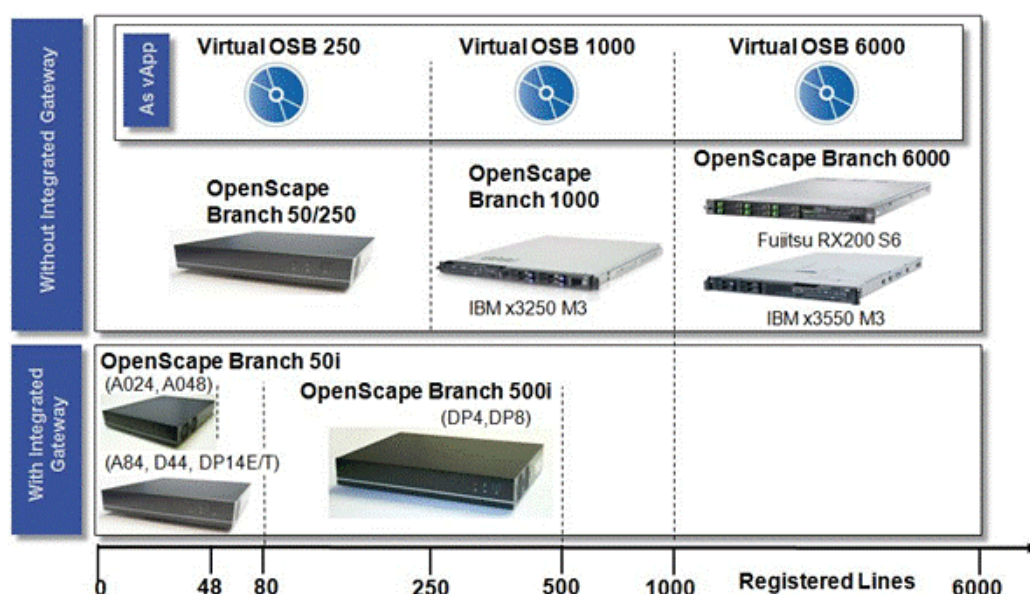
OpenScape Branch is supported on various platforms.

OpenScape Branch Platforms

OpenScape Branch is supported on various platforms and can be divided into three groups:

- Without Integrated Gateway and Analog Adapters
- With Integrated Gateway and Analog Adapters

The diagram below illustrates the various models for each group and their maximum capacity in registered lines.



OpenScape Branch servers Without Integrated Gateway and Analog Adapters

OpenScape Branch without integrated gateways include both hardware and vApp (V7 and Later) supported models.

- **vApp OpenScape Branch** - supported models Virtual OpenScape Branch 250, 1000 and 6000.
- **OpenScape Branch 50/250** – supported by Advantech SYS-2USM02-6M01E server without any Gateway and Analog Adapter interfaces. This Advantech SYS-2USM02-6M01E server supports up to 250 registered lines. This server is the successor of the Acrosser AR-ES5495SM server that supports up to 50 registered lines and the Advantech FWA-710SIME server that supports up to 250 registered lines.

These two servers are no longer available for new orders, however they continue to be supported on OpenScape Branch V2 and are not upgradable to later versions e.g. V7.

- **OpenScape Branch 1000** – (IBM x3250 M3/M5/M6 servers) for up to 1,000 registered lines.

- **OpenScape Branch 6000** – (IBM x3550 M3/M4,Lenovo SR530 (for OSB V9 only) or Fujitsu Primergy RX200 S6/S7 servers) for up to 6000 registered lines

OpenScape Branch servers With Integrated Gateway and Analog Adapters

- **OpenScape Branch 50i** – (Advantech SYS-2USM02-6M01E server) supports up to 80 registered lines with Integrated Gateway and Analog Adapter interfaces. The following combinations of integrated gateways and analog adapters are supported:
 - OpenScape Branch 50i **A84** (Analog - **8** ports FXO + **4** ports FXS)
 - OpenScape Branch 50i **D44** (Digital - **4** ports BRI + **4** ports FXS)
 - OpenScape Branch 50i **DP14E** (Digital - **1** PRI **E1** + **4** ports FXS)
 - OpenScape Branch 50i **DP14T** (Digital - **1** PRI **T1** + **4** ports FXS)
 - OpenScape Branch 50i **DP24** (Digital - **1** PRI **T1** + **4** ports FXS)
 - OpenScape Branch 50i **DP24** (Digital - **2** PRIs/CAS **E1** - FXS or **2** PRIs/CAS **T1** - FXS)
- **OpenScape Branch 50i** – (Advantech SYS-2USM01-6M01E server) for up to 80 registered lines. This server is longer in size when compared to the Advantech SYS-2USM02-6M01E. This server supports higher density of Integrated Analog Adapter interfaces and is available in two flavors:
 - OpenScape Branch 50i **A024** (Analog - **24** ports FXS)
 - OpenScape Branch 50i **A048** (Analog - **48** ports FXS)

OpenScape Branch servers With Integrated PRI Gateway only

- **OpenScape Branch 500i** – (Advantech SYS-2USM03-6M01E server) supports up to 500 registered lines with Integrated PRI Gateway interfaces. The following combinations of integrated gateways are supported:
 - OpenScape Branch 500i **DP4** (Digital - **4** PRI E1/T1)
 - OpenScape Branch 500i **DP8** (Digital - **8** PRI E1/T1)

The maximum number of OpenScape Branch units supported in a network is 3000. The following table shows the characteristics and limits of the profiles:

	OSB 50i	OSB 500i	OSB 50/250	OSB 1000	OSB 6000
Max. number of registered lines *	80	500	50** / 250	1000	6000
Max. number of concurrent Sessions (simultaneous calls)	40	300	40** / 50	200	2400
Max. number of call per second (continuous)	1 cps	5 cps	1** / 3 cps	5 cps	30 cps

NOTICE:

* Registered lines includes primary lines, secondary call appearances and phantom lines.

NOTICE: ** For OpenScape Branch 50 based on Acrosser AR-ES5495SM server.

OpenScape Branch Legacy Servers

The following servers are also available for upgrades to OpenScape Branch V2:

- **OpenScape Branch 50** – Acrosser AR-ES5495SM (V1 and V2 only)
- **OpenScape Branch 250** – Advantech FWA-710SIME (V1 and V2 only)
- **OpenScape Branch 1000** – IBM x3250 M2 (V1 and later)
- **OpenScape Branch 6000** – IBM x3550 M2, Fujitsu Primergy RX330 S1 (V1 and later)

1.3 Navigation

The Common Management Platform (CMP) is used to administer OpenScape Branches.

OpenScape Common Management Platform Overview

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

- **Function Tabs**

Located in the Common Management Platform initial window, these tabs provide access to Configuration, Maintenance and User Management functions.

- **System Bar**

Located in the Configuration function window upper most location includes access to administer products, OpenScape Voice, OpenScape Branch, RG8700 Unified Communications and CMP. NOTE: The V8 CMP provides an additional item for the OpenScape SBC. This item does not exist in earlier versions where both the OSB and SBC are managed from a common OSB Assistant. In V8, there are two separate Assistants that are provided.

- **Navigation Bar**

Located 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 next to the Work Area and provides topics belonging to the selected navigation menu option. NOTE: The topics and functional areas of the Navigation Tree differ between the V8 OSBs and OSBs of earlier versions.

- **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 Branch Administration

The OpenScape Branch administration, used to administer OpenScape Branches, introduces the following items in the Navigation Bar and Tree under

the **OpenScape Branch**. The Administration section of the Navigation Tree and its functional management topics are presented according to the version of the selected Branch Office (V8 or earlier than V8).

Profiles Section:

This section of the Navigation Tree is used to create Branch Profiles which can be assigned to multiple Branch Offices, reducing configuration time.

- **Profiles List**

Provides a list of profiles in the Work Area that can be associated with and OpenScape Branch office.

- **Select Profile**

Drop-down list to select a profile to associated with a Branch office. The Profile List appears in the work area.

- **Management**

Upon selecting a profile from the **Select Profile** drop-down **Management** is used to apply the profile to Branch offices.

- **Configuration**

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

- **Alarms**
- **Logging**
- **Media Server**
- **Network Services**
- **Security**
- **Survivability**
- **VoIP**

Administration Section:

This section of the Navigation Tree is used for configuring OpenScape Branch Offices.

- **Job Management**

Menu items to manage scheduled software upgrades.

- **Licensing**

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

- **Communication System**

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

- **Branch Office list**

Select **Branch Office list** to display and refresh OpenScape Branch information for the selected Communication System. Branch offices for the preselected Communications System will appear in the Work Area.

- **Branch Office**

Select a **Branch Office** drop-down-list is used to select a particular branch office. The Statistics and System Info for the Branch office selected appear in the Work Area.

NOTICE: Please be aware that the list of OpenScape SBCs and OpenScape Branches is not displayed in any particular order, i.e., the list is not sorted alphabetically on the Branch Name but is instead a random list of entries. However, the list displayed on the right side of the screen under OpenScape Branch Overview - All Systems is consistent with the order of the list displayed in the drop down list under Select Branch Office.

- **Management**

Used to manage a selected branch office. For a V8 this only selects OSB. SBCs are selected from the (new with V8) SBC Assistant.

- **Configuration (V7R1 and earlier OSB versions)**

OSB Menu items to configure particular **OpenScape Branch** devices.

- **Alarms**
- **Logging**
- **Media Server**
- **Network Services**
- **Security**
- **Survivability**
- **System**
- **VoIP**
- **ACD**
- **Auto attendant (only for OpenScape Branch V1R3 and later versions)**
- **Integrated gateways** (only for OpenScape Branch 50i models and OpenScape Branch V1R3 and later versions)
- **Phone Software** (only for OpenScape Branch V2 and later versions)

- **Configuration (V8 OSB)**

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

- **Local Dashboard**
- **System**
- **Network/Network Services**
- **VoIP**
- **Features**
- **Security**
- **Diagnostics & Logs**
- **Alarms**
- **Auto attendant**
- **Integrated gateways**

- **Maintenance**

Used to maintain a selected branch office.

- **Alarms**

Used to manage the alarms for a selected branch office.

2 OpenScape Branch 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 Branch office Status.
- Creating or selecting a Branch office of the OpenScape Branch type.
- Saving changes.
- Changing the password in the local Assistant's database.

NOTICE:

The OpenScape Branch Assistant can be used to display or configure branch offices of the OpenScape Branch V1R3, V1R4, V2 and V7 types. The online Help refers mainly to the OpenScape Branch V7 version. Therefore, if an OpenScape Branch V1R3, V1R4 or V2 system is selected, some sections may describe features that are not available for V1R3, V1R4 or V2 systems and some procedures may deviate from the ones described.

2.1 Business Groups and Branch Offices

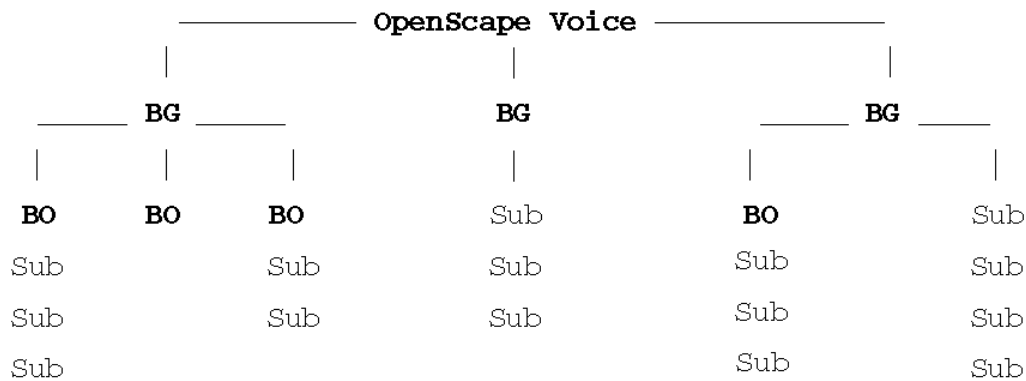
The relationship between Business Groups (BG) and, Session Border Controllers (SBC) and Branch Offices (BO) within OpenScape Voice is characterized by the following properties:

- 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 Create and Delete a Branch Office of the OpenScape Branch Type

A branch office always belongs to a business group. Therefore, creation and removal of a branch office is performed within the OpenScape Voice tab of the OpenScape Voice Assistant. Follow the steps to create a branch office.

Prerequisites

Adequate administrative permissions.

Step by Step

- 1) Navigate to **Configuration tab > 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 the Branch to be viewed.

The Business Group selected appears in the Available Business Groups pull-down.
- 3) Select the **Branch Office List > Branch Offices** in the Navigation Tree.

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

NOTICE: Please be aware that the list of OpenScape SBCs and OpenScape Branches is not displayed in any particular order, i.e., the list is not sorted alphabetically on the Branch Name but is instead a random list of entries. However, the list displayed on the right side of the screen under OpenScape Branch Overview - All Systems is consistent with the order of the list displayed in the drop down list under Select Branch Office.

4) Proceed as follows to create a new branch office:

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

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

- b) Fill in the **Branch Office Name** and **Representative Endpoint** fields.
c) Select a numbering plan for the branch office from the **Numbering Plan** selection list.
d) Select an office code from the **Office Code** selection list.
e) Select the routing area of the branch office 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.

When the Branch Office of the OpenScape Branch type is added to the OpenScape Voice Assistant, a record will be added to the OpenScape Branch Assistant's database. From that point the OpenScape Branch Assistant will be able to administer this Branch Office.

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

NOTICE: An OpenScape Branch must be deleted from the OpenScape Voice Assistant

- a) Select **Configuration > OpenScape Voice > Business Group (icon)**.
b) Select the associated business group from the **Business Group** field list.
c) Select **Branch Office List** and select the Branch Office to be deleted.

The **Delete** button becomes active.

- d) Click the **Delete** button to delete the selected Branch Office.

The corresponding record will be deleted from the OpenScape Voice Assistant and OpenScape Branch Assistant databases.

2.3 How to Display a Branch Office Via OpenScape Branch Assistant

The OpenScape Branch Assistant can administer branch offices of the OpenScape Branch type. Thus it keeps a list of branch offices in its database. The "OpenScape Branch Overview" displays all known branch offices and provides a search function to find a particular one.

Prerequisites

Adequate administrative permissions.

At least one 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) To display all branch offices: navigate to **Configuration tab > OpenScape Branch** 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).

If **All systems** is not currently selected, selecting All systems will display the **OpenScape Branch Overview** in the Work Area, with a current list of all known branch offices of all systems. If no branch offices are defined, the list is empty. If **All systems** was previously selected, then proceed to step 3.

- 3) Select **Branch Office list** in the Navigation Tree.

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

NOTICE: Please be aware that the list of OpenScape SBCs and OpenScape Branches is not displayed in any particular order, i.e., the list is not sorted alphabetically on the Branch Name but is instead a random list of entries. However, the list displayed on the right side of the screen under OpenScape Branch Overview - All Systems is consistent with the order of the list displayed in the drop down list under Select Branch Office.

- 4) To view a list of Branch Offices 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 find and select a particular branch office use one of the following options:

- In the Work Area select the checkbox to the left of the particular branch office in the list. Action Menu buttons are set active in the Work Area with the following options: **Manage**, **Password...**, **Refresh Selected**, **Edit...**, **Delete**. Selecting the **Manage** button updates the **Branch Office** field, in the Navigation Tree, with the selected branch office and displays information and data in the Work Area for that branch office.
- Choose a branch office from the **Branch Office** pull-down located in the Navigation Tree. Information and data are displayed in the Work Area.
- Enter filter search criteria to filter the list of branch offices.

Filtering is possible on the following criteria from the **in** field: **Branch Office** (name), **Business Group**, **IP Address**, **Version**, **Status**, **Mode**.

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

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

The system refreshes the list of displayed branch offices and displays the ones matching the search criteria.

- 7) Click The **Clear** button. The system clears the filter criteria field and displays all records of the default communication system selected in the **Communication System** field. If no specific communication system is selected, all branch offices of all systems are listed in the Work Area.

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

2.4 How to Edit an OpenScape Branch via OpenScape Branch Assistant

Proceed as follows to “edit” an OpenScape Branch via OpenScape Branch Assistant. Note: Adding and deleting an OpenScape Branch is initiated via the OpenScape Voice Assistant (See section, How to Create and Delete a Branch Office of the OpenScape Branch Type, for details):

Prerequisites

Adequate administrative permissions.

The connection to the OpenScape Voice system is up.

Step by Step

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

The system presents the **Branch Office Overview** in the Work Area with a current list of all branch offices.

NOTICE: Please be aware that the list of OpenScape SBCs and OpenScape Branches is not displayed in any particular order, i.e., the list is not sorted alphabetically on the Branch Name but is instead a random list of entries. However, the list displayed on the right side of the screen under OpenScape Branch Overview - All Systems is consistent with the order of the list displayed in the drop down list under Select Branch Office.

- 3) Proceed as follows to assign edit an OpenScape Branch:
 - a) Checkmark the OpenScape Branch Office to be edited from the list.
 - b) Click the **Edit...** button.

The **Edit OpenScape Branch** dialog is displayed.

The following parameters are display only: Branch Office Name, IP Address, Comm System, Business Group and Endpoint.

- c) Select the associated **Profile Name** from the pull-down field to select or change the profile.
- d) 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 Branch is first added to the OpenScape Branch Assistant. Once the OpenScape SBC requests an authorization statement and the OpenScape Branch 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 Branch to request a new authentication statement.

- e) Click the **OK** key to save the OpenScape Branch updates.

The **Edit OpenScape Branch** dialog is closed and the **OpenScape Branch Overview** is displayed with updated Security status information.

OpenScape Branch data is updated in the OpenScape Branch Assistant.

2.5 How to Update Branch Offices Status

The information for one particular branch office or all branch offices stored in the database can be updated.

Prerequisites

Adequate administrative permissions.

At least one branch office of the OpenScape Branch type has to be configured.

The connection to the OpenScape Voice system is up.

Step by Step

- 1) To display all branch offices: navigate to **Configuration tab > OpenScape Branch** 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).

If **All systems** is not currently selected, selecting All systems will display the **OpenScape Branch Overview** in the Work Area, with a current list of all known branch offices of all systems. If no branch offices are defined, the list is empty. If **All systems** was previously selected, then proceed to step 3.

NOTICE: Please be aware that the list of OpenScape SBCs and OpenScape Branches is not displayed in any particular order, i.e., the list is not sorted alphabetically on the Branch Name but is instead a random list of entries. However, the list displayed on the right side of the screen under OpenScape Branch Overview - All Systems is consistent with the order of the list displayed in the drop down list under Select Branch Office.

3) Select **Branch Office list** in the Navigation Tree.

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

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

- **Inventory** - Indicates the OpenScape Branch system is configured in the Assistant but not installed.
- **Authenticated** – Indicates the OpenScape Branch platform has contacted the OpenScape Branch Assistant with all appropriate credentials.
- **Installation started** – Indicates that the OpenScape Branch has all the data necessary and started the installation process.
- **File Transfer Started** - Indicates that the File Transfer has been started by the OpenScape Branch.
- **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 Branch has started.
- **Boot Failed** - Indicates that the OpenScape Branch 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 OSB 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 OSBs) and because the Operational state is not available for the Backup Node.
- **Unreachable** – check alarms.

4) To update all branch offices click the **Refresh All** button.

The system contacts all branch offices that are visible or invisible in the list and refreshes its internal information about these. Please note that this may cause delay time depending on the number of branch offices configured.

IMPORTANT: In order to view the **Refresh All** progress, edit the columns displayed and add the last-update column to the displays, then reselect the branch office list.

5) To update particular branch offices, check the respective branch offices in the list or use the filter fields to limit the number of displayed branch offices.

6) Click The **Refresh Selected** button.

The internal information of the branch offices checked is updated. Please note that this may cause delay time depending on the number of branch offices checked.

2.6 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 branch office of the OpenScape Branch type is configured and in operation.

The OpenScape Branch system is Version 1R3 or later.

The connection to the OpenScape Voice system is up.

Step by Step

- 1) To display all branch offices: navigate to **Configuration tab > OpenScape Branch** 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).

If **All systems** is not currently selected, selecting All systems will display the **OpenScape Branch Overview** in the Work Area, with a current list of all known branch offices of all systems. If no branch offices are defined, the list is empty. If **All systems** was previously selected, then proceed to step 3.

- 3) Select **Branch Office list** in the Navigation Tree.

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

- 4) Choose an OpenScape Branch Office by checking a checkbox of the particular branch office in the Branch Office List.
- 5) Click the **Password** button.

The **Password** dialog appears.

- 6) Select a user identification in the **User** selection list.
- 7) Enter the new password in the **New password** and **Confirm new password** fields. The password must be 8...36 characters.
- 8) Click the **Update appliance password** checkbox.
- 9) Click the **Change** button to set the new password or click the **Reset** button to reset the password to default.

A confirmation message is displayed.

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

- 10) Click the **Close** button.

The password is changed or reset in the local database of the OpenScape Branch Assistant.

Related concepts

[Password Management](#) on page 87

Related tasks

[How to Change or Reset Passwords](#) on page 264

3 OpenScape Branch Assistant – Maintenance

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

OpenScape Branch V1R3, V1R4, V2, V7,V8 and V9

The OpenScape Branch Assistant can be used to display and configure OpenScape Branch Offices. The online Help system may describe features that are not available for pre-V8 versions of OpenScape Branch and some procedures may deviate from the ones described.

3.1 System Information and Monitoring

Aggregated information on an Openscape Branch system can be displayed via the Common Management Platform (CMP).

3.1.1 The OpenScape Branch Dashboard via CMP

The **Dashboard** view of an OpenScape Branch system can be displayed via the Common Management Platform. It provides a variety of performance and system information. Several subwindows 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 branch office.

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 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 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 subwindow.

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 (Pre-V8 OSB):**

The operating system and its software version used for the selected branch office of the OpenScape Branch type.

- **Hardware Type (Pre-V8 OSB):**

The hardware type used for OpenScape 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 and the system is operating in "limited mode". A transition to survivable mode goes from: "normal" mode to "transition" mode to "survivable" mode. The proxy remains in "transition" mode 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 of the service.

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 the Redundancy has 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 Branch lost the connection with SIP server. "Active" represents full connectivity with the SIP server. "Transition" is presented when OpenScape Branch detects a connectivity problem with the SIP Server. "OK" represents the state where the binding has lower priority than the currently active binding.

- **WAN Outage Server**

Presents the address or FQDN used for check of WAN connectivity. In case of a WAN outage the box associated with it is red, otherwise it remains green. This information is only relevant in case of collocated or separated servers.

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.

- Show Registered Subscribers.
- Show Link Status.
- Show Dynamic port mapping.
- Show Backup Link status.
- Show Subscriber status.
- Show Denial of Service Mitigation status.

3.1.1.1 How to Display the OpenScape Branch Dashboard via CMP

The OpenScape Branch Assistant displays aggregated information and data for the selected branch office in the "Dashboard View" via the Common Management Platform.

Prerequisites

Adequate administrative permissions.

At least one 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 **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 Branch type:
 - a) Use the **Search for** and **in** fields to filter the list for OpenScape Branch systems.
 - b) Click the name of an Open Scape branch node 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 branch office.

Prerequisites

Adequate administrative permissions.

At least one branch office of the OpenScape Branch type 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 Branch type:
 - a) Use the **Search for** and **in** fields to filter the list for OpenScape Branch systems.
 - b) Click the name of an Open Scape branch node.

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 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 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.

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

Related tasks

[How to Display Alarm Details](#) on page 51

[How to Start Rapidstat to Perform a Health Check](#) on page 52

[How to Display Detailed Version Information](#) on page 53

[How to Display the Services Status of a V8 OpenScape Branch System](#) on page 55

[How to Display, Export and Clear Log Files for a V8 OSB](#) on page 60

3.1.1.3 How to Display Alarm Details

Perform the following steps to display details of a specific alarm of a particular branch office.

Prerequisites

Adequate administrative permissions.

At least one branch office of the OpenScape Branch type 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 Branch type:

- a) Use the **Search for** and **in** fields to filter the list for OpenScape Branch systems.
- b) Click the name of an Open Scape branch node.

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 branch office.

- 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:

```
NeID: brazil_253_10.1.111.253
EventGroupName: Communication
EventName: Loss of communication with primary OSV
Severity: 2
EventType: 2
EventTime: 2009-02-23T14:52:43+0000
FaultyObject: Primary OSV link
MonitoredValue: 1.000000
ThresholdValue: 0.000000
OpenBranchAlarm0501: Spontaneous Alarm from the managed
network element.
```

Related tasks

[How to Display Active Alarms](#) on page 49

[How to Start Rapidstat to Perform a Health Check](#) on page 52

[How to Display Detailed Version Information](#) on page 53

[How to Display the Services Status of a V8 OpenScape Branch System](#) on page 55

[How to Display, Export and Clear Log Files for a V8 OSB](#) on page 60

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 Branch system.

Prerequisites

Adequate administrative permissions.

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

The connection to the OpenScape Branch system is up.

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 Branch type:

- a) Use the **Search for** and **in** fields to filter the list for OpenScape Branch systems.
- b) Click the name of an Open Scape branch node.

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

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

The **Rapid Stat** dialog appears.

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

- 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 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

- Level 5:

B2BUA channel usage and interface information.

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 49

[How to Display Alarm Details](#) on page 51

[How to Display Detailed Version Information](#) on page 53

[How to Display the Services Status of a V8 OpenScape Branch System](#) on page 55

[How to Display, Export and Clear Log Files for a V8 OSB](#) on page 60

3.1.1.5 How to Display Detailed Version Information

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

Prerequisites

Adequate administrative permissions.

At least one branch office of the OpenScape Branch type 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 Branch type:

- a) Use the **Search for** and **in** fields to filter the list for OpenScape Branch systems.
- b) Click the name of an Open Scape branch node 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 Branch version information -
-----
Version           = V2R0.02.00
Internal Version  = osb-02.00.02.2
```

```
Date                = 2011-Aug-03 16:13:26
WSDL                = Version V4.00.00
Partition           = Second
```

```
-----
sw=mediaserver 3.3_5.12.0-1073
```

Related tasks

[How to Display Active Alarms](#) on page 49

[How to Display Alarm Details](#) on page 51

[How to Start Rapidstat to Perform a Health Check](#) on page 52

[How to Display the Services Status of a V8 OpenScape Branch System](#) on page 55

[How to Display, Export and Clear Log Files for a V8 OSB](#) on page 60

3.1.1.6 How to Display System Information for an OpenScape Branch Office

Perform the following steps to display system information for an OpenScape branch office.

Prerequisites

Adequate administrative permissions.

At least one branch office of the OpenScape Branch type 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 Branch type:

- a) Use the **Search for** and **in** fields to filter the list for OpenScape Branch systems.
- b) Click the name of an Open Scape branch node.

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

- 3) View the **System Info** field area. The following information is provided:
- CPU Usage:
Percentage of CPU processing power used.
 - Memory:
Percentage of available memory used.
 - Disk Usage:
Percentage of available disk space used.
 - Date and 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 11.3(i586).
 - Hardware Type:
Physical or Virtual hardware type e.g., Advantech 50i (PRI T1-FXS), Virtual OSB250.

The **System Information** is displayed for the selected branch office.

3.1.1.7 How to Display the Services Status of a V8 OpenScape Branch System

The current status of the available services of the selected OpenScape Branch system can be displayed.

Prerequisites

Adequate administrative permissions.

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

Step by Step

- 1) Navigate to **Configuration tab > OpenScape Branch**.

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

- 2) Click the **Branch Office List**.

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

- 3) Select a node of the OpenScape Branch type and click the Manage button.

The system presents the **Navigation Tree** view of the selected node.

- 4) Select the Local Dashboard.

The system presents the **Dashboard** view of the OpenScape Branch.

- 5) In the **System Status** field area, click the **Services status Show** button. For V8 go to the Dashboard via the Configuration > OpenScape Branch, select an OSB and Click Manage.

The **Services Status** window appears.

The current status (not running, active, running, stand-by) of available services for the selected system is displayed:

- Alarm Manager: Application responsible for generating and clearing the alarms.
- Audit: Application used to provide an assessment of a system's internal control.
- B2BUA (Back-to-Back User Agent): This application is used by MLHG (Multi Line Hunt Group) calls and calls from and to gateways in Survivability Mode, it provides a SIP back to back UA functionality such as create new SIP Requests (different call IDs, branch...). The B2BUA service always shows the status "running", regardless of the B2BUA flag or MLHG configuration.
- BLC: Backup Link Client application.
- BLS: Backup Link Server application.
- CDR (Call Detail Record): Ticket generation application: The tickets opened or closed in Survivability Mode will be stored internally and sent to the CDR server according to configuration (see Survivability Features). The status of the CDR applications is "stand-by" in normal operational mode or "running" in survivability mode.
- 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.
- Interface 1: First network interface.
- Interface 2: Second network interface.
- Interface 3: Third network interface.
- Interface 4: Fourth network interface.
- IPsec: Linux open source application that controls the IPsec encryption/authentication system.
- Media Server: This is the same application as in the OpenScape Voice system providing reduced announcement capabilities in Survivability Mode and operating as branch Media Server in Normal Mode.
- 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.
- MS (Media Server) Converter: This is a SIP-MGCP converter. It converts the SBC (Session Border Controller) message from SIP Server to MGCP (Media Gateway Control Protocol) and sends it to Media Server and vice-versa.

- 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 Branch redundant nodes
- RTP Proxy: The RTP (Realtime 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. It is 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.
- Message Rate Control: Open source Network Intrusion Prevention and Detection System (NIPS/NIDS)
- SSDP: (Smart Services Delivery Platform) Management through remote access.
- 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)
- Survivability Provider: Responsible for checking 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).
- 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 Branch Homepages by Web Browsers.

Related tasks

[How to Display Active Alarms](#) on page 49

[How to Display Alarm Details](#) on page 51

[How to Start Rapidstat to Perform a Health Check](#) on page 52

[How to Display Detailed Version Information](#) on page 53

[How to Display, Export and Clear Log Files for a V8 OSB](#) on page 60

3.1.1.8 How to Display the Services Status of a V8 OpenScape Branch System

The current status of the available services of the selected OpenScape Branch system can be displayed.

Prerequisites

Adequate administrative permissions.

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

Step by Step

1) Navigate to **Configuration tab > OpenScape Branch.**

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

2) Click the **Branch Office List.**

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

3) Select a node of the OpenScape Branch type and click the Manage button.

The system presents the **Navigation Tree** view of the selected node.

4) Select the Local Dashboard.

The system presents the **Dashboard** view of the OpenScape Branch.

5) In the **System Status field area, click the **Services status Show** button. For V8 go to the Dashboard via the Configuration > OpenScape Branch, select an OSB and Click Manage.**

The **Services Status** window appears.

The current status (not running, active, running, stand-by) of available services for the selected system is displayed:

- Alarm Manager: Application responsible for generating and clearing the alarms.
- Audit: Application used to provide an assessment of a system's internal control.
- B2BUA (Back-to-Back User Agent): This application is used by MLHG (Multi Line Hunt Group) calls and calls from and to gateways in Survivability Mode, it provides a SIP back to back UA functionality such as create new SIP Requests (different call IDs, branch...). The B2BUA service always shows the status "running", regardless of the B2BUA flag or MLHG configuration.
- BLC: Backup Link Client application.
- BLS: Backup Link Server application.
- CDR (Call Detail Record): Ticket generation application: The tickets opened or closed in Survivability Mode will be stored internally and sent to the CDR server according to configuration (see Survivability Features). The status of the CDR applications is "stand-by" in normal operational mode or "running" in survivability mode.
- 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.
- Interface 1: First network interface.
- Interface 2: Second network interface.

- Interface 3: Third network interface.
- Interface 4: Fourth network interface.
- IPsec: Linux open source application that controls the IPsec encryption/authentication system.
- Media Server: This is the same application as in the OpenScape Voice system providing reduced announcement capabilities in Survivability Mode and operating as branch Media Server in Normal Mode.
- 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.
- MS (Media Server) Converter: This is a SIP-MGCP converter. It converts the SBC (Session Border Controller) message from SIP Server to MGCP (Media Gateway Control Protocol) and sends it to Media Server and vice-versa.
- 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 Branch redundant nodes
- RTP Proxy: The RTP (Realtime 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. It is 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.
- Message Rate Control: Open source Network Intrusion Prevention and Detection System (NIPS/NIDS)
- SSDP: (Smart Services Delivery Platform) Management through remote access.
- 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)
- Survivability Provider: Responsible for checking 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).
- 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 Branch Homepages by Web Browsers.

Related tasks

[How to Display Active Alarms](#) on page 49

[How to Display Alarm Details](#) on page 51

[How to Start Rapidstat to Perform a Health Check](#) on page 52

[How to Display Detailed Version Information](#) on page 53

[How to Display, Export and Clear Log Files for a V8 OSB](#) on page 60

3.1.1.9 How to Display, Export and Clear Log Files for a V8 OSB

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

Prerequisites

Adequate administrative permissions.

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

Different log levels can be set under **Configuration > OpenScape Branch > Configuration > Diagnostics & Logs > Logs tab**.

Step by Step

1) Navigate to **Configuration > OpenBranch**.

2) Click the **Branch Office List**.

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

3) Select a node of the OpenScape Branch type and click the **Manage** button.

The system presents the **Navigation Tree** view of the selected node.

4) Select **Diagnostics & Logs** and then **Logs** choices.

The **Diagnostics & Logs** window appears.

- 5) In the Log Viewer data work area, select one of the following log files from the **Log data** drop down, and then click the Show button next to it.
- Alarm History:
Alarm history, showing all active or cleared alarms.
 - Alarm Manager:
Log of Alarm manager application.
 - B2BUA:
Back to back SIP user agent, this application is responsible for MLHG handling.
 - Boot:
Log of last boot.
 - CDR:
The Log of Call Detail Record application.
 - Continuous Tracing:
Log of the Continuous Tracing application.
 - Current processes:
A list of the current processes running on OpenScape Branch.
 - DAHDI
Need to add in descriptive text for DAHDI.
 - Install/Upgrade/Update:
Log from system installation, updates or upgrades. This includes also media server language installation information.
 - Media Server:
Log of Media server, MGCP Adapter and SIPMGCP converter applications.
 - Phone Software Management:
tba.
 - Process Manager:
Log of PM application.
 - RTP Proxy:
Log of RTP Proxy application.
 - Registration Blacklist:
tba.
 - SIP Server:
SIP stateful proxy or SBC (Session Border Controller) application.
 - SSM:
Log of SIP Services Module application.
 - Message Rate Control:
Log from Message Rate Control application.
 - Survivability Provider:
Log of Survivability provider application.
 - System:
Log of system events.

- Web server:

Log of the local web server application

6) The following options appear:

- To show the log file of the selected type, click the **Show...** 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.

- Click the **Close** button.

Related tasks

[How to Display Active Alarms](#) on page 49

[How to Display Alarm Details](#) on page 51

[How to Start Rapidstat to Perform a Health Check](#) on page 52

[How to Display Detailed Version Information](#) on page 53

[How to Display the Services Status of a V8 OpenScape Branch System](#) on page 55

3.1.1.10 How to Display, Export and Clear Log Files for a V8 OSB

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

Prerequisites

Adequate administrative permissions.

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

Different log levels can be set under **Configuration > OpenScape Branch > Configuration > Diagnostics & Logs > Logs tab**.

Step by Step

1) Navigate to **Configuration > OpenBranch**.

2) Click the **Branch Office List**.

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

3) Select a node of the OpenScape Branch type and click the **Manage** button.

The system presents the **Navigation Tree** view of the selected node.

4) Select **Diagnostics & Logs** and then **Logs** choices.

The **Diagnostics & Logs** window appears.

- 5) In the Log Viewer data work area, select one of the following log files from the **Log data** drop down, and then click the Show button next to it.
- Alarm History:
Alarm history, showing all active or cleared alarms.
 - Alarm Manager:
Log of Alarm manager application.
 - B2BUA:
Back to back SIP user agent, this application is responsible for MLHG handling.
 - Boot:
Log of last boot.
 - CDR:
The Log of Call Detail Record application.
 - Continuous Tracing:
Log of the Continuous Tracing application.
 - Current processes:
A list of the current processes running on OpenScape Branch.
 - DAHDI
Need to add in descriptive text for DAHDI.
 - Install/Upgrade/Update:
Log from system installation, updates or upgrades. This includes also media server language installation information.
 - Media Server:
Log of Media server, MGCP Adapter and SIPMGCP converter applications.
 - Phone Software Management:
tba.
 - Process Manager:
Log of PM application.
 - RTP Proxy:
Log of RTP Proxy application.
 - Registration Blacklist:
tba.
 - SIP Server:
SIP stateful proxy or SBC (Session Border Controller) application.
 - SSM:
Log of SIP Services Module application.
 - Message Rate Control:
Log from Message Rate Control application.
 - Survivability Provider:
Log of Survivability provider application.
 - System:
Log of system events.

- Web server:

Log of the local web server application

6) The following options appear:

- To show the log file of the selected type, click the **Show...** 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.

- Click the **Close** button.

Related tasks

[How to Display Active Alarms](#) on page 49

[How to Display Alarm Details](#) on page 51

[How to Start Rapidstat to Perform a Health Check](#) on page 52

[How to Display Detailed Version Information](#) on page 53

[How to Display the Services Status of a V8 OpenScape Branch System](#) on page 55

3.1.2 General System Information

For V9 OSBs the statistics are located under the Navigation Tree branch Diagnostics & Logs > Statistics.

Statistics

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

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.

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 Branch.

NOTICE:

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

- **Backup link Status:** For V9 OSB, the Backup Link Status is available from the Dashboard.

NOTICE:

A list of registered subscribers, the Backup link status and the Integrated Gateway's link status (only for OpenScape Branch 50i and 500i) can be displayed in separate windows

- **Link Status:** Select the **Show** button to display link status for the OpenScape Branch.

NOTICE:

Refer to section **How to Display the Integrated Gateway Link Status and Perform Channel Maintenance** for details.

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 Branch.
- **HW ID:**
The hardware I ID associated with the OpenScape Branch.
- **HW ID2:**
The hardware ID associated with the OpenScape Branch backup system, if a backup system is configured.

The following buttons are displayed:

- **Refresh:** Select the **Refresh** button to update the license file for the OpenScape Branch.
- **Device license update:** Select the **Device license update** button to update the licenses for devices associated with the OpenScape Branch.

- **Configure:** Select the **Configure** button to update the license file for the OpenScape Branch.

NOTICE:

Refer to section **How to Configure and Clear Licensing for an OpenScape Branch Office 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 Branch Base, OpenScape Branch Users, Auto Attendant, Backup ACD, SBC Sessions.

- **Configured:**

Number of available licenses configured in the CMP.

- **Reported Locally:**

Number of licenses assigned in the local OpenScape Branch.

- **Usage (Peak):**

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

OpenScape Branch Hardware Types

OpenScape Branch is supported on various platforms and can be divided into two groups:

- Without Integrated Gateway and Analog Adapters
- With Integrated Gateway and Analog Adapters

OpenScape Branch servers Without Integrated Gateway and Analog Adapters

- **OpenScape Branch 50/250** – supported by Advantech SYS-2USM02-6M01E server without any Gateway and Analog Adapter interfaces. This Advantech SYS-2USM02-6M01E server supports up to 250 registered lines. This server is the successor of the Acrosser AR-ES5495SM server that supports up to 50 registered lines and the Advantech FWA-710SIME server that supports up to 250 registered lines.

These two servers are no longer available for new orders, however they continue to be supported on OpenScape Branch V2.

- **OpenScape Branch 1000** – (IBM x3250 M3/M5/M6 servers) for up to 1,000 registered lines.
- **OpenScape Branch 6000** – (IBM x3550 M3/M4, Lenovo SR530 (OSB V9 only) or Fujitsu Primergy RX200 S6/S7 servers) for up to 6000 registered lines.

OpenScape Branch servers With Integrated Gateway and Analog Adapters

- **OpenScape Branch 50i** – (Advantech SYS-2USM02-6M01E server) supports up to 80 registered lines with Integrated Gateway and Analog

Adapter interfaces. The following combinations of integrated gateways and analog adapters are supported:

- OpenScape Branch 50i **A84** (Analog - 8 ports FXO + 4 ports FXS)
- OpenScape Branch 50i **D44** (Digital - 4 ports BRI + 4 ports FXS)
- OpenScape Branch 50i **DP14E** (Digital - 1 PRI E1 + 4 ports FXS)
- OpenScape Branch 50i **DP14T** (Digital - 1 PRI T1 + 4 ports FXS)
- OpenScape Branch 50i **DP24** (Digital - 2 PRIs/CAS E1 - FXS or 2 PRIs/CAS T1 - FXS)
- **OpenScape Branch 50i** – (Advantech SYS-2USM01-6M01E server) for up to 24 or 48 FXS ports. This server is longer in size when compared to the Advantech SYS-2USM02-6M01E. This server supports higher density of Integrated Analog Adapter interfaces and is available in two flavors:
 - OpenScape Branch 50i **A024** (Analog - 24 ports FXS)
 - OpenScape Branch 50i **A048** (Analog - 48 ports FXS)

NOTICE:

SIP subscribers and FXOs are not supported on this server.

OpenScape Branch servers With Integrated PRI Gateway only

- **OpenScape Branch 500i** – (Advantech SYS-2USM03-6M01E server) supports up to 500 registered lines with Integrated PRI Gateway interfaces. The following combinations of integrated gateways are supported:
 - OpenScape Branch 500i **DP4** (Digital - 4 PRI E1/T1)
 - OpenScape Branch 500i **DP8** (Digital - 8 PRI E1/T1)

3.1.2.1 How to Display a List of Registered Subscribers

Perform the following steps to display a list of all subscribers registered within a particular branch office.

Prerequisites

Adequate administrative permissions.

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

At least one subscriber is registered in the selected branch office.

Step by Step

- 1) Navigate to **Configuration tab > OpenScape Branch** 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 **Branch Office list** in the Navigation Tree under Administration.

The system presents the **Branch Office Overview** in the Work Area with a current list of all branch offices.

- 4) To view a list of Branch Offices 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 find and select a particular branch office use one of the following options:
 - In the Work Area select the checkbox to the left of the particular branch office in the list and select **Manage**. Selecting the **Manage** button updates the **Branch Office** field, in the Navigation Tree, with the selected branch office and displays information and data in the Work Area for that branch office.
 - Choose a branch office from the **Branch Office** pull-down located in the Navigation Tree. Information and data are displayed in the Work Area.
- 6) For V8 OSB, select the Local Dashboard under Management. The Local Dashboard is displayed.
- 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 branch office is displayed:

- Username:
Name of the subscriber.
- Contact:
SIP contact information.
- Expires:
The expiration time is based on the information sent by the subscriber on registration.

3.1.2.2 How to Display the Backup Link Status

Perform the following steps to display the status of the Backup Link Client service or Backup Link Server service.

Prerequisites

Adequate administrative permissions.

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

At least one subscriber is registered in the selected branch office.

Step by Step

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

The system presents the **Branch Office Overview** in the Work Area with a current list of all branch offices.

- 3) To view a list of Branch Offices 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 branch office use one of the following options:
 - In the Work Area select the checkbox to the left of the particular branch office in the list and select **Manage**. Selecting the **Manage** button updates the **Branch Office** field, in the Navigation Tree, with the selected branch office and displays information and data in the Work Area for that branch office.
 - Choose a branch office from the **Branch Office** pull-down located in the Navigation Tree. Information and data are displayed in the Work Area.
- 5) Click the **Backup link status Show...** button in the **System Info** field area. Note: For V8 OSB, the button is located on the Local Dashboard screen.

Depending on the mode of the OSB appliance configured in the **VoIP** window, **General** tab, (Client or Server) the status for either the Backup Link Client or Backup Link Server appears:

- **Backup Link Client Status:**

The status of the Backup Link Client contains the following information:

- BLS IP Address
- PPP Local IP Address
- PPP Remote IP Address
- Interface Name
- Negotiated Packetization Interval
- Local RTP Port
- Up Time
- IP Packets Received
- IP Packets Sent
- IP Packets Dropped
- RTP Packets Received
- RTP Packets Sent
- RTP Packets Lost

- **Backup Link Server Status:**

The BLS Clients Status list is displayed. The list contains the **BLC Host Names** and the respective **Up time**.

- 6) To view the detailed status of a particular BLS Client, select the respective entry in the **BLS Clients Status** list in the **Backup Link Server Status** dialog and click the **Show...** button.

The **BLS Client Status** dialog appears providing the following information on the selected BLS client:

- Tunnel Name
- BLC Hostname
- PPP Local IP Address
- PPP Remote IP Address
- Interface Name
- Packetization Interval
- Local RTP Port
- Up Time
- IP Packets Received
- IP Packets Sent
- IP Packets Dropped
- RTP Packets Received
- RTP Packets Sent
- RTP Packets Lost

- 7) Click the **Close** button to return to the **Backup Link Server Status** dialog.

3.1.2.3 How to Perform PRI Channel Maintenance

Channel maintenance can be performed on OpenScape Branch 500i PRI cards. Access to Channel Maintenance can be accomplished via the Link Status Window or the PRI Configuration Window. To perform channel maintenance proceed as follows.

Prerequisites

Adequate administrative permissions.

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

At least one subscriber is registered in the selected branch office.

Step by Step**1) To navigate to the Channel Maintenance via the Link Status window:**

- a) Navigate to **Configuration tab > OpenScape Branch** within the Navigation Bar in the Common Management Platform.
- b) Select the **Branch Office list** in the Navigation Tree under Administration.

The system presents the **Branch Office Overview** in the Work Area with a current list of all branch offices.

- c) To view a list of Branch Offices 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.

- d) To find and select a particular branch office use one of the following options:

- In the Work Area select the checkbox to the left of the particular branch office in the list and select **Manage**. Selecting the **Manage** button updates the **Branch Office** field, in the Navigation Tree, with the selected branch office and displays information and data in the Work Area for that branch office.

- Choose a branch office from the **Branch Office** pull-down located in the Navigation Tree. Information and data are displayed in the Work Area.

- e) Click the **Link status Show...** button in the **System Info** field area.
NOTE: For V8 OSB, the Link statusShow button is located on the Local Dashboard screen.
- f) Click the **Channel Maintenance** button in the **Link Status** dialog.

The Channel Maintenance window appears.

2) To navigate to the Channel Maintenance via the PRI Configure Window:

- a) Navigate to **Configuration tab > OpenScape Branch** within the Navigation Bar in Common Management Platform.
- b) Select the **Branch Office list** in the Navigation Tree under Administration.

The system presents the **Branch Office Overview** in the Work Area with a current list of all branch offices.

- c) To view a list of Branch Offices 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.

- d) To find and select a particular branch office use one of the following options:

- In the Work Area select the checkbox to the left of the particular branch office in the list and select **Manage**. Selecting the **Manage** button updates the **Branch Office** field, in the Navigation Tree, with the selected

branch office and displays information and data in the Work Area for that branch office.

- Choose a branch office from the **Branch Office** pull-down located in the Navigation Tree. Information and data are displayed in the Work Area.

- e) Navigate to **Configuration > OpenScape Branch > Integrated Gateways in the navigation tree under Administration**.
- f) Click the **Configure...** button associated with the PRI interface in the **Gateway configuration** field area.

The PRI window appears.

- g) Click the **Channel Maintenance** button in the **Method** field area.

The **Channel Maintenance** window appears and link status of channels and ports is displayed.

E1/T1 PRI (for the 500i)

The link status of E1/T1 PRI (E1/T1 PRI Rate Interface) Card 1 (ports 1-4) and Card 2 (ports 1-4) (if installed) is displayed. The status can be as follows:

The status of PRI **Ports** can be as follows:

- **Up**: green
- **Down**: red
- **Disabled**: yellow

The status of PRI **D Channel** (T1 channel 24, E1 channel 16) can be as follows:

- **In Service**: green
- **OOS** (Out of Service): red

NOTICE:

D-Channels are displayed with a "D" in the status indicator, where applicable.

The status of PRI **B Channels** (T1 channels 1-23, E1 channels 1-15 and 17-31) can be as follows:

- **Idle**: green
- **Busy**: blue
- **Manually Disabled**: Orange
- **OOS-NE** (Out of Service-Near End): red
- **OOS-NE** (Disabled - Out of Service-Near End): red
- **OOS-FE** (Out of Service-Far End): red

- 3) To perform PRI channel maintenance for a particular OpenScape Branch 500i system use the following options:

- **Restart selected channels** button - performs a restart for all selected channels on one or both PRI cards.
- **Block selected channels** button - disables access for all selected channels on one or both PRI cards.
- **Unblock selected channels** button - enables access for all selected channels on one or both PRI cards.

- 4) To **Restart** PRI channels initiate the following:
- Select the channels to be restarted. To select All Channels for a given port check the **All channel** checkbox. To select/deselect individual channels check/uncheck the associated channel for the port and card.
 - Click the **Restart selected channels** button to initiate the restart.

The selected channels will be restarted?

- 5) To **Block** PRI channels from being accessed initiate the following:
- Select the channels to be blocked. To select All Channels for a given port check the **All channels**. To select individual channels check the associated channel for the port and card.
 - Click the **Block selected channels** to block the selected channels.

NOTICE:

Blocking is only enabled for T1 PRI's (not E1) and BCAS must be enabled.

The channels shall remain blocked and not accessible until they are manually unblocked.

- 6) To **Unblock** PRI channels to allow access to the channel(s) initiate the following:
- Select the channels to be unblocked. To select All Channels for a given port check the **All channels**. To select individual channels check the associated channel for the port and card.
 - Click the **Unblock selected channels** to initiate the unblock.

NOTICE:

Unblocking is only enabled for T1 PRI's (not E1) and BCAS must be enabled.

The selected channels are unblocked and available for access.

Status and Channel Maintenance is performed as requested.

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 Branch System

Serviceability for a particular OpenScape Branch 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 Branch devices. The following methods and tasks are supported:

- Display a list of available software on the CMP (Common Management Platform) for downloading to the OpenScape Branch devices.
- Software transfer or activation for a list of OpenScape Branch devices.
- 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 Branch Local Management Tool Versus Assistant

For a new installation and complete setup of an OpenScape Branch system the OpenScape Branch 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 Branch Assistant may be used to maintain and configure the system as well.

3.2.1 OpenScape Branch File System

On the system's compact flash are partitions 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, Media Server, and external applications such as those that access the CDR (Call Detail Record) records, the same OpenScape Voice directory structure is preserved.

Compact Flash Partitioning

The compact flash is partitioned as follows:

- Partition "A" is used to hold the one copy of the uncompressed OpenScape Branch software.
- Partition "B" is used to hold a second copy of the uncompressed OpenScape Branch 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 Branch 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 Branch system 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 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, MS (Media Server) languages, CDR records, 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).

IMPORTANT: In case the maximum number of XML configuration files saved on your system exceeds 100, the older ones will be deleted until the compact flash is full with 100 files.

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 Branch system. Should the md5 checksum not match, the update will be stopped, removed and the user informed via an error message.

```
<?xml version="1.0" ?>
<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 81

3.2.1.1 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 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 Branch** within the Navigation Bar in the Common Management Platform.
- 2) Select the **Branch Office list** in the Navigation Tree under Administration.
The system presents the **Branch Office Overview** in the Work Area with a current list of all branch offices.
- 3) To view a list of Branch Offices 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 branch office use one of the following options:
 - In the Work Area select the checkbox to the left of the particular branch office in the list and select **Manage**. Selecting the **Manage** button updates the **Branch Office** field, in the Navigation Tree, with the selected branch office and displays information and data in the Work Area for that branch office.
 - Choose a branch office from the **Branch Office** pull-down located in the Navigation Tree. Information and data are displayed in the Work Area.
- 5) (V8 OSB) While within the Navigation Tree navigate to Maintenance > Restart. (Pre V8 OSB) navigate to **Configuration > System**.

The **System** dialog appears.

- 6) To restart the system use one of the following options:
 - Select **Current Version** in the **to** field to restart to the current version.
 - Select **Backup** in the **to** field to restart to the backup version.
- 7) (V8 OSB) Click either the Restart or Restart to backup button. (Pre V8 OSB) Click the **Restart** button.

A confirmation dialog appears.

- 8) Confirm the restart.

The system restarts.

3.2.1.2 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 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 Branch** within the Navigation Bar in the Common Management Platform.
- 2) Select the **Branch Office list** in the Navigation Tree under Administration.
The system presents the **Branch Office Overview** in the Work Area with a current list of all SBCs and branch offices.
- 3) To view a list of SBCs and Branch Offices 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 branch office use one of the following options:
 - In the Work Area select the checkbox to the left of the particular SBC or branch office in the list and select **Manage**. Selecting the **Manage** button updates the **Branch Office** field, in the Navigation Tree, with the selected SBC or branch office and displays information and data in the Work Area for that SBC or branch office.
 - Choose a SBC or branch office from the **Branch Office** pull-down located in the Navigation Tree. Information and data are displayed in the Work Area.
- 5) (V8 OSB) While within the Navigation Tree navigate to Maintenance > Import/Export. (Pre V8 OSB) navigate to **Configuration > System** in the navigation tree under Administration.
(V8 OSB) The Import/Export dialog appears. (Pre V8 OSB) 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 78

3.2.1.3 How to Select a Configuration File for Import

Proceed as follows to import a new configuration file where all configuration settings are stored. Custom DNS and DHCP files can also be imported starting with OpenScape V7

Prerequisites

Adequate administrative permissions.

At least one 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 Branch** within the Navigation Bar in the Common Management Platform.
- 2) Select the **Branch Office list** in the Navigation Tree under Administration.

The system presents the **Branch Office Overview** in the Work Area with a current list of all branch offices.
- 3) To view a list of Branch Offices 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 branch office use one of the following options:
 - In the Work Area select the checkbox to the left of the particular branch office in the list and select **Manage**. Selecting the **Manage** button updates the **Branch Office** field, in the Navigation Tree, with the selected branch office and displays information and data in the Work Area for that branch office.
 - Choose a branch office from the **Branch Office** pull-down located in the Navigation Tree. Information and data are displayed in the Work Area.

- 5) (V8 OSB) Navigate to Maintenance > Import/Export. For Pre OSB OSBs navigate to **Configuration > System** in the navigation tree under Administration.
(V8 OSB) The Import/Export dialog appears. (Pre V8 OSB) 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 to import a new configuration file to the OpenScape.
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 Branch appliance.

The action is completed. Configuration, DNS and DHCP files are imported.

Related tasks

[How to Load and Apply New Configuration Files](#) on page 77

3.2.1.4 How to Export Configuration Files

Proceed as follows to export a configuration file where all configuration settings are stored. Custom DNS and DHCP files will also be exported starting with OpenScape V7.

Prerequisites

Adequate administrative permissions.

At least one 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 Branch** within the Navigation Bar in the Common Management Platform.
- 2) Select the **Branch Office list** in the Navigation Tree under Administration.
The system presents the **Branch Office Overview** in the Work Area with a current list of all branch offices.

- 3) To view a list of Branch Offices 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 branch office use one of the following options:
 - In the Work Area select the checkbox to the left of the particular branch office in the list and select **Manage**. Selecting the **Manage** button updates the **Branch Office** field, in the Navigation Tree, with the selected branch office and displays information and data in the Work Area for that branch office.
 - Choose a branch office from the **Branch Office** pull-down located in the Navigation Tree. Information and data are displayed in the Work Area.
- 5) (V8 OSB) Navigate to Maintenance > Import/Export. (Pre V8 OSB) Navigate to **Configuration > System** in the navigation tree under Administration.

(V8 OSB) The Import/Export dialog appears. (Pre V8 OSB) 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. Configuration, DNS and DHCP files are exported.

3.2.2 Software Updates and Upgrades

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

OpenScape Branch 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 Branch appliance.

The following functions are provided:

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

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

Job Management

The OpenScape Branch Assistant can be used to create, view and configure scheduled batch jobs for upgrading/updating several branch offices via the Upgrade Manager in the navigation area.

Related concepts

[OpenScape Branch File System](#) on page 74

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

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

Prerequisites

Adequate administrative permissions.

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

The connection to the OpenScape Branch system is 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 Branch 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.
- 7) Perform a manual refresh to update the new software version in the CMP after a successful reboot of the OSB.

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

3.2.3 Job Management

OpenScape Branch Job Management enables the administrator to view the OpenScape Branch 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 Branch devices, the administrator displays OpenScape Branch 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 Branch Assistant can be used to create, view and configure batch jobs for mass upgrading/updating of OpenScape Branch devices. Proceed as follows to display a list of batch jobs and detailed information.

Prerequisites

Adequate administrative permissions.

Branch offices of the OpenScape Branch type are configured and in operation.

The connection to the OpenScape Voice system is up.

Step by Step

- 1) Navigate to **Configuration tab** > **OpenScape Branch** 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**, the **User ID** 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 84

[How to Edit or Cancel a Batch Job](#) on page 85

3.2.3.2 How to Create a New Batch Job

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

Prerequisites

Adequate administrative permissions.

Branch offices of the OpenScape Branch type are configured and in operation.

The connection to the OpenScape Voice system is up.

Step by Step

- 1) Navigate to **Configuration tab > OpenScape Branch** 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**, **XML Command**).

IMPORTANT:

In order to apply **Delta XML** as batch job for mass updating of OpenScape Branch devices, perform the **Assign profile** action and afterwards select **Profile: DeltaXML**.

NOTICE:

XML Command: convert to XML format.

- 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 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 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 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 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 83

[How to Edit or Cancel a Batch Job](#) on page 85

3.2.3.3 How to Edit or Cancel a Batch Job

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

Prerequisites

Adequate administrative permissions.

Branch offices of the OpenScape Branch type are configured and in operation.

The connection to the OpenScape Voice system is up.

Step by Step

- 1) Navigate to **Configuration tab > OpenScape Branch** 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 main window.
- 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 83

[How to Create a New Batch Job](#) on page 84

3.2.4 Hardware Upgrades

Depending on the customer's service concept, hardware updates can be performed to add additional integrated gateways and analog adapters.

OpenScape Branch Hardware Upgrades

OpenScape Branch 50i allows the customer to add additional gateway and adapter hardware to expand the current capability. Hardware can be extended to maximum allowed values keeping in mind the traffic requirements and server capabilities.

IMPORTANT:

V9R0 requires at least 4GB memory. The 2GB RAM replacement only impacts the Advantech SYS-2USM01-6M01E and SYS-2USM02-6M01E servers. These servers are used in the OSB 50/250 and the OSB 50i models. This upgrade is applicable to servers that were delivered prior to December 2013. The memory size of the server is displayed in **System Info** under the **General** tab of the OSB Management view.

OpenScape Branch 500i currently does not support adding additional PRI gateways to a DP4 model to create an OpenScape Branch DP8 model. The customer must choose a 4 port (DP4) or 8 port (DP8) configuration when purchasing the OpenScape Branch 500i server.

Upgrade to 64-bit

OSB V9 can run in 64-bit mode. The 64bit mode on OSB is needed for.

- synchronizing the code and implementation between OS-SBC (already running in 64bit mode) and OSB
- better utilizing security updates and Features
- utilizing the full RAM of 4Gig when available (provided with refresher OSBs).
- utilizing the 64bit Media Server (32bit support can be retired)
- preparing the OSB to be used in a container application on OS4K Gateways

The 64bit OSB Software Load will be usable in Hardware models:

- OSB50i all types with 8G-DOM and 2G-RAM (current Models)

- OSB50i all types with 16G-DOM and 4G-RAM (Refresher Models)
- OSB500i all types with 8G-DOM and 2G-RAM (current Models)
- OSB500i all types with 16G-DOM and 4G-RAM (Refresher Models)

IMPORTANT: The support of the 64bit mode will NOT require a full install, just regular update procedures. A fallback to the 32bits is also provided.

3.3 Password Management

The password management is used to change or reset passwords.

OpenScape Branch Passwords

Passwords to access an OpenScape Branch appliance can be defined for several user identities depending on the access rights. Via the OpenScape Branch Assistant these passwords can be configured via the 'Password' button located in the "OpenScape Branch Overview" display of 'All systems'. This is available via Configuration > OpenScape Branch > Branch Office List, then selecting the specific OSB and clicking the Password' button. The passwords are stored in the database of the OpenScape Branch appliance. On the OpenScape Branch Assistant's database only the passwords of the user ID "assistant" (V1R3) and "administrator" (V1R2) are stored.

After an update or a missed synchronization of the password, the access to an OpenScape Branch V1R3 or later version 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 **Local password...** button in the **OpenScape Branch Overview** screen.

Types of Users on the OpenScape Branch Appliance

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

- administrator,
- assistant,
- guest,
- redundancy (only for OpenScape SBC),
- service,
- ACD,
- cdr .

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

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

Types of Users on the OpenScape Branch Assistant

Depending on the version of the OpenScape Branch appliance, the following users are available for login:

- administrator (OpenScape Branch V1R2),
- administrator, assistant (OpenScape Branch V1R3 and later releases).
- administrator, assistant, redundancy (OpenScape SBC V1 and later releases)

For OpenScape Branch V1R2 appliances the password can not be changed.

Related tasks

[How to Change the Password in the Local Assistant Database](#) on page 44

[How to Change or Reset Passwords](#) on page 264

3.4 General Installation - Overview

This chapter describes the options for installing software and hardware for OpenScape Branches. In OpenScape Branch Version 2 simplified installation procedures were introduced. In addition, general configuration was added to OpenScape Branch Assistant to configure functions for communicating between OpenScape Branch Assistant and OpenScape Voice Assistant used during installation. In OpenScape Branch Version 7 a feature was introduced to allow secure OpenScape Branch management application access within the hosted OpenScape Voice solution (Option 5).

OpenScape Branch Assistant Configuration

"General Settings" is used to configure a secure method of transport between OpenScape Branch 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 five 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 Branch Assistant and is used to communicate from the OpenScape hardware to the OpenScape Branch 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 Branch Assistant must be configured with the software load required for this particular server.

NOTICE:

The OpenScape Branch and OpenScape SBC are 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 Branch or 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 Branch or OpenScape SBC will then accept that DHCP Offer from the second network interface (WAN) and use that interface to contact the CMP. If attempting to bring the OpenScape Branch up as Branch-SBC mode, then only have the DHCP Server configured to provide Option 43 on the WAN side interface of the OpenScape Branch. The OpenScape Branch and OpenScape SBC ignore any DHCP Offers which do not contain Option 43.

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

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

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

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

- **Option 4 (Local xml Config File):**

The OpenScape Branch server hardware requires a USB stick for installation. The USB stick is pre-loaded with required installation software including an xml configuration file for the OpenScape Branch Office 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.

- **Option 5 (Management Access to Hosted OpenScape Branch via VPN):**

To ensure secure management access within an insecure hosted network environment, VPNs shall be used while VoIP communications continues to utilize the existing SIP and RTP transport security protocols.

The OpenScape Branch 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 Branch Office, the CMP URL and Boot VPN information prior to shipping to the customer.

In addition, the xml file contains an Administration IP address to identify the gateway address (VPN network) to be used for routing IP packets.

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

Basic Installation:

The OpenScape Branch “Basic Installation” is the pre-Version 2 OpenScape Branch installation method. Installation requires the use of a memory stick with the current software load and the assigned IP address for the system. In addition, any of the media files associated with the Media Server language, ACD and Auto Attendant must be uploaded to the OpenScape Branch device explicitly.

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

IMPORTANT:

IP packets with the used ports (configured in OSB, SBC) 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.

3.4.1 OpenScape Branch Assistant - Configuration

This chapter describes configuration for the OpenScape Branch Assistant.

General Settings

The "General Settings" option is used to configure a secure method of transport between OpenScape Branch Assistant and the OpenScape Voice Assistant for the purpose of transferring configuration, ACD Music on Hold (MoH), ACD and Attendant media files.

3.4.1.1 How to Configure OpenScape Branch Assistant - General Settings

Proceed as follows to configure OpenScape Branch Assistant General Settings. General settings include transport security, data synchronization and Adding languages to the CMP media server repository.

Prerequisites

Adequate administrative permissions.

The connection to the OpenScape Branch system is up.

Step by Step

- 1) Navigate to **Configuration tab** and select **OpenScape Branch** within the Navigation Bar in Common Management Platform.
- 2) Select the **General Settings** in the Navigation Tree under Administration.
The system presents the **General Settings** dialog with the **Installation** tab displayed by default.
- 3) Proceed as follows to enable secure transport between the OpenScape Branch Assistant and the OpenScape Voice Assistant:
 - a) Check the **Secure transfer** checkbox.
 - b) The **Security transfer** checkbox enables secure communications via SOAP between the OpenScape Branch 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 Branch Assistant (certain files only apply to OpenScape Branch servers).

- - Software Load: HTTPS only
 - - Language files for Media Server other than default language: HTTPS only
 - - Configuration File: HTTPS or SOAP (Secure)
 - - ACD Music on Hold: HTTPS or SOAP (Secure)
 - - ACD Announcement Media Files: HTTPS or SOAP (Secure)
 - - Auto Attendant Media Files: 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 Branch Assistant will communicate securely to the OpenScape Voice Assistant.

- 4) Proceed as follows to add media server language files to the CMP media server language repository:

- a) Click the **Add...** button in the **Media Server language files** work area.

The **Add 1 files to Media server** dialog is displayed

- b) Click the **Browse...** button in the work area.

The browser dialog is displayed.

- c) Select a Media Server Language file.

The file format must be RPM (.rpm). The maximum size of a single file should not exceed 70 MB and is limited to 2 files.

- d) If additional files are required Click the **Browse...** button for associated with the next file to be added and browse to select another Media Server Language file.

- e) Click the **Save** button.

The **Add language files to Media server** dialog closes and the **General Settings** dialog is updated with the current language files in the Media Server Language Repository.

- f) Click the **Save** key to complete configuration.

3.4.2 Simplified Installation Steps

This chapter describes the general steps for OpenScape Branch Version 2 and later, and OpenScape SBC Version 2 and later, 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:

- Media server files

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

- Required for Option 1-5

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 Branch server.

- Required for Option 1-3, 5

NOTICE:

OpenScape SBC during DHCP server discovery sends out a DHCP Discover message with Option 60 Vendor Class Identifier automatically set to "OpenScapeBranch" (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 Branch or OpenScape SBC from the DHCP Server. The Option 43 parameters returned to the OpenScape Branch or OpenScape SBC in a DHCP Offer will include the Common Management Platform FQDN(s) or IP Address(es) so that the OpenScape Branch or 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 Branch or 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 Branch to OpenScape Voice Assistant:

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

- Required for Option 1-5

4) Configure the Software Load, Hardware Type and Media Server Files for the OpenScape Branch:

Configure the Software Load to be downloaded to the server, the Hardware Type of the server and Media Server Language files for the OpenScape Branch in the Common Management Platform (CMP), OpenScape Branch 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 1-5

5) Configure ACD Announcement files, ACD Music on Hold files Auto Attendant files and the Data Configuration File for the OpenScape Branch:

ACD announcement and Music on Hold files and Auto attendant files can be downloaded to the OpenScape Branch server. A Data configuration file can also be downloaded to the OpenScape Branch using the Common Management Platform (CMP), OpenScape Branch Assistant.

- Optional for Options 1-5

6) Add the LAN MAC Address to the OpenScape Branch Assistant:

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

- Required for Option 1 only

7) Connect the OpenScape Hardware to the Network:

Install the OpenScape server onto the network. Plug in the USB stick into the OpenScape Branch server and power up the server. Upon power up installation information is exchanged between the CMP and the OpenScape Branch server. The list of installation files includes the software load, configuration file and possibly media files and config.xml file for the database. In OpenScape Branch Version 7, Boot VPN information will be included for Option 5. 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 2-5

NOTICE:

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

8) Troubleshooting Installation Errors and Alarming:

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

9) Confirmation Installation is complete:

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

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

The OpenScape Branch 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 can be used to install multiple OpenScape Branch servers. Files include product software loads, media server software, ACD software, and Auto Attendant software.

Prerequisites

Adequate administrative permissions.

The connection to the OpenScape Voice system is up.

Step by Step

- 1) Navigate to **Maintenance tab > Inventory** within the Navigation Bar in 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:

Media server files (for OpenScape Branch) are transferred to the following directories in the CMP:

- **Offboard** (separate server used for CMP): /opt/siemens/openbranch/ob_config/ms_languages
- **Onboard** (aka Integrated, CMP runs in the same OSV server)/img/enterpriseimg/primary/openbranch/ob_config/ms_languages

NOTICE:

ACD (for OpenScape Branch), Auto Attendant (for OpenScape Branch) and Configuration files are transferred to the following directories in the CMP:

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

ACD Announcement directory: (OpenScape Branch)

```
/opt/siemens/openbranch/ob_config/<Logical_ID>/  
ACD_Announcements
```

Auto Attendant directory: (OpenScape Branch)

```
/opt/siemens/openbranch/ob_config/<Logical_ID>/  
AutoAttendant_Announcements
```

Configuration File directory:

```
/opt/siemens/openbranch/ob_config/<Logical_ID>/  
Configuration_File
```

- **Onboard** (aka Integrated, CMP runs in the same OpenScape Voice server):

ACD Announcement directory: (OpenScape Branch)

```
/img/enterpriseimg/primary/openbranch/ob_config/  
<Logical_ID>/ACD_Announcements
```

Auto Attendant directory: (OpenScape Branch)

```
/img/enterpriseimg/primary/openbranch/ob_config/  
<Logical_ID>/AutoAttendant_Announcements
```

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 servers.

3.4.2.2 How to Configure a Windows DHCP Server

OpenScape device DHCP client will Broadcast a DHCP discovery Request with Option 60 Vendor Class Identifier automatically set to "OpenScapeBranch". 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., OSB_VCI, **Description** e.g., OpenScape Branch Vendor Class Identifier.
- e) Click the field under the **ASCII** column in the table and enter the value "OpenScapeBranch" (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 (OSB_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., OSB-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 Branch requires.
 - h) Enter description in the **Description** field (optional) e.g., OSB 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 (OSB_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 Branch 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 Branch or 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 Branch or OpenScape SBC will then accept that DHCP Offer from the second network interface (WAN) and use that interface to contact the CMP. If attempting to bring the OpenScape Branch up as Branch-SBC mode, then only have the DHCP Server configured to provide Option 43 on the WAN side interface of the OpenScape Branch. The OpenScape Branch and OpenScape SBC ignore 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 Branch or 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 "OpenScapeBranch". 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 LINUX 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 Branch. The parameters below refer to the specific settings needed for the Simplified Installation with the OpenScape Branch 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.swsupply" 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 Branch and OpenScape SBC only recognize and accept Option 43 responses with Type Code 01. The "option Vendor.swsupply2" uses Type Code 02 which the OpenScape Branch and OpenScape SBC do not accept for representing a CMP address

- b) If the DHCP Discover message sent by the OpenScape Branch upon bootup contains Option 60 Vendor Class Identifier equal to the value "OpenScapeBranch", the DHCP Server will return in the DHCP Offer Option 43 with one of the values not commented out in "option Vendor.swsupply" 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.swsupply" can be active at a time within this dhcp.conf file. In the example below, having either of the "option Vendor.swsupply" 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.swsupply"

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

```
option space Vendor;
option Vendor.swsupply code 1 = string;
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.swsupply "10.234.3.35";
# option Vendor.swsupply "cmp35.simpinstall.com";
# option Vendor.swsupply "10.234.3.35,10.234.2.206";
# option Vendor.swsupply "cmp35.simpinstall.com";
# option Vendor.swsupply
  "cmp35.simpinstall.com,cmp36.simpinstall.com";
match if option vendor-class-identifier =
  "OpenScapeBranch";
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 Branch and OpenScape SBC are 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 Branch or 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 Branch or OpenScape SBC will then accept that DHCP Offer from the second network interface (WAN) and use that interface to contact the CMP. If attempting to bring the OpenScape Branch up as Branch-SBC mode, then only have the DHCP Server configured to provide Option 43 on the WAN side interface of the OpenScape Branch. The OpenScape Branch and OpenScape SBC ignore 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 Branch or 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 "OpenScapeBranch". 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 Branch 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: OpenScapeBranch

- 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(es) 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 Branch or OpenScape Session Border Controller.

3.4.2.5 How to Add an OpenScape Branch Office to OpenScape Voice

Proceed as follows to add an OpenScape Branch to OpenScape Voice for Simplified Installation Options 1-5:

Prerequisites

Endpoint Profile must be created.

Adequate administrative permissions.

The connection to the OpenScape Voice system is up.

Step by Step

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

- 2) Select the **<Business Group>** in the **Available Business Groups** pull-down associated the Branch to be viewed.

The Business Group selected appears 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., branch offices) associated with the selected Business Group.

- 4) Proceed as follows to create a new OpenScape Branch endpoint:

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

The **General tab** dialog is displayed by default.

- b) Fill in the **Name**, select the **Registered** checkbox (indicates static Registered), select an Endpoint Profile in the **Profiles** selection list and configure **other required** fields in the general tab work area.

The register checkbox will be grayed out until the Type to be selected is **"Static"** on the **SIP** tab.

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 Branch is deployed as a SIP proxy and because it does not authenticate the subscribers that use the proxy to register with the OSV, the endpoint must not be configured as "Trusted".

When setting an OpenScape Branch endpoint as "Not Trusted", it is possible that OPTIONS requests sent as keep-alive are challenged by an OpenScape Voice which is not on the latest patch set (OSV V6: < PS23 ; OSV V7: < PS8). For this reason, OpenScape Branch supports sending these OPTIONS requests on a different port (e.g. 5062). As it doesn't expect to be challenged on these OPTIONS requests, it is then necessary to configure the port used by OpenScape Branch for these OPTIONS requests as "Trusted". When setting a port of an OpenScape Branch to "Trusted" in the Endpoint configuration, ensure that the port used for the OPTIONS requests is not the same port as used for other requests sent by OpenScape Branch. If they are the same, you would effectively turn off Digest Authentication for the branch office phones if

the RTP Parameter Srx/Sip/AuthTraverseViaHdrs is set to "RtpTrue" on OpenScape Voice. Please note that this RTP parameter is recommended to be set to "RtpFalse" in the OpenScape Voice Security Checklist.

- 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
 - **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) or Branch Office **endpoint** is now created.

The OpenScape "Branch" must now be further configured in the OpenScape Voice Assistant database.

- 5) To configure the OpenScape Branch 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 branch offices associated with the selected Business Group.

- 6) Proceed as follows to create a new branch office:

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

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

- b) Fill in the **Branch Office Name** and **Representative Endpoint** fields.
- c) Select a numbering plan for the branch office from the **Numbering Plan** selection list.
- d) Select an office code from the **Office Code** selection list.
- e) Select the routing area of the branch office 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.

When the Branch Office of the OpenScape Branch type is added to the OpenScape Voice Assistant, a record will be added to the OpenScape Branch Assistant's database. From that point the OpenScape Branch Assistant will be able to administer this Branch Office.

NOTICE:

The OpenScape Branch Assistant Overview work area will display the OpenScape Branch **Status** as **Inventory**.

- 7) Proceed as follows to remove an existing branch office from the Branch Office list:

- a) Click the **Delete** button.

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

3.4.2.6 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 Branch or OpenScape SBC for Simplified Installation Options 1-5:

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 Branch > Administration > Branch Office List > Edit an existing OpenScape Branch/SBC > Configuration Installation button**) must be enabled to allow communication between the CMP and OpenScape Branch.

Adequate administrative permissions.

The connection to the OpenScape Voice system is up.

Step by Step

- 1) Navigate to **Configuration tab** and select **OpenScape Branch** within the Navigation Bar in Common Management Platform.
- 2) Select the **Branch Office list** in the Navigation Tree under Administration.
The system presents the **Branch Office Overview** in the Work Area with a current list of all SBCs and branch offices.
- 3) Select the OpenScape Branch or SBC from the **OpenScape Branch Overview** in work area by checking the associated checkbox.
The Edit button becomes active the **Branch Office Overview** Work Area.
- 4) Click the **Edit...** button in work area.
The **Edit OpenScape Branch** 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., V2R0.01.12.
- 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., Advantech, Advantech 50i, X3250, X3550, SR530, 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 Branch** dialog appears.

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

The **Edit OpenScape Branch** dialog closes and the **OpenScape Branch Overview** window appears and the OpenScape Branch or OpenScape SBC is now updated.

3.4.2.7 How to Add Media Server Language Files to the CMP Repository

Proceed as follows to add media server language files to the Media Server Language Files Repository in the Common Management Platform (CMP). These files are used for OpenScape Branch for Simplified Installation Options 1-5. Language files must be placed into the Media Server Language Files Repository prior to being assigned to an individual OpenScape Branch.

Prerequisites

Adequate administrative permissions.

The connection to the OpenScape Voice system is up.

Step by Step

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

The system presents the **General Settings** dialog with the **Installation** tab display as the default.
- 3) Click the **Add...** button in the **Media Server language files** work area.

The **Add language files to Media server** dialog is displayed.
- 4) Click the **Browse...** button in the work area.

The browser dialog is displayed.
- 5) Select a Media Server Language file.

The file format must be RPM (.rpm). The maximum size of a single file should not exceed 70 MB and is limited to 2 files.
- 6) If additional files are required Click the **Browse...** button for associated with the next file to be added and browse to select another Media Server Language file.

- 7) Click the **Save** button.

The **Add language files to Media sever** dialog closes and the **General Settings** dialog is updated with the current language files in the Media Server Language Repository.

- 8) Click the **Save** button in the **General Settings** dialog to complete saving of the selected files.

The **General Settings** dialog closes and the **OpenScape Branch Overview** window appears and the Media Server Language Repository in the Common Management Platform (CMP) is now updated.

3.4.2.8 How to Configure Media Server Language Files for an OpenScape Branch

Proceed as follows to configure Media Server Language files to an OpenScape Branch for Simplified Installation Options 1-5:

Prerequisites

Language files to be assigned to an OpenScape Branch must be placed into the Media Server Language Files Repository.

Adequate administrative permissions.

The connection to the OpenScape Voice system is up.

Step by Step

- 1) Navigate to **Configuration tab** and select **OpenScape Branch** within the Navigation Bar in Common Management Platform.
- 2) Select the **Branch Office list** in the Navigation Tree under Administration.
The system presents the **Branch Office Overview** in the Work Area with a current list of all SBCs and branch offices.
- 3) Select the OpenScape Branch from the **OpenScape Branch Overview** in work area by checking the associated checkbox.
The Edit button becomes active the **Branch Office Overview** Work Area.
- 4) Click the **Edit...** button in work area.
The **Edit OpenScape Branch** dialog becomes active.
- 5) Click the **Configure Installation** button.
The **Installation info** dialog becomes active.
- 6) Select the **Media Server languages files** tab.
The **Media server language** dialog is displayed with a list of files for the OpenScape Branch.
- 7) Click the **Add...** button in the **Media Server language files** work area.
The **Add Media Server language files** dialog is displayed with a list of available languages.
- 8) Select a media server language files from the list of files. A maximum of one languages can be selected at a time.
- 9) Click the **OK** button.
The **Media Server languages files** dialog is updated with the selected media server language file displayed.

10) Repeat the add MS Language files steps to add additional media server language files.

11) Click the **OK** button.

The **Installation info** dialog closes and the **Edit OpenScape Branch** dialog appears.

12) Click the **OK** button.

The **Edit OpenScape Branch** dialog closes and the **OpenScape Branch Overview** window appears and the OpenScape Branch is now updated.

3.4.2.9 How to Configure ACD Announcement Files

Proceed as follows to configure ACD announcement files for the OpenScape Branch for Simplified Installation Options 1-5:

Prerequisites

Adequate administrative permissions.

The connection to the OpenScape Voice system is up.

Step by Step

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

2) Select the **Branch Office list** in the Navigation Tree under Administration.

The system presents the **Branch Office Overview** in the Work Area with a current list of all SBCs and branch offices.

3) Select the OpenScape Branch from the **OpenScape Branch Overview** in work area by checking the associated checkbox.

The Edit button becomes active the **Branch Office Overview** Work Area.

4) Click the **Edit...** button in work area.

The **Edit OpenScape Branch** dialog becomes active.

5) Click the **Configure Installation** button.

The **Installation info** dialog becomes active.

6) Select the **ACD announcement files** tab.

The **ACD announcement files** dialog is displayed with a list of available announcements for the OpenScape Branch.

7) Click the **Add...** button in the **ACD announcement files** work area.

The **Add Files to ACD Announcement** dialog is displayed.

NOTICE:

File must adhere to the following format: Only WAV audio files (.wav) with Bit Rate 128 kbps, Audio Sample Size:16 bit, Channels: Mono. Sampling Rate: 8 KHz, Audio Format: PCM. The maximum file size must not exceed 50 MB per file. The maximum total size for ACD announcements must not exceed 100 MB.

- 8) Click the **Browse...** button in the work area.
The browser dialog is displayed.
- 9) Select an ACD announcement file.
- 10) Add additional files as required. If additional files are required Click the "Add another File" **Add** button and browse to select another ACD announcement file.
- 11) Click the **Save** button.
The **ACD announcement files** dialog is updated and the **ACD announcement files** dialog (tab) appears with the selected ACD announcement files displayed.
- 12) Click the **OK** button.
The **Installation info** dialog closes and the **Edit OpenScape Branch** dialog appears.
- 13) Click the **OK** button.
The **Edit OpenScape Branch** dialog closes and the **OpenScape Branch Overview** window appears and the OpenScape Branch is now updated.

3.4.2.10 How to Configure ACD Music on Hold Files

Proceed as follows to configure ACD Music on Hold files for the OpenScape Branch for Simplified Installation Options 1-5:

Prerequisites

Adequate administrative permissions.

The connection to the OpenScape Voice system is up.

Step by Step

- 1) Navigate to **Configuration tab** and select **OpenScape Branch** within the Navigation Bar in Common Management Platform.
- 2) Select the **Branch Office list** in the Navigation Tree under Administration.
The system presents the **Branch Office Overview** in the Work Area with a current list of all SBCs and branch offices.
- 3) Select the OpenScape Branch from the **OpenScape Branch Overview** in work area by checking the associated checkbox.
The Edit button becomes active the **Branch Office Overview** Work Area.
- 4) Click the **Edit...** button in work area.
The **Edit OpenScape Branch** dialog becomes active.
- 5) Click the **Configure Installation** button.
The **Installation info** dialog becomes active.
- 6) Select the **ACD music on Hold files** tab.
The **ACD music on Hold files** dialog is displayed with a list of available announcements for the OpenScape Branch.

- 7) Click the **Add...** button in the **ACD music on Hold files** work area.
The **Add Files to ACD Music on hold** dialog is displayed.

NOTICE:

File must adhere to the following format: Only WAV audio files (.wav) with Bit Rate 128 kbps, Audio Sample Size:16 bit, Channels: Mono. Sampling Rate: 8 KHz, Audio Format: PCM. The maximum file size must not exceed 50 MB per file. The maximum total size for ACD Music on hold must not exceed 100 MB.

- 8) Click the **Browse...** button in the work area.
The browser dialog is displayed.
- 9) Select an ACD music on Hold file.
- 10) Add additional files as required. If additional files are required Click the "Add another File" **Add** button and browse to select another ACD music on Hold file.
- 11) Click the **Save** button.

The **ACD Music on Hold files** dialog is updated and the **ACD music on Hold files** dialog (tab) appears with the selected ACD music on Hold files displayed.

NOTICE:

If **ACD Music on Hold (ACD MOH)** File is configured and OSB is in Proxy-ACD mode, **ACD MOH** will be used when OSB receives hold request (SDP with "inactive" attribute) regardless if OSB operates in normal mode or in survivability mode without having **Enable Music On Hold for Gateways and Subscribers** survivability feature active on OSB.

NOTICE:

In normal mode, OSV will send media attribute inactive, if MOH service is not available on subscriber or Media Server is not active. In this case, Asterisk MOH will be played. If MOH service is enabled on subscriber and Media Server is active, Media Server MOH will be played.

NOTICE:

In survivability mode, Media Server MOH will be played if **Enable Music On Hold for Gateways and Subscribers** survivability feature is active. If **Enable Music On Hold for Gateways and Subscribers** survivability feature is not active, Asterisk MOH will be played.

- 12) Click the **OK** button.
The **Installation info** dialog closes and the **Edit OpenScape Branch** dialog appears.

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

The **Edit OpenScape Branch** dialog closes and the **OpenScape Branch Overview** window appears and the OpenScape Branch is now updated.

3.4.2.11 How to Configure Auto Attendant Announcement Files

Proceed as follows to configure Auto attendant announcement files for the OpenScape Branch for Simplified Installation Options 1-5:

Prerequisites

Adequate administrative permissions.

The connection to the OpenScape Voice system is up.

Step by Step

- 1) Navigate to **Configuration tab** and select **OpenScape Branch** within the Navigation Bar in Common Management Platform.
- 2) Select the **Branch Office list** in the Navigation Tree under Administration.
The system presents the **Branch Office Overview** in the Work Area with a current list of all SBCs and branch offices.
- 3) Select the OpenScape Branch from the **OpenScape Branch Overview** in work area by checking the associated checkbox.
The Edit button becomes active the **Branch Office Overview** Work Area.
- 4) Click the **Edit...** button in work area.
The **Edit OpenScape Branch** dialog becomes active.
- 5) Click the **Configure Installation** button.
The **Installation info** dialog becomes active.
- 6) Select the **Auto attendant announcement files** tab.
The **Auto attendant announcement files** dialog is displayed with a list of available announcements for the OpenScape Branch.
- 7) Click the **Add...** button in the **Auto attendant announcement files** work area.
The **Add Files to Auto attendant announcement** dialog is displayed.

NOTICE:

File must adhere to the following format: Only WAV audio files (.wav) with Bit Rate 128 kbps, Audio Sample Size:16 bit, Channels: Mono. Sampling Rate: 8 KHz, Audio Format: PCM. The maximum file size must not exceed 50 MB per file. The maximum total size for Auto attendant announcements must not exceed 100 MB.

- 8) Click the **Browse...** button in the work area.
The browser dialog is displayed.
- 9) Select an Auto attendant announcement file.

- 10) Add additional files as required. If additional files are required Click the "Add another File" **Add** button and browse to select another Auto attendant announcement file.

- 11) Click the **Save** button.

The **Auto attendant announcement files** dialog is updated and the **Auto attendant announcement files** dialog (tab) appears with the selected Auto attendant announcement files displayed.

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

The **Installation info** dialog closes and the **Edit OpenScape Branch** dialog appears.

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

The **Edit OpenScape Branch** dialog closes and the **OpenScape Branch Overview** window appears and the OpenScape Branch is now updated.

3.4.2.12 How to Configure the Data Configuration File

Proceed as follows to configure the data configuration file for the OpenScape Branch for Simplified Installation Options 1-5:

Prerequisites

Adequate administrative permissions.

The connection to the OpenScape Voice system is up.

Step by Step

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

- 2) Select the **Branch Office list** in the Navigation Tree under Administration.

The system presents the **Branch Office Overview** in the Work Area with a current list of all SBCs and branch offices.

- 3) Select the OpenScape Branch from the **OpenScape Branch Overview** in work area by checking the associated checkbox.

The Edit button becomes active the **Branch Office Overview** Work Area.

- 4) Click the **Edit...** button in work area.

The **Edit OpenScape Branch** 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 Branch.

- 7) Click the **Browse...** button in the work area.

The browser dialog is displayed.

- 8) Select an Data Configuration file.

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

NOTICE:

File must adhere to the following format: Only WAV audio files (.wav) with Bit Rate 128 kbps, Audio Sample Size:16 bit, Channels: Mono. Sampling Rate: 8 KHz, Audio Format: PCM. The total size must not exceed 10 MB.
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 Branch** dialog appears.

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

The **Edit OpenScape Branch** dialog closes and the **OpenScape Branch Overview** window appears and the OpenScape Branch is now updated.

3.4.2.13 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.

OpenScape load files have been uploaded to the CMP repository.

Step by Step

- 1) Navigate to **Configuration tab** and select **OpenScape Branch** within the Navigation Bar in Common Management Platform.
- 2) Select the **Branch Office list** in the Navigation Tree under Administration.
The system presents the **Branch Office Overview** in the Work Area with a current list of all SBCs and branch offices.
- 3) Select the OpenScape SBC from the **OpenScape Branch Overview** in work area by checking the associated checkbox.
The Edit button becomes active the **Branch Office Overview** Work Area.
- 4) Click the **Edit...** button in work area.
The **Edit OpenScape Branch** dialog becomes active with the General tab displayed by default.
- 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 Branch** dialog appears.
- 11) Click the **OK** button.
The **Edit OpenScape Branch** dialog closes and the **OpenScape Branch Overview** window appears and the OpenScape SBC is now updated.

3.4.2.14 How to Install Hardware for Simplified Installation

Proceed as follows to install an OpenScape Branch or 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 Branch Assistant is pre-loaded with all required installation software and Configuration file.

The USB stick is pre-loaded with all required installation software (Options 2-5).

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 1-3,5).

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

The OpenScape Branch or 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 Branch > General Tab** is unchecked.

The OpenScape SBC and OpenScape Branch is configured in OpenScape Branch Assistant with a Unique ID (MAC Address for Option 1, Logical ID for options 2-5), Software load, Hardware type, Media Server and Language files.

OpenScape Branch/SBC Access to CMP (unsecured port 4709) must be configured in the OpenScape Branch 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 2-5).
- 3) Power up the OpenScape Server.

The following installation functions take place:

- OpenScape Branch or OpenScape SBC will send a DHCP Request (Options 1-3, 5)
- 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 Branch or SBC will contact the CMP server.
- The Branch or SBC device is validated by the OpenScape Branch Assistant. For Option 1 the MAC address (LAN MAC) is used for validation and for Options 2-5, the logical ID is used for validation.
- The Branch or SBC sends a request for a list of installation files to the OpenScape Branch Assistant.
- The OpenScape Branch 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, any media files associated with the Media Server languages (other than the default languages), and any ACD/Auto Attendant files that need to be downloaded by the OpenScape device. OpenScape Branch Assistant also updates the device state in the GUI.
- The OpenScape device Server installs the files using HTTP(s) based on information in the file provided by OpenScape Branch Assistant.
- Once the EZ-Install has completed normal operation, for Option 5 (Hosted Management via VPN) the VPN connection, used for hosted management operation, will be established to be used by the OpenScape Branch.
- A final boot is required to apply the xml file data and activate the software (SW) version download from the CMP.
- The OpenScape device logs the error cases and will also send alarms if possible.

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

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

- **Inventory** - Indicates the OpenScape Branch or OpenScape SBC system is configured in the Assistant but not installed.
 - **Authenticated** – Indicates the OpenScape Branch or OpenScape SBC platform has contacted the OpenScape Branch Assistant with all appropriate credentials.
 - **Installation started** – Indicates that the OpenScape Branch or 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 Branch or OpenScape SBC.
 - **File Transfer Successful.**
 - **File Transfer failed:** <filename>-<HttpErrorCode> - Indicates that one of the file has failed to transfer.
 - **Bootting** - Indicates the Boot of the OpenScape Branch or OpenScape SBC has started.
 - **Boot Failed** (and reason if provided) - Indicates that the OpenScape Branch or 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 OSB 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 OSBs) 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 device alerts when the installation is complete. If the Installation is successful the OpenScape Device will beep once, pause, and repeat. Beeps will occur for 10 cycles.

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

3.4.2.15 How to Troubleshoot Installation Errors and Alarms

The OpenScape Branch and Assistant will provide error log information locally. This information must be retrieved manually. The OpenScape device will provide audible beeps, if hardware supports, to the installer so the installer can

determine the nature of the problem. If the OpenScape 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 Branch will abort installation and fallback to the default IP 192.168.0.1 (park state). After the issues are resolved, the OpenScape Branch can be restarted and the simplified installation process will be restarted.

- 2) 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 device
- DHCP server not configured to return CMP URL

- 3) 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>:<Branch Office/SBC Name>

- 4) 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 device
- SOAP Requests received that have invalid data

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

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

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

- **Inventory** - Indicates the OpenScape Branch or OpenScape SBC system is configured in the Assistant but not installed.
- **Authenticated** – Indicates the OpenScape Branch or OpenScape SBC platform has contacted the OpenScape Branch Assistant with all appropriate credentials.
- **Installation started** – Indicates that the OpenScape Branch or 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 Branch or OpenScape SBC.
- **File Transfer Successful.**
- **File Transfer failed:** <filename>-<HttpErrorCode> - Indicates that one of the file has failed to transfer (error log file only).
- **Bootting** - Indicates the Boot of the OpenScape Branch or OpenScape SBC has started.
- **Boot Failed** - Indicates that the OpenScape Branch or 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.
- **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 OSB 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 Branch log file name is **autoinstall.log** under the following directory **/opt/siemens/openbranch/var/log/openbranch/**
- 6) Power up the OpenScape Server once the errors have been corrected.
- The **Communicating over Secured channel** checkbox for the OpenScape Branch configuration in the OpenScape Branch Assistant must be unchecked (Unsecured mode) to allow installation and reinstall an OpenScape SBC.
- 7) The OpenScape device alerts when the installation is complete. If the Installation is successful the OpenScape Device will beep once, pause, and repeat. Beeps will occur for 10 cycles.

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

3.5 Storage of Phone Software Loads - Overview

This feature provides the functionality to store several phone software loads locally on an OpenScape Branch allowing the software to then be redistributed locally to the phones in the branch. This avoids the need to download each individual phone from a ftp/HTTPS Server and therefore reduces uplink transport bandwidth issues that may arise due to the size of the phone software and contention with voice traffic for the bandwidth, especially in busy traffic hours.

Overview

The Storage of Phone Software Loads feature is used for the following:

- This functionality is initially intended to support Unify phones that support retrieving phone software from HTTPS Servers (i.e. OpenStage phones).
 - OpenStage 15, 29 and 40 phones (one software image)
 - OpenStage 60 and 80 phones (one software image)
- The scope of this feature does not include the following:
 - phones to retrieve phone software from OpenScape Branch via ftp i.e. Optipoint phones are not supported.
 - OptiClient
 - 3rd party SIP phones
- This feature is supported for the OpenScape Branch devices that run on the Advantech SYS-2USM02-6M01E Server i.e. OpenScape Branch 50i, new OpenScape Branch 250.

NOTICE:

The existing OSB 50 and OSB 250 will now only be offered on the same HW that is used today for the OSB 50i (Advantech SYS-2USM02-6M01E Server) and that the

OSB 50 will no longer be sold but the customer can still purchase the OSB 250 and licenses for only 50 users. OSB 250 (including customers with only 50 users) is supported for this feature as long as the OSB250 is running on the Advantech SYS-2USM02-6M01E Server.

- OpenScape Branch 1000 and OpenScape Branch 6000 branches are supported but it may become necessary to provide a separate HTTPS Server due to the large number of phones that would be trying to retrieve phone software from the local OpenScape Branch device.
- The Central HTTPS phone software server and all OpenScape Branch device with an OpenScape Branch phone software repository must have a common root path where all phone software resides.
- Alarming and logging is provided for blocking conditions when files are downloaded to the OpenScape Branch or uploaded to the phones.
- The transfer of phone software to the OpenScape Branch is only supported during off-hours.

Basic Operation

The solution provides a means for the phones to download phone software from the local OpenScape Branch. This creates a more efficient utilization of the branch's uplink transport bandwidth, and with that, the maintenance of better voice quality service as the uplink doesn't get overloaded especially in busy traffic hours.

Step 1: Phone sw is loaded onto a "Central" HTTPS phone software Server.

Step 2: OpenScape Branch syncs (Mirrors) in the middle of the night with the Central HTTPS phone software Server (port 444) to ensure the OpenScape Branch has the latest phone software.

Step 3: DLS software instructs the phones to go to the local OpenScape Branch to obtain updated phone software.

Step 4: Phones use existing functionality and interfaces obtain phone software from the local OpenScape Branch device.

3.5.1 How to Configure Phone Software Storage in the OpenScape Branch

Proceed as follows to configure Phone Software Management for OpenScape Branch devices:

Prerequisites

Adequate administrative permissions.

The Central HTTPS phone software server is configured to interwork with the OpenScape Branch(s) and operational (via CMP GUI - port 444)

The connection to the OpenScape Voice system is up.

Step by Step

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

- 2) Select the **Branch Office list** in the Navigation Tree under Administration.

The system presents the **Branch Office Overview** in the Work Area with a current list of all SBCs and branch offices.

- 3) To view a list of SBCs and Branch Offices 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 branch office use one of the following options:
- In the Work Area select the checkbox to the left of the particular SBC or branch office in the list and select **Manage**. Selecting the **Manage** button updates the **Branch Office** field, in the Navigation Tree, with the selected SBC or branch office and displays information and data in the Work Area for that SBC or branch office.
 - Choose a SBC or branch office from the **Branch Office** pull-down located in the Navigation Tree. Information and data are displayed in the Work Area.

- 5) (V8 OSB) Select the Enable phone management software checkbox and click the associated Configure button. (Pre V8 OSB) Select the **Phone Software** in the Navigation Tree under **Administration > Configuration**.

The system presents the **Phone Software Management** dialog with the **General tab** displayed by default.

- 6) Proceed as follows to assign the general configuration of phone software management for mirroring the central HTTPS server phone software in the OpenScape Branch:
- a) Check the **Enable** checkbox in the General tab work area to allow phone software management.

The associated management functions become active including the **Available phone software tab**.
 - b) Check the **Enable** checkbox under **Periodic OSB pulling software from central server** area in the General tab work area to allow the latest phone software to be downloaded to the OpenScape Branch.

The associated management functions become active.
 - c) Enter the **Start time**, in 24 hour format, for download of phone software from the Central HTTPS server phone software server to the OpenScape Branch. The default time is 2 am.
 - d) Enter the **Stop time**, in 24 hour format, to stop the download of phone software from the Central HTTPS server phone software server to the

OpenScape Branch if the download has not completed. The default time is 6 am.

- e) Enter the location of the Central HTTPS phone software server in the **Central phone software server URL:** field. The URL shall point to the Phone Software Repository (port 444).
- f) Click to **Start now** key (optional step) to manually initiate a download of phone software from the Central HTTPS phone software server to the OpenScape Branch.

The central phone software is downloaded into the OpenScape branch.

The available phone software can then be viewed in the **Available phone software** tab work dialog once the download is complete.

- g) Click the **OK** key to save the General Phone Management configuration.

When the General Phone Management configuration is added to the OpenScape Branch, from that point the phone software will be mirrored from the Central HTTPS phone software server to the OpenScape Branch.

- 7) Proceed as follows to enable phones to upload the latest phone software from the OpenScape Branch phone software repository:
 - a) Select the **Available phone software** tabsheet.
 - b) Check the **Enable** checkbox in the work area to allow phones to upload (pull) software from the OpenScape Branch.

The associated management functions become active.

- c) Select the number of phones from the **Maximum parallel access** pull-down that can simultaneously upload phone software from the OpenScape Branch. The default is 3 phones.
- d) Click the **OK** key to save the configuration.

When the configuration is added to the OpenScape Branch, from that point phones can upload software from the OpenScape Branch.

- 8) Proceed as follows to view and delete available phone software images in the OpenScape Branch phone software repository:
 - a) Select the **Available phone software** tabsheet.

Software phone images are displayed with the associated name in the **Name** column.

- b) To delete a phone software image, place a checkmark in the checkbox associated with the image to be deleted.

The **Delete** key become active.

- c) Click to **Delete** key to remove the selected phone images
- d) Click the **OK** key to save the configuration changes.

When the Phone Software Management dialog closes.

The Phone Software Management settings are complete and operational.

3.6 OpenScape Branch and OpenScape SBC Licensing Files

For OpenScape Branch, 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 Branch/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 Branch or OpenScape SBC is deployed at a customer who does not have a Common Management Platform (CMP) with OpenScape Branch Assistant or the CMP is not upgraded to a version that supports OpenScape Branch licensing.

The stand alone license file must have been previously generated and supplied to the customer, using the MAC ID of the OpenScape Branch or SBC. These customers use the OpenScape Branch or OpenScape SBC local GUI to manage the OpenScape Branch or 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.

OpenScape Branch License file:

The following types of files are contained in the OpenScape Branch License file:

- OpenScape Branch Base Licenses (maximum allowed 3,000)
- OpenScape Branch Registered Line Licenses (maximum allowed 100,000)
- Auto Attendant Licenses (maximum allowed 3,000)
- Backup ACD Licenses (maximum allowed 3,000)

OpenScape SBC License File:

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 Branch and OpenScape SBC license type.

OpenScape Branch File:

- 3,000 OpenScape Branch Base Licenses
- 100,000 OpenScape Branch Registered Line Licenses
- 3,000 Auto Attendant Licenses
- 3,000 Backup ACD Feature Licenses

OpenScape SBC file:

- 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:

OpenScape Branch File:

- 1 OpenScape Branch Base License (if evaluating OSB)
- 1 Auto Attendant Feature License (if evaluating OSB)
- 1 Backup ACD Feature License (if evaluating OSB)
- 50 OpenScape Branch Registered Line Licenses (if evaluating OSB)

OpenScape SBC File:

- 1 OpenScape SBC Evaluation License (if evaluating SBC)
- 100 OpenScape SBC Session Licenses (if evaluating OSB or SBC)

Redundancy

For redundant OpenScape systems the active node populates its' licensing to the backup node. No additional licenses are required.

3.6.1 OpenScape Regular License File (OSB and SBC)

OpenScape Branch Assistant supports Regular License files. The Regular license is a customer purchased license that does not expire.

License Functionality

- The OpenScape Branch Regular license file provides the license types and quantities necessary for a customer to use OpenScape Branch functionality, including Branch base functions, Branch Users, Auto Attendant feature, Backup ACD feature without expiration
- 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 Branch Assistant is informed by the License Management service that a new RLF license file has been applied including the total number of OpenScape Branch licenses for each license type and the expiration date of the license file. OpenScape Branch 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 Branch Assistant provides a popup to inform the craft the RLF license file does not have enough licenses. In this situation OpenScape Branch 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 Branch Assistant will check-out the licenses for each device.
- The OpenScape Branch 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 Branch Assistant tab.
- If OpenScape Branch Assistant is informed by the License Management service that an RLF license file has expired, the OpenScape Branch 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.

3.6.2 OpenScape Software Subscription License File (OSB and SBC)

OpenScape Branch 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 Branch 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 Branch. 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 Session Border Controller V2 Product Instance for Service Provider Licensing
 - OpenScape Session Border Controller V2 Product Instance for Enterprise Licensing

- **Subscription License-** The following licenses are provided via SSL Licensing:
 - Monthly Subscription License Service Provider OpenScape Session Border Controller Session License (per session)
 - Monthly Subscription License Enterprise Provider OpenScape Session Border Controller Session License (per session)

License Functionality

- The OpenScape Branch Software Subscription licenses provide the capability for a customer to use OpenScape Branch functionality, including Branch base features, Branch Users, Auto Attendant feature, Backup ACD feature for the length of the software subscription.
- 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 Branch 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 Branch Assistant.
- If OpenScape Branch Assistant is informed by the License Management service that a Regular License File (RLF) license file has expired, the OpenScape Branch 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 Branch 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 Branch License usage counters are calculated on every counter change and written to OpenScape Branch 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

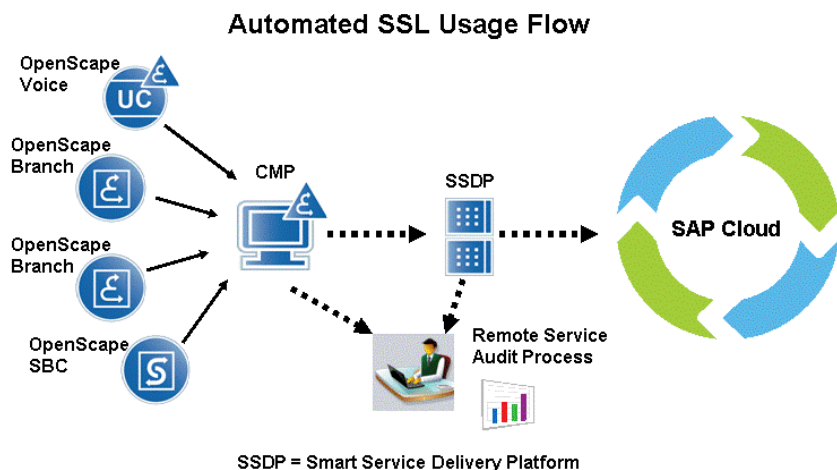
- A monitoring and reporting mechanism resides in the OpenScape Branch Assistant and CMP License Management Server for support of Software Subscription Licensing (SSL).
- OpenScape Branch Assistant provides calculation and reporting of OpenScape Branch User and OpenScape SBC Session license usage.

3.6.2.1 OpenScape Software Subscription License (SSL) Monitoring and Reporting - Details (OSB and SBC)

OpenScape Branch Assistant supports Software Subscription License (SSL) files with monitoring and reporting capabilities in Version 7 and beyond.

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 Branch User Usage:**
 - For the OpenScape Branch User the usage is calculated based on the statically configured license usage.
 - OpenScape Branch User usage is defined as the high watermark for the number of consumed OpenScape Branch Registered Line Licenses in the month.
- **OpenScape SBC Session Usage:**
 - For the OpenScape SBC Session usage a “mixed” model is followed. The usage on the OpenScape Branch is calculated based on the statically configured license usage, while the usage on the OpenScape SBC is calculated based on the concurrent 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 Branch/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 Branch Assistant whenever SSL usage data is reported to the SSL service.

CMP License Management service updates the a usage counter for the following:

- Whenever a modification is done in the number of the total configured OpenScape Branch Registered Line Licenses. If the modified number of total configured licenses 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 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 Branch Assistant and SBC Assistant Usage Calculation

OpenScape Branch 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 be 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 Branch Assistant updates the a usage counter for the following:

- Whenever an update is done in the total configured OpenScape SBC sessions (case of OpenScape Branch) or in the number of the simultaneously actually used OpenScape SBC sessions (case of OpenScape SBC). 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 Branch Assistant resets the usage counter to the current value of the corresponding counter.

NOTICE:

In case of redundant systems, OpenScape Branch Assistant takes into consideration only the licenses of the Master Node.

OpenScape Branch Assistant and SBC Assistant License Management Interface with the SSL Service

OpenScape Branch 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 Branch Assistant performs the following:

- retrieves the usage counter of the OpenScape Branch User from the License Management service.
- reports the SSL usage counters for OpenScape Branch User and OpenScape SBC session to SSL service.
- request license information (OpenScape SBC Session usage included) from the OpenScape SBC appliances.
- reports the SSL usage counters for OpenScape Branch User and OpenScape SBC session to SSL service

The OpenScape Branch 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 received for the month. This shall be reported as a string with format: yyyy-mm-dd hh:ss	16 characters	numeric plus "-" and "." characters
Violation	The violation flag indicates whether the license of the affected product is violated.	1 character	true / false

In addition, OpenScape Branch 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 Branch Assistant
- SSL Node Group - N/A (an empty string)

The additional parameters are not needed for SAP.

3.6.3 OpenScape Evaluation License File (OSB and SBC)

OpenScape Branch 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 Branch Evaluation license file provides the license types and quantities necessary for a customer to evaluate OpenScape Branch functionality, including Branch base functions, Branch Users, Auto Attendant feature, Backup ACD feature for up to 180 days.
- 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 Branch 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 Branch Assistant.
- If OpenScape Branch Assistant is informed by the License Management service that an Evaluation license file has expired, the OpenScape Branch 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.

3.6.4 OpenScape Branch Base License Type (OSB only)

The OpenScape Branch Base license type provides full usage of the basic switch software.

The OpenScape Branch Base license type is not tied to a software release or hardware type. OpenScape Branch Base licenses are used to track the number of OpenScape Branch(s) in the field.

OpenScape Branch Base licenses are configured via the OpenScape Branch Assistant. The OpenScape Branch Assistant will then request the license from the existing License Management Service. If the OpenScape Branch Base licenses are not available, the OpenScape Branch Assistant will not allow the configuration of the Base License. The OpenScape Branch Assistant keeps track of the usage counters and displays the OpenScape Branch Base licenses assigned to OpenScape Branch devices.

An OpenScape Branch Base License is required for the following Branch types:

- OpenScape Branch - Proxy
- OpenScape Branch - SBC Proxy
- OpenScape Branch - Proxy ACD
- OpenScape Branch - Proxy ATA
- OpenScape Branch - Branch SBC

The maximum number of OpenScape Branch base licenses in a license file on the CMP is 3,000.

One OpenScape Branch Base License must be allocated and assigned to each OpenScape Branch managed by the CMP

3.6.5 OpenScape Branch Registered Line License Type (OSB only)

OpenScape Branch Registered Line Licenses control the number of lines that can register with an OpenScape Branch.

The OpenScape Branch Registered Line License type is not tied to a software release or hardware type. OpenScape Branch Registered Line Licenses are used to track the number of system-wide OpenScape Branch Users.

OpenScape Branch Registered Line Licenses are configured via the OpenScape Branch Assistant. The OpenScape Branch Assistant will then request the license from the existing License Management Service. If the OpenScape Branch Registered Line Licenses are not available, the OpenScape Branch Assistant will not allow the configuration of the User License. The OpenScape Branch Assistant keeps track of the usage counters and displays the OpenScape Branch Registered Line Licenses assigned to OpenScape Branch devices.

One OpenScape Branch Registered Line License is required for the registration of each line or device including phantom and secondary lines.

The number of User licenses in the license pool determines the following:

- The number of primary, phantom and secondary lines that can be registered concurrently.

Example: OpenScape Branch Keyset with 1 prime line, 1 phantom line and 1 secondary line would use 1 OpenScape Voice dynamic license and 3 OpenScape Branch Registered Line Licenses.

- The number of non-keyset DNs that can have one or more telephones/soft clients simultaneously registered on the system. One OpenScape Branch Registered Line License per registration request and one OpenScape Voice dynamic license per unique DN.

NOTICE:

Licenses that are purchased or included with a particular package only become available on the OpenScape Branch server when the license file is applied to the OpenScape Branch Assistant server and configured for the OpenScape Branch server. Until then, only the default number of licenses will be available on the OpenScape Branch server.

Upon SIP registration, the user is granted a single license from the pool of available licenses allocated to the OpenScape Branch server based on the rules stated above.

OpenScape Branch warning threshold occurs, as follows:

- If the User licenses allocated exceeds the configurable warning threshold (e.g. 80% of the assigned licenses), a warning is generated to the customer's system administrator. At this point, purchasing additional licenses may be necessary to provide a margin of safety.

Attempt to exceed user licensing:

- The number of allowed registrations is the number of user licenses + 10% for 1000 user licenses or less. The number of allowed registrations is the number of user licenses + 5% for over 1000 user licenses. Attempts to exceed these amounts will result in blocked registrations and a critical alarm is generated daily with text indicating registration(s) blocked due to insufficient user licenses. The alarm must be manually cleared.
- Registration is on a first come first served basis

Users may reside in the following Branch types:

- OpenScape Branch - Proxy
- OpenScape Branch - SBC Proxy

- OpenScape Branch - Proxy ACD
- OpenScape Branch - Proxy ATA
- OpenScape Branch - Branch SBC
- Remote 3rd party Branch device

After enforcement is initiated and the license pool is completely depleted by the number of incoming SIP registered users, the next endpoint is denied registration and is unable to originate or terminate calls, including emergency calls.

3.6.6 OpenScape Branch Auto Attendant License (OSB only)

An OpenScape Branch Auto Attendant license allows access to Auto Attendant features.

Auto Attendant feature licenses are configured via the OpenScape Branch Assistant. An Auto Attendant feature license is optional and need not be purchased if Attendant functionality is not required.

The maximum number of Auto Attendant licenses is 1 per OpenScape Branch.

3.6.7 OpenScape Branch Backup ACD (Automatic Call Distribution) License (OSB only)

OpenScape Branch Backup ACD licenses control access to the ACD backup communication links feature provided during survivability processing.

Backup ACD feature licenses are configured via the OpenScape Branch Assistant. A Backup ACD feature license is optional and need not be purchased if ACD Backup functionality is not required.

The maximum number of Backup ACD licenses is 1 per OpenScape Branch - Proxy ACD.

3.6.8 OpenScape Session Border Controller (SBC) Base License (SBC only)

The OpenScape Session Border Controller (SBC) Base license provides full usage of the basic SBC software for a given version e.g. OpenScape SBC V2 base software.

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 Branch Assistant. The OpenScape Branch Assistant will then request the license from the Existing License Management Service. If the OpenScape SBC Base licenses are not available, the OpenScape Branch Assistant will not allow the configuration of the Base License. The OpenScape Branch 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

3.6.9 OpenScape SBC Session License (OSB and SBC)

OpenScape SBC Session licenses are shared between OpenScape Branch and OpenScape SBC, and control the maximum number of connections to OpenScape SBC and OpenScape Branch SBC.

OpenScape SBC Session licenses are configured via the OpenScape Branch Assistant. The OpenScape Branch Assistant will then request the licenses from the existing License Management Service. If the OpenScape SBC Session licenses are not available, the OpenScape Branch Assistant will not allow the configuration of the Session License. The OpenScape Branch 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).

3.6.10 Upgrade License - Overview

The OpenScape Upgrade Licenses are required when upgrading from an OpenScape Branch with pre-Version 2 software to an OpenScape Branch with Version 2 or later software; and is also required when upgrading from an OpenScape SBC with pre-Version 2 software to an OpenScape SBC Version 2 or later.

The enforcement of OpenScape License files begins with OpenScape Branch Version 2 and OpenScape SBC Version 2.

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 Branch and OpenScape SBC

The following applies to handling of software upgrades for OpenScape Branch and OpenScape SBC:

- OpenScape Branch Assistant upgrade from a version that does not support licensing to a version that does support licensing:
 - Prior to upgrading an OpenScape Branch or OpenScape SBC device in a customer network to a software release that supports OpenScape licensing, the OpenScape Branch Assistant must be upgraded to a revision that provides provisioning of OpenScape Branch and OpenScape SBC Licenses. If the OpenScape Branch Assistant is not upgraded, then licensing of Branch or SBC via Common Management Platform (CMP) is not possible. Stand Alone licensing must be used directly on the Branch or SBC.
 - The OpenScape Branch Assistant must be provisioned with the OpenScape Branch and OpenScape SBC licensing information; otherwise, the OpenScape devices will not allow licensed features to work when the OpenScape Branch or OpenScape SBC devices are upgraded and start requesting licensing information. A license file, generated with the MAC ID of the Assistant, must be applied to the Assistant.
- OpenScape Branch Assistant upgrade from a version that does support licensing:
 - OpenScape Branch and OpenScape SBC license data must be maintained whenever the OpenScape Branch Assistant is upgraded.
- After performing an OpenScape Branch or OpenScape SBC software upgrade from a release that did not support OpenScape Branch or OpenScape SBC licensing to a release that does support licensing, the OpenScape Branch or OpenScape SBC device will begin requesting licenses automatically.
- When performing an OpenScape Branch or OpenScape SBC software upgrade from a release that does support OpenScape Branch or OpenScape SBC licensing to a newer release, the upgrade is performed as usual and the device will begin to request its licenses automatically when it reconnects to the network.

OpenScape Branch Upgrade Licenses

The following Upgrade Licenses apply to OpenScape Branch:

- OpenScape Branch V2 Upgrade Base from Branch V1
- OpenScape Branch V2 Upgrade User from Branch V1
- OpenScape Branch V2 Upgrade Auto Attendant License from Branch V1
- OpenScape Branch V2 Backup ACD License from V1
- OpenScape SBC V2 Upgrade Session License from SBC V1

OpenScape SBC Upgrade Licenses

The following Upgrade Licenses apply to OpenScape SBC:

- OpenScape SBC V2 Upgrade Base License from SBC V1
- OpenScape SBC V2 Upgrade Session License from SBC V1

3.7 Managing Licenses

This chapter provides information about the following topics:

- License Management Concept
- License Information

- Activating Licenses

3.7.1 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.

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).

IMPORTANT:

Applying licenses requires SIP server to restart in OSB so this should be done in a maintenance window.

The licenses and their related information are displayed in Common Management Platform. The total number of licenses, which licenses are assigned to which OpenScape Branches or OpenScape SBCs, 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 Branch Assistant stores licensing information encrypted on the disk.

Licensing in Stand Alone Mode

Stand Alone Mode is defined as when an OpenScape Branch or OpenScape SBC is deployed at a customer who does not have a Common Management Platform (CMP) with OpenScape Branch Assistant or the CMP is not upgraded to a version that supports OpenScape Branch licensing. The standalone license file must have been previously generated and supplied to the customer, using the MAC ID of the OpenScape Branch or SBC. These customers use the OpenScape Branch or OpenScape SBC local GUI to manage the OpenScape Branch or 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.

3.7.2 License Information

This Common Management Platform (CMP) and the OpenScape Branch 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
- 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 Branch CMP supports display of Software Subscription License (SSL) information in Version 7 and beyond.

License Information via OpenScape Branch Assistant

The following information can be displayed using the OpenScape Branch Assistant:

- **General license information per Branch or 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 Branch or SBC
- when the license was last updated to the Branch or SBC

- **License thresholds**

License thresholds can be set and displayed for the following license types:

- OpenScape Branch Base
- OpenScape SBC Base
- OpenScape Branch Users
- Auto Attendant feature
- Backup ACD feature
- 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.

3.7.2.1 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 **License** navigation menu item.
- 2) Select **Information** in the navigation tree.

- 3) A list of all features available in the OpenScape system is displayed in the work area. This list contains for each entry the following information:

Product Name

Shows the name of the product for which the license information is being displayed e.g., OpenScape Branch / SBC V2.

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).
- Enter the desired filter term in the field Pattern. You can either enter the complete term or the initial letters followed by * (e. g. *HiPath*).
 - From the list displayed, select whether the filtering is to be applied to the Product Name or Feature Name column.
 - Click on **Go** to activate the filter. Only the list elements which correspond to the pattern entered are displayed.
 - 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.
- Click the **CSV icon** in the work area to the right of the Items/Page controls.
 - From the File Download dialog select **Save**.
 - Enter the **Save in:** location and **File Name** and click on **Save**.
 - The CSV file is saved and the **License Information** work area appears.

3.7.2.2 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

- On the **Maintenance** navigation tab click on the **License** navigation menu item.
- 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 name of the node for which the license information is being displayed e.g., bocaosb1.

Node Type

Indicates the type of node associated with subscription license reported e.g., OpenScape Branch, OpenScape Branch/SBC.

License Type

Indicates the type of subscription license reported e.g., OpenScape Branch User, OpenScape Branch Session.

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 days left in the subscription licenses for the node. e.g., 155 days.

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).
- Enter the desired filter term in the field Pattern. You can either enter the complete term or the initial letters followed by * (e. g. *HiPath*).
 - From the list displayed, select whether the filtering is to be applied to the Node Type or Product ID.
 - 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.

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

3.7.2.3 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 **License** 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**.

3.7.2.4 How to Display License Information via OpenScape Branch Assistant

To display license information via the OpenScape Branch Assistant, proceed as follows:

Prerequisites

Adequate administrative permissions.

Step by Step

- 1) Navigate to **Configuration tab** and select **OpenScape Branch** within the Navigation Bar in 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 Branches, OpenScape Branch application features and OpenScape SBCs are displayed in the work area. This list contains for each entry the following information:

Name

Shows the name of the OpenScape Branch or OpenScape SBC for which the license information is being displayed.

License Type

Type of Licenses are as follows:

- OpenScape Branch Base
- OpenScape Branch Users
- Auto Attendant feature
- Backup ACD feature
- SBC sessions
- OpenScape SBC Base

Configured licenses

Specifies how many licenses are configured in the OpenScape Branch Assistant for this logical device.

- OpenScape Branch Base (values - 0-1)
- OpenScape Branch Users (values - 0-6000)
- Auto Attendant feature (values - 0-1)
- Backup ACD feature (values - 0-1)
- 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 Branch or OpenScape SBC.

Last updated

Date and time when the license information was last updated between the CMP and OpenScape Branch or OpenScape SBC.

- 5) The Licences list can be filtered by Name.
- a) Enter the desired filter term in the field Pattern. You can either enter the complete term or the initial letters followed by * (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.

3.7.2.5 How to Display and Manage Licensing Thresholds via OpenScape Branch Assistant

This feature allows the administrator to manage the allocation of licenses by specifying the threshold values for licenses associated with OpenScape Branch and 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 Branch Assistant, proceed as follows:

Prerequisites

Adequate administrative permissions

Step by Step

- 1) Navigate to **Configuration tab** and select **OpenScape Branch** within the Navigation Bar in 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 Branch Base (%):

The default value is 80%, and the valid range is [0 % ...100 %].

OpenScape SBC Base (%):

The default value is 80%, and the valid range is [0 % ...100 %].

OpenScape Branch Users (%):

The default value is 80%, and the valid range is [0 % ...100 %].

Auto Attendant feature (%):

The default value is 90%, and the valid range is [0 % ...100 %].

Backup ACD feature (%):

The default value is 90%, 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.

3.7.2.6 How to Display Licensing for an OpenScape Branch Office or SBC Via OpenScape Branch Assistant

The OpenScape Branch Assistant can administer OpenScape Branch Offices and OpenScape SBCs. Thus it keeps a list of branch offices and SBCs in its database. The "OpenScape Branch Overview" displays all known branch offices

and provides a search function to find a particular one. The administrator can select a single OpenScape Branch or OpenScape SBC to view and configure.

Prerequisites

Adequate administrative permissions.

At least one OpenScape branch office or OpenScape 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 Branch** within the Navigation Bar in Common Management Platform.

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

If **All systems** is not currently selected, selecting All systems will display the **OpenScape Branch Overview** in the Work Area, with a current list of all known SBCs and branch offices of all systems. If no SBCs or branch offices are defined, the list is empty. If **All systems** was previously selected, then proceed to step 3.

3) Select **Branch Office list** in the Navigation Tree.

The system presents the **OpenScape Branch Overview** in the Work Area, with a current list of all known SBCs and branch offices of all systems. If no SBCs or branch offices are defined, the list is empty.

4) To view a list of SBCs and Branch Offices 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 find and select a particular branch office use one of the following options:

- In the Work Area select the checkbox to the left of the particular SBC or branch office in the list. Action Menu buttons are set active in the Work Area with the following options: **Manage**, **Password...**, **Refresh Selected**, **Edit...**, **Delete**. Selecting the **Manage** button updates the **Branch Office** field, in the Navigation Tree, with the selected SBC or branch office and displays information and data in the Work Area for that SBC or branch office.
- Choose a SBC or branch office from the **Branch Office** pull-down located in the Navigation Tree. Information and data are displayed in the Work Area.
- Enter filter search criteria to filter the list of SBC and branch offices.

Filtering is possible on the following criteria from the **in** field: **Branch Office** (name), **Business Group**, **IP Address**, **Version**, **Status**, **Mode**.

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

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

The system refreshes the list of displayed branch offices and displays the ones matching the search criteria.

- 7) Click The **Clear** button. The system clears the filter criteria field and displays all records of the default communication system selected in the **Communication System** field. If no specific communication system is selected, all SBCs and branch offices of all systems are listed in the Work Area.

- 8) 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 Branch or OpenScape SBC in the form of System Name:Business Group Name:OpenScape Branch or SBC Name.

Hw ID:

Unique Hardware ID associated with the hardware of the OpenScape Branch or OpenScape SBC.

License type

Type of Licenses are as follows: OpenScape Branch Base, OpenScape Branch Users, Auto Attendant feature, Backup ACD feature, SBC sessions and OpenScape SBC Base.

Configured

Specifies how many licenses are configured in the OpenScape Branch Assistant for this logical device.

Locally Configured

Specifies how many licenses are configured for this physical device, OpenScape Branch or SBC.

Usage (Peak)

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 Branch or OpenScape SBC from the OpenScape Branch Assistant database.

Device license update button

Used to request an update of license data from the OpenScape Branch Assistant, to the OpenScape Branch or OpenScape SBC device.

Configure button

Used to access configuration of licenses for the OpenScape Branch or OpenScape SBC. In addition, provides access to clear license counters at the OpenScape Branch and SBC devices.

- 9) Configuration and update of licenses can be accomplished for a single OpenScape Branch Office or OpenScape SBC.

The data displayed is provided by the OpenScape Branch assistant database and the OpenScape Branch or SBC hardware itself. This means that the data might be out of date if it was changed on the SBC or branch office without the assistant being notified. Refresh button must be used to synchronize data when changes are made.

3.7.2.7 How to Configure and Clear Licensing for an OpenScape Branch Office (or SBC Via SBC Assistant)

The OpenScape Branch Assistant can administer licensing for a particular OpenScape Branch Office or OpenScape SBC.

Prerequisites

Adequate administrative permissions.

At least one OpenScape branch office or 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 and branch offices: navigate to **Configuration tab > OpenScape Branch** (or OpenScape SBC) within the Navigation Bar in Common Management Platform.

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

If **All systems** is not currently selected, selecting All systems will display the **OpenScape Branch Overview** (or OpenScape SBC Overview) in the Work Area, with a current list of all known SBCs and branch offices of all systems. If no SBCs or branch offices are defined, the list is empty. If **All systems** was previously selected, then proceed to step 3.

- 3) Select **Branch Office list** in the Navigation Tree.

The system presents the **OpenScape Branch Overview** (or OpenScape SBC Overview) in the Work Area, with a current list of all known SBCs and branch offices of all systems. If no SBCs or branch offices are defined, the list is empty.

- 4) To view a list of SBCs and Branch Offices 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 find and select a particular branch office use one of the following options:

- In the Work Area select the checkbox to the left of the particular SBC or branch office in the list. Action Menu buttons are set active in the Work Area with the following options: **Manage**, **Password...**, **Refresh Selected**, **Edit...**, **Delete**. Selecting the **Manage** button updates the **Branch Office** field, in the Navigation Tree, with the selected SBC or

branch office and displays information and data in the Work Area for that SBC or branch office.

- Choose a SBC or branch office from the **Branch Office** pull-down located in the Navigation Tree. Information and data are displayed in the Work Area.
- Enter filter search criteria to filter the list of SBC and branch offices.

Filtering is possible on the following criteria from the **in** field: **Branch Office** (name), **Business Group**, **IP Address**, **Version**, **Status**, **Mode**.

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

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

The system refreshes the list of displayed branch offices and displays the ones matching the search criteria.

- 7) Click The **Clear** button. The system clears the filter criteria field and displays all records of the default communication system selected in the **Communication System** field. If no specific communication system is selected, all SBCs and branch offices of all systems are listed in the Work Area.

- 8) This Step should be executed when changing out OpenScape Branch or 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 Branch or 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 Branch or OpenScape SBC hardware.

The licenses on the OpenScape Branch or OpenScape SBC are cleared and the General OpenScape 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 Branch Assistant. This will link the licenses allocated to the device with the devices' hardware ID.

The General OpenScape work area appears.

- 9) Enter the number of licenses to be assigned to the OpenScape Branch Office or OpenScape SBC for each license type. The number of assigned licenses can not exceed the number of available licenses shown e.g.,

Available: 5017, for the associated license type. License types include the following:

- **OpenScape Branch Base** (for Branch)
- **OpenScape Branch Users** (for Branch)
- **Auto Attendant feature** (for Branch)
- **Backup ACD feature** (for Branch)
- **SBC Sessions** (for Branch or SBC)
- **OpenScape SBC Base** (for SBC)

- 10) Click the **Save** button to complete the assignment of licenses in the OpenScape Branch Assistant for the OpenScape Branch or OpenScape SBC device.

NOTICE:

This action also updates OpenScape Branch or OpenScape SBC licenses in the OpenScape hardware.

IMPORTANT: Applying or changing licenses assigned to an OSB will cause the OSB to restart the sip server process which will have an affect on transient (non-stable) calls.

Licenses are now allocated in the OpenScape Branch Assistant for the OpenScape Branch or OpenScape SBC and the General OpenScape work area appears.

- 11) Click the **Device license update** button, in the Licensing Information work area to update license information in the OpenScape Branch or OpenScape SBC device.

NOTICE:

This action transfers licensing information from the OpenScape Branch Assistant (OpenScape SBC) to the OpenScape Branch or OpenScape SBC hardware.

Licenses are now configured in the OpenScape Branch or OpenScape SBC hardware.

- 12) Click the **Refresh** button, in the Licensing Information work area to refresh the OpenScape Branch or OpenScape SBC licensing information from the OpenScape Branch Assistant only.

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

3.7.2.8 How to Display Licensing Warnings for an OpenScape Branch Office or SBC

The OpenScape Branch Assistant automatically displays licensing warnings to notify the administrator of possible licensing issues. Warnings can occur during display and configuration of OpenScape Branches and OpenScape SBCs.

Prerequisites

Adequate administrative permissions.

At least one OpenScape branch office or 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 Branch** (or OpenScape SBC) within the Navigation Bar in Common Management Platform.

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

If **All systems** is not currently selected, selecting All systems will display the **OpenScape Branch Overview** (OpenScape SBC Overview) in the Work Area, with a current list of all known SBCs and branch offices of all systems. If no SBCs or branch offices are defined, the list is empty. If **All systems** was previously selected, then proceed to step 3.

- 3) Select **Branch Office list** in the Navigation Tree.

The system presents the **OpenScape Branch Overview** (OpenScape SBC Overview) in the Work Area, with a current list of all known SBCs and branch offices of all systems. If no SBCs or branch offices are defined, the list is empty.

- 4) To view a list of SBCs and Branch Offices 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 find and select a particular branch office use one of the following options:

- In the Work Area select the checkbox to the left of the particular SBC or branch office in the list. Action Menu buttons are set active in the Work Area with the following options: **Manage**, **Password...**, **Refresh Selected**, **Edit...**, **Delete**. Selecting the **Manage** button updates the **Branch Office** field, in the Navigation Tree, with the selected SBC or branch office and displays information and data in the Work Area for that SBC or branch office.
- Choose a SBC or branch office from the **Branch Office** pull-down located in the Navigation Tree. Information and data are displayed in the Work Area.
- Enter filter search criteria to filter the list of SBC and branch offices.

Filtering is possible on the following criteria from the **in** field: **Branch Office** (name), **Business Group**, **IP Address**, **Version**, **Status**, **Mode**.

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

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

The system refreshes the list of displayed branch offices and displays the ones matching the search criteria.

- 7) Click The **Clear** button. The system clears the filter criteria field and displays all records of the default communication system selected in the **Communication System** field. If no specific communication system is selected, all SBCs and branch offices of all systems are listed in the Work Area.

- 8) Choose a particular OpenScape Branch or OpenScape SBC.

OpenScape Branch and OpenScape SBC associated information is displayed. 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.

- 9) Warnings can occur during display and configuration of OpenScape Branches and OpenScape SBCs.

The administrator is warned about licensing issues and can then correct the pending issue.

3.7.3 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.

IMPORTANT:

Applying licenses requires SIP server to restart in OSB so this should be done in a maintenance window.

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.

3.7.3.1 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 Branch Assistant version supports OpenScape Branch/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 **License** 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 Branches or OpenScape SBCs.

3.7.3.2 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 are 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 Branches or OpenScape SBCs.

3.7.4 License Enforcement and Update

This Common Management Platform (CMP) and the OpenScape Branch 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
User license (OSB only)	- If no Licenses of any type are available, operate as today but alarm daily. After 30 days of no licenses block all registrations. - If licenses of any type are provided during the 30 day period OpenScape Branch begins to operate based on the licenses available.	Attempts to exceed license: - The number of allowed registrations is the number of user licenses + 10% for 1000 user licenses or less. The number of allowed registrations is the number of user licenses + 5% for over 1000 user licenses. Attempts to exceed these amounts will result blocked registrations and a critical alarm is generated daily with text indicating registration(s) blocked due to insufficient user licenses. The alarm must be manually cleared. - Registration is on a first come first served basis

	Install / Upgrade License Enforcement	Operation License Enforcement
SBC Session license (OSB and SBC)	- 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 Branch or 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.
Attendant license (OSB Only)	- If no Licenses of any type are available, operate normal but alarm daily. After 30 days of no licenses calls to the Attendant are not possible (all calls are blocked). - If licenses of any type are provided during the 30 day period OpenScape Branch begins to operate based on the licenses available.	Attempts to exceed license: Reject calls to the Attendant with response code 606 (a warning header may be included for diagnostic purposes) and a critical alarm is generated daily with text indicating Attendant calls blocked due to no Attendant License. The alarm must be manually cleared.
Backup ACD license (OSB only)	- If no Licenses of any type are available, operate normal but alarm daily. After 30 days of no licenses calls going into the queue are not possible (all calls are blocked). - If licenses of any type are provided during the 30 day period OpenScape Branch begins to operate based on the licenses available.	Attempts to exceed license: Reject calls to Backup ACD with response code 606 (a warning header may be included for diagnostic purposes) and a critical alarm is generated daily with text indicating Backup ACD calls blocked due to no Backup ACD. The alarm must be manually cleared.

• Additional Enforcement Scenarios and Responses

Scenarios:

- OpenScape Branch and 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 Branch or OpenScape SBC has successfully received license information from

OpenScape Branch 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 Branch 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 Branch 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 Branch or 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 Branch or OpenScape SBC will operate normal for 30 days and generate a daily alarm with text indicating how many days before the OpenScape Branch or OpenScape SBC will not provide any calls since no licenses are installed.

License Update

The OpenScape Branch and OpenScape SBC requests licensing update for the following:

- after every reboot
- after changing from survivable mode to normal mode (OpenScape Branch)
- every 24 hours (based on the last reboot time)

License Validation

The OpenScape Branch and OpenScape SBC validate licenses periodically with the central License Server (CMP). If validation fails, additional attempts are made to validate licenses:

- OpenScape Branch/OpenScape SBC to License Server (CMP) Validation:
The OpenScape Branch/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 a 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 Branch/OpenScape SBC to the License server (CMP) is restored within the grace period; the grace period operation returns to normal (30 days).
- If the grace period expires, licensed features will stop working (e.g. OSB users cannot place calls, ACD will not work, Attendant will not work, SBC Sessions will not be allowed).

Subscribers that are registered will continue to work unless the user's phone is powered off. When the phone is powered on the user will not

register and won't be able to make calls. Attempts to register new users after the 30 day grace period expires will be unsuccessful.

Periodic checking from the OpenScape Branch/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 (30 days).

- The Network must be fixed to allow communication between the OpenScape Branch and the License server (CMP) for centralized license operation. Stand-alone licensing can be used at the OpenScape Branch/OpenScape SBC to bring operation back to normal (Notice: The OpenScape Branch/OpenScape SBC must be configured for Stand Alone license operation).
- Number of Users in the OpenScape Branch Exceeds the Number of Allowed Registered Users: If the number of users in the OpenScape Branch exceeds the number of allowed registered users, additional registrations are allowed. The number of additional registrations allowed depends on the OpenScape Branch type.

3.7.5 License Security

This Common Management Platform (CMP), OpenScape Branch and OpenScape SBC secures licensing information in the following ways:

Securing Licensing in the OpenScape Branch and OpenScape SBC

- Licensing information stored in the OpenScape Branch and OpenScape SBC is secured by encryption.
- The OpenScape Branch and OpenScape SBC automatically sets the Branch or 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 and are usable after restore.

Securing Licensing in the OpenScape Branch Assistant

- Licensing information stored in the OpenScape Branch Assistant is secured by encryption. Secured information includes the Logical-IDs, MAC addresses, Authentication Statements and License counts
- The OpenScape Branch 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 encrypted and persist over restarts and upgrades.

4 OpenScape Branch Assistant – Configuration

In the main navigation area of the OpenScape Branch Assistant the instances of the OpenScape Branch appliance can be configured.

OpenScape Branch V1R3, V1R4, V2, V7 and V8

The OpenScape Branch Assistant can be used to display and configure OpenScape Session Border Controllers and OpenScape Branch Offices. The online Help system may describe features that are not available for pre-V8 versions of OpenScape Branch and some procedures may deviate from the ones described.

Note: The Navigation Tree presented for the V8 OSB is quite different from the Pre V8 OSBs. The specific details are documented in the specific sections of this document.

4.1 Alarm Configuration Overview

The Alarms section under Configuration allows to display and configure the alarm settings and trap destinations for the OpenScape Branch appliance.

The OpenScape Branch 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-EventId).
- Manually delete an alarm identified by GroupId-EventId.
- 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 Branch appliance.

The OpenScape Branch Assistant Plug-in receives SNMP (Simple Network Management Protocol) traps from one or more OpenScape Branch appliances. Alarms received by OpenScape Branch appliances will be stored in the Assistant database.

Alarm Settings

The OpenScape Branch 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 "port number". It is possible to configure the same IP address for more than one trap destination. 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 Branch 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 Alarm 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 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 Branch** within the Navigation Bar in the Common Management Platform.
- 2) Select the **Branch Office list** in the Navigation Tree under Administration.

The system presents the **Branch Office Overview** in the Work Area with a current list of all branch offices.

- 3) To view a list of Branch Offices 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 branch office use one of the following options:
 - In the Work Area select the checkbox to the left of the particular branch office in the list and select **Manage**. Selecting the **Manage** button updates the **Branch Office** field, in the Navigation Tree, with the selected branch office and displays information and data in the Work Area for that branch office.
 - Choose a branch office from the **Branch Office** pull-down located in the Navigation Tree. Information and data are displayed in the Work Area.
- 5) Navigate to **Configuration > Alarms** in the navigation tree under Administration.

(V8 OSB) Next click on Alarm Settings. (Pre V8 OSB) 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 describes the alarm. It is closely related to the trap name as defined in the OpenScape 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 branch to branch, but it is fixed for a particular 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)
- Authentication (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)

4.1.1.2 How to Edit Alarm 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 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 Branch** within the Navigation Bar in Common Management Portal.
- 2) Select the **Branch Office list** in the Navigation Tree under Administration.
The system presents the **Branch Office Overview** in the Work Area with a current list of all SBCs and branch offices.
- 3) To view a list of SBCs and Branch Offices 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 branch office use one of the following options:
 - In the Work Area select the checkbox to the left of the particular SBC or branch office in the list and select **Manage**. Selecting the **Manage** button updates the **Branch Office** field, in the Navigation Tree, with the selected SBC or branch office and displays information and data in the Work Area for that SBC or branch office.
 - Choose a SBC or branch office from the **Branch Office** pull-down located in the Navigation Tree. Information and data are displayed in the Work Area.
- 5) Navigate to **Configuration > Alarms** in the navigation tree under Administration.
(V8 OSB) Next click on Alarm Settings. (Pre V8 OSB) 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 describes the alarm. It is closely related to the trap name as defined in the OpenScape Branch 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 branch to branch, 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.

4.1.1.3 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 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 Branch** within the Navigation Bar in the Common Management Platform.
- 2) Select the **Branch Office list** in the Navigation Tree under Administration.
The system presents the **Branch Office Overview** in the Work Area with a current list of all branch offices.
- 3) Select the **Branch Office list** in the Navigation Tree under Administration.
The system presents the **Branch Office Overview** in the Work Area with a current list of all branch offices.
- 4) To find and select a particular branch office use one of the following options:
 - In the Work Area select the checkbox to the left of the particular branch office in the list and select **Manage**. Selecting the **Manage** button updates the **Branch Office** field, in the Navigation Tree, with the selected branch office and displays information and data in the Work Area for that branch office.
 - Choose a branch office from the **Branch Office** pull-down located in the Navigation Tree. Information and data are displayed in the Work Area.
- 5) Navigate to **Configuration > Alarms** in the navigation tree under Administration.
(V8 OSB) Next click on Alarm Settings. (Pre V8 OSB) 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.

- 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. A maximum of 5 trap destinations can be configured.

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.

4.1.1.4 How to Display and Delete Trap Destinations

The configured trap destinations can be displayed.

Prerequisites

Adequate administrative permissions.

At least one 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 Branch** within the Navigation Bar in the Common Management Platform.
- 2) Select the **Branch Office list** in the Navigation Tree under Administration.

The system presents the **Branch Office Overview** in the Work Area with a current list of all branch offices.

- 3) To view a list of Branch Offices 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 branch office use one of the following options:
 - In the Work Area select the checkbox to the left of the particular branch office in the list and select **Manage**. Selecting the **Manage** button updates the **Branch Office** field, in the Navigation Tree, with the selected branch office and displays information and data in the Work Area for that branch office.
 - Choose a branch office from the **Branch Office** pull-down located in the Navigation Tree. Information and data are displayed in the Work Area.

- 5) Navigate to **Configuration > Alarms** in the navigation tree under Administration.

(Pre V8 OSB) The **Alarms** window appears with the **Settings** tab selected by default.

- 6) Select the **Trap destinations** value (V8 OSB) or tab (Pre V8 OSB).

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

Logging allows the administrator to set log levels for OpenScape Branch applications.

LogTypes

The following logs are available:

- Alarm History (view only):
Alarm history, showing all active or cleared alarms.
- Alarm Manager:
Log of Alarm manager application.
- B2BUA:
Back to back SIP user agent, this application is responsible for MLHG handling.
- Backup Link Client:
Log of the Backup Link Client application.
- Backup Link Server:
Log of the Backup Link Server application.
- Boot (view only):
Log of last boot.
- CAS:
The Log of Central Answering Service application.
- CDR:
The Log of Call Detail Record application.
- Current process (view only):
A list of the current processes running on OpenScape Branch.
- Continuous Tracing:
Log of the Continuous Tracing application.
- Redundancy: (V2)
Log of redundant Branch systems for active and standby status.
- Install/Update/Upgrade (view only):
Log from system installation, updates or upgrades (also includes language installation logs).
- ISDN:
Log of ISDN Layer 2 and Layer 3 messages of ISDN cards.
- Media Server:
Log of Media server, MGCP (Media Gateway Control Protocol) adapter and SIP/MGCP converter applications.
- MS 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.
- SIP Server:
SIP statefull proxy or SBC application.
- Message Rate Control (view only):
Log from Message Rate Control application.
- Survivability Provider:
Log of Survivability provider application.
- SSM (SIP Services Module)
Log of SIP Services
- System (view only):
Log of system events.
- Web server (view only):
Log of the local web server application
- DAHDI:
Log of the DAHDI driver. Applies to the OSB 50i and OSB 500i only.

OpenScape Branch Applications and Functional Components

For the following OpenScape Branch applications and functional components log levels can be set:

- Alarm Manager
- B2BUA (Back to Back SIP User Agent)
- Backup Link Client
- Backup Link Server
- CAS (Centralized Answering Service)
- CDR (Call Detail Record)
- Continuous Tracing
- ISDN: This is only valid for OSB V1R3 and higher.
- Media server
- MS Adapter (view only)
- Process Manager
- Redundancy
- 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 and can be assigned individually to each OpenScape Branch application or functional component:

General Log Levels:

- **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. This level may affect the system performance.

- **Notice**

Notice will report conditions that are not errors, but should require some attention. This level may affect the system performance.

ISDN Log Levels:

- **Info (Q.931)**

Info (Q931) ISDN layer 3 messages for ISDN cards.

This level may affect the system performance

- **Debug (Q.931 and Q.921)**

Debug (Q931 + Q921) enables layer 2 and layer 3 ISDN message logs for ISDN cards.

This level may affect the system performance and will generate several log files.

CAS Log Levels:

- **MF Trace**

Channel Associated Signaling traces that report MFC tones that leave or arrive.

- **Stack trace**

Channel Associated Signaling traces that report the stack messages.

- **Trace**

Channel Associated Signaling traces that report line signaling.

- **All**

Channel Associated Signaling traces that report all log levels.

- **None**

Do not report any messages.

- **Error, Warning, Notice and Debug**

See General Log Level descriptions (above).

4.2.1.1 How to Edit Settings for Logs

Proceed as follows to assign log levels for OpenScape Branch applications or functional components and configure the fallback data.

Prerequisites

Adequate administrative permissions.

At least one branch office of the OpenScape Branch type 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 Branch** within the Navigation Bar in Common Management Platform.
- 2) Select the **Branch Office list** in the Navigation Tree under Administration.
The system presents the **Branch Office Overview** in the Work Area with a current list of all branch offices.
- 3) To view a list of Branch Offices 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 branch office use one of the following options:
 - In the Work Area select the checkbox to the left of the particular branch office in the list and select **Manage**. Selecting the **Manage** button updates the **Branch Office** field, in the Navigation Tree, with the selected branch office and displays information and data in the Work Area for that branch office.
 - Choose a branch office from the **Branch Office** pull-down located in the Navigation Tree. Information and data are displayed in the Work Area.
- 5) (V8 OSB) Navigate to Diagnostics & Logs > Logs in the navigation tree under Administration. (Pre V8 OSB) 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 Branch application or functional component the selection list provides the following entries:

General Log Levels:

- **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. This level may affect the system performance.
- **Notice**
Notice will report conditions that are not errors, but should require some attention. This level may affect the system performance.

ISDN Log Levels:

- **Info (Q.931)**
Info (Q931) ISDN layer 3 messages for ISDN cards.
This level may affect the system performance
- **Debug (ISDN Q.931 and Q.921)**
Debug (Q931 + Q921) enables layer 2 and layer 3 ISDN message logs for ISDN cards.
This level may affect the system performance and will generate several log files.

CAS Log Levels:

- **MF Trace**
Channel Associated Signaling traces that report MFC tones that leave or arrive.
- **Stack trace**
Channel Associated Signaling traces that report the stack messages.
- **Trace**
Channel Associated Signaling traces that report line signaling.
- **All**
Channel Associated Signaling traces that report all log levels.
- **None**
Do not report any messages.
- **Error, Warning, Notice and Debug**
See General Log Level descriptions (above).

NOTICE:

Depending on the log category, different log levels exist.

- a) Select a log level for **SIP Server** (Session Initiation Protocol).
 - b) Select a log level for **B2BUA** (Back to Back SIP User Agent).
 - c) Select a log level for **Media server**.
 - d) Select a log level for **CAS** (Channel Associated Signaling)(valid for OSB V2 and higher).
 - e) Select a log level for **CDR** (Call Data Record).
 - f) Select a log level for **Process Manager**.
 - g) Select a log level for **Survivability Provider**.
 - h) Select a log level for **Alarm Manager**.
 - i) Select a log level for **Backup Link Client**.
 - j) Select a log level for **Backup Link Server**.
 - k) Select a log level for **RTP Proxy** (Real-time Transport Protocol).
 - l) Select a log level for **SSM** (SIP Service Module).
 - m) Select a log level for **Redundancy** (valid for OSB V2 and higher).
 - n) Select a log level for **ISDN**. This field is only valid for OSB V1R3 and higher.
 - o) Select a log level for **Continuous Tracing**.
- 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 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 gets and decodes IP packages from the IP network.

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 branch office of the OpenScape Branch type 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 Branch** within the Navigation Bar in the Common Management Platform.
- 2) Select the **Branch Office list** in the Navigation Tree under Administration.
The system presents the **Branch Office Overview** in the Work Area with a current list of all branch offices.
- 3) To view a list of Branch Offices 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 branch office use one of the following options:
 - In the Work Area select the checkbox to the left of the particular branch office in the list and select **Manage**. Selecting the **Manage** button updates the **Branch Office** field, in the Navigation Tree, with the selected branch office and displays information and data in the Work Area for that branch office.
 - Choose a branch office from the **Branch Office** pull-down located in the Navigation Tree. Information and data are displayed in the Work Area.
- 5) (V8 OSB) Navigate to Diagnostics & Logs > Debugging in the navigation tree under Administration. (Pre V8 OSB) Navigate to **Configuration > Logging in the navigation tree under Administration**.
(Pre V8 OSB) The **Logging** window appears with the **Settings** tab selected by default.
- 6) (V8 OSB) Select the Debugging value under Diagnostics & Logs. (Pre V8 OSB) Select the **Debugging** tab in the **Logging** window

- 7) Use one 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 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 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), MS (Media Server), MS adapter, SIP/MGCP/Q931.

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 are 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 Branch 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_nnnn
(ex: nnn =
0001), <OpenBranchNodeName>_<LogType>_<yyyymmddhhmmss>.log.bz2_nnnn
<LogType> = sip|b2b|ms|cdr|pm|sp|rtp|alm|alh|sys|boot|snt|
updttrc|red
```

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 Branch system must be configured to connect to the trace server in order to transfer trace files in the **OpenScape Branch > Configuration** in the navigation tree **Administration** area > **Logging > Continuous Tracing** tabsheet.

Two additional trace options are provided:

- SIP/Q931 Trace
- MGCP Trace

The configuration of the log levels must be configured in the **OpenScape Branch > Configuration** in the navigation tree **Administration** area. (V8 OSB) Settings are managed in the Log Settings work area under Diagnostics & Logs and (Pre V8 OSB) are located under **Logging > 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 OpenBranch to OSV-TM:

- Alarm History (view only),
- Alarm Manager,
- B2BUA,
- Backup Client Server
- Backup Link Server
- Boot (view only),
- CAS,
- CDR,

- Continuous Tracing
- Update/Upgrade/Install,
- ISDN
- Media Server,
- Message Rate Control (view only),
- MS Adapter,
- 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
B2BUA	Error
Backup Client Server	None
Backup Link Server	None
CAS	None
CDR	Error
Continuous Tracing	Error
ISDN	None
Media Server	Error
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. The log type can be one of the following:

- Alarm Manager.
- B2BUA,
- Backup Link Client
- Backup Server Client
- CDR,
- Continuous Tracing
- ISDN
- Media Server,
- Process Manager,
- Redundancy

- RTP Proxy,
- SIP Server,
- SSM
- Survivability Provider,

The following log levels are predefined and 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 Branch office.

Prerequisites

Adequate administrative permissions.

At least one branch office of the OpenScape Branch type 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.

Step by Step

- 1) Navigate to **Configuration tab > OpenScape Branch** within the Navigation Bar in the Common Management Platform.
- 2) Select the **Branch Office list** in the Navigation Tree under Administration.
The system presents the **Branch Office Overview** in the Work Area with a current list of all branch offices.
- 3) To view a list of Branch Offices 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 branch office use one of the following options:
 - In the Work Area select the checkbox to the left of the particular branch office in the list and select **Manage**. Selecting the **Manage** button updates the **Branch Office** field, in the Navigation Tree, with the selected branch office and displays information and data in the Work Area for that branch office.
 - Choose a branch office from the **Branch Office** pull-down located in the Navigation Tree. Information and data are displayed in the Work Area.

- 5) (V8 OSB) Navigate to Diagnostics & Logs > Logs in the navigation tree under Administration. (Pre V8 OSB) Navigate to **Configuration > Logging in the navigation tree under Administration**.

(V8 OSB) The Diagnostics & Log window appears with the Logs tab selected by default. (Pre V8 OSB) 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 Branch resets the trace configuration back to default.
- 8) Select the (V8 OSB) **Trace** or the (Pre V8 OSB) **Continuous Tracing** tabsheet.
- 9) To activate the continuous tracing function, check the **Enable** checkbox.
- 10) Configure the general settings as follows:
 - a) Enter the IP address 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 name of the SFTP server in the **System name** field.
 - b) Enter the username for identification on the SFTP server in the (V8 OSB) **SFTP Username** field or (Pre V8 OSB) Username field.
 - c) Enter the password to identify on the SFTP server in the (V8 OSB) **SFTP Password** field or (Pre V8 OSB) 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 Start, Stop and Configure On Demand Tracing

Proceed as follows start, stop and configure the settings for on demand tracing for an OpenScape Branch branch office.

Prerequisites

Adequate administrative permissions.

At least one branch office of the OpenScape Branch type 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 Branch > Configuration** in the navigation tree **Administration** area > **Logging > Continuous Tracing** tabsheet.

Step by Step

- 1) Navigate to **Configuration tab > OpenScape Branch** within the Navigation Bar in the Common Management Platform.
- 2) Select the **Branch Office list** in the Navigation Tree under Administration.
The system presents the **Branch Office Overview** in the Work Area with a current list of all branch offices.
- 3) To view a list of Branch Offices 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 branch office use one of the following options:
 - In the Work Area select the checkbox to the left of the particular branch office in the list and select **Manage**. Selecting the **Manage** button updates the **Branch Office** field, in the Navigation Tree, with the selected branch office and displays information and data in the Work Area for that branch office.
 - Choose a branch office from the **Branch Office** pull-down located in the Navigation Tree. Information and data are displayed in the Work Area.
- 5) (V8 OSB) Navigate to **Diagnostics & logs > Logs** in the navigation tree under Administration. (Pre V8 OSB) Navigate to **Configuration > Logging in the navigation tree under Administration**.
(V8 OSB) The **Diagnostics & Logs** window appears with the **Logs** tab selected by default. (Pre V8 OSB) The **Logging** window appears with the **Settings** tab selected by default.
- 6) Select the (V8 OSB) **Trace of (Pre V8 OSB) On Demand Trace** tab.

- 7) Select the log type to be created in the **Log Type** selection list. The following log types are listed:

- Alarm Manager,
- B2BUA,
- Backup Link Client,
- Backup Link Server,
- CAS
- CDR,
- Continuous Tracing,
- ISDN,
- 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 Media Server Configuration — Overview

The Media Server within the OpenScape Branch appliance is used to provide tones, announcements, conference channels, user prompts and exceptions to support the functionality of many features provided.

4.3.1 Media Server for OpenScape Branch

A Media Server assigned to a OpenScape Branch system can provide all necessary support to a particular branch.

The local OpenScape Media Server is used for tones, announcements, and conferencing, which minimizes the WAN bandwidth to the host OpenScape Voice when in normal mode; it also permits the branch to have access to media server capabilities when it is operating in survivability mode.

If a media server is not associated with a specific branch as described above, the subscriber's routing area can be used to determine which media server he or she is directed to when one is required.

Media Server Capabilities

The following capabilities are supported by the OpenScape Branch media server:

- Play fixed and variable announcements to branch subscribers.
- Play tones to branch subscribers.
- Collect Digits from branch subscribers.
- Set up conference connections initiated by branch subscribers.
- Provide call progression tones during third party calls.
- Support survivability mode operation with backup data link.

Multiple Language Support

OpenScape Voice V4.0 and later supports the following language installation and the OpenScape Branch media server provides support for these languages (and dialects). The appropriate language files are available and supplied during initial installation. Any language may be installed on the media server regardless of the country it is installed in. A maximum of 2 languages may be installed on an OpenScape Branch 50, 50i, 250 and 500i users (with all possible codec types). The languages currently supported by OpenScape Voice are as follows:

- Argentina - Spanish (Argentine)
- Australia - English (United Kingdom)
- Austria - German
- Belgium - French
- Brazil - Portuguese
- Chile - Spanish (Argentine)
- China - Mandarin
- Czech Republic - Czech
- Denmark - Danish
- Finland - Finnish
- France - French
- Germany - German
- Hungary - Hungarian
- India - English
- Ireland - English
- Italy - Italian
- Luxemburg - French
- Mexico - Spanish
- Netherlands - Dutch
- New Zealand - English
- Norway - Norwegian
- Poland - Polish
- Portugal - Portuguese
- South Africa - English
- Spain - Spanish
- Sweden - Swedish
- Switzerland - French, German, Italian

- United Kingdom - English
- United States - English

Configuration Parameters

The following table shows the characteristics and limits of the different application profiles of the OpenScape Branch system:

	OSB 50i	OSB 500i	OSB 50/250	OSB 1000	OSB 6000
Max. number of Announcement ports	10	20	10	32	100
Max. number of Conference ports	15	40	30	32	150
Max. Number of Supported Languages	2	2	2	2	2

4.3.1.1 How to Enable the Media Server

Proceed as follows to configure the port and IP address of the Call Agent and the preferred language.

Prerequisites

Adequate administrative permissions.

At least one 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 Branch** within the Navigation Bar in the Common Management Platform.

2) Select the **Branch Office list** in the Navigation Tree under Administration.

The system presents the **Branch Office Overview** in the Work Area with a current list of all branch offices.

3) To view a list of Branch Offices 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 branch office use one of the following options:

- In the Work Area select the checkbox to the left of the particular branch office in the list and select **Manage**. Selecting the **Manage** button updates the **Branch Office** field, in the Navigation Tree, with the selected branch office and displays information and data in the Work Area for that branch office.

- Choose a branch office from the **Branch Office** pull-down located in the Navigation Tree. Information and data are displayed in the Work Area.
- 5) (V8 OSB) Navigate to Features in the navigation tree under Administration.
(Pre V8 OSB) Navigate to **Configuration > Media Server in the navigation tree under Administration**.
- (V8 OSB) Locate the Features Available in Normal Mode and Survivability Mode work area. (Pre V8 OSB) The **Media Server** dialog appears.
- 6) Check the **Enable** checkbox to enable the media server.
- 7) Click the **OK** button to store the changes temporarily in the administrator's login session.
The **Media Server** dialog disappears.
- 8) Click the **Apply changes** button in the main window to save the changes permanently.

The media server is enabled.

4.3.1.2 How to Configure Connectivity Settings of the Media Server

Proceed as follows to configure the port and IP address of the Call Agent and the preferred language.

Prerequisites

Adequate administrative permissions.

At least one 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 Branch** within the Navigation Bar in the Common Management Platform.
- 2) Select the **Branch Office list** in the Navigation Tree under Administration.
The system presents the **Branch Office Overview** in the Work Area with a current list of all branch offices.
- 3) To view a list of Branch Offices 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 branch office use one of the following options:
 - In the Work Area select the checkbox to the left of the particular branch office in the list and select **Manage**. Selecting the **Manage** button updates the **Branch Office** field, in the Navigation Tree, with the selected branch office and displays information and data in the Work Area for that branch office.

- Choose a branch office from the **Branch Office** pull-down located in the Navigation Tree. Information and data are displayed in the Work Area.
- 5) (V8 OSB) Navigate to Features in the navigation tree under Administration.
(Pre V8 OSB) Navigate to **Configuration > Media Server in the navigation tree under Administration**.

(V8 OSB) Locate the Features Available in Normal Mode and Survivability Mode work area. (Pre V8 OSB) The **Media Server** dialog appears.
- 6) Check the **Enable** checkbox to enable the media server. (V8 OSB) Also click the Configure button next to the Enable checkbox.
- 7) Enter the port number of the port which the media server uses to communicate with the call agent in the **Media Server Listen Port** field.
- 8) Check the (V8 OSB) Use system FQDN or (Pre V8 OSB) **Use FQDN** checkbox if the Fully Qualified Directory Number is to be used for identification.
- 9) Select the preferential language from the **Language** selection list.

NOTICE: To configure media server adapter/converter settings or assign language files please refer to the respective sections in this chapter.

- 10) Beginning in V8 OSB, check the **Enable Whisper Mode** checkbox to enable this function. Whisper mode is a media server capability that allows a supervisor agent to whisper to a monitored agent. Checking this checkbox will enable this capability on the media server.
- 11) Click the **OK** button to store the changes temporarily in the administrator's login session.

The **Media Server** dialog disappears.
- 12) (V8 OSB) Click OK to close the Features window. Click the **Apply changes** button in the main window to save the changes permanently.

The settings are applied to the system.

4.3.1.3 How to Configure the Conference Settings

Proceed as follows to configure the conference parameters.

Prerequisites

Adequate administrative permissions.

At least one 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 Branch** within the Navigation Bar in the Common Management Platform.

- 2) Select the **Branch Office list** in the Navigation Tree under Administration.
The system presents the **Branch Office Overview** in the Work Area with a current list of all branch offices.
- 3) To view a list of Branch Offices 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 branch office use one of the following options:
 - In the Work Area select the checkbox to the left of the particular branch office in the list and select **Manage**. Selecting the **Manage** button updates the **Branch Office** field, in the Navigation Tree, with the selected branch office and displays information and data in the Work Area for that branch office.
 - Choose a branch office from the **Branch Office** pull-down located in the Navigation Tree. Information and data are displayed in the Work Area.
- 5) (V8 OSB) Navigate to Features in the navigation tree under Administration.
(Pre V8 OSB) Navigate to **Configuration > Media Server in the navigation tree under Administration**.
(V8 OSB) Locate the Features Available in Normal Mode and Survivability Mode work area, then click the Enable checkbox and the Configure button next to the Enable checkbox. (Pre V8 OSB) The **Media Server** dialog appears.
- 6) Enter the maximum amount of ports that is opened for providing conferences in the **Number of conference ports** field. The default and maximum values depend on the OpenScape Branch platform as described in the "Media Server for OpenScape Branch" section.
- 7) Enter the maximum time a conference is allowed to be active in the **Maximum conference time (sec):** field. Default value: 42800 seconds. If the time is to be unlimited, check the **Unlimited** checkbox.
- 8) Enter the prefix required in SIP R-URI to access a Media Server conference in the (V8 OSB) Conference Prefix access code or (Pre V8 OSB) **Prefix access code** field.
- 9) Click the **OK** button to store the changes temporarily in the administrator's login session.
The **Media Server** dialog disappears.
- 10) (V8 OSB) Click OK to close the Features window. Click the **Apply changes** button in the main window to save the changes permanently.

The settings are applied to the system.

4.3.1.4 How to Configure Announcement Settings

Proceed as follows to configure the announcement parameters.

Prerequisites

Adequate administrative permissions.

At least one 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 Branch** within the Navigation Bar in the Common Management Platform.
- 2) Select the **Branch Office list** in the Navigation Tree under Administration.
The system presents the **Branch Office Overview** in the Work Area with a current list of all branch offices.
- 3) To view a list of Branch Offices 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 branch office use one of the following options:
 - In the Work Area select the checkbox to the left of the particular branch office in the list and select **Manage**. Selecting the **Manage** button updates the **Branch Office** field, in the Navigation Tree, with the selected branch office and displays information and data in the Work Area for that branch office.
 - Choose a branch office from the **Branch Office** pull-down located in the Navigation Tree. Information and data are displayed in the Work Area.
- 5) (V8 OSB) Navigate to Features in the navigation tree under Administration.
(Pre V8 OSB) Navigate to **Configuration > Media Server in the navigation tree under Administration**.
(V8 OSB) Locate the Features Available in Normal Mode and Survivability Mode work area, then click the Enable checkbox and the Configure button next to the Enable checkbox. (Pre V8 OSB) The **Media Server** dialog appears.
- 6) Enter the maximum amount of ports that is opened for providing announcements in the **Number of announcement Ports** field. The default and maximum values depend on the OpenScape Branch platform as described in the "Media Server for OpenScape Branch" section.
- 7) Enter the maximum time which an announcement session is allowed to be inactive in the **Maximum announcement time (sec):** field. Default value: 1800 seconds. If the time is to be unlimited, check the **Unlimited** checkbox.
- 8) Enable or disable the **Stop announcement on DTMF** checkbox. If it this Check box is enabled, the announcement will stop when the Media Server receives a DTMF (Dual Tone Multifrequency).
- 9) Click the **OK** button to store the changes temporarily in the administrator's login session.
The **Media Server** dialog disappears.
- 10) (V8 OSB) Click OK to close the Features window. Click the **Apply changes** button in the main window to save the changes permanently.

The settings are applied to the system.

4.3.1.5 How to Configure the Media Server Adapter

The MS Adapter is used for NAT traversal of the MGCP (Media Gateway Control-Protocol) communication between the local Media Server and the Call Agent when the OpenScape Branch is in SBC (Session Border Controller) mode. Proceed as follows to configure the adapter parameters.

Prerequisites

Adequate administrative permissions.

At least one 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 Branch** within the Navigation Bar in the Common Management Platform.
- 2) Select the **Branch Office list** in the Navigation Tree under Administration.
The system presents the **Branch Office Overview** in the Work Area with a current list of all branch offices.
- 3) To view a list of Branch Offices 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 branch office use one of the following options:
 - In the Work Area select the checkbox to the left of the particular branch office in the list and select **Manage**. Selecting the **Manage** button updates the **Branch Office** field, in the Navigation Tree, with the selected branch office and displays information and data in the Work Area for that branch office.
 - Choose a branch office from the **Branch Office** pull-down located in the Navigation Tree. Information and data are displayed in the Work Area.
- 5) (V8 OSB) Navigate to Features in the navigation tree under Administration.
(Pre V8 OSB) Navigate to **Configuration > Media Server in the navigation tree under Administration**.
(V8 OSB) Locate the Features Available in Normal Mode and Survivability Mode work area, then click the Enable checkbox and the Configure button next to the Enable checkbox. (Pre V8 OSB) The **Media Server** dialog appears.
- 6) Click the (V8 OSB) Advanced or (Pre V8 OSB) **(Advanced features: Configure...** button in the **General** field area.
The **Media Server Advanced** window appears.
- 7) (V8 OSB) Enter the maximum duration of a MGCP transaction of a MGCP transaction in SBC mode in seconds in the Transaction Time to Live field in

the MS Adaptor field area. (Pre V8 OSB) Enter the maximum duration of a MGCP transaction in SBC mode in seconds in the **Time to Live** field in the **Adaptor** field area.

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

The **Media Server Advanced Features** dialog disappears.

- 9) Click the **OK** button to store the changes temporarily in the administrator's login session.

The **Media Server** dialog disappears.

- 10) (V8 OSB) Click OK to close the Features window. Click the **Apply changes** button in the main window to save the changes permanently.

The settings are applied to the system.

4.3.1.6 How to Configure the Media Server Converter

The MS Converter is used to control the Media Server services during Survivable Mode. For OpenScape Branch V1R4 and later releases no additional configuration is required.

Prerequisites

Not Applicable

4.3.1.7 How to Assign a Language File

Proceed as follows to assign the language file to the system.

Prerequisites

Adequate administrative permissions.

At least one 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 Branch** within the Navigation Bar in the Common Management Platform.
- 2) Select the **Branch Office list** in the Navigation Tree under Administration.
The system presents the **Branch Office Overview** in the Work Area with a current list of all branch offices.
- 3) To view a list of Branch Offices 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 branch office use one of the following options:
 - In the Work Area select the checkbox to the left of the particular branch office in the list and select **Manage**. Selecting the **Manage** button updates the **Branch Office** field, in the Navigation Tree, with the selected branch office and displays information and data in the Work Area for that branch office.
 - Choose a branch office from the **Branch Office** pull-down located in the Navigation Tree. Information and data are displayed in the Work Area.
- 5) (V8 OSB) Navigate to Features in the navigation tree under Administration. (Pre V8 OSB) Navigate to **Configuration > Media Server in the navigation tree under Administration**.

(V8 OSB) Locate the Features Available in Normal Mode and Survivability Mode work area, then click the Enable checkbox and the Configure button next to the Enable checkbox. (Pre V8 OSB) The **Media Server** dialog appears.
- 6) Click the (V8 OSB) Advanced or (Pre V8 OSB) **Advanced features: Configure...** button in the **General** field area.

The **Media Server Advanced** window appears.
- 7) Click the **Browse...** button in the **Language file** field area.

The file selection tree appears.
- 8) Locate the language file in the system.
- 9) Click the **Open** button.

The file selection tree disappears and the file selected appears in the **Language file** field.
- 10) (V8 OSB) Click the Install or (Pre V8 OSB) **Add** button.

The Language file is displayed.
- 11) Click the **OK** button.

The **Media Server Advanced Features** dialog disappears and the **Media Server** dialog appears.
- 12) Click the **OK** button to store the changes temporarily in the administrator's login session.

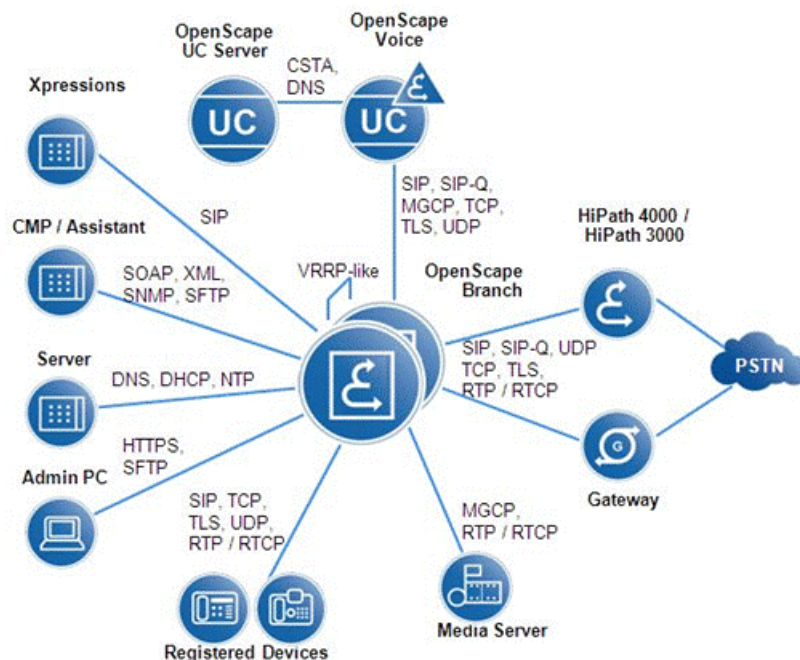
The **Media Server** dialog disappears.
- 13) (V8 OSB) Click OK to close the Features window. Click the **Apply changes** button in the main window to save the changes permanently.

The setting is applied to the system. The assignment of a media server language is logged in the Install/Update/Upgrade log file.

4.4 Network Services — Overview

Network Services comprise configuration of interfaces, routing and traffic shaping as well as NTP (Network Time Protocol), DNS (Domain Name System) and DHCP (Dynamic Host Configuration Protocol) settings.

External Interfaces Overview



Via network services the following data can be configured:

- **Interfaces**

Depending on the hardware used, up to four interfaces can be configured for the WAN (Wide Area Network), LAN (Local Area Network) and VLAN (Virtual LAN) connections. 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**

OpenScape Branches can be deployed and configured with redundancy and run in a Master and Backup arrangement. The Master sends a heartbeat to the Backup every 3 seconds. If the Backup does not receive a heartbeat for 10 seconds, it assumes that the Master is down and starts to take control.

V7R1 introduces redundancy to the OpenScape Branch 500i E1/T1 PRI interfaces by utilizing a splitter box. The splitter box is totally passive, requiring no power.

- **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 Branch appliance in the network.

- **DNS**

The Domain Name System client can be configured in the OpenScape Branch in order to resolve FQDNs (Fully Qualified Domain Name). The OpenScape Branch system acts as DNS client. In the server section the OpenScape Branch Domain Name can be configured. A pre-defined configuration of the gateway can be done using the USB Stick Wizard.

- **DHCP**

The Dynamic Host Configuration Protocol server manages a pool of IP addresses and information about client configuration parameters such as default gateway, domain name, the DNS servers.

4.4.1 How to Configure the Interfaces

Proceed as follows to configure the interfaces.

Prerequisites

Adequate administrative permissions.

At least one 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 Branch** within the Navigation Bar in the Common Management Platform.
- 2) Select the **Branch Office list** in the Navigation Tree under Administration.
The system presents the **Branch Office Overview** in the Work Area with a current list of all branch offices.
- 3) To view a list of Branch Offices 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 branch office use one of the following options:
 - In the Work Area select the checkbox to the left of the particular branch office in the list and select **Manage**. Selecting the **Manage** button updates the **Branch Office** field, in the Navigation Tree, with the selected branch office and displays information and data in the Work Area for that branch office.
 - Choose a branch office from the **Branch Office** pull-down located in the Navigation Tree. Information and data are displayed in the Work Area.
- 5) Navigate to **Network/ Net Services > Settings** in the navigation tree (V8 OSB), else if it is an earlier version OSB, navigate to **Network Services**.
The interface configuration is displayed in the list.
- 6) Select the interface to be configured in the list.

- 7) Click the **Edit...** button to modify interface settings (Pre V8 OSB only).
The **Edit Network Services Interface 1...4** window appears, depending on your selection.
- 8) To enable or disable the interface, check or uncheck the **Enable** checkbox.

NOTICE: Any changes to this field will result in a system reboot. Active and ongoing calls may fail.

- 9) Enter the IP address of the interface in the (V8 OSB) Interface 1 Main IP Address field or (Pre V8 OSB) **IP Address Node 1:** field.
- 10) Enter the netmask of the interface of the interface in the **Subnet Mask** field.
- 11) Enter the IP address for the redundant node in the (V8 OSB) Interface 2 Main IP Address field. (Pre V8 OSB) **IP Address Node 2** field. This node will take over if node 1 fails.
- 12) Enter the Virtual IP address in the **Virtual IP Address** field. This is the virtual IP address in the same subnet as the OpenScape Branch.

NOTICE: Any changes to these field values will result in a system reboot. Active and ongoing calls may fail.

- 13) Enter the Admin IP address for the WAN interface (only) the in the **Admin IP Address** field. This is the IP address used for CMP management access to the OpenScape Branch and allows separation of the Management network from the VoIP network. Leave this field blank if network separation is not required.

NOTICE:

If secure management is required then configure an IPsec VPN under Security in the Navigation tree.
If secure VoIP is required then configure an IPsec VPN under Security in the Navigation tree.

- 14) Enter the netmask associated with the WAN interface **Admin IP Address**, in the **Subnet Mask** field.
- 15) Select the interface speed to be used, from the **Speed** selection list to specify a specific network speed and override auto-sensing (V7R1). (Values: Auto (default), 10MB, 100 MB, 1000 MB).

NOTICE: Auto indicates auto-sensing is used to identify the network speed.

- 16) Select the operating mode to be used, from the **Duplex Mode** selection list (V7R1). (Values: Full and Half).

NOTICE: This field is disabled if the **Speed** parameter is set to **Auto**.

- 17) Enter the MTU size for the interface in the **MTU Size** field (V7R1). The default value is **1500** byte packets and can be set to any value between **300** and **1500**.

NOTICE: Allowed MTU size values for IPv6 should be at least **1280** octets.

- 18) (V8 OSB) Select the VLAN configuration button. (Pre V8 OSB) Select the **VLAN** tab.

The VLAN (Virtual LAN) settings are displayed in the list.

- 19) To edit or add VLAN settings, click the **Edit...** or **Add...** button.

The **Edit VLAN** or **Add VLAN** subwindow appears depending on your selection.

- 20) Enter the **Message Rate Limit(s)** ranging from 1 to 100.
- 21) Enter the **Trust Level** as N/A, minimal or medium.
- 22) Enter the **ID**, the **IP Address** and the **Netmask** of the virtual LAN in the respective fields.
- 23) Click the **OK** button to close the subwindow.
- 24) Click the **OK** button to close the **Interface Settings** window.
- 25) Click the **OK** button to store the changes temporarily in the administrator's login session.

The **Network Services** dialog disappears.

- 26) (Pre V8 OSB) Click the **Apply changes** button in the main window.

NOTICE: Changes to Interface Network Settings require a system restart to apply!

4.4.2 How to Configure the Default Gateway Address

Proceed as follows to enter or change the default gateway address.

Prerequisites

Adequate administrative permissions.

At least one 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 Branch** within the Navigation Bar in the Common Management Platform.
- 2) Select the **Branch Office list** in the Navigation Tree under Administration.

The system presents the **Branch Office Overview** in the Work Area with a current list of all branch offices.

- 3) To view a list of Branch Offices 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 branch office use one of the following options:

- In the Work Area select the checkbox to the left of the particular branch office in the list and select **Manage**. Selecting the **Manage** button updates the **Branch Office** field, in the Navigation Tree, with the selected branch office and displays information and data in the Work Area for that branch office.
- Choose a branch office from the **Branch Office** pull-down located in the Navigation Tree. Information and data are displayed in the Work Area.

- 5) Navigate to **Network/Net Services > Settings in the navigation tree (if V8 OSB) else if it is an earlier version OSB, navigate to Network Services**.

The **Network Services** window appears.

- 6) Select the **Routing** tab.

- 7) Enter the IP address to be used as default gateway address in the **Default Gateway Address** field in the **Gateway** field area.

- 8) Click the **OK** button to store the changes temporarily in the administrator's login session.

The **Network Services** dialog disappears.

- 9) Click the **Apply changes** button in the main window to save the changes permanently.

The setting is applied to the system.

4.4.3 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 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 Branch** within the Navigation Bar in the Common Management Platform.
- 2) Select the **Branch Office list** in the Navigation Tree under Administration.

The system presents the **Branch Office Overview** in the Work Area with a current list of all branch offices.

- 3) To view a list of Branch Offices 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 branch office use one of the following options:
 - In the Work Area select the checkbox to the left of the particular branch office in the list and select **Manage**. Selecting the **Manage** button updates the **Branch Office** field, in the Navigation Tree, with the selected branch office and displays information and data in the Work Area for that branch office.
 - Choose a branch office from the **Branch Office** pull-down located in the Navigation Tree. Information and data are displayed in the Work Area.
- 5) Navigate to **Network/Network Services > Setting in the navigation tree (if V8 OSB), else if it is an earlier version OSB, navigate to Network Services**.

The **Network Services** window appears.

The interface configuration is displayed in the list.

- 6) (V8 OSB) Navigate to Settings > Routing work area or (Pre V8 OSB) Select the **Routing** tab.

The routes are displayed in the list.

- 7) To configure a route, 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 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.

(Pre V8 OSB only) The **Edit Network Services Routing** or the **Add Network Services Routing** subwindow appears, depending on your selection.

- 9) Enter or modify the IP address of the destination server in the **Destination** field.
- 10) Enter or modify the netmask of the destination server in the **Netmask** field.
- 11) Enter or modify the IP address of the gateway in the **Gateway** field.
- 12) Enter or modify the interface used to route the IP packets in the **Interface** field.
- 13) (Pre V8 OSB) Click the **OK** button to close the subwindow.
- 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 to save the changes permanently.

The route settings are applied to the system.

4.4.4 How to Configure, Enable and Disable Redundancy

Proceed as follows to configure, enable and disable Redundancy for the OpenScape Branch appliance. V7R1 introduces redundancy to the OpenScape Branch 500i E1/T1 PRI interfaces by utilizing a splitter box.

Prerequisites

Adequate administrative permissions.

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

The Node1 and Node 2 must be installed with the same hardware and in operation.

The Node 1 and Node 2 must be installed with the same software level.

For the redundant system, the OSV Endpoints must be created. One for each physical IP address of each node and one virtual IP address for the redundant system.

NOTICE:

The IP for each node is only configured for administration purposes. Therefore the flag **Do not Audit Endpoint** is recommended to be enabled.

For OpenScape Branch 500i E1/T1 PRI redundancy install the splitter box.

The connection to the OpenScape Voice system is up.

NOTICE:

The features Backup Data Link, Auto Attendant and ACD are not supported in the redundancy for V1R4.

IMPORTANT: The OpenScape Branch redundancy does not maintain the current active calls during a switchover.

Step by Step

- 1) Navigate to **Configuration tab > OpenScape Branch** within the Navigation Bar in the Common Management Platform.
- 2) Select the **Branch Office list** in the Navigation Tree under Administration.
The system presents the **Branch Office Overview** in the Work Area with a current list of all branch offices.
- 3) To view a list of Branch Offices 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 branch office use one of the following options:
 - In the Work Area select the checkbox to the left of the particular branch office in the list and select **Manage**. Selecting the **Manage** button updates the **Branch Office** field, in the Navigation Tree, with the selected branch office and displays information and data in the Work Area for that branch office.
 - Choose a branch office from the **Branch Office** pull-down located in the Navigation Tree. Information and data are displayed in the Work Area.
- 5) (V8 OSB) Navigate to **Network/Network Services > Settings in the navigation tree under Administration**. (Pre V8 OSB) navigate to Network Services.

The **Network Services** window appears.

The interface configuration is displayed in the list.

- 6) (Pre V8 OSB) Select the IP address of node 1 branch office and select the **Edit...** button.
- 7) (V8 OSB) Enter the IP address for the redundant node via Settings > Interface 2 Main IP address field or via the **IP Address Node 2** field if (Pre V8 OSB). This node will take over if node 1 fails.
- 8) Enter the Virtual IP address for the in the **Virtual IP Address** field. This is the virtual IP address in the same subnet as the OpenScape Branch.
- 9) Click the **OK** button to close the **Edit Interface** window.

The **Network Services** window appears.

- 10) (V8 OSB) Select the **Redundancy** work area. When it is pre V8 OSB select the Redundancy tab.
- 11) To enable the Redundancy for the OpenScape Branch, check the **Enable Redundancy** checkbox.
- 12) To enable the Redundancy for the OpenScape Branch 500i E1/T1 PRI Interfaces:
 - a) Check the **Enable PRI Redundancy** checkbox.

NOTICE: The **Enable Redundancy** checkbox must first be enabled and the OpenScape Branch 500i must be operating in either Proxy, Proxy ACD or SBC Proxy mode.

- b) Select the number of links that must fail to initiate a switchover, in the **Failed links threshold** field list. If the number of links that have failed is greater than or equal to the setting, then failover to the Backup will be initiated by the Master. The default is 0 with the maximum number equal to the number of enabled PRIs.

NOTICE:

Setting the **Failed links threshold** to 0 will disable node switchover for PRI failures.

- 13) Click the **OK** button to close the **Network Services** window.
- 14) Click the **Apply changes** button in the main window.

Enabling/Disabling redundancy requires a system restart.

15) Enabling Redundancy

- a) 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.

- b) To enable Redundancy, it is necessary to configure the IP address of Nodes 1 and 2 and the redundant virtual IP address.
- c) Restart the system.

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.

16) Disabling Redundancy configure Node 1 and Node 2 separately as follows:

- a) 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 be unable to take control since the IP address was changed.

The other node will remain in Backup state for approximately 9 minutes and then will become the Master node. It is now possible to change the configuration on the new Master node.

- b) Configure a temporary IP in the new Master node and uncheck the **Redundancy Enable** checkbox. The system will restart.

After the restarts completes both systems will operate with Redundancy disabled.

- c) Reconfigure the IP addresses for both nodes to the original IP addresses.

The disabling of redundancy is complete.

17) Upgrading a Redundant System

- a) The upgrade process is started in the Master node.

The Local GUI/CMP shows the upgrade process only while upgrading the Master node. The upgrade completion of the other node must be verified by checking the software information (version).

- b) Once the upgrade in the Master node is finished the system will reboot (after user confirmation or via scheduled upgrade) and the Backup node will become the Master node. When the previous node is running again (approximately 5 minutes) the Software image will be uploaded to the former Backup node (now Master node).
- c) After the upload is finished the Master node will start the upgrade. When the upgrade is complete this system reboots.

The Backup node will become the Master node again, once the Backup node is running. Both nodes are now upgraded.

The settings for redundancy are applied on the OpenScape Branch system.

4.4.5 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.

4.4.5.1 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 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 Branch** within the Navigation Bar in the Common Management Platform.
- 2) Select the **Branch Office list** in the Navigation Tree under Administration.
The system presents the **Branch Office Overview** in the Work Area with a current list of all branch offices.
- 3) To view a list of Branch Offices 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 branch office use one of the following options:
 - In the Work Area select the checkbox to the left of the particular branch office in the list and select **Manage**. Selecting the **Manage** button updates the **Branch Office** field, in the Navigation Tree, with the selected branch office and displays information and data in the Work Area for that branch office.

- Choose a branch office from the **Branch Office** pull-down located in the Navigation Tree. Information and data are displayed in the Work Area.
- 5) (V8 OSB) Navigate to Network/Network Services in the navigation tree.
(Pre V8 OSB) navigate to Network Services.
- The **Network Services** window appears.
- The interface configuration is displayed in the list.
- 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.
- (Pre V8 OSB) 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) (Pre V8 OSB) 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.

4.4.6 How to Configure System NTP Settings

Proceed as follows to configure the time and date settings for the OpenScape Branch appliance using a NTP (Network Time Protocol) server.

Prerequisites

Adequate administrative permissions.

At least one 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 Branch** within the Navigation Bar in the Common Management Platform.
- 2) Select the **Branch Office list** in the Navigation Tree under Administration.
The system presents the **Branch Office Overview** in the Work Area with a current list of all branch offices.
- 3) To view a list of Branch Offices 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 branch office use one of the following options:
 - In the Work Area select the checkbox to the left of the particular branch office in the list and select **Manage**. Selecting the **Manage** button updates the **Branch Office** field, in the Navigation Tree, with the selected branch office and displays information and data in the Work Area for that branch office.
 - Choose a branch office from the **Branch Office** pull-down located in the Navigation Tree. Information and data are displayed in the Work Area.
- 5) (V8 OSB) Navigate to **Network/Network Services in the navigation tree. (Pre V8 OSB) Navigate to Network Services.**
The **Network Services** window appears.
The interface configuration is displayed in the list.
- 6) Select the **NTP** tab.
- 7) Select the time zone to be used in OpenScape Branch, 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:

- **(V8 OSB) Synchronize with NTP server or (Pre V8 OSB) 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 (V8 OSB Synchronize now) or **(Pre V8 OSB) 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 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.
- 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 Branch system.

4.4.7 How to Synchronize Manually with the NTP Server

Proceed as follows to synchronize the time and date settings for the OpenScape Branch appliance manually with the NTP (Network Time Protocol) server.

Prerequisites

Adequate administrative permissions.

At least one branch office of the OpenScape Branch type 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 Branch** within the Navigation Bar in the Common Management Platform.

2) Select the **Branch Office list** in the Navigation Tree under Administration.

The system presents the **Branch Office Overview** in the Work Area with a current list of all branch offices.

3) To view a list of Branch Offices 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 branch office use one of the following options:

- In the Work Area select the checkbox to the left of the particular branch office in the list and select **Manage**. Selecting the **Manage** button updates the **Branch Office** field, in the Navigation Tree, with the selected branch office and displays information and data in the Work Area for that branch office.
- Choose a branch office from the **Branch Office** pull-down located in the Navigation Tree. Information and data are displayed in the Work Area.

5) (V8 OSB) Navigate to **Network/Network Services in the navigation tree.**
(Pre V8 OSB) **Navigate to Network Services.**

The **Network Services** window appears.

The interface configuration is displayed in the list.

6) Select the **NTP** tab.

7) (V8 OSB) Click the **Synchronize now button.** (Pre V8 OSB) **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 Branch system has been synchronized manually with the NTP server.

4.4.8 Configuration of DNS Server

Depending on the network environment the OpenScape SBC or Branch 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 or Branch DNS Server:

- DNS Server acts a slave of a master DNS outside of OpenScape SBC or Branch 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 or Branch 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

In version 7 and later, the DNS server can be configured as a Master via customized configuration. During custom configuration, in the **DNS** Configuration tab of the **Network Services** window; the Named.com file is uploaded with definitions for the Master DNS configuration. Depending on the

custom configuration, several files may require upload e.g. zones configuration. The configuration will be preserved in case of upgrades. In the case of re-installation of OpenScape Branch, files must be exported outside of the server to be used during re-installation.

4.4.8.1 How to Configure System DNS Settings

Proceed as follows to configure the DNS (Domain Name System) settings for the OpenScape Branch appliance.

Prerequisites

Adequate administrative permissions.

At least one 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 Branch** within the Navigation Bar in the Common Management Platform.
- 2) Select the **Branch Office list** in the Navigation Tree under Administration.
The system presents the **Branch Office Overview** in the Work Area with a current list of all branch offices.
- 3) To view a list of Branch Offices 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 branch office use one of the following options:
 - In the Work Area select the checkbox to the left of the particular branch office in the list and select **Manage**. Selecting the **Manage** button updates the **Branch Office** field, in the Navigation Tree, with the selected branch office and displays information and data in the Work Area for that branch office.
 - Choose a branch office from the **Branch Office** pull-down located in the Navigation Tree. Information and data are displayed in the Work Area.
- 5) (V8 OSB) Navigate to **Network/Network Services in the navigation tree.**
(Pre V8 OSB) **Navigate to Network Services.**

The **Network Services** window appears with the **Interfaces** tab selected by default.

The interface configuration is displayed in the list.

- 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 **DNS Configure** button.
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** of a new DNS server in the address field and click the **Add** button.
 - 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.

NOTICE:

Alias configuration is required under following cases:

- - If phone is configured with a record FQDN for “Gateway” different than the default FQDN (Hostname.Domain) configured in the OpenScape Branch.
- - If phone is configured with DNS SRV record for “Gateway”.

Note: Missing alias configuration could cause calls toward the OpenScape Branch to be rejected (with 403 loose routing reject) and/or rejection of registrations toward the OpenScape Branch (with 483).

- 11) Use one of the following options:
 - To add an alias to the list, enter an **IP Address** 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) (V8 OSB) Refresh DNS. (Pre V8 OSB) Use the **Synch manually** button to synchronize with the DNS server promptly.
- 14) Enter the OpenScape Branch domain name in the **OpenScape Branch Domain Name** field, 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 **DNS Configure** button.
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** 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 customize configuration of the internal DNS server, configure the following:

The **Enable Customization** checkbox allows the user to upload files to customize configuration of DNS. Files are uploaded by clicking on the **Administer Custom Files** button. The **Named.com** file is uploaded with definitions for a Master DNS configuration or non-master customized configuration. Depending on the custom configuration, several files may require upload e.g. zones configuration. The configuration will be preserved in case of upgrades. In case of a re-installation of OpenScape Branch, files must be exported outside of the server to be used during re-installation.

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 **Enable Customization** checkbox is checked the DNS server configuration through the local management GUI will be disabled.

IMPORTANT: Only customized zone files with extension are valid. For instance, test.zone instead of testzone.

-
- a) To enable customized DNS configuration check the **Enable Customization** checkbox. The Enable customization of DNS checkbox allows upload of custom configuration for DNS.

NOTICE:

The **Enable DNS Server** must be checked prior to selecting **Enable Customization**.

-
- b) To configure what files will be uploaded click the **Administer Custom Files...** button.

The **DNS Custom List** window appears. The dialog contains a list of custom DNS file names.

- c) To remove a DNS file from the DNS Custom List, select the respective row and click the **Delete** button. The file is removed from the list.
- d) To select a custom DNS file, click the **Browse...** button and search for the custom DNS configuration file. Select the file to be uploaded.

The Browse dialog appears to allow selection of a custom DNS configuration file.

- e) To upload the selected DNS file and add the file to the DNS Custom List, click the **Add** button.

The selected DNS file is uploaded and the DNS Custom List is updated with the selected DNS configuration file.

Configuration files are temporarily stored.

- f) Click the **Close** button to go back to the **Network Services** window

The custom DNS configuration files are uploaded and the **Network Services** dialog appears.

- g) Click the **Apply Changes** button in the **Network Services** window

NOTICE:

Upload of custom configuration files requires “Apply changes” in the Main window.

IMPORTANT:

The DNS custom file must be backed up to survive a re-installation of the OpenScape Branch. Backup of the custom file will be included in the “Export all” function that can be found in the section **How to Export Configuration Files**.

After a re-installation of the OSB, the custom files must be restored to the OpenScape Branch 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.

- 20) 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.

- 21) Select the zone type (**Slave** or **Forward**) from the **Type** selection list.
- 22) Enter the zone domain name in the **Zone name** field.
- 23) Enter the IP address or IP address list (separated by commas) for the configured zone type in the **IP Masters/Forwards** field. When the Zone type is configured as forward, the IP address should be included in the Forward IP List.
- 24) Enter the file name to read the server data from in the **File name** field.
- 25) Click the **OK** button to close the **Add Zone** dialog.
- 26) Click the **OK** button to store the changes temporarily in the administrator’s login session.

The **Network Services** window disappears.

- 27) Click the **Apply changes** button in the main window to save the changes permanently.

The DNS Server settings are applied on the OpenScape Branch system.

4.4.9 Configuration of DHCP

DHCP (Dynamic Host Configuration Protocol) servers are used to distribute IP addresses down to client computers.

It is also a common practice to assign static (permanent) IP addresses to critical servers in the network, which are expected to be in continuous operation. The advantage of using DHCP are several:

- More efficient use of IP addresses. A computer that is only used part-time only gets an IP address when it is in use, and returns it into a common address pool when it is disconnected or turned off.
- Less manual configuration of each device is required because the DHCP server will automatically configure the device when it is powered up, with critical parameters such as the IP address, net mask, default router address, and DNS server addresses.
- Easier inventory control because it is not necessary to keep track of which IP address was permanently assigned to any specific device. A device that is removed from inventory does not take its IP address with it.

DHCP and OpenScape Voice

The OpenScape Voice solution does not, in general, require the use of DHCP. Phones and servers can be manually configured and will work properly without the presence of DHCP servers. However, the following features are available only when DHCP is in use:

- The plug-and-play phone installation process, which allows a fresh “out-of-box” SIP phone to be connected to the network and automatically brought into service, requires the use of DHCP. Without DHCP, a portion of the telephone configuration must be done manually via the telephone keys before the phone can be brought into service.
- The E911 auto-location process, which deduces the callers location based on IP address assignment, and automatically adapts if the phone is moved, requires the use of dynamically assigned IP addresses, and therefore DHCP.

Therefore, the decision to use or not use DHCP for phones and soft clients is part of the architectural design of the VoIP network, and should be based on the customer requirements and existing IP infrastructure design and policies.

DHCP and Branches

In a distributed deployment of OpenScape Voice, where OpenScape Voice is serving multiple remote locations (branches), the network planner must place a DHCP server (or pair) at each branch, or accept the possibility that an extended WAN outage between the branch and the central DHCP server could result in a telephony outage as well.

4.4.9.1 How to Configure DHCP Settings

Proceed as follows to configure the DHCP (Dynamic Host Configuration Protocol) settings for the OpenScape Branch appliance.

Prerequisites

Adequate administrative permissions.

At least one 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 Branch** within the Navigation Bar in the Common Management Platform.

- 2) Select the **Branch Office list** in the Navigation Tree under Administration.

The system presents the **Branch Office Overview** in the Work Area with a current list of all branch offices.

- 3) To view a list of Branch Offices 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 branch office use one of the following options:
 - In the Work Area select the checkbox to the left of the particular branch office in the list and select **Manage**. Selecting the **Manage** button updates the **Branch Office** field, in the Navigation Tree, with the selected branch office and displays information and data in the Work Area for that branch office.
 - Choose a branch office from the **Branch Office** pull-down located in the Navigation Tree. Information and data are displayed in the Work Area.

- 5) (V8 OSB) Navigate to **Network/Network Services in the navigation tree.**
(Pre V8 OSB) **Navigate to Network Services.**

The **Network Services** window appears.

The interface configuration is displayed in the list.

- 6) Select the **DHCP** tab.

The DHCP settings are displayed.

- 7) To enable the DHCP Server service check the **Enable DHCP Server** checkbox (V8 OSB).

- 8) To customize configuration of the DHCP server, configure the following:

The **Enable Customization** checkbox allows the user to upload files to customize configuration of DHCP. Files are uploaded by clicking on the **Administer Custom Files** button. The custom of files may include the DLS server configuration for the Phones. The configuration will be preserved in case of upgrades. In case of a re-installation of OpenScape Branch, files must be exported outside of the server to be used during re-installation.

IMPORTANT:

The syntax and the contents of the file(s) will not be checked, so wrong configuration may cause the DHCP service to not start. When the **Enable Customization**

checkbox is checked the DHCP server configuration through the local management GUI will be disabled.

- a) To enable customized DHCP configuration check the **Enable Customization** checkbox. The Enable customization of DHCP checkbox allows upload of custom configuration for DHCP.
-

NOTICE:

The **Enable DHCP** must be checked prior to selecting **Enable Customization**.

- b) To configure what files will be uploaded click the **Administer Custom Files...** button.

The **DHCP Custom List** window appears. The dialog contains a list of custom DHCP file names.

- c) To remove a DHCP file from the DHCP Custom List, select the respective row and click the **Delete** button. The file is removed from the list.
 - d) To select a custom DHCP file, click the **Browse...** button and search for the custom DHCP configuration file. Select the file to be uploaded.
-

NOTICE:

The custom file may include the DLS server configuration for the phones. In this case the DLS configuration must be manually set in the custom file.

The Browse dialog appears to allow selection of a custom DHCP configuration file.

- e) To upload the selected DHCP file and add the file to the DHCP Custom List, click the **Add** button.

The selected DHCP file is uploaded and the DHCP Custom List is updated with the selected DHCP configuration file.

- f) Click the **Close** button to go back to the **Network Services** window

The custom DHCP configuration files are uploaded and the **Network Services** dialog appears.

NOTICE:

Upload of custom configuration files requires “Apply changes” in the Main window.

IMPORTANT:

The DHCP custom file must be backed up to survive a re-installation of the OSB. Backup of the custom file will be included in the “Export all” function that can be found in the section **How to Export Configuration Files**.

After a re-installation of the OSB, the custom files must be restored to the OpenScape Branch 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.

- 9) Enter the Interface for the DHCP server to listen on in the **Interface** field.
- 10) Enter the update-method to be applied by this DHCP server to the Domain Name System in the **Update mode** field. Possible entries: **None**, **Interim**, **Ad-Hoc**.
- 11) To configure the list of static IP addresses to be used, (V8 OSB) click the Static IP address list configuration button or if (Pre V8 OSB) click the **Configure** button beside the **Static IP list** label.
The **Static IP list** window appears. The static IP settings are listed with hostname, MAC address and IP address.
- 12) Use one of the following options:
 - Select an entry in the list and click the **Delete** button to remove a static IP address from the list.
 - Select an entry in the list and click the **Edit** button to modify a static IP setting.
 - To add an entry to the list, click the **Add** button.
 (V8 OSB) A row is opened in the Static IP Address window. (Pre V8 OSB) The **Add/Edit static IP** window appears.
- 13) Enter or modify the hostname which applies for the configured IP address in the **Hostname** field.
- 14) Enter or modify the MAC (Media Access Control) address associated with the configured IP in the **MAC address** field.
- 15) Enter or modify the static IP address to be configured in the **IP address** field.
- 16) Click the **OK** button to go back to the **Static IP list** window.
- 17) Click the **OK** button to go back to the **DHCP** tab window.
- 18) To configure the DNS (Domain Name System) server list for DHCP, (V8 OSB) click the Add button next to the DNS server IP address or (Pre V8 OSB) click the **Configure** button besides the **DNS server list** label.
The **DNS Server list** window appears.
- 19) Use one of the following options:
 - To add a new server to the list, enter an IP address of a DNS server into 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.
- 20) (Pre V8 OSB) Click the **Close** button to go back to the **DHCP** tab window.
- 21) The subnet IP address which will be served by this DHCP server is displayed in the **Subnet** field.
- 22) The network mask associated with the subnet is displayed in the **Netmask** field.
- 23) Enter the range of IP addresses that will be available in the **IP range start** and **end** fields.
- 24) Enter the range of IP addresses that will be excluded in the (V8 OSB) Except IP address from field or if (Pre V8 OSB) **IP Exclusion range from:** and **to:** fields.
- 25) Enter the default lease time (in seconds) of the DHCP leasing mechanism in the **Lease time** field.

- 26) Enter the maximum lease time (in seconds) to be applied in the (V8 OSB) **Maximum Lease time max** field or if (Pre V8 OSB) Lease Time max field.
- 27) The broadcast IP address to be used for DNS is displayed in the **Broadcast address** field.
- 28) Enter the router IP address to be used in the **Router** field.
- 29) Enter the domain name to be applied for DNS in the **Domain name** field.
- 30) Enter the IP address of the Wins server to be used in the **Wins server** field.
- 31) Enter the IP address of the Print server to be used in the **Print server** field.
- 32) Enter the IP address of the DLS server in **DLS Server** field.
- 33) Enter the port used for DLS in the **DLS Port** field.
- 34) To enable sending of NTP information check the **Enable NTP** checkbox.
- 35) Click the **OK** button to store the changes temporarily in the administrator's login session.
The **Network Services** dialog disappears.
- 36) Click the **Apply changes** button in the main window to save the changes permanently.

The DHCP Server settings are applied on the OpenScape Branch system.

4.5 Security Configuration — Overview

Security configuration comprises general settings, configuration of Message Rate Control settings, firewall settings, port forwarding, password administration and RADIUS support (V7 and later).

The OpenScape Branch application 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)
Open VPN can be used to provide a secure link to an OpenScape Voice system in the main office.
 - IPsec (Internet Protocol Security)
IPsec can be used to provide a secure link to an OpenScape Voice system in the main office. IPsec may also be used to secure the MGCP signaling stream from an external media server.

OpenScape Branch Security Strategy

The two main goals of OpenScape Branch 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.

4.5.1 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 connection, when the type of authentication is defined as secret.

Configuration

TLS Certificates (X.509 certificates, CA certificates, Key files) and shared secret files can be displayed, created, uploaded or deleted by the administrator.

In OpenScape Version 7 and later, 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 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 Branch or 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 OSB / 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 OSB / OS SBC. The OSB / 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 OSB / OS SBC do 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 – OSB / OS SBC are responsible for initiating and keeping the connection alive. SIP Service Provider shall always reuse an already established TLS connection. OSB / 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. OSB / 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, OSB / 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, OSB / 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.

4.5.1.1 How to Manage TLS Certificates

Proceed as follows to select a manage TLS (Transport Layer Security) Certificates for the OpenScape Branch system.

Prerequisites

Adequate administrative permissions.

At least one 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 Branch** within the Navigation Bar in the Common Management Platform.
- 2) Select the **Branch Office list** in the Navigation Tree under Administration.
The system presents the **Branch Office Overview** in the Work Area with a current list of all branch offices.
- 3) To view a list of Branch Offices 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 Branch use one of the following options:
 - In the Work Area select the checkbox to the left of the particular branch office in the list and select **Manage**. Selecting the **Manage** button updates the **Branch Office** field, in the Navigation Tree, with the selected branch office and displays information and data in the Work Area for that or branch office.
 - Choose a branch office from the **Branch Office** pull-down located in the Navigation Tree. Information and data are displayed in the Work Area.
- 5) Navigate to **Configuration > Security in the navigation tree under Administration**.
Select the General choice. The **Security** window appears with the **General** tab selected by default.
- 6) Click the **Certificate Management...** 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.

IMPORTANT: The generated certificates are **SHA-1** only.

9) Display Certificates

- a) (V8 OSB) The certificates are listed in the CA certificates work area else if (Pre V8 OSB) 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 (V8 OSB)

- a) Click the **Browse** button in the CA Certificates upload area and navigate to the certificate of interest.
- b) Click the **Upload** button in the CA Certificates work area.

The **Add Certificate** dialog appears.

- c) To upload a certificate, Click the **Upload** radio button. 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 create certificates, Click the **Create** radio button. Select the type of certificate (**TLS Certificates**) from the field list and Enter the name of the certificate to be created in the **Name** field.
- e) 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 download and certificate profiles field lists.

11) Certificate Upload (Pre V8 OSB)

- 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, Click the **Upload** radio button. 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 create certificates, Click the **Create** radio button. Select the type of certificate (**TLS Certificates**) from the field list and Enter the name of the certificate to be created in the **Name** field.
- e) 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 download and certificate profiles field lists.

12) 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.

4.5.1.2 How to Create, Edit and Delete Certificate Profiles

Proceed as follows to create, edit and delete Certificate Profiles for OpenScape Branch systems. A Certificate Profile can be assigned to one or more OpenScape Branch (Gateways) in version 7 allowing for faster configuration of certificates.

Prerequisites

Adequate administrative permissions.

At least one 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 Branch** within the Navigation Bar in the Common Management Platform.
- 2) Select the **Branch Office list** in the Navigation Tree under Administration.
The system presents the **Branch Office Overview** in the Work Area with a current list of all branch offices.
- 3) To view a list of Branch Offices 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 Branch use one of the following options:
 - In the Work Area select the checkbox to the left of the particular branch office in the list and select **Manage**. Selecting the **Manage** button updates the **Branch Office** field, in the Navigation Tree, with the selected branch office and displays information and data in the Work Area for that branch office.
 - Choose a branch office from the **Branch Office** pull-down located in the Navigation Tree. Information and data are displayed in the Work Area.
- 5) Navigate to **Configuration > Security in the navigation tree under Administration**.
Select the General choice. The **Security** window appears with the **General** tab selected by default.
- 6) Click the **Certificate Management Configure...** button.
The **Certificate Management** window appears with the **General Configuration** tab displayed as default.
- 7) (Pre V8 OSB) 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:
 - OSV Solution
 - Certificate Service
 - Client Certificate File
 - Server Certificate File
 - Local CA File
 - Remote CA File
 - Local Key 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.

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-LTS** (default), **HTTPS** 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 the local certificates from the **Local CA file** field selection list.

(Pre V8 OSB) 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 for path validation of the certificate received from the remote endpoint from the **Remote CA file** field selection list.

(Pre V8 OSB) 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) Select the Key file that contains the private key from the **Local key file** field selection list.

Validation Settings Configuration:

- i) (V8 OSB) Click on a Certificate Profile in the Certificates Profiles work area and click the Edit button. (Pre V8 OSB) Select the **Validation** tab.
(V8 OSB) The Certificate Profile dialog appears. (Pre V8 OSB) The Validation tab dialog appears
- j) 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
- k) 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.

- l) 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:

- m) (V8 OSB) Click on a Certificate Profile in the Certificate Profiles work area and then click on the Edit button. (Pre V8 OSB) Select the **Renegotiation** tab.
(V8 OSB) The Certificate Profile dialog appears. (Pre V8 OSB) The Renegotiation tab dialog appears
- n) Checkmark the **Enforce TLS session renegotiation** checkbox, if renegotiation of an established TLS session is enabled for this endpoint. (default is disabled)
- o) 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.
- p) Select the TLS version supported from the **TLS version** field selection list. Values: **TLSv1.0** (default), **TLSv1.1** or **TLSv1.2**.

NOTICE: In V10R2, after full installation, the default value for Minimum TLS version has been changed to TLS V1.2 in Certificate Profile.

- q) 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.
- r) 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** work area (V8 OSB) or tab window (Pre V8 OSB); 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** work area (V8 OSB) tab window (Pre V8 OSB); 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 be presented to the user indicating the reason of the failure. This validation prevents the administrator from configuring an invalid certificate.

4.5.1.3 How to Configure Certificate Expiration Checking

Proceed as follows to configure certificate expiration checking for the OpenScape Branch system.

Prerequisites

Adequate administrative permissions.

At least 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 Branch** within the Navigation Bar in the Common Management Platform.
- 2) Select the **Branch Office list** in the Navigation Tree under Administration.

The system presents the **Branch Office Overview** in the Work Area with a current list of all branch offices.

- 3) To view a list of Branch Offices 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 Branch use one of the following options:
 - In the Work Area select the checkbox to the left of the particular branch office in the list and select **Manage**. Selecting the **Manage** button updates the **Branch Office** field, in the Navigation Tree, with the selected branch office and displays information and data in the Work Area for that branch office.
 - Choose a branch office from the **Branch Office** pull-down located in the Navigation Tree. Information and data are displayed in the Work Area.

- 5) Navigate to **Configuration > Security in the navigation tree under Administration**.

Select the General choice. The **Security** window appears with the **General** tab selected by default.

- 6) Click the **Certificate Management** button.

The General Configuration tab manages the following:

- System TLS Certificate selection
- Certificate creation
- Certificate upload
- Certificate download

- 7) (V8 OSB) Navigate to the Certificate Expiration Checking work area. (Pre V8 OSB) 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. Value 0 - 300 days, default: 60 days.
- 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. Value 0 - 60 days, default: 7 days.
- 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 (00:00 - 23:59, default: 00:00).
- 11) Click the **OK** button to store the settings.

The changes are saved automatically.

4.5.1.4 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 Branch systems.

Prerequisites

Adequate administrative permissions.

At least one 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 Branch** within the Navigation Bar in the Common Management Platform.
- 2) Select the **Branch Office list** in the Navigation Tree under Administration.
The system presents the **Branch Office Overview** in the Work Area with a current list of all branch offices.
- 3) To view a list of Branch Offices 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 Branch use one of the following options:
 - In the Work Area select the checkbox to the left of the particular branch office in the list and select **Manage**. Selecting the **Manage** button updates the **Branch Office** field, in the Navigation Tree, with the selected branch office and displays information and data in the Work Area for that branch office.
 - Choose a branch office from the **Branch Office** pull-down located in the Navigation Tree. Information and data are displayed in the Work Area.
- 5) Navigate to **Configuration > Security in the navigation tree under Administration**.
Select the General choice. The **Security** window appears with the **General** tab selected by default.
- 6) Click the **Certificate Management** button.
The **Certificate Management** window appears with the **General Configuration** tab displayed as default.

- 7) (V8 OSB) Navigate to the Certificate Revocation List work area. (Pre V8 OSB) 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 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. Values: 0 - 168 hours. 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. Values: 15 - 1440 minutes.
Default value:60 minutes.

- g) Enter the specific time of day at which to start the CRL check, in the **CRL download interval** field. The format for time of day is hh:mm (00:00 - 23:59, default: 00:00).

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 Branch > Log files: Show button > in the Log Viewer select Web Server from the Select Log: field list**

4.5.1.5 How to Select a Shared Secret File for Use

Proceed as follows to select a shared secret file for use in the OpenScape Branch system.

Prerequisites

Adequate administrative permissions.

At least one 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 Branch** within the Navigation Bar in the Common Management Platform.
- 2) Select the **Branch Office list** in the Navigation Tree under Administration.
The system presents the **Branch Office Overview** in the Work Area with a current list of all branch offices.
- 3) To view a list of Branch Offices 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 Branch use one of the following options:
 - In the Work Area select the checkbox to the left of the particular branch office in the list and select **Manage**. Selecting the **Manage** button updates the **Branch Office** field, in the Navigation Tree, with the selected branch office and displays information and data in the Work Area for that branch office.
 - Choose a branch office from the **Branch Office** pull-down located in the Navigation Tree. Information and data are displayed in the Work Area.
- 5) Navigate to **Configuration > Security in the navigation tree under Administration**.
Select the General choice. The **Security** window appears with the **General** tab selected by default.
- 6) Use the **Shared Secret Files** selection list to choose a shared secret file to be used.

The changes are saved automatically.

4.5.1.6 How to Create Shared Secret Files

Proceed as follows to display, add and delete Shared Secret files for OpenScape Branch systems.

Prerequisites

Adequate administrative permissions.

At least one 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 Branch** within the Navigation Bar in the Common Management Platform.
- 2) Select the **Branch Office list** in the Navigation Tree under Administration.
The system presents the **Branch Office Overview** in the Work Area with a current list of all branch offices.
- 3) To view a list of Branch Offices 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 Branch use one of the following options:
 - In the Work Area select the checkbox to the left of the particular branch office in the list and select **Manage**. Selecting the **Manage** button updates the **Branch Office** field, in the Navigation Tree, with the selected branch office and displays information and data in the Work Area for that branch office.
 - Choose a branch office from the **Branch Office** pull-down located in the Navigation Tree. Information and data are displayed in the Work Area.
- 5) Navigate to **Configuration > Security in the navigation tree under Administration**.
Navigate to the general selection.
The **Security** window appears with the **General** tab selected by default.
Display and Configure Shared Secret Files
- 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) (Pre V8 OSB) Click the **Add** button.

The **Add Certificate** dialog appears.

- b) To upload a shared secret file certificate, Click the **Browse** button. Locate and select the file to be uploaded. Click the **Upload** radio button. The type of certificate is **Shared Secret File** in the field list.
- c) To create a shared secret file certificate, enter the name of the certificate to be created in the **Name** field. Click the **Create** radio button. The type of certificate is **Shared Secret File** in the field list.
- 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** 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 be presented to the user indicating the reason of the failure. This validation prevents the administrator from configuring an invalid certificate.

4.5.2 SSH with Public Key Infrastructure (PKI) Configuration - Overview

This V7R1 feature introduces an SSH with PKI mechanism that allows external users to log into other systems, such as PCs or other Linux servers, to execute scripts or other commands on an OpenScape Branch without having to explicitly

log into the OpenScape Branch. This is done by storing the external user's public key on the OpenScape Branch.

V7R1 also introduces an HTTPS Certificate Profile to allow customers to conveniently change https certificates.

How SSH with PKI works

An external user who is logged in on their own computer can generate a public key, which, when appended to the `authorized_keys` file of an applicable OpenScape Branch user, will allow that external user to log in to the OpenScape Branch without having to provide the OpenScape Branch user's password.

The External User will begin by logging into their own machine. They will then generate a public/private key pair. The private key will remain on their computer, but the public key will be sent to a person who has authority to append their public key on the OpenScape Branch. For example, if the External User wants to be able to log in to the OpenScape Branch as the administrator user without having to enter the administrator password; they would send their public key to the administrator user (e.g., in an email). The administrator user will then append the key to their `/home/administrator/.ssh/authorized_keys` file. Now, when the External User logs in on the OpenScape Branch as the administrator user, a password is not required.

SSH with PKI Restrictions

This capability will only be supported for the "administrator" and "service" users on the OpenScape Branch. Note that, if SSH doesn't find an external user's public key for the OpenScape Branch user that they are trying to log in to, then a password will be required.

HTTPS Certificate Profiles

This feature allows a customer to change the certificate files for the https application (e.g., Apache web server) and maintain the communication between the CMP to/from the OpenScape Branch.

The customer creates a HTTPS Certificate Profile and associates the profile with the https application.

4.5.2.1 How to Configure PKI Capability

Proceed as follows to configure the Public Key Infrastructure (PKI) capability to allow external user logon for administration of systems.

Prerequisites

Adequate administrative permissions.

At least one 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 Branch** within the Navigation Bar in the Common Management Platform.

- 2) Select the **Branch Office** list in the Navigation Tree under Administration.

The system presents the **Branch Office Overview** in the Work Area with a current list of all branch offices.

- 3) To view a list of Branch Offices 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 branch office use one of the following options:

- In the Work Area select the checkbox to the left of the particular branch office in the list and select **Manage**. Selecting the **Manage** button updates the **Branch Office** field, in the Navigation Tree, with the selected branch office and displays information and data in the Work Area for that branch office.
- Choose a branch office from the **Branch Office** pull-down located in the Navigation Tree. Information and data are displayed in the Work Area.

- 5) Navigate to **Configuration > Security** in the navigation tree under **Administration**.

Navigate to the General selection. The **Security** window appears with the **General** tab selected by default.

- 6) (V8 OSB) Locate the PKI Configuration work area. (Pre V8 OSB) Select the **PKI Configuration** tab.

The PKI functions are displayed.

- 7) Checkmark the **Enable** check box if PKI configuration is to be used.

- 8) (V8 OSB) Click the **PKI Configuration** button or (Pre V8 OSB) or click the Config button to bring up the **PKI Configuration** screen with **SSH PKI Configuration** tab displayed as the default.

The PKI Configuration screen is displayed with the SSH PKI Configuration table and following functions:

- **External User ID:** This field contains the username and any other identifying details about the external user.
- **Internal Username:** This field contains the internal username that is granting public key access (administrator or service).
- **Add:** The Add button will open a new "Add/Update Public Key" screen to select the public key file to be uploaded.
- **Delete:** The Delete button allows the user to delete public keys that are no longer required/authorized. The user must first select a row in the table. The user must confirm the deletion.
- **Edit:** (V8 OSB) Update or (Pre V8 OSB) The Update button allows the user to update an existing entry in the table. The user must first select a row in the table. When clicked, the "Add/Edit Public Key" screen will be popped up, with applicable fields already filled in.
- **HTTPS PKI Configuration field:** The list of certificate profiles that have Certificate Service set to HTTPS. The HTTPS System Default option is the first option at the top of the list.

- 9) To configure the PKI, use one of the following options:
- To remove an entry from the PKI Configuration list, select the respective row and click the **Delete** button. The PKI entry is removed from the list.
 - To edit an PKI entry in the list, select the respective row and click the **Edit** button.
 - To add a PKI entry to the list, click the **Add** button.

The **Add/Update Public Key** window appears.

- 10) Select the associated internal user for this PKI entry, from the **Associated Internal User** filed selection list. Values are **administrator** and **service**.
- 11) Enter the full path and filename of the public key that will be uploaded in the **Public Key File** field or select the **Browse...** button to navigate to the public key file.

NOTICE:

Only a PPK file (.ppk) is allowed as a public key file.

- 12) Click the **Add** button to append a new public key, in the case of Add; or **Update** button to replace an existing public key, in the case of an update, for the applicable authorized keys file.
- 13) Click the **OK** button to go back to the **SSH PKI Configuration Table** window.
- 14) (V8 OSB) Locate the HTTPS PKI Configuration work area. (Pre V8 OSB) Select the **HTTPS PKI Configuration** tab.
- (V8 OSB) HTTPS Profile or (Pre V8 OSB) HTTPS PKI Configuration field:** This field contains a list of certificate profiles that have Certificate Service set to HTTPS. The **HTTPS System Default** option is the first option at the top of the list. The https application can only be associated with one profile at a time.
- 15) Select the certificate profile to be associated with the https application.
- a) To remove a profile association from an application, select the **HTTPS System Default** option to restore the default configuration that was created at system installation time.
- 16) Click the **OK** button to go back to the **Security** window.
- 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.

The PKI settings are applied on the OpenScape Branch system.

4.5.3 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 Branch 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.

4.5.3.1 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 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 Branch** within the Navigation Bar in the Common Management Platform.
- 2) Select the **Branch Office list** in the Navigation Tree under Administration.
The system presents the **Branch Office Overview** in the Work Area with a current list of all branch offices.
- 3) To view a list of Branch Offices 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 branch office use one of the following options:
 - In the Work Area select the checkbox to the left of the particular branch office in the list and select **Manage**. Selecting the **Manage** button updates the **Branch Office** field, in the Navigation Tree, with the selected branch office and displays information and data in the Work Area for that branch office.
 - Choose a branch office from the **Branch Office** pull-down located in the Navigation Tree. Information and data are displayed in the Work Area.
- 5) Navigate to **Configuration > Security in the navigation tree under Administration**.
The **Security** window appears with the **General** tab selected by default.
- 6) Select the **Message Rate Control** work area / 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 enter the address in the **IP address** field and click the **Add** button.
 - 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 Branch system.

4.5.4 Firewall Configuration

A firewall is installed on the OpenScape Branch system in order to protect access to systems behind it, limiting their exposure to the Internet.

Filter Rules

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.

NAT Traversal — Masquerading

Masquerading masks the LAN addresses in the WAN to hide the entire internal address space. Masquerading is only possible if the OpenScape Branch system works in SBC (Session Border Controller) mode.

Port Forwarding

Port forwarding is only possible if the OpenScape Branch system works in SBC (Session Border Controller) mode.

Allowing/Blocking Services

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 Branch and outgoing connections (Devices under OpenScape SBC and Branch trying to access WAN services).

NOTICE: OpenScape supports SNMP to send alarms from the OpenScape Branch to the CMP. The OSB supports SNMP Gets of MIB-II however, Set SNMP operations are not supported

Allowing/Blocking IPs/Ports (OSB V1R3 and later versions only, and OpenScape SBC V1 and later versions)

Configuring a "black" and a "white" list allows to block or allow incoming and outgoing WAN network connections for a specific IP/Port.

4.5.4.1 How to Configure the Firewall

Proceed as follows to configure the firewall rules.

Prerequisites

Adequate administrative permissions.

At least one 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 Branch** within the Navigation Bar in the Common Management Platform.
- 2) Select the **Branch Office list** in the Navigation Tree under Administration.
The system presents the **Branch Office Overview** in the Work Area with a current list of all branch offices.
- 3) To view a list of Branch Offices 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 branch office use one of the following options:
 - In the Work Area select the checkbox to the left of the particular branch office in the list and select **Manage**. Selecting the **Manage** button updates the **Branch Office** field, in the Navigation Tree, with the selected branch office and displays information and data in the Work Area for that branch office.
 - Choose a branch office from the **Branch Office** pull-down located in the Navigation Tree. Information and data are displayed in the Work Area.
- 5) Navigate to **Configuration > Security in the navigation tree under Administration**.
- 6) Select the **Firewall** work area / tab.
- 7) (V8 OSB) Select a row for an Interface (LAN, WAN) and click the Edit button located on the Firewall Settings work area. The Firewall Configuration window opens.
- 8) To activate masquerading, check the **Enable masquerading** checkbox. 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

- 9) Use the checkboxes in the (V8 OSB) **Incoming VoIP network connections or (Pre V8 OSB) Incoming WAN VoIP 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.
- 10) Use the checkboxes in the (V8 OSB) **Incoming/Outgoing network connections or (Pre V8 OSB) Incoming/Outgoing WAN network connections** field area to enable protocols of the incoming VoIP connections.
- 11) (Pre V8 OSB) 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.

The **Black List** list shows the IPAddresses/subnets and Ports which are blocked.

- 12) 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.

(Pre V8 OSB) The **Add Black List** window appears.

- 13) Enter the IP address to be blocked in the **IP address/Subnet** field.

NOTICE: Please note that an IP address can either belong to the white list OR the black list.

- 14) Enter the port number to be blocked in the **Port** field. If the **Port** field is empty, all ports will be blocked.
- 15) (Pre V8 OSB) Click the **OK** button to close the **Add Black List** window.
- 16) (Pre V8 OSB) Click the **OK** button to close the **Black List** window.
- 17) (Pre V8 OSB) 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.

The **White List** 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.

(Pre V8 OSB) The **Add White List** window appears.

19) Enter the IP address to be blocked in the **IP address/Subnet** field.

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) (Pre V8 OSB) Click the **OK** button to close the **Add White List** window.

22) (Pre V8 OSB) Click the **OK** button to close the **White List** window.

23) Click the **OK** button to store the changes temporarily in the administrator's login session.

The **Security** dialog disappears.

24) Click the **Apply changes** button in the main window.

The firewall settings are applied on the OpenScape Branch system.

NOTICE: Message Rate Control (if enabled) will be restarted if the firewall rules are changed.

4.5.4.2 How to Configure Port Forwarding

Proceed as follows to configure the port forwarding settings.

Prerequisites

Adequate administrative permissions.

At least one 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 Branch** within the Navigation Bar in the Common Management Platform.

2) Select the **Branch Office list** in the Navigation Tree under Administration.

The system presents the **Branch Office Overview** in the Work Area with a current list of all branch offices.

- 3) To view a list of Branch Offices 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 branch office use one of the following options:
 - In the Work Area select the checkbox to the left of the particular branch office in the list and select **Manage**. Selecting the **Manage** button updates the **Branch Office** field, in the Navigation Tree, with the selected branch office and displays information and data in the Work Area for that branch office.
 - Choose a branch office from the **Branch Office** pull-down located in the Navigation Tree. Information and data are displayed in the Work Area.
- 5) Navigate to **Configuration > Security in the navigation tree under Administration**.
Select the Firewall work area / tab.
- 6) (V8 OSB) Select an Interface row (WAN, LAN and click Edit. (Pre V8 OSB) Select the **Port FW** tab.
- 7) To activate port forwarding, check the **Enable port forwarding** checkbox. (V8 OSB) Click the COnfigure button located next to the Enable port forwarding checkbox.

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

- 8) (V8 OSB) The Port Forward window or (Pre V8 OSB) **Rule list** shows the port forwarding parameters: Outgoing IP address to be used, incoming port number, outgoing port number, 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.

(Pre V8 OSB)The **Add/Edit Security Port FW** window appears.
- 9) (Pre V8 OSB) Enter a name associated with the port forwarding in the **Name** field.
- 10) (Pre V8 OSB) Enter the incoming IP address in the **Source IP** field.
- 11) Enter the outgoing IP address in the (V8 OSB) Out IP address or (Pre V8 OSB) **Destination IP** field.
- 12) Enter the incoming port number in the **In port** field.
- 13) Enter the outgoing port number in the **Out port** field.
- 14) Select the protocol in the **Protocol** selection list. The following values are possible: TCP (Transmission Control Protocol), UDP (User Datagram Protocol), All.

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

The **Add Security Port FW** window disappears (Pre V8 OSB only) and a new row is created in the Port FW list. The changes are stored temporarily.

- 16) Click the **OK** button to store the changes temporarily in the administrator's login session and close the **Security Firewall** window.

- 17) Click the **Apply changes** button in the main window.

The port forwarding rules are applied on the OpenScape Branch system.

NOTICE: Message Rate Control (if enabled) will be restarted if the firewall rules are changed.

4.5.5 Configuration of IP Security

IPsec (Internet Protocol Security) serves for securing IP communications by authenticating and encrypting each IP packet of a data stream.

IP security and OpenScape Voice

- OpenScape Voice provides IPsec protection for the OpenScape Voice SOAP (Simple Object Access Protocol) and SNMP (Simple Network Management Protocol) management interfaces to the external OpenScape Voice Assistant.
- IPsec may also be used to secure the MGCP (Media Gateway Control Protocol) signaling stream from an external media server.
- IPsec protection for CDR (Call Detail Record) delivery when using FTP (File Transfer Protocol) pull- or push-mode interface between OpenScape Voice and the billing server.

IP security and OpenScape Branch

IP security is used to encrypt all communication between the OpenScape Branch and associated servers, including the OpenScape Voice system.

Hosted OpenScape Management Using a VPN

In OpenScape Branch Version 7 a feature was introduced to allow secure OpenScape Branch management application access within the hosted OpenScape Voice solution (Option 5).

IP security is used to encrypt all communication between the OpenScape Branch and management applications.

Refer to the OpenScape Branch Installation and Upgrade documentation for details on Simplified installation Option 5.

Private IP Address on IPsec

In OpenScape Branch Version 7 R1 a feature was introduced to allow the capability to create a VPN tunnel to transport SIP, MGCP and (S)RTP messages through IPsec with a private IP address. Configuration will allow multiple OpenScape Branches to be added to the network and communicate to the data center over the VPN tunnel; without additional configuration.

4.5.5.1 How to Configure the IP Security Settings

Proceed as follows to configure the connection information of the VPN tunnels to remote hosts using IPsec (Internet Protocol Security).

Prerequisites

Adequate administrative permissions.

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

The connection to the OpenScape Voice system is up.

The IP sec configuration applies only when the WAN interface is enabled.

Step by Step

- 1) Navigate to **Configuration tab > OpenScape Branch** within the Navigation Bar in the Common Management Platform.
- 2) Select the **Branch Office list** in the Navigation Tree under Administration.
The system presents the **Branch Office Overview** in the Work Area with a current list of all branch offices.
- 3) To view a list of Branch Offices 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 branch office use one of the following options:
 - In the Work Area select the checkbox to the left of the particular branch office in the list and select **Manage**. Selecting the **Manage** button updates the **Branch Office** field, in the Navigation Tree, with the selected branch office and displays information and data in the Work Area for that branch office.
 - Choose a branch office from the **Branch Office** pull-down located in the Navigation Tree. Information and data are displayed in the Work Area.
- 5) Navigate to **Configuration > Security in the navigation tree under Administration**.
(Pre V8 OSB) The **Security** window appears with the **General** tab selected by default.

- 6) (V8 OSB) Select Security > Tunnel Connections. (Pre V8 OSB) Select the **IPsec** tab.

The IP Security settings are displayed in a list with the following columns:

- **Connection Name**: Defines the IPsec connection name.
- **Partner**: Defines the public IP address of the partner VPN (Virtual Private Network) device.
- **Partner Network**: Defines the subnet protected by the partner VPN device.
- **Partner netmask**: Defines the network mask of the subnet protected by the partner VPN device.
- **Side**: Defines if the local host will be the left or right VPN device.
- **Local**: Defines the Public IP address which will be used to establish the IPsec connection.
- **Local network**: Defines the subnet protected by the local VPN device.
- **Local netmask**: Defines the network mask of the subnet protected by the local VPN device.

- 7) To configure the IPsec connections, use one of the following options:

- To remove an entry from the IPsec connections list, select the respective row and click the **Delete** button. The IPsec connection is removed from the list.
- To edit an IPsec connection in the list, select the respective row and click the **Edit** button.
- To add an IPsec connection to the list, click the **Add** button.

(Pre V8 OSB) The **Add/Edit System IP sec** window appears.

- 8) Enter the IPsec connection name in the **(V8 OSB) Connection Name** field or (Pre V8 OSB) **Name**. An unique name should be used for each connection.
- 9) Enter the side of the VPN device (left or right) in the **Side** field.
- 10) Enter the public IP address of the partner VPN device in the **Partner** field.
- 11) Enter the subnet protected by the partner VPN device in the **Partner network** field.
- 12) Enter the network mask of the subnet protected by the partner VPN device in the **Partner netmask** field.
- 13) Enter the Public IP address which will be used to establish the IPsec connection in the **Local** field.
- 14) Enter the subnet protected by the local VPN device in the **Local network** field.
- 15) Enter the network mask of the subnet protected by the local VPN device in the **Local netmask** field.
- 16) Enter the type of authentication in the **(V8 OSB) Auth type or (Pre V8 OSB) Authentication type** field. Possible values: secret, x509 client, x509 server
- 17) Enter the file name for the secret key in the **Secret key file** field. This field defines the shared secret key file for the connection, when the type of authentication is set to "secret".
- 18) 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.

- 19) Checkmark the **(V8 OSB) Compression or (Pre V8 OSB) Enable compression** check box if compression is to be used for this link.
- 20) Checkmark the **(V8 OSB) PFS or (Pre V8 OSB) Enable PFS** check box if Perfect Forward Security (PFS) is to be used for this link.
- 21) (Pre V8 OSB) Click the **OK** button to go back to the **Security** window.
- 22) Click the **OK** button to store the changes temporarily in the administrator's login session and close the **Security** window.
The **Security** dialog disappears.
- 23) Click the **Apply changes** button in the main window, work area, to save the changes permanently.

The IP Security settings are applied on the OpenScape Branch system.

4.5.6 RADIUS Support - Overview

RADIUS-enabled network support is available in OpenScape Branch V7 and later. The OpenScape Branch is enhanced for RADIUS (Authentication, Authorization, and Accounting - AAA) functionality (RFCs 2865ff).

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 Branch solution.

OpenScape Branch provides the ability to connect to two different RADIUS servers.

NOTICE:

The OSB will not support SNMP or SIP authentication or accounting, and it will also not support the RADIUS challenge/response capabilities.

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.

4.5.6.1 How to Configure Radius

Proceed as follows to configure RADIUS-enabled network support, available in OpenScape Branch V7 and later.

Prerequisites

Adequate administrative permissions.

At least one 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 Branch** within the Navigation Bar in the Common Management Platform.
- 2) Select the **Branch Office list** in the Navigation Tree under Administration.
The system presents the **Branch Office Overview** in the Work Area with a current list of all branch offices.

- 3) To view a list of Branch Offices 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 branch office use one of the following options:
 - In the Work Area select the checkbox to the left of the particular branch office in the list and select **Manage**. Selecting the **Manage** button updates the **Branch Office** field, in the Navigation Tree, with the selected branch office and displays information and data in the Work Area for that branch office.
 - Choose a branch office from the **Branch Office** pull-down located in the Navigation Tree. Information and data are displayed in the Work Area.
- 5) Navigate to **Configuration > Security in the navigation tree under Administration**.

(Pre V8 OSB) The **Security** window appears with the **General** tab selected by default.

- 6) Select the **Radius** work area / tab.
- 7) Checkmark the **Enable RADIUS** checkbox to enable configuration of RADIUS servers, authentication and accounting.
- 8) To configure Server 1, proceed as follows:
 - a) Enter the IP Address/FQDN for Server 1 in the (V8 OSB) Address or (Pre V8 OSB) **IP Address/FQDN** field.
 - b) Enter the port number or radius in the **Port** field. The Port field is optional, but can be specified as either **1812** or '**radius**', the latter of which will be looked up from /etc/services.
 - c) Enter the Secret in the **Secret** field. The entry is mandatory and identifies the shared secret that the RADIUS server and the OpenScape Branch share.

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. The length of the secret is limited to 16 characters. It can consist of upper or lower case letters, digits, or special characters. Special characters can be any of the following set:
~!@#\$%^&*()_+|\=-'{}[]:"';<>?/.,

- d) Enter the Timeout in the **Timeout** field in the number of minutes. The value is 1-10 (default = 3).

- 9) To configure Server 2, proceed as follows:
 - a) Enter the IP Address/FQDN for Server 2 in the (V8 OSB) **Address or (Pre V8 OSB) IP Address/FQDN** field.
 - b) Enter the port number or radius in the **Port** field. The Port field is optional, but can be specified as either **1812** or '**radius**', the latter of which will be looked up from /etc/services to derive a port number.
 - c) Enter the Secret in the **Secret** field. The entry is mandatory and identifies the shared secret that the RADIUS server and the OpenScape Branch share.

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. The length of the secret is limited to 16 characters. It can consist of upper or lower case letters, digits, or special characters. Special characters can be any of the following set: ~!@#\$\$%^&*()_+|=‘{ }[]:”’; <>?/.,
 - d) Enter the Timeout in the **Timeout** field to specify how long the OpenScape Branch will wait for a response. The value is 1-10 seconds (default = 3 seconds).t
- 10) To configure RADIUS Authentication, proceed as follows:
 - a) Checkmark the **Enable RADIUS Authentication** checkbox to enable configuration of RADIUS authentication.
 - b) Checkmark the appropriate checkboxes to apply authentication. Checkboxes: CLI, SSH and Web.
- 11) To configure RADIUS Accounting, proceed as follows:
 - a) Checkmark the **Enable RADIUS Accounting** checkbox to enable configuration of RADIUS accounting.
 - b) Checkmark the appropriate checkboxes to apply accounting. Checkboxes: CLI, SSH and Web.
- 12) Click the **OK** button to store the changes temporarily in the administrator's login session.

The **Security** dialog disappears.
- 13) 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. Thus it is not applied to the OpenScape Branch appliance. Please refer to the "OpenScape Branch Assistant – Primary Administration" chapter of this documentation for more information.

4.6 Survivability — Overview

Survivability is the capability of a network to maintain service continuity in the presence of faults within the network.

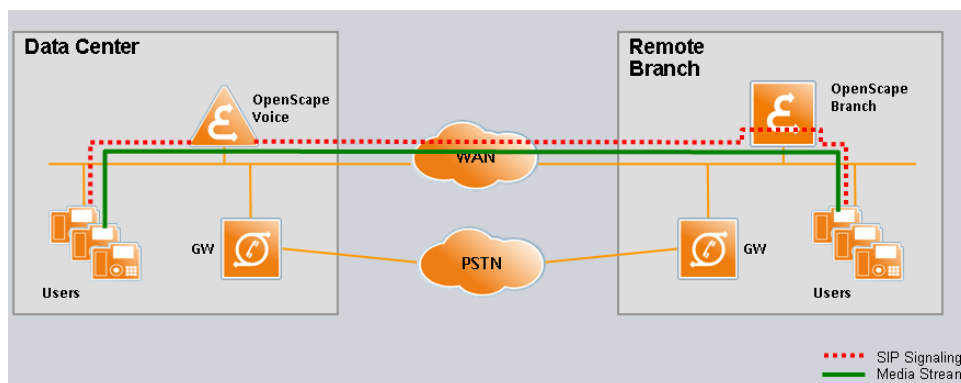
Survivability Mechanisms within OpenScape Voice

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.

Operational States

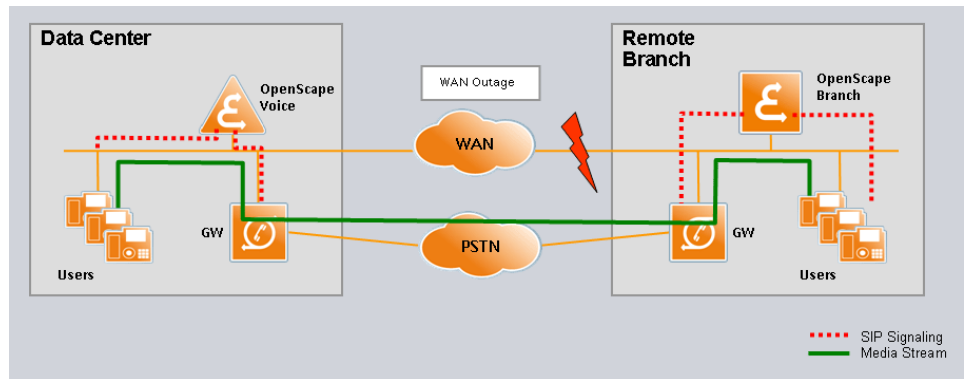
Depending on the network operating state, the OpenScape Branch can be in either one of these three operational states:

- **Normal**



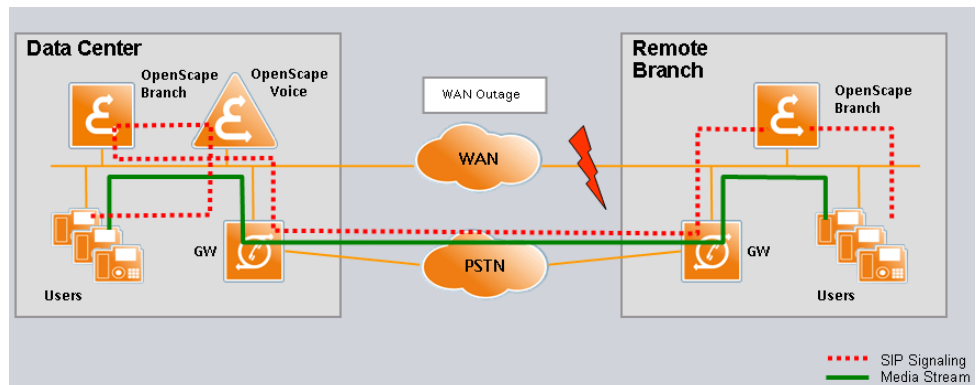
At this state the OpenScape Branch is in full access to the OpenScape Voice and Applications. The openScape Branch relays all the messages to the OpenScape Voice, which provides all the features to the remote users. The payload for inter-branch calls go through the WAN. At the diagram below we see the signaling and media stream path for a call from a user in the branch to a user in the data center.

- **Survivable**



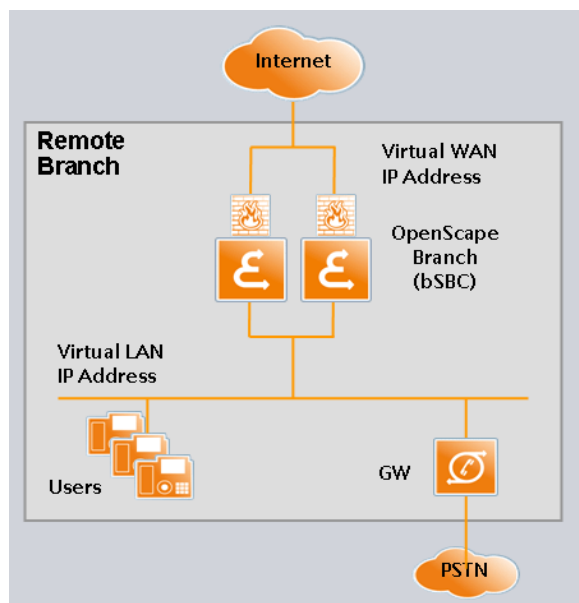
The OpenScape Branch enters in this operational state when there is a partial or complete WAN failure. This state can be reached when a certain number of messages between the OSB and OSV gets lost or are not replied indicating a WAN failure. At this point the OpenScape Branch continues the service to the remote users by its own survivability features, but being a limited feature set compared to the OpenScape Voice features. In addition, for OpenScape Branch V1R4 and higher, music on hold over the survivable gateway/PSTN is supported. All inter-branch calls go through the PSTN. The diagram below shows the signaling and media stream path for a call from a user in the branch to a user in the data center.

- **Backup**



At this state, when the network is configured to support the Backup Signalling Link, the remote OpenScape Branch establish a new path via the PSTN for signalling traffic to the OpenScape Voice to continue to provide the OpenScape Voice high feature set to the remote users. This functionality is currently available to the OpenScape Branch 50 and 50i models. To support this operating state, an OpenScape Branch unit also needs to be deployed at the Data Center to interconnect with the OpenScape Voice. At the diagram below we see the signaling and media stream path for a call from a user in the branch to a user in the data center.

Redundancy



OpenScape Branch Redundancy allows redundancy of an OpenScape Branch unit by having a second unit located on the same subnet having exactly the same database. A communication channel between the two OSB units is used to keep call state information synchronized between the active and standby unit, in order to provide failover with minimal impact on active calls. Some calls may be lost depending on the timing of the failover relative to the calls SIP signaling activity, particularly when a connection oriented protocol (TCP or TLS) is used for the SIP signaling transport. If the Active unit fails, the Stand-by unit becomes the Active and takes over the functionality.

OpenScape Branch — Supported Survivability Features

The OpenScape Branch supports a few features on the B-side of the call:

- Keyset support, forking

During survivability mode, keyset notifications for secondary lines cannot be delivered. However, OpenSER will actively fork the calls to all registered contacts of the keyset. The keyset phones are notified about the limited operational mode with a NOTIFY when the OpenScape Branch entered survivability mode. Forking INVITE messages to keysets means that the INVITE message is sent to each registered contact. When a contact responds with a 200 OK, then all other invited contacts receive a CANCEL request to bring them back to the idle state.

NOTICE: The OpenScape Branch does NOT store any keyset-related subscriptions (e.g. keyset-info). Any such subscription during survivability mode is rejected with a 503 Service Unavailable response.

- Calling a multi line hunt group

To support multi-line hunt groups during survivability mode, the line hunt group members must be manually stored in the OpenScape Branch database by the administrator. The OpenScape Branch supports the

following line hunt groups: pilot hunt group (pilot = subscriber) and non-pilot hunt group (with no master).

Prior to OpenScape Voice V7, data such as Multi-Line Hunt Groups (MLHGs) and Emergency List had to be provisioned separately on OpenScape Branch and OpenScape Voice in order to support these features in the standalone mode. Although MLHG, MLHG members and Emergency List data provisioning is still supported on OpenScape Branch, the administrator may provision these features on OpenScape Voice via OpenScape Voice Assistant, which then synchronizes the data on the OpenScape Branch systems, as needed. The data provisioned via Mass Provisioning is periodically synchronized by OpenScape Voice Assistant. This ensures that all the plausibility checks are done, thus ensuring the data on OpenScape Voice and OpenScape Branch are the same for these features.

NOTICE:

The MLHG configuration is not available if OSB operates in Proxy ACD mode.

- **Emergency Calls**

For OSB V1R3 and higher a list of Emergency numbers is provided. When a number from this list is dialed, the OpenScape Branch identifies it as an Emergency Call.

For OSB V1R2 one emergency number is provided.

For example in the USA this is the 911 emergency number. A call to a number from 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 following:

- 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 (Location Identification Numbers) table.

- **Call forwarding**

Calls forwarded to another destination via a 302 response on the INVITE message are handled as follows: Possibly forked INVITE messages to other registered contacts are cancelled. The "302 request" is modified and forwarded to the calling party. The calling party is responsible for setting up the new call.

- **Call Detail Records during survivability**

OpenScape Branch generates CDRs (Call Detail Records) only for calls that where initiated or terminated during survivability mode. During normal mode all CDR handling is done by the OpenScape Voice System. CDR handling in OpenScape Branch is done by the CDR handler process. This process starts operation when OpenScape Branch enters survivability mode and at least one transaction is completed. The CDR handler terminates operation when the last record that was created during survivability mode is closed, written in the billing file and all the billing files are send via SFTP (Secure File Transfer Protocol) (push mode) to the billing server (primary or backup).

- Music on Hold

For OSB V1R4 and higher Music on Hold is retained during survivability mode. Music on Hold is maintained via the survivable gateway/PSTN.

- SIP Session Refresh

SIP Session Refresh is supported in Survivability Mode, for calls between branch subscribers. It is not supported for the connection with SIP Service Provider.

OpenScape Branch — Survivability Configuration

The OpenScape Branch infrastructure has to be configured according to the survivability model used.

- Multiline Hunting Groups configuration (OSB V1R3 and later Versions only)
- Emergency calling configuration
- Emergency numbers (OSB V1R3 and later Versions only)
- Call Data Records configuration
- Music on Hold configuration

NOTICE:

When operating in Survivability Mode, OSB uses the B2BUA SIP mapped port 10000 identity headers (Via, Contact and From) in the outgoing messages, when a call is routed to SSP via OSB WAN interface. Note that OSB uses internal B2BUA, instead of OSV, when operating in Survivability Mode. Based on this, SSP shall route the messages back to the OSB, based on the Record-Route and not on the Contact header, because OSB doesn't listen on the mapped port on the WAN side.

It is also possible to enable the Global Flag 14 in the OSB configuration file (.xml). Then, the mapped port in Contact header is not included. Enabling this flag also prevents OSB from adding some private parameters in the Record-Route headers.

4.6.1 How to Configure Multiline Hunt Groups for Survivability

Proceed as follows to edit the MLHG (Multiline Hunt Groups) settings for survivability for OpenScape Branch V1R3 or later versions.

Prerequisites

Adequate administrative permissions.

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

The connection to the OpenScape Voice system is up.

The OpenScape Branch Appliance is operating in SBC, SBC Proxy or Proxy mode. The MLHG configuration is not available in Proxy ACD mode.

Notice: Prior to OpenScape Voice V7, data such as Multi-Line Hunt Groups (MLHGs) and Emergency List had to be provisioned separately on OpenScape Branch and OpenScape Voice in order to support these features in the standalone mode. Although MLHG, MLHG members and Emergency List data provisioning is still supported on OpenScape Branch, the administrator may provision these features on OpenScape Voice via OpenScape Voice Assistant, which then synchronizes the data on the OpenScape Branch systems, as needed. The data provisioned via Mass Provisioning is periodically synchronized by OpenScape Voice Assistant. This ensures that all the plausibility checks are done, thus ensuring the data on OpenScape Voice and OpenScape Branch are the same for these features.

Synchronization is limited to Pilot/Members within a single OpenScape Branch. Synchronization will not be possible to multiple OpenScape Branches configured with the same pilot/members in a peer OpenScape Branch setup.

Step by Step

- 1) Navigate to **Configuration tab > OpenScape Branch** within the Navigation Bar in the Common Management Platform.
- 2) Select the **Branch Office list** in the Navigation Tree under Administration.
The system presents the **Branch Office Overview** in the Work Area with a current list of all branch offices.
- 3) To view a list of Branch Offices 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 branch office use one of the following options:
 - In the Work Area select the checkbox to the left of the particular branch office in the list and select **Manage**. Selecting the **Manage** button updates the **Branch Office** field, in the Navigation Tree, with the selected branch office and displays information and data in the Work Area for that branch office.
 - Choose a branch office from the **Branch Office** pull-down located in the Navigation Tree. Information and data are displayed in the Work Area.
- 5) (V8 OSB) Navigate to **Configuration > Features or (Pre V8 OSB) Configuration > Survivability** in the navigation tree under **Administration**.
(V8 OSB) The Features window appears. (Pre V8 OSB) The **Survivability** window appears with the **Multiline Hunting Groups** tab selected by default. The table lists the MLHGs configured for survivability in the OpenScape Branch system.
- 6) (V8 OSB) Locate the Features Available in Survivability Mode Only work area and click the Configure button located next to the Multiline Hunt Group item.

- 7) To edit the Multiline Hunting Groups table, choose one of the following options:
 - To remove a MLHG from the list, check the respective checkbox and click the **Delete** button.
 - To edit the settings of a MLHG, (V8 OSB) Click on the specific data value(s) to be modified and replace it by typing the new value in its place. (Pre V8 OSB) Check the respective checkbox and click the **Edit...** button.
 - To add a new MLHG to the list, click the **Add...** button.(Pre V8 OSB) Depending on the action, the **Add Survivability Multiline Hunting Group** or **Edit Survivability Multiline Hunting Group** window appears.
- 8) Select **Enable** in the checkmark box.
- 9) Enter the MLHG access code in the **Pilot Number** field.
- 10) Select the pilot type from the **Pilot Type** selection list. The following types are available. **pilot**: This type must refer to an existent subscriber destination number. The pilot destination number will be the first group member. **Non pilot**: This can be any code and must not be related to an existent subscriber destination number.
- 11) Select the hunt type from the **Hunt Type** selection list. The following types are available. **Linear**: The hunting will be done always in the same sequence according to the group members order. **Cyclic**: The hunting will be done based on the last subscriber that answered the call, then the next one will be called. **Parallel**: All members will ring simultaneously. **UCD**: The hunting will be done based on the agent who has not been presented a call for the longest period of time (Uniform Call Distribution).
- 12) Enter the time period that each member rings before the next member will be called in seconds in the **No answer advance timer** field.
- 13) Enter the overflow destination in the **Overflow destination** field. In case of no member answers the call, the overflow destination is called. The overflow destination can be a subscriber or another MLHG.
- 14) Enter the members separated by comma in the **Members** field. The order of the members is relevant according to the hunt strategy.
- 15) Click the **OK** button to go back to the **Survivability** window.
- 16) Click the **OK** button to store the changes temporarily in the administrator's login session.

The **Survivability** dialog disappears.
- 17) Click the **Apply changes** button in the main window.

The settings for the multiline hunting groups are applied on the OpenScape Branch system.

4.6.2 How to Configure Emergency Calling for Survivability

Proceed as follows to edit the emergency calling settings for survivability.

Prerequisites

Adequate administrative permissions.

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

The connection to the OpenScape Voice system is up.

Notice: Prior to OpenScape Voice V7, data such as Multi-Line Hunt Groups (MLHGs) and Emergency List had to be provisioned separately on OpenScape Branch and OpenScape Voice in order to support these features in the standalone mode. Although MLHG, MLHG members and Emergency List data provisioning is still supported on OpenScape Branch, the administrator may provision these features on OpenScape Voice via OpenScape Voice Assistant, which then synchronizes the data on the OpenScape Branch systems, as needed. The data provisioned via Mass Provisioning is periodically synchronized by OpenScape Voice Assistant. This ensures that all the plausibility checks are done, thus ensuring the data on OpenScape Voice and OpenScape Branch are the same for these features.

Step by Step

- 1) Navigate to **Configuration tab > OpenScape Branch** within the Navigation Bar in the Common Management Platform.
- 2) Select the **Branch Office list** in the Navigation Tree under Administration.
The system presents the **Branch Office Overview** in the Work Area with a current list of all branch offices.
- 3) To view a list of Branch Offices 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 branch office use one of the following options:
 - In the Work Area select the checkbox to the left of the particular branch office in the list and select **Manage**. Selecting the **Manage** button updates the **Branch Office** field, in the Navigation Tree, with the selected branch office and displays information and data in the Work Area for that branch office.
 - Choose a branch office from the **Branch Office** pull-down located in the Navigation Tree. Information and data are displayed in the Work Area.
- 5) (V8 OSB) Navigate to **Configuration > Features or (Pre V8 OSB) Configuration > Survivability** in the navigation tree.
(V8 OSB) The **Features** window appears. (Pre V8 OSB) The Survivability window appears with the **Multiline Hunting Groups** tab selected by default.

- 6) For OpenScape Branch V1R2, proceed as follows:

- a) Select the **Emergency Calling** tab.

The emergency calling settings for survivability are displayed including a table which contains the configuration of the emergency calling subnets.

- b) Add the emergency number in the **Emergency Number** field. Only one emergency number is available.
c) Continue with step 8.

If this number is dialed, OpenScape Branch identifies it as an "Emergency Call" (for 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).

- 7) (Pre V8 OSB) For OpenScape Branch V1R3 and later versions through V7R1, select the **Emergency Number** tab.

A list of numbers to be identified as emergency calls is displayed.

- 8) (V8 OSB) Locate the Features Available in Survivability Mode Only work area and click the Configure button located next to the Emergency Calling them.

- 9) To add an emergency number to the list, enter the number (e.g. 911 or 112) and click the **Add** button.

If a number from the list is dialed, OpenScape Branch identifies it as an "Emergency Call" (for USA this represents the 911 emergency calls). A call to a number from the emergency number list will trigger the server to try to establish an outgoing call to an available gateway (highest priority).

(V10R2 OSB) It is possible to add regular expression rules in order to set a specific range of numbers. Only numerical digits and the characters *, # and + are supported as literals. The literals * and + must be inside of []. 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 %. A 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).

IMPORTANT:

The "-" suggests a range of numbers but can't be used without [].

IMPORTANT: 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.

- 10) To configure the emergency trunk, proceed as follows:
- Navigate to **(V8 OSB) Configuration > Features or (Pre V8 OSB) Configuration > VoIP**.
(V8 OSB) The Features window appears.
(Pre V8 OSB) The **Voice over IP** window appears with the **General** tab selected by default.
 - Select the **(V8 OSB) Enable gateways/trunk checkbox or (Pre V8 OSB) Enable** checkbox and click the **Configure...** button in the **Gateways** field area.

The **(V8 OSB) Gateways/Trunks or (Pre V8 OSB) Gateways** window appears displaying the gateways configured for the OpenScape Branch system selected in a list.
 - Add the emergency trunk to the list using the **Add...** button.

The **Add VoIP Gateways** window appears.
 - Select the type address for signaling in the **Signaling Address Type** selection list. The following types are available: **IP Address or FDQN or DNS SRV**.
 - Enter the URL of the gateway into the Remote URL field if the **Signaling Address Type** value is set to DNS SRV.
 - Enter the gateway 's IP address or FQDN in the **IP Address/FQDN** field. Either the IP address or FQDN (Fully Qualified Domain Name) can be configured; not both.
 - Enter the SIP (Session Initiation Protocol) port used for communication with gateway in the **Port** field, e.g. 5060.
 - Select the Trunk interface in the **Interface** field, e.g. LAN.
 - Need to add in a Mapped Port field here as it appears to be missing.
 - Enter the SIP transport protocol to be used in communication with the gateway in the **Transport** field, e.g. TCP.
 - Enter the routing prefix in the **Routing Prefix/FQDN** field, e.g. 911999. This parameter defines a valid Dial Number to be used in search for the gateways. The match is done on outgoing gateway calls only and the best match is always used.
 - Select the type of the gateway in the **(V8 OSB) Gateway/Trunk Type or (Pre V8 OSB) Type** selection list. The following types are available: 3k/4k..., RG..., Mediatrix..., Peer OSB, SIP Trunk, Others.
 - Set the functional type of the gateway in the **Functional Type** selection list to **Emergency**. If an emergency call in **Survivability Mode** is set, this route will be used to execute the call. If no emergency is found, the first egress route will be used.

INFO:

(V10R2 OSB) If the gateway is required to make Emergency as well as normal calls, select the **All Modes Egress/Ingress** option.

- Set the trunk profile in the **Trunk Profile** field. This field must be set as Gateway.
- Enter the number of digits to be deleted of the destination URI (Uniform Resource Identifier) in the **Output digit strip** field. The digits are

deleted from the beginning e.g. Output Strip digit = 1 and User dials 9911 which results in the output equal 911.

- p) Enter the digit string to be added to digits of URI in the **Output digit add** field. The digits are added to the beginning.
- q) Leave the **Priority** field blank. The emergency trunk/trunk group has no priority because the emergency trunks/trunk group is connected to the only Central Office or PSAP that has the jurisdiction of the emergency caller area.
- r) Click OK to close the Gateway Configuration window.

- 11) (V8 OSB) Navigate to **Configuration > Features or (Pre V8 OSB) navigate to Configuration > Survivability** and select the **Emergency Calling** tab.

(V8 OSB) Click the Emergency Calling Configure button located in the Features Available in Survivability Mode Only work area. (V8 OSB and Pre V8 OSB) The emergency calling settings for survivability are displayed including a table which contains the configuration of the emergency calling subnets.

- 12) Click the **Add...** button to add a new emergency calling subnet to the list: (V8 OSB) The Emergency Calling Subnet window appears. (Pre V8 OSB) The **Add Emergency Calling** window appears with the **General** tabsheet selected by default.
- 13) Enter the IP address (or range of IP addresses) of the subscriber(s) in the **IP Address** field.
- 14) Enter the IP subnet 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.

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.

- 15) Select the routing prefix from the **Routing Prefix** selection list, e.g. 911999. 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.

INFO:

(V10R2 OSB) If the gateway is required to make Emergency as well as normal calls, select **None**.

- 16) Enter the default destination in the **Default destination** field. The default destination is a fully registered and callable local SIP phone number. When the emergency call to the PSAP (Public Safety Answering Point) fails, the emergency call is redirected to this default destination (attendant) which may have a PSTN land line to call the PSAP directly to report the emergency for the original caller.
- 17) Use the **Send LIN instead of CPN** field. This option enables the use of LINs (Location Identification Number) for emergency calls instead of using the CPN (Calling Party Number) in MIME (Multipurpose Internet Mail Extensions). Use the **Send LIN instead of CPN** option if the Gateway does

not accept the emergency calls using MIME. Default setting: Not checked/ not enabled.

NOTICE:

If all configured LINs are in use; the next emergency call will send CPN information even if the **Send LIN instead of CPN** option is enabled.

- 18) (V8 OSB) Locate the LIN work area. (Pre V8 OSB) Select the **LIN** tabsheet. A table containing Location Identification numbers is displayed. One LIN 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.
- 19) Note: Check the **Use default callback number** checkbox and any callback call is redirected to the default callback number instead of to the original caller.
- 20) To edit the list of the Location Identification Numbers, choose one of the following options:
 - To remove a LIN from the list, check the respective checkbox and click the **Delete** button.
 - To edit the settings of a LIN, check the respective checkbox and click the **Edit...** button.
 - To add a new Location Identification Number to the list, click the **Add...** button.Depending on the action, the **Add LIN** or **Edit LIN** dialog appears.
- 21) Enter the Location Identification Number in the **LIN** field. It is the Location Identification Number used to associate a subscriber to its physical location. Only numerical digits or the character + are supported.

NOTICE: Multiple LINs can be configured per subnet in order to support emergency callbacks from the Emergency Center.

- 22) Enter the **CallBack Number**. It is a callable phone number registered at the PSAP. If an outgoing emergency call is unintentionally interrupted, the remote operator may place a callback call at this number. OpenScape Branch will then redirect the call to the original phone which started the emergency call.
- 23) Enter the **Default CallBack Number**. It is a callable phone number to which the callback call will be redirected if the **Use Default CallBack Number** checkbox is enabled.
- 24) Click the **OK** button to go back to the **(V8 OSB) Emergency Calling or (Pre V8 OSB) Add emergency calling** window.
- 25) Click the **OK** button to go back to the **(V8 OSB) Features window or (Pre V8 OSB) Survivability** window.
- 26) Click the **OK** button to store the changes temporarily in the administrator's login session.
- 27) Click the **Apply changes** button in the main window.

The settings for emergency calls in survivability mode are applied on the OpenScape Branch system.

4.6.3 How to Configure CDR Handling for Survivability

Proceed as follows to configure the settings for CDR (Call Detail Records) handling when the OpenScape Branch operates in survivability mode.

Prerequisites

Adequate administrative permissions.

At least one 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 Branch** within the Navigation Bar in the Common Management Platform.
- 2) Select the **Branch Office list** in the Navigation Tree under Administration.
The system presents the **Branch Office Overview** in the Work Area with a current list of all branch offices.
- 3) To view a list of Branch Offices 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 branch office use one of the following options:
 - In the Work Area select the checkbox to the left of the particular branch office in the list and select **Manage**. Selecting the **Manage** button updates the **Branch Office** field, in the Navigation Tree, with the selected branch office and displays information and data in the Work Area for that branch office.
 - Choose a branch office from the **Branch Office** pull-down located in the Navigation Tree. Information and data are displayed in the Work Area.
- 5) (V8 OSB) Navigate to **Configuration > Features or (Pre V8 OSB) Configuration > Survivability** in the navigation tree.
(V8 OSB) The Features window appears. (Pre V8 OSB) The **Survivability** window appears with the **Multiline Hunting Groups** tab selected by default.
- 6) (Pre V8 OSB) Select the **Call Detail Records** tab.
The settings for the billing servers and billing files are displayed.
- 7) To enable the call detailed tickets being stored during survivability, check the **Enable Ticket Generation** checkbox.
- 8) (V8 OSB) Locate the Features Available in Survivability Mode Only work area. Check the Enable Call Detail Records checkbox and click the Configure button located next to the checkbox.

- 9) Enter the IP address or FQDN of the primary billing server in the **Hostname** field.
- 10) Enter the user name for the primary billing server account to access the server in the **User Name** field.
- 11) Enter the password for the primary billing server account used to access the server in the **Password** field.
- 12) Enter the password for the primary billing server again in the **Confirm Password** field.
- 13) Enter the IP address or FQDN of the secondary billing server in the **Hostname** field.
- 14) Enter the user name for the secondary billing server account to access the server in the **User Name** field.
- 15) Enter the password for the secondary billing server account used to access the server in the **Password** field.
- 16) Enter the password for the secondary billing server again in the **Confirm Password** field.
- 17) Enter the maximal number of CDR records stored in a single billing file in the **Maximum number of records** field.
- 18) Enter the time interval for the billing files to be stored in the permanent storage device (FLASH memory or DISK) in the **Maximum time interval (min)** field.
- 19) Enter the maximal size in kbytes of the billing file in the **Maximum file size (kbytes)** field.
- 20) Enter the transfer method in the **Transfer method** field. This defines the method used to transfer the files to the Billing Server. In **push** mode OpenScape Branch will send the billing files to the billing server. In **pull** mode OpenScape Branch stores the billing files and the billing server is responsible for retrieving the billing files via SFTP. Default value: push
- 21) Enter the port used for SFTP when accessing the remote billing server in the **Port** field.
- 22) Enter the time duration OpenScape Branch shall wait before re-attempting an SFTP transfer in push mode in the **Re-attempt timer (min)** field.
Allowed min value: 1, allowed max value: 1440 (1 day), default value: 5.
- 23) To choose the "allow file overwrite" option, check the **Allow file overwrite** checkbox. Billing files may be overwritten.
- 24) To enable the "E.164 Translation" option, check the **E.164 Translation** checkbox. (Pre V8 OSB) Select the **Configure** button.

The **Digit Translation** dialog appears and displays a list of Matching digits and Translation digits.
- 25) To add numbers to be translated to the list, click the **Add** button.

(Pre V8 OSB) The **Add Digit Translation** dialog appears and displays a list of Matching digits and Translation digits.
- 26) Enter the digits to be matched in the **Matching Digits** field. When a match is found on the digit string the digits will be converted to the Translation digits.
- 27) Enter the translated-to digits for the associated matching digits in the **Translation** field.

- 28) (Pre V8 OSB) Click the **OK** button to store the changes temporarily in the administrator's login session.
- (V8 OSB) The Call Detail Records window disappears. (Pre V8 OSB) The **Add Digit Translation** dialog disappears and the **Digit Translation** dialog appears with the updated translation list.
- 29) Click the **OK** button to store the changes temporarily in the administrator's login session.
- (V8 OSB) The **Features or (Pre V8 OSB) Survivability** dialog disappears.
- 30) Click the **Apply changes** button in the main window.

The settings for CDR in survivability mode are applied on the OpenScape Branch system.

4.6.4 How to Configure Music on Hold Handling for Survivability

Proceed as follows to configure the settings for Music on Hold (MoH) handling when the OpenScape Branch operates in survivability mode.

Prerequisites

Adequate administrative permissions.

At least one 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 Branch** within the Navigation Bar in the Common Management Platform.
- 2) Select the **Branch Office list** in the Navigation Tree under Administration.
The system presents the **Branch Office Overview** in the Work Area with a current list of all branch offices.
- 3) To view a list of Branch Offices 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 branch office use one of the following options:
 - In the Work Area select the checkbox to the left of the particular branch office in the list and select **Manage**. Selecting the **Manage** button updates the **Branch Office** field, in the Navigation Tree, with the selected branch office and displays information and data in the Work Area for that branch office.
 - Choose a branch office from the **Branch Office** pull-down located in the Navigation Tree. Information and data are displayed in the Work Area.

- 5) (V8 OSB) Navigate to **Configuration > Features or (Pre V8 OSB) The Survivability** in the navigation tree under **Administration**.
The **Survivability** window appears with the **Multiline Hunting Groups** tab selected by default.
- 6) (V8 OSB) Locate the Features Available in Survivability Mode only work area. (Pre V8 OSB) Select the **Music On Hold** tab.
The settings for survivability music on hold are displayed.
- 7) To enable music on hold during survivability for external calling parties in the public network, (V8 OSB) Enable the checkbox and select the Enable Music On Hold for Gateways drop down value or (Pre V8 OSB) check the **Enable MOH** checkbox.
- 8) To enable music on hold during survivability for internal calling subscribers in the private network, (V8 OSB) Enable the checkbox and select the Enable Music On Hold for Gateways and Subscribers drop down selection or (Pre V8 OSB) check the **Enable MOH for Subscribers** checkbox.
(Pre V8 OSB) The Enable MOH option must be enabled to select this option.
- 9) Click the **OK** button to store the changes temporarily in the administrator's login session.
(V8 OSB) Features or (Pre V8 OSB) the **Survivability** dialog disappears.
- 10) Click the **Apply changes** button in the main window.
- 11) Need to add in information related to System calling number suppression access code checkbox at the bottom of the screen.

The settings for Music on Hold in survivability mode are applied on the OpenScape Branch system.

4.7 System Settings — Overview

The system settings mainly serve to configure the protocols and password settings of the OpenScape Branch system and enables the administrator to perform some service tasks.

General Settings

Via OpenScape Branch Assistant the following protocols, interfaces or system parameters can be configured:

- **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. OpenScape Branch devices will register with the License Server URI to obtain licensing information (note: the URI will be provisioned with the OpenScape Branch Assistant IP and port 4709 for OpenScape Branch access but in the future the license server may be another server).
- 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 Branch or OpenScape SBC.

Password

To access an OpenScape Branch 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 Branch device.

There is a one (common) default password for all OpenScape SBC and Branch devices in order to ease the access of CMP (Common Management Platform) to different OpenScape SBCs and Branch 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 or Branch device and has no expiration time.

NOTICE:

Changing the password stored in the assistant's local database is possible via the **Password** button in the **Overview** window. This it is not applied to the OpenScape SBC or Branch appliance. Please refer to the "OpenScape Branch Assistant – Primary Administration" chapter of this documentation 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.

In OpenScape Branch V8, the Import and Export functions are supported under **Configuration > OpenScape Branch > Configuration > System**.

In OpenScape Branch V7 and earlier, the Import and Export functions are supported in the OpenScape Branch Assistant under **Configuration > OpenScape Branch > Configuration > Maintenance**.

Additional System Settings:

The following system parameters are configured in the Network Service section.

DLS (Deployment and Licensing Tool)

DLS serves to update the phone image from a DLS server. In order to configure the phones automatically, DHCP is used and one field of the DHCP message to the phones contains the DLS address.

NOTICE:

Please refer to the **Configuration chapter, Network Services section** of this document for configuration information.

Redundancy

The system settings also provide the configuration of redundancy for OpenScape Branch offices. In case a node fails, redundancy handles basic call processing. Call Detailed Records (CDR) is not synchronized between nodes.

NOTICE:

Please refer to the **Configuration chapter, Network Services section** of this document for configuration information.

4.7.1 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 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 Branch** within the Navigation Bar in the Common Management Platform.
- 2) Select the **Branch Office list** in the Navigation Tree under Administration.
The system presents the **Branch Office Overview** in the Work Area with a current list of all branch offices.
- 3) To view a list of Branch Offices 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 branch office use one of the following options:
 - In the Work Area select the checkbox to the left of the particular branch office in the list and select **Manage**. Selecting the **Manage** button updates the **Branch Office** field, in the Navigation Tree, with the selected branch office and displays information and data in the Work Area for that branch office.
 - Choose a branch office from the **Branch Office** pull-down located in the Navigation Tree. Information and data are displayed in the Work Area.

- 5) (V8 OSB) Click the Licenses selection and locate the General work area in the System window. (Pre V8 OSB) 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 Port:**

Note: The URI will be provisioned with the OpenScape Branch Assistant IP and port 4709 for OpenScape Branch access but in the future the license server may be another server.

- **Backup management server and port:**

Note: The URI will be provisioned with the OpenScape Branch Assistant IP and port 4709 for OpenScape Branch access but in the future the license server may be another server.

NOTICE: The values in the Licensing section are pre-configured via the USB stick installation of the OpenScape Branch.

- 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 Branch system.

4.7.2 How to Change or Reset Passwords

Proceed as follows to change or reset the login passwords for the access to the OpenScape Branch system.

Prerequisites

Adequate administrative permissions.

At least one 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 Branch** within the Navigation Bar in the Common Management Platform.

- 2) Select the **Branch Office list** in the Navigation Tree under Administration.

The system presents the **Branch Office Overview** in the Work Area with a current list of all branch offices.

- 3) To view a list of Branch Offices 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 branch office use one of the following options:
 - In the Work Area select the checkbox to the left of the particular branch office in the list and select **Manage**. Selecting the **Manage** button updates the **Branch Office** field, in the Navigation Tree, with the selected branch office and displays information and data in the Work Area for that branch office.
 - Choose a branch office from the **Branch Office** pull-down located in the Navigation Tree. Information and data are displayed in the Work Area.

- 5) (V8 OSB) Click the Password button in the displayed OpenScape Branch Overview. (Pre V8 OSB) Navigate to **Configuration > System in the navigation tree under Administration**.

The **System** window appears with the **General** tab selected by default.

- 6) (Pre V8 OSB) 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, ACD, cdr.
- 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 Branch 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, ACD, assistant, cdr, redundancy user.
 - b) Check the Update password on appliance checkbox and enter the old password in the **Current appliance password** field.
 - c) Enter the new password of the OpenScape Branch appliance in the **New Password** field. The password must be 8...36 characters, with at least one upper case letter, one lower case, one digit and one special character.
 - d) Enter the new local password of the OpenScape Branch 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 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 is not applied to the OpenScape Branch appliance. Please refer to the "OpenScape Branch Assistant – Primary Administration" chapter of this documentation for more information.

Related concepts

[Password Management](#) on page 87

Related tasks

[How to Change the Password in the Local Assistant Database](#) on page 44

4.7.3 How to Import/Export and Select Configuration Files via OpenScape Branch Assistant

Proceed as follows to import/export and select configuration files using OpenScape Branch Assistant.

Prerequisites

Adequate administrative permissions.

At least one 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 Branch** within the Navigation Bar in the Common Management Platform.
- 2) Select the **Branch Office list** in the Navigation Tree under Administration.
The system presents the **Branch Office Overview** in the Work Area with a current list of all branch offices.
- 3) To view a list of Branch Offices 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 branch office use one of the following options:
 - In the Work Area select the checkbox to the left of the particular branch office in the list and select **Manage**. Selecting the **Manage** button updates the **Branch Office** field, in the Navigation Tree, with the selected branch office and displays information and data in the Work Area for that branch office.
 - Choose a branch office from the **Branch Office** pull-down located in the Navigation Tree. Information and data are displayed in the Work Area.

- 5) (V8 OSB) Navigate to **Configuration > Maintenance** in the navigation tree. *(Pre V8 OSB) Navigate to **Configuration > System** in the navigation tree under **Administration**.*

(Pre V8 OSB) The **System** window appears with the **General** tab selected by default.

- 6) Select the **Import/Export** tab to import or export a configuration file, or select the configuration to use.

(V8 OSB) The Configuration file in use or (Pre V8 OSB) **File in use** field displays the name of the configuration file currently in use.

- 7) (V8 OSB) Locate the Import work area and 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 Upload button. The 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) (Pre V8 OSB) Click the **Import** button to import a new configuration file to the OpenScape.

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.

- 9) 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 Change in the main window.

- 10) 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 Change in the main window.

- 11) To select (load) a new configuration file for use:
 - a) Select the configuration file in the **(V8 OSB) Import work area's Select a configuration file dropdown or (Pre V8 OSB) Use a new configuration file** field list.
 - b) Click the **Load** button

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

- 12) (V8 OSB) Close or (Pre V8 OSB) click the **OK** button to store the changes temporarily in the administrator's login session.

The **System** dialog disappears.

- 13) Click the **Apply changes** button in the main window.

The configuration files are stored to the OpenScape Branch system.

IMPORTANT:

Action **Restore** of OpenScape Branch data functionality is not supported. Please import configuration file from **Import / Export** functionality in OpenScape Branch Assistant.

4.7.4 How to access & apply Delta XML to an OSB via OpenScape Branch Assistant

Proceed as follows to access & apply Delta XML to an OSB via OpenScape Branch Assistant.

Prerequisites

Adequate administrative permissions.

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

The connection to the OpenScape Voice system is up.

A `deltaXml.xml` file created and uploaded to the CMP

Step by Step

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

The system presents the **Branch Office Overview** in the Work Area with a current list of all branch offices.

NOTICE: Please be aware that the list of OpenScape SBCs and OpenScape Branches is not displayed in any particular order, i.e., the list is not sorted alphabetically on the Branch Name but is instead a random list of entries. However, the list displayed on the right side of the screen under OpenScape Branch Overview - All Systems is

consistent with the order of the list displayed in the drop down list under Select Branch Office.

- 3) Proceed as follows :
 - a) Checkmark the OpenScape Branch Office to be edited from the list.
 - b) Click the **Edit...** button.

The **Edit OpenScape Branch** dialog is displayed.
 - c) Select the associated **Profile Name** from the pull-down field to select or change the profile.
 - d) Select the OSB that you want to apply the delta XML (It has to be an OSB of version **V9 R0.03.00** and above) and press the **Edit...** button.
 - e) In the popup that will open, select the **Delta XML** from the Profile Name drop down menu. Press **OK**, and the `deltaXml.xml` file will be applied to the OSB.

You will get a success message with the success result together with the contents of the `fileResultFtp<OSB_IP>`

If not, you will get an error message with the reason that the action failed.
- 4) Navigate to **Job Management** in the navigation tree under **Administration**.
- 5) Click the **Add...** button to add a new job.
- 6) In the **Add Schedule** PopUp that opens, select **Action: Assign profile**, then press the button ... next to the **Profile textfield** to select a Profile. Select the DeltaXML profile in the **select Profile** popup and press **OK**.
- 7) In the list of Nodes at the bottom of the **Add Schedule** PopUp, press the **Add...** button to add a node.
- 8) In the popup that opens, you will see a list of OSBs of Version **V9 R0.03.00** and above. Select one and press **OK**.
- 9) Click the **OK** button to save the schedule. The schedule will be saved and few seconds later if you press the **Refresh** button on the list of Jobs, its state will turn to **IN PROGRESS**.
- 10) If you press the **Refresh** button again, after a few seconds If the job is finished successfully, you will see the status **COMPLETED** next to the Job. If not, you will see the status **FAILED**.
 - a) If failed, you can select this job, press the "**ViewDetailed Status...**" button and a popup appears.
 - b) In this popup, if you select the **FAILED** status in the list of Statuses, and press the **View results...** button, you will see the reason that the `LoadDeltaXmlFtp` request failed.

4.8 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 Branch Assistant allows to configure the settings for "Voice over IP" telephony, the communication system and periphery for OpenScape Branch.

General Configuration

Some functionality and configuration is specific to OpenScape Branch.

- Country Configuration Display (V7R1)
- Supported deployment modes: Central SBC (OpenScape SBC), Proxy, Proxy ACD, SBC Proxy, Branch SBC, Proxy ATA (V2).
- SIP Header Manipulation (applies in survivability mode)
- SIP Routing
- Error Codes
- Call Forwarding (applies in survivability mode) (this feature is only available for OSB V1R4 and later versions)
- Listening Ports
- Port Mapping
- Backup Data Channel (this feature is only available for OSB V1R3 and later versions)
- Remote Endpoints
- Gateways
- SIP Service Provider Profiles (this feature is only available for OSB V1R3 and later versions)
- Quality of Service
- Media Servers
- Ms Profiles
- Signaling and Transport Settings (TCP, INVITE)
- Office Codes per Trunk Group

Communication System Configuration

- Comm System Type
- Outbound SIP Server
- Trusted IP Addresses
- Node 1 settings
- Node 2 settings
- Administration for Hosted Branch

Timers and Thresholds

Several timers and thresholds can be configured to control the system performance of the OpenScape Branch appliance.

Codecs

Configuration of the codec priority list for codec negotiation.

RTP (Real Time Protocol) Settings

The configuration of the RTP settings is only relevant for systems with an integrated gateway such as the OpenScape Branch 50i and if the integrated gateway is enabled.

Throttling, Registration Expiry and Remote Subscribers

Throttling and registration expiry can be configured for an OpenScape 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.

Country Specific Parameters

The OpenScape Branch can be configured to fulfill the country specific parameters. The following countries are supported:

- Argentina
- Australia
- Belgium
- Brazil
- Bulgaria
- Chile
- China
- Czech Republic
- Denmark
- Estonia
- Finland
- France
- Germany
- Greece
- Hungary
- India
- Israel
- Italy
- Japan
- Lithuania
- Malaysia
- Mexico
- Netherlands
- New Zealand
- Norway
- Panama
- Philippines
- Poland
- Portugal
- Russian Federation
- Singapore
- South Africa
- Spain
- Sweden
- Switzerland
- Taiwan
- Thailand
- Turkey
- United Kingdom
- United States / North America
- United States Circa 1950 / North America
- Venezuela

Service Endpoint Profiles

Endpoint Service Profiles provides the ability to configure integrated gateways FXS associated parameters in the OpenScape Branch 50i and for the Proxy ATA.

4.8.1 Country Configuration - Overview

The OpenScape Branch configuration moved to VoIP from the Integrated Gateway configuration area in V7R1. This allows configuration and display for country related parameters for an OpenScape Branch that is not configured with an integrated gateway.

4.8.1.1 How to Display Country Configuration Information

Proceed as follows to view country specific configuration information.

Prerequisites

Adequate administrative permissions.

The connection to the OpenScape Voice system is up.

The OpenScape Branch is already enabled.

Step by Step

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

2) Select the **Branch Office list** in the Navigation Tree under Administration.

The system presents the **Branch Office Overview** in the Work Area with a current list of all branch offices.

3) To view a list of Branch Offices 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 branch office use one of the following options:

- In the Work Area select the checkbox to the left of the particular branch office in the list and select **Manage**. Selecting the **Manage** button updates the **Branch Office** field, in the Navigation Tree, with the selected branch office and displays information and data in the Work Area for that branch office.
- Choose a branch office from the **Branch Office** pull-down located in the Navigation Tree. Information and data are displayed in the Work Area.

- 5) (V8 OSB) Navigate to **Configuration > System > Settings** in the navigation tree under **Administration** or (Pre V8 OSB) navigate to **Configuration > VoIP** in the navigation tree under **Administration**.

(V8 OSB) The System configuration window appears with the **Settings** tab elected. (Pre V8 OSB) The **Voice over IP** configuration window appears with the **General** tab selected by default.

- 6) Select a country in the **Country** field.
7) Click the **Country Configuration Info...** button.

The **Country Configuration** window appears displaying the default settings of the hookflash timers, ring cadence and tone frequency.

- 8) Click the **(V8 OSB) Country Configuration** button or **(Pre V8 OSB) Close** button to return to the **Voice over IP** window.

Example

The detailed information for the United States is as follows:

```
# General
#
country                = United States / North America (us)
DTMF Interdigit time   = 40 ms
DTMF high level        = -10 dbm
DTMF low level         = -10 dbm
MFR1 level             = -10 dbm
MFR2 level             = -8 dbm
Ring cadence           = 2000,4000 ms
#
# The tonelist itself is defined by a comma-separated
# sequence of elements.
# Each element consist of a frequency (f) with an optional
# duration (in ms)
# attached to it (f/duration). The frequency component may
# be a mixture of two
# frequencies (f1+f2) or a frequency modulated by another
# frequency (f1*f2).
# The implicit modulation depth is fixed at 90%, though.
# If the list element starts with a !, that element is NOT
# repeated,
# therefore, only if all elements start with !, the
# tonelist is time-limited,
# all others will repeat indefinitely.
#
# Frequency (Hz)
# Duration (ms)
#
dial tone               = 350+440
busy tone               = 480+620/500,0/500
ring tone               = 440+480/2000,0/4000
congestion tone         = 480+620/250,0/250
callwaiting tone        = 440/300,0/10000
dialrecall tone         = !350+440/100,!0/100,!350+440/100,!
0/100,!350+440/100,!0/100,350+440
record tone             = 1400/500,0/15000
info tone               = !950/330,!1400/330,!1800/330,0
```

```
stutter tone          = !350+440/100,!0/100,!350+440/100,!
0/100,!350+440/100,!0/100,!350+440/100,!0/100,!
350+440/100,!0/100,!350+440/100,!0/100,350+440
```

4.8.1.2 How to Configure Country Specific Information

Proceed as follows to view country specific configuration information.

Prerequisites

Adequate administrative permissions.

The connection to the OpenScape Voice system is up.

The OpenScape Branch is already enabled.

Step by Step

- 1) Navigate to **Configuration tab > OpenScape Branch** within the Navigation Bar in the Common Management Platform.
- 2) Select the **Branch Office list** in the Navigation Tree under Administration.
The system presents the **Branch Office Overview** in the Work Area with a current list of all branch offices.
- 3) To view a list of Branch Offices 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 branch office use one of the following options:
 - In the Work Area select the checkbox to the left of the particular branch office in the list and select **Manage**. Selecting the **Manage** button updates the **Branch Office** field, in the Navigation Tree, with the selected branch office and displays information and data in the Work Area for that branch office.
 - Choose a branch office from the **Branch Office** pull-down located in the Navigation Tree. Information and data are displayed in the Work Area.
- 5) (V8 OSB) Navigate to **Configuration > System > Settings**. (Pre V8 OSB) Navigate to **Configuration > VoIP** in the navigation tree under **Administration**.
(V8 OSB) The System configuration window appears with the Settings tab selected. (Pre V8 OSB) The **Voice over IP** configuration window appears with the **General** tab selected by default.
- 6) Select a country in the **Country** field list.
- 7) (Optional) (V8 OSB) Click the **Country Configuration button** or (Pre V8 OSB) **Country Configuration Info...** button.
The **Country Configuration** window appears displaying the default settings of the hookflash timers, ring cadence and tone frequency.
- 8) (Optional) Click the **Close** button to return to the (V8 OSB) **System** or (Pre V8 OSB) **Voice over IP** window.

- 9) Click the **OK** button to close the **(V8 OSB) System or (Pre V8 OSB) Voice over IP** window.
- 10) Click the **Apply changes** button in the main window to complete the update.

The setting of the country specific parameters are applied on the OpenScape Branch system.

4.8.2 Branch Deployment Modes

The OpenScape Branch has the flexibility to support, depending on the network topology, four different operating modes.

OpenScape Branch can operate in one of the following modes:

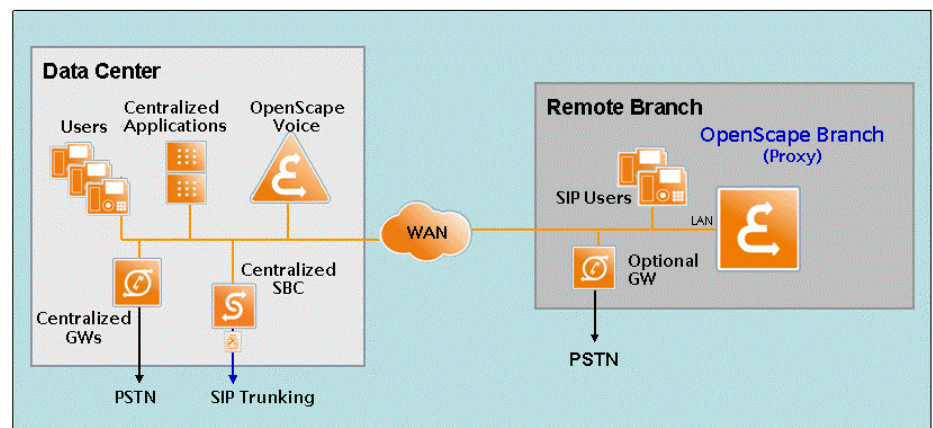
- **Branch Proxy**
- **Branch SBC-Proxy**
- **Branch SBC**
- **Proxy ACD**
- **Proxy ATA**

All modes provide the forwarding and redirect functionality for traffic from and to the Endpoints, Media server and Trunks associated with the OpenScape Branch. The OpenScape Branch provides survivability in case the OpenScape Voice system is not reachable.

The OpenScape Session Border Controller is an additional mode defined under OpenScape Branch configuration. Refer to OpenScape Session Border Controller documentation for details.

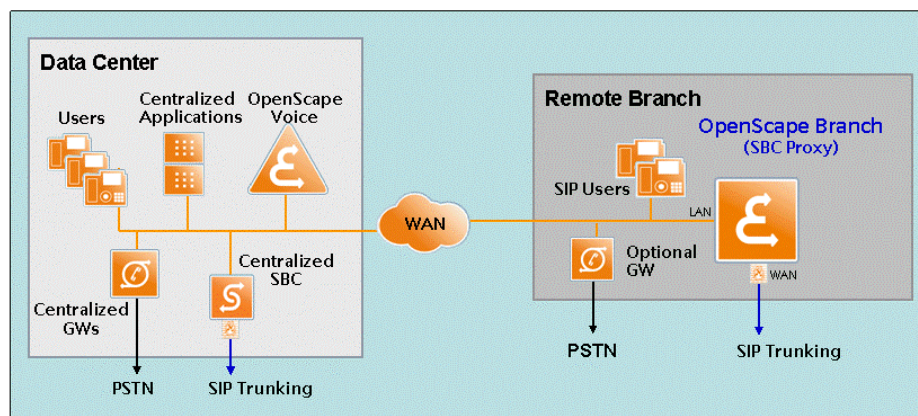
- **Central SBC**

Branch Proxy Operating Mode



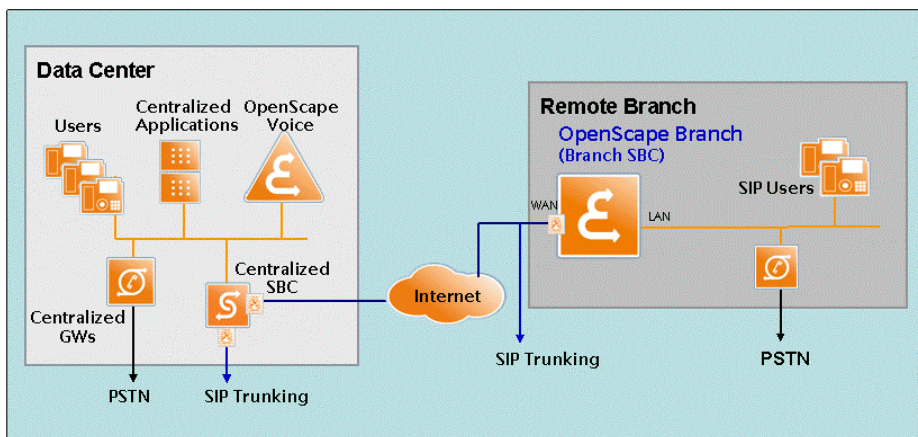
The Proxy mode is for regular proxy usage when branch is connected via a private network.

Branch SBC- Proxy Operating Mode



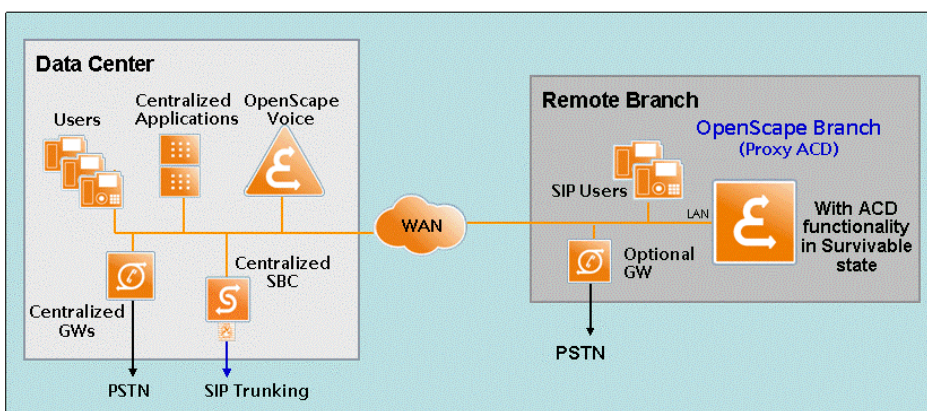
The SBC Proxy mode is for regular proxy connected via a private network and with Branch SBC SIP Trunking connectivity.

Branch SBC Operating Mode



The Branch SBC (Session Border Controller) mode is for deployments when the Branch is connected via a public network and require the use of SBCs.

Proxy ACD Operating Mode



The Proxy ACD (Automatic Call Distribution) mode is for regular proxy connected via a private network and the capability to provide ACD functionality during survivability.

Proxy ATA Operating Mode

There are several OpenScape 50i Proxy ATA applications (Version 2).

OpenScape 50i Proxy ATA Connected via a Proxy OpenScape Branch:

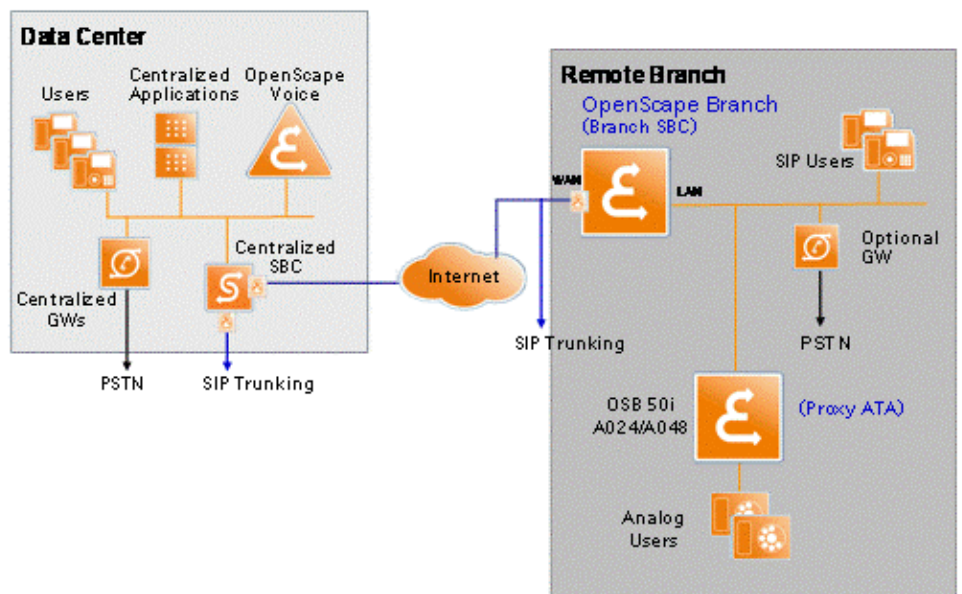
In the figure below, the upstream device is shown as an OpenScape Branch with an external gateway. An alternative to this arrangement would be to use an OpenScape Branch 50i with an internal gateway. The OpenScape Branch is connected to the OpenScape Voice over a corporate WAN, but it could also be connected over a LAN if the Remote Branch is co-located with the OpenScape Voice.

The Proxy ATA registers with only one OpenScape Branch. The Proxy ATA will not support SIP Service Provider trunks.

In this application, the OpenScape Voice can be either in simplex node, or a pair of nodes operating as a cluster (co-located).

If Survivability is required for the OpenScape Branch 50i A024/A048, it will require another upstream device to provide its connectivity to the PSTN. In this configuration, it is required that the upstream device be in the same physical location as the OpenScape Branch 50i A024/A048.

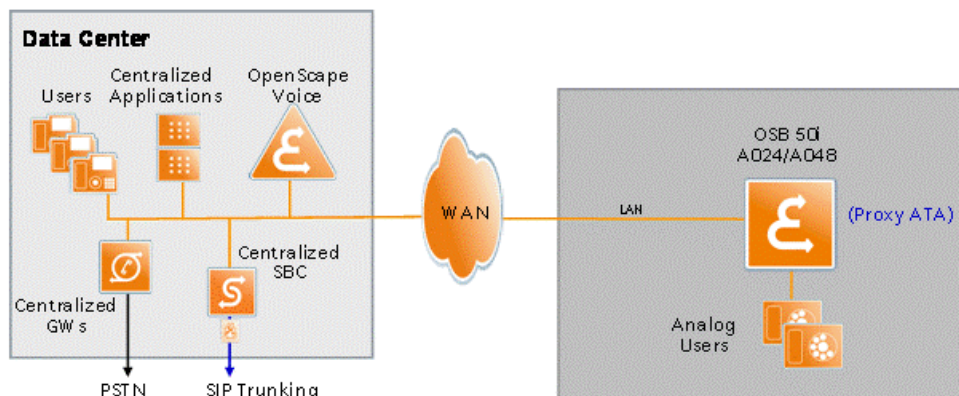
Connected via a Proxy OpenScape Branch



OpenScape 50i Proxy ATA Connected Directly to OpenScape Voice:

The OpenScape Branch 50i A024/A048 can also be utilized as an Analog Terminal Adapter (ATA) connected directly to an OpenScape Voice. The figure below, shows the configuration where the connection to the OpenScape Voice is across a WAN.

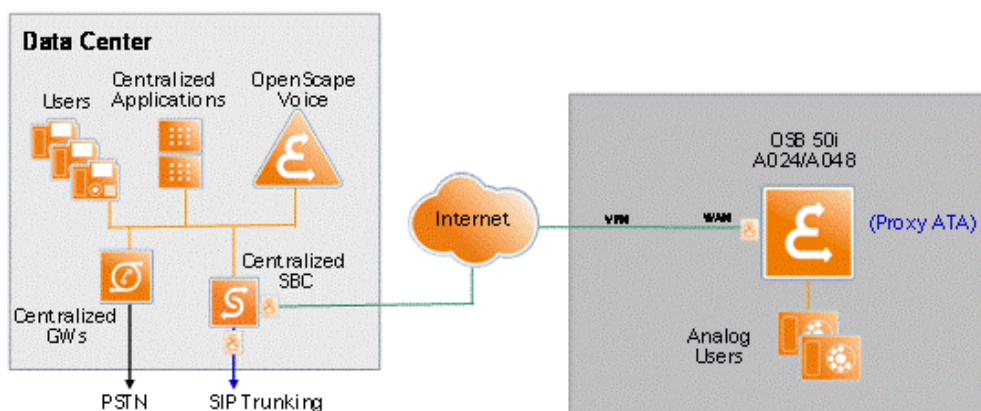
Connected Directly to OpenScape Voice



OpenScape 50i Proxy ATA Connected OpenScape Voice Across the Public Network:

The application, as shown in the figure below, has the OpenScape Branch 50i A024/A048 connected to the OpenScape Voice across a public network. In this configuration, the OpenScape SBC is used. The VPN connection is established at the NAT device.

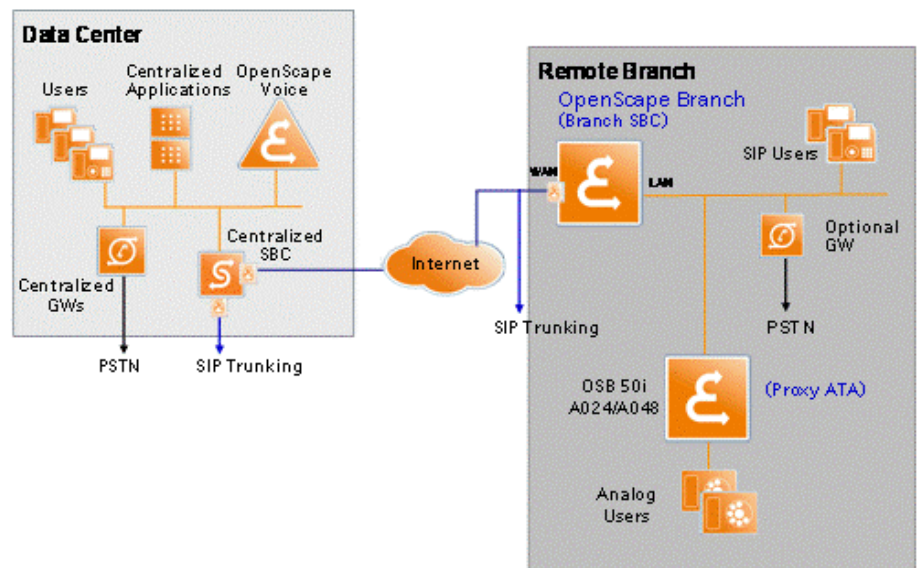
Connected to OpenScape Voice Across Public Network



OpenScape 50i Proxy ATA Connected to OpenScape Branch 50i in Branch SBC Mode:

This application shows the OpenScape Branch 50i A024/A048 connected to a OpenScape SBC via another OpenScape Branch running in Branch SBC mode.

Connected to OpenScape Branch 50i in Branch SBC Mode



4.8.2.1 How to Set the Deployment Mode

Proceed as follows to set the OpenScape Branch appliance to Proxy, Proxy ACD, SBC Proxy or to Branch SBC mode.

Prerequisites

Adequate administrative permissions.

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

The connection to the OpenScape Voice system is up.

The OpenScape Voice system has been configured according to the deployment mode of the OpenScape Branch system to be configured.

Step by Step

- 1) Navigate to **Configuration tab > OpenScape Branch** within the Navigation Bar in the Common Management Platform.
- 2) Select the **Branch Office list** in the Navigation Tree under Administration.
The system presents the **Branch Office Overview** in the Work Area with a current list of all branch offices.
- 3) To view a list of Branch Offices 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 branch office use one of the following options:
- In the Work Area select the checkbox to the left of the particular branch office in the list and select **Manage**. Selecting the **Manage** button updates the **Branch Office** field, in the Navigation Tree, with the selected branch office and displays information and data in the Work Area for that branch office.
 - Choose a branch office from the **Branch Office** pull-down located in the Navigation Tree. Information and data are displayed in the Work Area.
- 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 deployment mode in the **Mode** selection list. Possible values: Branch Proxy, Branch SBC, Branch SBC-Proxy, Proxy ACD or Proxy ATA.
- **Branch Proxy**
OpenScape Branch 500i (OSB) V2 and later supports **Proxy** mode.
 - **Branch SBC**
The WAN interface will be activated and is used to access the OpenScape Voice network.
OpenScape Branch 500i (OSB) V7 and later supports **Branch SBC** mode .
 - **Branch SBC-Proxy**
The WAN interface will be activated and is used to access SIP Service Providers. Subscribers and OpenScape Voice are in LAN as in Proxy mode.
OpenScape Branch 500i (OSB) V7 and later supports **SBC-Proxy** mode .
 - **Proxy ACD**
When the OpenScape Branch mode is changed to Proxy ACD mode, in the Survivability Features tab the MLHG (Multi Line Hunting Group) feature is replaced by the Automatic Call Distribution (ACD) feature.
OpenScape Branch 500i (OSB) V7 and later supports **Proxy ACD** mode .
 - **Proxy ATA (OSB V2)**
Configured for OpenScape Branch 50i with A024 or A048 FXS ports.
The following functions are not permitted with server in Proxy ATA mode: Multiline Hunt Group, Call Detailed Records, Backup Data Channel, External Gateways/Trunks, Automatic Call Distribution (ACD) and Auto-Attendant.

- 7) Click the **OK** button to close the **Voice over IP** window.
- 8) Click the **OK** button to store the changes temporarily in the administrator's login session.

The **System** dialog disappears.

- 9) Click the **Apply changes** button in the main window.

IMPORTANT: The system restarts after saving the configuration when the mode has been changed. Therefore active calls may be dropped.

The setting of the deployment mode is applied on the OpenScape Branch system and the system restarts automatically.

4.8.3 SIP Header Manipulation

When the OpenScape Branch system operates in survivability mode, the SIP headers are modified according to rules. SIP header manipulation is not applied for emergency numbers called.

Parameters to Define Rules

To define rules for the header manipulation, the following parameters are available:

- Match digits
This parameter defines the matching digits. Only numerical digits and the characters *, # and + are supported.
- Match position
This parameter defines from which digit position the matching is performed on the header. The first position is 0.
- Header
Defines the SIP header the rule applies for. For Proxy ACD mode, only R-URI and From headers are supported.
- Delete/insert position
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
Defines digits to be inserted at the defined position. Only numerical digits and the characters *, # and + are supported.
- Add prefix
This parameter is used to set the prefix to be added to the digits on the header. Only numerical digits and the characters *, # and + are supported.
- Replace all with
The digits to replace all header digits. Only numerical digits and the characters *, # and + are supported.
- Call type
Defines which calls the rule is applied: SIP-SIP, SIP-PSTN, PSTN-SIP or to all call types. NOTE: For Proxy ACD mode, the unique supported option is for all call types.

More Than One Rule Matches

If the header digits of a message match more than one rule, only the best matching rule is applied to this header. The best matching rule is the rule that matches the header digits and complies the following criteria, from the higher priority to the lower priority:

- The biggest "Match digits" length.
- The smallest "Match position" value.
- The biggest "Match digits" value in lexicographical order.

A rule for header manipulation may look as follows:

Row	Match digits	Match position	Header	Delete/Insert position	Number of digits to delete	Insert digits	Add prefix	Replace all with
1	53	4	R-URI		1			5558880000
2	561719	0	R-URI		6		555888	
3	305	0	R-URI	1	2	44		
4	52	0	R-URI				555888	

The following table describes what OpenScape Branch will do based on the SIP manipulation rules in this examples (rules priority applies for best match from left to right):

Row	
1	OpenScape Branch will try to match 53 to the called number starting on digits position 4 (count 0 through 4 from the left of the called number). If a match is found OpenScape Branch will replace all digits with 5558880000. User Dials 7777535000 --> match (Position 4), after translation: 5558880000.
2	OpenScape Branch will try to match 561719 to the called number starting on digits position 0. If a match is found OpenScape Branch will delete 6 digits and add prefix 555888. User Dials 5617195200 --> match (position 0), after translation 5558885200.
3	OpenScape Branch will try to match 305 to the called number starting on digits position 0. If a match is found OpenScape Branch will delete 2 digits from position 1 and then append 44. User Dials 3053333240 --> match (position 0), after translation 3443333240.
4	OpenScape Branch will try to match 52 to the called number starting on digit position 0. If match is found OpenScape Branch will add prefix 555888. User Dials 523333240 --> match (position 0), after translation 55588852333240.

4.8.3.1 How to Configure the SIP Header Manipulation Rules

SIP (Session Initiation Protocol) header manipulation allows to configure how the SIP headers are changed during Survivability Mode (except from an Emergency Number).

Prerequisites

Adequate administrative permissions.

At least one 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 Branch** within the Navigation Bar in the Common Management Platform.
- 2) Select the **Branch Office list** in the Navigation Tree under Administration.
The system presents the **Branch Office Overview** in the Work Area with a current list of all branch offices.
- 3) To view a list of Branch Offices 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 branch office use one of the following options:
 - In the Work Area select the checkbox to the left of the particular branch office in the list and select **Manage**. Selecting the **Manage** button updates the **Branch Office** field, in the Navigation Tree, with the selected branch office and displays information and data in the Work Area for that branch office.
 - Choose a branch office from the **Branch Office** pull-down located in the Navigation Tree. Information and data are displayed in the Work Area.
- 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 **Manipulation...** button in the **SIP** field area.
The **VoIP SIP Header Manipulation** window appears. The rules are displayed in a list.
- 7) 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.

- 8) 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.
- 9) 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.
- 10) Select the SIP header the rule applies for in the **Header** selection list. Options area as follows:
 - R-URI
 - From
 - P-Asserted Identity
 - P-Preferred Identity
 - Diversion
- 11) 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".
- 12) 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.
- 13) Enter the digits to be inserted at the defined position in the **Insert digits** field.
- 14) Enter the prefix to be added to the digits on the header in the **Add prefix** field.
- 15) Enter the digits to replace all header digits with in the **Replace all with** field.
- 16) Select the Call Type that digit manipulation applies for in the **Call Type** selection list. Options area as follows:
 - All
 - PSTN-SIP
 - SIP-PSTN
 - SIP-SIP
- 17) 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.
- 18) Click the **OK** button to store the changes temporarily in the administrator's login session.

The **Voice over IP** dialog appears.
- 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.

The setting of SIP manipulation is applied on the OpenScape Branch system.

4.8.4 Office Code Mapping - Overview

In V7R1 and later the OpenScape Branch system allows the capability to create a relationship between an extension number and its corresponding Office Code and outgoing gateway on the OpenScape Branch. This feature is applicable to all OSB models except the Proxy ATA. A subscriber in one office code will be able to dial another subscriber in a different office code on the same branch by simply dialing the extension number.

Parameters to Define Office Code Mapping

When a subscriber makes a call over the PSTN or some other external device, the call will utilize the trunk group that is associated with the that belongs to that subscriber. This capability is described as source-based routing.

This capability applies to both normal and survivable modes.

To define rules for the office code mapping, the following parameters are available:

- **Office Code mapping** (button)
Clicking the **Office Code Mapping** button, in the **Voice over IP** window will bring up a screen that allows the customer to specify the details for mapping extension numbers to office codes and gateway prefixes.
- **Enable source-based routing in Normal Mode** (checkbox)
This checkbox, in the **Office Code mapping** screen, selects between the two options "Normal Mode" and "Survivable Mode".
If an SN Range is entered with a Destination Prefix, it is possible to route external calls via a gateway that is chosen based on the calling party number. This is the definition of source-based routing. The default value for the checkbox is unchecked (Survivable Mode). This field allows the feature to also be used in Normal mode.
- **SN Range**
This field defines the range of extension numbers that are assigned to the office code.
The extension numbers can be entered either individually, or in ranges. Ranges can not overlap, e.g., 0010-0100 and 0020-0090 would not be allowed. When entered as a range, the numbers must be separated by a dash. Only the digits 0 through 9, a space, and a dash are permitted in this field.
Individual extensions and/or SN ranges can also be entered, (e.g. 2001 and 1000-1999). Extension numbers should be defined with the same digit length for all office codes. The maximum number of digits in an extension number is 7. The default value for the field is 'empty'. This field is required. It should be noted that it is not possible to input commas when entering specific extensions. Each extension is added manually and the OSB Assistant adds the comma as a delimiter for display purposes on the main Office Code mapping window.
- **Office Code**
This field defines the Office Code number that relates to all of the entries in the SN Range. Only the digits 0 through 9 are allowed. A maximum of 14 digits can be entered. The default value for the field is 'empty'. This field is not required.

- **Destination Prefix**

The destination prefix identifies which outgoing trunk group or SSP in the gateway table should be used to route external calls from an extension within the Office Code. DIVERSION, REFERRED-BY or FROM headers (checked in that order) are used to look up the destination prefix that should be used. This field allows up to 100 characters. Only digits 0 through 9, '*', '#' or '+' are allowed. The default value for this field is 'empty'.

This field can be used in Normal Mode and Survivable Mode and is not a required field.

- **Insert Office Code**

This field is a checkbox. When enabled, causes the insertion of the Office Code of the called party into the R-URI. If the called party is an extension number, its office code is inserted into the R-URI of the INVITE message. The call will then be passed to the OSV for SIP Manipulation and other handling in order to complete the call. This field is disabled by default.

- **Add button**

Click the “Add” button, to configure a new entry. The user is limited to 20 entries in the table.

- **Edit button**

Click the “Edit” button after selecting an entry to edit that entry. A screen will pop up that is populated with the table record data and it will allow the user to edit the entries for the fields.

- **Delete button**

If the user clicks the “Delete” button after selecting a record, standard delete handling shall be invoked.

Reference information on the Gateway 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:

- 1-9, 0 * # +
- Maximum 100 digits
- + - denotes repetition of the previous item one or more times
- * - denotes repetition of the previous item zero or more times
- # - end of digits

Applications

The Office Code Mapping feature applies to both Normal and Survivable Mode and handling is different for the two cases.

- **New Call Path - Normal Mode**

In Normal Mode, the OpenScape Voice (OSV) is responsible for SIP Manipulation, while the OpenScape Branch (OSB) handles gateway selection and Type of Number (TON) handling.

The OSV will also be responsible for prefixing a dialed extension number with an office code.

- 1) The user must define a business group in the OSV that covers the entire branch. Each extension number will be defined as a PAC (Prefix Access Code) with instructions to insert the office code.

If the called party is an extension number, the OSV PAC handling will recognize it as such and insert the office code into the dialed number.

If the dialed number is not an extension, then the call will be handled as per current functionality.

Once the OSV has completed its work and sent the INVITE back to the OSB, the OSB will check if the Destination Prefix should be saved for later use in normal Mode (the “Enable source-based routing in Normal Mode” checkbox). If the checkbox is set, then the (top-most) DIVERSION, REFERRED BY, or FROM header (they must be checked in that order) will be used to look up the entry in the new table that corresponds with it. It will then extract the Destination Prefix and store it in a temporary variable before passing control onto the next part of the sequence, which is to check if the called party is a registered endpoint on the OSB and, if yes, the call will be routed to it.

If it is not a registered endpoint, then the **Destination Prefix** parameter will insert the temporary variable into the R-URI before passing control onto the code that checks the Gateway table.

If the table lookup yields no matching entry then processing will continue without any further action (this corresponds with current behavior).

Since the “Destination Prefix” function on the OSB will look up the Destination Prefix, there is no need for the OSV to insert a prefix into the R-URI. To achieve this, the OSV can be configured with a Rate Area per destination (trunk group). Subscribers can then be associated with the rate area, and the rate area gets associated with the destination, which can be set up with no routing prefix.

- **New Call Path - Survivable Mode**

In Survivable Mode, the OpenScape Branch is responsible for SIP Manipulation, gateway selection, and Type of Number (TON) handling.

Two functions in the call flow manage the handling of the inter-office code extension dialing and identification of the outgoing gateway for calls to external devices or the PSTN.

First, the (top-most) DIVERSION, REFERRED BY, or FROM header (they must be checked in that order) will be used to look up the entry in the new table that corresponds with it. It will then extract the Destination Prefix and store it in a temporary variable before passing control onto the next part of the sequence.

Second, the called party will be checked to see if it is an extension number. The “Office Code Lookup” function will use the called party extension number to look up the entry in the new table that corresponds with it. It will then extract the office code and insert it at the beginning of the R-URI of the INVITE message. The INVITE will then be passed on to the SIP

Manipulation function. This functionality is bypassed if the **Insert Office Code** checkbox is not enabled.

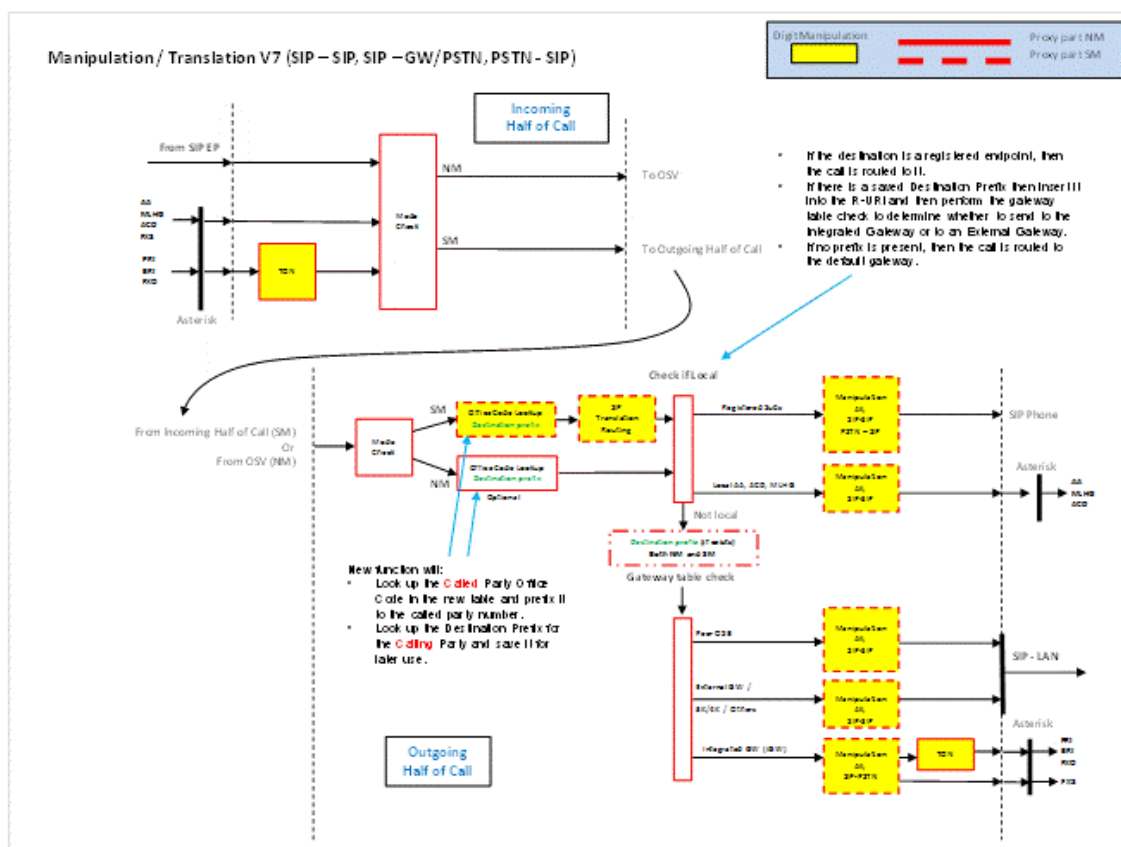
If the table lookup yields no matching entry then processing will continue without any modification to the R-URI (this corresponds with current behavior).

Once SIP Manipulation is complete, the INVITE is processed further and Kamailio will check if the called party is a registered endpoint on the OSB. If yes, the call will be routed to it.

If it is not a registered endpoint, then the new function labeled as “Destination Prefix” will insert the temporary variable into the R-URI before passing control onto the existing code that checks the Gateway table.

If the table lookup yields no matching entry then processing will continue without any further action (this corresponds with current behavior).

New Call Path - Normal and Survivable (below):



Office Code Table Content

The following shows the relationship between Trunk Group, Gateway and Office Code configuration, as well as, Office Code mapping details.

- Maximum of 20 entries per Office Code Mapping table.
- The user will first define trunk groups, assigning whichever channels (FXO, BRI, PRI) they prefer to populate the trunk groups. Each trunk group will be given an FQDN.
- The gateway table will be created next, where a trunk group FQDN will be used to associate it with a particular routing prefix. Alternate routes can be

created as needed. The example below shows Routing Prefix 10% with three alternatives. They will be chosen in ascending order of their “Priority”.

- Handling of emergency calls is no different from how they are handled at present, except that an extension number in the Office Code mapping table must not match the configured emergency number(s).
- In the Office Code mapping table, the SN Range field contains a set of extension numbers. The entries in the set are comma separated. An entry can be a single SN, or a range of SNs separated by a dash. The Office Code column contains the office code that is applicable to that set of extensions. The Destination Prefix field contains the digits that will be matched to the Gateway table Routing Prefix field when choosing which gateway to use for outgoing calls dialed by the SN Range entries.

NOTICE:

An extension number can only appear against one office code.

Configuration Relationships are as follows:

Trunkgroup				Gateway			
FQDN				FQDN	Routing Prefix	O/P Digit Strip	Priority
PRI.tkg342526.com				PRI.tkg342526.com	10%	2	1
PRI.tkg7220749.com				PRI.tkg7220749.com	20%	2	1
PRI.tkg7220769.com				PRI.tkg7220769.com	30%	2	1
PRI.tkg7191599.com				PRI.tkg7191599.com	40%	2	1
PRI.tkg758669.com				PRI.tkg758669.com	50%	2	1
PRI.tkg342519.com				PRI.tkg342519.com	60%	2	1
				PRI.tkg7220749.com	10%	2	2
				PRI.tkg7220769.com	10%	2	3
				10.234.14.56	911	0	

Office Code mapping table			
SN Range	Office Code	Destination Prefix	Insert Office Code
101, 102, 111, 125 - 129, 242 - 245, 253, 255, 263, 317, 318	711 342526	10	X
204, 229	711 7220749	20	X
207 - 208	711 7220769	30	X
238 - 239	711 7191599	40	X
103, 202 - 203, 236, 240, 250 - 252, 259, 261, 264 - 265, 269 - 272, 277, 282, 284, 287, 299, 304	711 758669	50	X
104, 131 - 140, 306	711 342519	60	X

4.8.4.1 How to Configure Office Code Mapping

Office Code Mapping allows the capability to create a relationship between an extension number and its corresponding Office Code and outgoing gateway on the OpenScape Branch 50i and 500i.

Prerequisites

Adequate administrative permissions.

The Gateway configuration must be completed e.g., routing prefix configured.

At least one 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 Branch** within the Navigation Bar in the Common Management Platform.
- 2) Select the **Branch Office list** in the Navigation Tree under Administration.
The system presents the **Branch Office Overview** in the Work Area with a current list of all branch offices.
- 3) To view a list of Branch Offices 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 branch office use one of the following options:
 - In the Work Area select the checkbox to the left of the particular branch office in the list and select **Manage**. Selecting the **Manage** button updates the **Branch Office** field, in the Navigation Tree, with the selected branch office and displays information and data in the Work Area for that branch office.
 - Choose a branch office from the **Branch Office** pull-down located in the Navigation Tree. Information and data are displayed in the Work Area.
- 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 **Office Code mapping...** button in the **SIP** field area.

The **Office Code mapping** window appears. The office code mapping entries are displayed in a list with additional parameters.

- **Enable source-based routing in Normal Mode** (checkbox)

This checkbox, in the **Office Code mapping** screen, selects between the two options "Normal Mode" and "Survivable Mode". The default value for the checkbox is unchecked (Survivable Mode).

- **SN Range**

This field will allow the user to enter the extension numbers that are included in the Office Code.

- **Office Code**

This field defines the Office Code number that relates to all of the entries in the SN Range.

NOTICE:

Office code is not allowed for Proxy ATA mode.

Either **Office code** or **Destination Prefix** must be configured.

- **Destination Prefix**

The destination prefix identifies which outgoing trunk group or SSP in the gateway table should be used to route external calls from an extension within the Office Code. DIVERSION, REFERRED-BY or FROM headers (checked in that order) are used to look up the destination prefix that should be used.

NOTICE:

Either **Office code** or **Destination Prefix** must be configured.

- **Insert Office Code**

This field is a checkbox. When enabled, causes the insertion of the Office Code of the called party into the R-URI. If the called party is an extension number, its office code is inserted into the R-URI of the INVITE message. The call will then be passed to the OSV for SIP Manipulation and other handling in order to complete the call. This field is disabled by default.

- 7) Checkmark the **Enable source-based routing in Normal Mode** if the configuration is to be used for Normal Mode of operation. Leave unchecked if the configuration is to be used for Survivable Mode.
- 8) To configure the Office Code mapping table, 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 entry to the list.

The **Add Office Code mapping** window appears with the **General** tab displayed by default.

- 9) Enter the Office Code to be mapped to in the **Office Code** field. This field defines the Office Code number that relates to all of the entries in the SN Range. Only the digits 0 through 9 are allowed. A maximum of 14 digits can be entered. The default value for the field is 'empty'. This field is optional.
- 10) Enter the Destination Prefix that applies in the **Destination Prefix** parameter field. Regular expressions may be used for matching. This field is optional. The default value for this field is 'empty'. This field can be used in Normal Mode and Survivable Mode.
- The destination prefix identifies which outgoing trunk group or SSP in the gateway table should be used to route external calls from an extension within the Office Code. DIVERSION, REFERRED-BY or FROM headers (checked in that order) are used to look up the destination prefix that should be used.
 - 1-9, 0 * # +
 - Maximum of 100 characters
 - + - denotes repetition of the previous item one or more times
 - * - denotes repetition of the previous item zero or more times
 - # - end of digits
- 11) Checkmark the **Insert Office Code** if the OSB table is used to prefix the office code, as is done in Survivable mode. The call will then be passed to the OSV for SIP Manipulation and other handling.
- This checkbox, when set, causes the insertion of the Office Code of the called party into the R-URI. If the called party is an extension number, its office code is inserted into the R-URI of the INVITE message in order to complete the call. This functionality is bypassed if the checkbox is not set. This field is disabled by default.
- 12) Select the **SN Range** tab
- The list of SN range values are displayed.
- 13) To configure the SN Range values, the following options appear:
- Select an entry from the list and click the **Delete** button to remove an entry from the list.
 - Enter the new value in the add field and click the **Add** button to add a new entry to the list. This field defines the range of extension numbers that are assigned to the office code.
- The extension numbers can be entered either individually, or in ranges. Ranges can not overlap e.g., 0010-0100 and 0020-0090 would not be allowed. When entered as a range, the numbers must be separated by a dash. Only the digits 0 through 9, a space, and a dash and comma are permitted in this field.
- Multiple extension numbers and/or SN ranges can also be entered, separated by a comma (e.g. 1000-1999, 2001). Extension numbers should be defined with the same digit length for all office codes. The maximum number of digits in an extension number is 7. The default value for the field is 'empty'. This field is required.

NOTICE: The same extension number can not be configured for different office codes.

The new value is added to the list.

- 14) Click the **OK** button to store the changes temporarily.
The **Office Code mapping** window appears.
- 15) Click the **OK** button to store the changes temporarily in the administrator's login session.
The **Voice over IP** dialog appears.
- 16) Click the **OK** button to store the changes temporarily in the administrator's login session.
The **Voice over IP** dialog disappears.
- 17) Click the **Apply changes** button in the main window.

The setting of Office Code mapping is applied on the OpenScape Branch system.

4.8.5 SIP Routing Rules

SIP (Session Initiation Protocol) Routing serves for the routing of SIP messages during survivability mode. Therefore rules have to be defined.

SIP calls can be rerouted if:

- A gateway cannot process a connection request. The calls can be of type offnet (to the PSTN via a SIP gateway) or on-net (to another SIP or SIP-Q network such as a QSIG (QSIG=Q (reference point) Signaling) gateway or the OpenScape UC Application).
- A WAN failure occurs. SIP and SIP-Q calls between subscribers are rerouted through the PSTN (Public Switched Telephone Network).
- A SIP response code indicates a bandwidth restriction.

Functional Description

The OpenScape Voice provides rerouting of SIP calls for unreachable gateways or subscribers in the case of WAN failure or after receipt of a SIP response code indicating an error condition such as a bandwidth restriction (e.g. 606). The SIP calls can be of type off-net (to the PSTN via a SIP gateway), on-net (to another SIP network, such as OpenScape) or to a registered SIP subscriber. A rerouting timer provides rerouting in case no response is received from the SIP gateway, SIP server or SIP subscriber after an INVITE has been sent to them. The timer is configured under Survivability, Timers and Thresholds.

Requirements

Rerouting for SIP subscribers relies on particular conditions:

- The called subscriber has to be registered from a survivable branch (e.g. OpenScape Branch).
- The called subscriber has to reside in that survivable branch. This means that the called subscriber is registered with its provisioned 'Survivable' SIP Proxy endpoint.
- The called subscriber has a 'Survivable' SIP Endpoint (SIP Gateway - no SIP Proxy) provisioned as associated Endpoint and it is registered directly with the OpenScape Voice. (in this case the first two points are not necessary).
- The called subscriber has to have a valid public E.164 number.

- The calling subscriber must be calling from a different survivable branch or must be directly registered with the OpenScape Voice.

Parameters to Define Rules for Routing

To define rules for the SIP routing, the following parameters are available:

- Source IP (Internet Protocol) address

This parameter defines the Source IP address of the message to be routed.

- Condition (error codes)

The reply codes are used to reroute the messages. The following codes can be assigned:

Error Code	Related error
300	Multiple Choices
301	Moved Permanently
302	Moved Temporarily
305	Use Proxy
380	Alternative Service
401	Unauthorized
402	Payment Required
403	Forbidden
404	Not Found
405	Method Not Allowed
406	Not Acceptable
407	Proxy Authentication Required
408	Request Timeout
410	Gone
413	Request Entity Too Large
414	Request URI Too Large
415	Unsupported Media Type
416	Unsupported URI Scheme
420	Bad Extension
421	Extension Required
422	Session Interval Too Small
423	Interval Too Brief
480	Temporarily Unavailable
486	Busy Here
488	Not Acceptable Here
493	Undecipherable
500	Server Internal Error

Error Code	Related error
501	Not Implemented
502	Bad Gateway
503	Service Unavailable
504	Server Time Out
600	Busy Everywhere
606	Not Acceptable

- **Destination IP**
This parameter defines the destination IP address of the message to be routed.
- **Destination tag**
This parameter defines a tag to be added to rerouted SIP headers.
- **Destination type**
The destination type determines the type of route used for the rule.
- **Priority**
The priority defines which route will be used first in case of more than one route applies.

4.8.5.1 How to Configure SIP Routing Rules

Proceed as follows to display and configure SIP (Session Initiation Protocol) routing rules which modify the routing of SIP messages during survivability mode.

Prerequisites

Adequate administrative permissions.

At least one 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 Branch** within the Navigation Bar in the Common Management Platform.
- 2) Select the **Branch Office list** in the Navigation Tree under Administration.
The system presents the **Branch Office Overview** in the Work Area with a current list of all branch offices.
- 3) To view a list of Branch Offices 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 branch office use one of the following options:
 - In the Work Area select the checkbox to the left of the particular branch office in the list and select **Manage**. Selecting the **Manage** button updates the **Branch Office** field, in the Navigation Tree, with the selected branch office and displays information and data in the Work Area for that branch office.
 - Choose a branch office from the **Branch Office** pull-down located in the Navigation Tree. Information and data are displayed in the Work Area.
- 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 **Routing...** button in the **SIP** field area.

The **VoIP SIP Routing** window appears. The rules are displayed in a list.

- 7) 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 Routing** window appears.

- 8) Enter the source IP address of the message to be routed in the **Source IP** field.
- 9) Enter the conditions to reroute the messages in the **Condition (error codes)** field. The SIP response (error) codes have to be separated by commas.
- 10) Enter the destination IP address of the message to be routed in the **Destination IP/FDQN** field.
- 11) Enter the destination tag in the **Destination Port** field. The destination ports to be rerouted to.
- 12) Select the destination transport type in the **Destination Transport** selection list. The destination transport can be **TCP**, **UDP** or **TLS**.
- 13) Enter the destination tag in the **Destination tag** field. The destination tag is added to rerouted SIP headers.
- 14) Select the destination type in the **Destination type** selection list. The destination type determines the type of route used for the rule. A destination type can be "Voice Mail", "Gateway" or "other SIP EP (Endpoint)".
- 15) Click the **OK** button to go back to the **Voice over IP** window.
- 16) Click the **OK** button to store the changes temporarily in the administrator's login session.

The **Voice over IP** dialog disappears.

- 17) Click the **Apply changes** button in the main window.

The configuration of the SIP routing rules is applied on the OpenScape Branch system.

4.8.5.2 How to Configure SIP Error Codes

Proceed as follows to view supported SIP (Session Initiation Protocol) error codes and to configure error codes for rerouting during normal mode and survivability mode.

Prerequisites

Adequate administrative permissions.

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

The connection to the OpenScape Voice system is up.

The settings for survivability have been configured accordingly.

Step by Step

- 1) Navigate to **Configuration tab > OpenScape Branch** within the Navigation Bar in the Common Management Platform.
- 2) Select the **Branch Office list** in the Navigation Tree under Administration.
The system presents the **Branch Office Overview** in the Work Area with a current list of all branch offices.
- 3) To view a list of Branch Offices 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 branch office use one of the following options:
 - In the Work Area select the checkbox to the left of the particular branch office in the list and select **Manage**. Selecting the **Manage** button updates the **Branch Office** field, in the Navigation Tree, with the selected branch office and displays information and data in the Work Area for that branch office.
 - Choose a branch office from the **Branch Office** pull-down located in the Navigation Tree. Information and data are displayed in the Work Area.
- 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 **Error Codes...** button in the **SIP** field area.
The **SIP Error Codes (View)** window appears displaying the error codes:
 - The **Code** column contains the error code numbers.
 - The **Enable routing in survivable mode** column and **Enable rerouting in normal mode** column indicates when the error codes will be used for rerouting.
 - The **Description** column provides a brief description of the error code e.g., Forbidden, Unauthorized, etc.

- 7) To enable or disable “all” error codes for normal or survivable mode four buttons are provided:
 - a) Select the **Enable all in survivable mode** button to enable “all” error codes for survivable mode rerouting.
 - b) Select the **Enable all in normal mode** button to enable “all” error codes for normal operating mode.
 - c) Select the **Disable all in survivable mode** button to enable “all” error codes for survivable mode rerouting.
 - d) Select the **Disable all in normal mode** button to enable “all” error codes for normal operating mode.

The updated error codes are displayed.

 - e) Proceed to Step 7 to temporarily save changes.
 - 8) To configure individual error codes for rerouting, proceed as follows:
 - a) Select the radio button of the error code to be configured for rerouting.
 - b) Click the **Edit...** button.

The **SIP Error Codes (Configure)** subwindow appears.

 - c) Check the **Enable rerouting in survivable mode** checkbox to enable.
 - d) Check the **Enable rerouting in normal mode** checkbox to enable.
 - e) Click the **OK** button to temporarily save the data and go back to the **SIP Error Codes (View)** window. The updated error code is displayed.

The updated error code is displayed.

 - f) Select another error code if applicable and configure.
 - 9) Click the **OK** button to go back to the **Voice over IP** window.
 - 10) Click the **OK** button to store the changes temporarily in the administrator’s login session.
- The **Voice over IP** dialog disappears.
- 11) Click the **Apply changes** button in the main window.

The configuration of the SIP error codes are applied on the OpenScape Branch system.

4.8.5.3 How to Configure VoIP SIP Settings

Proceed as follows to configure the ports in LAN (Local Area Network) where OpenScape Branch will be listening, the Options source port, and the port mapping parameters.

Prerequisites

Adequate administrative permissions.

At least one SBC 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 Branch** within the Navigation Bar in the Common Management Platform.

- 2) Select the **Branch Office list** in the Navigation Tree under Administration.

The system presents the **Branch Office Overview** in the Work Area with a current list of all branch offices.

- 3) To view a list of Branch Offices 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 branch office use one of the following options:

- In the Work Area select the checkbox to the left of the particular branch office in the list and select **Manage**. Selecting the **Manage** button updates the **Branch Office** field, in the Navigation Tree, with the selected branch office and displays information and data in the Work Area for that branch office.
- Choose a branch office from the **Branch Office** pull-down located in the Navigation Tree. Information and data are displayed in the Work Area.

- 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 of each protocol TCP (Transmission Control Protocol), UDP (User Datagram Protocol), TLS (Transparent LAN Service) in the **TCP**, **UDP**, and **TLS** fields, in the Listening ports field area:

TCP:**5060**,UDP:**5060**, TLS:**5061**, MTLS:**5161**

- 7) Leave this field blank or enter the TCP Listening port.

If the OpenScape Branch is connected to an OpenScape Voice which is not on the latest patch set (OSV V6:<PS23; OSV V7:< PS8), enter the Options source number in the Options Source port field, in the listening ports field area. Enter a different port than the ports entered in step 6) (e.g., 5062). This is the port that needs to be set as "Trusted" in the OpenScape Voice configuration for the OpenScape Branch. Other messages using different ports will still get challenged.

- 8) Configure **Port Mapping** as follows:

- a) Enter the RTP (Real-time Transport Protocol) port range to be used by the RTP Proxy application and in Firewall configuration in the **RTP ports min/max** fields, under **Port Map**. These fields are always enabled in Branch SBC/SBC-Proxy (Session Border Controller) modes. The fields may also be used in **Proxy** and **Proxy-ACD** modes when Integrated Gateway feature or other B2BUA (Back-to-Back User Agent) provided feature is used (e.g. Automatic Call Distribution (ACD) Groups, Auto Attendant (AA), Multi Line Hunt Group (MLHG), Voicemail).

NOTICE:

The B2BUA application may not use the port range configuration used by the RTP Proxy when there is a match between negotiated media and the media profile used by the B2BUA (igw_features_lan). In this case, the RTP Port Range is fixed to 10000 - 19999 and the **"RTP ports min/max"** fields are ignored.

- 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 modes.
 - c) Enter the SIP port range to be used in SIP messages in the **SIP ports min/max** fields, under **Port Mapping**. The fields are only enabled in SBC modes.
 - d) Enter the SIP trunk port range to be used in SIP trunk messages in the **SIP Ports min/max** fields, under **Port Mapping**. The fields are only enabled in SBC modes.
- 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.

The configuration of the SIP settings is applied on the OpenScape Branch system.

4.8.5.4 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 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 Branch** within the Navigation Bar in the Common Management Platform.
- 2) Select the **Branch Office list** in the Navigation Tree under Administration.

The system presents the **Branch Office Overview** in the Work Area with a current list of all branch offices.
- 3) To view a list of Branch Offices 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 branch office use one of the following options:
 - In the Work Area select the checkbox to the left of the particular branch office in the list and select **Manage**. Selecting the **Manage** button updates the **Branch Office** field, in the Navigation Tree, with the selected branch office and displays information and data in the Work Area for that branch office.
 - Choose a branch office from the **Branch Office** pull-down located in the Navigation Tree. Information and data are displayed in the Work Area.

- 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 **Show...** button in the **Port mapping** field area. Port Mapping only applies to branches configured in Branch SBC or Branch SBC-Proxy mode.

The **Registered Subscribers Port Mapping** window appears displaying the settings in a list. The following data of all subscribers of the selected branch office is displayed:

- **Contact:** Contact information of the subscriber.
- **Internal IP:** Internal IP Address of the subscriber.
- **Internal port:** Internal port number of the subscriber.
- **External IP:** External IP Address of the subscriber.
- **External port:** External port number of the subscriber.
- **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.

- 7) Click the **Close** button to go back to the **Voice over IP** window

Registered subscriber ports were displayed.

4.8.6 Call Forwarding in Survivable Mode

The OpenScape Branch has the capability in V1R4 and later releases to forward to voice mail when the Branch is in Survivable mode. Forwarding of calls is applicable for calls whose original destination is a registered subscriber on the OpenScape Branch regardless of the caller.

OpenScape Branch survivable mode call forward reasons are as follows:

- **Call Forward No Reply**
- **Call Forward on Busy**
- **Call Forward On Do not Disturb**
- **Call Forward On Error**

System Call Forwarding takes precedence over Call Forwarding configured for survivable mode and rerouting configured in “SIP routing”.

It is currently not possible to execute call forward of calls which were initiated in normal mode and then switched to survivable mode since OpenScape Voice longer has control of the call in survivable mode.

4.8.6.1 How to Configure Call Forwarding for Survivable Mode

Proceed as follows to configure the Call Forwarding for Survivable Mode settings for the OpenScape Branch. One or more types of call forwarding may be configured for survivable call forwarding.

Prerequisites

Adequate administrative permissions.

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

The connection to the OpenScape Voice system is up.

It is recommended that all subscribers in the Branch be configured to use the same Voice Mail server.

Step by Step

- 1) Navigate to **Configuration tab > OpenScape Branch** within the Navigation Bar in the Common Management Platform.
- 2) Select the **Branch Office list** in the Navigation Tree under Administration.
The system presents the **Branch Office Overview** in the Work Area with a current list of all branch offices.
- 3) To view a list of Branch Offices 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 branch office use one of the following options:
 - In the Work Area select the checkbox to the left of the particular branch office in the list and select **Manage**. Selecting the **Manage** button updates the **Branch Office** field, in the Navigation Tree, with the selected branch office and displays information and data in the Work Area for that branch office.
 - Choose a branch office from the **Branch Office** pull-down located in the Navigation Tree. Information and data are displayed in the Work Area.
- 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 **Call Forward...** button.
The **VoIP Call Forward** window appears.
- 7) **Call Forward No Reply During Survivable Mode:**
 - a) Check the **Activate** checkbox in the Call Forward No Reply field area to enable call forwarding no reply, during survivable mode.
 - b) Enter the forward-to destination e.g. voice mail in the **Redirect Number** field (value: 1-24 digits). The Redirect Number destination may route via the PSTN (public network).
 - c) Enter the ring duration, number of seconds prior to redirection, in the **Ring Duration** field (value: 1 - 60 seconds, default 24 seconds).
 - d) Enter the Source IP address or Subnet used to identify subscribers in the Branch; in the **Source IP address** field. Subnets should be specified with a mask e.g. 10.200.3.0/24

8) Call Forward on Busy During Survivable Mode:

- a) Check the **Activate** checkbox in the Call Forward on Busy field area to enable call forwarding on busy, during survivable mode.
- b) Enter the forward-to destination e.g. voice mail in the **Redirect Number** field.
- c) Enter the Source IP address or Subnet used to identify subscribers in the Branch; in the **Source IP address** field. Subnets should be specified with a mask following the CIDR notation e.g. 10.200.3.0/24. If parameter **Activate** is enabled, this parameter must be configured.

9) Call Forward on DND During Survivable Mode:

- a) Check the **Activate** checkbox in the Call Forward On Do not Disturb (DND) field area to enable call forwarding when the subscriber has DND active during survivable mode.
- b) Enter the forward-to destination e.g. voice mail in the **Redirect Number** field (value: 1-24 digits). The Redirect Number destination may route via the PSTN (public network).
- c) Enter the Source IP address or Subnet used to identify subscribers in the Branch; in the **Source IP address** field. Subnets should be specified with a mask following the CIDR notation e.g. 10.200.3.0/24. If parameter **Activate** is enabled, this parameter must be configured.

10) Call Forward on Error During Survivable Mode:

- a) Check the **Activate** checkbox in the Call Forward On Error field area to enable call forwarding based on error codes, during survivable mode.
- b) Enter the forward-to destination e.g. voice mail in the **Redirect Number** field (value: 1-24 digits). The Redirect Number destination may route via the PSTN (public network).
- c) Enter the Source IP address or Subnet used to identify subscribers in the Branch; in the **Source IP address** field. Subnets should be specified with a mask following the CIDR notation e.g. 10.200.3.0/24. If parameter **Activate** is enabled, this parameter must be configured.

11) Click the **Error Codes button.**

The **VoIP - Call Forward - Error Codes** dialog appears and error codes associated with error code forwarding are displayed in a list.

12) To configure the error codes for call forwarding, 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 Error Codes drop-down list and click the **Add** button to add a new error code to the list.

13) Click the **OK button to store the changes temporarily in the administrator's login session.**

The **VoIP Error Codes** dialog disappears and the **VoIP Call Forward** dialog appears.

14) Click the **OK button to store the changes temporarily in the administrator's login session.**

The **VoIP Call Forward** dialog disappears and the **Voice over IP** dialog appears.

15) Click the **OK button to store the changes temporarily in the administrator's login session.**

The **Voice over IP** dialog disappears.

16) Click the **Apply changes** button in the main window.

The Call Forwarding during Survivable Mode settings for the OpenScape Branch are configured.

NOTICE:

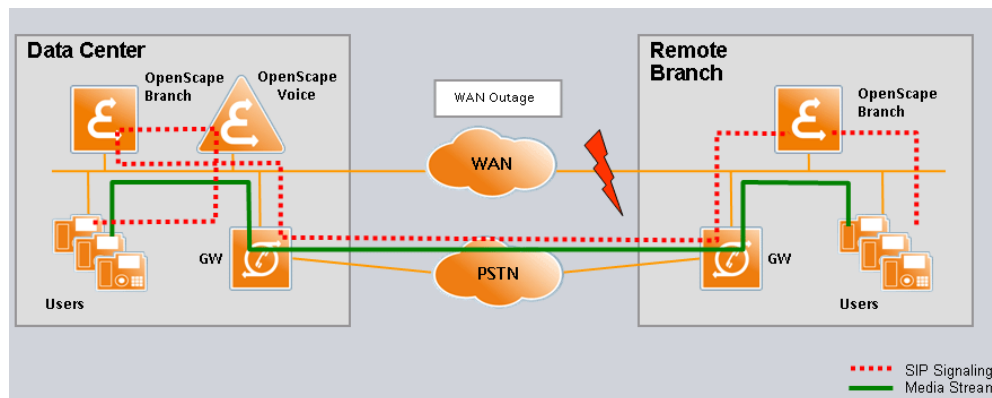
If a call is routed to the Voice Mail server via PSTN (public network), it is highly probable that no Diversion information will be provided to allow the identification of the mailbox account. Therefore, the Voice Mail server shall prompt the caller to reenter the mailbox account.

4.8.7 Configuration of Backup Data Channel

OpenScape Branch can be used to set up a backup link between a branch office and a data center in case of a WAN outage between the data center and the branch office. This functionality is only available for OpenScape Branch V1R3 and later versions. OpenScape Branch V1R4 and later versions, provides for multiple backup links. This allows a larger number of connections to be supported via backup links in case of a WAN failure.

General Information

The OpenScape Branch is deployed in the remote branch office and the data center. The OpenScape Branch in the branch office serves as BLC (Backup Link Client) and the OpenScape Branch in the data center will serve as BLS (Backup Link Server).



Functional Overview

Once the OpenScape Branch office detects that OpenScape Voice is unreachable (Transition Mode), it sets up a backup link or multiple links (in OpenScape Branch V1R4 and later) to the OpenScape Branch appliance in the data center.

A single backup signaling channel can support approximately up to 100 users. This is not enough for OpenScape Branch 250, 1000 and 6000. Therefore, multiple backup links can be configured for these larger models.

Once established, the backup link(s) is used to send all information that is destined for the OpenScape Voice in the data center. With an established

backup link(s), the OpenScape Branch in the data center will also be able to deliver packets to the remote branch office.

The backup link client and server are implemented as a SIP modem like device on the OpenScape Branch that can establish a data call outgoing via the local gateway destined for the OpenScape Branch in the data center. The integrity of the payload in the backup data channel is guaranteed by establishing a Point-to-Point Protocol (PPP) connection between the branch office and the data center OpenScape Branch appliances. OpenScape Voice detects whether it is using a backup link versus the WAN by interpreting traps received from a configured IP address. The OpenScape Branch in the data center must support sending these same traps.

Backup Link Client

The Backup Link Client is simply an additional process on the Proxy, Proxy ACD, SBC Proxy or Branch SBC.

NOTICE:

Please note that for OpenScape Branch V1R3 the Backup Data Channel is only supported for the OSB 50 and 50i models. Only one Channel is supported (BRI Clear Channel).

The Backup Link Client process:

- provides a state machine that is activated as soon as the OpenScape Branch's operational mode becomes 'Transitional'. The state machine guides the OpenScape Branch to establish a backup link to (one of) the configured Backup Link Server(s).
- sends OPTIONS requests to (all) the configured Backup Link Server(s) while a backup link is established.
- filters the IP packets that are sent on the backup link. Only SIP and MGCP messages and SNMP traps are allowed.

Backup Link Server

A Backup Link Server should not be used as a branch SBC, a SIP Proxy or a SIP Proxy ACD. It may be used as a centralized SBC. The Backup Link Server process:

- provides a state machine for each incoming INVITE Request with the Backup Link DID number. The state machine is only started when the Survivability Provider's primary target is in Normal Mode (i.e. it can talk to the local OpenScape Voice Node).
- answers any incoming OPTIONS request with "488 Not Acceptable Here" while the Survivability Provider's primary target is in the penalty box.
- is able to select which backup link channel can be allowed and which one is rejected.
- filters the IP packets sent on the backup links. Only SIP and MGCP messages are allowed.
- sends an SNMP trap to the local OpenScape Voice node every time a tunnel is established or closed.
- The OSV does not issue SNMP Gets and the OSB does not respond. The OSV only gets the link status from traps.

- sends back ICMP 'destination unreachable' packets for all the branch offices that do not have a backup link open. Packets for branch offices that do have a backup link open are simply routed via the backup link.

Operation and Calculation of Backup Link Requirements

Basic Backup Link Operation

Calculation of Backup Link Bandwidth

Adding PPP links to the Multilink PPP Connection

Removing PPP Links from the Multilink PPP Connection

For large branch offices, the bandwidth required for signaling may be greater than the 64kbps. The administrator should have an idea about the normal average signaling traffic from the branch office. To help determine the bandwidth requirements on the signaling for the OpenScape Branch, the administrator needs to know the expected number of registered users and keyset lines. Based on the result, 3 variables can be determined:

- Minimum Bandwidth required for the backup link. This is calculated as the bandwidth required for supporting a uniform registration and calling distribution during normal operation.
- Initial Bandwidth required for the backup link. This is the minimum bandwidth of the backup link that must be established before messages are passed through the backup link. This is to prevent that large branch offices move back to normal mode too early to handle the expected traffic.
- Maximum Bandwidth required for the backup link. This is calculated as the bandwidth required for handling all the registrations and subscriptions of the subscribers and keysets in a burst.

With these variables set (they can be adjusted manually), the OpenScape Branch can set up multiple backup links whenever it detects a WAN outage. If the backup link can be established while the OpenScape Branch is in normal mode, the initial amount of backup links should be set up immediately. If the backup link can only be established after the OpenScape Branch already went in survivable mode, the maximum amount of backup links should be set up immediately because a burst of registrations and subscriptions is expected as soon as the OpenScape Branch moves into backup link mode. Messages are only passed through the backup link once the minimum bandwidth has been set up using backup links.

There are four main functions when establishing backup link operation:

- 1) The OpenScape Branch detects the WAN outage and orders the Backup Link Client to establish the backup link towards the Backup Link Server in the data center.
- 2) The Backup Link Client opens the initial (or maximum) amount of backup links towards the Backup Link Server. For the OpenScape Branch application all backup links look like a single backup link towards the data center.
- 3) The phone in the branch office keeps sending its signaling messages to the OpenScape Branch application that on its turn sends the messages to the backup link towards the data center.

- 4) The Backup Link Server in the data center forwards the signaling messages to the OpenScape Voice who uses normal call processing to identify the desired destination for the call.

To calculate the bandwidth requirements for the backup link, the administrator needs to know the number of registered SIP users (note that each line of a keyset is a registered SIP user):

The initial/minimum bandwidth requirements can be derived from the following table:

Number of registered Users	Initial / Minimum bandwidth requirements
0-50	1
51-250	1
251-1000	2
1001-3000	3
3001-6000	4

The initial bandwidth requirements are used when the backup link is first set up. Based on usage the bandwidth can always go down to the minimum bandwidth (up to a single backup link Point-to-Point Protocol (PPP) connection (e.g. at night even the busiest branch could go down to a single backup link PPP connection)). However, the minimum should be calculated for normal operation of a branch office. The defaults for minimum and initial bandwidth shall be the same. The minimum bandwidth has to be smaller than or equal to the initial bandwidth.

The backup link shall only transport messages from the OpenScape Branch if the minimum bandwidth conditions have been met. This is important as a backup link with not enough bandwidth may cause very sluggish or even inconsistent behavior of a branch office. Some calls would make it and others would not. With backup links this can never really be ruled out, but with adhering to the minimum bandwidth requirements, the probability of inconsistent behavior is small.

The maximum bandwidth requirements for the backup link are designed for the situation where a backup link is established while the OpenScape Branch is in survivable mode. When an OpenScape Branch comes out of survivable mode, it sends notifications to all users which will trigger a flurry of registrations. The maximum allowed number of registrations per second in this case is 100 in case the WAN is available. In order to achieve such a number with backup links, one would have to establish 100 backup links. As this is probably too high of a number to handle, the maximum number will come down to what the customer thinks is an acceptable time to transition the branch office from survivable mode to normal mode using backup links.

The following Maximum Bandwidth Requirements table can help making that decision:

Number of registered Users	Maximum Bandwidth Requirements					
	WAN available (transition time from Survivable to Normal mode in seconds)	Number of Backup Links (transition time from Survivable to Normal mode in seconds)				
		20 min	10 min	5 min	1 min	30 sec
0	0	n/a	n/a	n/a	n/a	n/a
50	0.5	n/a	n/a	n/a	1	2
100	1	n/a	n/a	1	2	4
150	1.5	n/a	n/a	1	3	5
200	2	n/a	n/a	1	4	7
250	2.5	n/a	n/a	1	5	9
300	3	n/a	n/a	1	5	10
600	6	n/a	1	2	10	20
900	9	1	2	3	15	20
1200	12	1	2	4	20	40
1800	18	2	3	6	30	60
2400	24	2	4	8	40	80
3000	30	3	5	10	50	100
3600	36	3	6	12	60	n/a
4200	42	4	7	14	70	n/a
4800	48	4	8	16	80	n/a
5400	54	5	9	18	90	n/a
6000	60	5	10	20	100	n/a

Default maximum Bandwidth Requirements

The default values for the OpenScape Branches will be set based on the device mode:

Device Model	Minimum Number of Backup Links	Maximum Number of Backup Links	Maximum Time to Transition from Survivable Mode to Normal Mode Using Backup Links
OSB 50	1	1	Less than 1 minutes
OSB 250	1	3	Less than 2 minutes
OSB 1000	2	6	Less than 3 minutes
OSB 6000	4	10	Less than 10 minutes

The Backup Link Client (BLC) will initiate adding a new Point-to-Point Protocol (PPP) link to the connection if a high watermark on the existing bandwidth is reached. This high watermark will be calculated as a percentile of the bandwidth

of a single link in the multi-link PPP. The high watermark is a function of the number of PPP links in the multi-link PPP connection as follows:

High Water (n) = (n – 1 + (High Water Percentile/100)) x 8000 Bytes (with n < Max Backup Links ≤ 100).

Every second the amount of Bytes transmitted during the last second is compared against the High Water mark and if the amount of bytes transmitted is consistently higher than the current high watermark for a configurable period and if the maximum number of backup links has not been reached yet, then the BLC will add a new backup link to the multi-link PPP connection.

The default value for the high watermark will be 90% and the configurable range will be between 75 and 100%.

The default value for the High Watermark Detection window is 1 second and is configurable between 1 and 10 seconds.

NOTICE:

Note that it is recommended to keep this value low in order to prevent messages from being discarded by the OpenScape Branch in the branch office because of a low bandwidth backup link connection.

The Backup Link Client (BLC) will initiate removing a new Point-to-Point Protocol (PPP) link to the connection if a low watermark on the existing bandwidth is reached. This low watermark will also be a percentile of the bandwidth of a single link in the multi-link PPP. The low watermark is a function of the number of PPP links in the multi-link PPP connection as follows:

Low Water (n) = (n – 2 + (Low Water Percentile/100)) x 8000 Bytes (with n ≥ Minimum Bandwidth ≥ 1).

Every second the amount of Bytes transmitted during the last second is compared against the Low Water mark and if the amount of bytes transmitted is consistently lower than the current low watermark for a configurable period and if the minimum number of backup links has not been reached yet, then the BLC will remove a backup link from the multi-link PPP connection.

The default value for the low watermark will be 50% and the configurable range will be between 25 and 75%.

Survivable Mode Avoidance

It is very important to try to avoid the occurrence of a branch office going in survivable mode. The subscribers in the branch office are notified of this event by showing the 'temporary limited mode' message on the display of their phones. The situation, however, becomes dramatic when the branch office moves back to normal mode. In order to provide the best service possible, the phones are required to re-register and re-subscribe with OpenScape Voice because their registrations got suspended and their subscriptions may have expired during the WAN outage.

If the WAN is available, the phones are brought back to service at a rate of 100 phones per second. For a large 6000 subscriber branch office it would therefore take 60 seconds before all phones are brought back to normal operational mode.

If the WAN is not available and communication with the OpenScape Voice in the data center is established by successfully creating a backup link, the bandwidth of the established backup link does not allow bringing the phones back to normal operational mode at a rate of 100 phones per second.

To avoid that the OpenScape Branch moves into survivable mode, the ping between the OpenScape Voice and OpenScape Branch is prioritized in order to keep their current operational mode status in case of overload conditions.

Bandwidth Control During Backup Link Mode

To guarantee bringing back the phones into normal mode without causing too many re-registrations and re-subscriptions to be rejected, the OpenScape Branch controls the rate at which the phones are brought back. To control the rate, OpenScape Branch knows the kind of phones registered. A registration of a non-keyset phone which contains no line appearances has less registrations than a keyset phone with multiple subscriptions.

To be able to efficiently throttle the message load, the OpenScape Branch sends a normal mode notification to a phone if it can handle the expected load of the re-registration and re-subscriptions that occur as a consequence of this notification.

Therefore, the OpenScape Branch keeps statistics about the registrations during normal mode and uses these statistics to throttle the registrations during backup link mode.

4.8.7.1 How to Configure OSB as Backup Link Client

Proceed as follows to configure the OpenScape Branch appliance to act as BLC (Backup Link Client). All the fields shall be set to default values on creating the BLC configuration.

Prerequisites

Adequate administrative permissions.

The OpenScape Branch appliance is in operation.

The OpenScape Branch system is Version 1R3 or later.

The connection to the OpenScape Voice system is up.

Step by Step

- 1) Navigate to **Configuration tab > OpenScape Branch** within the Navigation Bar in the Common Management Platform.
- 2) Select the **Branch Office list** in the Navigation Tree under Administration.
The system presents the **Branch Office Overview** in the Work Area with a current list of all branch offices.
- 3) To view a list of Branch Offices 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 branch office use one of the following options:
 - In the Work Area select the checkbox to the left of the particular branch office in the list and select **Manage**. Selecting the **Manage** button updates the **Branch Office** field, in the Navigation Tree, with the selected branch office and displays information and data in the Work Area for that branch office.
 - Choose a branch office from the **Branch Office** pull-down located in the Navigation Tree. Information and data are displayed in the Work Area.

- 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) Set the **Backup link mode** field to **Client**.
- 7) Click the **Configure...** button.

The **Backup Link Client** window appears with the **General** tab selected.

- 8) Enter the primary DID (Direct Inward Dialing) number, in the Target area, to reach the BLS (Backup Link Server) located at Node 1 in the **Primary DID Number** field. (Possible values: E.164 number type - maximum 15 digits).
- 9) Enter the secondary DID number, in the Target area, to reach the BLS located at Node 2 in the **Secondary DID Number** field. (Possible values: E.164 number type - maximum 15 digits).
- 10) Enter the **Congestion delay** time, in the **IP Connection** area. Possible values < 20 to 120 seconds>; Default: 20 seconds.

NOTICE: The OpenScape Branch shall use this parameter in retry-after header field for response to the subscribers in the branch when backup link congestion is detected.

- 11) Enter the **PPP authentication**, in the **PPP Connection** area. Possible values are None, PAP (Password Authentication Protocol) or MSCHAP-V2 (MS Challenge Handshake Authentication Protocol V2).
- 12) Enter the **Username** and **Password** in the **PPP Connection** area. The must be entered in unix password format.

NOTICE: This input is mandatory entry if PPP Authentication is PAP or MSCHAP. Otherwise not mandatory.

- 13) Enter the time value for RTP session in the **Packetization interval** field, in the **RTP Connection** area. Allowed values are 10, 20, 30, 40, 50 and 60 ms. (default 20 ms)
- 14) Enter the minimum RTP port used by the Backup Link Client in the **RTP port min** field, in the **RTP Connection** area. The minimum port shall be greater than the default and less than the RTP port maximum value. (Range 35000-65535).
- 15) Enter the maximum RTP port used by the Backup Link Client in the **RTP port max** field, in the **RTP Connection** area. The maximum port shall be less than the default and greater than the RTP port minimum value (Range 35000-65535).

- 16) Enter the minimum number of B channels used by the Backup Link Client in the **Minimum number of B channels** field, in the **Multiple Links** area. (Range 1-100).
- 17) Enter the maximum number of B channels used by the Backup Link Client in the **Maximum number of B channels** field, in the **Multiple Links** area. (Range 1-100).
- 18) Enter the initial number of B channels used by the Backup Link Client in the **Initial number of B channels** field, in the **Multiple Links** area.
- 19) The minimum bandwidth (kbps) used by the Backup Link Client is displayed in the **Minimum bandwidth** field, in the **Multiple Links** area. This value is based on the number of B channels specified in the **Minimum number of B channels** field.
- 20) The maximum bandwidth (kbps) used by the Backup Link Client is displayed in the **Maximum bandwidth** field, in the **Multiple Links** area. This value is based on the number of B channels specified in the **Maximum number of B channels** field.
- 21) The initial bandwidth (kbps) used by the Backup Link Client is displayed in the **Initial bandwidth** field, in the **Multiple Links** area. This value is based on the number of B channels specified in the **Initial number of B channels** field.
- 22) Enter the high watermark (%), to indicate what percentage of the maximum bandwidth is used for overload, in the **High watermark** field, in the **Multiple Links** area. (Range 50-90).
- 23) Enter the high watermark detection window (seconds), to indicate the length of time the high watermark must be present prior to reporting the high watermark, in the **High watermark detection window** field, in the **Multiple Links** area. (Range 1-10).
- 24) Enter the low watermark (%) in the **Low watermark** field, in the **Multiple Links** area. (Range 30-70).
- 25) Enter the low watermark detection window (seconds), to indicate the length of time the high watermark must be present prior to reporting the high watermark, in the **Low watermark detection window** field, in the **Multiple Links** area. (Range 120-600).
- 26) Select the **Routing** tab to configure backup link client IP Addresses and Associated descriptions. Multiple IP addresses can be assigned.

The **Routing** tab window appears and displays backup link client IP Addresses with associated descriptions.
- 27) Click the **Add...** button.

The **Add Routing IP** window appears.
- 28) Enter the IP Address of the primary backup link server in the **IP Address** field.
- 29) Enter a description for the primary backup link server in the **Description** field.
- 30) Click the **OK** button to store the settings temporarily.

The **Add Routing IP** window is closes and the **Routing** tab is displayed with the IP address and description for the primary backup link server.
- 31) Click the **OK** button to store the settings temporarily.

The **Backup Link Client** window is closed.

- 32) Click the **OK** button to store the changes temporarily in the administrator's login session.

The **Voice over IP** dialog disappears.

- 33) Click the **Apply changes** button in the main window.

The configuration of the OpenScape Branch system as Backup Link Client has been finished.

4.8.7.2 How to Configure OSB as Backup Link Server

Proceed as follows to configure the OpenScape Branch appliance as BLS (Backup Link Server). All the fields shall set to default values on configuring BLS for each Backup link connection.

Prerequisites

Adequate administrative permissions.

The OpenScape Branch appliance is in operation.

The OpenScape Branch system is Version 1R3 or later.

The connection to the OpenScape Voice system is up.

Step by Step

- 1) Navigate to **Configuration tab > OpenScape Branch** within the Navigation Bar in the Common Management Platform.
- 2) Select the **Branch Office list** in the Navigation Tree under Administration.
The system presents the **Branch Office Overview** in the Work Area with a current list of all branch offices.
- 3) To view a list of Branch Offices 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 branch office use one of the following options:
 - In the Work Area select the checkbox to the left of the particular branch office in the list and select **Manage**. Selecting the **Manage** button updates the **Branch Office** field, in the Navigation Tree, with the selected branch office and displays information and data in the Work Area for that branch office.
 - Choose a branch office from the **Branch Office** pull-down located in the Navigation Tree. Information and data are displayed in the Work Area.
- 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) Set the **Backup link mode** field to `Server`.

- 7) Click the **Configure...** button.
The **Backup Link Server** window appears with the General tab selected.
- 8) Enter the maximum number of backup links in the **Max backup links** field.
- 9) Enter the maximum number of B channels used by the Backup Link Client in the **Maximum number of B channels** field, in the Multiple Links area. (Range 1-100).
- 10) Enter PPP Subnet IP / Netmask bits, used for backup link selection, in the **PPP Subnet IP/ Netmask bits** field.
- 11) Enter OpenScape Voice Link Status Monitor IP Address in the **OSV LSM IP address** field. This address/mask is the OpenScape Voice destination where the backup link server sends the indication that the WAN is down.
- 12) Enter the time value for RTP session in the **Packetization interval** field, in the RTP Connection area. Allowed values are 10, 20, 30, 40, 50 and 60 ms. (default 20 ms)
- 13) Enter the minimum RTP port used by the Backup Link Client in the **RTP port min** field, in the RTP Connection area. The minimum port shall be greater than the default and less than the RTP port maximum value. (Range 35000-65535).
- 14) Enter the maximum RTP port used by the Backup Link Client in the **RTP port max** field, in the RTP Connection area. The maximum port shall be less than the default and greater than the RTP port minimum value (Range 35000-65535).
- 15) Select the **Client** tab to configure backup link client server association.
The **Client** tab window appears and displays a list of backup link clients with associated information (**Tunnel name**, **BLC Host Name**, **Priority** and **Retry-after**).
- 16) Select the **Add...** button to configure backup link client server associated information.
The **Add BLS Client** window appears.
- 17) Enter the tunnel name in the **Tunnel name** field, used to inform the SNMP trap sent to OpenScape Voice to set up CAC policy. (Possible values: E.164 number type - maximum 15 digits (no special characters)).
- 18) Enter the Branch Link Client host name in the **BLC Host Name** field, used to indicate which client will use the tunnel.
- 19) Enter the priority in the **Priority** field which indicates which branches have priority for available backup links. (Value 1-nnn).
- 20) Enter the **PPP authentication**, in the PPP Connection area. Possible values are None, PAP (Password Authentication Protocol) or MSCHAP-V2 (MS Challenge Handshake Authentication Protocol V2).
- 21) Enter the **Username** and **Password** in the PPP Connection area. The must be entered in unix password format.

NOTICE: This input is mandatory entry if PPP Authentication is PAP or MSCHAP. Otherwise not mandatory.

- 22) Enter the amount of time (seconds) the link will wait to retry establishing a link, in the **Retry-after** field.

- 23) Select the **Routing** tab to configure backup link client IP Addresses and Associated descriptions. Multiple IP addresses can be assigned.
The **Routing** tab window appears and displays backup link client IP Addresses with associated information (**IP Address**, **Description**, **Tunnel name**).
- 24) Click the **Add...** button.
The **Add Routing IP** window appears.
- 25) Enter the IP Address of the primary backup link client in the **IP Address** field.
- 26) Enter a description for the primary backup link server in the **Description** field.
- 27) Select the backup tunnel name in the **Tunnel name** list, used to inform the SNMP trap sent to OpenScape Voice to set up CAC policy.
- 28) Click the **OK** button to store the settings temporarily.
The **Add Routing IP** window is closes and the Routing tab is displayed with the IP address and description for the primary backup link server.
- 29) Click the **OK** button to store the settings temporarily.
The **Backup Link Server** window is closed.
- 30) Click the **OK** button to store the changes temporarily in the administrator's login session.
The **Voice over IP** dialog disappears.
- 31) Click the **Apply changes** button in the main window.

The configuration of the OpenScape Branch system as Backup Link Client has been finished.

4.8.8 Configuration of Gateways

The OpenScape Branch supports PSTN (Public Switched Telephone Network) gateways to be configured on the proxy for normal and survivability mode.

The following issues appear:

- Up to ten Gateways can be configured.
- In the OpenScape Voice system the gateway also has to be configured as an endpoint with an IP-address or FQDN (Fully Qualified Domain Name).
- If the RG8700 is used as PSTN gateway the transport protocol must be set to TCP, otherwise a timeout can occur due to INVITE retransmission. In this case the failover rule is not followed.

NOTICE: The configuration of integrated gateways for OpenScape Branch 50i systems is described in the Integrated Gateways - Overview section.

The following table shows an example for the configuration of gateways of an OpenScape Branch system:

Row	IP Address/ FQDN	Port	Interf	Trans port	Route Prefix	Type	Functional type	Trunk Profile	Output digit strip	Output digit add	Prio- rity
1	10.234.1.238	5060	LAN	TCP		3k/4k	All Modes Egress/ Ingress	Gateway	0		0
2	10.234.1.237	5060	LAN	UDP	237	Media Matrix	Survivability Mode Egress/ Ingress	Gateway	0		1
3	RG1Nat.rg8700.com	5060	LAN	TCP	91	RG	All Modes Egress/ Ingress	Gateway	1		1
4	RG1Loc.rg8700.com	5060	LAN	TCP	9	RG	All Modes Egress/ Ingress	Gateway	0	5	1
5	RG1Int.rg8700.com	5060	LAN	TCP	9011	RG	All Modes Egress/ Ingress	Gateway	0		1
6	RG1Unk.rg8700.com	5060	LAN	TCP		RG	All Modes Egress/ Ingress	Gateway	0		1
7	RG2Nat.rg8700.com	5060	LAN	TCP	91	RG	All Modes Egress/ Ingress	Gateway	2		2

The following table describes the function of each configured gateway (each row) in the example table:

Row	Description
1	Default gateway (Priority 0) is used if called number is not a registered subscriber (after SIP manipulation) or an existing gateway rule. OpenScape Branch sends all digits to gateway 10.234.1.238. Only one gateway can be configured as default. No prefix can be configured in this rule.
2	Gateway used for Survivability Mode only (Incoming and Outgoing calls), when user dials 237 + any digits. OpenScape Branch deletes prefix (237) and sends the rest to Gateway 10.234.1.237.
3	Highest priority gateway rule (Normal/Survivability Mode Incoming/ Outgoing calls) for user dialing 91 + any digits (row 3 priority 1, row 7 priority 2). OpenScape Branch uses DNS or /etc/host file to resolve RG1Nat.rg8700.com, deletes 1 digit (9), and sends the rest to respective gateway. If gateway is not available/busy/etc then row 7 rule is used; OpenScape Branch deletes 2 digits (91), and sends the rest of the digits to RG2Nat.rg8700.com. If using different PRIs on a single RG8700 as failover routes of each other, then transport protocol must be set to TCP in Survivability Mode.

Row	Description
4	Normal Mode gateway rule (Incoming and Outgoing calls) for user dialing 9 + any digits (won't be used if 91 or 9011 are better match). OpenScape Branch will use DNS or /etc/host file to resolve RG1Loc.rg8700.com, delete 1 digit (9), prefix 5, and send digits to the respective gateway.
5	Gateway rule (Normal/Survivability Mode Incoming/Outgoing calls) for user dialing 9011 + any digits. OpenScape Branch will use DNS or /etc/host file to resolve RG1Int.rg8700.com, delete 1 digit (9), and send digits to respective gateway.
6	Gateway rule for Incoming calls only (prefix configured is dummy). OpenScape Branch will use DNS or /etc/host file to resolve RG1Unk.rg8700.com. Gateway manipulation rules do not apply. If needed to change the called number this can be done in SIP manipulation rules.
7	See Row 3 description. Row 7 is a fail over route to Row 3.

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).

IMPORTANT:

the “-” suggests a range of numbers but can't be used without []

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.

Examples of routing prefixes

[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.

8[3_6]% - only 83xxxx and 86xxxx are redirected to 1.2.3.4

7[3-6]% - calls 73xxxx, 74xxxx, 75xxxxx and 76xxxx are redirected to 5.6.7.8

6_8% - in this case, only calls 6x8xxxx (e.g. 618xxx, 698xxx) are redirected to configured destination

SIP Service Provider Profiles

SIP Service Providers can be displayed and configured. A SIP Service Provider is identified by information fields such as **Name**, **Privacy Support** and **Default Home DN**. Among others, the following attributes can be assigned to a profile:

- **Allow sending of insecure Referred-By header** - If assigned, a Referred-By header field will be sent for calls that have been transferred to the related service provider.
- **Send P-Preferred-Identity rather than P-Asserted-Identity** - If assigned, a P-Preferred-Identity header field will be sent whenever a P-Asserted-Identity header field would normally be 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** - If assigned, a SIP Diversion header field will not be sent. This attribute is primarily intended for use when connecting to a SIP Service Provider that does not understand the Diversion header field.

IMPORTANT: This flag only applies to **Survivability** mode.

- **Send URI in telephone-subscriber format** - If assigned, the character '+' will be added as prefix to R-URI, and the From, To, PAI and Diversion headers where the username is a number, according to the Global Number Format (GNF).
- **Send authentication number in Diversion header** - If assigned, the redirecting or transferring subscriber DN will be included in the Diversion header, to be used for authentication.
- **Send authentication number in P-Asserted-Identity header** - If assigned, the redirecting or transferring subscriber DN will be included in the PAI or PPI header, to be used for authentication.
- **Send authentication number in From header** - If assigned, the redirecting or transferring subscriber DN will be included in the From header, to be used for authentication.
- **Include restricted numbers in From header** - If assigned, the authentication number present in PAI, PPI or Diversion headers will be present in From header in situations where it should be anonymized.
- **TLS Certificates** - The CA file, Certificate file and Key file for TLS can be assigned.

4.8.8.1 How to Configure Gateways

Proceed as follows to add a gateway to the Voice over IP gateway list. Gateways must be configured for both, normal mode and survivability mode.

Prerequisites

Adequate administrative permissions.

At least one 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 Branch** within the Navigation Bar in the Common Management Platform.
- 2) Select the **Branch Office list** in the Navigation Tree under Administration.
The system presents the **Branch Office Overview** in the Work Area with a current list of all branch offices.
- 3) To view a list of Branch Offices 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 branch office use one of the following options:
 - In the Work Area select the checkbox to the left of the particular branch office in the list and select **Manage**. Selecting the **Manage** button updates the **Branch Office** field, in the Navigation Tree, with the selected branch office and displays information and data in the Work Area for that branch office.
 - Choose a branch office from the **Branch Office** pull-down located in the Navigation Tree. Information and data are displayed in the Work Area.
- 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 **Enable** checkbox in the **Gateways** field area.
The **Configure...** and **SIP Service Provider Profiles...** buttons become active. The SIP Service Providers Profiles button does not activate if the branch Mode is set to Branch Proxy.
- 7) Select the **System Caller Number Suppression** checkbox in the **Gateways** field area to enable Caller Number Suppression. For integrated gateways only PRI, BRI and FXS.
In Version 2, Caller Number Suppression is supported in survivability mode for all subscribers registered to the OpenScape Branch.
If an INVITE is received in the OpenScape Branch with the DN in the R-URI prefixed with the Caller Number Suppression Activation Code or if the PRI Caller Number Suppression is enabled, the Setup shall contain a Calling Number with Presentation Indicator set to Presentation Restricted. In case of CAS, the Calling Number will just not be provided.
- 8) Enter the Caller Number Suppression Access code in the **Caller Number Suppression Access Code** field in the **Gateways** field area. To suppress the calling party number during an outgoing call, the caller enters this

access code prior to dialing the outgoing number e.g. *67. For integrated gateways only PRI, BRI and FXS.

Any calls whose dialed number begins with the Caller Number Suppression Activation Code for which the requested number suppression can not be honored will be rejected. Two example scenarios are:

- Caller Number Suppression Activation Code is dialed in a call to another SIP Subscriber or to an external gateway;
- Caller Number Suppression Activation Code is dialed by the Caller and Number Suppression is disabled.

- 9) Enter the DNS refresh interval time (minutes) in the **DNS Refresh Interval** field in the **Gateways** field area. This timing is used only for gateways/trunks configured using FQDNs.
- 10) Click the **Configure...** button in the **Gateways** field area.

The **Gateways** window appears displaying the gateways configured for the OpenScape Branch system selected in a list.

- 11) Click the **Add...** button. To edit a gateway select the gateway and click the **Edit...** button.

The **Add Gateways** window appears.

- 12) Select the type of signaling in the **Signaling Address Type** selection list (Supported in Version 2). The following types are available: **IP Address or FQDN**, or **DNS SRV**. Certain Service Provider (SP) networks require identities reflect the Service Provider DNS SRV SIP Service Address, so OpenScape Branch and OpenScape SBC is responsible for ensuring the identities are properly set before forwarding the request. If dynamic SIP SP registration is used, the SP SIP servers may be located using DNS-SRV. OpenScape Branch and OpenScape SBC manages the addressing of the resolved SIP servers in both normal and survivability modes including responding to all authentication challenges.
- 13) Enter the gateway 's IP address or FQDN in the **IP Address/FQDN** field. Either the IP address or FQDN (Fully Qualified Domain Name) can be configured; not both. The FQDN is resolved via DNS (Domain Name System) or the /etc/host file.
- 14) Enter the SIP (Session Initiation Protocol) port used for communication with gateway in the **Port** field.
- 15) Select the Gateway/Trunk interface in the **Interface** field list. Possible values: **LAN** (Local Area Network), **WAN** (Wide Area Network).
- 16) Select the SIP transport protocol to be used in communication with the gateway in the **Transport** field list. Possible values are TCP, UDP, TLS.
- 17) Enter the mapped port to be used on the WAN side mapped to the port on the LAN side, in the **Mapped Port** field. This parameter applies to Branch-SBC and SBC-Proxy modes only.
- 18) Enter the routing prefix in the **Routing Prefix/FQDN** field. This parameter defines a valid Dial Number to be used in search for the gateways. The match is done on outgoing gateway calls only and the best match is always used.

- 19) Select the type of the gateway in the **Type** selection list. The following types are available: **3k/4k, Rg, Mediatatrix, Peer OSB, SIP Trunk, Integrated Gateway, Backup Link Server, Others, Voice Mail.**

NOTICE: When the OpenScape Branch is configured with ACD-Proxy Mode; the gateway type must be **Others**.

- 20) Select the functional type of the gateway in the **Functional Type** selection list. The following types are available:
- **All Modes Egress/Ingress:** Sets the gateway to make outgoing calls and accept incoming calls in Normal or Survivability Mode.
 - **All Modes Ingress:** Sets the gateway to accept incoming calls in Normal or Survivability Mode.
 - **Normal Mode Egress/Ingress:** Sets the gateway to make outgoing calls and accept incoming calls only in Normal Mode.
 - **Survivability Mode Egress/Ingress:** Sets the gateway to make outgoing calls and accept incoming calls only in Survivability Mode.
 - **Emergency:** If an emergency call in Survivability Mode is set, this route will be used to execute the call. If no emergency is found, the first egress route will be used.

NOTICE:

For Peer OSB and SIP Trunk this field must be set as **All Modes Egress/Ingress**. Incoming and outgoing calls will be accepted in Normal or Survivability Mode.

- 21) Select the trunk profile in the **Trunk Profile** selection list based on the list of profiles configured.
- Note:** For gateway **Type** equal Gateways and Peer OSB the trunk profile must be set as **Gateway**.
- 22) Enter the number of digits to be deleted of the destination URI (Uniform Resource Identifier) in the **Output digit strip** field. The digits are deleted from the beginning.
- 23) Enter the digit string to be added to digits of URI in the **Output digit add** field. The digits are added to the beginning.
- 24) Select the priority from the **Priority** selection list (0...10). This value defines which gateway will be used first. Lowest number has the highest priority.

NOTICE: For the default gateway the priority "0" is to be used. SIP Peer and SIP Trunks do not accept priority "0".

- 25) Check the **Mode in OPTIONS respond** checkbox to enable the OpenScape Branch to inform its operation mode (Normal, backup link, survivable, transition mode) in the 200OK response to the OPTIONS request.

- 26) Select the **TLS tab** to configure TLS settings.

NOTICE:

The **TLS tab** is only available if the **Transport** field is configured as TLS.

- a) 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.
 - b) 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.
 - c) Checkmark the **TLS keep-alive** checkbox, to enable the keep-alive mechanism if the connection was established by the OpenScape Branch as TLS client.
 - d) 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.
 - e) 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.
- 27) Click the **OK** button.
- The **Add Gateways** window disappears and a new row is created in the VoIP gateways table. The changes are stored temporarily.
- 28) Click the **OK** button to go back to the **Voice over IP** window.
- 29) Click the **OK** button to store the changes temporarily in the administrator's login session.
- The **Voice over IP** dialog disappears.
- 30) Click the **Apply changes** button in the main window.

The configuration of gateways is applied on the OpenScape Branch system.

4.8.8.2 How to Configure SIP Service Provider Profiles

Proceed as follows to configure SIP Service Provider Profiles.

Prerequisites

Adequate administrative permissions.

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

The OpenScape Branch system is Version 1R3 or later.

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 Branch** within the Navigation Bar in the Common Management Platform.
- 2) Select the **Branch Office list** in the Navigation Tree under Administration.
The system presents the **Branch Office Overview** in the Work Area with a current list of all branch offices.
- 3) To view a list of Branch Offices 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 branch office use one of the following options:
 - In the Work Area select the checkbox to the left of the particular branch office in the list and select **Manage**. Selecting the **Manage** button updates the **Branch Office** field, in the Navigation Tree, with the selected branch office and displays information and data in the Work Area for that branch office.
 - Choose a branch office from the **Branch Office** pull-down located in the Navigation Tree. Information and data are displayed in the Work Area.
- 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 **Enable** checkbox in the **Gateways** field area.
The **Configure...** and **SIP Service Provider Profiles...** buttons become active. The SIP Service Providers Profiles button does not activate if the the branch Mode is set to Branch Proxy.
- 7) Click the **SIP Service Provider Profiles...** button in the **Gateways** field area.
The SIP Service Provider Profiles window appears displaying the SIP Service Provider Profiles configured for the OpenScape Branch 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)
- Orange
- Skype-IP Auth
- Sprint
- Telefonica
- Vodophone/Arcor
- Verizon-EAME IP Trunking
- Verizon-IPCC Trunking
- Verizon-US IP Trunking

NOTICE:

It is highly recommended to not disable/uncheck fields that are automatically set when a "Default SIP Service Provider Profile" is chosen

- 11) Choose a privacy support configuration from the **Privacy Support** field, in the **Information** area. Possible values are: **Basic**, **Full**, **Full Send** or **Full Receive**.

- **Basic** - If Privacy Support is set to Basic, the OpenScape Branch SHALL NOT send a P-Asserted-Identity header field in the messages (requests or responses) to the endpoint. The OpenScape Branch SHALL also ignore any received P-Asserted-Identity header fields. See deviations to this statement in the note below.
- **Full** - If Privacy Support is set to Full, the OpenScape Branch SHALL send a P-Asserted-Identity (or a P-Preferred-Identity) header field in the messages (requests and responses) to the endpoint. The OpenScape Branch SHALL also accept any received P-Asserted-Identity header fields.
- **Full Send** - If Privacy Support is set to Full-Send, the OpenScape Branch SHALL send a P-Asserted-Identity (or a P-Preferred-Identity) header field in the messages to the endpoint. However, the OpenScape Branch SHALL ignore any received P-Asserted-Identity header fields.
- **Full Receive** - If Privacy Support is set to Full-Receive, the OpenScape Branch SHALL NOT send a P-Asserted-Identity header field in the messages (requests or responses) to the endpoint. However, the OpenScape Branch SHALL accept any received P-Asserted-Identity header fields. See deviations to this statement in the note below.

NOTICE:

OpenScape Branch will send a P-Asserted-Identity (or a P-Preferred-Identity) header field to a SIP Trunk which has Privacy Support set to Basic or Full-Receive, IF the SIP SP has the "Send authentication number

in P-Asserted-Identity" attribute enabled. For these scenarios, the OpenScape Branch system will only include the P-Asserted-Identity (or P-Preferred-Identity) header field in the initial SIP INVITE request sent to the SIP Trunk.

- 12) Check the **Mandatory default home DN** checkbox (Supported in Version 2). If the default home DN will always be used as the authentication number, for all outgoing calls.
- 13) Enter the Default home Destination Number in the **Default home DN** field, in the Information area (Supported in Version 2).

This parameter will contain the Default Home DN which will be used in the following situations:

- The Mandatory Default Home DN parameter is enabled. In this case the Default Home DN will always be used as the authentication id in Survivability mode.
- In Survivability Mode the Calling party is not an OpenScape Branch subscriber and there is no redirecting or transferring party.
- In Survivability Mode the redirecting or transferring party is not an OpenScape Branch subscriber.
- The parameter Registration Required is enabled. In this case the Default Home DN will be used to register to the SIP Service Provider.

- 14) Check the **Use SIP Service Address for all identity headers** checkbox, in the **Use SIP Service Address** work area. If enabled, for both normal and survivability modes, all identity header fields are modified to include the DNS SRV SIP Service Address network domain field for SIP REGISTER (if registration used), INVITE, ACK, and BYE request methods. By default, the following headers are modified to include the SIP Service Address:

- Request-URI
- From
- To
- P-Asserted-Identity
- Diversion

(OSB V10R2) Additionally, it is also possible to add the SIP Service Address on the following headers:

- Contact
- Via
- P-Preferred-Identity

- 15) Enter the SIP Service Address a character string identifying the network domain for the SIP Service Provider, in the **SIP Service Address** field.

- 16) Check the **Required** checkbox, in the Registration required area. The OpenScape Branch will be responsible for performing the registration in 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.

- 17) 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.

- 18) 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.

- 19) 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.

- 20) Enable digest authentication support by checking the **Supported** checkbox, in the **Digest Authentication supported** work area (Supported for Version 2). If the parameter Digest Authentication Supported is enabled, the OpenScape Branch or OpenScape SBC will accept being challenged by the SIP Service Provider and will respond with the credentials.

In Normal mode, the Digest Authentication will be performed by the OpenScape Voice. In Survivability mode, the Digest Authentication must be performed by the OpenScape Branch. The challenge from the SIP SP will be accepted if the parameter Digest Authentication Supported is enabled.

- 21) 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.

IMPORTANT:

Do not use "@" as delimiter, use "%" instead.

The following special characters are forbidden : "#", "% "and "/" ".The forbidden special characters are changed to "#", "%", ":" and "/" .

- 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 user names and passwords.

If Digest Authentication fails, an alarm shall be generated.

22) Select the **Options tab.**

The **Options** tab window is displayed.

23) Select the settings for the Service Provider Profile by checking the respective checkboxes, in the Settings area.

- **Allow Sending of Insecure Referred By Header** - Enable the sending of the Referred-By header in the case of Blind Transfer.
- **Send P-Preferred Identity rather than P-Asserted** - Replace P-Asserted-Identity by P-Preferred-Identity.
- **Do not send diversion header** - Diversion header is not sent in case of call redirection.

IMPORTANT: This flag only applies to **Survivability** mode.

- **Send Uri in Telephone Subscriber Format** - The + is added at the beginning of the DN in all headers.
- **Send authentication number in Diversion header** - The authentication number is sent in the Diversion header in case of redirected or transferred call.
- **Send authentication number in P-Asserted Identity header** - The authentication number is sent in the P-Asserted-Identity header in case of redirected or transferred call.
- **Send authorization number in From header** - The authentication number is sent in the From header in case of redirected or transferred call.
- **Include restricted numbers in the From header** - If enabled will ensure the Service Provider business account identity is included in the From header field when the identity is restricted (Supported in Version 2).

- 24) Select the TLS signaling from the **TLS signaling** field list in the **TLS Certificates** work area, to specify the way TLS as a transport type will be handled in SIP messages. Values are:

- **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.

- **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.

- **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.

25) Select the **Flags tab.**

The **Flags** tab window is displayed.

26) Select flags for the Service Provider Profile by checking the respective checkboxes, in the Flags area.

- FQDN in Request to URI
- FQDN to header SSP
- Refer supported SSP
- Use TO to populate the R-URI
- Spare Flag 2 - Spare Flag 10

27) Click the **OK button.**

The **Flags** window disappears and a new profile is created in the SIP Service Provider Profiles table. The changes are stored temporarily.

28) Select the **SIP manipulation tab to configure SIP Manipulation rules.**

The **SIP manipulation** tab window appears. The rules are displayed in a list.

29) 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.**

30) 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.

In **Normal Mode**, the OSV is responsible for SIP Manipulation, while the OSB handles gateway selection and Type of Number (TON) handling. The OSV will also be responsible for prefixing a dialed subscriber number with an office code.

In **Survivable Mode**, the OSB is responsible for SIP Manipulation, gateway selection, and Type of Number (TON) handling. A new rule is added by

clicking the **Add** button. To delete a rule, first click on the row in the table to select it then click the **Delete** button.

- 31) 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.
- 32) 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.
- 33) Select the SIP header the rule applies for in the **Header** selection list. Options are as follows:
 - **R-URI**
 - **From**
 - **P-Asserted Identity**

The P-Preferred-Identity header field is supported in the SIP Trunking interface, but only in the messages (requests or responses) sent FROM OpenScape Branch TO the SIP Trunking/Gateway.
 - **P-Preferred identity**

The P-Asserted-Identity and the Privacy header fields are supported in the SIP Trunking interface in both directions (i.e. FROM and TO the SIP Trunking endpoint).
 - **Diversion**
- 34) 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".
- 35) 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.
- 36) Enter the digits to be inserted at the defined position in the **Insert digits** field.
- 37) Enter the prefix to be added to the digits on the header in the **Add prefix** field.
- 38) Enter the digits to replace all header digits with in the **Replace all with** field.
- 39) Select the Call Type that digit manipulation applies for in the **Call Type** selection list. Options are as follows:
 - **All**
 - **PSTN-SIP**
 - **SIP-PSTN**
 - **SIP-SIP**
- 40) 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.
- 41) Click the **OK** button.

The **SIP Service Providers Profile** window dis appears and a new row is created in the VoIP gateways table. The changes are stored temporarily.
- 42) Click the **OK** button to go back to the **Voice over IP** window.

- 43) Click the **OK** button to store the changes temporarily in the administrator's login session.

The SIP Service Provider Profiles dialog disappears.

- 44) Click the **Apply changes** button in the main window.

The configuration of SIP Service Provider Profiles is applied on the OpenScape Branch system.

4.8.9 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.

4.8.9.1 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 or the OpenScape Branch system.

Prerequisites

Adequate administrative permissions.

At least one 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 Branch** within the Navigation Bar in the Common Management Platform.
- 2) Select the **Branch Office list** in the Navigation Tree under Administration.
The system presents the **Branch Office Overview** in the Work Area with a current list of all branch offices.
- 3) To view a list of Branch Offices 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 branch office use one of the following options:
 - In the Work Area select the checkbox to the left of the particular branch office in the list and select **Manage**. Selecting the **Manage** button

updates the **Branch Office** field, in the Navigation Tree, with the selected branch office and displays information and data in the Work Area for that branch office.

- Choose a branch office from the **Branch Office** pull-down located in the Navigation Tree. Information and data are displayed in the Work Area.

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 non Circuit RTP (Audio)** or **DSCP for Circuit RTP (Audio)** 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 (Value 1-63). 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.

The configuration of the QoS is applied on the OpenScape Branch system.

4.8.10 Endpoint Service Profiles Configuration

Endpoint Service Profiles provides the ability to configure integrated gateways FXS associated parameters in the OpenScape Branch 50i and for the Proxy ATA.

Configuration of the endpoint e.g., indicating the endpoint is a Fax, allows processing of calls and access to features based on customer needs.

4.8.10.1 How to Configure Endpoint Service Profiles

Proceed as follows to display, delete, edit or add endpoint service profiles in the Voice over IP settings or the OpenScape Branch system (V7R1).

Prerequisites

Adequate administrative permissions.

At least one 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 Branch** within the Navigation Bar in the Common Management Platform.
- 2) Select the **Branch Office list** in the Navigation Tree under Administration.
The system presents the **Branch Office Overview** in the Work Area with a current list of all branch offices.
- 3) To view a list of Branch Offices 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 branch office use one of the following options:
 - In the Work Area select the checkbox to the left of the particular branch office in the list and select **Manage**. Selecting the **Manage** button updates the **Branch Office** field, in the Navigation Tree, with the selected branch office and displays information and data in the Work Area for that branch office.
 - Choose a branch office from the **Branch Office** pull-down located in the Navigation Tree. Information and data are displayed in the Work Area.

- 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 **Endpoint service profiles** button in the **Endpoint service profiles** field area.

The **Endpoint service profiles** window appears with the **General** tab displayed by default. The Profile table is displayed with a list of profiles and parameters for those profiles.

- **Profile name:** Name configured for the profile.
- **Blocked call disconnection:** Indicated if a blocked call will disconnect with an announcement or without an announcement.

- 7) To Add up to 10 service profiles, modify or delete a profile, the following options appear:

- Select a profile from the list and click the **Delete** button to remove the profile from the list.

NOTICE:

A profile can not be deleted if there is at least one FXS port using that profile. Exception: A force lease of profiles is possible via the Local OpenScape Branch Management GUI.

- Select a profile from the list and click the **Edit...** button to edit the profile.
- Click the **Add** button to add a new profile to the list.

The **Endpoint service profiles** window appears with the **General** tab displayed by default.

- 8) Enter the profile name in the **Profile name** field.
- 9) Select the disconnect method used when a call is initiated and blocked, in the **Blocked call disconnection** field selection list. The profile shall be enabled for **Announcement** with disconnect or **Disconnect** (with reorder tone). The default value is **Disconnect**.
- 10) Select the **Blocked Call List** tab to add, modify or delete dial restriction rules associated with the endpoint service profile.

The **Blocked Call List** tab window appears, and a list of Denied Numbers patterns is displayed with associated Operational mode. The list contains up to 20 rules.

- 11) To Add up to 20 blocked call list rules, modify or delete a rule, the following options appear:
 - Select a blocked call rule from the list and click the **Delete** button to remove the rule from the list.
 - Select a blocked call rule from the list and click the **Edit...** button to edit the rule.
 - Click the **Add** button to add a new rule to the list.

The **Blocked Call** window appears.

- 12) Enter the denied number dial pattern in the **Denied Number** field. The dial pattern entered are not accepted for the endpoints associated with this endpoint service profile.

NOTICE:

The digit sequence will only be verified if the FXS dials itself. In case the FXS is involved in calls in which a SIP Subscriber deflects, blind transfers or forwards the dialed number will not be verified.

Regular expressions may be used for matching. The most important regular expression patterns are the following:

Rules for Dialing Patterns:

- % - 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).
- ^ - denotes matches or exceptions

^123% - Any number that starts a sequence of "123" at the beginning of string or line.

^[123%] - Any number that starts a sequence of 1, 2 or 3 at the beginning of string or line

[^123] Matches any number other than 1, 2 or 3

General Examples:

[09]% - A number starting with 0 or 9 and followed by any other digits.

[*][0-9]* - A number starting with literal * followed by 0 or more numerical 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.

87%|92% - A number that starts with 87 or 92 and followed by any other digits.

- 13) Select the operational mode used for when the profile will be used, in the **Operational Mode** field selection list. The profile shall be enabled for **Survivable Mode** only or **Both** survivable mode and normal modes.

- 14) Click the **OK** button to store the settings temporarily.

The **Blocked Call** window disappears, a new rule is displayed in the list in the **Blocked Call List** window.

- 15) Click the **OK** button to go back to the **Endpoint service profiles** window. The new profile is displayed in the Endpoint service profiles table.

- 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.

The configuration of the Endpoint Service Profile(s) is applied on the OpenScape Branch system.

4.8.11 Communication System Settings

The OpenScape Branch appliance is connected to the Open Scape Voice communication system.

Single Node and Node Redundancy

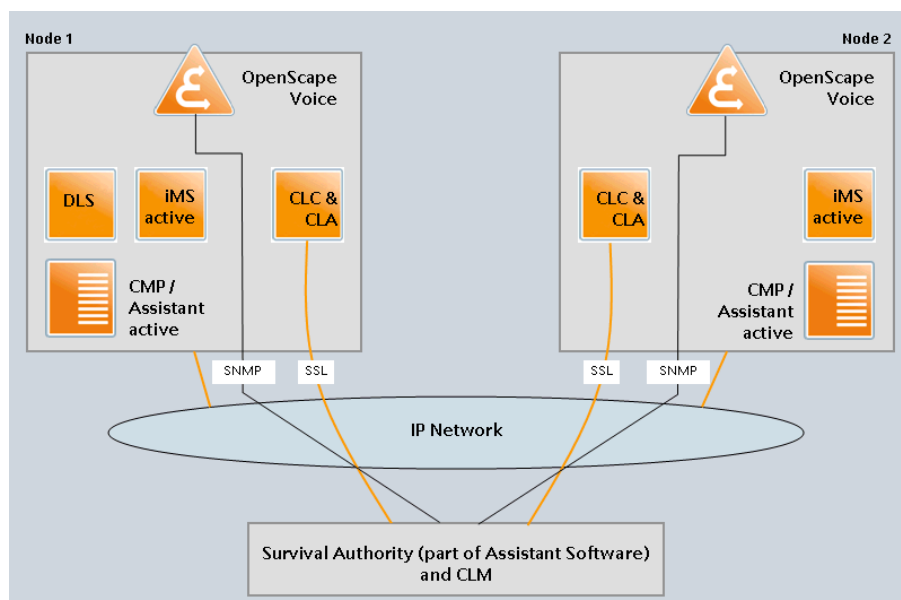
The OpenScape Voice system type depends on the redundancy concept of the IP network.

- Single Node

A non-redundant OpenScape Voice system running on a single server machine.

- Node redundancy

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.

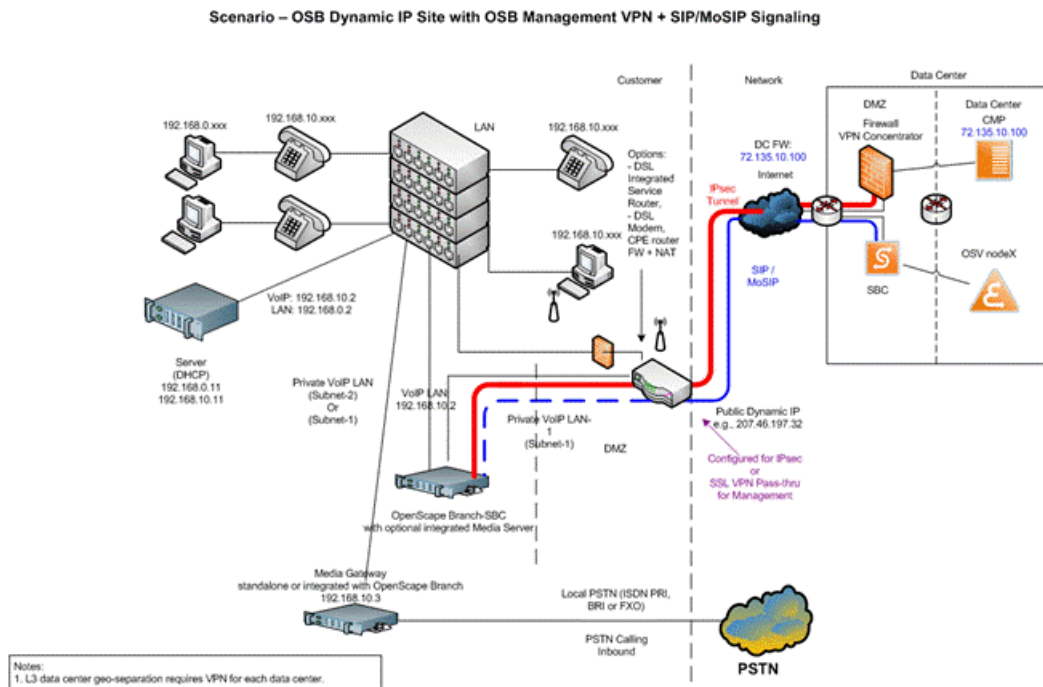


Trusted Addresses

The list of Voice over IP trusted addresses is used for geo-separated installations of the openScape Voice communication system and shows trusted SIP Servers, from which requests can be accepted.

Dynamic IP Addresses

Dynamic IP Address overview



OpenScope SBC requires the NAT device (e.g., the ISP's DSL modem) that is serving a remote branch to be assigned a static IP address.

OpenScope Branch V7 and later provides the capability to support multiple devices behind NAT (fixed or dynamic IP) is requested, e.g., to support multiple SIP phones behind same NAT of a residential home network.

Such deployments are typical for xDSL networks due to high costs for static IP addressing by network providers. The OSB appliance on the customer LAN will utilize the customer NAT router interfacing to the xDSL modem (or integrated xDSL modem/ NAT router as the IP gateway) for all communications.

The primary features are:

- Ensuring VoIP communication is maintained whenever the network provider changes the Branch IP address.
- Support media anchoring or media release based on network connectivity network associations established for the remote branch.

4.8.11.1 How to Configure the Communication System

Proceed as follows to display and configure the settings for the connected OpenScope Voice communication system.

Prerequisites

Adequate administrative permissions.

At least one 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 Branch** within the Navigation Bar in the Common Management Platform.
- 2) Select the **Branch Office list** in the Navigation Tree under Administration.
The system presents the **Branch Office Overview** in the Work Area with a current list of all branch offices.
- 3) To view a list of Branch Offices 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 branch office use one of the following options:
 - In the Work Area select the checkbox to the left of the particular branch office in the list and select **Manage**. Selecting the **Manage** button updates the **Branch Office** field, in the Navigation Tree, with the selected branch office and displays information and data in the Work Area for that branch office.
 - Choose a branch office from the **Branch Office** pull-down located in the Navigation Tree. Information and data are displayed in the Work Area.
- 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 Branch is connected to the OpenScape Voice network. Possible values:
 - **Simplex**: Single node configuration.
 - **Collocated**: In this mode redundant SBCs are configured with one SBC in active mode and the other SBC in standby mode.
 - **Geo-Separated**: This mode means that the two nodes are at different locations.

NOTICE: If the configuration is set to "Cluster" or "Geo-Separated", the Node 2 fields and the Outbound SIP server field will be enabled.

- 8) Select the node in the **Outbound SIP Server** selection list. This configures, which node OpenScape Branch will use to forward the SIP requests.
Possible values: **Node 1, Node 2**.
- 9) 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.

- 10) 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.

- 11) Enter or modify the trusted server IP address or FQDN (Fully Qualified Domain Name) in the **IP Address/FQDN** field.
- 12) Enter / modify the SIP port of the trusted server in the **Port** field.
- 13) 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).
- 14) 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.
- 15) Check the **Enable outbound proxy** checkbox (For Proxy ATA).
- 16) Enter the **Outbound proxy**, in the General work area, (For Proxy ATA and Proxy - SBC). The outbound Proxy IP Address shall be used when the Enable outbound proxy is enabled.
- 17) Enter the **Outbound proxy port**, in the General work area (For Proxy ATA). The outbound proxy port where OpenCape Branch in Proxy-ATA mode will attempt to connect when the Enable outbound proxy is enabled.
- 18) Check the **Enable path tagging** checkbox (For Proxy ATA and SBC-Proxy). Allows OpenScape Branch in Proxy ATA mode to send the header "Path" in the SIP messages and an OpenScape Branch which has connected ATA to handle the messages with this header.
- 19) Check the **Branch behind SBC** checkbox if this OpenScape Branch is connection behind a Session Border Controller (SBC). This applies to an OpenScape Branch configured for SBC-Proxy mode, when connected to an OpenScape SBC which is connected to an OpenScape Voice.
- 20) Check the **Branch behind NAT** checkbox if this OpenScape Branch is connection behind a NAT and specify the X-Siemens-Identity header field containing the encrypted BRANCH_NAME shall be included in the survivability SIP OPTIONS request message..
- 21) 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 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 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: The SRV record where the IP addresses of the primary and the secondary server are retrieved from. Each DNS-SRV/FQDN name must be made up only of letters, numbers, and the hyphen character "-". The characters are not case-sensitive. Each section of an FQDN can be up to 63 characters long.
 - i) **Transport** field: SIP protocol used to communicate with the server.
- 22) 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 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 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: The SRV record where the IP addresses of the primary and the secondary server are retrieved from. Each DNS-SRV/FQDN name must be made up only of letters, numbers, and the hyphen character "-". The characters are not case-sensitive. Each section of an FQDN can be up to 63 characters long.
 - i) **Transport** field: SIP protocol used to communicate with the server.
- 23) Click the **OK** button to go back to the **Voice over IP** window.
- 24) Click the **OK** button to store the changes temporarily in the administrator's login session.
- The **Voice over IP** dialog disappears.
- 25) Click the **Apply changes** button in the main window.

The configuration of the communication system is applied on the OpenScape Branch system.

4.9 How to Configure Timers and Thresholds

Proceed as follows to configure the timers and thresholds to control the system performance of the OpenScape Branch appliance.

Prerequisites

Adequate administrative permissions.

At least one 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 Branch** within the Navigation Bar in the Common Management Platform.
- 2) Select the **Branch Office list** in the Navigation Tree under Administration.
The system presents the **Branch Office Overview** in the Work Area with a current list of all branch offices.
- 3) To view a list of Branch Offices 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 branch office use one of the following options:
 - In the Work Area select the checkbox to the left of the particular branch office in the list and select **Manage**. Selecting the **Manage** button updates the **Branch Office** field, in the Navigation Tree, with the selected branch office and displays information and data in the Work Area for that branch office.
 - Choose a branch office from the **Branch Office** pull-down located in the Navigation Tree. Information and data are displayed in the Work Area.
- 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 Branch 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 Branch 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 Branch system.

4.10 How to Configure the VoIP Codec Priority List

Proceed as follows to configure the priority of the supported codecs on the codec negotiation.

Prerequisites

Adequate administrative permissions.

At least one 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 Branch** within the Navigation Bar in the Common Management Platform.

2) Select the **Branch Office list** in the Navigation Tree under Administration.

The system presents the **Branch Office Overview** in the Work Area with a current list of all branch offices.

3) To view a list of Branch Offices 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 branch office use one of the following options:

- In the Work Area select the checkbox to the left of the particular branch office in the list and select **Manage**. Selecting the **Manage** button updates the **Branch Office** field, in the Navigation Tree, with the selected branch office and displays information and data in the Work Area for that branch office.
- Choose a branch office from the **Branch Office** pull-down located in the Navigation Tree. Information and data are displayed in the Work Area.

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 **Codecs** tab.

The codec priority list is displayed.

7) The codec priority list contains the priority of each supported codec on the codec negotiation. The same codec can not be set to different priorities.

- a) To assign a codec to a priority select the codec in the **Select codec** selection lists. Possible values: G711U, G711A, G729, G722, G7221 24K bitrate, G7221 32K bitrate, iLBC, iSAC, "empty string".
- b) Click the **Add** button and assign the codec to a priority.
- c) To change the codec priority, check the respective line in the list and use the **Move up** and/or **Move down** buttons.

- 8) Click the **OK** button to store the changes temporarily in the administrator's login session.

The **Voice over IP** dialog disappears.

- 9) Click the **Apply changes** button in the main window.

The settings for the codec negotiation are applied on the OpenScape Branch system.

4.11 How to Configure RTP Settings

Proceed as follows to configure the RTP (Real-time Transport Protocol) settings for the OpenScape Branch 50i hardware.

Prerequisites

Adequate administrative permissions.

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

The connection to the OpenScape Voice system is up.

The system is of the OpenScape Branch 50i type and the integrated gateway is enabled.

Step by Step

- 1) Navigate to **Configuration tab > OpenScape Branch** within the Navigation Bar in the Common Management Platform.
- 2) Select the **Branch Office list** in the Navigation Tree under Administration.
The system presents the **Branch Office Overview** in the Work Area with a current list of all branch offices.
- 3) To view a list of Branch Offices 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 branch office use one of the following options:
 - In the Work Area select the checkbox to the left of the particular branch office in the list and select **Manage**. Selecting the **Manage** button updates the **Branch Office** field, in the Navigation Tree, with the selected branch office and displays information and data in the Work Area for that branch office.
 - Choose a branch office from the **Branch Office** pull-down located in the Navigation Tree. Information and data are displayed in the Work Area.
- 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 **RTP** tabsheet.

- 7) The integrated gateway supports the generation and reception of RTCP messages. Enter the interval between the RTCP (Real-time Control Protocol) messages in the **RTCP Interval** field in milliseconds.
- 8) Check the **RTP Protection** checkbox: Packets coming from an IP address which is different to the source of the RTP stream are discarded.
- 9) Configure the settings of the jitter buffer. In order to reduce the effect of jitter, a buffer is used to ensure the continuous transmission of audio over the network.
 - a) Check the **Jitter Buffer** checkbox to activate the jitter buffer.
 - b) Enter the maximum buffer size in milliseconds in the **Maximum size** field. It is enabled if Jitter buffer is enabled.
 - c) The jitter can have a fixed size or it can be adapted dynamically. Select the functionality in the **Implementation** selection list. Possible values are *Fixed*, *Adaptive*.
- 10) The packetization time determines the interval between the RTP packets. Select the value in milliseconds (Possible values: 10, 20, 30) in the **Packetization Time** field.
- 11) Check the **Enable RFC 2833** checkbox: to allow negotiation and signaling of DTMF information through the RTP stream.
- 12) Click the **OK** button to store the changes temporarily in the administrator's login session.

The **Voice over IP** dialog disappears.
- 13) Click the **Apply changes** button in the main window.

The RTP settings for the integrated gateway of the OpenScape Branch 50i are configured.

4.12 How to Configure Signaling and Transport Settings

Proceed as follows to configure the Signaling and Transport settings e.g., TCP and INVITE settings for the OpenScape Branch hardware.

Prerequisites

Adequate administrative permissions.

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

The connection to the OpenScape Voice system is up.

The system is of the OpenScape Branch type and the integrated gateway is enabled.

Step by Step

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

The system presents the **Branch Office Overview** in the Work Area with a current list of all branch offices.

- 3) To view a list of Branch Offices 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 branch office use one of the following options:
 - In the Work Area select the checkbox to the left of the particular branch office in the list and select **Manage**. Selecting the **Manage** button updates the **Branch Office** field, in the Navigation Tree, with the selected or branch office and displays information and data in the Work Area for that branch office.
 - Choose a branch office from the **Branch Office** pull-down located in the Navigation Tree. Information and data are displayed in the Work Area.

- 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 **Signaling and Transport Settings** tabsheet.
- 7) Enter the timeout value for INVITE in normal mode of operation in the **INVITE timeout Normal Mode** field in milliseconds (Value: 120000 - 600000 ms). This timer is used if no final reply for an INVITE arrives after the 100 trying was received.

NOTICE:

Certain applications, such as OpenScape Mobile (OSMO), require values greater than the 360000 ms default to operate correctly.

- 8) Enter the timeout value for INVITE in survivable mode of operation in the **INVITE timeout Survivable Mode** field in milliseconds (Value: 120000 - 600000 ms). This timer is used if no final reply for an INVITE arrives after the 100 trying was received.

NOTICE:

Certain applications, such as OpenScape Mobile (OSMO), require values greater than the 180000 ms default to operate correctly.

- 9) Enter the TCP connection lifetime value in the **TCP connection lifetime** field. This parameter is used to indicate how long the TCP connection will be extended after any activity on the TCP connection has ceased. (Value: 60- 1200 seconds, Default: 350 seconds).
- 10) Enter the TCP connect timeout value in the **TCP connect timeout** field. When attempting to establish an outgoing TCP connection; this parameter is used to indicate the length of time allowed to establish the connection. If timeout occurs, the attempt to establish the TCP connection will be stopped. (Value: 1 - 10 seconds, Default: 4 seconds).
- 11) Enter the TCP send timeout value in the **TCP send timeout** field. Once a TCP connection is established, if there is no response from the destination; this parameter is used to indicate the length of time the TCP connection will

wait for a response before closing the connection. (Value: 1 - 10 seconds, Default: 3 seconds).

- 12) Click the **OK** button to store the changes temporarily in the administrator's login session.

The **Voice over IP** dialog disappears.

- 13) Click the **Apply changes** button in the main window.

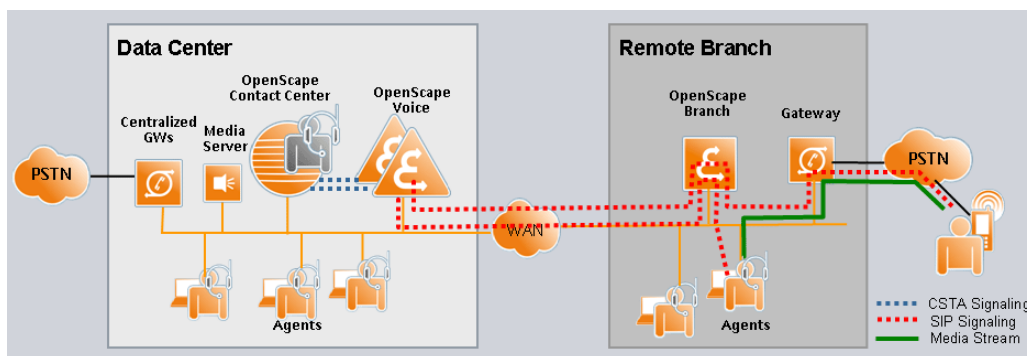
The Signaling and Transport settings for the OpenScape Branch are configured.

4.13 Automatic Call Distribution — Overview

OpenScape Voice supports both OpenScape Contact Center (OSCC) and Genesys as external Automatic Call Distribution (ACD) solutions. OpenScape Branch ACD operates as a backup to OSCC and Genesys when the Branch is in survivability mode.

If the OpenScape Branch enters survivability mode, OpenScape Branch ACD allows for operating a call center with up to 250 attendants within a branch office. With OpenScape Branch V1R3 up to 100 ACD queues are supported, with OpenScape Branch V1R2 up to 10 ACD queues are supported in branch survivability mode.

ACD Application Scenario with External ACD Solution in Normal Operation



Incoming calls are sent via the OpenScape Branch proxy to the OpenScape Voice system. If these calls are for the call center, the call gets sent to the OpenScape Contact Center (OSCC) or Genesys SIP Server (SIP S) in the branch office responsible for the call center number.

During Normal operation, incoming calls are sent via OpenScape Branch proxy to the OpenScape Voice. If these calls are for the contact center, the OpenScape Contact Center Server is informed about the call via CSTA Monitoring. The OpenScape Contact Center is able to make a routing decision for this call and send the routing decision to OpenScape Voice which will forward the call to the defined destination:

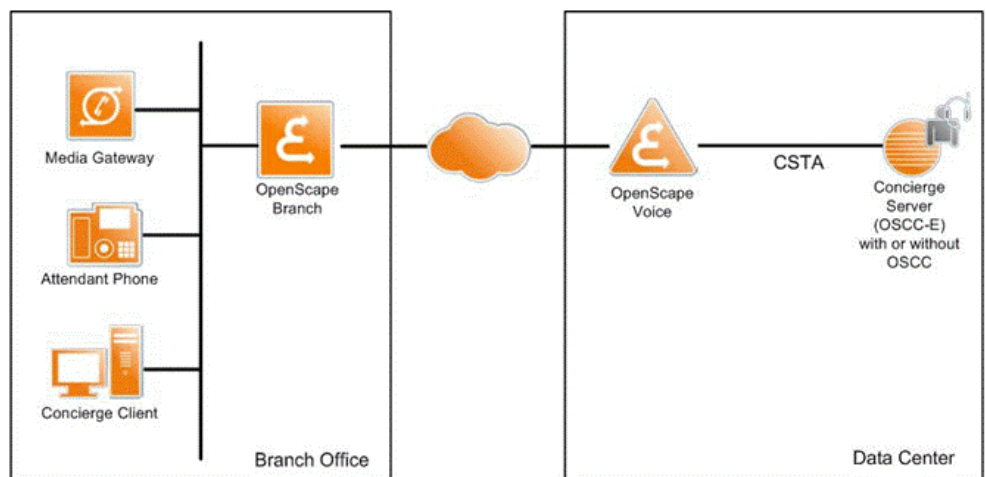
- Send call to a free agent.
- Queue the call at the OpenScape Voice.
- Send call to Voice Mail if no agent is free (option)
- Other treatments such as playing a greeting announcement, getting information, etc.

The Genesys SIP Server triggers the Genesys URS (Universal Routing Server) in the data center to request a routing decision for this call. Depending on what the URS knows about the call center number and the ACD that is handling this number, it sends a routing decision back to the SIP server:

- Send call to a free agent.
- Queue the call at the Genesys SIP S.
- Other treatments such as playing a greeting announcement, getting information, etc.

When the SIP server gets the request to send the call to a free call agent, it hands the media stream for the call over to the OpenScape Voice system which calls the agent. In normal operation mode the backup ACD configuration of the OpenScape Branch system is not in use.

ACD Application Scenario with OpenScape Concierge Attendant with OpenScape Concierge Server (OSCC-E)



OpenScape Concierge is an attendant console application that uses the call control capabilities of the CSTA protocol to OpenScape Voice to deliver calls to the intended recipients. Calls are initially delivered to OpenScape Voice Multi-Line Hunt Groups (MLHGs) from where these calls may be “picked” (answered) by Concierge attendants.

The Concierge operations are controlled by the Concierge Server (OSCC-E).

It is also possible to perform the call control of the OpenScape Concierge by means of the OpenScape Contact Center (OSCC).

If the solution is composed of the OSCC-E and OSCC, the attendants will be handled as agents by the OSCC.

In the case of a scenario with a branch, the Concierge Attendant Console is located behind an OpenScape Branch. The Concierge Attendant Console usually consists of a client application in a desktop and an OpenStage phone.

In the case of and OpenScape Concierge without the OSCC server the Attendant will pickup the calls from the Concierge Client.

4.13.1 Automatic Call Distribution and Survivability

Survivability for ACD is the capability of the system to maintain service continuity in the presence of faults.

Local Branch ACD backup is supported for OpenScape Concierge Server (OSCC-E) with or without OpenScape Contact Centers (OSCC), and Genesys Contact Centers in survivability mode due to component or network failure.

Feature Overview

The OpenScape Branch supports a fallback mechanism for Call Center call distribution when the system is operating in survivability mode.

For OpenScape Branch V2 the OpenScape Concierge is supported and is handled as an Agent if the solution is composed of the OpenScape Concierge Server (OSCC-E) and the OpenScape Contact Center (OSCC).

For OpenScape Branch V1R3 and later versions a mechanism is implemented to automatically synchronize the agent status in normal and survivability mode. In OSB V1R2 the fallback mechanism is performed by a maximum of 10 ACD queues which are configured in the OpenScape Branch. In OSB V1R3 the maximum number has been increased to 100 ACD Queues.

In OSB V1R2, if all agents are busy, or if there are no agents logged for the ACD queue into which a call is queued, the OpenScape Branch offers the possibility to send the call to an overflow destination or to disconnect the call. In OSB V1R3 and later versions it is possible to overflow to a local Voice Mail system.

- Call queuing and routing based upon basic agent groups.
- Up to 250 agents or OpenScape Concierge Attendants can be configured in an OpenScape Branch.
- Number of logged on agents, OpenScape Concierge Attendants and call capacities are platform dependent.
- Agent and OpenScape Concierge Attendant status is synchronized between OpenScape Branch and OpenScape Contact Center.
- Circular/round-robin agent/OpenScape Concierge Attendant assignment with announcements and music-on-hold.
- OpenScape Branch queued calls can be transferred to the OSCC queues when the fault is resolved.

Additional Considerations:

- During normal mode the Centralized OSCC Media Server are used for Music on Hold and Announcements.
- In survivable mode the ACD related Music on Hold and interims Queue related Announcements are provided by the ACD function.
- The OpenScape Branch needs to be in "Proxy ACD" operating mode. No ACD Support for OpenScape Branch in "branch SBC" mode.
- The OpenScape Branch ACD functionality is supported for survivability only. No OpenScape Branch ACD support during normal operating mode.
- Call Admission Control (CAC) set to 0 is supported for Contact Center agents and OpenScape Concierge Attendants in OpenScape Version 2.

If CAC is set to 0 (zero) in the OpenScape Voice, and the final destination is not in the same branch as the media gateway, the payload shall traverse through a PSTN call. If the call comes in from a media gateway in the

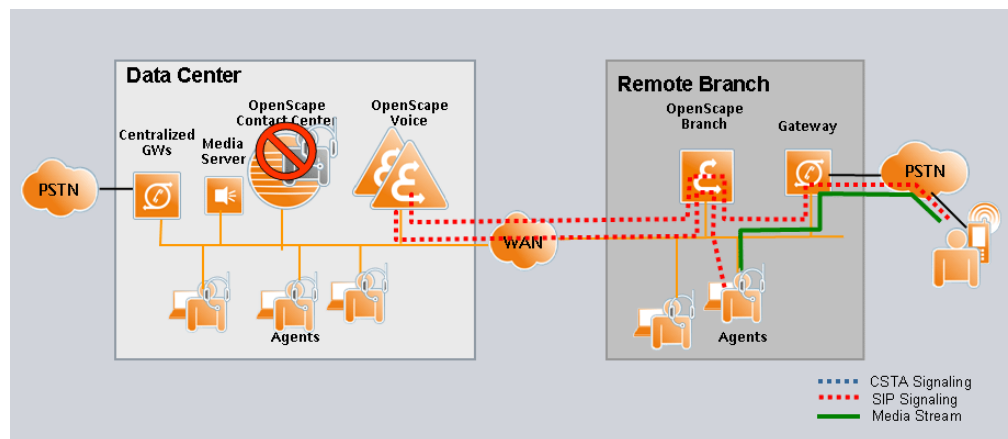
branch, it shall go out through a gateway in this same branch to the remote destination.

NOTICE:

CAC 0 with Concierge will only be applied if the Music on Hold while the call is in the queue is provided by the Media Server in the Branch

- Free Media Choice (FMC) is not currently supported for Contact Center agents.
- OpenScape Branch V1 R3 is released to interwork with OSCC V7 R3 and V8.
- OpenScape Branch V2 is released to interwork with OSCC V8 R1 and later versions.
- OpenScape Branch V2 is released to interwork with OSCC-E V1 R3.

OSCC/OSCC-E & OSB ACD – Normal Mode – OSCC-E (Concierge) and/or OSCC Failure



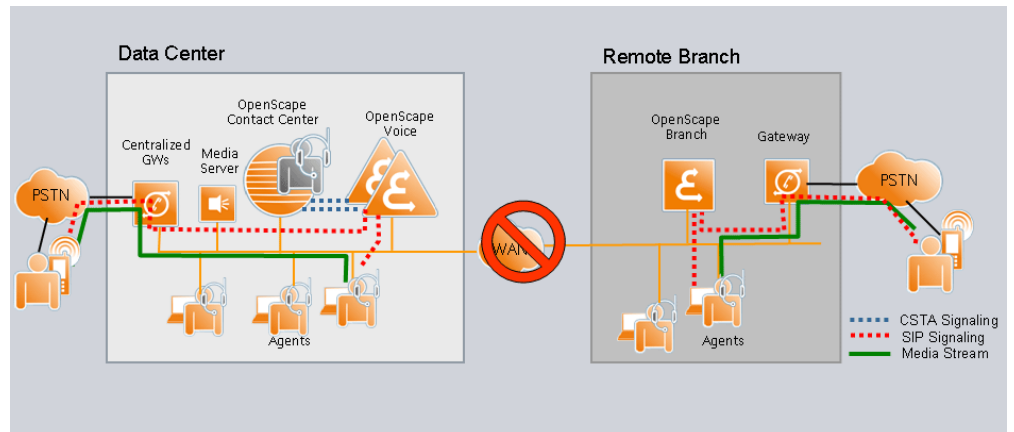
Calls can arrive at the Branch and/or at the Data Center and can be routed to agents at the Branch and/or at the Data Center.

In this example, a call arrives at a Branch and is routed by the fallback OSV MLHG mechanism to a free agent.

NOTICE:

Membership of the Attendant in the each MLHG is operationally relevant only when the IP connection between the Voice Server and the OSCC-E server is down. In this case, the OpenScape Voice will use its basic MLHG routing logic to deliver calls to the Attendants.

OSCC & OSB ACD – In Survivable mode (WAN Failure)



The OpenScape Branch system will be in survivable mode in case there is a WAN outage between the branch office and the OpenScape Voice system in the data center.

In Survivability Mode, OpenScape Branch cannot deliver the incoming calls from the public network to the OpenScape Voice. These calls are transferred to an ACD queue on the OpenScape Branch. The Attendant subscribers which are in the branch shall be automatically logged in as Agents to an ACD Queue in the OpenScape Branch.

- Calls arriving at the Data Center are routed to an agent at the Data Center by OSCC.
- Calls arriving at the Branch are routed to an agent at the Branch by OpenScape Branch's backup ACD routing.

Agents need to be logged into OpenScape Branch ACD.

- OSCC has no statistics about the ACD calls at the branch.

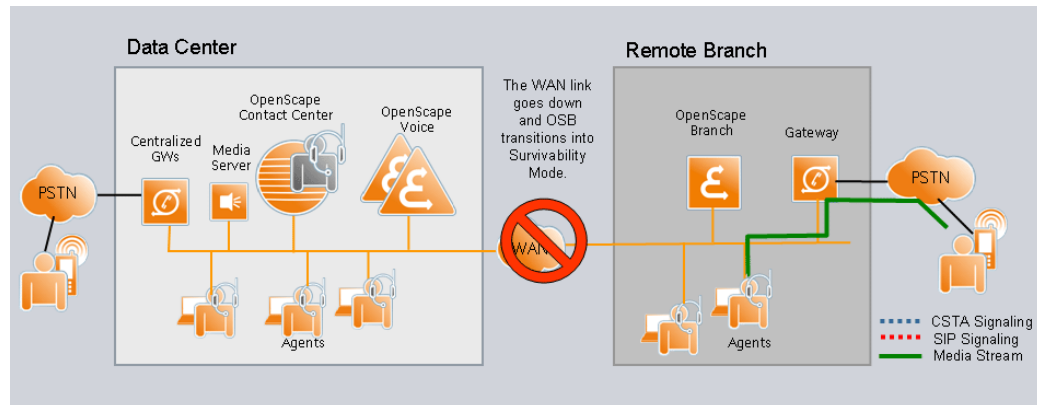
Agent or OpenScape Concierge Attendant has no access to client application.

- The Concierge solution uses the Backup ACD in the OSB to distribute the calls to the Attendants in the branch.
- During this mode of operation the dial plan rules in OSB must be set up to route this call to B2BUA which will distribute the call via an ACD Queue to an available Attendant. The sip server will send the outgoing INVITE request from B2BUA to the requested Attendant.
- Features like Park, Intercept on No Answer, Intercept on Busy and Transfer Security Intercept are not supported in Survivability Mode. Concierge Client will not be able to pickup calls from queue in Survivability Mode.

NOTICE:

In Survivability Mode, subscribers in other branches can be reached via the PSTN.

OSCC & OSB ACD – Transition into Survivability Mode



- Active and pending incoming calls in the OSB will only be disconnected when the calling party disconnects.
- Calls which are queued in the MLHG queues in the OpenScape Voice will only be disconnected if the MLHG is configured to time out the call.
- Active calls are only disconnected by Session Timer (default of 30 minutes).
- The status of the agent will only be updated towards the OSCC, if the call to which it was connected is disconnected in the OpenScape Voice side.
- The ready / not ready status of the agent will not be updated towards the OSCC.
- The subscriber state will only be changed if the Registration Timer expires.
- In case of Concierge with OSCC, the Attendant will be automatically logged into the Backup ACD in the OpenScape Branch.
- In case of Concierge without OSCC, the Attendant must manually log in to the Backup ACD when it starts the Concierge client.

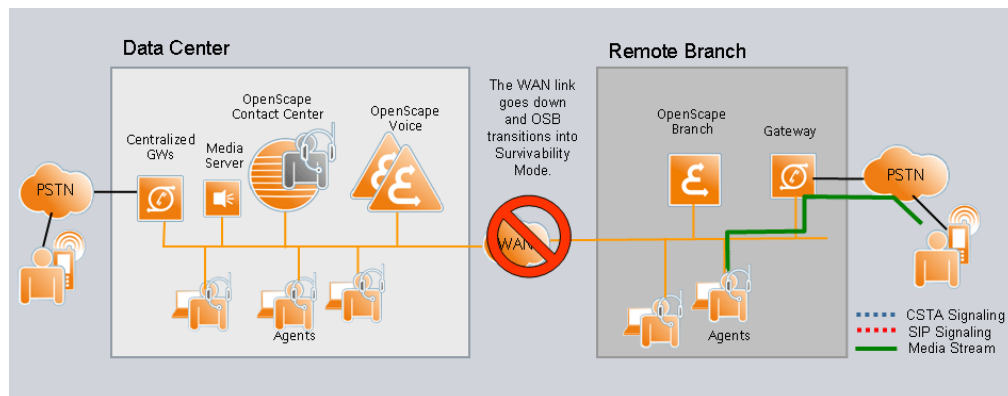
NOTICE:

New incoming calls are handled by the OpenScape Branch as described in Survivable Mode.

NOTICE:

By transitioning to survivability mode, calls which are listening to MoH at the local integrated Media Server will be lost. Since the calls were routed to the local Media Server by the OpenScape Voice, the OpenScape Branch is crossed by two legs of the same call: from the GW to OpenScape Voice and from OpenScape Voice to Media Server. However, both these legs can not be correlated and due to that it is not possible to get control of the calls when the OSB enters in survivability mode. In this case, the PSTN channels in the Media Gateway and the media channels in the local OpenScape Branch media server remain occupied. In order to avoid that the customer is waiting forever without any chance to be attended, the OpenScape Branch Media Server shall be restarted to release the media channels. By getting silence, it is expected that the callers will disconnect releasing the resources.

OSCC & OSB ACD – Transition to Normal Mode



- The subscriber state will only be changed if the Registration Timer expires. During transition from survivability mode to normal mode, the calls which are queued in B2BUA will be de-queued from B2BUA and will be forwarded to OpenScape Voice. By re-queuing the calls to OpenScape Voice, if the first call is not successfully re-queued, the process is interrupted and the calls remain in the ACD queues in OpenScape Branch. The status of the agent will only be updated towards the OSCC, if the call to which it was connected is disconnected in the OpenScape Voice side.
- The subscriber state will be updated because the Agent/Attendant subscriber will send a new REGISTER request.
- The ready / not ready status of the agent will be automatically updated towards the OSCC because the subscriber will send SUBSCRIBE for the Toggle key.

4.13.2 Automatic Call Distribution Configuration

OpenScape Branch ACD (Automatic Call Distribution) allows for operating a call center within a branch office of the OpenScape Branch type, when the branch enters survivability mode.

OpenScape Branch Assistant allows to configure the settings for the OpenScape Branch ACD application used during branch survivability mode. The OpenScape Branch ACD application can take over from the OpenScape Contact Center and OpenScape Concierge Server in the case of communication loss between the branch and the data center, or the Genesys SIP Server in case it is inoperable because it cannot communicate with the Universal Routing Server located in the data center together with the OpenScape Voice Application.

General Configuration

The general ACD configuration covers the ACD agent's/OpenScape Concierge Attendant's settings which are valid for all agents/OpenScape Concierge Attendants (e.g. access codes, timeout) and the assignment of audio files for announcements. The status of all agents/OpenScape Concierge Attendants configured can be displayed in a separate dialog window.

Agent/OpenScape Concierge Attendant timeout versus queue advance timeout behavior:

- The Agent timeout is set lower or equal than the queue advance timeout:
When the ACD call rings on the agent until the agent timeout expiration, the agent will stop ringing, will be logged off and the next available agent/ OpenScape Concierge Attendant will be called.
- The Agent timeout is set greater than the Queue advance timeout:
When the ACD call rings on the agent/OpenScape Concierge Attendants until the queue advance timeout expiration, the agent will stop ringing (but not logging off) and the next available agent will be called.

NOTICE:

The difference between the timeouts shall be at least 5 seconds in order to avoid delays caused by cell calls for example.

Toggle Key Configuration (OSB V1R3 and later versions only)

In normal operation of the Contact Center with OpenScape Contact Center (OSCC), the Keyset Toggle key is used on the phone to toggle between Available and Unavailable. In parallel, this key is used to automatically logon to the OpenScape Branch ACD so if the OpenScape Branch switches to survivability mode and the OpenScape Branch ACD takes over the call distribution; the agents are already logged on to the queues they were configured for in the OpenScape Branch. In the case of the branch entering survivability mode with the Genesys application, agents must manually logon to the OpenScape Branch ACD.

NOTICE:

Currently, Keyset Toggle key status is not applicable when Agent timeout is in use.

Queue Configuration

ACD queue configuration allows the administrator to define up to 100 backup ACD queues for OSB V1R3 (10 for OSB V1R2) which can be assigned to profiles. The configured ACD queues are ready to distribute calls in normal mode as well as in survivable mode.

The backup ACD queues (e.g. 15615559999) on OpenScape Branch need to be configured in advance. These queues must be associated to the incoming call center numbers (e.g. 18005551111). The same association must be created on the OpenScape Voice system. Call center calls must be primarily delivered to the Genesys SIP Server (with 18005551111) and if that does not succeed an alternate route is provisioned that allows the call to be delivered to OpenScape Branch (with 15615559999).

Configuration of Profiles

A profile can be assigned to the backup ACD queues. Each ACD agent/ OpenScape Concierge Attendant is assigned to a profile. The profile name and the numbers of the queues assigned can be configured.

Configuration of Agents and OpenScape Concierge Attendants

To distribute calls, the agents have to log in to backup ACD queues entering a password. The password, ID, Name and profile assigned to an agent/ OpenScape Concierge Attendant can be configured.

Configuration Restrictions

A maximum number of 250 agents is allowed to configure. The following features should not be used in ACD agents:

- Do Not Disturb,
- Call Refuse,
- Call Deflect,
- Call Forwarding (all types),
- Large conference,
- Keysets/line appearances,
- Call Waiting,
- Hot/Warm line.

Requirements

The following are the OpenScape Voice system requirements:

- ACD requires the system-wide feature 'Endpoint Rerouting' to be provisioned. This feature allows rerouting of calls once a primary route of a destination is inaccessible or otherwise unavailable
- Activating the system-wide feature 'Registration Renewal' is highly recommended as this allows an inaccessible route of a destination to be audited for return to normal conditions.

4.13.2.1 How to Configure General ACD Agent Settings

Proceed as follows to edit the general settings for the ACD (Automatic Call Distribution) agents which apply for all agents configured.

Prerequisites

Adequate administrative permissions.

The branch office of the OpenScape Branch type is configured and in operation.

The connection to the OpenScape Voice system is up.

The corresponding system components of the external ACD solution (e.g. OpenScape Contact Center or Genesys) are configured.

Step by Step

- 1) Navigate to **Configuration tab > OpenScape Branch** within the Navigation Bar in the Common Management Platform.
- 2) Select the **Branch Office list** in the Navigation Tree under Administration.
The system presents the **Branch Office Overview** in the Work Area with a current list of all branch offices.

- 3) To view a list of Branch Offices 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 branch office use one of the following options:
 - In the Work Area select the checkbox to the left of the particular branch office in the list and select **Manage**. Selecting the **Manage** button updates the **Branch Office** field, in the Navigation Tree, with the selected branch office and displays information and data in the Work Area for that branch office.
 - Choose a branch office from the **Branch Office** pull-down located in the Navigation Tree. Information and data are displayed in the Work Area.
- 5) Navigate to **Configuration > ACD in the navigation tree under Administration**.

The **ACD** window appears with the **General** tab selected by default.

- 6) Enter the log on service access code in the **Log On Service Access Code** field. The value must be different from the log off service access code. Valid digits are 0-9 and "*". This access code can be used in both survivable and normal modes of operation.
- 7) Enter the log off service access code in the **Log Off Service Access Code** field. The value must be different from the log on service access code. Valid digits are 0-9 and "*". This access code can be used in both survivable and normal modes of operation.
- 8) Enter the time in seconds how long an agent will ring before the agent is considered unavailable and is logged off from the queues in the **Timeout** field.

NOTICE: The agent will need to log on again after he has been logged off from the queues assigned. It will not have effect if the advance timeout is greater than the queue advance timeout.

- 9) For OpenScape Branch V1R3 and later versions, the toggle key can be configured as follows:

- a) To activate the keyset toggle key function for survivability, check the **Support Keyset Toggle Key** checkbox.

The **Agent ID** in OpenScape Branch must be configured with the Business Group Line (BGL) number for correct Keyset Toggle Key operation.

The ACD Agent will be automatically logged in to the Backup ACD in Normal Mode according the state of the Keyset Toggle key. In Survivability Mode, the ACD Agent is also able to manually log in and log out by hitting the Keyset Toggle key. In this case, the ACD Agent will not be able to login by dialing the access code.

If the checkbox is disabled, the ACD Agent must manually log in by dialing the access code.

- b) Enter the code which will be used to toggle between Available and Unavailable in the **Keyset Toggle Service access code** field.

- 10) For OpenScape Branch, Audio files can be selected for ACD Music on Hold and Announcements:

- a) To select a file for Music on Hold click the **Music on Hold Configure... button**.

The Music on Hold dialog appears.

- b) Enter the file location of the Music on Hold file or click the **Browse...** button to select a file.
- c) Once a file is located click the **Add...** button to add the file to the Music on Hold available files. Additional files can be added.

The Music on Hold files can then be assigned to the ACD Queue in the **Queue** tabsheet.

NOTICE:

Only WAV audio files (.wav) that comply with the following requirements can be uploaded:

- Bit Rate: 128 kbps
- Audio Sample size: 16 bit
- Channels: Mono
- Sampling Rate: 8 kHz
- Audio Format: PCM

For systems with only 2GB of flash memory; it is not recommended to upload more than 20MB of wave files to a system for Music on Hold and Announcements.

The Music on Hold file name appears in the list of available files.

- d) Click the **Close** button when finished.

The Music on Hold dialog disappears and the ACD dialog re-appears.

- e) To select a file for Announcement click the **Announcement Configure... button**.

The Announcement dialog appears.

- f) Enter the file location of the Announcement file or click the **Browse...** button to select a file.
- g) Once a file is located click the **Add...** button to add the file to the Announcement available files. Additional files can be added.

The announcement files can then be assigned to the ACD Queue in the **Queue** tabsheet.

NOTICE:

Only WAV audio files (.wav) that comply with the following requirements can be uploaded:

- Bit Rate: 128 kbps
- Audio Sample size: 16 bit
- Channels: Mono
- Sampling Rate: 8 kHz
- Audio Format: PCM

For systems with only 2GB of flash memory; it is not recommended to upload more than 20MB of wave files to a system for Music on Hold and Announcements.

The Announcement file name appears in the list of available files.

h) Click the **Close** button when finished.

The Announcement dialog disappears and the ACD dialog re-appears.

- 11) Click the **OK** button to store the changes temporarily in the administrator's login session.

The **ACD** dialog disappears.

- 12) Click the **Apply changes** button in the main window.

The settings are applied on the OpenScape Branch system.

4.13.2.2 How to Show the Status of ACD Agents

Proceed as follows to show the status of all ACD (Automatic Call Distribution) agents configured.

Prerequisites

Adequate administrative permissions.

The branch office of the OpenScape Branch type is configured and in operation.

The connection to the OpenScape Voice system is up.

The corresponding system components of the external ACD solution (e.g. OpenScape Contact Center or Genesys) are configured.

Step by Step

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

- 2) Select the **Branch Office list** in the Navigation Tree under Administration.

The system presents the **Branch Office Overview** in the Work Area with a current list of all branch offices.

- 3) To view a list of Branch Offices 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 branch office use one of the following options:
 - In the Work Area select the checkbox to the left of the particular branch office in the list and select **Manage**. Selecting the **Manage** button updates the **Branch Office** field, in the Navigation Tree, with the selected branch office and displays information and data in the Work Area for that branch office.
 - Choose a branch office from the **Branch Office** pull-down located in the Navigation Tree. Information and data are displayed in the Work Area.

- 5) Navigate to **Configuration > ACD** in the navigation tree under **Administration**.

The **ACD** window appears with the **General** tab selected by default.

- 6) Click the **Show** button in the **Agents Settings** field area.

The **Show agent status** dialog appears displaying a table with the following information for all agents configured:

- **ID** - ID number associated with the agent
- **Name** - Name of the agent
- **Status** - ACD status of the agent
- **Phone Number** - DN associated with the agent
- **Assigned Profile** - assigned to the agent

A filter is provided allowing filtering by **Name** or **Status** (Status: **logged On**, **logged Off**).

- 7) Click the **Close** button to go back to the **ACD** window.

The **Show agent status** dialog disappears.

4.13.2.3 How to Display the ACD Log Files

Proceed as follows to display the ACD (Automatic Call Distribution) Log files used for ACD statistics.

Prerequisites

Adequate administrative permissions.

The branch office of the OpenScape Branch type is configured and in operation.

The connection to the OpenScape Voice system is up.

The corresponding system components of the external ACD solution (e.g. OpenScape Contact Center or Genesys) are configured.

Step by Step

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

- 2) Select the **Branch Office list** in the Navigation Tree under Administration.

The system presents the **Branch Office Overview** in the Work Area with a current list of all branch offices.

- 3) To view a list of Branch Offices 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 branch office use one of the following options:

- In the Work Area select the checkbox to the left of the particular branch office in the list and select **Manage**. Selecting the **Manage** button updates the **Branch Office** field, in the Navigation Tree, with the selected

branch office and displays information and data in the Work Area for that branch office.

- Choose a branch office from the **Branch Office** pull-down located in the Navigation Tree. Information and data are displayed in the Work Area.

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

The **ACD** window appears with the **General** tab selected by default.

6) Click the **Go** button in the **Log file** field area.

The **IE Browser** dialog appears.

7) Click the **Open** or **Save** button to select and view a log file(s) or save the file(s) to another location.

8) Close the browser to go back to the **ACD** window.

The ACD log files are displayed or saved to a specified location for viewing.

4.13.2.4 How to Add, Edit, Delete Queues for ACD

Proceed as follows to add, edit or delete a backup ACD (Automatic Call Distribution) queue.

Prerequisites

Adequate administrative permissions.

The branch office of the OpenScape Branch type is configured as ACD proxy and in operation.

The connection to the OpenScape Voice system is up.

The corresponding system components of the external ACD solution (e.g. OpenScape Contact Center or Genesys) are configured.

Step by Step

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

The system presents the **Branch Office Overview** in the Work Area with a current list of all branch offices.

- 3) To view a list of Branch Offices 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 branch office use one of the following options:

- In the Work Area select the checkbox to the left of the particular branch office in the list and select **Manage**. Selecting the **Manage** button updates the **Branch Office** field, in the Navigation Tree, with the selected branch office and displays information and data in the Work Area for that branch office.

- Choose a branch office from the **Branch Office** pull-down located in the Navigation Tree. Information and data are displayed in the Work Area.
- 5) Navigate to **Configuration > ACD in the navigation tree under Administration**.
The **ACD** window appears with the **General** tab selected by default.
 - 6) Select the **Queue** tabsheet.
The queue list is displayed.
 - 7) To remove a queue from the list, select the respective list entry and click the **Delete** button.
The queue is removed from the list.
 - 8) The following options are available:
 - To add a new queue to the list click the **Add...** button.
 - To edit an existing queue from the list click the **Edit...** button.The **Add ACD Queue** or **Edit ACD Queue** window appears with the **General** tabsheet displayed by default.
 - 9) Proceed as follows to configure the general parameters of the ACD queue:
 - a) The internal number of the queue in the **ID** field is generated by the system (0 – 999). It is used for profile assignment and can not be configured.
 - b) Enter a queue name in the **Name** field. The name must be up to 30 alphanumeric characters (0-9, a-z, A-Z). This is a mandatory parameter.
 - c) Enter the overflow destination number in the **Destination (Overflow, Voice Mail)** field. The overflow destination is used for calls in the queue that exceeded the maximum waiting time or when the queue size exceeds the maximum number. In the case where Voice Mail is the overflow, enter the Voice Mail overflow destination number.
 - d) Select the **Overflow to Voice Mail Server** checkbox to specify that the calls will overflow to the Voice Mail server if no agent is free to receive a call.
 - e) Select the **Generate diversion header** checkbox to specify that when a call is forwarded to the Voice Mail server, a diversion header with the original dialed destination number, will be added and sent to the Voice Mail server.
 - f) Enter the time to advance the call to the next available agent position if the current ringing agent does not pick up the call in the **Queue advance time out** field. The timeout range is 10 to 120 seconds with a default value of 35 seconds. The queue timeout starts counting only after the join announcement ending.

NOTICE: If the agent timeout is elapsed before the queue advance timeout, this value will never be reached because the agent will be logged off automatically and the call will be advanced to the next available agent. The agent timeout value is configured branch wide in the **ACD** window in the **General** tabsheet.

- g) Enter the time to keep the agent unavailable after he/she hangs up on a call in the **Agent wrap up time** field. This time allows the agent to do post-call processing. The timer value is between 1 to 60 seconds with a default value of 5 seconds.

- h) Select the **Play ring tone instead of music on hold** checkbox to specify that the calls are receiving ringing tone instead of music on hold. This can be useful for queues for which the average holding time is very low. Default is to play ring tone instead of music.
- i) Select wave file for music on hold from the **Music on hold** selection list. This is enabled only when **Play ring tone instead of music on hold** is not selected.

NOTICE: The wave files available in the selection list can be configured branch wide in the **ACD** window in the **General** tabsheet.

- 10) Proceed as follows to configure the caller parameters of the ACD queue:
 - a) Enter the maximum time that a caller can be in a queue before being transferred to the overflow destination in the **Maximum waiting time** field. The time must be between 60 to 3600 seconds with a default value of 1200 seconds.
 - b) Enter the maximum number of calls that can be queued in the ACD queue in the **Callers max** field. When this value is reached, the call will be further treated by the overflow destination.
 - c) Select the **Unlimited** checkbox to indicate that there is no maximum caller limit and the maximum callers data is ignored.
- 11) Select the **DID** tabsheet to configure the DID (Direct Inward Dialing) numbers that need treatment by a backup ACD queue:
 - Enter the DID Directory Number and click the **Add** button to add a DID number to the list. There is no limit on the DID numbers, no DID can be associated with more than one queue and it can't be associated twice. During transition to normal mode, OpenScape Branch de-queues queued calls to OpenScape Voice using the same DID number that was used to dial the ACD group.
 - Checkmark the DID Directory Number(s) in the list and click the **Delete** button to remove a DID number(s) from the list.
- 12) Select the **Announcements** tabsheet to configure the announcements for the callers in the ACD queue:
 - a) **Queue join** announcement - This announcement is played when a call is entered in the queue after no available agent was found in desired backup ACD group. The announcement file is selected from uploaded announcement file list. The default is no announcement.
 - b) **Queue waiting** announcement - This announcement is periodically played to the caller. The announcement file is selected from uploaded announcement file list. The default is no announcement.
 - c) **Agent** announcement - This announcement is played to the agent before the call is connected. The announcement file is selected from uploaded announcement file list.
 - d) **Position/hold time announcement frequency** - This box defines (in seconds) how often the announcements of position and estimated hold time are played to the caller. The time must be between 10 to 600 seconds with a default value of 120 seconds.
 - e) **Announce position to caller** - When this check box is selected an announcement informing the position in queue is periodically played to the caller. The default is no announcement.

- f) **Announce estimated hold time to caller** - When this check box is selected an announcement informing the estimated hold time is periodically played to the caller. The default is no announcement.
 - g) **Announce hold time to agent** - When this check box is selected an announcement informing the time the caller has been waiting in the queue is played to the agent before the call is connected. The default is no announcement.
 - h) **Interval between queue join and queue waiting** announcements
- This box defines (in seconds) how often the queue waiting announcement is played to the caller after the queue join announcement. The time must be between 10 to 300 seconds with a default value of 60 seconds.
- 13) Click the **OK** button to go back to the **ACD** window.
- 14) Click the **OK** button to store the changes temporarily in the administrator's login session.
- The **ACD** dialog disappears.
- 15) Click the **Apply changes** button in the main window.

The settings for the backup ACD queues are applied on the OpenScape Branch system.

4.13.2.5 How to Display Agents Assigned to a Queue for ACD

Proceed as follows to display all agents assigned to a particular ACD (Automatic Call Distribution) queue.

Prerequisites

Adequate administrative permissions.

The branch office of the OpenScape Branch type is configured as ACD proxy and in operation.

The connection to the OpenScape Voice system is up.

The corresponding system components of the external ACD solution (e.g. OpenScape Contact Center or Genesys) are configured.

At least one ACD queue is configured and at least one agent is assigned to it.

Step by Step

- 1) Navigate to **Configuration tab > OpenScape Branch** within the Navigation Bar in the Common Management Platform.
- 2) Select the **Branch Office list** in the Navigation Tree under Administration.
The system presents the **Branch Office Overview** in the Work Area with a current list of all branch offices.
- 3) To view a list of Branch Offices 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 branch office use one of the following options:
 - In the Work Area select the checkbox to the left of the particular branch office in the list and select **Manage**. Selecting the **Manage** button updates the **Branch Office** field, in the Navigation Tree, with the selected branch office and displays information and data in the Work Area for that branch office.
 - Choose a branch office from the **Branch Office** pull-down located in the Navigation Tree. Information and data are displayed in the Work Area.
- 5) Navigate to **Configuration > ACD in the navigation tree under Administration**.
The **ACD** window appears with the **General** tab selected by default.
- 6) Select the **Queue** tabsheet.
The queue list is displayed.
- 7) To display the Identification numbers of agents assigned to a particular queue in the list, click the respective **show** link in the **Assigned Agent IDs** column.
The **Assigned Agent Ids** dialog appears displaying the Ids of the assigned agents for the selected queue.
A filter is provided allowing filtering by **Name** or **DID**.
- 8) Click the **Close** button to go back to the **ACD** window.

4.13.2.6 How to Add, Edit, Delete Profiles for ACD

Proceed as follows to add, edit or delete an ACD (Automatic Call Distribution) profile.

Prerequisites

Adequate administrative permissions.

The branch office of the OpenScape Branch type is configured as ACD proxy and in operation.

The connection to the OpenScape Voice system is up.

The corresponding system components of the external ACD solution (e.g. OpenScape Contact Center or Genesys) are configured.

At least one ACD queue is configured in the OpenScape Branch system.

Step by Step

- 1) Navigate to **Configuration tab > OpenScape Branch** within the Navigation Bar in the Common Management Platform.
- 2) Select the **Branch Office list** in the Navigation Tree under Administration.
The system presents the **Branch Office Overview** in the Work Area with a current list of all branch offices.

- 3) To view a list of Branch Offices 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 branch office use one of the following options:
 - In the Work Area select the checkbox to the left of the particular branch office in the list and select **Manage**. Selecting the **Manage** button updates the **Branch Office** field, in the Navigation Tree, with the selected branch office and displays information and data in the Work Area for that branch office.
 - Choose a branch office from the **Branch Office** pull-down located in the Navigation Tree. Information and data are displayed in the Work Area.

- 5) Navigate to **Configuration > ACD in the navigation tree under Administration**.

The **ACD** window appears with the **General** tab selected by default.

- 6) Select the **Profiles** tabsheet.

The profiles list with the **Name** column and **Assigned Queue IDs** column is displayed.

A filter is provided allowing filtering by **Name**.

- 7) To remove a profile from the list, select the respective list entry and click the **Delete** button.

The profile is removed from the list.

- 8) The following options are available:
 - To add a new profile to the list click the **Add...** button. A maximum number of 100 profiles is allowed. The **Add...** button is disabled when this limit is reached.
 - To edit an existing profile from the list click the **Edit...** button.

The **Add Profile** or **Edit Profile** window appears.

- 9) Enter or modify the profile name in the **Name** field.
- 10) Enter or modify the identification numbers of the queues assigned to the current profile in the **Assigned Queue IDs** field. To assign more than one queue ID to the same profile, enter the IDs separated by commas.
- 11) Click the **OK** button to go back to the **ACD** window.
- 12) Click the **OK** button to store the changes temporarily in the administrator's login session.

The **ACD** dialog disappears.

- 13) Click the **Apply changes** button in the main window.

The settings for the ACD profiles are applied on the OpenScape Branch system.

4.13.2.7 How to Add, Edit, Delete Agents for ACD

Proceed as follows to add, edit or delete an ACD (Automatic Call Distribution) agent.

Prerequisites

Adequate administrative permissions.

The branch office of the OpenScape Branch type is configured as ACD proxy and in operation.

The connection to the OpenScape Voice system is up.

The corresponding system components of the external ACD solution (e.g. OpenScape Contact Center or Genesys) are configured.

At least one ACD profile is configured in the OpenScape Branch system.

Step by Step

- 1) Navigate to **Configuration tab > OpenScape Branch** within the Navigation Bar in the Common Management Platform.
- 2) Select the **Branch Office list** in the Navigation Tree under Administration.
The system presents the **Branch Office Overview** in the Work Area with a current list of all branch offices.
- 3) To view a list of Branch Offices 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 branch office use one of the following options:
 - In the Work Area select the checkbox to the left of the particular branch office in the list and select **Manage**. Selecting the **Manage** button updates the **Branch Office** field, in the Navigation Tree, with the selected branch office and displays information and data in the Work Area for that branch office.
 - Choose a branch office from the **Branch Office** pull-down located in the Navigation Tree. Information and data are displayed in the Work Area.
- 5) Navigate to **Configuration > ACD in the navigation tree under Administration**.
The **ACD** window appears with the **General** tab selected by default.
- 6) Select the **Agents** tabsheet.
The agents list with the **Id** column, the **Name** column and **Assigned Profile** column is displayed.
A filter is provided allowing filtering by **Name** or **Profile Name**.
- 7) To remove an agent from the list, select the respective list entry and click the **Delete** button.

- 8) The following options are available:
- To add a new agent to the list click the **Add...** button.
 - To edit an existing agent from the list click the **Edit...** button.

The **Configure Agent** window appears.

- 9) Enter or modify the agent's identification number name in the **ID** field. The ID number is used in logon/logoff procedures. The ID can not be duplicated. Only numerical values are allowed.

NOTICE:

The Business Group Line (BGL) Number must be configured as the ID, if the Keyset Toggle Key is used.

- 10) Enter or modify the name of the agent to identify the person in the **Name** field.
- 11) Enter or modify the agent's password which will be used in logon/logoff procedures in the **Password** field. Only numerical values are allowed.
- 12) Repeat the agent's password in the **Confirm password** field.
- 13) Select a profile from the **Profile** selection list.
- 14) Click the **OK** button to go back to the **ACD** window.
- 15) Click the **OK** button to store the changes temporarily in the administrator's login session.

The **ACD** dialog disappears.

- 16) Click the **Apply changes** button in the main window.

The settings for the ACD agents are applied on the OpenScape Branch system.

4.14 OpenScape Voice Call Recording Solution Based on SIPREC — Overview

SIPREC defines an SIP client (UAC) - SIP server (UAS) interface used to establish a Recording Session (RS) to record a SIP multimedia Communication Session (CS) between two SIP peers.

The SIPREC architecture identifies key roles for the SIPREC UAC as a SIPREC client (SRC) and SIPREC UAS as a SIPREC server (SRS). The SRC establishes an RS with the SRS whenever a multimedia CS is to be recorded. The RS is established as a typical multimedia session.

The SIPREC based OpenScape Voice Call Recording solution offers an OpenScape Voice VoIP (Voice over IP) recording solution for calls passing through a remote OpenScape Branch. This solution is a hybrid one as each solution component provides a contribution in the overall call recording solution.

The OpenScape Voice Call Recording solution based on SIPREC is introduced in order to overcome the loss of recorded speech with CSTA based recording solution, that exists in case of network delays.

In this solution OpenScape Branch operates in two modes: **Normal Mode (NM)** and **Survivability Mode (SM)**.

In NM, OpenScape Branch as an SRC is able to communicate with the OpenScape Voice server. OpenScape Voice is in control of the SIPREC interface, determining on a call by call basis which SIP CS must be recorded. When OpenScape Voice determines a SIP CS is to be recorded, OpenScape Voice injects proprietary SIP signaling information to the OpenScape Branch-SRC.

In SM, OpenScape Branch has lost connectivity with OpenScape Voice or is entering NM, coming out of SM with existing calls being recorded, call recording continues. So, while OpenScape Branch is in SM mode, the OpenScape Branch-SRC establishes an RS with the SRS for each call establishing a SIP CS.

OpenScape Branch has two SRC capable configurations: **Proxy** and **Proxy-SBC**.

Recording is only supported for SIP endpoints managed via the OpenScape Branch, as OpenScape Branch must be involved in the call for recording to take place.

NOTICE:

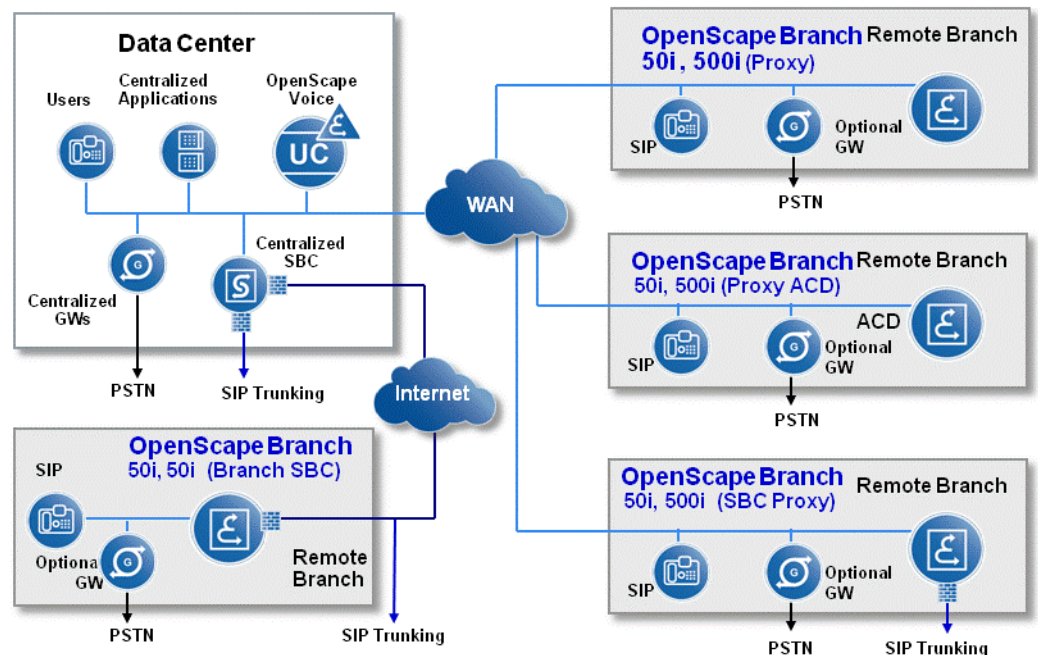
SIPREC based OpenScape Voice Call Recording solution does not use the OpenScape Media Server as a conference bridge to support the media stream breakout to the recorder.

The recording solution provides configuration options through IP or FQDN. However, it does not support load balancing or redundancy of SIP recording, even when used with a DNS server. This limitation should be considered when designing the system architecture to ensure reliability and scalability.

4.15 Integrated Gateways — Overview

The Integrated Gateways configuration applies to OpenScape Branch systems of the OpenScape Branch 50i type for V1R3 and later versions and to OpenScape Branch 500i for V2 and later.

Application Scenario Example



Description

The OpenScape Branch 50i appliance for up to 80 registered lines and with Integrated Gateway and Analog Adapter is currently available:

OpenScape Branch servers With Integrated Gateway and Analog Adapters

- **OpenScape Branch 50i** – (Advantech SYS-2USM02-6M01E server) supports up to 80 registered lines with Integrated Gateway and Analog Adapter interfaces. The following combinations of integrated gateways and analog adapters are supported:
 - OpenScape Branch 50i **A84** (Analog - 8 ports FXO (Foreign eXchange Office) + 4 ports FXS (Foreign eXchange Station))
 - OpenScape Branch 50i **D44** (Digital - 4 ports BRI + 4 ports FXS)
 - OpenScape Branch 50i **DP14E** (Digital - 1 PRI E1 + 4 ports FXS)
 - OpenScape Branch 50i **DP14T** (Digital - 1 PRI T1 + 4 ports FXS)
 - OpenScape Branch 50i **DP24** (Digital - 2 PRIs/CAS E1 - FXS or 2 PRIs/CAS T1 - FXS)
- **OpenScape Branch 50i** – (Advantech SYS-2USM01-6M01E server) for up to 80 registered lines. This server is longer in size when compared to the

Advantech SYS-2USM02-6M01E. This server supports higher density of Integrated Analog Adapter interfaces and is available in two flavors:

- OpenScape Branch 50i **A024** (Analog - **24** ports FXS)
- OpenScape Branch 50i **A048** (Analog - **48** ports FXS)

OpenScape Branch servers With Integrated PRI Gateway only

- **OpenScape Branch 500i** – (Advantech SYS-2USM03-6M01E server) supports up to 500 registered lines with Integrated PRI Gateway interfaces. The following combinations of integrated gateways are supported:
 - OpenScape Branch 500i **DP4** (Digital - **4** PRI E1/T1)
 - OpenScape Branch 500i **DP8** (Digital - **8** PRI E1/T1)

QoS (Quality of Service)

QoS parameters can be reported based on one of the following two criteria:

- On threshold crossing (e.g. packet loss > 1%, Jitter > 2%, etc).
- Quality data Collection of each call session.

The following parameters are reported: jitter, packet loss and average round trip delay. Several parameters can be configured to facilitate a QoS monitoring.

Media Configuration

Media configuration allows for the following (supported in OpenScape Version 2):

- Media protocol selection e.g., RTP, SRTP-best effort.
- Key exchange method i.e. SDES and MIKEY.
- Setting media security

Codec Configuration

Codec configuration allows for the following (supported in OpenScape Version 2):

- Codec selection.
- Codec selection priority.

Restrictions

HiPath 3000 and or HiPath 4000 systems shall not be in the same branch as an OSB 50i system.

The OpenScape Branch appliance may not operate in Proxy ACD mode.

ISDN Supplementary Services are not be supported.

Endpoint Service Profiles

Endpoint Service Profiles provides the ability to configure integrated gateways FXS associated parameters in the OpenScape Branch 50i and for the Proxy ATA.

4.15.1 How to Configure General Settings for an Integrated Gateway

Proceed as follows to configure the general settings of an integrated gateway of an OpenScape Branch 50i or 500i system.

Prerequisites

Adequate administrative permissions.

The system is of the OpenScape Branch 50i or 500i type and in operation.

The connection to the OpenScape Voice system is up.

Step by Step

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

2) Select the **Branch Office list** in the Navigation Tree under Administration.

The system presents the **Branch Office Overview** in the Work Area with a current list of all branch offices.

3) To view a list of Branch Offices 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 branch office use one of the following options:

- In the Work Area select the checkbox to the left of the particular branch office in the list and select **Manage**. Selecting the **Manage** button updates the **Branch Office** field, in the Navigation Tree, with the selected branch office and displays information and data in the Work Area for that branch office.
- Choose a branch office from the **Branch Office** pull-down located in the Navigation Tree. Information and data are displayed in the Work Area.

5) Navigate to **Configuration > Features > Integrated Gateways** in the navigation tree under **Administration**.

The **Integrated Gateway Configuration** window appears with the **General** tab selected by default.

In the **Gateway configuration** field area the **Card 1** and **Card 2** fields show the interface configuration or the OpenScape Branch 50i or 500i system for one or more of the following: FXS (Foreign eXchange Station), FXO (Foreign eXchange Office), BRI (Basic Rate Interface) or PRI (Primary Rate Interface).

In the **Gateway configuration** field area the **Per-card clock source** checkbox is checked and is read-only, if only one PRI (Primary Rate Interface) card is installed for the OpenScape 500i. If two PRI cards are installed for the OpenScape 500i, the checkbox by default is not checked and it is possible to configure the PRI clock source individually per port or used a "Combined clock source".

6) To activate the integrated gateway, click the **Enable** checkbox, in the general work area.

- 7) Select the country of the location of the OpenScape Branch system in the **Country** field. To view the country specific parameters, click the **Country Configuration Info...** button.

The **Country Configuration Info** window appears displaying the default settings of the hookflash timers, ring cadence and tone frequency.

- 8) Click the **OK** button to store the settings temporarily.

The **Integrated Gateway Configuration** window is closed.

- 9) Click the **Apply changes** button in the main window.

The general integrated gateway configuration of the OpenScape Branch 50i system has been finished.

4.15.2 How to Configure QoS Monitoring for an Integrated Gateway

Proceed as follows to configure the settings for QoS (Quality of Service) monitoring of an integrated gateway of an OpenScape Branch 50i or 500i system.

Prerequisites

Adequate administrative permissions.

The system is of the OpenScape Branch 50i or 500i type and in operation.

The connection to the OpenScape Voice system is up.

The integrated gateway is configured.

Step by Step

- 1) Navigate to **Configuration tab > OpenScape Branch** within the Navigation Bar in the Common Management Platform.
- 2) Select the **Branch Office list** in the Navigation Tree under Administration.
The system presents the **Branch Office Overview** in the Work Area with a current list of all branch offices.
- 3) To view a list of Branch Offices 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 branch office use one of the following options:
 - In the Work Area select the checkbox to the left of the particular branch office in the list and select **Manage**. Selecting the **Manage** button updates the **Branch Office** field, in the Navigation Tree, with the selected branch office and displays information and data in the Work Area for that branch office.
 - Choose a branch office from the **Branch Office** pull-down located in the Navigation Tree. Information and data are displayed in the Work Area.

- 5) Navigate to **Configuration > Features > Integrated Gateways** in the navigation tree under **Administration**.

The **Integrated Gateway Configuration** window appears with the **General** tab selected by default.

- 6) Select the **QoS Monitoring** tabsheet.
- 7) To activate the QoS monitoring, click the **Enable QoS Monitoring** checkbox.
- 8) To activate the transmission of traps to QCU (Quality Control Unit), click the **Send Traps** checkbox.
- 9) Enter the IP address and port number of the Quality Control Unit in the **QCU IP Address** and **QCU Port** fields.
- 10) Select the QoS reporting mechanism in the **Reporting mechanism** selection list. Possible values are **Threshold crossing** or **Collection of each call session**. If Threshold crossing has been selected, the following thresholds can be changed from its default values:
 - a) **Maximum jitter threshold**: Threshold for maximum jitter in the RTP stream. The default value is 20 ms
 - b) **Average Round trip delay threshold**: Threshold for maximum round trip delay in the RTP stream. The default is 100 ms.
 - c) **Lost packets threshold compressing**: Threshold for count of lost packets in RTP stream for compressed codecs. The default value is 10 (1%).
 - d) **Lost packets threshold not compressing**: Threshold for count of lost packets in RTP steam for non-compressed codecs. The default value is 10 (1%).
- 11) Click the **OK** button to store the settings temporarily.

The **Integrated Gateway Configuration** window is closed.
- 12) Click the **Apply changes** button in the main window.

The general QoS monitoring configuration of the OpenScape Branch 50i system has been finished.

4.15.3 How to Configure Media for an Integrated Gateway

Proceed as follows to configure the settings for Media of an integrated gateway of an OpenScape Branch system.

Prerequisites

Adequate administrative permissions.

The system is of the OpenScape Branch type and in operation.

The connection to the OpenScape Voice system is up.

The integrated gateway is configured.

Step by Step

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

- 2) Select the **Branch Office list** in the Navigation Tree under Administration.
The system presents the **Branch Office Overview** in the Work Area with a current list of all branch offices.

- 3) To view a list of Branch Offices 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 branch office use one of the following options:
 - In the Work Area select the checkbox to the left of the particular branch office in the list and select **Manage**. Selecting the **Manage** button updates the **Branch Office** field, in the Navigation Tree, with the selected branch office and displays information and data in the Work Area for that branch office.
 - Choose a branch office from the **Branch Office** pull-down located in the Navigation Tree. Information and data are displayed in the Work Area.

- 5) Navigate to **Configuration > Features > Integrated Gateways** in the navigation tree under **Administration**.

The **Integrated Gateway Configuration** window appears with the **General** tab selected by default.

- 6) Select the **Media** tabsheet and configure media as follows.
- 7) Select the media protocol in the **Media protocol** list field, in the Media field area (in the Media tab). Options are **STRP - Best effort** and **RTP**

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 no selection is possible. The entry should be "none".

- 8) Select the Key exchange method in the **Key Exchange Method** list field. Values: **SDES**, **MIKEY**, **None**. Select **None** if this method does not apply.
- 9) Checkmark the **Mark SRTP call leg as secure for FXS** checkbox, if the secure media is negotiated for an FXS subscriber, the call will be indicated as secure.

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

- 10) Click the **OK** button to store the settings temporarily.

The **Integrated Gateway Configuration** window is closed.

- 11) Click the **Apply changes** button in the main window.

The general QoS monitoring configuration of the OpenScape Branch 50i system has been finished.

4.15.4 How to Configure Codecs for an Integrated Gateway

Proceed as follows to add codecs and configure codec selection for an integrated gateway of an OpenScape Branch system.

Prerequisites

Adequate administrative permissions.

The system is of the OpenScape Branch type and in operation.

The connection to the OpenScape Voice system is up.

The integrated gateway is configured.

Step by Step

- 1) Navigate to **Configuration tab > OpenScape Branch** within the Navigation Bar in the Common Management Platform.
- 2) Select the **Branch Office list** in the Navigation Tree under Administration.
The system presents the **Branch Office Overview** in the Work Area with a current list of all branch offices.
- 3) To view a list of Branch Offices 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 branch office use one of the following options:
 - In the Work Area select the checkbox to the left of the particular branch office in the list and select **Manage**. Selecting the **Manage** button updates the **Branch Office** field, in the Navigation Tree, with the selected branch office and displays information and data in the Work Area for that branch office.
 - Choose a branch office from the **Branch Office** pull-down located in the Navigation Tree. Information and data are displayed in the Work Area.
- 5) Navigate to **Configuration > Features > Integrated Gateways** in the navigation tree under **Administration**.
The **Integrated Gateway Configuration** window appears with the **General** tab selected by default.
- 6) Select the **Codecs** tabsheet.
The codec priority list is displayed and contains the priority of each supported codec on the codec negotiation. The same codec can not be set to different priorities.
- 7) To add a codec:
 - a) Select a codec from the **Select codec** selection list. Possible values: G711U, G711A, G729, G722, G7221 24K bitrate, G7221 32K bitrate, iLBC, iSAC, "empty string".
 - b) Click the **Add** button and assign the codec to a priority.

The selected codec is added to the list of codecs that can be used.

- 8) To arrange the priority that codecs are selected:
 - a) Select a codec by placing a checkmark in the checkbox associated with the codec to be moved.
The **Move up**, **Move down** and **Delete** buttons are activated.
 - b) Click the **Move up** or **Move down** button to moved the selected codec in the priority list.
The selection priority for the codec is adjusted and re-displayed in the codec priority list.
- 9) To delete codecs from the codecs priority list:
 - a) Select one or more codecs by placing a checkmark in the checkbox associated with the codec to be deleted.
The **Delete** button is activated.
 - b) Click the **Delete** to remove the selected codec(s) in the priority list.
The selection priority for the remaining codecs is adjusted and re-displayed in the codec priority list.
- 10) Click the **OK** button to store the settings temporarily.
The **Integrated Gateway Configuration** window is closed.
- 11) Click the **Apply changes** button in the main window.

The general QoS monitoring configuration of the OpenScape Branch 50i system has been finished.

4.15.5 How to Configure the FXS Card of an Integrated Gateway

Proceed as follows to configure the FXS (Foreign eXchange Station) card of an integrated gateway of an OpenScape Branch 50i system.

Prerequisites

Adequate administrative permissions.

The connection to the OpenScape Voice system is up.

The system is of the OpenScape Branch 50i type and in operation.

The system is equipped with a FXS card.

Step by Step

- 1) Navigate to **Configuration tab > OpenScape Branch** within the Navigation Bar in the Common Management Platform.
- 2) Select the **Branch Office list** in the Navigation Tree under Administration.
The system presents the **Branch Office Overview** in the Work Area with a current list of all branch offices.
- 3) To view a list of Branch Offices 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 branch office use one of the following options:
 - In the Work Area select the checkbox to the left of the particular branch office in the list and select **Manage**. Selecting the **Manage** button updates the **Branch Office** field, in the Navigation Tree, with the selected branch office and displays information and data in the Work Area for that branch office.
 - Choose a branch office from the **Branch Office** pull-down located in the Navigation Tree. Information and data are displayed in the Work Area.
- 5) Navigate to **Configuration > Features > Integrated Gateways** in the navigation tree under **Administration**.

The **Integrated Gateway Configuration** window appears with the **General** tab selected by default.

In the **Gateway configuration** field area the **Card 1** and **Card 2** fields show the interface configuration or the OpenScape Branch 50i system FXS, FXO (Foreign eXchange Office), BRI (Basic Rate Interface) or PRI (Primary Rate Interface (V1R4).

- 6) Click the **Configure** button associated with the FXS card in the **Gateway configuration** field area.

The **FXS List** window appears displaying the settings of each port of the interface.

- 7) Select the **Card configuration** tabsheet to configure ringing, hookflash and loop current for the gateway card.

NOTICE:

The **Card Configuration** work area appears.

- 8) Select the loop current (in mA) for the FXS card from the **Loop Current** selection list (Values: 20, 23, 26, 29, 32, 35, 38, 41, default: 20mA)

IMPORTANT: Modifying this parameter will cause existing calls to be lost when applying changes.

- 9) Select the **Manual ring settings** checkbox to enable setting of the Ring Frequency and ring Voltage for the FXS card.

IMPORTANT: Modifying these parameters will cause existing calls to be lost when applying changes.

- a) Select the Ring Frequency for the FXS card from the **Ring Frequency** selection list (Values: 20, 25, 50, default 20).
- b) Select the ring voltage (in volts) for the FXS card from the **Ring Voltage** selection list (Values: 50, 75, 89, default 75).

- 10) Select the **Hook flash** checkbox to enable voice features that require a hook flash to initiate. This feature is supported in OpenScape Branch V1R4 and later releases. Examples of features supported via hookflash are:
- Call Hold
 - Call Return - Activate
 - Call Waiting
 - Caller ID on Call Waiting
 - Disable Caller ID for Next Call
 - Do Not Disturb - Activate/Deactivate
 - Three-way calling
- a) Select the hookflash duration from the **Hook flash duration** selection list. Hook flash duration is either **Long** (1250 ms.) or **Short** (200 ms.). A hookflash that exceeds the configured value will be considered a disconnect. This feature is supported in OpenScape Branch V1R4 and later releases.
- 11) Three **Spare flags** are supported for custom requirements and future use.
- 12) To enable and disable all FXS ports and control echo cancellation for all ports initiate the following in the **Port Configuration** work area:
- a) Select the **Enable All** button, for the **All ports** field to enable all FXS ports. Only ports with a valid DN will be enabled. Select the **Disable All** button to disable all FXS ports. Only ports that are enabled shall be disabled.
- The **Enabled** column in the list of ports is updated to reflect enabling or disabling echo cancellation.
- b) Select the **Enable All** button, for the **Echo cancellation** field to enable echo cancellation for all FXS ports, or select the **Disable All** button to disable echo cancellation for all FXS ports.
- The **Echo cancellation** column in the list of ports is updated to reflect enabling or disabling echo cancellation.
- c) Click the **OK** button to store the settings temporarily.
- The **FXS List** window is closed and the **Integrated Gateway Configuration** window appears.
- d) Click the **OK** button to store the settings temporarily.
- The **Integrated Gateway Configuration** window is closed.
- e) Click the **Apply Changes** button in the main window to store the settings.
- 13) To edit a single port configuration, check the respective checkbox and click the **Edit...** button, in the Port Configuration work area.
- The **Edit - FXS List** dialog appears with the **General** tab displayed by default.

14) In the Edit - FXS dialog General Tab:

This tab contains Subscriber information, receive and transmit values and fax configuration.

- a) Enable or disable the physical port with the **Enable** checkbox.
- b) The FXS port number is displayed in the **Physical Port** field.
- c) Enter or change the subscriber's directory number in the **Subscriber number** field (Value: up to 26 digits). This is a mandatory field. Note: The directory numbers shall not be duplicated for different FXS ports.
- d) Enter the subscriber's name used in the display on the device in the **Subscriber name** field (Value: up to 30 characters). This is a mandatory field.
- e) Enter the **Registration interval timer** in seconds (Value: 30 - 7200 seconds, default 3600 seconds).
- f) Enable or disable echo cancellation with the **Echo cancellation** checkbox.
- g) Enter the receive gain value in decibel in the **Receive Gain** field (Value: -30 dB - +20 dB, default 0 dB). This is a mandatory field. A negative value decreases the gain, a positive value increases the gain.
- h) Enter the transmit gain value in decibel in the **Transmit Gain** field (Value: -30 dB - +20 dB, default 0 dB). This is a mandatory field. A negative value decreases the gain, a positive value increases the gain.
- i) Three **Spare flags** are supported for customer requirements and future use.
- j) To activate the T.38 fax standard for the integrated gateway, check the **Enable Fax T.38** checkbox.
- k) To activate the detection of CNG (Fax Calling Tone), check the **Enable CNG Detection** checkbox.
- l) To activate the FXS Hoot Line functionality, check the **Enable FXS Hoot Line** checkbox.
- m) To activate the Hotline/Warmline functionality, check the **Enable Hotline/Warmline** checkbox. When the user clicks on the edit FXS Port Configuration table, the following fields are displayed on the new Hotline/Warmline section header:

Enable- This checkbox is used to enable the Hotline or Warmline feature. The default setting is unchecked. A new text entry field is labeled Wait time (Sec). This field is used to enter a delay time in whole seconds. The default value is zero. Permissible values are 0-30. Recommended value is set at 2 seconds or even a single second. This field is disabled when the Enable checkbox is unchecked. This field must contain a permissible value when the Enable checkbox is checked. When this field is set to 0, Hotline behavior is assumed. When set to a non-zero value, Warmline behavior is assumed.

Destination - This field is used to store the hotline or the Warmline destination number. It can contain up to 24 digits using 0 - 9. It is disabled when the Enable checkbox is unchecked. This field must contain a permissible value when the Enable checkbox is checked.

Number of time to repeat - This field indicates how many times to retry an external hotline/warmline destination in the event that it is busy. Permissible values are integers between 0 and 30. Default value is zero. This field is disabled when the Enable checkbox is unchecked.

It must contain a permissible value when the Enable checkbox is checked.

Repeat Interval (Seconds) - This field indicates in whole seconds the time between retries and the time until the first retry. Permissible values are 1 to 30. Default value is 5. This field is disabled when the Enable checkbox is unchecked. It must contain a permissible value when the Number of times to repeat is greater than zero.

- n) To activate this port for Fax check the **Fax device** checkbox. Enabling this option will restrict a call waiting call from camping on to this FXS line.
- o) Select the Endpoint service profile, from the **Endpoint service profile** field selection list, used to restrict dialing destinations from the FXS line (V7R1). The Endpoint service profile contains dialing pattern blocking restrictions, as well as, operational modes (Survivable and Both) for FXS operation.

15) Select the Digest Authentication tab.

The **Digest Authentication** work area appears.

16) In the Edit - FXS dialog Digest Authentication Tab:

- a) Enter or change the realm for the selected port in the **Realm** field (Value: 0-128 characters). The realm must be unique for each port. This is a mandatory field if digest authentication is used on OpenScape Voice.
- b) Enter or change the user ID for the selected port in the **User ID** field (Value: 6-64 characters). This is a mandatory field if digest authentication is used on OpenScape Voice.
- c) Enter or change the password for the selected port in the **Password** field (Value: 6-20 characters). The password for the post must be the same as the password for the OpenScape voice subscriber. This is a mandatory field if digest authentication is used on OpenScape Voice.

17) Click the OK button to store the settings temporarily.

The **Edit - FXS** window is closed and the **Integrated Gateway Configuration** window appears.

18) Click the OK button to store the settings temporarily.

The **Integrated Gateway Configuration** window is closed.

19) Click the Apply Changes button in the main window.

The FXS interface is configured.

NOTICE:

End of Dial - In OpenScape Branch V1R4 and later releases, it is possible for a subscriber to dial the '#' digit at the end of the dialing sequence. This digit will be interpreted as the end of dialing and digit translation will begin immediately. The addition of this capability reduces the time that a subscriber currently needs to wait for the end of dialing timeout to expire. If the '#' digit is the first digit, it will not be treated as end of dialing. There is no configuration for this capability.

4.15.6 How to Configure the FXO Card of an Integrated Gateway

Proceed as follows to configure the FXO (Foreign eXchange Office) card of an integrated gateway of an OpenScape Branch 50i system.

Prerequisites

Adequate administrative permissions.

The connection to the OpenScape Voice system is up.

The system is of the OpenScape Branch 50i type and in operation.

The system is equipped with a FXO card.

Step by Step

- 1) Navigate to **Configuration tab > OpenScape Branch** within the Navigation Bar in the Common Management Platform.
- 2) Select the **Branch Office list** in the Navigation Tree under Administration.
The system presents the **Branch Office Overview** in the Work Area with a current list of all branch offices.
- 3) To view a list of Branch Offices 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 branch office use one of the following options:
 - In the Work Area select the checkbox to the left of the particular branch office in the list and select **Manage**. Selecting the **Manage** button updates the **Branch Office** field, in the Navigation Tree, with the selected branch office and displays information and data in the Work Area for that branch office.
 - Choose a branch office from the **Branch Office** pull-down located in the Navigation Tree. Information and data are displayed in the Work Area.
- 5) Navigate to **Configuration > Features > Integrated Gateways** in the navigation tree under **Administration**.

The **Integrated Gateway Configuration** window appears with the **General** tab selected by default.

In the **Gateway configuration** field area the **Card 1** and **Card 2** fields show the interface configuration or the OpenScape Branch 50i system FXS (Foreign eXchange Station), FXO or BRI (Basic Rate Interface).

The **Disable FXO Audit** flag manages to disable the 12 hours audit for all FXO ports. In the OSB, all FXO calls have by default an audit that disconnect the call after 12 hours. This checkbox changes this behavior and if enabled, the call is not disconnected.

- 6) Click the **Configure** button associated with the FXO card in the **Gateway configuration** field area.

The **FXO List** window appears displaying Fax information and the settings of each port of the interface.

- 7) To configure T.38 fax standard, the following checkboxes are available in the FAX t.38 work area:
 - a) To activate the T.38 fax standard for the integrated gateway, check the **Enable Fax T.38** checkbox.
 - b) To activate the detection of CNG (Fax Calling Tone), check the **Enable CNG Detection** checkbox.
- 8) To edit a port configuration, check the respective checkbox and click the **Edit** button. The **Port Configuration** dialog appears.

The **Port Configuration** dialog appears, with the **General** tab selected by default.

- 9) In the **Port Configuration** dialog, perform the following steps in the General tabsheet:
 - a) Enable or disable the physical port with the **Enable** checkbox.
 - b) The physical port is displayed.
 - c) The signaling mode is set to **Loop Start** by default and can not be changed.
 - d) Enable/disable the detection of answer and disconnection via silent reversal with the **Answer by polarity reversal** and **Disconnect by polarity reversal** checkboxes.
 - e) If both, the **Answer by polarity reversal** and **Disconnect by polarity reversal** checkboxes are enabled: Enter the minimum time interval between the answer polarity switch and hang up polarity switch in the **Polarity reversal delay hang up** field.
 - f) Enable the **Loop Supervision** checkbox to change the signaling mode to Kewlstart, which is a variation of the loop start signaling mode.
 - g) Enable or disable echo cancellation with the **Echo cancellation** checkbox.
 - h) Enter the receive gain value in decibel in the **Receive Gain** field. The default value is 0 db. This is a mandatory field.
 - i) Enter the transmit gain value in decibel in the **Transmit Gain** field. The default value is 0 db. This is a mandatory field.
 - j) Enter the **Ring detection timeout** value in seconds. Devices must have a timeout to determine if there was a hang up before the line was answered.
 - k) The integrated gateway is able to detect busy tone: Check the **Busy Detect Disconnect** checkbox to enable the Busy tone detection.
 - l) If busy tone detection is enabled, enter how many tone cycles the system shall wait before disconnecting the call in the **Minimum busy detect count** field.
 - m) Enter a default destination number in the **Default destination DN** field.
- 10) Analog trunks are able to provide the Calling Party information via some specific protocols which depend on the country. Select the **CID tabsheet** and continue with the configuration of the CID (Caller ID) settings:
 - a) Enable the Caller ID functionality with the **Enable** checkbox.
 - b) Select the Caller ID Signaling protocol in the **CID signaling** field. The possible values are: **Bell202 US**, **DTMF**, **V23 UK** and **V23 Japan**.
 - c) Select the indication of the start of caller ID in the **CID start** selection list. Possible values: **Ring**, **Polarity reversal**, **Polarity India** (Polarity Reversal for India) and **DTMF Before Ring**.
 - d) Enter the **Pre Answer delay for CID**. A delay in Dial Plan is added before the call is answered for FXO. This is an integer value and required, if caller ID is enabled.

- 11) Click the **OK** button to return to the **FXO** window.

The **Port Configuration** dialog is closed and the configuration is displayed in the FXO list.

- 12) Click the **OK** button to store the settings temporarily.

The **Integrated Gateway Configuration** window is closed.

- 13) Click the **Apply changes** button in the main window.

The FXO card of the integrated gateway of an OpenScape Branch 50i system is configured.

4.15.7 How to Configure the BRI/S0 Card of an Integrated Gateway

Proceed as follows to configure the BRI (Basic Rate Interface) card of an integrated gateway of an OpenScape Branch 50i system.

Prerequisites

Adequate administrative permissions.

The connection to the OpenScape Voice system is up.

The system is of the OpenScape Branch 50i type and in operation.

The system is equipped with a BRI card.

Step by Step

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

The system presents the **Branch Office Overview** in the Work Area with a current list of all branch offices.
- 3) To view a list of Branch Offices 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 branch office use one of the following options:
 - In the Work Area select the checkbox to the left of the particular branch office in the list and select **Manage**. Selecting the **Manage** button updates the **Branch Office** field, in the Navigation Tree, with the selected branch office and displays information and data in the Work Area for that branch office.
 - Choose a branch office from the **Branch Office** pull-down located in the Navigation Tree. Information and data are displayed in the Work Area.

- 5) Navigate to **Configuration > Features > Integrated Gateways** in the navigation tree under **Administration**.

The **Integrated Gateway Configuration** window appears with the **General** tab selected by default.

In the **Gateway configuration** field area the **Card 1** and **Card 2** fields show the interface configuration or the OpenScape Branch 50i system FXS, FXO (Foreign eXchange Office), BRI (Basic Rate Interface) or PRI (Primary Rate Interface (V1R4)).

- 6) Click the **Configure** button associated with the BRI interface in the **Gateway configuration** field area.

The **BRI** window appears displaying Fax information and the settings of each port in a list on the **Port Configuration** tab.

- 7) To configure T.38 fax standard, the following checkboxes are available in the FAX t.38 work area:
 - a) To activate the T.38 fax standard for the integrated gateway, check the **Enable Fax T.38** checkbox.
 - b) To activate the detection of CNG (Fax Calling Tone), check the **Enable CNG Detection** checkbox.
- 8) To edit a port configuration, check the respective checkbox and click the **Edit** button. The **Edit - BRI** dialog appears
- 9) In the **Edit - BRI** dialog, perform the following steps:
 - a) Enable or disable the physical port with the **Enable** checkbox.
 - b) The physical port is displayed in the **Physical Port** field.
 - c) Enable or disable echo cancellation with the **Echo cancellation** checkbox.
 - d) Enter the **Clock source priority**. The priorities must be different/unique between the BRI ports, except for priority 0. Priority 0 means that this port will not be used as a clock source for this card /system. Possible values: 0...4.
 - e) The **Switch type** is set to `euroisdn` by default and can not be changed.
 - f) Check the **Exclusive channel** checkbox to indicate that the B-channel on an outgoing ISDN call is marked as “preferred” or “exclusive”. By setting a channel to exclusive, it is not possible to negotiate the seizing of other channels in case of collision.
 - g) Enter the time in seconds to restart unused B channels in the **Idle reset interval** field. If the field is empty/blank, the functionality is disabled.
 - h) Enter or change the receive gain value in decibel in the **Receive gain** field. The default value is 0 db. A negative value decreases the gain, and a positive value increases the gain. This is a mandatory field.
 - i) Enter or change the transmit gain value in decibel in the **Transmit gain** field. The default value is 0 db. A negative value decreases the gain, and a positive value increases the gain. This is a mandatory field.
 - j) Enter a default destination number in the **Default destination** field. This number is used to route the call in case of a call with no or an incomplete calling number. The call is released when no called digits

are received and the default destination is not configured. This is needed for Austria.

- k) Enter a value in the **T302 timer** field. This is the time to wait for digits. Possible values: 5...15 sec.
- l) Enable or disable the Inband Announcement after disconnect with the **Far end disconnect with inband announcement** checkbox.
- m) Enable or disable the parallel B-Channel restarts with the **B-Channel parallel restarts** checkbox. If the flag is enabled, a RESTART message for each individual b-channel is sent simultaneously for all b-channels. If the flag is disabled, a RESTART message is sent for the first b-channel and RESTART ACKNOWLEDGE is required for this b-channel before sending RESTART for the next b-channel.
- n) Enable or disable the PI8 in the ALERT with the **Always send PI8 in Alert** checkbox. If the flag is enabled, the OpenScape Branch sends ALERT with PI8 (progress indicator: In-band information or an appropriate pattern). Otherwise PI8 is never sent in ALERT.
- o) Select the type of Setup progress indicator from the **Setup Progress Indicator** selection list. Values: **Non-ISDN Destination**, **Non-ISDN Origin**, **Not end to end ISDN**, **None** (default).
- p) Enable or disable the Early media on Call Processing with the **Start Early Media on CALL PROCESSING** checkbox. If the flag is enabled, the OpenScape Branch sends ALERT with PI8 (progress indicator: In-band information or an appropriate pattern). Otherwise PI8 is never sent in ALERT.

OpenScape Branch will process the subsequent ISDN messages as follows:

- - PROGRESS without PI8: The OSB shall ignore this message (i.e. it shall not send back a SIP 183 Session Progress).
- - PROGRESS with PI8: The OSB shall send back a SIP 183 Session Progress with SDP Answer and without the "**P-Early-Media**" header-field. Note that the SDP Answer must be the same as the one sent in the initial SIP 183 Session Progress.
- - ALERTING: The OSB shall send back a SIP 180 Ringing response with SDP Answer and without the "**P-Early-Media**" header-field. Note that the SDP Answer must be the same as the one sent in the initial SIP 183 Session Progress.
- - CONNECT: The OSB shall send back a SIP 200 OK response with the same SDP Answer as the one sent in the initial SIP 183 Session Progress.

- - DISCONNECT: The OSB shall send back the equivalent 4xx/5xx/6xx response code.
- q) Select the behavior to be used when receiving a 183 Session Progress without SDP from the **183 Session progress without SDP** selection list. This parameter does not apply to CAS.

The following values can be assigned:

- **Alerting:** The 183 Session Progress without SDP is converted to Alerting. (Used for BRI)
 - **Alerting and progress:** The 183 Session Progress without SDP is converted to Alerting and then Progress with PI-2. (Used for BRI)
 - **Progress with PI2:** The 183 Session Progress without SDP is converted to Progress with PI-2. (Used for BRI)
 - **None:** The 183 Session Progress without SDP is ignored. (Used for BRI)
- r) Enable or disable the Disable far end restart with the **Disable Far End Restart** checkbox. In scenarios in which 50i or 500i is connected to a CO switch, that does not accept RESTART message during BRI span bring up.
- s) **Spare Flag 1 - Spare Flag 3** checkboxes are reserved for future use.
- 10) Click the **OK** button to return to the **BRI** window.
- The **Add - BRI** or **Edit - BRI** dialog is closed and the configuration is displayed in the BRI list.
- 11) Select the **Card configuration** tabsheet to configure access type and Multiple Subscriber Numbers (MSNs) for the gateway card.

NOTICE:

The **Card Configuration** work area appears displaying the Access type and list of MSNs.

- a) Select the Access type in the **Access type** selection list. Possible values are **PP-Point to point** or **PMP-Point to multiple point**. If PMP-Point to multiple point has been selected, Multiple Subscriber Numbers (MSNs) can be configured.

NOTICE:

For PP-Point to point, the carrier provides a pilot number (office code) to the customer with an allocated number range under this pilot. For PMP-Point to multiple point, the carrier provides Multiple Subscriber Numbers (MSNs) which are most of the time not in sequence. It is highly probable that an office code can not be defined from the group of numbers and as a consequence there will be no association between the MSN and an internal subscriber and there shall be a number mapping between the external numbers (MSN) and the internal numbers (subscriber DN or MultiLine Hunt Group (HLHG)).

The BRI operating in PMP mode allows connecting more than one DN device to this same bus. ISDN devices which are also connected to the ISDN bus are

connected to the carrier in parallel with the OpenScape Branch 50i. Specific MSNs can be configured to be handled by each of the devices connected to the bus.

- b) Enter the Multiple Subscriber Number in the **MSN** field up to 12 digits and select the **Add** button to create the MSN. A list of up to 10 MSNs can be configured to indicate that MSNs which are handled by the OpenScape Branch. The MSN is from 1 to 12 digits long. If a SETUP is received for an MSN which is not configured, the call will be ignored. If no MSN is configured all calls will be accepted.

NOTICE:

The MSNs which are provided by the ISDN carrier might not be in sequence. Therefore it may not be possible to determine an Office Code for the branch. As a consequence, the MSNs will not correspond to subscriber numbers in the OpenScape Voice system. In this case, the site must be configured with private numbers. Each MSN shall be configured as a Home DN and an External Caller Id shall be associated to each subscriber.

- Normal mode - the MSN must be routed by the OpenScape Voice. The site must be configured in the OpenScape Voice with private numbers.
- Survivable mode for incoming calls a rule must be configured in the SIP Manipulation table to translate each MSN which is being sent in the R-URI to a subscriber DN, an MLHG, a Gateway, a Trunk or a Voice Mail so that the call can be properly routed.
- Survivable mode for outgoing calls a rule must be configured in the SIP Manipulation table to translate the From header to a valid MSN. It is strongly recommended to use only one MSN as the caller id for all the outgoing calls. This recommendation would require only one rule for the outgoing calls.

-
- 12) Select the **Extra configuration** tabsheet to configure additional BRI capabilities. This tab is reserved for future configuration.

NOTICE:

The **Extra configuration** work area appears displaying the **Spare flag 1 - Spare flag 3**.

-
- 13) Click the **OK** button to store the settings temporarily.

The **Integrated Gateway Configuration** window is closed.

- 14) Click the **Apply changes** button in the main window.

The BRI interface of the integrated gateway of an OpenScape Branch 50i system is configured.

4.15.8 How to Configure the T1 PRI Card/E1 PRI Card of an Integrated Gateway for OpenScape Branch 50i

Proceed as follows to configure the PRI (T1 or E1 Primary Rate Interface) card of an integrated gateway of an OpenScape Branch 50i system.

Prerequisites

Adequate administrative permissions.

The connection to the OpenScape Voice system is up.

The system is of the OpenScape Branch 50i type and in operation.

The system is equipped with a PRI card.

Step by Step

- 1) Navigate to **Configuration tab > OpenScape Branch** within the Navigation Bar in the Common Management Platform.
- 2) Select the **Branch Office list** in the Navigation Tree under Administration.
The system presents the **Branch Office Overview** in the Work Area with a current list of all branch offices.
- 3) To view a list of Branch Offices 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 branch office use one of the following options:
 - In the Work Area select the checkbox to the left of the particular branch office in the list and select **Manage**. Selecting the **Manage** button updates the **Branch Office** field, in the Navigation Tree, with the selected branch office and displays information and data in the Work Area for that branch office.
 - Choose a branch office from the **Branch Office** pull-down located in the Navigation Tree. Information and data are displayed in the Work Area.
- 5) Navigate to **Configuration > Integrated Gateways** in the navigation tree under **Administration**.

The **Integrated Gateway Configuration** window appears with the **General** tab selected by default.

In the **Gateway configuration** field area the **Card 1** and **Card 2** fields show the interface configuration of the OpenScape Branch 50i system for one or more of the following: FXS (Foreign eXchange Station), FXO (Foreign eXchange Office), BRI (Basic Rate Interface) or PRI (Primary Rate Interface).

- 6) Click the **Configuration** button associated with the PRI interface in the **Integrated Gateway Configuration** field area.

The **PRI/CAS Configuration** window appears displaying card and fax information as well as the settings of each port in a table list, as below:

- **Method:** E1 or T1.
- **Fax T.38:** Indicates if the T.38 fax standard for the integrated gateway is activated.
- **GNG detection:** Indicates if the detection of GNG (Fax Calling Tone) is activated.
- **Enable:** Indicates if the port is enabled for traffic.
- **Circuit ID:** Displays the name of the configured port. Value - string with up to 20 alphanumeric characters.
- **Card:** Card value 1 or 2 identifies which card the associated ports belong to.
- **Physical Port:** Identifies the ports associated with the card.
- **Signaling method:** Displays the signaling method for the port. Values - D4, ESF, ISDN=CRC4, CAS=Double.
- **Clock source priority:** Displays the priority for selection of the port used for clocking.
- **Coding:** Type of coding. Values - **AMI** , **B8ZS** or **HDB3**.
- **Switch Type:** Display values- **EuroISDN**, **NI2** , **4ESS**, **5ESS custom**.
- **Line build out:** Values - **0**, **5**, **6**, **7**.
- **Terminal Mode:** If checked, the mode is Terminal side. If unchecked the mode is Network side.

- 7) To change the method used by the PRI card, select a value from the **Method** drop-down list in the Card Configuration work area. Values - E1, T1.
- 8) To configure T.38 fax standard, the following checkboxes are available in the FAX T.38 work area:
 - a) To activate or deactivate the T.38 fax standard for the integrated gateway, check or uncheck the **Enable Fax T.38** checkbox.
 - b) To activate or deactivate the detection of CNG (Fax Calling Tone), check or uncheck the **Enable CNG Detection** checkbox.
- 9) To enable or disable a physical port:
 - a) Locate the row corresponding to the port in the table list.
 - b) Check or uncheck the **Enable** checkbox.
- 10) To edit the priority for selection of a port used for clocking:
 - a) Locate the row corresponding to the port in the table list.
 - b) Click on the **Clock source priority** cell and select the desired value.

Priorities must be different between the PRI ports, except for priority 0 for this card / system. Priority 0 means that this port will not be used as a clock source for this card /system. Possible values: 0-1.

IMPORTANT: Modifying this parameter will cause existing calls to be lost when applying changes.

- 11) To edit a port configuration, check the respective checkbox and click the **Edit** button. The **PRI Configuration** window appears and the **General tab** is displayed by default.

12) In the PRI Configuration window General tab, perform the following steps:

- a) The physical port is displayed in the **Port** field (read only).
- b) Select the signaling method from the **Signaling method** selection list. For T1 PRI select **D4** for superframe and **ESF** for Extended Super Frame. For E1 PRI select **ISDN=CRC4** or **CAS=Double** for Channel Associated Signaling.

IMPORTANT: Modifying this parameter will cause existing calls to be lost when applying changes.

Upon selecting **CAS** the **CAS Settings** Tab in the PRI window will activate for further configuration.

- c) Select the line build out value from the **Line build out** selection list (Value: 0, 5, 6, 7).

IMPORTANT: Modifying this parameter will cause existing calls to be lost when applying changes.

- d) Select the type of coding from the **Coding** selection list (Value: **AMI** Alternate Mark Inversion, **B8ZS** or **HDB3** High-Density Bipolar 3).
- e) The **Switch type** is set to **EuroISDN** (`euroisdn`) for E1 PRI and is set to **NI2** (`National`) for T1 PRI by default. In addition, Switch type **4ESS** and **5ESS custom** is supported.

NOTICE:

Individual PRIs do not need to have the same value. For example: Card 1 Port 1 might be set to 4ESS while Card 1 Port 2 might be set to NI2.

- f) Enable or disable Cyclic Redundancy Check (CRC) operation with the **CRC** checkbox (Only for E1 method).
- g) Enable or disable B-Channel Availability Signalling (BCAS) operation with the **BCAS** checkbox (Only for 4ESS and 5ESS custom switch types).
- h) Select the B-Channel Availability Signalling (BCAS) message that will be sent after restart from the **BCAS service message after restart** selection list (Values: **In service** or **Out of service**).
- i) Enable or disable echo cancellation with the **Echo cancellation** checkbox. When selected allows configuration of the Echo Tail parameter.
- j) Select the Echo Tail value from the **Echo Tail (ms)** selection list (Values: **32**, **64**, **128** milliseconds). (Applies to OpenScape Branch 500i only).
- k) Enable or disable terminal mode operation with the **Terminal Mode** checkbox. If checked, the mode is Terminal side. If unchecked the mode is Network side.
- l) Enter or change the receive gain value in decibel in the **Receive gain** field. The range is -30 dB - +20 dB, default value is 0 dB. A negative value decreases the gain, and a positive value increases the gain. This is a mandatory field.
- m) Enter or change the transmit gain value in decibel in the **Transmit gain** field. The range is -30 dB - +20 dB, default value is 0 dB. A negative

value decreases the gain, and a positive value increases the gain. This is a mandatory field.

- n) Enter a default destination number in the **Default destination** field (Value: 24 digits). This number is used to route the call in case of a call with no or an incomplete calling number. The call is released when no called digits are received and the default destination is not configured. This is needed for Austria.
- o) The **Clock source priority** (Per-card clock source) is displayed (read-only).
- p) Check the **Exclusive channel** checkbox to indicate that the B-channel on an outgoing ISDN call is marked as “preferred” or “exclusive”. By setting a channel to exclusive, it is not possible to negotiate the seizing of other channels in case of collision.

13) Select the **Advance tabsheet:**

- a) To indicate sending complete shall be sent, checkmark the **Sending Complete** checkbox. This parameter is for E1 PRI is mandatory (not for CAS).
- b) Enable or disable the Inband Announcement after disconnect with the **Far end disconnect with inband announcement** checkbox, for T1 and E1 (not CAS).
- c) Enable or disable the calling name delay with the **Calling Name Delay** checkbox.

This parameter is for T1 and E1 PRI Interfaces (not CAS). Indicates the Calling Name will be provided in a separate ISDN message and the SIP INVITE message will postponed until the Facility with Calling Name is received or after a fixed 2 seconds timer expires.

- d) Enable or disable the second screening indicator with the **Second Screening Indicator** checkbox.

This parameter is for T1 and E1 PRI Interfaces (not CAS). If enabled, for an incoming setup message to the OpenScape branch arriving with two calling parties, the first calling party will not be used as screening indicator and the second one will be used instead.

This happens in case the screening indicator of the second Calling Party Number is "network-provided". The following table shows which Calling party Number is used by OSB:

Received	Second Screening Indicator	Used
USER-1st/USER-2nd	0	USER-2nd
USER-1st/USER-2nd	1	USER-2nd
NET-1st/NET-2nd	0	NET-1st
NET-1st/NET-2nd	1	NET-2nd
NET-1st/USER-2nd	0	USER-2nd
NET-1st/USER-2nd	1	NET-1st
USER-1st/NET-2nd	0	USER-1st
USER-1st/NET-2nd	1	NET-2nd

- e) Enable or disable Incoming calls with digital information bearer capability with the **Data calls allowed** checkbox. This parameter is for E1 PRI Interfaces only.

- f) Select the type of Setup progress indicator from the **Setup Progress Indicator** selection list. Values: **Non-ISDN Destination**, **Non-ISDN Origin**, **Not end to end ISDN**, **None** (default). This parameter does not apply to CAS.
- g) Enable or disable the sending of PI8 in the ALERT message with the **Always send PI8 in alert** checkbox.
- h) Enable or disable the sending of early media on call proceeding with the **Start early media on call proceeding** checkbox.
- i) Enable or disable the restart link start-up with the **Restart Link Start-up** checkbox. This parameter does not apply to CAS.
- j) Enable or disable the Disable far end restart with the **Disable Far End Restart** checkbox.

In scenarios in which 50i or 500i is connected to a CO switch such as MUNDRA in India, that does not accept RESTART message during PRI span bring up. The flag is for use only with NET5 type switch and specific CO such as MUNDRA in India.

- k) Select the L3 trunk restart type from the **L3 trunk restart type** selection list.

Depending on the selected option the OSB50i will send the Q931 RESTART message accordingly: Restart **Channel** - A RESTART message is sent for each channel, if the channel is enabled and assigned to any trunk group. The channel will be considered IN SERVICE if the respective RESTART ACKNOWLEDGE response is received for that channel. Restart **Interface** - One RESTART message is sent with Restart indicator information element set to "All Interfaces", if all channels are enabled and assigned to any trunk group. Otherwise, a RESTART for each channel will be sent just for the enabled and assigned channels. If a RESTART ACKNOWLEDGE is received with Restart indicator information element set to "All Interfaces" all the channels for that E1/T1 will be considered IN SERVICE. Possible values: **Channel** or **Interface**. This parameter is for E1 PRI Interfaces. This parameter does not apply to CAS.

- l) Enter the time in seconds to restart unused B channels in the **Idle reset interval** field (Range: empty or 60-7200 seconds). If the field is empty/blank, the functionality is disabled. This parameter does not apply to CAS.
- m) Enable or disable parallel restarting of B-channels with the **B-channel parallel restarts** checkbox.
- n) Enable or disable the send calling party name with the **Send calling party name** checkbox.

For E1: For both User side and Network side, the calling party will be sent if Send Calling Party Name is enabled. The name is sent in an IE DISPLAY. However, the Calling Name can also be received in the IE FACILITY. The Calling Name will always be sent in the SETUP message. For T1: For both User side and Network side, the calling party will be sent if Send Calling Party Name is enabled. The name is sent in an IE FACILITY. The Calling Name will always be sent in the SETUP message.

- o) Select the IE to be used when sending calling party name information from the **Calling party name** selection list. The **Send calling party**

name must be enabled to use this value. This parameter does not apply to CAS.

The following values can be assigned:

- **Facility IE:** The name is sent in the Facility IE. Used for NI-2 and Euro-ISDN (default). Not supported for 4ESS and 5ESS/custom.
 - **Display IE:** The name is sent in the Display IE. Not support for NI-2, 4ESS and 5ESS/Custom. Supported for Euro-ISDN.
- p) Enable or disable the sending of the redirecting number in the diversion header for outgoing calls from the Integrated Gateway with the **Send redirecting number** checkbox.
- q) Select the IE to be used when sending redirecting number information from the **Redirecting number** selection list. The **Send redirecting number** must be enabled to use this value. This parameter does not apply to CAS.

The following values can be assigned:

- **Facility IE:** The redirecting number is sent in the Facility IE. Not supported for NI-2, 4ESS and 5ESS/Custom. Supported for Euro-ISDN (default)
 - **Redirecting number IE:** The redirecting number is sent in the Redirecting number IE. Used for NI-2, 4ESS, 5ESS/Custom (Default) and Euro-ISDN.
- r) Select the behavior to be used when receiving a 183 Session Progress without SDP from the **183 Session progress without SDP** selection list. The This parameter does not apply to CAS.

The following values can be assigned:

- **Alerting:** The 183 Session Progress without SDP is converted to Alerting. Used for NI-2, 4ESS, 5ESS/Custom (Default) and Euro-ISDN.
- **Alerting and progress:** The 183 Session Progress without SDP is converted to Alerting and then Progress with PI-2. Used for NI-2, 4ESS, 5ESS/Custom and Euro-ISDN)
- **Progress with PI2:** The 183 Session Progress without SDP is converted to Progress with PI-2. Used for NI-2, 4ESS, 5ESS/Custom (Default) and Euro-ISDN.
- **None:** The 183 Session Progress without SDP is ignored. Used for NI-2, 4ESS, 5ESS/Custom (Default) and Euro-ISDN.

14) Select the **Timers tabsheet:**

- a) Assign timer values to each timer that applies to the interface.
- b) Enter a value in the **T302 timer** field. This is the time to wait for digits for E1 only. Possible values: 5...15 sec, default: 15 seconds.
- c) Enter a value in the **T305 timer** field. This is the time to wait for disconnect acknowledgement for T1 and E1 (not CAS). Possible values: 5...60 seconds, default: 30 seconds.
- d) Enter a value in the **T308 timer** field. This is the time to wait for Release acknowledgement for T1 and E1 (not for CAS). Possible values: 4...20 seconds, default: 4 seconds.
- e) Enter a value in the **T309 timer** field. This is the time to maintain active calls on Layer 2 disconnection for T1 and E1. Possible values: 5...100 seconds or 0 (default 0, calls are immediately cleared).
- f) Enter a value in the **T313 timer** field. This is the time to wait for CONNECT acknowledge, CPE side only. Possible values: 3...20 seconds, default: 4 seconds.

15) Select the **Channels tabsheet:**

- a) Check or uncheck the **All channels** checkbox to enable or disable all channels.
- b) Enable or disable the channel by checking or unchecking the **Enable** checkbox.
- c) Click the **OK** button to return to the **PRI Configuration** window. The update is displayed.

16) Click the **OK button to return to the **PRI** window.**

The **PRI** dialog is closed and the configuration is displayed in the PRI list.

17) Select the Channel Associated Signaling **CAS Settings tabsheet (supported in Version 2).**

Note: Framing for the port must be set to CAS (Channel Associated Signaling) to enable the CAS Setting tab.

18) Select the **CAS profile... button to create a CAS profile.**

The **CAS profile list** window appears.

- a) Select a default CAS profile from the **Default CAS Profiles** field list and click the **Add Profile** button. Default CAS Profiles below (additional profiles may be added when required).

The selected CAS profile is added to the list with default parameters displayed.

Profile	Max ANI	Max DNIS	Get ANI first	Skip Category	Immediate Accept	MF Back Timer	Meter Pulse Timer	Charge Calls	Forced Release
Argentina Telefonía	20	4	No						
Telecom Argentina	10	4				5000	200		
Brazil Embratel 1	20	4	No						
Brazil Embratel 2	20	4	No		No	1500	def	Yes	Yes
Brazil Oi 1	20	4	Yes						

Profile	Max ANI	Max DNIS	Get ANI first	Skip Category	Immediate Accept	MF Back Timer	Meter Pulse Timer	Charge Calls	Forced Release
Brazil Oi 2	20	20	No						
Brazil Oi 3	20	20	No				500		
Brazil Oi 4	20	4	No			4000			
Brazil CTBC	20	4	No		No	3000	def		
Brazil Telefonica	20	4	No		No	3000	def		
Mexico	10	4	No			def	def		

- b) Select a profile and click the **Edit...** button to edit a profile or click the **Add...** button to create a new profile.

The **Edit - CAS profile** window or **Add - CAS profile** window appears.

- c) Enter the CAS profile name in the **Name** field if creating a new profile.
- d) Checkmark the **ANI before DNIS** checkbox if ANI information shall be used before DNIS information.
- e) Select the maximum number of ANI digits that a channel on this context expects, from the **Maximum amount of ANI** field list. Value: 0-24 digits.
- f) Select the maximum number of DNIS digits that a channel on this context expects, from the **Maximum amount of DNIS** field list. Value: 0-24 digits.
- g) Enter the maximum wait time for a backward request, in the **Maximum Waiting time for MF Back Tone** field. Value: 0-1000000, e.g. 5000.
- h) Enter the maximum wait time for meter pulses, in the **Meter Pulse Timeout** field. Value: 0-1000.
- i) Checkmark the **Immediate Accept** checkbox to accept the call bypassing and the use of group B and II tones.
- j) Checkmark the **Forced Release** checkbox if forced release is allowed.
- k) Checkmark the **Skip category** checkbox to skip the category request and immediately go to GII/B signals.
- l) Checkmark the **Charge calls** checkbox to indicate call charging is active.
- m) Click the **OK** button to store the settings temporarily.

The **CAS profile list** window appears with the new or modified CAS profile displayed.

- n) Click the **OK** button to store the settings temporarily.

The **PRI** window appears with the new or modified CAS profile displayed.

- 19) Edit the CAS Advanced setting by selecting the **Enable** checkbox in the **CAS Advanced settings** work area.
 - a) Select a default CAS profile from the **Default CAS Profiles** field list and click the **Add Profile** button.

The selected CAS profile is added to the list with default parameters displayed
 - b) Select a profile and click the **Edit...** button to edit a profile or click the **Add...** button to create a new profile.

The **Edit - CAS profile** window or **Add - CAS profile** window appears.
 - c) Enter the maximum timeout value for a MF back resume cycle, in the **Timeout for MF back resume cycle** field. Value: 0-1000000, e.g. 150.
 - d) Enter the Call Forward protection timing, in the **Call Forward safety** field. Protection is required to avoid a call which is forwarded to a mobile phone times out due to a delay from the mobile switch to acknowledge the seize request. Value: 0-1000000, e.g. 30000.
 - e) Enter the maximum timeout value to wait for a seizure acknowledgement, in the **Wait for seizure acknowledgement** field. Value: 0-1000000, e.g. 8000.
 - f) Enter the maximum timeout value to wait for an answer acknowledgement, in the **Wait for answer** field. Value: 0-1000000, e.g. 6000.
 - g) Enter the time for a second answer, in the **Double answer** field. Value: 0-1000000, e.g. 400.
 - h) Enter the time to delay answer, in the **Answer delay** field. Value: 0-1000000, e.g. 150.
 - i) Enter the time to validate the CAS state changes, in the **Persistence check** field. Value: 0-1000000, e.g. 500.
 - j) Enter the time to wait prior to DTMF dialing, in the **DTMF start dial** field. Value: 0-1000000, e.g. 500.
 - k) Enter the maximum MF threshold timing, in the **MF threshold** field. Value: 0-1000000.
 - l) **Spare timer 1-5**: Used for future CAS requirements.
 - m) Click the **OK** button to store the settings temporarily.

The **PRI/CAS Configuration** window appears with the new or modified CAS profile displayed.
 - n) Click the **OK** button to store the settings temporarily.

The **Integrated Gateway Configuration** window appears.
- 20) Click the **OK** button to store the settings temporarily.

The **Integrated Gateway Configuration** window is closed.
- 21) Click the **Apply changes** button in the main window.

The PRI interface of the integrated gateway of an OpenScape Branch 50i or 500i system is configured.

4.15.9 How to Configure the T1 PRI Card/E1 PRI Card of an Integrated Gateway for OpenScape Branch 500i

Proceed as follows to configure the PRI (T1 or E1 Primary Rate Interface) card of an integrated gateway of an OpenScape Branch 500i system.

Prerequisites

Adequate administrative permissions.

The connection to the OpenScape Voice system is up.

The system is of the OpenScape Branch 500i type and in operation.

The system is equipped with a PRI card.

Step by Step

- 1) Navigate to **Configuration tab > OpenScape Branch** within the Navigation Bar in the Common Management Platform.
- 2) Select the **Branch Office list** in the Navigation Tree under Administration.
The system presents the **Branch Office Overview** in the Work Area with a current list of all branch offices.
- 3) To view a list of Branch Offices 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 branch office use one of the following options:
 - In the Work Area select the checkbox to the left of the particular branch office in the list and select **Manage**. Selecting the **Manage** button updates the **Branch Office** field, in the Navigation Tree, with the selected branch office and displays information and data in the Work Area for that branch office.
 - Choose a branch office from the **Branch Office** pull-down located in the Navigation Tree. Information and data are displayed in the Work Area.
- 5) Navigate to **Configuration > Features > Integrated Gateways** in the navigation tree under **Administration**.

The **Integrated Gateway Configuration** window appears with the **General** tab selected by default.

In the **Gateway configuration** field area the **Card 1** and **Card 2** fields show the interface configuration or the OpenScape Branch 500i system for PRI (Primary Rate Interface).

In the **Gateway configuration** field area the **Per-card clock source** checkbox is checked and is read-only, if only one PRI (Primary Rate Interface) card is installed for the OpenScape 500i. If two PRI cards are installed for the OpenScape 500i, the checkbox by default is not checked and it is possible to configure the PRI clock source individually per port or used a "Combined clock source".

- 6) Click the **Configuration** button associated with the PRI interface in the **Integrated Gateway Configuration** field area.

The **PRI/CAS Configuration** window appears displaying card and fax information as well as the settings of each port in a table list, as below:

- **Method:** E1 or T1.
- **Fax T.38:** Indicates if the T.38 fax standard for the integrated gateway is activated.
- **GNG detection:** Indicates if the detection of GNG (Fax Calling Tone) is activated.
- **Enable:** Indicates if the port is enabled for traffic.
- **Circuit ID:** Displays the name of the configured port. Value - string with up to 20 alphanumeric characters.
- **Card:** Card value 1 or 2 identifies which card the associated ports belong to.
- **Physical Port:** Identifies the ports associated with the card.
- **Signaling method:** Displays the signaling method for the port. Values - D4, ESF, ISDN=CRC4, CAS=Double.
- **Clock source priority:** Displays the priority for selection of the port used for clocking.
- **Coding:** Type of coding. Values - **AMI** , **B8ZS** or **HDB3**.
- **Switch Type:** Display values- **EuroISDN**, **N12** , **4ESS**, **5ESS custom**.
- **Line build out:** Values - **0**, **5**, **6**, **7**.
- **Terminal Mode:** If checked, the mode is Terminal side. If unchecked the mode is Network side.

- 7) To change the method used by the PRI card, select a value from the **Method** drop-down list in the Card Configuration work area. Values - E1, T1.

NOTICE:

If the method is changed, the interfaces will be reset to the default values for the method chosen and the PRI-B channels will be removed from the trunk groups

- 8) To enable or disable a physical port:
- a) Locate the row corresponding to the port in the table list.
 - b) Check or uncheck the **Enable** checkbox.
- 9) To edit the priority for selection of a port used for clocking:
- a) Locate the row corresponding to the port in the table list.
 - b) Click on the **Clock source priority** cell and select the desired value.

Priorities must be different between the PRI ports, except for priority 0 for this card / system. Priority 0 means that this port will not be used as a clock source. Possible values: 0-8 .

IMPORTANT: Modifying this parameter will cause existing calls to be lost when applying changes.

- 10) To edit a port configuration, check the respective checkbox and click the **Edit** button. The **PRI Configuration** window appears and the **General tab** is displayed by default.

- 11) In the **PRI Configuration** window General tab, perform the following steps:
 - a) The physical port is displayed in the **Port** field (read only).
 - b) Select the signaling method from the **Signaling method** selection list.
For T1 PRI select **D4** for superframe and **ESF** for Extended Super

Frame. For E1 PRI select **ISDN=CRC4** or **CAS=Double** for Channel Associated Signaling.

IMPORTANT: Modifying this parameter will cause existing calls to be lost when applying changes.

Upon selecting **CAS** the **CAS Settings** Tab in the PRI window will activate for further configuration.

- c) Select the line build out value from the **Line build out** selection list (Value: 0, 5, 6, 7).

IMPORTANT: Modifying this parameter will cause existing calls to be lost when applying changes.

- d) Select the type of coding from the **Coding** selection list (Value: **AMI** Alternate Mark Inversion, **B8ZS** or **HDB3** High-Density Bipolar 3).

IMPORTANT: Modifying this parameter will cause existing calls to be lost when applying changes.

- e) The **Switch type** is set to **EuroISDN** (`euroisdn`) for E1 PRI and is set to **NI2** (`National`) for T1 PRI by default. In addition, Switch type **4ESS** and **5ESS custom** is supported.

NOTICE:

Individual PRIs do not need to have the same value. For example: Card 1 Port 1 might be set to 4ESS while Card 1 Port 2 might be set to NI2.

IMPORTANT: Modifying this parameter will cause existing calls to be lost when applying changes.

- f) Enable or disable Cyclic Redundancy Check (CRC) operation with the **CRC** checkbox (Only for E1 method).

IMPORTANT: Modifying this parameter will cause existing calls to be lost when applying changes.

- g) Enable or disable B-Channel Availability Signalling (BCAS) operation with the **BCAS** checkbox (Only for 4ESS and 5ESS custom switch types).

NOTICE:

If BCAS is activated and NI2 trunk is used, then Restart Channel must be used.

- h) Select the B-Channel Availability Signalling (BCAS) message that will be sent after restart from the **BCAS service message after restart** selection list (Values: **In service** or **Out of service**).
- i) Enable or disable echo cancellation with the **Echo cancellation** checkbox. When selected allows configuration of the Echo Tail parameter.

- j) Select the Echo Tail value from the **Echo Tail (ms)** selection list (Values: **32, 64, 128** milliseconds). (Applies to OpenScape Branch 500i only).
 - k) Enable or disable terminal mode operation with the **Terminal Mode** checkbox. If checked, the mode is Terminal side. If unchecked the mode is Network side.
 - l) Enter or change the receive gain value in decibel in the **Receive gain** field. The range is -30 dB - +20 dB, default value is 0 dB. A negative value decreases the gain, and a positive value increases the gain. This is a mandatory field.
 - m) Enter or change the transmit gain value in decibel in the **Transmit gain** field. The range is -30 dB - +20 dB, default value is 0 dB. A negative value decreases the gain, and a positive value increases the gain. This is a mandatory field.
 - n) Enter a default destination number in the **Default destination** field (Value: 24 digits). This number is used to route the call in case of a call with no or an incomplete calling number. The call is released when no called digits are received and the default destination is not configured. This is needed for Austria.
 - o) The **Clock source priority** (Per-card clock source) is displayed (read-only).
 - p) Check the **Exclusive channel** checkbox to indicate that the B-channel on an outgoing ISDN call is marked as "preferred" or "exclusive". By setting a channel to exclusive, it is not possible to negotiate the seizing of other channels in case of collision.
- 12) Select the **Advance** tabsheet:**
- a) To indicate sending complete shall be sent, checkmark the **Sending Complete** checkbox. This parameter is for E1 PRI is mandatory (not for CAS).
 - b) Enable or disable the Inband Announcement after disconnect with the **Far end disconnect with inband announcement** checkbox, for T1 and E1 (not CAS).
 - c) Enable or disable the calling name delay with the **Calling Name Delay** checkbox. This parameter is for T1 and E1 PRI Interfaces (not CAS). Indicates the Calling Name will be provided in a separate ISDN message and the SIP INVITE message will postponed until the Facility with Calling Name is received or after a fixed 2 seconds timer expires.
 - d) Enable or disable the second screening indicator with the **Second Screening Indicator** checkbox.

This parameter is for T1 and E1 PRI Interfaces (not CAS). If enabled, for an incoming setup message to the OpenScape branch arriving with two calling parties, the first calling party will not be used as screening indicator and the second one will be used instead.

This happens in case the screening indicator of the second Calling Party Number is "network-provided". The following table shows which Calling party Number is used by OSB:

Received	Second Screening Indicator	Used
USER-1st/USER-2nd	0	USER-2nd
USER-1st/USER-2nd	1	USER-2nd
NET-1st/NET-2nd	0	NET-1st

Received	Second Screening Indicator	Used
NET-1st/NET-2nd	1	NET-2nd
NET-1st/USER-2nd	0	USER-2nd
NET-1st/USER-2nd	1	NET-1st
USER-1st/NET-2nd	0	USER-1st
USER-1st/NET-2nd	1	NET-2nd

- e) Enable or disable Incoming calls with digital information bearer capability with the **Data calls allowed** checkbox. This parameter is for E1 PRI Interfaces only.
- f) Select the type of Setup progress indicator from the **Setup Progress Indicator** selection list. Values: **Non-ISDN Destination**, **Non-ISDN Origin**, **Not end to end ISDN**, **None** (default). This parameter does not apply to CAS.
- g) Enable or disable the sending of PI8 in the ALERT message with the **Always send PI8 in alert** checkbox.
- h) Enable or disable the sending of early media on call proceeding with the **Start early media on call proceeding** checkbox.
- i) Enable or disable the restart link start-up with the **Restart Link Start-up** checkbox. This parameter does not apply to CAS.
- j) Enable or disable the Disable far end restart with the **Disable Far End Restart** checkbox. In scenarios in which 50i or 500i is connected to a CO switch such as MUNDRA in India, that does not accept RESTART message during PRI span bring up. The flag is for use only with NET5 type switch and specific CO such as MUNDRA in India.
- k) Select the L3 trunk restart type from the **L3 trunk restart type** selection list. Depending on the selected option the OSB50i will send the Q931 RESTART message accordingly: Restart **Channel** - A RESTART message is sent for each channel, if the channel is enabled and assigned to any trunk group. The channel will be considered IN SERVICE if the respective RESTART ACKNOWLEDGE response is received for that channel. Restart **Interface** - One RESTART message is sent with Restart indicator information element set to "All Interfaces", if all channels are enabled and assigned to any trunk group. Otherwise, a RESTART for each channel will be sent just for the enabled and assigned channels. If a RESTART ACKNOWLEDGE is received with Restart indicator information element set to "All Interfaces" all the channels for that E1/T1 will be considered IN SERVICE. Possible values: **Channel** or **Interface**. This parameter is for E1 PRI Interfaces. This parameter does not apply to CAS.
- l) Enter the time in seconds to restart unused B channels in the **Idle reset interval** field (Range: empty or 60-7200 seconds). If the field is empty/blank, the functionality is disabled. This parameter does not apply to CAS.
- m) Enable or disable parallel restarting of B-channels with the **B-channel parallel restarts** checkbox.
- n) Enable or disable the send calling party name with the **Send calling party name** checkbox. For E1: For both User side and Network side, the calling party will be sent if Send Calling Party Name is enabled. The name is sent in an IE DISPLAY. However, the Calling Name can also be received in the IE FACILITY. The Calling Name will always be sent

in the SETUP message. For T1: For both User side and Network side, the calling party will be sent if Send Calling Party Name is enabled. The name is sent in an IE FACILITY. The Calling Name will always be sent in the SETUP message.

- o) Select the IE to be used when sending calling party name information from the **Calling party name** selection list. The **Send calling party name** must be enabled to use this value. This parameter does not apply to CAS.

The following values can be assigned:

- **Facility IE:** The name is sent in the Facility IE. (Used for NI-2 4ESS/5ESS, Euro-ISDN (default))
 - **Display IE:** The name is sent in the Display IE. (Not support for NI-2 4ESS/5ESS, Euro-ISDN)
- p) Enable or disable the sending of the redirecting number in the diversion header for outgoing calls from the Integrated Gateway with the **Send redirecting number** checkbox.
 - q) Select the IE to be used when sending redirecting number information from the **Redirecting number** selection list. The **Send redirecting number** must be enabled to use this value. This parameter does not apply to CAS.

The following values can be assigned:

- **Facility IE:** The redirecting number is sent in the Facility IE. (Not supported for NI-2 4ESS/5ESS, Euro-ISDN (default))
 - **Redirecting number IE:** The redirecting number is sent in the Redirecting number IE. (Used for NI-2 4ESS/5ESS, Euro-ISDN)
- r) Select the behavior to be used when receiving a 183 Session Progress without SDP from the **183 Session progress without SDP** selection list. The This parameter does not apply to CAS.

The following values can be assigned:

- **Alerting:** The 183 Session Progress without SDP is converted to Alerting. (Used for NI-2 4ESS/5ESS, Euro-ISDN (default))
- **Alerting and progress:** The 183 Session Progress without SDP is converted to Alerting and then Progress with PI-2. (Used for NI-2 4ESS/5ESS, Euro-ISDN)
- **Progress with PI2:** The 183 Session Progress without SDP is converted to Progress with PI-2. (Used for NI-2 4ESS/5ESS (Default), Euro-ISDN)
- **None:** The 183 Session Progress without SDP is ignored. (Used for NI-2 4ESS/5ESS, Euro-ISDN (default))

13) Select the **Timers tabsheet:**

- a) Assign timer values to each timer that applies to the interface.
- b) Enter a value in the **T302 timer** field. This is the time to wait for digits for E1 only. Possible values: 5...15 sec, default: 15 seconds.
- c) Enter a value in the **T305 timer** field. This is the time to wait for disconnect acknowledgement for T1 and E1 (not CAS). Possible values: 5...60 seconds, default: 30 seconds.
- d) Enter a value in the **T308 timer** field. This is the time to wait for Release acknowledgement for T1 and E1 (not for CAS). Possible values: 4...20 seconds, default: 4 seconds.
- e) Enter a value in the **T309 timer** field. This is the time to maintain active calls on Layer 2 disconnection for T1 and E1. Possible values: 5...100 seconds or 0 (default 0, calls are immediately cleared).
- f) Enter a value in the **T313 timer** field. This is the time to wait for CONNECT acknowledge, CPE side only. Possible values: 3...20 seconds, default: 4 seconds.

14) Select the **Channels tabsheet:**

- a) Check or uncheck the **All channels** checkbox to enable or disable all channels.
- b) Enable or disable the channel by checking or unchecking the **Enable** checkbox.
- c) Click the **OK** button to return to the **PRI Configuration** window. The update is displayed.

15) Click the **OK button to return to the **PRI** window.**

The **PRI** dialog is closed and the configuration is displayed in the PRI list.

16) Select the Channel Associated Signaling **CAS Settings tabsheet (supported in Version 2).**

Note: Framing for the port must be set to CAS (Channel Associated Signaling) to enable the CAS Setting tab.

17) Select the **CAS profile... button to create a CAS profile.**

The **CAS profile list** window appears.

- a) Select a default CAS profile from the **Default CAS Profiles** field list and click the **Add Profile** button. Default CAS Profiles below (additional profiles may be added when required).

The selected CAS profile is added to the list with default parameters displayed.

Profile	Max ANI	Max DNIS	Get ANI first	Skip Categ	Immedi Accept	MF Back Timer	Meter Pulse Timer	Charç Calls	Forced Release
Argentina Telefonía	20	4	No						
Telecom Argentina	10	4				5000	200		
Brazil Embratel 1	20	4	No						

Profile	Max ANI	Max DNIS	Get ANI first	Skip Category	Immediate Accept	MF Back Timer	Meter Pulse Timer	Charge Calls	Forced Release
Brazil Embratel 2	20	4	No		No	1500	def	Yes	Yes
Brazil Oi 1	20	4	Yes						
Brazil Oi 2	20	20	No						
Brazil Oi 3	20	20	No				500		
Brazil Oi 4	20	4	No			4000			
Brazil CTBC	20	4	No		No	3000	def		
Brazil Telefonica	20	4	No		No	3000	def		
Mexico	10	4	No			def	def		

- b) Select a profile and click the **Edit...** button to edit a profile or click the **Add...** button to create a new profile.

The **Edit - CAS profile** window or **Add - CAS profile** window appears.

- c) Enter the CAS profile name in the **Name** field if creating a new profile.
- d) Checkmark the **ANI before DNIS** checkbox if ANI information shall be used before DNIS information.
- e) Select the maximum number of ANI digits that a channel on this context expects, from the **Maximum amount of ANI** field list. Value: 0-24 digits.
- f) Select the maximum number of DNIS digits that a channel on this context expects, from the **Maximum amount of DNIS** field list. Value: 0-24 digits.
- g) Enter the maximum wait time for a backward request, in the **Maximum Waiting time for MF Back Tone** field. Value: 0-1000000, e.g. 5000.
- h) Enter the maximum wait time for meter pulses, in the **Meter Pulse Timeout** field. Value: 0-1000.
- i) Checkmark the **Immediate Accept** checkbox to accept the call bypassing and the use of group B and II tones.
- j) Checkmark the **Forced Release** checkbox if forced release is allowed.
- k) Checkmark the **Skip category** checkbox to skip the category request and immediately go to GII/B signals.
- l) Checkmark the **Charge calls** checkbox to indicate call charging is active.
- m) Click the **OK** button to store the settings temporarily.

The **CAS profile list** window appears with the new or modified CAS profile displayed.

- n) Click the **OK** button to store the settings temporarily.

The **PRI** window appears with the new or modified CAS profile displayed.

- 18) Edit the CAS Advanced setting by selecting the **Enable** checkbox in the **CAS Advanced settings** work area.
- a) Select a default CAS profile from the **Default CAS Profiles** field list and click the **Add Profile** button.

The selected CAS profile is added to the list with default parameters displayed
 - b) Select a profile and click the **Edit...** button to edit a profile or click the **Add...** button to create a new profile.

The **Edit - CAS profile** window or **Add - CAS profile** window appears.
 - c) Enter the maximum timeout value for a MF back resume cycle, in the **Timeout for MF back resume cycle** field. Value: 0-1000000, e.g. 150.
 - d) Enter the Call Forward protection timing, in the **Call Forward safety** field. Protection is required to avoid a call which is forwarded to a mobile phone times out due to a delay from the mobile switch to acknowledge the seize request. Value: 0-1000000, e.g. 30000.
 - e) Enter the maximum timeout value to wait for a seizure acknowledgement, in the **Wait for seizure acknowledgement** field. Value: 0-1000000, e.g. 8000.
 - f) Enter the maximum timeout value to wait for an answer acknowledgement, in the **Wait for answer** field. Value: 0-1000000, e.g. 6000.
 - g) Enter the time for a second answer, in the **Double answer** field. Value: 0-1000000, e.g. 400.
 - h) Enter the time to delay answer, in the **Answer delay** field. Value: 0-1000000, e.g. 150.
 - i) Enter the time to validate the CAS state changes, in the **Persistence check** field. Value: 0-1000000, e.g. 500.
 - j) Enter the time to wait prior to DTMF dialing, in the **DTMF start dial** field. Value: 0-1000000, e.g. 500.
 - k) Enter the maximum MF threshold timing, in the **MF threshold** field. Value: 0-1000000.
 - l) **Spare timer 1-5**: Used for future CAS requirements.
 - m) Click the **OK** button to store the settings temporarily.

The **PRI** window appears with the new or modified CAS profile displayed.
 - n) Click the **OK** button to store the settings temporarily.

The **Integrated Gateway Configuration** window appears.
- 19) Click the **OK** button to store the settings temporarily.

The **Integrated Gateway Configuration** window is closed.
- 20) Click the **Apply changes** button in the main window.

The PRI interface of the integrated gateway of an OpenScape Branch 50i or 500i system is configured.

4.15.9.1 How to Configure Clock Source for T1 PRI Card/E1 PRI Card

Proceed as follows to configure the clock source for PRI (T1 or E1 Primary Rate Interface) cards of an integrated gateway of an OpenScape Branch 500i system.

Prerequisites

Adequate administrative permissions.

The connection to the OpenScape Voice system is up.

The system is of the OpenScape Branch 500i type and in operation.

The system is equipped with a PRI card.

Step by Step

- 1) Navigate to **Configuration tab > OpenScape Branch** within the Navigation Bar in the Common Management Platform.
- 2) Select the **Branch Office list** in the Navigation Tree under Administration.
The system presents the **Branch Office Overview** in the Work Area with a current list of all branch offices.
- 3) To view a list of Branch Offices 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 branch office use one of the following options:
 - In the Work Area select the checkbox to the left of the particular branch office in the list and select **Manage**. Selecting the **Manage** button updates the **Branch Office** field, in the Navigation Tree, with the selected branch office and displays information and data in the Work Area for that branch office.
 - Choose a branch office from the **Branch Office** pull-down located in the Navigation Tree. Information and data are displayed in the Work Area.
- 5) Navigate to **Configuration > Features > Integrated Gateways** in the navigation tree under **Administration**.

The **Integrated Gateway Configuration** window appears with the **General** tab selected by default.

In the **Gateway configuration** field area the **Card 1** and **Card 2** fields show the interface configuration of the OpenScape Branch 50i or 500i system for one or more of the following: FXS (Foreign eXchange Station), FXO (Foreign eXchange Office), BRI (Basic Rate Interface) or PRI (Primary Rate Interface).

In the **Gateway configuration** field area the **Per-card clock source** checkbox is checked and is read-only, if only one PRI (Primary Rate Interface) card is installed for the OpenScape 500i. If two PRI cards are installed for the OpenScape 500i, the checkbox by default is not checked and it is possible to configure the PRI clock source individually per port or used a "Combined clock source".

- 6) Click the **Configuration** button associated with the PRI interface in the **Integrated Gateway Configuration** field area.

The **PRI/CAS Configuration** window appears displaying card and fax information as well as the settings of each port in a table list, as below:

- **Method:** E1 or T1.
- **Fax T.38:** Indicates if the T.38 fax standard for the integrated gateway is activated.
- **GNG detection:** Indicates if the detection of GNG (Fax Calling Tone) is activated.
- **Enable:** Indicates if the port is enabled for traffic.
- **Circuit ID:** Displays the name of the configured port. Value - string with up to 20 alphanumeric characters.
- **Card:** Card value 1 or 2 identifies which card the associated ports belong to.
- **Physical Port:** Identifies the ports associated with the card.
- **Signaling method:** Displays the signaling method for the port. Values - D4, ESF, ISDN=CRC4, CAS=Double.
- **Clock source priority:** Displays the priority for selection of the port used for clocking.
- **Coding:** Type of coding. Values - **AMI** , **B8ZS** or **HDB3**.
- **Switch Type:** Display values- **EuroISDN**, **N12** , **4ESS**, **5ESS custom**.
- **Line build out:** Values - **0, 5, 6, 7**.
- **Terminal Mode:** If checked, the mode is Terminal side. If unchecked the mode is Network side.

- 7) To edit the priority for selection of a port used for clocking:
- a) Locate the row corresponding to the port in the table list.
 - b) Click on the **Clock source priority** cell and select the desired value.

Priorities must be different between the PRI ports, except for priority 0 for this card / system. Priority 0 means that this port will not be used as a clock source. The values are 0, 1-4 if one card is installed and 0, 1-8 if two cards are installed. The value 0 can be used by multiple PRIs.

IMPORTANT: Modifying this parameter will cause existing calls to be lost when applying changes.

- 8) Click the **OK** button to store the settings temporarily.
The **PRI** window is closed.
- 9) Click the **OK** button to store the settings temporarily.
The **Integrated Gateway Configuration** window is closed.
- 10) Click the **Apply changes** button in the main window.

The PRI interface of the integrated gateway of an OpenScape Branch 500i system is configured.

4.15.10 How to Configure Trunk Groups for the OpenScape Branch 50i

Proceed as follows to configure a trunk group with BRI (Basic Rate Interface), PRI (Primary Rate Interface) or FXO (Foreign eXchange Office).

Prerequisites

Adequate administrative permissions.

The connection to the OpenScape Voice system is up.

The system is of the OpenScape Branch 50i type and in operation.

The system is equipped with a BRI or PRI card.

Step by Step

- 1) Navigate to **Configuration tab > OpenScape Branch** within the Navigation Bar in the Common Management Platform.
- 2) Select the **Branch Office list** in the Navigation Tree under Administration.
The system presents the **Branch Office Overview** in the Work Area with a current list of all branch offices.
- 3) To view a list of Branch Offices 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 branch office use one of the following options:
 - In the Work Area select the checkbox to the left of the particular branch office in the list and select **Manage**. Selecting the **Manage** button updates the **Branch Office** field, in the Navigation Tree, with the selected or branch office and displays information and data in the Work Area for that branch office.
 - Choose a branch office from the **Branch Office** pull-down located in the Navigation Tree. Information and data are displayed in the Work Area.
- 5) Navigate to **Configuration > Features > Integrated Gateways** in the navigation tree under **Administration**.
The **Integrated Gateway Configuration** window appears with the **General** tab selected by default.
In the **Gateway configuration** field area the **Card 1** and **Card 2** fields show the interface configuration or the OpenScape Branch 50i system for one or more of the following: FXS (Foreign eXchange Station), FXO (Foreign eXchange Office), BRI (Basic Rate Interface) or PRI (Primary Rate Interface).
- 6) Click the **Trunk Group...** button in the **Gateway configuration** field area.
The **Trunk Group Configuration** window appears displaying the parameters of each trunk group in a list.

- 7) The following actions can be performed:
- To delete a trunk group, check the respective checkbox and click the **Delete** button. The trunk group is removed from the list.
 - To edit a trunk group, check the respective checkbox and click the **Edit...** button.
 - To add an entry to the trunk group list, click the **Add...** button.
- 8) In the **Trunk Group Configuration** dialog, perform the following steps in the **General** tabsheet:
- a) Enter the Fully Qualified Domain Name of the trunk group in the **FQDN** field.
 - b) Enter the **Trunk group name**. This is a mandatory field.
 - c) Select the **Trunk group selection** from the selection list. Possible values: Top to bottom, Bottom to top. This is a mandatory field.
 - d) Select the hunt type in the **Hunt type** selection list. Possible values: **Linear**, **Circular**. This is a mandatory field.
 - e) Select the direction of traffic flow on the trunk group in the **Direction** selection list. Possible values: **Both**, **Originating**, **Terminating**. This is a mandatory field.
 - f) Enable or disable the **Mark sRTP call-leg as secure** checkbox. If a secure media is negotiated for a trunk (FXO, BRI or PRI), the call will be indicated as secure (ST-Siemens-Call-Type: secure).

The SRTP parameters apply to Proxy and Proxy ATA. SRTP parameters do not apply to Proxy ACD, Branch SBC and SBC-Proxy.
 - g) Enter the Prefixes as there are: **International PNAC** (International Public Network Access Code), **International Prefix**, **National PNAC**, **National Prefix**, **Subscriber PNAC**, **Subscriber Prefix**.
 - h) Enter the **Country code (L2)**, **Local area code (L1)** and **Exchange code**.
 - i) Enable or disable the **TON length check** checkbox. If enabled, an additional check for Type Of Number (TON) match for the Called Party in the outgoing direction to the PSTN for inclusive numbers is performed. National (10) and Subscriber (7) must be configured. Applies to US Numbering Plan only.
 - j) Enter the **National number length**. If the TON (Type Of Number) length check is enabled and a match for PNAC and/or Prefix is found, the length of the number check will be performed, after stripping the PNAC and/or Prefix; if the remaining length is equal to the National PNAC length the TON will be set to National.
 - k) Enter the **Subscriber number length**. If the TON (Type Of Number) length check is enabled and a match for PNAC and/or Prefix is found, the length of the number check will be performed, after stripping the PNAC and/or Prefix; if the remaining length is equal to the Subscriber PNAC length the TON will be set to Subscriber.
 - l) Select the **Voice transfer capability** from the selection list. Possible values: **Speech** or **3.1 kHz Audio**.

- 9) Select the **Network specific facilities** tabsheet:
 - a) Enable or disable the send NSF with the **Send NSF** checkbox.
Note: Network Specific Facility function applies to T1 PRI.
 - b) Enter the network specific facility in the **Network ID** field (Value: 4 digit string). This parameter is mandatory for T1 PRI (does not apply to CAS). Note: Send NSF must be enable.
 - c) Select the facility coding value from the **Facility Coding Value** selection list. Values are but not limited to the following: Hotel-Motel, Long Distance, Call Redirection, Foreign Exchange, and more. Note: Send NSF must be enabled. This parameter does not apply to CAS.
 - d) Enter the service parameters in the **Service Parameters** field (Value: 0-5 digit string). Note: Send NSF must be enable. This parameter does not apply to CAS.
- 10) Select the **Spare flags** tabsheet:
 - a) Select the appropriate **Spare flag** if required for configuration.
Spare flags are supported for future use or special custom requirements.
 - b) Click the **OK** button.
The **Spare flags** dialog for the trunk Group Configuration dialog is updated.
- 11) Select the **Channels list** tabsheet for assigning PRI:
 - a) Assign one or more interfaces (PRI: Port 1...4, Channels 1-23 (PRI T1), 1-32 (PRI E1) to the trunk group using the **Add** button.
 - b) Use the **Delete** button to remove an assigned interface from a trunk group.
- 12) Select the **Interfaces** tabsheet for assigning BRI:
 - a) Assign one or more interfaces (BRI: Port 1...4) to the trunk group using the **Add** button.
 - b) Use the **Delete** button to remove an assigned interface from a trunk group.
- 13) Select the **Number Modification** tabsheet:
 - a) Select the normalization of numbers which are received from the BRI interfaces in the **Modification (Except Called Party Number in Survivable Mode)** selection list in the **Incoming Calls** work area. Possible values are Not Modified, Prefixed or E.164.
 - b) Select the **Called Party Number Type of Number (Survivable Mode)**. Possible values: International, National or Subscriber.
 - c) Check the **Unknown prefixed numbers from PSTN** checkbox to indicate the calling party received with TON UNKNOWN and with prefix. Otherwise, all numbers will be handled as subscribers.
 - d) Enter the **Max Overlap digit length** for the number of digits that can be received in an overlap dialing incoming call. When the number of incoming digits matches this configuration, the called number is considered complete even when no SENDING COMPLETE information is received. (Value: 1-24 digits).
 - e) Checkmark the **Specific Overlap digit pattern** checkbox to allow configuration of the dialing patterns for processing an incoming call. Indicates that the system must process incoming digits in accordance

with the patterns defined in the table. If this parameter is enabled and there are entries in the table, **Max Overlap Digit Length** is ignored.

Row number, **Dial Pattern** and **Maximum digit length** is displayed in the in theDial Pattern table.

- f) Click the **Configure...** button next to the Specific overlap dialing patterns to configure specific dialing patterns.
- g) Click the **Add...** button to add a dialing pattern or select an existing dialing pattern and click the **Edit...** button to modify the dialing pattern. To delete a dialing pattern select an existing dialing patterns and click the **Delete** button.
- h) Enter the **Dialing Pattern** for up to 20 patterns for each BRI or PRI trunk group. The dialing pattern accepts numeric values and the percent character only. Dialing Pattern is used in combination with the **Maximum digit length** to determine if sufficient incoming digits have been dialed to permit the call to continue processing. No match will result in the call waiting for the next digit to be received.

Rules for Dialing Patterns:

- - % can be used only at the end of a dialing pattern.
- - If % is not present in the Dialing Pattern, the number of dialed digits must match Maximum digit length for the row.
- - A Dialing Pattern must not be duplicated between rows.
- - If only % is present in the Dialing Pattern, the Maximum digit length for the row must be the greatest in the table.
- - % represents any string of 1 or more digits.
- - If Specific Overlap Dialing Patterns is set, the table must have at least one entry.

Examples of valid entries:

- Dialing Pattern / Maximum digit length.
- - 979390% / 8 digits: This pattern will match any 8-digit number that begins with 979390.
- - % / 10 digits : This pattern will match any 10 digit number.
- - 5619235555 / 10 digits: This pattern will match exactly 5619235555.
- - 7% / 5 digits: This pattern will match any 5 digit number that begins with 7.

Example of conflicting entries:

- The following example shows a case where two similar patterns can conflict with another.
- - 4933197939% with length 11.
- - 49331979397% with length 12.
- The first pattern is expecting one more digit in the 11th position, and the second pattern indicates that 12 digits are required when the 11th digit is a 7. The first pattern cannot be resolved until the 11th digit is dialed. If the 11th digit is anything other than a 7, then the number is resolved immediately, while if it is a 7, then another digit is required.
- i) Enter the **Max digit length** specifies the maximum overlap digit length for the row. (Value: 1-24 digits).

- j) Click the **OK** button to return to the **Specific overlap dialing patterns** window.

The list of dialing patterns is updated with the new, modified or deleted dialing pattern.

- k) Click the **OK** button to return to the **Trunk Group Configuration > Number Modification** tab.
- l) Select the **Type** of Number from the selection list for the Calling Party, in the **Outgoing Calls** work area. Possible values: **International**, **National** or **Subscriber**.
- m) Check the **Set TON to unknown** checkbox for the Calling Party Number to send the number with the Unknown label even if the number is prepared in the right format.
- n) Check the **Add Prefix** checkbox for the Calling Party Number to indicate that the International, National or Subscriber Prefix shall be added to the number which is sent to PSTN.
- o) Select the **Type** of Number from the selection list for the Called Party Number. Possible values: **Received TON**, **International**, **National** and **Subscriber**.
- p) Check the **Set TON to unknown** checkbox for the Called Party Number to send the number with the Unknown label even if the number is prepared in the right format.
- q) Check the **Add Prefix** checkbox for the Called Party Number to indicate that the International, National or Subscriber Prefix shall be added to the number which is sent to PSTN.
- r) Enter the **Pre Dial delay for DTMF** value in ms. This is a mandatory field. If DTMF digits are dialed before the DTMF receiver is allocated, the first digits can be lost. This parameter applies to FXO configuration.
- s) Select the type of collect call control in the **Collect call control** selection list, in the **Collect Calls** work area (supported in Version 2). Collect Calls parameters are only applicable when **Framing** is configured as **CAS** and are not applicable for BRI. The Collect Call Barring is configured to define if the control is performed by the integrated Gateway or by the OpenScape Voice. If the control is set to the gateway, the control will be system wide. Possible values: **Gateway** or **Server**.

If the parameter Collect Call Control is set to gateway, the parameters "Permission for Receiving Collect Calls By Category (only for Brazil)" and "Permission for Receiving collect Calls By Double Answer (only for Brazil)" are valid for normal and survivability mode.

If the parameter Collect Call Control is set to server, the parameters "Permission for Receiving Collect Calls By Category (only for Brazil)" and "Permission for Receiving collect Calls By Double Answer (only for Brazil)" are only valid for survivability mode.

- t) Checkmark the **Permission for receiving Collect calls by category** checkbox, if collect calls can only be received by category only. (supported in Version 2).
- u) Enter the **Permission for receiving Collect calls by double Answer** (supported in Version 2).
- v) Select a Channel Associated Signaling (CAS) profile in the **CAS profile** selection list (supported in Version 2). Possible values: Based on CAS created for the trunk interface.

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

The **Trunk Group Configuration** dialog is closed and the configuration is displayed in the trunk group list.

- 15) Click the **OK** button to return to the **Integrated Gateway Configuration** window.

- 16) Click the **OK** button to store the settings temporarily.

The **Integrated Gateway Configuration** window is closed.

- 17) Click the **Apply changes** button in the main window.

The trunk group of the integrated gateway is configured.

4.15.11 How to Configure Trunk Groups for the OpenScape Branch 500i

Proceed as follows to configure a trunk group with PRI (Primary Rate Interface) for the OpenScape Branch 500i.

Prerequisites

Adequate administrative permissions.

The connection to the OpenScape Voice system is up.

The system is of the OpenScape Branch 500i type and in operation.

The system is equipped with a PRI card.

Step by Step

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

The system presents the **Branch Office Overview** in the Work Area with a current list of all branch offices.

- 3) To view a list of Branch Offices 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 branch office use one of the following options:
 - In the Work Area select the checkbox to the left of the particular branch office in the list and select **Manage**. Selecting the **Manage** button updates the **Branch Office** field, in the Navigation Tree, with the selected branch office and displays information and data in the Work Area for that branch office.
 - Choose a branch office from the **Branch Office** pull-down located in the Navigation Tree. Information and data are displayed in the Work Area.

- 5) Navigate to **Configuration > Features > Integrated Gateways** in the navigation tree under **Administration**.

The **Integrated Gateway Configuration** window appears with the **General** tab selected by default.

In the **Gateway configuration** field area the **Card 1** and **Card 2** fields show the interface configuration or the OpenScape Branch 500i system for PRI (Primary Rate Interface).

- 6) Click the **Trunk Group...** button in the **Gateway configuration** field area.

The **Trunk Group Configuration** window appears displaying the parameters of each trunk group in a list.

- 7) The following actions can be performed:

- To delete a trunk group, check the respective checkbox and click the **Delete** button. The trunk group is removed from the list.
- To edit a trunk group, check the respective checkbox and click the **Edit...** button.
- To add an entry to the trunk group list, click the **Add...** button.

- 8) In the **Trunk Group Configuration** dialog, perform the following steps in the **General** tabsheet:

- a) Enter the Fully Qualified Domain Name of the trunk group in the **FQDN** field.
- b) Enter the **Trunk group name**. This is a mandatory field.
- c) Select the **Trunk group selection** from the selection list. Possible values: Top to bottom, Bottom to top. This is a mandatory field.
- d) Select the hunt type in the **Hunt type** selection list. Possible values: **Linear**, **Circular**. This is a mandatory field.
- e) Select the direction of traffic flow on the trunk group in the **Direction** selection list. Possible values: **Both**, **Originating**, **Terminating**. This is a mandatory field.
- f) Enable or disable the **Mark sRTP call-leg as secure** checkbox. If a secure media is negotiated for a trunk (FXO, BRI or PRI), the call will be indicated as secure (ST-Siemens-Call-Type: secure).

The SRTP parameters apply to Proxy and Proxy ATA. SRTP parameters do not apply to Proxy ACD, Branch SBC and SBC-Proxy.

- g) Enter the Prefixes as there are: **International PNAC** (International Public Network Access Code), **International Prefix**, **National PNAC**, **National Prefix**, **Subscriber PNAC**, **Subscriber Prefix**.
- h) Enter the **Country code (L2)**, **Local area code (L1)** and **Exchange code**.
- i) Enable or disable the **TON length check** checkbox. If enabled, an additional check for Type Of Number (TON) match for the Called Party in the outgoing direction to the PSTN for inclusive numbers is performed. National (10) and Subscriber (7) must be configured. Applies to US Numbering Plan only.
- j) Enter the **National number length**. If the TON (Type Of Number) length check is enabled and a match for PNAC and/or Prefix is found, the length of the number check will be performed, after stripping the PNAC and/or Prefix; if the remaining length is equal to the National PNAC length the TON will be set to National.
- k) Enter the **Subscriber number length**. If the TON (Type Of Number) length check is enabled and a match for PNAC and/or Prefix is found, the length of the number check will be performed, after stripping the

PNAC and/or Prefix; if the remaining length is equal to the Subscriber PNAC length the TON will be set to Subscriber.

- l) Select the **Voice transfer capability** from the selection list. Possible values: **Speech** or **3.1 kHz Audio**.
- 9) Click the **Restart trunk group channels** button to initiate a restart on all channels associated with the trunk group.
- 10) Select the **Network specific facilities** tabsheet:
 - a) Enable or disable the send NSF with the **Send NSF** checkbox.
 Note: Network Specific Facility function applies to T1 PRI.
 - b) Enter the network specific facility in the **Network ID** field (Value: 4 digit string). This parameter is mandatory for T1 PRI (does not apply to CAS). Note: Send NSF must be enable.
 - c) Select the facility coding value from the **Facility Coding Value** selection list. Values are but not limited to the following: Hotel-Motel, Long Distance, Call Redirection, Foreign Exchange, and more. Note: Send NSF must be enabled. This parameter does not apply to CAS.
 - d) Enter the service parameters in the **Service Parameters** field (Value: 0-5 digit string). Note: Send NSF must be enable. This parameter does not apply to CAS.
- 11) Select the **Spare flags** tabsheet:
 - a) Select the appropriate **Spare flag** if required for configuration.
 Spare flags are supported for future use or special custom requirements.
 - b) Click the **OK** button.
 The **Spare flags** dialog for the trunk Group Configuration dialog is updated.
- 12) Select the **Channels list** tabsheet:
 - a) Assign one or more interfaces (PRI: Card 1-2, Port 1...4, Channels 1-23 (PRI T1), 1-32 (PRI E1) to the trunk group using the **Add** button.
 - b) Use the **Delete** button to remove an assigned interface from a trunk group.
 - c) Click the **OK** button.
 The **Trunk group channels** dialog is closed and the channels list in the trunk Group Configuration dialog is updated with the channels assigned to the trunk group.
- 13) Select the **Number Modification** tabsheet:
 - a) Select the normalization of numbers which are received from the BRI interfaces in the **Modification (Except Called Party Number in Survivable Mode)** selection list in the **Incoming Calls** work area. Possible values are Not Modified, Prefixed or E.164.
 - b) Select the **Called Party Number Type of Number (Survivable Mode)**. Possible values: International, National or Subscriber.
 - c) Check the **Unknown prefixed numbers from PSTN** checkbox to indicate the calling party received with TON UNKNOWN and with prefix. Otherwise, all numbers will be handled as subscribers.
 - d) Enter the **Max Overlap digit length** for the number of digits that can be received in an overlap dialing incoming call. When the number of incoming digits matches this configuration, the called number is considered complete even when no SENDING COMPLETE information is received. (Value: 1-24 digits).

- e) Checkmark the **Specific Overlap digit pattern** checkbox to allow configuration of the dialing patterns for processing an incoming call. Indicates that the system must process incoming digits in accordance with the patterns defined in the table. If this parameter is enabled and there are entries in the table, **Max Overlap Digit Length** is ignored.

Row number, Dial Pattern and Maximum digit length is displayed in the in theDial Pattern table.

- f) Click the **Configure...** button next to the Specific overlap dialing patterns to configure specific dialing patterns.
- g) Click the **Add...** button to add a dialing pattern or select an existing dialing pattern and click the **Edit...** button to modify the dialing pattern. To delete a dialing pattern select an existing dialing patterns and click the **Delete** button.
- h) Enter the **Dialing Pattern** for up to 20 patterns for each BRI or PRI trunk group. The dialing pattern accepts numeric values and the percent character only. Dialing Pattern is used in combination with the **Maximum digit length** to determine if sufficient incoming digits have been dialed to permit the call to continue processing. No match will result in the call waiting for the next digit to be received.

Rules for Dialing Patterns:

- - % can be used only at the end of a dialing pattern.
- - If % is not present in the Dialing Pattern, the number of dialed digits must match Maximum digit length for the row.
- - A Dialing Pattern must not be duplicated between rows.
- - If only % is present in the Dialing Pattern, the Maximum digit length for the row must be the greatest in the table.
- - % represents any string of 1 or more digits.
- - If Specific Overlap Dialing Patterns is set, the table must have at least one entry.

Examples of valid entries:

- Dialing Pattern / Maximum digit length.
- - 979390% / 8 digits: This pattern will match any 8-digit number that begins with 979390.
- - % / 10 digits: This pattern will match any 10 digit number.
- - 5619235555 / 10 digits: This pattern will match exactly 5619235555.
- - 7% / 5 digits: This pattern will match any 5 digit number that begins with 7.

Example of conflicting entries:

- The following example shows a case where two similar patterns can conflict with another.
- - 4933197939% with length 11.
- - 49331979397% with length 12.
- The first pattern is expecting one more digit in the 11th position, and the second pattern indicates that 12 digits are required when the 11th digit is a 7. The first pattern cannot be resolved until the 11th digit is dialed. If the 11th digit is anything other than a 7, then the number is resolved immediately, while if it is a 7, then another digit is required.

- i) Enter the **Max digit length** specifies the maximum overlap digit length for the row. (Value: 1-24 digits).
- j) Click the **OK** button to return to the **Specific overlap dialing patterns** window.

The list of dialing patterns is updated with the new, modified or deleted dialing pattern.

- k) Click the **OK** button to return to the **Trunk Group Configuration > Number Modification** tab.
- l) Select the **Type** of Number from the selection list for the Calling Party, in the **Outgoing Calls** work area. Possible values: **International**, **National** or **Subscriber**.
- m) Check the **Set TON to unknown** checkbox for the Calling Party Number to send the number with the Unknown label even if the number is prepared in the right format.
- n) Check the **Add Prefix** checkbox for the Calling Party Number to indicate that the International, National or Subscriber Prefix shall be added to the number which is sent to PSTN.
- o) Select the **Type** of Number from the selection list for the Called Party Number. Possible values: **Received TON**, **International**, **National** and **Subscriber**.
- p) Check the **Set TON to unknown** checkbox for the Called Party Number to send the number with the Unknown label even if the number is prepared in the right format.
- q) Check the **Add Prefix** checkbox for the Called Party Number to indicate that the International, National or Subscriber Prefix shall be added to the number which is sent to PSTN.
- r) Enter the **Pre Dial delay for DTMF** value in ms. This is a mandatory field. If DTMF digits are dialed before the DTMF receiver is allocated, the first digits can be lost. This parameter applies to FXO configuration.
- s) Select the type of collect call control in the **Collect call control** selection list, in the **Collect Calls** work area (supported in Version 2). Collect Calls parameters are only applicable when **Framing** is configured as **CAS**. The Collect Call Barring is configured to define if the control is performed by the integrated Gateway or by the OpenScape Voice. If the control is set to the gateway, the control will be system wide. Possible values: **Gateway** or **Server**.

If the parameter Collect Call Control is set to gateway, the parameters "Permission for Receiving Collect Calls By Category (only for Brazil)" and "Permission for Receiving collect Calls By Double Answer (only for Brazil)" are valid for normal and survivability mode.

If the parameter Collect Call Control is set to server, the parameters "Permission for Receiving Collect Calls By Category (only for Brazil)" and "Permission for Receiving collect Calls By Double Answer (only for Brazil)" are only valid for survivability mode.

- t) Checkmark the **Permission for receiving Collect calls by category** checkbox, if collect calls can only be received by category only. (supported in Version 2).
- u) Enter the **Permission for receiving Collect calls by double Answer** (supported in Version 2).
- v) Select a Channel Associated Signaling (CAS) profile in the **CAS profile** selection list (supported in Version 2). Possible values: Based on CAS created for the trunk interface.

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

The **Trunk Group Configuration** dialog is closed and the configuration is displayed in the trunk group list.

- 15) Click the **OK** button to return to the **Integrated Gateway Configuration** window.

- 16) Click the **OK** button to store the settings temporarily.

The **Integrated Gateway Configuration** window is closed.

- 17) Click the **Apply changes** button in the main window.

The trunk group of the integrated gateway is configured.

4.15.12 Configuration in OSV V8 when configuring MTLS in OSB V9

From an OSV V9 perspective, if MTLS is configured as transport type for a Gateway endpoint then MTLS will be enforced on every endpoint on the path from the gateway via the proxies and/or SBC to the OSV.

NOTICE:

In order for MTLS to work, at least 2 EP need to be configured on the OSV: 1. EP Configuration reflecting the Proxy with MTLS configured as transport protocol. 2. EP Configuration reflecting gateway behind the Proxy configured with corresponding transport protocol. For integrated gateways' EPs, only UDP or TCP are used. See examples below.

Example 1: OSB 500i/500i configured as Proxy/Gateway

- Configure EP for OSB Proxy with transport protocol MTLS
- Configure EP for OSB 500i/500i Integrated Gateway NET5/NI2/CAS E1/CAS T1 with transport protocol UDP (alias should have <FQDN>:5096)

NOTICE:

OSB 500i/500i integrated gateway endpoint must be created behind a Proxy Endpoint.

- Configure EP for OSB 500i/500i Integrated Gateway Qsig / Cornet with transport protocol TCP (alias should have <FQDN>:5096)

NOTICE: OSB 500i/500i integrated gateway endpoint must be created behind a Proxy Endpoint.

Example 2: OSB 500i/500i as GW only

- Configure EP for OSB Main with transport protocol MTLS

Two additional endpoints shall be configured for each gateway in order to provide an alternative if the OSB Main is not accessible:

- Configure EP for OSB 50i/500i GW only
- Configure EP for Integrated Gateway 50i/500i (alias should have <FQDN>:5096)

NOTICE:

OSB 50i/500i Integrated Gateway endpoint must be created behind OSB Main Endpoint.

NOTICE: Attribute Route via Proxy to route the calls via the associated endpoint. Attribute Public/ Offnet Traffic must be also enabled.

IMPORTANT:

Do not Send Invite without SDP attribute must NOT be selected on OSB50i/OSB500i Integrated Gateway End Point.

Example

Example 3: **External gateway or SSP behind an OSB**

- Configure EP for OSB Proxy with transport protocol MTLS
- Configure EP for external gateway or SSP with transport protocol UDP, TCP, TLS or MTLS

NOTICE:

If a 500i/50i GW only is connected directly to a OSV with a single EP, the possible configurations are UDP, TCP or TLS.

NOTICE:

The ATA can be configured with a MTLS EP, as their subscribers should be configured with UDP.

IMPORTANT: The transport MTLS for EP external gateway or SSP shall be used only if the connection between the external gateway or SSP and OSB is TLS and TLS mode is set as **Mutual Authentication**.

4.16 Auto Attendant — Overview

The OpenScape Branch supports the automated attendant functionality. This feature is only available for OpenScape Branch V1R3 and later versions.

Overview

The OpenScape Branch supports Automated Attendant functionality. The system can be configured to automatically playback announcements to a line,

enable the caller to navigate through the application via the usage of DTMF tones in order to be forwarded to other announcements, subscriber lines or voicemail boxes.

The Auto Attendant functionality presents the same behavior during normal operating mode as well as during survivable mode. OpenScape Branch supports up to 6 different Auto-Attendant instances. Each instance must be associated to a destination number.

The Auto Attendant functionality is provided for all types of the OpenScape Branch. For OSB 50i:

- FXO interface – the default destination will be associated to an Auto-Attendant instance.
- BRI interface – the called party number shall be associated to an Auto-Attendant instance. In the case of pilot number dialing for Austria, the default destination shall be associated to an Auto-Attendant instance.

Functional Description

The Automated Attendant application provides the following services:

- Prompt Response - answering the call on the first ring and providing a customizable greeting.
- Dial by Extension - through a menu the Auto Attendant can route the caller to a specific line by entering the user extension.
- Information Services – through a menu the Auto Attendant can route the caller to get answer to common questions (like location address, operating hours, etc...).
- Call Redirection – through a menu the Auto Attendant can route the caller to an appropriate number representing a department (Short dialing).
- To cover all incoming calls, an FQDN must be used to identify the calls to Auto-Attendant.

Auto Attendant Menus

The auto-answering function is responsible for answering the call and for applying an entry prompt which offers the following options:

- Information Service.
- Short Dialing.
- Extension Dialing.

After the recorded information is provided, the caller may be asked to dial the destination or the call can be released.

The auto-attendant feature allows the selection of any destination number. A destination number or FQDN is associated to an Auto-Attendant routing table. When a call comes in to the OpenScape Branch, the destination number is evaluated. If this destination number is configured as served by the Auto-Attendant function, the call will be answered and forwarded to the Auto-Attendant.

An initial greeting is played to the caller. For the destination selection, up to 3 menus can be associated to each valid destination number which shall be served by the Auto-Attendant feature.

In principle, the menus are to be used as follows:

- One profile for business hours.
- One profile for after hours.

- One profile for the weekend.

Selecting the Destination

There are 2 ways to select the destination which can be activated together or separately:

- By short dialing.

The auto-answering feature supports short dialing. This is possible by the association of digits to destinations via configuration.

- By dialing the full destination.

In this operating mode the facility detects digits. When the call is answered, a greeting message is played to guide the caller.

If an invalid destination is dialed, the caller will receive a failure prompt and will be routed to the default destination. If no default destination was configured the call will be released.

Caller is prompted to dial one digit:

For example, it is possible to support prompts like: "Dial 1 for Sales, dial 2 for Service Support...". By dialing 1, an announcement will be played and the call will be routed to 2200 which had been previously associated to short dialing 1 for that profile via configuration. If the parameter Extension Dialing is unchecked, the dial process will be immediately be concluded when the caller dials the first digit, otherwise the auto attendant service must wait for the interdigit timeout of '#' dialing.

Caller is prompted to dial the full destination number:

The following is an example of a recorded message: "You have reached the Unify company. Dial the extension number you would like to reach: 2200 for Sales Department or 2300 for Technical Support".

If the DID (Direct Inward Dialing) does not detect a valid DTMF (Dual Tone Multi-Frequency) signal within 10 seconds of the greeting message, a second message is played and the call is transferred to an Attendant.

Forced Announcement

It is possible to configure a menu to operate as a Forced Announcement. In this case, a first greeting announcement will be played and the call will be routed to the original dialed destination, which can be a subscriber or an attendant console. In order to enable this functionality, the parameter "Forward to Original Destination" must be checked.

Restrictions

There are no restrictions. The Auto Attendant functionality is provided for all operational modes.

4.16.1 How to Configure Basic Auto Attendant Settings

Proceed as follows to configure the basic settings of the auto attendant functionality within the OpenScape Branch system: Enable/disable the auto attendant, view the system time, set general telephony parameters.

Prerequisites

Adequate administrative permissions.

At least one 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 Branch** within the Navigation Bar in the Common Management Platform.

2) Select the **Branch Office list** in the Navigation Tree under Administration.

The system presents the **Branch Office Overview** in the Work Area with a current list of all branch offices.

3) To view a list of Branch Offices 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 branch office use one of the following options:

- In the Work Area select the checkbox to the left of the particular branch office in the list and select **Manage**. Selecting the **Manage** button updates the **Branch Office** field, in the Navigation Tree, with the selected branch office and displays information and data in the Work Area for that branch office.
- Choose a branch office from the **Branch Office** pull-down located in the Navigation Tree. Information and data are displayed in the Work Area.

5) Navigate to **Configuration > Auto Attendant in the navigation tree under Administration**.

The **Auto Attendant** window appears with the **General** tab selected by default. The time information fields present a date/day/time snapshot from when the window has been opened.

6) To enable/disable the automated attendant functionality, use the **Enable** checkbox.

7) To configure the general settings which are valid for the whole auto attendant function:

- a) Enter the time the system will wait for digits to be dialed in the **Interdigit timer** field. Possible values: 3...15 seconds. Default: 5 seconds.
- b) Enter the delay time to get connected to announcements in the **Wait to go to menu** field. Possible values: 0...10 seconds. Default: 1 second.
- c) Enter the **Record access code**. Subscribers who can be reached by the short dialing of the Auto Attendant can record their own announcements.

- 8) Click the **OK** button to store the changes temporarily in the administrator's login session.

The **Auto Attendant** window disappears.

- 9) Click the **Apply changes** button in the main window.

The general settings for the automated attendant functionality have been configured.

4.16.2 How to Configure Announcements for Auto Attendant

Proceed as follows to display, add or delete announcement files to be used for the auto attendant functionality within the OpenScape Branch system.

Prerequisites

Adequate administrative permissions.

At least one 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 Branch** within the Navigation Bar in the Common Management Platform.

- 2) Select the **Branch Office list** in the Navigation Tree under Administration.

The system presents the **Branch Office Overview** in the Work Area with a current list of all branch offices.

- 3) To view a list of Branch Offices 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 branch office use one of the following options:

- In the Work Area select the checkbox to the left of the particular branch office in the list and select **Manage**. Selecting the **Manage** button updates the **Branch Office** field, in the Navigation Tree, with the selected branch office and displays information and data in the Work Area for that branch office.
- Choose a branch office from the **Branch Office** pull-down located in the Navigation Tree. Information and data are displayed in the Work Area.

- 5) Navigate to **Configuration > Auto Attendant in the navigation tree under Administration**.

The **Auto Attendant** window appears with the **General** tab selected by default. The **Announcements** field area present a list of the announcements stored on the system.

- 6) To add a new announcement to the system:
 - a) Click the **Browse...** button and select the file (*.wav) of the new announcement.
 - b) Click the **Add** button.

The announcement file is added to the list of available announcements.

- 7) To delete an announcement file from the system:
 - a) Check the checkbox of the respective file name in the announcements list.
 - b) Click the **Delete** button.

the announcement file is removed from the list of available announcements and deleted from the system.

- 8) Click the **OK** button to store the changes temporarily in the administrator's login session.

The **Auto Attendant** window disappears.

- 9) Click the **Apply changes** button in the main window.

The announcement configuration for the automated attendant functionality is completed. To assign the announcements please use the **Menus** tabsheet.

4.16.3 How to Configure Routing for Auto Attendant

Proceed as follows to configure the routing parameters for each destination that shall be served by the automated attendant function.

Prerequisites

Adequate administrative permissions.

At least one 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 Branch** within the Navigation Bar in the Common Management Platform.
- 2) Select the **Branch Office list** in the Navigation Tree under Administration.

The system presents the **Branch Office Overview** in the Work Area with a current list of all branch offices.
- 3) To view a list of Branch Offices 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 branch office use one of the following options:
 - In the Work Area select the checkbox to the left of the particular branch office in the list and select **Manage**. Selecting the **Manage** button updates the **Branch Office** field, in the Navigation Tree, with the

selected branch office and displays information and data in the Work Area for that branch office.

- Choose a branch office from the **Branch Office** pull-down located in the Navigation Tree. Information and data are displayed in the Work Area.

5) Navigate to **Configuration > Auto Attendant** in the navigation tree under **Administration**.

The **Auto Attendant** window appears with the **General** tab selected by default.

6) Select the **Routing** tab.

The system presents a list of all configured auto attendant destinations and its settings.

7) To delete an entry from the system:

- Check the checkbox of the respective entry in the list.
- Click the **Delete** button.

The routing parameters for the destination are removed from the list.

8) To add new routing parameters to the system or edit an existing entry:

- Click the **Add** button or select the entry to be edited and click the **Edit** button.

Depending on the action the **Add Routing** or **Edit Routing** dialog appears.

- Enter the name of the routing table in the **Name** field.
- Select the format of the destination identification (IP/FQDN or Destination Number (DN)) in the **Routing method** field.
- Enter the IP/FQDN / DN for which this routing table shall be serving in the **IP/FQDN or DN** field.
- Select a menu created in the **Menus** tabsheet in each of the **Menu 1**, **Menu 2** and **Menu 3** fields in order to assign them to the routing.

NOTICE: If there is any time overlapping in the menus, the Menu 1 will have precedence on Menu 2, which will have precedence on Menu 3.

- Select the greeting file from the selection list, that will be played when the caller reaches the Auto Attendant in the **Initial Greeting** field.
- If the first announcement shall be played and then the call shall be immediately routed to the original destination, check the **Forward to original destination** checkbox.

NOTICE: If "Forward to original destination" is enabled, the "IP/FQDN or DN" must be configured as an FQDN.

- Enter the **Default Destination** (Value: 1-24 digits). This is an alternate destination for routing a call when the Menus routing is not active. Routing via Menus takes precedence over the Routing default destination.
- Enter the **Routing Code**. In the case of Forced Announcement, it is necessary to manipulate the originally dialed number by adding a routing code. This allows the OSV system to correctly route the call to the Auto Attendant so that the initial greeting can be played to the caller. This routing code must be configured in the OSV to route to the OSB!

- 9) Click the **OK** button to confirm the settings and return to the **Auto Attendant** window.
- 10) Click the **OK** button to store the changes temporarily in the administrator's login session.

The **Auto Attendant** window disappears.

- 11) Click the **Apply changes** button in the main window.

The routing configuration for the automated attendant functionality is completed.

4.16.4 How to Configure Auto Attendant Menus

Proceed as follows to configure the menus which setup the rules for the auto answering functionality.

Prerequisites

Adequate administrative permissions.

At least one 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 Branch** within the Navigation Bar in the Common Management Platform.
- 2) Select the **Branch Office list** in the Navigation Tree under Administration.
The system presents the **Branch Office Overview** in the Work Area with a current list of all branch offices.
- 3) To view a list of Branch Offices 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 branch office use one of the following options:
 - In the Work Area select the checkbox to the left of the particular branch office in the list and select **Manage**. Selecting the **Manage** button updates the **Branch Office** field, in the Navigation Tree, with the selected branch office and displays information and data in the Work Area for that branch office.
 - Choose a branch office from the **Branch Office** pull-down located in the Navigation Tree. Information and data are displayed in the Work Area.
- 5) Navigate to **Configuration > Auto Attendant in the navigation tree under Administration**.

The **Auto Attendant** window appears with the **General** tab selected by default.

- 6) Select the **Menus** tab.

The system presents a list of all configured auto attendant menus.

- 7) To delete an entry from the list:
 - a) Check the checkbox of the respective entry in the list.
 - b) Click the **Delete** button.The menu is removed from the list.
- 8) To add new menus to the system or edit an existing entry:
 - To add new menus to the system click the **Add** button.
 - To edit an existing menu, click the **Edit** button.Depending on the action the **Add Menu** or **Edit Menu** dialog appears.
- 9) Enter the name of the menu in the **Name** field. This name will be presented in the selection list to select the menu in the Routing Table.
- 10) Enter the **Timeout**. This is the timer before the incoming call is routed to the default destination.
- 11) Select the **Activation mode** for this menu. Possible values:
 - **Automatic** – the Time range will be verified. If the current time is in the configured time range, the menu will be active. Two ranges can be configured in order to cover morning and afternoon time for business hours.
 - **Manual** – the menu can be manually enabled / disabled via access code.
 - **Both** – in this case the timers must be configured but the user is also able to manually disable / enable the menu.
- 12) Enter the time range information:
 - a) Select the days from the **Day start** and **Day stop** selection lists. The end value can not be before the day entered in the **Day start** field.
 - b) Enter **Time 1 start** and **Time 2 start** (Two ranges can be configured in order to cover morning and afternoon time for business hours).
 - c) Enter **Time 1 stop** and **Time 2 stop**. The stop time must not be earlier than the corresponding start time.

NOTICE: This option is only valid if the activation mode is set to "Automatic" or "Both".
- 13) Enter the **Activation code** and the **Deactivation code**. This access codes can be configured to manually activate and deactivate a menu.

NOTICE: This option is only valid if the activation mode is set to "Manual" or "Both".
- 14) Select the **Destination selection greeting file** from the selection list. This announcement guides the caller to select a destination.
- 15) Select the **Failure prompt file** from the selection list. This prompt is presented to the caller when the destination entered is invalid.
- 16) Select the **Default Destination prompt file** from the selection list. This prompt is presented to the caller when the call is transferred to the default destination e.g., attendant.
- 17) Select the **Final prompt file** from the selection list. This prompt is presented to the caller when the destination is invalid and the default destination could not answer the call or is not configured. The call is then disconnected.

- 18) Select the **Transfer prompt file** from the selection list. This prompt is presented to the caller when the call is transferred to the chosen destination.
- 19) Select the **Dial method** from the selection list. Possible values:
 - **Extension dialing** – The digit entering process must be finished by timeout or by dialing '#'.

When **Extension dialing** is selected **by itself**, to allow the customer the option to offer the subscriber the option of repeating the current menu or going back to the previous menu; the digits * and # can be configured. Digits 1 - 9 and 0 are disabled.

The number of digits for extension dialing is defined by the **Number of Extension Dialing Digits** field (Value: 2-10 digits (default=7 digits)).
 - **Digit selection** – The call will be immediately routed according to the Abbreviated Dialing table in the **Digits** tabsheet by dialing the first digit.
 - **Both** – Extension dialing and digit selection is supported.
 - **Neither** - If selected setting a **Default destination** is mandatory. This shall allow a customer to route all calls to a particular DN/FQDN/IP Address to an announcement and then forward on to a destination.
- 20) Enter the **Default destination** (Value: 1-24 digits). This parameter defines where the call will be routed based on the Menu routing if, for example, a subscriber does not input a menu selection.
- 21) Select maximum number of digits for an extension from the **Number of Extension Dialing Digits** pull-down field (Value: 2-10 digits, default = 7 digits). This parameter defines the maximum number of digits allowed for extension dialing when the **Dial method** is **Extension dialing** or **Both**.
- 22) Select the **Digits** tabsheet. This tab becomes enabled if **Dial method** is set to **Both**, **Extension Dialing**, or **Digit selection**.

The digits selection table is displayed. This table contains for each of the digits 1 - 9, 0, * and # the configuration settings.
- 23) To configure the settings for a specific digit, check the respective checkbox and click the **Edit...** button.
 - a) The digit to be configured is displayed in the **Digit** field.
 - b) Enter the name of the dial rule in the **Name** field.
 - c) Assign an announcement file from the **File** selection list. This announcement is played after this digit is dialed. An existing file can be selected.
 - d) Enter the DN in the **Destination** field. This indicates the destination to which the call will be routed. The destination must be a valid DN and could be another Auto Attendant Menu or ACD queue. The Auto Attendant Menu destination must not be used as an ACD DID and vice-versa when configuring **ACD > Queue > DID**.
 - e) The **Allow recording** checkbox is used to enable or disable recording the announcement for that destination.
 - f) The **Repeat this menu** checkbox is used to enable or disable, when the subscriber selects this digit, the last menu recording/announcement played to the subscriber.
 - g) Click **OK** to confirm the settings and to return to the **Add menu** window.

The configuration is displayed in the digits selection table.
- 24) Click **OK** to confirm the settings and to return to the **Auto Attendant** window.

- 25) Click the **OK** button to store the changes temporarily in the administrator's login session.

The **Auto Attendant** window disappears.

- 26) Click the **Apply changes** button in the main window.

The menu configuration for the automated attendant functionality is completed.

5 OpenScape Branch Assistant – Profile Configuration

In the main navigation area of the OpenScape Branch Assistant profiles can be configured to assist when configuring multiple OpenScape Branch appliances. Configuration of “Profiles” does not apply to OpenScape Session Border Controllers.

OpenScape Branch Assistant Online Help

The OpenScape Branch Assistant is used to display and configure OpenScape Session Border Controllers V7 and OpenScape Branch Offices V7. The online Help refers mainly to OpenScape SBC V7 and OpenScape Branch V7 version. Therefore, if an OpenScape Branch V1R3, V1R4 or V2 system is selected some sections may describe features that are not available for V1R3, V1R4 or V2 systems and some procedures may deviate from the ones described.

5.1 Profiles Configuration - Overview

The Profiles section in the navigation area allows to display and configure profiles for a Branch appliance.

Profiles provide pre-configuration and administration for groups of functions applied to Branches. Attributes are defined to allow for pre-configuration of certain functions for the following areas:

- Alarms trap destinations.
- Logging settings and continuous tracing.
- Media Server general functions.
- Network Services for NTP and DNS.
- Security firewall and Message Rate Control settings.
- Survivability Call Detail Recording (CDR).
- System general DLS settings.
- VoIP general, timer and threshold settings.

Administration supports up to 256 Profiles.

5.1.1 Branch Deployment Modes

The OpenScape Branch has the flexibility to support, depending on the network topology, four different operating modes.

OpenScape Branch can operate in one of the following modes:

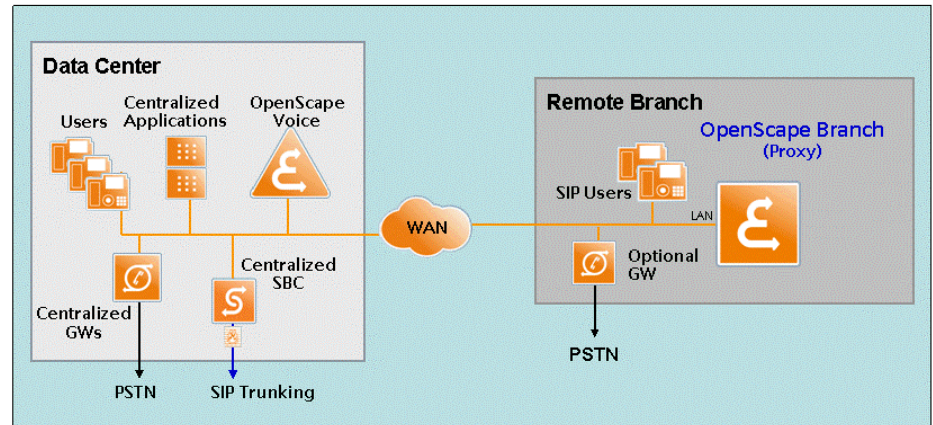
- **Proxy**
- **Proxy ATA**
- **Proxy ACD**
- **SBC Proxy**
- **Branch SBC**

All modes provide the forwarding and redirect functionality for traffic from and to the Endpoints, Media server and Trunks associated with the OpenScape Branch. The OpenScape Branch provides survivability in case the OpenScape Voice system is not reachable.

The OpenScape Session Border Controller is an additional mode defined under OpenScape Branch configuration. Refer to OpenScape Session Border Controller documentation for details.

- **Central SBC**

Proxy Operating Mode



The Proxy mode is for regular proxy usage when a branch is connected via a private network.

Proxy ATA Operating Mode

There are several OpenScape 50i Proxy ATA applications (Version 2).

OpenScape 50i Proxy ATA Connected via a Proxy OpenScape Branch:

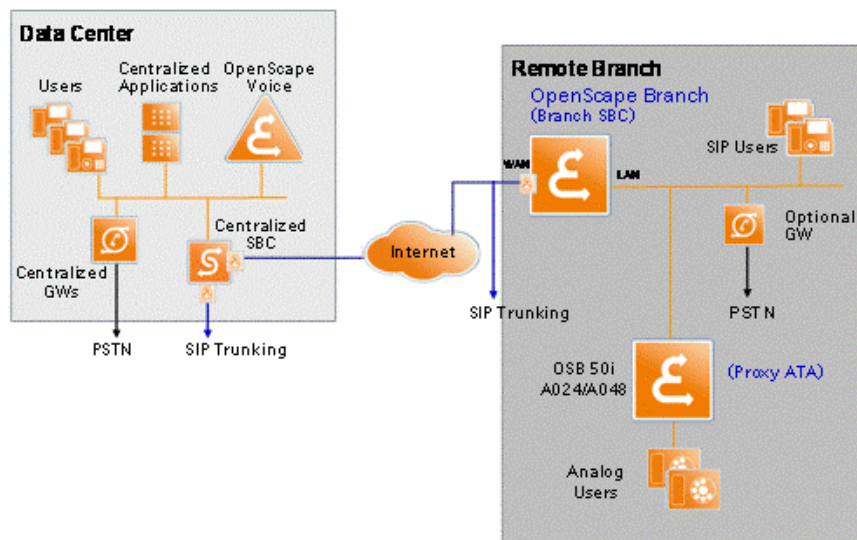
In the figure below, the upstream device is shown as an OpenScape Branch with an external gateway. An alternative to this arrangement would be to use an OpenScape Branch 50i with an internal gateway. The OpenScape Branch is connected to the OpenScape Voice over a corporate WAN, but it could also be connected over a LAN if the Remote Branch is co-located with the OpenScape Voice.

The Proxy ATA registers with only one OpenScape Branch. The Proxy ATA will not support SIP Service Provider trunks.

In this application, the OpenScape Voice can be either in simplex node, or a pair of nodes operating as a cluster (co-located).

If Survivability is required for the OpenScape Branch 50i A024/A048, it will require another upstream device to provide its connectivity to the PSTN. In this configuration, it is required that the upstream device be in the same physical location as the OpenScape Branch 50i A024/A048.

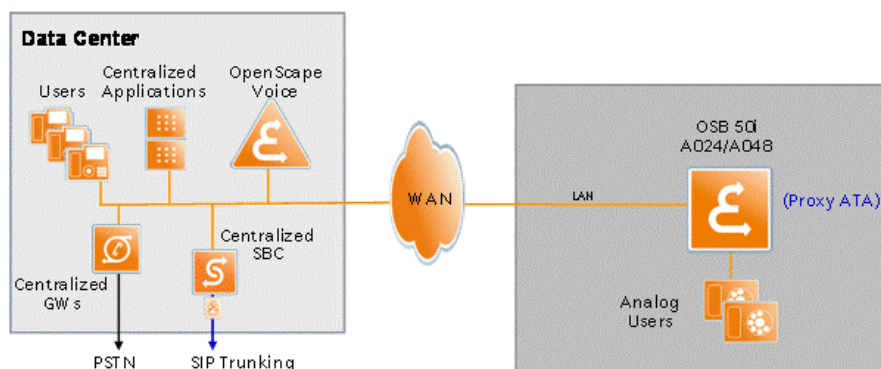
Connected via a Proxy OpenScape Branch



OpenScape 50i Proxy ATA Connected Directly to OpenScape Voice:

The OpenScape Branch 50i A024/A048 can also be utilized as an Analog Terminal Adapter (ATA) connected directly to an OpenScape Voice. The figure below, shows the configuration where the connection to the OpenScape Voice is across a WAN.

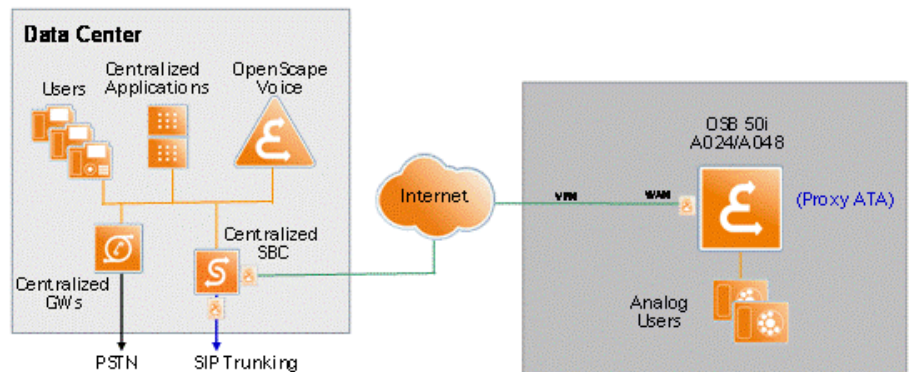
Connected Directly to OpenScape Voice



OpenScape 50i Proxy ATA Connected OpenScape Voice Across the Public Network:

The application, as shown in the figure below, has the OpenScape Branch 50i A024/A048 connected to the OpenScape Voice across a public network. In this configuration, the OpenScape SBC is used. The VPN connection is established at the NAT device.

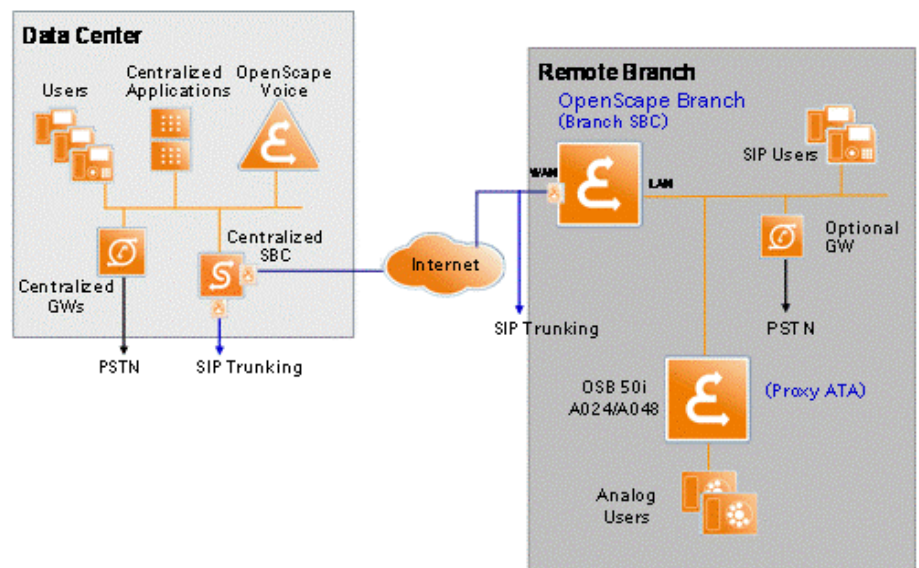
Connected to OpenScope Voice Across Public Network



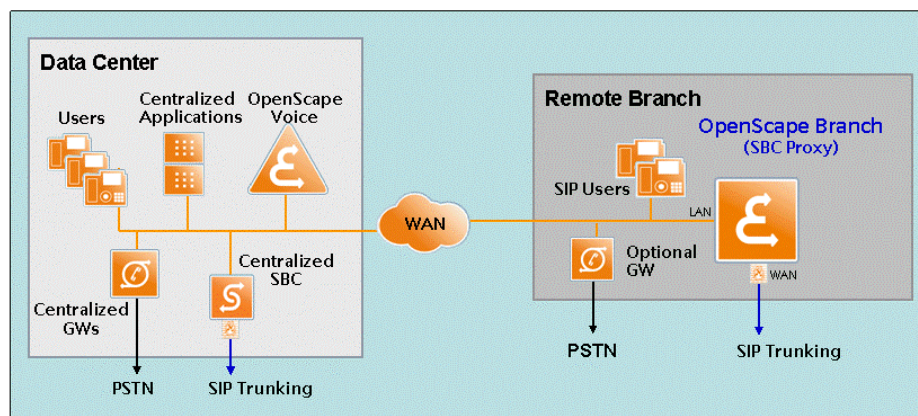
OpenScope 50i Proxy ATA Connected to OpenScope Branch 50i in Branch SBC Mode:

This application shows the OpenScope Branch 50i A024/A048 connected to a OpenScope SBC via another OpenScope Branch running in Branch SBC mode.

Connected to OpenScope Branch 50i in Branch SBC Mode

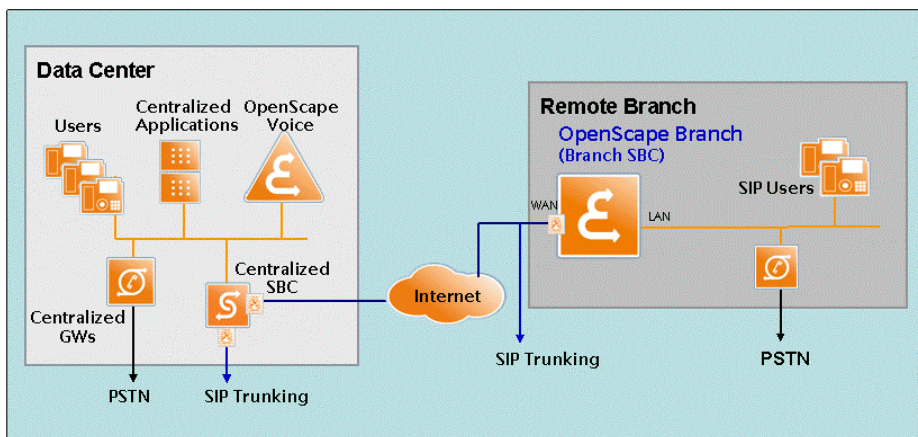


Branch SBC- Proxy Operating Mode



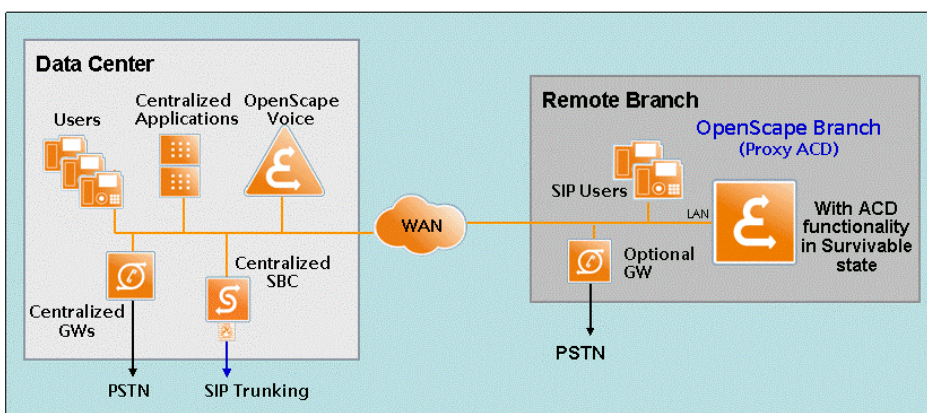
The SBC Proxy mode is for regular proxy connected via a private network and with Branch SBC SIP Trunking connectivity.

Branch SBC Operating Mode



The Branch SBC (Session Border Controller) mode is for deployments when a Branch is connected via a public network and require the use of SBCs.

Proxy ACD Operating Mode



The Proxy ACD (Automatic Call Distribution) mode is for regular proxy connected via a private network and the capability to provide ACD functionality during survivability.

5.1.1.1 How to Edit, Clone and Add Profiles

Proceed as follows to create a profile for OpenScape Branches. The operating mode and associated software version is selected when the Profile is created. Once OpenScape Branch profile is created the mode or version can not be modified. Profile configuration can now be applied to the profile.

Prerequisites

Adequate administrative permissions.

At least one 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 Branch** within the Navigation Bar in the Common Management Platform.

2) Select **Profiles List** under **Profiles** in the navigation tree.

The list with the profiles configured is displayed in the work area and the **Add...** button becomes active:

- **Profile Name**

This column displays the name associated with the profile.

- **Mode:**

This column displays the operation mode e.g. Proxy, Central SBC for the associated profile.

- **Version:**

This column displays the version and release of the OpenScape Branch this profile is to be used for.

3) To modify an existing profile, select the profile in the list and click the **Edit** button.

The **Edit - Profile** window appears.

4) To modify the profile name, enter the new name in the **Name** field (Value: up to 30 Alpha Numeric characters). The Mode and Version fields can not be modified.

5) Click the **OK** button to confirm the changes.

The **Edit - Profile** window disappears and the profile is modified.

6) To clone an existing profile, select the profile in the list and click the **Clone** button.

The **Clone - Profile** window appears.

7) To modify the profile name, enter the new name in the **Name** field. To modify the mode, select the mode in the **Mode** pull-down field. The version can be modified by selecting the version in the **Version** pull-down field.

8) Click the **OK** button to confirm the changes.

The **Clone - Profile** window disappears and the profile is cloned and saved. The new profile appears in the Profiles list in the work area.

- 9) To add a new profile, select the **Add...** button in the work area.
The **Add - Profile** window appears.
- 10) To add the new profile name, enter the name in the **Name** field.
- 11) Select one of the following operating modes **BranchSBC**, **SBC-Proxy**, **Proxy**, or **Proxy ACD**, in the **Mode** pull-down field.
- 12) Select the version in the **Version** pull-down field.
- 13) Click the **OK** button to confirm the changes.

The **Add - Profile** window disappears and the profile is saved. The new profile appears in the Profiles list in the work area.

NOTICE:

Once the profile is created the operating mode and version can not be modified.

This modification or addition of profiles is completed and applied to the system. Additional profile configuration can now be applied to the profile.

5.1.1.2 How to Display and Delete Profiles

Proceed as follows to display and delete existing OpenScape Branch profiles.

Prerequisites

Adequate administrative permissions.

At least one 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 Branch** within the Navigation Bar in the Common Management Platform.
- 2) Select **Profiles List** under **Profiles** in the navigation tree.

The list with the profiles configured is displayed in the work area and the **Add...** button becomes active:

- **Profile Name**

This column displays the name associated with the profile.

- **Mode:**

This column displays the operation mode e.g. Proxy, Central SBC for the associated profile.

- **Version:**

This column displays the version and release of the OpenScape Branch this profile is to be used for.

- 3) To delete an existing profile, select the respective profile in the list and click the **Delete** button.

If a profile has been deleted, the modification is completed and applied to the system.

5.1.1.3 How to Assign a Profile to an OpenScape Branch

The OpenScape Branch Assistant can administer OpenScape Session Border Controllers of the OpenScape Branch type. Thus it keeps a list of SBCs and Branch offices in its database. The "OpenScape Branch Overview" displays all known SBCs and Branch offices and provides a search function to find a particular one. A Profile can be assigned to an OpenScape "Branch".

Prerequisites

Adequate administrative permissions.

At least one 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) To assign a profile to an OpenScape Branch: Navigate to **Configuration tab > OpenScape Branch** 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).

If **All systems** is not currently selected, selecting All systems will display the **OpenScape Branch Overview** in the Work Area, with a current list of all known SBCs and Branch offices of all systems. If no SBCs or Branch offices are defined, the list is empty. If **All systems** was previously selected, then proceed to step 3.

3) Select **Branch Office list** in the Navigation Tree.

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

4) To view a list of SBCs and Branch Offices 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) Select a particular OpenScape Branch office in the work area by selecting the checkbox to the left of the OpenScape branch.

Menu buttons are set active in the Work Area with the following options: **Manage, Local Password..., Refresh Selected, Edit..., Delete.**

6) Select the **Edit...** button to edit the selected OpenScape Branch.

The Edit OpenScape Branch window opens.

7) Select the profile to be applied to the OpenScape Branch by selecting the profile in the **Profile Name** field pull-down.

- 8) Select the **OK** button to save the selected profile to the OpenScape Branch.

The Edit OpenScape Branch window closes and the profile is assigned to the OpenScape Branch.

The OpenScape Branch assistant database is updated.

5.2 Alarm Profile Configuration - Overview

The Alarms section under Profile Configuration allows to display and configure the trap destinations for the OpenScape Branch appliance.

The OpenScape Branch alarming application provides several configuration and administration functions. The Alarm profile configuration allows:

- Define trap destinations that alarms are sent to.
- Change the Reporting Class.

5.2.1 Alarm Settings

The Alarms section under Profile Configuration allows to display and configure the trap destinations for the OpenScape Branch appliance.

The OpenScape Branch Assistant Plug-in receives SNMP (Simple Network Management Protocol) traps from one or more OpenScape Branch devices. Alarms received by Branch devices will be stored in the Assistant database.

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 and Branch 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 }

```

5.2.1.1 How to Edit and Add Profile Trap Destinations

Already configured profile trap destinations can be edited and new trap destinations can be added.

Prerequisites

Adequate administrative permissions.

At least one OpenScape 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 Branch** within the Navigation Bar in the Common Management Platform.
- 2) Select a particular profile to edit from the **Select Profile** pull-down in the **Profiles** navigation area.
- 3) Navigate to **Configuration > Alarms** in the **Profiles** navigation area.

The **Alarms** window appears with the **Trap destinations** tab selected by default. The list of trap destinations configured for this profile 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 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 (Simple Network Management Protocol) trap. The same value is configured in the Alarm Table.

- 4) 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.

- 5) To modify the IP address used for sending the trap, enter the new address in the **IP Address** field.
- 6) To modify the port number of the internal port used for sending the trap, enter the new number in the **Port** field.

- 7) To modify the value used as reporting class, enter the new value in the range of 0...7 in the **Reporting class set** field. The same value is configured in the **Settings** tab representing the Alarm table.
- 8) To block or unblock a trap check or uncheck the **Blocked** checkbox.
- 9) Click the **OK** button to confirm the changes.

The **Edit trap destinations SNMP** window disappears and the **Alarms** window is displayed. Changes are temporarily saved in the administrator's login session.

- 10) Click the **OK** button to confirm the changes.

The **Alarms** window disappears and changes are temporarily saved in the administrator's login session.

- 11) Click the **Apply Changes** button in the main window to save the changes permanently.
- 12) To add a new trap destination, click the **Add...** button.

The **Add trap destination SNMP** window appears.

- 13) Enter the IP address used for sending the trap, in the **IP Address** field.
- 14) Enter the port number of the internal port used for sending the trap, in the **Port** field.
- 15) Select the value used as reporting class, in the range of 0...7 in the **Reporting class set** field. The same value is configured in the **Settings** tab representing the Alarm table.
- 16) To block or unblock a trap check or uncheck the **Blocked** checkbox.
- 17) Click the **OK** button to confirm the changes.

The **Add trap destinations SNMP** window disappears and the **Alarms** window is displayed. Changes are temporarily saved in the administrator's login session.

- 18) Click the **OK** button to confirm the changes.

The **Alarms** window disappears and changes are temporarily saved in the administrator's login session.

- 19) 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 selected profile.

5.2.1.2 How to Display and Delete Profile Trap Destinations

The configured trap destinations for a selected profile can be displayed and deleted.

Prerequisites

Adequate administrative permissions.

At least one 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 Branch** within the Navigation Bar in the Common Management Platform.
- 2) Select a particular profile to edit from the **Select Profile** pull-down in the **Profiles** navigation area.
- 3) Navigate to **Configuration > Alarms** in the **Profiles** navigation area.

The **Alarms** window appears with the **Trap destinations** tab selected by default. The list of trap destinations configured for this profile 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 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 (Simple Network Management Protocol) trap. The same value is configured in the Alarm Table.

- 4) 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.

- 5) Click the **OK** button to save the changes temporarily in the administrator's login session.
- 6) 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 profile.

5.3 Logging Profile Configuration - Overview

The logging profile configuration enables the administrator to modify and enter logging settings to be applied to multiple OpenScape Branches by assigning a profile. Continuous Tracing serve for analyzing the software, network, and configuration problems for maintenance purposes. Debugging and On Demand Tracing is not part of the Logging Profile Configuration.

5.3.1 Logging Profile for OpenScape Branch

Logging allows the administrator to set log levels for OpenScape Branch. A Profile can be configured to specify logging for a multiple OpenScape Branches.

Log Types

Not all logging can be set in a profile. The following logs are available for OpenScape Branches:

- Alarm History (view only):
Alarm history, showing all active or cleared alarms.
- Alarm Manager:
Log of Alarm manager application.
- B2BUA:
Log of Back to Back User Agent activity.
- Boot (view only):
Log of last boot.
- CAS:
Log of Centralized Answering Service.
- CDR:
Log of Call Detail Recording.
- Current process (view only):
A list of the current processes running on OpenScape SBC or Branch.
- Continuous Tracing:
Log of the Continuous Tracing application.
- Install/Update/Upgrade (view only):
Log from system installation, updates or upgrades (also includes language installation logs).
- ISDN (Not Applicable in a Profile):
Log of ISDN Layer 2 and Layer 3 messages of ISDN cards.
- Media Server:
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.
- SIP Server:
SIP stateful proxy or SBC application.
- Message Rate Control (view only):
Log from Message Rate Control application.
- Survivability Provider:
Log of Survivability provider application.
- SSM (SIP Services Module) (Not Applicable in a Profile):
Log of SIP Services
- System (view only):
Log of system events.
- Web server (view only):
Log of the local web server application

OpenScape Branch Applications and Functional Components

For the following OpenScape Branch and functional components log levels can be set:

- Alarm Manager
- B2BUA
- CAS
- CDR
- Continuous Tracing
- Media Server
- Process Manager
- RTP (Real-time Transport Protocol) Proxy
- SIP (Session Initiation Protocol) Server
- Survivability Provider

Log Levels

The following log levels are predefined and can be assigned individually to each OpenScape Branch application or functional component:

- 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.
- CAS MF Trace
- CAS stack trace
- CAS Trace
- CAS All

5.3.1.1 How to Edit Settings for Logs Associated with a Profile

Proceed as follows to assign log levels and fallback data associated with a profile assigned to one or more OpenScape Branch applications.

Prerequisites

Adequate administrative permissions.

At least one Branch office of the OpenScape Branch type 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 Branch** within the Navigation Bar in the Common Management Platform.
- 2) Select a particular profile to edit from the **Select Profile** pull-down in the **Profiles** navigation area.
- 3) Navigate to **Configuration > Logging** in the **Profiles** navigation tree area.
The **Logging** window appears with the **Settings** tab selected by default.

- 4) For each OpenScape Branch 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.
 - **CAS MF Trace**
Used for Channel Associated Signaling traces.
 - **CAS stack trace**
Used for Channel Associated Signaling traces.
 - **CAS trace**
Used for Channel Associated Signaling traces.
 - **CAS All**
Used for Channel Associated Signaling traces.
 - a) Select a log level for **SIP Server** (Session Initiation Protocol).
 - b) Select a log level for **B2BUA** (Back to Back User Agent).
 - c) Select a log level for **Media Server**.
 - d) Select a log level for **CDR** (Call Detail Recording).
 - e) Select a log level for **Process Manager**.
 - f) Select a log level for **Survivability Provider**.
 - g) Select a log level for **Alarm Manager**.
 - h) Select a log level for **RTP Proxy** (Real-time Transport Protocol).
 - i) Select a log level for **Continuous Tracing**.
 - j) Select a log level for **CAS** (Channel Associated Signaling)(valid for OSB V2).
- 5) 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.
- 6) Enter the IP address of the external Server to be used to store the log files in the **Syslog server** field.

- 7) 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.
- 8) Enter the fallback time in the **Fallback time** fields (format hh.mm, default value 16:30). This is the time of the day when the OpenScape Branch resets the continuous tracing configuration back to default.
- 9) Click the **OK** button to save the changes temporarily in the administrator's login session.
- 10) Click the **Apply Changes** button in the main window to save the changes permanently.

The settings for logging are completed and applied to the selected profile.

5.3.2 Profiles with Continuous Tracing

A profile can be configured to include Continuous Tracing. 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.

On-Demand Tracing is not associated with configuration of profiles.

Functional Sequence

The SIP (Session Initiation Protocol) traces or MGCP (Media Gateway Control Protocol) traces can be started, stopped or restarted by the OpenScape Branch 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,<OpenBranchNodeName>  
<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 Branch must be configured to connect to the trace server in order to transfer trace files in the **Logging > Continuous Tracing** tabsheet.

The configuration of the log levels must be configured in the **Logging > 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 Branch to OSV-TM (Trace Manager):

- Alarm History (view only),
- Alarm Manager,
- B2BUA,
- Boot (view only),
- CDR,
- Current process (view only),
- Continuous Tracing,
- Install/Update/Upgrade (view only),
- ISDN (Not Applicable in a Profile),
- Media Server,
- Process Manager,
- RTP (Real-Time Transport Protocol) Proxy,
- SIP Server,
- Message Rate Control (view only),
- Survivability Provider,
- SSM (SIP Services Module) (Not Applicable in a Profile),
- System (view only),
- Web server (view only)

The log levels of the following logs can be configured:

Log	Default Level
Alarm Manager	Error
B2BUA	Error
CDR	Error
Continuous Tracing	Error
Media Server	Error
Process Manager	Error
RTP Proxy	Error
SIP Server	Error
Survivability Provider	Error

On Demand Trace Configuration

The On Demand Trace is not associated with configuration of profiles.

5.3.2.1 How to Configure a Profile for Continuous Tracing

Proceed as follows to configure continuous tracing for an OpenScape Branch office.

Prerequisites

Adequate administrative permissions.

At least one Branch office of the OpenScape Branch type 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 Branch** within the Navigation Bar in the Common Management Platform.
- 2) Select a particular profile to edit from the **Select Profile** pull-down in the **Profiles** navigation area.
- 3) Navigate to **Configuration > Logging** in the **Profile** navigation tree area.
The **Logging** window appears with the **Settings** tab selected by default.
- 4) 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.
- 5) Enter the fallback time in the **Fallback time** fields (format hh.mm, default value 16:30). This is the time of the day when the OpenScape Branch resets the trace configuration back to default.
- 6) Select the **Continuous Tracing** tabsheet.
- 7) To activate the continuous tracing function, check the **Enable** checkbox.
- 8) Configure the general settings in the **General** field area as follows:
 - a) Enter the IP address 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.
- 9) 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** field.
 - c) Enter the password to identify on the SFTP server in the **Password** field.
- 10) Click the **OK** button to save the changes temporarily in the administrator's login session.

- 11) Click the **Apply Changes** button in the main window to save the changes permanently.

The settings for continuous tracing are applied to the profile selected.

5.4 Media Server Profile Configuration - Overview

The OpenScape Branch supports Media Server configuration used for tones, announcements, and conferencing. Profiles can be applied to configure multiple OpenScape Branches.

5.4.1 How to Configure a Profile for Media Server

Proceed as follows to configure media server general attributes, conference, announcement and media server adapter functions for an OpenScape Branch office profile.

Prerequisites

Adequate administrative permissions.

At least one Branch office of the OpenScape Branch type 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 Branch** within the Navigation Bar in the Common Management Platform.
- 2) Select a particular profile to edit from the **Select Profile** pull-down in the **Profiles** navigation area.
- 3) Navigate to **Configuration > Media Server** in the **Profile** navigation tree area.
The **Media Server** window appears.
- 4) To activate the media server function, check the **Enable** checkbox.
- 5) Enter the port number of the port which the media server uses to communicate with the call agent in the **Media Server Listen Port** field e.g. 2427, in the **General** work area.
- 6) Check the **Use FQDN** checkbox if the Fully Qualified Directory Number is to be used for identification.
- 7) Click the **Advanced features: Configure...** button associated to configure the Media Server Adapter and Converter.
The **Advanced features** window appears.
- 8) Enter the maximum duration of a MGCP transaction in SBC mode in seconds, in the **Time to Live** field, in the **Adapter** work area.
- 9) Click the **OK** button to save the changes temporarily in the administrator's login session.
- 10) Enter the maximum time a conference is allowed to be active in the **Maximum conference time (sec):** field, in the **Conference** work area.

Default value: 42800 seconds. If the time is to be unlimited, check the **Unlimited** checkbox.

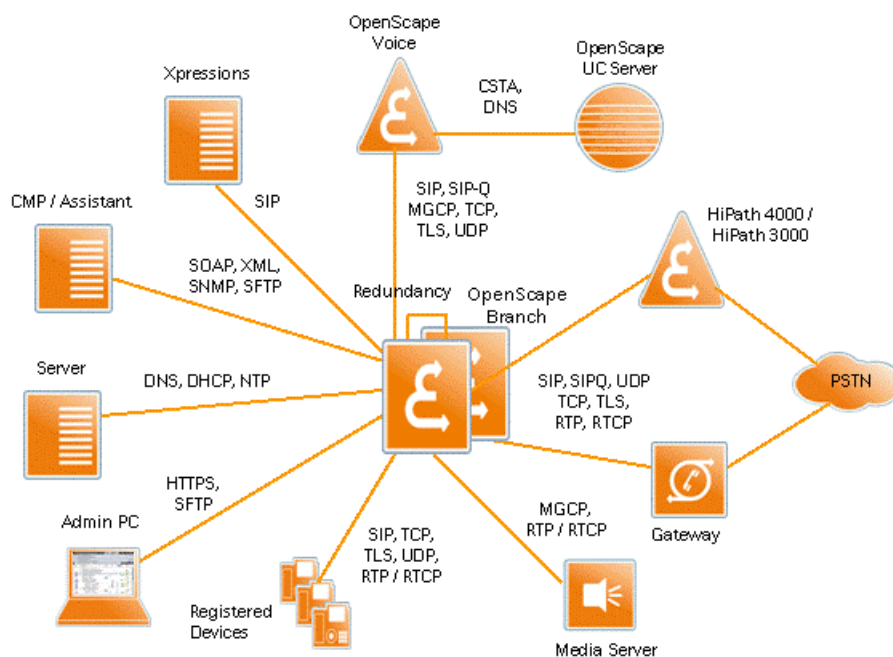
- 11) Enter the prefix required in SIP R-URI to access a Media Server conference in the **Prefix access code** field, in the Conference work area.
- 12) Enter the maximum time which an announcement session is allowed to be inactive in the **Maximum announcement time (sec):** field, in the Announcements work area. Default value: 1800 seconds. If the time is to be unlimited, check the **Unlimited** checkbox.
- 13) Enable or disable the **Stop announcement on DTMF** checkbox. If it this Check box is enabled, the announcement will stop when the Media Server receives a DTMF (Dual Tone Multifrequency).
- 14) Click the **OK** button to save the changes temporarily in the administrator's login session.
- 15) Click the **Apply Changes** button in the **Management** window to save the changes permanently.

The settings for media server are applied to the profile selected.

5.5 Network Services Profile Configuration - Overview

Network Services comprise configuration of interfaces, routing and traffic shaping as well as NTP (Network Time Protocol) and DNS (Domain Name System) settings. NTP and DNS settings can be configured in the profile assigned to multiple OpenScape Branches.

External Interfaces Overview



OpenScape Branch supported interfaces and protocols

- **NTP**

Network Time Protocol is used for synchronizing the time and date of the OpenScape Branch appliance in the network.

- **DNS**

The Domain Name System client can be configured in the OpenScape Branch in order to resolve FQDNs (Fully Qualified Domain Name). The OpenScape Branch system acts as DNS client. In the server section the OpenScape Branch Domain Name can be configured. A pre-defined configuration of the gateway can be done using the USB Stick Wizard.

- **DHCP**

(Not applicable to profile configuration)

The Dynamic Host Configuration Protocol server manages a pool of IP addresses and information about client configuration parameters such as default gateway, domain name, the DNS servers.

- **Interfaces**

(Not applicable to profile configuration)

Depending on the hardware used, up to four interfaces can be configured for the WAN (Wide Area Network), LAN (Local Area Network) and VLAN (Virtual LAN) connections. A pre-defined configuration of interfaces can be done using the USB Stick Wizard.

- **Routing**

(Not applicable to profile configuration)

Routing regarding the network services comprise the configuration of the default gateway address and IP routes.

- **Redundancy**

(Not applicable to profile configuration)

There are various options for redundancy used to protect connectivity through the customers network.

- **Traffic Shaping**

(Not applicable to profile configuration)

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.

5.5.1 How to Configure System NTP Profile Settings

Proceed as follows to configure a profile with time and date settings. The profile can then be assigned to multiple OpenScape Branch appliances using a NTP (Network Time Protocol) server.

Prerequisites

Adequate administrative permissions.

At least one 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 Branch** within the Navigation Bar in the Common Management Platform.
- 2) Select a particular profile to edit from the **Select Profile** pull-down in the **Profiles** navigation area.
- 3) Navigate to **Configuration > Network Services** in the **Profiles** navigation tree area.

The **Network Services** window appears with the **NTP** tab selected by default.

- 4) Select the time zone to be used in OpenScape Branch, e.g. GMT (Greenwich Mean Time), from the **Time zone** selection list.
- 5) Check the **Enable local NTP server** checkbox to activate the local NTP server. In this case both, manual and synchronized time settings are allowed.
- 6) Click the **OK** button to store the changes temporarily in the administrator's login session.

The **Network Services** dialog disappears.

- 7) Click the **Apply changes** button in the main window, work area.

The settings for NTP are applied on the Profile.

5.5.2 Profile Configuration of DNS Server

DNS Server attributes can be configured in a profile to be used by multiple OpenScape Branches. Depending on the network environment the OpenScape Branch is operating in, different configurations of the DNS (Domain Name System) server settings apply.

There are three possibilities of handling the names using OpenScape Branch DNS Server:

- DNS Server acts a slave of a master DNS outside of OpenScape Branch 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 Branch 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

In version 7 and later, the DNS server can be configured as a Master via customized configuration. During custom configuration, in the **DNS** Configuration tab of the **Network Services** window; the Named.com file is uploaded with definitions for the Master DNS configuration. Depending on the custom configuration, several files may require upload e.g. zones configuration. The configuration will be preserved in case of upgrades. In the case of re-installation of OpenScape Branch, files must be exported outside of the server to be used during re-installation.

5.5.2.1 How to Configure a Profile for System DNS Settings

Proceed as follows to configure the DNS (Domain Name System) settings for a Profile to be assigned to OpenScape Branch appliances.

Prerequisites

Adequate administrative permissions.

At least one 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 Branch** within the Navigation Bar in the Common Management Platform.
- 2) Select a particular profile to edit from the **Select Profile** pull-down in the **Profiles** navigation area.
- 3) Navigate to **Configuration > Network Services** in the **Profiles** navigation tree area.

The **Network Services** window appears with the **NTP** tab selected by default.

- 4) 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.

- 5) To configure the DNS server list click the **Configure** button associated with 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.

- 6) Use one of the following options:

- To add a server to the list enter an IP address of a new DNS server in the address field and click the **Add** button.
- Select an IP address in the list and click the **Delete** button to remove a server from the list.

- 7) Click the **Close** button to go back to the **Network Services** window.

- 8) 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.

- 9) Use one of the following options:

- To add an alias to the list, enter an **IP address** 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.

- 10) Click the **Close** button to go back to the **Network Services** window.

- 11) Enter the OpenScape Branch domain name in the **OpenScape Branch Domain Name** field, e.g. *company.com*, in the **Server work area**.

- 12) To enable the internal DNS Server service check the **Enable DNS** checkbox.

- 13) To configure the forward IPs list, click the **Configure** button associated with 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.

- 14) Use one of the following options:
 - To add an IP address to the list, enter an IP address 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.
- 15) Click the **Close** button to go back to the **Network Services** window.
- 16) 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.
- 17) Select the zone type (Values: **Slave** or **Forward**) from the **Type** selection list.
- 18) Enter the zone domain name in the **Zone name** field.
- 19) Enter the IP address 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.
- 20) Enter the file name to read the server data from in the **File name** field.
- 21) Click the **OK** button to close the **Add Zone** dialog.
- 22) Click the **OK** button to store the changes temporarily in the administrator's login session.

The **Network Services** window disappears.
- 23) Click the **Apply changes** button in the main window to save the changes permanently.

The DNS Server settings are applied on the Profile.

5.6 Security Profile Configuration - Overview

The security profile configuration enables the administrator to modify and enter security settings to be applied to multiple OpenScape Branches by assigning the profile. Security profile configuration allows configuration of Message Rate Control settings and firewall settings. Additional Security settings must be done at the OpenScape Branch specific levels.

The OpenScape Branch application 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)

Open VPN can be used to provide a secure link to an OpenScape Voice system in the main office.
 - IPsec (Internet Protocol Security)

IPsec can be used to provide a secure link to an OpenScape Voice system in the main office. IPsec may also be used to secure the MGCP signaling stream from an external media server.

OpenScape Branch-SBC Security Strategy

The two main goals of OpenScape SBC and Branch 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.

5.6.1 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 Branch 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.

5.6.1.1 How to Configure a Profile for Message Rate Control Rules

Proceed as follows to configure a profile for the network intrusion prevention and detection system Message Rate Control.

Prerequisites

Adequate administrative permissions.

At least one 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 Branch** within the Navigation Bar in the Common Management Platform.
- 2) Select a particular profile to edit from the **Select Profile** pull-down in the **Profiles** navigation area.
- 3) Navigate to **Configuration > Security** in the **Profiles** navigation tree area.
The **Security** window appears with the **Message Rate Control** tab selected by default.
- 4) To activate Message Rate Control, check the **Message Rate Control** checkbox.
- 5) 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 (default = 20000).
- 6) Enter the blocking time of the IP address in seconds in the **Block period** field (default = 60).
- 7) The **IP address** list, in the white list work area, 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 enter the address in the address field and click the **Add** button.
 - Select an IP address from the list and click the **Delete** button to delete an IP address from the list.
- 8) Click the **OK** button to store the changes temporarily in the administrator's login session and close the **Security** window.
The **Security** dialog disappears.
- 9) Click the **Apply changes** button in the main window, work area.

The Message Rate Control rules are applied on the selected Profile.

5.6.2 Firewall Profile Configuration

A firewall is installed on the OpenScape Branch system in order to protect access to systems behind it, limiting their exposure to the Internet. A profile can be configured with firewall attributes. The profile can then be assigned to multiple OpenScape SBCs or Branches.

Filter Rules

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.

NAT Traversal — Masquerading

Masquerading masks the LAN addresses in the WAN to hide the entire internal address space. Masquerading is only possible for Session Border Controllers e.g., the OpenScape Branch system works in SBC (Session Border Controller) mode.

Port Forwarding

Port forwarding is only possible for Session Border Controllers e.g. the OpenScape Branch system is configured in SBC (Session Border Controller) mode.

Allowing/Blocking Services

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 Branch and outgoing connections (Devices under OpenScape SBC and Branch trying to access WAN services).

NOTICE: OpenScape supports SNMP to send alarms from the OpenScape Branch to the CMP. The OSB supports SNMP Gets of MIB-II however, Set SNMP operations are not supported.

Allowing/Blocking IPs/Ports (OSB V1R3 and later versions only, and OpenScape SBC V1 and later versions)

Configuring a "black" and a "white" list allows to block or allow incoming and outgoing WAN network connections for a specific IP/Port.

5.6.2.1 How to Configure a Profile for a Firewall

Proceed as follows to configure a profile with firewall rules.

Prerequisites

Adequate administrative permissions.

At least one 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 Branch** within the Navigation Bar in the Common Management Platform.
- 2) Select a particular profile to edit from the **Select Profile** pull-down in the **Profiles** navigation area.
- 3) Navigate to **Configuration > Security** in the **Profiles** navigation tree area.
The **Security** window appears with the **Message Rate Control** tab selected by default.
- 4) Select the **Firewall** tab.

- 5) To activate masquerading, check the **Enable masquerading** checkbox. 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

- 6) 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. (Values: DNS, FTP, HTTPS, NTP, PING, SNMP, SSH, TELNET)
- 7) Use the checkboxes in the **Incoming WAN VoIP connections** field area to enable protocols of the incoming VoIP connections. (Values: MGCP, RTP/sRTP, SIP, TLS)
- 8) 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.

- 9) 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.

- 10) Enter the IP address to be blocked in the **IP address/Subnet** field.

NOTICE: Please note that an IP address can either belong to the white list OR the black list.

- 11) Enter the port number to be blocked in the **Port** field. If the **Port** field is empty, all ports will be blocked.
- 12) Click the **OK** button to close the **Add Black List** window.
- 13) Click the **OK** button to close the **Black List** window.
- 14) 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.

15) 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.

16) Enter the IP address to be blocked in the **IP address/Subnet** field.

NOTICE: Please note that an IP address can either belong to the white list OR the black list.

17) Enter the port number to be blocked in the **Port** field. If the **Port** field is empty, all ports will be blocked.

18) Click the **OK** button to close the **Add White List** window.

19) Click the **OK** button to close the **White List** window.

20) Click the **OK** button to store the changes temporarily in the administrator's login session.

The **Security** dialog disappears.

21) Click the **Apply changes** button in the main window, work area.

The firewall settings are applied to the profile.

5.6.3 Radius

5.6.3.1 How to Enable RADIUS User Authentication

Proceed as follows to enable an OpenScape Branch system for user authentication via a central pair of RADIUS servers. This eliminates the need to manage individual accounts on each OpenScape for networks with many OSBs.

Prerequisites

Adequate administrative permissions.

The OpenScape Branch is configured and in operation.

The RADIUS servers are configured and in operation.

IMPORTANT:

A Web or CLI user who is defined on the RADIUS server does not need to be defined on the OSB. When a user who is not defined on the OSB logs in via RADIUS, that user will be granted the privileges of the default 'service' user. This will then allow the user logging in to perform the type of functions that the service user can perform, as defined in section. If a user attempts to log in to the Web or CLI application using a username that is only defined on the RADIUS servers, and the

RADIUS servers are down, then login will fail. The user will need to attempt to login locally using one of the default usernames.

Step by Step

- 1) Login to the OSB local management portal via local administrative user and password.
- 2) Navigate to **Security > RADIUS**.
The **RADIUS** window appears.
- 3) Set the **Enable RADIUS** checkbox.
- 4) Enter the following information associated with the two RADIUS servers:
 - a) **Address** - the IP Address of server.
 - b) **Port** - the IP Port used by RADIUS server (normally 1812).
 - c) **Secret** - the security message digest used by the RADIUS server.
 - d) **Timeout** - for logins via the RADIUS server.
- 5) Set the **Enable RADIUS Accounting** checkboxes for the management interfaces as required by the specific customer deployment, e.g. for statistical purposes.
 - a) **CLI**
 - b) **SSH**
 - c) **WEB**
- 6) Click the **OK** button to store the changes temporarily in the administrator's login session.
The **System** dialog disappears.
- 7) Click the **Apply changes** button in the main window.
The user authentications will now be performed by the RADIUS servers.

5.6.4 Custom

5.6.4.1 How to Configure Custom Security Settings

Proceed as follows to configure a profile with firewall rules.

Prerequisites

Adequate administrative permissions.

At least one 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 Branch** within the Navigation Bar in Common Management Portal.
- 2) Select a particular profile to edit from the **Select Profile** pull-down in the **Profiles** navigation area.

- 3) Navigate to **Configuration > Security** in the **Profiles** navigation tree area.
The **Security** window appears with the **Message Rate Control** tab selected by default.
- 4) Select the **Custom** tab.
- 5) To enable only the fields on the Custom tab check the checkbox called **Enable only the fields below (all other OSB profile fields will be disabled)** checkbox and the three other tabs, **Message Rate Control**, **Firewall**, and **Radius** will be greyed out.
- 6) Use the data entry boxes in the **User Passwords** field area to enter and/or change password information. For each type of password: root, administrator, ACD, guest, and service, there are data fields for the entry of **Current password, New password, Confirm new password, for each of above password types**. Standard password creation and syntax rules apply.
- 7) Use the data entry boxes in the **Partner Passwords** field area to enter and/or change password information. For each type of password: assistant, cdr, and redundancy, there are data fields for the entry of **Current password, New password, Confirm new password, for each of above password types**. It should be noted that if one of these passwords is changed then the Password at the partner device must be changed as well to ensure proper operation. Standard password creation and syntax rules apply.
- 8) Use the data entry boxes for entering the **SNMP Community String** information which includes the SNMP Community String and the SNMP Community IP Address.
- 9) To select and upload one or more Certificate Files click on the Choose File button. The following types of Certificate Files can be selected for upload: Local Client certificate file, Local server certificate file, Local CA file, Remote CA file, and the Local Key file.
- 10) To enter Password Policy information scroll down to the bottom of the Custom tab area and enter the following data: **Password Aging Max Days, Minimum Three Class length, Minimum Four Class length, Password Iteration NR, and Password Iteration Length**.
- 11) Click the **OK** button to store the changes temporarily in the administrator's login session.
The **Security** dialog disappears.
- 12) Click the **Apply changes** button in the main window, work area.

The firewall settings are applied to the profile.

5.7 Survivability Profile Configuration - Overview

The configuration of Profiles is currently not supported. Survivability is the capability of a network to maintain service continuity in the presence of faults within the network. Profiles allows the capability to configure survivability for

Call Detail Recording and Music On Hold to be applied to multiple OpenScape Branches.

5.7.1 How to Configure Profiles for CDR Handling in Survivability

Proceed as follows to configure profile settings for CDR (Call Detail Records) handling when the OpenScape Branch operates in survivability mode.

Prerequisites

Adequate administrative permissions.

At least one 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 Branch** within the Navigation Bar in the Common Management Platform.
- 2) Select a particular profile to edit from the **Select Profile** pull-down in the **Profiles** navigation area.
- 3) Navigate to **Configuration > Survivability** in the **Profiles** navigation tree area.
The **Survivability** window appears with the **Call Detail Records** tab selected by default.
- 4) To enable the call detailed tickets being stored during survivability, check the **Enable Ticket Generation** checkbox.
- 5) Enter the IP address or FQDN of the primary billing server in the **Hostname** field, for the Primary billing server.
- 6) Enter the user name for the primary billing server account to access the server in the **Username** field, for the Primary billing server.
- 7) Enter the password for the Primary billing server account used to access the server in the **Password** field.
- 8) Enter the password for the Primary billing server again in the **Confirm password** field.
- 9) Enter the IP address or FQDN of the secondary billing server in the **Hostname** field for the Secondary billing server.
- 10) Enter the user name for the secondary billing server account to access the server in the **Username** field, for the Secondary billing server.
- 11) Enter the password for the Secondary billing server account used to access the server in the **Password** field.
- 12) Enter the password for the Secondary billing server again in the **Confirm password** field.
- 13) Enter the maximal number of CDR records stored in a single billing file in the **Max number of records** field, in the **General & SFTP Billing File Settings** work area.
- 14) Enter the time interval for the billing files to be stored in the permanent storage device (FLASH memory or DISK) in the **Max time interval (min)** field.

- 15) Enter the maximal size in kbytes of the billing file in the **Max file size (kbytes)** field.
- 16) Enter the transfer method in the **Transfer method** field. This defines the method used to transfer the files to the Billing Server. In **push** mode OpenScape Branch will send the billing files to the billing server. In **pull** mode OpenScape Branch stores the billing files and the billing server is responsible for retrieving the billing files via SFTP. Default value: push
- 17) Enter the port used for SFTP when accessing the remote billing server in the **Port** field.
- 18) Enter the time duration OpenScape Branch shall wait before re-attempting an SFTP transfer in push mode in the **Re-attempt timer (min)** field. Allowed min value: 1, allowed max value: 1440 (1 day), default value: 5.
- 19) To choose the "allow file overwrite" option, check the **Allow file overwrite** checkbox. Billing files may be overwritten.
- 20) Click the **OK** button to store the changes temporarily in the administrator's login session.
The **Survivability** dialog disappears.
- 21) Click the **Apply changes** button in the main window.

The settings for CDR in survivability mode are applied on the OpenScape Branch system.

5.7.2 How to Configure Profiles for Music on Hold Handling in Survivability

Proceed as follows to configure profile settings for Music On Hold (MOH) handling when the OpenScape Branch operates in survivability mode.

Prerequisites

Adequate administrative permissions.

At least one 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 Branch** within the Navigation Bar in the Common Management Platform.
- 2) Select a particular profile to edit from the **Select Profile** pull-down in the **Profiles** navigation area.
- 3) Navigate to **Configuration > Survivability** in the **Profiles** navigation tree area.

The **Survivability** window appears with the **Call Detail Records** tab selected by default.

- 4) To enable music on hold during survivability for external calling parties in the public network, check the **Enable MOH** checkbox.
- 5) To enable music on hold during survivability for internal calling subscribers in the private network, check the **Enable MOH for Subscribers** checkbox.

The Enable MOH option must be enabled to select this option.

- 6) Click the **OK** button to store the changes temporarily in the administrator's login session.

The **Survivability** dialog disappears.

- 7) Click the **Apply changes** button in the main window.

The settings for CDR in survivability mode are applied on the OpenScape Branch system.

5.8 System Profile Settings - Overview

System settings mainly serve to configure the protocols and password settings of an OpenScape Branch and enables the administrator to perform some service tasks. These settings apply to specific OpenScape Branches.

NOTICE:

System settings are not applicable to profile configuration.

5.9 Voice over Internet Protocol Profile Configuration - Overview

A Profile can be configured with certain Voice Over IP attributes. The profile can then be assigned to multiple OpenScape Branches. VoIP (Voice over Internet Protocol) is a transmission technology for delivery of voice communications over IP networks such as the Internet.

OpenScape Branch Assistant allows to configure profile settings for "Voice over IP" telephony, the communication system and periphery for OpenScape Branches.

General Configuration

Some functionality and configuration is specific to OpenScape Branch. Certain areas of configuration are not applicable to profiles.

- Supported deployment modes: Proxy, Proxy ACD, SBC-Proxy, BranchSBC.
- Listening Ports
- Port Mapping
- Quality of Service
- SIP Header Manipulation (applies in survivability mode)
- SIP Routing
- Error Codes
- Backup Data Channel (this feature is only available for OSB V1R3 and later versions) (Not applicable for profiles)
- Remote Endpoints and Gateways (Not applicable for profiles)
- SIP Service Provider Profiles (this feature is only available for OSB V1R3 and later versions) (Not applicable for profiles)
- Media Servers (Not applicable for profiles)
- MS Profiles (Not applicable for profiles)

Communication System Configuration

The following are not applicable for configuration of profiles.

- 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 for the profile to control the system performance of OpenScape Branch appliances.

Throttling, Registration Expiry and Remote Subscribers

Throttling and registration expiry can be configured in the profile for an OpenScape Branch appliance. Remote Subscriber firewall, domain and emergency service settings do not apply to profile configuration.

5.9.1 SIP Header Manipulation

When the OpenScape Branch system operates in survivability mode, the SIP headers are modified according to rules. SIP header manipulation is not applied for emergency numbers called.

Parameters to Define Rules

To define rules for the header manipulation, the following parameters are available:

- 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.
- Header
Defines the SIP header the rule applies for.
- Delete/insert position
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
Defines the digits to be inserted at the defined position.

- Add prefix

This parameter is used to set the prefix to be added to the digits on header.

- Replace all with

The digits to replace all header digits.

More Than One Rule Matches

If the header digits of a message match more than one rule, only the best matching rule is applied to this header. The best matching rule is the rule that matches the header digits and complies the following criteria, from the higher priority to the lower priority:

- It has the biggest "Match digits" length.
- It has the smallest "Match position" value.
- It has the biggest "Match digits" value in lexicographical order.

A rule for header manipulation may look as follows:

Row	Match digits	Match position	Header	Delete/Insert position	Number of digits to delete	Insert digits	Add prefix	Replace all with
1	53	4	R-URI		1			5558880000
2	5617190		R-URI		6		555888	
3	305	0	R-URI	1	2	44		
4	52	0	R-URI				555888	

The following table describes what OpenScape Branch will do based on the SIP manipulation rules in this examples (rules priority applies for best match from left to right):

Row	
1	OpenScape Branch will try to match 53 to the called number starting on digits position 4 (count 0 through 4 from the left of the called number). If a match is found OpenScape Branch will replace all digits with 5558880000. User Dials 7777535000 --> match (Position 4), after translation: 5558880000.
2	OpenScape Branch will try to match 561719 to the called number starting on digits position 0. If a match is found OpenScape Branch will delete 6 digits and add prefix 555888. User Dials 5617195200 --> match (position 0), after translation 5558885200.
3	OpenScape Branch will try to match 305 to the called number starting on digits position 0. If a match is found OpenScape Branch will delete 2 digits from position 1 and then append 44. User Dials 3053333240 --> match (position 0), after translation 3443333240.

Row	
4	OpenScape Branch will try to match 52 to the called number starting on digit position 0. If match is found OpenScape Branch will add prefix 555888. User Dials 523333240 --> match (position 0), after translation 555888523333240.

5.9.1.1 How to Configure Profile SIP Header Manipulation Rules

Proceed as follows to configure a profile with SIP (Session Initiation Protocol) header manipulation rules on how the SIP headers are changed during Survivability Mode (except from an Emergency Number).

Prerequisites

Adequate administrative permissions.

At least one 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 Branch** within the Navigation Bar in the Common Management Platform.
- 2) Select a particular profile to edit from the **Select Profile** pull-down in the **Profiles** navigation area.
- 3) Navigate to **Configuration > VoIP** in the **Profiles** navigation tree area.
The **Voice over IP** window appears with the **General** tab selected by default.
- 4) Click the **Manipulation...** button in the **SIP** field area.
The **VoIP SIP Header Manipulation** window appears. The rules are displayed in a list.
- 5) 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.
- 6) 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.
- 7) 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.

- 8) Select the SIP header the rule applies for in the **Header** selection list. Options area as follows:
 - R-URI
 - From
 - P-Asserted Identity
 - P-Preferred Identity
 - Diversion
- 9) 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".
- 10) 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.
- 11) Enter the digits to be inserted at the defined position in the **Insert digits** field.
- 12) Enter the prefix to be added to the digits on the header in the **Add prefix** field.
- 13) Enter the digits to replace all header digits with in the **Replace all with** field.
- 14) Select the Call Type that digit manipulation applies for in the **Call Type** selection list. Options area as follows:
 - All
 - PSTN-SIP
 - SIP-PSTN
 - SIP-SIP
- 15) 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.
- 16) Click the **OK** button to store the changes temporarily in the administrator's login session.
The **Voice over IP** dialog appears.
- 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.

The setting of SIP manipulation is applied on the OpenScape Branch system.

5.9.2 SIP Routing Rules

SIP (Session Initiation Protocol) Routing serves for the routing of SIP messages during survivability mode. Therefore rules have to be defined.

SIP calls can be rerouted if:

- A gateway cannot process a connection request. The calls can be of type offnet (to the PSTN via a SIP gateway) or on-net (to another SIP or SIP-Q network such as a QSIG (QSIG=Q (reference point) Signaling) gateway or the OpenScape UC Application).
- A WAN failure occurs. SIP and SIP-Q calls between subscribers are rerouted through the PSTN (Public Switched Telephone Network).
- A SIP response code indicates a bandwidth restriction.

Functional Description

The OpenScape Voice provides rerouting of SIP calls for unreachable gateways or subscribers in the case of WAN failure or after receipt of a SIP response code indicating an error condition such as a bandwidth restriction (e.g. 606). The SIP calls can be of type off-net (to the PSTN via a SIP gateway), on-net (to another SIP network, such as OpenScape) or to a registered SIP subscriber. A rerouting timer provides rerouting in case no response is received from the SIP gateway, SIP server or SIP subscriber after an INVITE has been sent to them. The timer is configured under Survivability, Timers and Thresholds.

Requirements

Rerouting for SIP subscribers relies on particular conditions:

- The called subscriber has to be registered from a survivable branch (e.g. OpenScape Branch).
- The called subscriber has to reside in that survivable branch. This means that the called subscriber is registered with its provisioned 'Survivable' SIP Proxy endpoint.
- The called subscriber has a 'Survivable' SIP Endpoint (SIP Gateway - no SIP Proxy) provisioned as associated Endpoint and it is registered directly with the OpenScape Voice. (in this case the first two points are not necessary).
- The called subscriber has to have a valid public E.164 number.
- The calling subscriber must be calling from a different survivable branch or must be directly registered with the OpenScape Voice.

Parameters to Define Rules for Routing

To define rules for the SIP routing, the following parameters are available:

- Source IP (Internet Protocol) address
This parameter defines the Source IP address of the message to be routed.
- Condition (error codes)

The reply codes are used to reroute the messages. The following codes can be assigned:

Error Code	Related error
300	Multiple Choices
301	Moved Permanently
302	Moved Temporarily
305	Use Proxy
380	Alternative Service
401	Unauthorized
402	Payment Required

Error Code	Related error
403	Forbidden
404	Not Found
405	Method Not Allowed
406	Not Acceptable
407	Proxy Authentication Required
408	Request Timeout
410	Gone
413	Request Entity Too Large
414	Request URI Too Large
415	Unsupported Media Type
416	Unsupported URI Scheme
420	Bad Extension
421	Extension Required
422	Session Interval Too Small
423	Interval Too Brief
480	Temporarily Unavailable
486	Busy Here
488	Not Acceptable Here
493	Undecipherable
500	Server Internal Error
501	Not Implemented
502	Bad Gateway
503	Service Unavailable
504	Server Time Out
600	Busy Everywhere
606	Not Acceptable

- Destination IP
This parameter defines the destination IP address of the message to be routed.
- Destination tag
This parameter defines a tag to be added to rerouted SIP headers.
- Destination type
The destination type determines the type of route used for the rule.
- Priority
The priority defines which route will be used first in case of more than one route applies.

5.9.2.1 How to Configure Profile SIP Routing Rules

Proceed as follows to display and configure SIP (Session Initiation Protocol) routing rules which modify the routing of SIP messages during survivability mode.

Prerequisites

Adequate administrative permissions.

At least one 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 Branch** within the Navigation Bar in the Common Management Platform.
- 2) Select a particular profile to edit from the **Select Profile** pull-down in the **Profiles** navigation area.
- 3) Navigate to **Configuration > VoIP** in the **Profiles** navigation tree area.
The **Voice over IP** window appears with the **General** tab selected by default.
- 4) Click the **Routing...** button in the **SIP** field area.
The **SIP Routing** window appears. The rules are displayed in a list.
- 5) 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 SIP Routing** window appears.
- 6) Enter the source IP address of the message to be routed in the **Source IP** field.
- 7) Enter the conditions to reroute the messages in the **Condition (error codes)** field. The SIP response (error) codes have to be separated by commas.
- 8) Enter the destination IP address of the message to be routed in the **Destination IP/FDQN** field.
- 9) Enter the destination tag in the **Destination Port** field. The destination port is to be rerouted to.
- 10) Select the destination transport type in the **Destination Transport** selection list. The destination transport can be **TCP**, **UDP** or **TLS**.
- 11) Enter the destination tag in the **Destination tag** field. The destination tag is added to rerouted SIP headers.
- 12) Select the destination type in the **Destination type** selection list.
The destination type determines the type of route used for the rule. A destination type can be "Voice Mail", "Gateway" or "other SIP EP (Endpoint)".
- 13) Click the **OK** button to go back to the **SIP routing** window.
The **SIP Routing** window appears. The new rule is displayed in the list.

- 14) Click the **OK** button to store the changes temporarily in the administrator's login session.

The **Voice over IP** dialog disappears.

- 15) Click the **OK** button to store the changes temporarily in the administrator's login session.

The **Voice over IP** dialog disappears and the **Main** window.

- 16) Click the **Apply changes** button in the main window.

The configuration of the SIP routing rules is applied on the OpenScape Branch system.

5.9.2.2 How to View and Configure Profile SIP Error Codes

Proceed as follows to configure in the profile, error codes for rerouting during normal mode and survivability mode.

Prerequisites

Adequate administrative permissions.

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

The connection to the OpenScape Voice system is up.

The settings for survivability have been configured accordingly.

Step by Step

- 1) Navigate to **Configuration tab > OpenScape Branch** within the Navigation Bar in the Common Management Platform.
- 2) Select a particular profile to edit from the **Select Profile** pull-down in the **Profiles** navigation area.

- 3) Navigate to **Configuration > VoIP** in the **Profiles** navigation tree area.

The **Voice over IP** window appears with the **General** tab selected by default.

- 4) Click the **Error Codes...** button in the **SIP** field area.

The **SIP Error Codes (View)** window appears displaying the error codes:
The **Enable rerouting in survivable mode** column and **Enable rerouting in normal mode** column indicates when the error codes will be used for rerouting.

- 5) To enable or disable “all” error codes for normal or survivable mode four buttons are provided:
 - a) Select the **Enable all in survivable mode** button to enable “all” error codes for survivable mode rerouting.
 - b) Select the **Enable all in normal mode** button to enable “all” error codes for normal operating mode.
 - c) Select the **Disable all in survivable mode** button to enable “all” error codes for survivable mode rerouting.
 - d) Select the **Disable all in normal mode** button to enable “all” error codes for normal operating mode.

The updated error codes are displayed.

- e) Proceed to Step 7 to temporarily save changes.
- 6) To configure individual error codes for rerouting, proceed as follows:
 - a) Select the radio button of the error code to be configured for rerouting.
 - b) Click the **Edit...** button.

The **SIP Error Codes (Configure)** subwindow appears.

- c) Check the **Enable rerouting in survivable mode** checkbox to enable.
- d) Check the **Enable rerouting in normal mode** checkbox to enable.
- e) Click the **OK** button to temporarily save the data and go back to the **SIP Error Codes (View)** window. The updated error code is displayed.

The updated error code is displayed.

- f) Select another error code if applicable and configure.
- 7) Click the **OK** button to go back to the **Voice over IP** window.
- 8) Click the **OK** button to store the changes temporarily in the administrator’s login session.

The **Voice over IP** dialog disappears.

- 9) Click the **Apply changes** button in the main window.

The configuration of the SIP error codes are applied on the OpenScape Branch system.

5.9.3 SIP VoIP Port Profile Configuration and Display

A profile can be configured with SIP VoIP settings. The profile can then be assigned to multiple OpenScape Branches.

Requirements

SIP port profile configuration and displays are as follows:

- Configure VoIP setting for ports

5.9.3.1 How to Configure Profile VoIP SIP Settings

Proceed as follows for profile configuration of ports in the LAN (Local Area Network) where OpenScape Branch will be listening, the Options source port, and the port mapping parameters.

Prerequisites

Adequate administrative permissions.

At least one 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 Branch** within the Navigation Bar in the Common Management Platform.
- 2) Select a particular profile to edit from the **Select Profile** pull-down in the **Profiles** navigation area.
- 3) Navigate to **Configuration > VoIP** in the **Profiles** navigation tree area.
The **Voice over IP** window appears with the **General** tab selected by default.
- 4) Enter the port number of each protocol TCP (Transmission Control Protocol), UDP (User Datagram Protocol), TLS (Transparent LAN Service) in the **TCP**, **UDP**, and **TLS** fields, in the **Listening ports** work area.
TCP:5060,UDP:5060, TLS:5061
- 5) Leave this field blank or enter the TCP Listening port. If the OpenScape Branch is connected to an OpenScape Voice which is not on the latest patch set (OSV V6: < PS23; OSV V7: < PS8), enter the Options source port number in the Options Source Port field, in the Listening ports field area. Enter a different port than the ports entered in step 4) (e.g., 5062). This is the port that needs to be set as "Trusted" in the OpenScape Voice configuration for the OpenScape Branch. Other messages using different ports will still get challenged.
- 6) Enter the RTP (Real-time Transport Protocol) port range to be used in RTP traffic in the **RTP ports min/max** fields, in the **Port Mapping** work area. The fields are only enabled in SBC (Session Border Controller) mode.
- 7) Enter the disconnection timer for non RTP activity in the **Time to live** field, in the **Port Mapping** work area. The field is only enabled in SBC mode.
- 8) Enter the SIP port range to be used in SIP messages in the **SIP ports min/max** fields, in the **Port Mapping** work area. 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 to the Profile.

5.9.4 Gateways Profile Configuration and Display

A profile can be configured with Gateway settings. The profile can then be assigned to multiple OpenScape Branches.

Requirements

Gateway profile configuration and displays are as follows:

- Configure general gateway settings
- Configure SIP Service Provider Profiles
- Configure SIP Manipulation rules within a SIP Service Provider Profile

5.9.4.1 How to Configure a Profile with Gateway General Settings

Proceed as follows to configure a Profile with general gateway settings.

Prerequisites

Adequate administrative permissions.

At least one 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 Branch** within the Navigation Bar in the Common Management Platform.
- 2) Select a particular profile to edit from the **Select Profile** pull-down in the **Profiles** navigation area.
- 3) Navigate to **Configuration > VoIP** in the **Profiles** navigation tree area.
The **Voice over IP** window appears with the **General** tab selected by default.
- 4) Enter the DNS refresh interval time (minutes) in the **DNS Refresh Interval** field in the **Gateways** field area. This timing is used only for gateways/trunks configured using FQDNs.
- 5) Click the **OK** button to store the changes temporarily in the administrator's login session.

The **Voice over IP** dialog disappears.

- 6) Click the **Apply changes** button in the main **Management** window.

The configuration of gateways is applied on the OpenScape Branch Profile.

5.9.4.2 How to Configure a Profile with Gateway SIP Service Provider Profiles

Proceed as follows to configure a Profile with SIP Service Provider Profile information.

Prerequisites

Adequate administrative permissions.

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

The OpenScape Branch system is Version 2 or later.

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 Branch** within the Navigation Bar in the Common Management Platform.
- 2) Select a particular profile to edit from the **Select Profile** pull-down in the **Profiles** navigation area.
- 3) Navigate to **Configuration > VoIP** in the **Profiles** navigation tree area.
The **Voice over IP** window appears with the **General** tab selected by default.
- 4) Click the **SIP Service Provider Profile...** button in the **Gateways** work area.
The **SIP Service Provider Profiles** window appears displaying the Profile information.
- 5) Click the **Add...** button.
The **Add SIP Service Provider Profile** window appears with the **Basic** tabsheet selected.
- 6) Enter the name of the SIP Service Provider in the **Name** field, in the **Information** area.
- 7) Choose a privacy support configuration from the **Privacy Support** field, in the Information area. Possible values are: **Basic**, **Full**, **Full Send** or **Full Receive**.
 - **Basic** - If Privacy Support is set to Basic, the OpenScape Branch SHALL NOT send a P-Asserted-Identity header field in the messages (requests or responses) to the endpoint. The OpenScape Branch SHALL also ignore any received P-Asserted-Identity header fields. See deviations to this statement in the note below.
 - **Full** - If Privacy Support is set to Full, the OpenScape Branch SHALL send a P-Asserted-Identity (or a P-Preferred-Identity) header field in the messages (requests and responses) to the endpoint. The OpenScape Branch SHALL also accept any received P-Asserted-Identity header fields.
 - **Full Send** - If Privacy Support is set to Full-Send, the OpenScape Branch SHALL send a P-Asserted-Identity (or a P-Preferred-Identity) header field in the messages to the endpoint. However, the OpenScape Branch SHALL ignore any received P-Asserted-Identity header fields.

- **Full Receive** - If Privacy Support is set to Full-Receive, the OpenScape Branch SHALL NOT send a P-Asserted-Identity header field in the messages (requests or responses) to the endpoint. However, the OpenScape Branch SHALL accept any received P-Asserted-Identity header fields. See deviations to this statement in the note below.

NOTICE:

OpenScape Branch will send a P-Asserted-Identity (or a P-Preferred-Identity) header field to a SIP Trunk which has Privacy Support set to Basic or Full-Receive, IF the SIP SP has the “Send authentication number in P-Asserted-Identity” attribute enabled. For these scenarios, the OpenScape Branch system will only include the P-Asserted-Identity (or P-Preferred-Identity) header field in the initial SIP INVITE request sent to the SIP Trunk.

- 8) Check the **Mandatory default home DN** checkbox (Supported in Version 2). If the default home DN will always be used as the authentication number, for all outgoing calls.
- 9) Enter the Default home Destination Number in the **Default home DN** field, in the Information area (Supported in Version 2).

This parameter will contain the Default Home DN which will be used in the following situations:

- The Mandatory Default Home DN parameter is enabled. In this case the Default Home DN will always be used as the authentication id in Survivability mode.
 - In Survivability Mode the Calling party is not an OpenScape Branch subscriber and there is no redirecting or transferring party.
 - In Survivability Mode the redirecting or transferring party is not an OpenScape Branch subscriber.
 - The parameter Registration Required is enabled. In this case the Default Home DN will be used to register to the SIP Service Provider.
- 10) Check the **Use SIP Service Address for all identity headers** checkbox, in the **Use SIP Service Address** work area. If enabled, for both normal and survivability modes, all identity header fields are modified to include the DNS SRV SIP Service Address network domain field for SIP REGISTER (if registration used), INVITE, ACK, and BYE request methods. By default, the following headers are modified to include the SIP Service Address:
 - Request-URI
 - From
 - To
 - P-Asserted-Identity
 - Diversion(OSB V10R2) Additionally, it is also possible to add the SIP Service Address on the following headers:
 - Contact
 - Via
 - P-Preferred-Identity

- 11) Enter the SIP Service Address a character string identifying the network domain for the SIP Service Provider, in the **SIP Service Address** field.
- 12) Check the **Required** checkbox, in the Registration required area. The OpenScape Branch will be responsible for performing the registration in the SIP Service Provider.

NOTICE:

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.

- 13) Enter the **Interval**, in the Registration required area (Value: 60-7200 seconds). This configures the expiration time for the registration performed by the OpenScape Branch in the SIP Service Provider. This setting will be used by the system only if the **Registration Required** option is selected.
- 14) 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.

- 15) 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.
- 16) Enable digest authentication support by checking the **Supported** checkbox, in the **Digest Authentication supported** work area (Supported for Version 2). If the parameter Digest Authentication Supported is enabled, the OpenScape Branch or OpenScape SBC will accept being challenged by the SIP Service Provider and will respond with the credentials.

In Normal mode, the Digest Authentication will be performed by the OpenScape Voice. In Survivability mode, the Digest Authentication must be performed by the OpenScape Branch. The challenge from the SIP SP will be accepted if the parameter Digest Authentication Supported is enabled.

- 17) 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.
 - 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 user names and passwords.

If Digest Authentication fails, an alarm shall be generated.

- 18) Select the **Options** tab.

The **Options** tab window is displayed.

- 19) Select the settings for the Service Provider Profile by checking the respective checkboxes, in the Settings area.

- **Allow Sending of Insecure Referred By Header** - Enable the sending of the Referred-By header in the case of Blind Transfer.
- **Send P-Preferred Identity rather than P-Asserted** - Replace P-Asserted-Identity by P-Preferred-Identity.
- **Do not send diversion header** - Diversion header is not sent in case of call redirection.

IMPORTANT: This flag only applies to **Survivability** mode.

- **Send Uri in Telephone Subscriber Format** - The + is added at the beginning of the DN in all headers.
 - **Send authentication number in Diversion header** - The authentication number is sent in the Diversion header in case of redirected or transferred call.
 - **Send authentication number in P-Asserted Identity header** - The authentication number is sent in the P-Asserted-Identity header in case of redirected or transferred call.
 - **Send authorization number in From header** - The authentication number is sent in the From header in case of redirected or transferred call.
 - **Include restricted numbers in the From header** - If enabled will ensure the Service Provider business account identity is included in the From header field when the identity is restricted (Supported in Version 2).
- 20) Select the TLS signaling from the **TLS signaling** field list in the **TLS Certificates** work area, to specify the way TLS as a transport type will be handled in SIP messages. Values are: Transport=TLS, Default, Per Configuration and SIPS Scheme.

- 21) Select the **Flags** tab.

The **Flags** tab window is displayed.

- 22) Select flags for the Service Provider Profile by checking the respective checkboxes, in the Flags area.

- FQDN in Request to URI
- FQDN to header SSP
- Refer supported SSP
- Use TO to populate the R-URI
- Spare Flag 2 - Spare Flag 10

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

The **Flags** window disappears and a new profile is created in the SIP Service Provider Profiles table. The changes are stored temporarily.

- 24) Select the **SIP Manipulation** tab to configure SIP Manipulation rules.

The **SIP Header Manipulation** tab window appears. The rules are displayed in a list.

- 25) 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.

- 26) 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.

- 27) 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.

- 28) 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.

- 29) Select the SIP header the rule applies for in the **Header** selection list. Options are as follows:

- **R-URI**
- **From**
- **P-Asserted Identity**

The P-Preferred-Identity header field is supported in the SIP Trunking interface, but only in the messages (requests or responses) sent FROM OpenScope Branch TO the SIP Trunking/Gateway.

- **P-Preferred identity**

The P-Asserted-Identity and the Privacy header fields are supported in the SIP Trunking interface in both directions (i.e. FROM and TO the SIP Trunking endpoint).

- **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:

- **All**
- **PSTN-SIP**
- **SIP-PSTN**
- **SIP-SIP**

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 Providers Profile** window disappears and a new row is created in the VoIP gateways table. The changes are stored temporarily.

38) Click the **OK** button to go back to the **Voice over IP** window.

39) Click the **OK** button to store the changes temporarily in the administrator's login session.

The SIP Service Provider Profiles dialog disappears.

40) Click the **Apply changes** button in the main window.

The configuration of SIP Service Provider Profiles is applied on the OpenScape Branch Profile.

5.9.5 Quality of Service Profile Configuration

A profile can be configured with Quality of Service settings. The profile can then be assigned to multiple OpenScape Branches. 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.

5.9.5.1 How to Configure a Profile with VoIP QoS Rules

Proceed as follows to display, delete, edit or add a Quality of Service rules in the Voice over IP settings for a profile. The profile can be assigned to multiple OpenScape Branches.

Prerequisites

Adequate administrative permissions.

At least one 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 Branch** within the Navigation Bar in the Common Management Platform.
- 2) Select a particular profile to edit from the **Select Profile** pull-down in the **Profiles** navigation area.
- 3) Navigate to **Configuration > VoIP** in the **Profiles** navigation tree area.
The **Voice over IP** window appears with the **General** tab selected by default.
- 4) Check the **Enable** field in the **QoS** field area to enable the QoS functionality.
- 5) Click the **Configure...** button in the **QoS** field area.
The **VoIP QoS** window appears. The QoS rules are displayed in a list.
- 6) 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 **QoS** window appears.
- 7) Enter a DSCP (Differentiated Services Codepoint) SIP value to be set in the IP packets for the QoS rule in the **DSCP for SIP** field. (values: 1-63) If there are not enough digits to be deleted from the defined position on the header, this operation will be ignored.
- 8) Enter a DSCP (Differentiated Services Codepoint) RTP value to be set in the IP packets for the QoS rule in the **DSCP for non Circuit RTP (Audio)** or **DSCP for Circuit RTP (Audio)** field (values 1-63). If there are not enough digits to be deleted from the defined position on the header, this operation will be ignored.
- 9) Click the **OK** button to store the settings temporarily.
The **QoS** window disappears and the **Voice over IP** window appears.
- 10) Click the **OK** button to store the changes temporarily in the administrator's login session.
The **Voice over IP** dialog disappears.
- 11) Click the **Apply changes** button in the main window, work area.

The configuration of the QoS is applied on the OpenScape Branch system.

5.9.6 How to Configure a Profile for Timers and Thresholds

Proceed as follows to configure profile for the timers and thresholds to control the system performance of the OpenScape Branch. Once configured, the profile can be assigned to multiple OpenScape Branches.

Prerequisites

Adequate administrative permissions.

At least one 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 Branch** within the Navigation Bar in the Common Management Platform.
- 2) Select a particular profile to edit from the **Select Profile** pull-down in the **Profiles** navigation area.
- 3) Select a particular Branch office in the **Branch Office** selection list in the navigation tree.
- 4) Navigate to **Configuration > VoIP** in the **Profiles** navigation tree area.
The **Voice over IP** window appears with the **General** tab selected by default.
- 5) Select the **Timers and Thresholds** tab.
The settings for the timers and thresholds are displayed.
- 6) Enter the number of failure attempts that OpenScape SBC or Branch will count until a node failure is considered in the **Failure threshold (pings)** field.
- 7) Enter the number of positive responses to wait until node activation can be considered in the **Success threshold (pings)** field.
- 8) Enter the number of failure attempts during transition mode that OpenScape SBC or Branch counts until it switches to survivable mode in the **Transition Mode threshold (pings)** field.
- 9) Enter the time interval to send OPTIONS to the server in the **OPTIONS interval (sec)** field.
- 10) Enter the timeout when waiting for 200OK from SIP server in the **OPTIONS request timeout (sec)** field.
- 11) Click the **OK** button to store the changes temporarily in the administrator's login session.
The **Timers and Threshold** dialog disappears.
- 12) Click the **Apply changes** button in the main window, work area.

The settings for timers and thresholds are applied on the Profile.

6 OpenScape Branch - Local Management

IMPORTANT:

The **OpenScape Branch platform** is available in the following languages: English, German and French (starting from V10R2.1.0). You may choose the language of your preference (English, German or French) before login.

6.1 Dashboard

This top level screen presents the most important system information and gives quick access to alarm details and system status.

Alarms

- **Alarm summary** - The alarm summary section 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** - Clicking this button brings up a new screen that shows the alarm status in greater detail.

System Status

- **Branch mode** - The Branch can operate as a Branch Session Border Controller (SBC), an SBC-Proxy, a SIP Proxy, a SIP Proxy with ACD, or a Proxy ATA.
- **Auto refresh timer** - Using this drop-down box, an auto refresh timer can be set. After the timer expires the Status, System Info and Alarm information is refreshed automatically. When setting Auto refresh timer to 'never', the user has to refresh each tab individually using the refresh icon.

NOTICE:

While setting the timer via CMP, you don't need to save the configuration, the screen is updated with the configured time.

- **Operational state** - Operational state shows the system connectivity with the central SIP Server. The state **normal** indicates full connectivity to the primary and/or backup server. The state **survivable** indicates no connectivity and that the branch is operating in limited mode. A transition to survivable mode goes from: normal mode to transition mode to survivable mode. The proxy remains in "transition" state for N times "OPTIONS interval" seconds where N is the "Transition Mode threshold" (see also "Comm System" configuration).

In **Standalone** Operational State, OSB works without connection with OSV. All features related to the normal mode operation are disabled. No information related to the connection to the OSV will be available in the dashboard.

- **Redundancy state** - When Redundancy is enabled, this state shows the status of the Redundant system.
 - 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 between the redundant systems.

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 fields present the addresses or FQDNs of the central SIP Servers, the green/red boxes indicate the state of the server. For a Proxy ATA the Orange color is used to indicate that the outbound proxy has no connection to the main server.

Displayed for both **Com Node 1** and **Com Node 2**.

- **Penalty box state** - These fields represent the state of the central SIP servers, "NotRunning" is the state reported when survivability provider is not running, "In Penalty Box" is presented when the Branch has lost the connection with the SIP server. "Active" represents full connectivity with the SIP server. "Transition" is presented when the Branch detects a connectivity problem with the SIP Server. "OK" represents the state where the binding has lower priority than the currently active binding. "Reachable" represents the state where the binding has lower priority than the currently active binding. "Active - Survivable" represents the state where the binding has lower priority than the currently active binding.
- Displayed for both **Com Node 1** and **Com Node 2**.
- The enclosed field includes a number of status screens that can be shown by clicking the applicable "Show" button. For capabilities that do not apply to the selected Branch mode, or have not been configured on the Branch, the "Show" button will be disabled. See the applicable Help screens for each of the capabilities for more details.

System Info

- **CPU** - This field presents the CPU usage as a percentage; the data is updated as per the 'Auto refresh timer' setting and shows a snapshot at the time of reading. 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 field gives the percentage of the usage of RAM memory; the data is updated as per the 'Auto refresh timer' setting and shows a snapshot at the time of reading. Depending on the system load it will indicate from 0% to 100% of usage. Total memory is also displayed for all hardware types.
- **Disk** - This field gives the percentage of disk usage; the data is updated as per the 'Auto refresh timer' setting and shows a snapshot at the time of reading. Depending on the system load it will indicate from 0% to 100% of usage. Disk size is also displayed for all hardware types.

- **System uptime** - This field shows how long the system has been running; the data is updated as per the 'Auto refresh timer' setting and shows a snapshot at the time of reading. 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".
- **Software version** - This field indicates the software version running on the system. More detailed information is available by clicking the "Software Info" buttons.
- **Hardware Type** - This field shows the hardware type (CPU) used for the Branch. For the OSB 500i and OSB 50i, it also shows what type of PCI cards are installed.
- **Hostname** - This field shows the node name. The name is defined in the node.cfg file and set during a full installation.
- **Software Info** - The enclosed box presents the current Software version that is running on the Branch. Specific details about the software that is loaded on each partition can be viewed by clicking the "Active" or "Backup" buttons.

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.

6.1.1 Dashboard > Alarm Details

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.

- **Group ID** - corresponds to the last 2 numbers of the SNMP trap object ID (OID). An alarm trap is cleared by a trap with the same OID of severity 'cleared'.
- **Event ID** - corresponds to the last 2 numbers of the SNMP trap object ID (OID). An alarm trap is cleared by a trap with the same OID of severity 'cleared'.
- **Group name** - groups together alarms of a similar kind.
- **Event name** - is a character string that describes 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 date and time when the alarm occurred.
- **Threshold** - is the value that needs to be crossed by Monitored value 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** - 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** - is the alarm severity assigned to that particular alarm (warning, minor, major, critical). The Severity is fixed per Event ID.
- **Flow timer** - indicates the minimum time to wait before generating the 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
 - Processing error
 - Quality of service
- **Node** - Column shows when OSB is configured as Redundant system.

An alarm can be cleared either individually or by group.

Once an alarm is cleared, it will only appear in the Alarm History log.

6.1.2 Dashboard > Services Status

Shows 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.
- **B2BUA** – Back to Back SIP User Agent, this application is responsible for MLHG/ACD/Integrated Gateway and Auto Attendant call handling.
- **CDR** – Call Detail Record application. CDR is responsible for the call ticket generation, storing and sending the tickets to billing server. This application runs in Survivable mode only.
- **Continuous Tracing** – Trace application that collects the system logs and traces and sends them 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 IP-based 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** – Linux open source application that controls the IPsec encryption/authentication system.

- **Media Server** – Internal proprietary application responsible for announcements and large conferences.
- **MS Adapter** – Running only in SBC mode, and in modes **Proxy** and **SBC-Proxy**, if the flag **Branch Behind NAT** is enabled, the MS Adapter application is a Proxy for MGCP messages, which converts messages from WAN to LAN and sends it to the Media Server, and is also responsible for answering the NOTIFY audit.
- **MS Converter** – It is a SIP to/from MGCP message converter.
- **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 applications. Responsible for monitoring and restarting applications in case of failure or re-configuration.
- **Redundancy** – Application which provides redundancy.
- **RTP Proxy** – Open source application that proxies payloads from outside to inside IP addresses and vice-versa (WAN to LAN and LAN to WAN). It runs in Branch SBC, SBC-Proxy and Centralized SBC modes.
- **SIP Server** – Application that controls SIP Requests. It can operate as an SBC or a Proxy. It is 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.
- **Message Rate Control** – Open source Network Intrusion Prevention and Detection System (NIPS/NIDS).
- **SSDP** – SSDP is a service tool that provides external connectivity to enterprise server, for SSDP plug-in configuration and usage please refer to Configuration Guide for Service Plug-In.
- **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 example, Music on Hold (MOH).
- **Survivability Provider** – The SP is responsible for checking the Operational State and sending 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.
- **VPN** – Open source Virtual Private Network (VPN) application which provides encrypted tunnels between host computers.
- **Web server** – Application used to host and provide access to Homepages by Web Browsers.
- **Continuous Symptom Collector**-A process used to send normallog messages from one server to another server via a network connection.
The logs will be saved locally and remotely.
- **Kernel Console Collector**- A kernel feature that allows kernel log messages to be sent via an express network connection (ethernet protocol) to be captured by another server.
- **Streaming Server**-The Streaming Feature provides the capability of Streaming content for Music On Hold based on an Internet radio stream (e.g Web Radio) or a local Wave file in Normal & Survivable Mode invoked by MGCP Message.

Overall, applications can have status "running" or "not running". "running" means the application is enabled and running and "not running" can either

mean that the application is disabled or that some error occurred and the application has stopped.

The Continuous Tracing and the Redundancy applications are kept running even when they are disabled. While running, these two applications can have status "active" in case they are enabled or "stand-by" in case they are disabled.

The CDR application while running can be "active" in case the operational mode is survivability or "stand-by" for normal mode.

The B2BUA service always shows as running, regardless of the B2BUA flag or MLHG configuration.

The ethernet interfaces eth2, eth3 will be shown if they are configured on system.

6.1.3 Dashboard > Link Status

This screen shows the status of the available integrated gateway interfaces (PCI cards).

The LED status of the physical port on the back of the box for BRI/PRI E1/PRI T1 cards is shown below.

- **Green** - indicates that the port is synchronized with the remote switch.
- **Yellow** - indicates that the port is synchronizing, or is receiving a red alarm from the remote switch.
- **Red** - indicates that the port cannot maintain near end synchronization with the remote switch.

Note that it is possible for the physical port to display green but it could be disabled via maintenance. You must check this via the Link Status screen.

For FXS cards the LEDs are always green if the port is configured and yellow if the port is disabled.

For E1 and T1 PRI cards, the status of each individual B-channel is also shown.

- **IDLE (green)** – indicates that the channel is enabled and idle, ready to be used.
- **BUSY (blue)** – indicates that the channel is enabled and being used.
- **OOS/NE (red)** – indicates that the channel is out of service, due to a near-end issue, or is disabled.
- **OOS/FE (red)** – indicates that the channel is out of service, due to a far-end issue.
- **DOWN (red)** – indicates that there is a general issue in the E1/T1 card/interface.
- **MANOOS/NE (orange)** – Manual Out of Service Near-End. The channel has been blocked by the user locally.
- **MANOOS/FE (orange)** – Manual Out of Service Far-End. The channel has been blocked by the remote side.
- **MANOOS/NE/FE (orange)** – Manual Out of Service Near-End and Far-End. The channel has been blocked by the remote side and locally.
- **Service pending (orange)** – the channel is waiting for a SERVICE ACKNOWLEDGE reply message from the remote side.

For E1 and T1 PRI cards, the status of the D-channel is shown OOS (red) or IN-SERVICE (green).

Ring Down Configuration. T1 CAS: 24 ports per span E1 CAS: 30 ports per span being 1 to 15 and 17 to 31.

If PRI redundancy on an OSB 500i system has been enabled, the Backup node will only show the link status of the local and remote node. If the node is running as Master, it will show the link and channel status for the local node and only the link status of the remote node.

- **Channel maintenance** - if the user clicks the "Channel Maintenance" button, he/she will be redirected to the channel maintenance window. This capability only applies for the OSB 500i.

NOTICE:

By resizing some browsers, the scroll cursor will not be shown and the window could hide the last channels.

IMPORTANT: The limitations on feature interactions between PRI and CAS Ring Down are consequence of CAS RD calls restrictions. Own number is an example. Call transfer, forwarding and other features will only work if the own number matches the calling number of the feature call. Feature calls that generate outgoing calls through PRI port won't show this restrictions.

6.1.3.1 Dashboard > Link Status > Channel Maintenance

The Channel Maintenance screen allows the user to restart, block, and unblock selected channels. Blocking and unblocking is only available for PRIs that have B-Channel Availability Signaling (BCAS) enabled.

- The screen shows the user the current status of the BCAS setting, as well as the clock source priority information for all ports.
- **Restart selected channels** - this button issues an ISDN RESTART command for each selected channel. If all channels from all ports are selected the complete gateway application will be restarted. If all channels from one port are selected the whole interface will be restarted according to the "L3 Trunk Restart Type" option. If the "Disable Far End Restart" parameter is enabled the channels will be internally restarted and no ISDN RESTART command will be sent to the far end.
- **Block selected channels** - this button issues an ISDN SERVICE command for each selected channel with the change status option set to "out of service" (0x2). This action is taken only if BCAS is enabled on the PRI Interface. The channel is blocked and no longer allocated for outgoing calls. The channel presents status MANOOS/NE (manually out of service near-end). The remote side will present status MANOOS/FE (manually out of service far-end) and is not allowed to initiate calls on this channel. If the channel is in state MANOOS/NE and receives a SERVICE command with the change status option set to "in service" (0x1), it will remain in state MANOOS/NE and reply with a SERVICE ACKNOWLEDGE response with change status "out of service" (0x2). The channel presents status "Pending" until a SERVICE ACKNOWLEDGE message is received.
- **Unblock selected channels** - this button issues an ISDN SERVICE command for each selected channel with the change status option set to "in service" (0x1). This action is taken only if BCAS is enabled on the PRI

Interface. If the remote side replies with SERVICE ACKNOWLEDGE with the change status option set to "in service" (0x1), it will present status "Idle" and the channel will be available for new calls. If the remote side replies with SERVICE ACKNOWLEDGE with the change status option set to "out of service" (0x2), it will present status "MANOOS/FE". The channel presents status "Pending" until a SERVICE ACKNOWLEDGE message is received.

NOTICE:

On the OSB 500i, the "B-channel parallel restarts" flag setting is used during both the link start-up process and the PRI enabling process, but it is not used for Restart actions initiated from the Channel Maintenance tab. Any Restart action on the Channel Maintenance tab will always result in B-channel parallel restarts.

6.1.4 Dashboard > Backup Link Status

The "Backup Link Status" screen is activated by clicking the "Backup link status" button. This button is only available when a backup link has been established. The screen shows information and statistics about the established Backup Links.

Backup Link Client Status

The following information is available:

- BLS IP address
- Interface name
- Number of B-channels

The following statistics are available:

- Up Time
- IP Packets received
- IP Packets sent
- IP Packets dropped
- RTP Packets received
- RTP Packets sent
- RTP Packets lost

Backup Link Server Status

The following information is available:

- Tunnel name
- BLC hostname
- Interface name
- Number of B-channels

The following statistics are available:

- Up time
- IP packets received
- IP packets sent
- IP packets dropped
- RTP packets received

- RTP packets sent
- RTP packets lost

6.1.4.1 Dashboard > Backup Link Status Target Statistics

This window shows information and statistics about any established Backup Link.

Backup Link Client Status

The following information is available:

- BLS IP address
- Interface name
- Number of B-channels

The following statistics are available:

- Up Time
- IP Packets received
- IP Packets sent
- IP Packets dropped
- RTP Packets received
- RTP Packets sent
- RTP Packets lost

Backup Link Server Status

The following information is available:

- Tunnel name
- BLC hostname
- Interface name
- Number of B-channels

The following statistics are available:

- Up time
- IP packets received
- IP packets sent
- IP packets dropped
- RTP packets received
- RTP packets sent
- RTP packets lost

6.1.4.2 Dashboard > Backup Link Status PPP Connection Statistics

This window shows information and statistics about any established Backup Link.

Backup Link Client Status

The following information is available:

- BLS IP address
- Interface name

- Number of B-channels

The following statistics are available:

- Up Time
- IP Packets received
- IP Packets sent
- IP Packets dropped
- RTP Packets received
- RTP Packets sent
- RTP Packets lost

Backup Link Server Status

The following information is available:

- Tunnel name
- BLC hostname
- Interface name
- Number of B-channels

The following statistics are available:

- Up time
- IP packets received
- IP packets sent
- IP packets dropped
- RTP packets received
- RTP packets sent
- RTP packets lost

6.1.4.3 Dashboard > Backup Link Status IP Statistics

This window shows information and statistics about any established Backup Link.

Backup Link Client Status

The following information is available:

- BLS IP address
- Interface name
- Number of B-channels

The following statistics are available:

- Up Time
- IP Packets received
- IP Packets sent
- IP Packets dropped
- RTP Packets received
- RTP Packets sent
- RTP Packets lost

Backup Link Server Status

The following information is available:

- Tunnel name
- BLC hostname
- Interface name
- Number of B-channels

The following statistics are available:

- Up time
- IP packets received
- IP packets sent
- IP packets dropped
- RTP packets received
- RTP packets sent
- RTP packets lost

6.1.4.4 Dashboard > Backup Link Status RTP Statistics

This window shows information and statistics about any established Backup Link.

Backup Link Client Status

The following information is available:

- BLS IP address
- Interface name
- Number of B-channels

The following statistics are available:

- Up Time
- IP Packets received
- IP Packets sent
- IP Packets dropped
- RTP Packets received
- RTP Packets sent
- RTP Packets lost

Backup Link Server Status

The following information is available:

- Tunnel name
- BLC hostname
- Interface name
- Number of B-channels

The following statistics are available:

- Up time
- IP packets received
- IP packets sent
- IP packets dropped
- RTP packets received
- RTP packets sent
- RTP packets lost

6.1.5 Dashboard > Registered Subscribers

This button opens a new window that shows the subscribers that are registered internally on the Branch. The presented expiration time is based on the information sent by the subscriber at registration time, therefore the time used by expiration may be shorter if the central SIP server modifies the expiration timer.

The total number of registered subscribers depends on the number of OpenScape Branch Registered Line Licenses assigned and it is also limited by the hardware type:

- **Advantech 250** - maximum of 300 subscribers.
- **IBM x3250** - maximum of 1200 subscribers.
- **IBM x3550, Lenovo SR530, Fujitsu RX330 and Fujitsu RX200** - maximum of 6300 subscribers.
- **Advantech 50i** - maximum of 88 subscribers.
- **Advantech 500i** - maximum of 600 subscribers.
- **ProxyATA** - supports 24/48 FXS registrations depending on ProxyATA model.

6.1.6 Dashboard > Dynamic Port Mapping

Dynamic Port mapping

NOTICE: This screen is available for Branch SBC and SBC-Proxy modes only.

- **Select All** -
- **Search for** -
- **Table** -
 - Delete -
 - Contact - For gateways the Contact, Internal IP and Internal Port fields are set according to the configuration of the Gateways/Trunks table.
 - For SIP phones, Contact is set by the received Contact of the SIP message and is the same Contact field presented in the Registered Subscribers table. Internal IP is the IP Address of the SIP phone, and Internal Port is the port where the Branch is listening to the SIP messages from the SIP phone.
 - Internal IP - Refer to 'Contact', above.
 - Internal Port - Refer to 'Contact', above.
 - External IP - External IP is the WAN IP address
 - External Port - External Port is the external port allocated according to the configured SIP port range.
 - Map time -
 - Expire time from server -
- **Delete** - Setting the 'Select all' checkbox and clicking the "Delete" button will result in all port mapping entries being removed. Active calls are affected and subscribers must register again. Individual entries in the port mapping table can be deleted by setting their 'Delete' checkbox and then clicking the "Delete" button.

6.1.7 Dashboard > Subscriber Data

By clicking on the "Show" button, a screen is opened which contains the following subscriber data parameters:

- **Directory Number** - Subscriber directory number.
- **Alias List** - List of aliases to be used by this subscriber.
- **DA Username** - Digest Authentication Username.
- **DA Realm** - Digest Authentication Realm.

NOTICE:

This data cannot be edited. It is possible to clear the list of subscribers by selecting and deleting specific entries in the table.

6.1.8 Dashboard > Denial of Service Mitigation

The following parameters are displayed on the Denial of Service Mitigation screen.

- **IP** - IP address.
- **Quarantine TTL** - Quarantine time to live.
- **Interface** - Interface type.

There is a delete column also displayed on this screen.

6.1.9 Dashboard > Software Info

Software Partition information

- **Software version** - This read-only field indicates the version of the currently running software on the Branch.
- **Active** - By clicking this button, a new window opens to show the user more detailed information regarding the installed software components that are installed on the active partition.
- **Backup** - By clicking this button, a new window opens to show the user more detailed information regarding the installed software components that are installed on the backup partition.

6.2 System

This administrative area contains the advanced settings for the Branch

6.2.1 System > Settings

General

- **Branch Mode** - The Branch can operate as a Branch Session Border Controller (SBC), an SBC-Proxy, a SIP Proxy, a SIP Proxy with ACD, or a Proxy ATA.

For Branch SBC and SBC-Proxy modes the WAN interface must be activated.

When the Branch mode is changed to Proxy ACD, in the Features screen, Survivability section, the Multi Line Hunt Groups feature is replaced by the Automatic Call Distribution (ACD) feature.

Proxy ATA mode is only available if the hardware type is an Advantech 50i and there is one or two 24-port FXS Cards. Other modes are not available if at least one 24-port card is detected.

The system will reset upon applying the mode change.

NOTICE:

For Branch SBC mode, the WAN interface is used to access the central SIP servers. For SBC-Proxy mode, the WAN interface is used to access SIP Service Providers. Subscribers and the central SIP servers are in the LAN, as in Proxy mode.

-
- **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.
 - **Gateway only** - If checked the OSB shall operate exclusively as a gateway. It can be enabled for OSB50i/OSB500i or OSB in Proxy-SBC mode with IPv6 SIP Trunk.

IMPORTANT:

When OSB50i/OSB500i are configured as **Gateway only**, behind proxy or directly to OSV, then only base license is required.

- **Enable Standalone Mode** - If checked the OSB50i/OSBi shall operate exclusively as converter from TDM to SIP Trunking converter. This flag can only be enabled in the branch mode **Proxy-SBC**.

In Standalone Mode, OSB works without connection with OSV. All features related to the normal mode operation are disabled. No information related to the connection to the OSV will be available in the dashboard.

This mode also does not support subscribers. Only calls from PSTN to SIP Trunking or SIP Trunking to PSTN will be possible.

Standalone mode requires the Base license, SBC Sessions license and PSTN license that will determine the number of PSTN interface that can be connected to the OSB. Only the stand alone license type can be used in this mode. No license server can be configured in this mode.

In the case of Standalone mode, the current SSP profiles supported are:

- **AT&T Flex Reach (MIS/PTN)**
- **AT&T Toll-Free**
- **BT**
- **COLT Telecom**
- **DTAG/T-Systems (Sonus)**
- **Level 3 Communications**
- **Lync Mediation Server**
- **Orange**
- **Skype-IP Auth (IP Authentication)**
- **Sprint**
- **Telefonica**
- **Vodafone/Arcor**
- **Verizon-EMEA IP Trunking**
- **Verizon-IPCC Trunking**
- **Verizon US IP Trunking**
- **TSip Connect1.0**

IMPORTANT: Please verify if the compliance tests between the SSP provider and the OSB were completed.

Country Configuration

- **Country** - This field defines the country where the branch is located. It is used to set up the default values for such items as hookflash timer, ringing cadence and tone frequency. It applies to the Integrated Gateway and the ACD/AA features.

Administration

- **Session expiry timer** - This field is used to extend the https session timeout. The possible timer values are:
 - 1 hour
 - 2 hours
 - 3 hours
- **Enable SSDP** - If checked, this field enables the Smart Services Delivery Platform plug-in.

Watchdog configuration

The watchdog feature enables the continuous monitoring of the system processes health. If these processes are interrupted by CPU spikes, outages or overload it triggers a controlled HW restart to prevent the system to enter into a blockage state.

- **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.
- **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
 - 4 minutes
 - 5 minutes

Open VM Tools

- **Enable Open VM Tools**
If checked, this field enables the Open Virtual Machine Tools (open-vm-tools)

6.2.1.1 System > Settings > Country Configuration Viewer

This screen shows the details of the Country-related configuration data such as DTMF Interdigit time, DTMF volume levels, MF volume levels, Ring cadence, and several others.

6.2.2 System > Licenses

General

- **License server** - This is the IP address of the license server.

NOTICE:

The **Licenses** field accepts both IPv4 and IPv6 addresses.

- **License server port** - This is the SOAP port of the license server.
 - **Hardware ID** - This is the MAC address of the Branch LAN interface used to identify the Branch on the Assistant. It is a read-only field.
 - **Logical ID** - This is the unique identifier used on the Assistant for authentication purposes.
 - **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. Note: The DNS Server must be enabled.
-

License Information

- **License Version** - Indicates the version associated with the license obtained from the Central License Server (CLS).
- **SIEL ID** - shows the Standardized Integrated Equipment Life-cycle (SIEL) that is delivered to each network element with licenses file from the Central License Server (CLS).
- **License type** - This is the type of the Branch license. Possible values are:
 - None - If no licenses are 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 Branch 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 a license this will show how many days are still available in the grace period.
- **Stand alone license file** - By clicking the **Choose File** button, the user can select one valid license file (.lic). The **Upload** button will then be used to upload the selected license file, validate it and activate the license(s) contained within.

NOTICE:

Standalone mode requires the Base license, SBC Sessions license and PSTN license that will determine the number of PSTN interface that can be connected to the OSB. Only the stand alone license type can be used in this mode. No license server can be configured in this mode.

- **Refresh from License Server** - This button is used to request licenses from the configured license server. After a request is sent, the screen is updated with the new values.
- The license counters are presented in table format, where the first column shows the license type, the second column shows the number of licenses configured on the system and third column shows the license usage (watermark value reset monthly). The following is a brief description of each type of license.
 - **Base** - This is the Branch base license used by the Assistant to permit the branch to be used.
 - **Branch users** - This license is used to determine the maximum number of system-wide Branch Users that can register with the device. The Branch will not allow users (phones) to register if OpenScape Branch Registered Line Licenses are not available.
 - **Auto Attendant** - This is the license to use the Auto Attendant feature. If no license is available the feature will be disabled and blocked for configuration.
 - **Voice Mail** - This is the license to use the Voice Mail feature. If no license is available the feature will be disabled and blocked for configuration.
 - **Backup ACD** - This is the license to use the Backup ACD feature. If no license is available the feature will be disabled and blocked for configuration.
 - **SBC Sessions** - This license determines the maximum number of system wide SBC Sessions. The SBC sessions license counters are shown even if OSB is configured with Proxy / Proxy ACD modes.

Open Source Software Licenses

- **Open source software licenses** - The user can select an open source software component from the drop-down list and then click the **Show** button. A new window will open to display the license.

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.

Available options: **EULA**, **licenses_addon**, **licenses_in_install**

6.2.3 System > Branding > Branding Settings

- **Company Name** - The Company Name that is entered here is displayed on Local Management screens. 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** - The Product Name that is entered here is displayed on Local Management screens. 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** - This field allows the changing of the Trademark License Agreement that is presented on Local Management screens. 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** - The user can change the Logo Picture that is displayed 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 pixel dimensions (160x40) for proper display. Note: the file size is recommended to be less than 5 kB.
- If the "Import" button is clicked, a new screen opens to allow the user to select and upload an image. Once uploaded, the image will be available for selection in the "Logo picture" drop-down box.
- The "Delete" button is used for deleting an image file that has been selected in the "Logo picture" drop-down box.
- The option "default" is used to select the original logo picture.

NOTICE:

Regarding the browser cache: Any changing user interface element may not be immediately visible on all versions of all supported browsers. A browser reload associated with discarding the browser cache (usually Ctrl-F5) may be needed for updating the pages correctly. It is possible that the browsing history may need to be cleared in some cases.

6.3 Network/Net Services

In this administrative area the user can configure the network services. A pre-defined configuration for the LAN and, where applicable, WAN interfaces and default gateway can be created using the USB Stick Wizard.

6.3.1 Network/Net Services > Settings

Most of the hardware models of the Branch have only two network interfaces. In some models four network interfaces are available. Additional interfaces are not configurable via the Management Portal. One interface is identified as LAN (core) and the other is identified as WAN (access).

Physical network Interface

- **Interface** - This read-only field identifies the name of the interface.
- **Enabled** - This checkbox allows the user to enable or disable the interface. The LAN interface cannot be disabled.

- **NOTICE:**

Enabling or disabling an interface will result in a reboot of the system. Active and ongoing calls may fail.

- **MTU Size** - Enables the user to adjust the Maximum Transmission Unit (MTU) Size. The range for this field is 300 to 1500 bytes, with the default value being 1500 bytes.

NOTICE: Allowed MTU size values for IPv6 should be at least **1280** octets

- **Speed (Mbps)** - In this field it is possible to configure the interface speed. 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 will be disabled if Speed is set to **auto**.

IMPORTANT:

Some systems will NOT allow using **half duplex** mode with gigabit (**1000 Mbps**) speed.

-
- **Interface Bonding** - Checkbox for enabling the creation of bonding groups composed of multiple (at least two) Ethernet interfaces.

Bonding groups provide added reliability or added bandwidth. A system that uses bonding groups for reliability will typically use pairs of Ethernet ports, with each port being connected to different switch/router. A system that uses

bonding groups for added bandwidth will typically use pairs of Ethernet ports, with both ports being connected to the same switch/router.

A bonding group shall consist of exactly two selected Ethernet interfacesports.

If **Interface bonding** is enabled, then each row of the lower table must have exactly two checkboxes checked before the screen can be saved by clicking **OK**

If **Interface bonding** is checked, and any bonding group does not have two Ethernet interfaces ports assigned, then clicking the **OK** button must result in an error message and the screen must remain open until the error is corrected.

NOTICE:

The OSB 50, OSB 50i, OSB 250, and the OSB 500i are limited to having two Ethernet interfaces ports and, hence, will be limited to one bonding group, while the OSB 1000 and OSB 6000 will be limited to two bonding groups, depending on how many Ethernet interfaces ports they have, although no more than 4 ports will be made available for bonding, even if a greater number are installed.

-
- **Bond Interface** - This read-only field identifies the name of the bond interface.

eth0 is always associated with bond0 and eth1 is always associated with bond1 when there are two bonding groups. If there is only one bonding group, it will be bond0, and eth1 can be assigned to it. The associated checkboxes must be checked and disabled.

NOTICE:

The bond1 row must only be visible when there are 4 Ethernet ports, otherwise, only the bond0 row should be visible.

-
- **Enabled** - This checkbox allows the user to enable or disable the interface. The LAN interface cannot be disabled

NOTICE:

While breaking a bonding interface or disabling interface bonding altogether once operational is not typically performed, it can be accomplished.

IMPORTANT: If the feature is disabled, all references to bond0 must be replaced with eth0, and all references to bond1 must be replaced with eth1.

-
- **Type** -Available options: "Redundancy" and "Loadsharing". Default value: "Redundancy".
 - **eth0** - This read-only field identifies the name of the interface.
 - **eth1** - This read-only field identifies the name of the interface.

- **eth2** - If eth2 has been selected for one of the bonding groups, it cannot be selected for the other bonding group. The default setting for the eth2 checkbox is disabled.
- **eth3** - If eth3 has been selected for one of the bonding groups, it cannot be selected for the other bonding group. The default setting for the eth3 checkbox is unchecked.

Refer to the following bonding combinations:

Model	Mode	#Eth	#Bond	
OSB 50	Proxy, Proxy ACD	2	1	bond0=eth0+eth1
OSB 50	SBC Proxy, Branch SBC	2	0	Bonding not supported in these modes
OSB 50i	Proxy, Proxy ACD, Proxy ATA	2	1	bond0=eth0+eth1
OSB 50i	Gateway Only	2	1	bond0=eth0+eth1
OSB 50i	SBC Proxy, Branch SBC	2	0	Bonding not supported in these modes
OSB 250	Proxy, Proxy ACD	2	1	bond0=eth0+eth1
OSB 250	SBC Proxy, Branch SBC	2	0	Bonding not supported in these modes
OSB 500i	Proxy, Proxy ACD	2	1	bond0=eth0+eth1
OSB 500i	Gateway Only	2	1	bond0=eth0+eth1
OSB 500i	SBC Proxy, Branch SBC	2	0	Bonding not supported in these modes
OSB 1000	Proxy, Proxy ACD	2	1	bond0=eth0+eth1
OSB 1000	Proxy, Proxy ACD	3	1	bond0=eth0+eth1 OR bond0=eth0+eth2
OSB 1000	Proxy, Proxy ACD	4	1	bond0=eth0+(eth1 or eth2 or eth3)
OSB 1000	SBC Proxy, Branch SBC	2	0	Bonding not supported in these modes
OSB 1000	SBC Proxy, Branch SBC	3	1	bond0=eth0+eth2 OR bond1=eth1+eth2
OSB 1000	SBC Proxy, Branch SBC	4	2	bond0=eth0+(eth2 or eth3) END / OR bond1=eth1+(eth3 or eth2)
OSB 6000	Proxy, Proxy ACD	2	1	bond0=eth0+eth1
OSB 6000	Proxy, Proxy ACD	3	1	bond0=eth0+eth1 OR bond0=eth0+eth2

Model	Mode	#Eth	#Bond	
OSB 6000	Proxy, Proxy ACD	4	1	bond0=eth0+(eth1 or eth2 or eth3)
OSB 6000	SBC Proxy, Branch SBC	2	0	Bonding not supported in these modes
OSB 6000	SBC Proxy, Branch SBC	3	1	bond0=eth0+eth2 OR bond1=eth1+eth2
OSB 6000	SBC Proxy, Branch SBC	4	2	bond0=eth0+(eth2 or eth3) END / OR bond1=eth1+(eth3 or eth2)

Interface Configuration (LAN and WAN)

- **Type** - This is a pre-configured drop-down box that shows the interface type. Possible values are "Main IPv4", "Main IPv6", "VLAN IP", and (for WAN only) "Main admin".

NOTICE:

The Type **Main IPv6** indicates that the IPv6 is enabled for the system

- Selecting "Main admin" allows the user to specify the IP address for the management interface in the case where the customer wishes to separate the Management network from the VoIP network. The Subnet mask is defined in the field alongside. This option is not supported when Branch redundancy has been enabled.
- **IP address** - This field allows the user to specify the IP address associated with the interface type. It can be an IPv4 or an IPv6 address depending on the selected Type.

IMPORTANT: IPs 198.18.0.0/15 cannot be used for LAN/ WAN IP address - they are reserved for Network Interconnect Device Benchmark Testing [RFC3330]

- **Subnet mask** - This field defines the mask for the IP address. It can be an IPv4 or an IPv6 subnet mask depending on the selected Type.
- **VLAN tag** - This field defines the VLAN tag
- **UDP port** - This field defines the UDP port
- **TCP port** - This field defines the TCP port
- **TLS port** - This field defines the TLS port
- **Message rate limit (sec)** - (Applies to WAS interface only) - Message rate limit per second for the SIP listening IP:port for the WAN interface. Possible values :5,10,25,50,75,100. Default value is set at 100 which is an indication that the system-wide message rate limits are being applied.
- **Trust level** - (Applies to WAN interface only) - This field identifies the level of trust to be applied for the interface and is used to determine the quarantine interval to be used if a network interface exceeds the provisioned Message Rate Limit (sec). Possible values : 'N/A', 'Minimal', 'Medium'. Default value is set at 'N/A'

Routing

- **Default gateway address** - This field defines the IP address to be used as a Gateway.
- **Default gateway IPV6 address** - This field defines the IPV6 address.
- **Routing configuration** - A new route is created by clicking the "Add" button. It is then possible to configure the destination IP address, gateway IP address, network mask, and choose which interface will be used to route the IP packets.

To delete a route select the route and then click the "Delete" button.

Once the routes are created, edited, or deleted click the "OK" button to save the configuration and the window will close. To apply this configuration the user must click the "Apply Changes" button.

NOTICE:

The Default gateway, Destination, Gateway and Netmask fields are configurable for either IPv4 or IPv6 addresses.

Redundancy

Redundancy uses a non-proprietary protocol, which is used to increase the availability of the Branch. Redundancy is based on a virtual IP address that is in the same subnet as the Branch. The "Enable redundancy" checkbox enables the Redundancy protocol.

The features Backup Data Link, Auto Attendant and ACD have limitations in Redundancy Mode, please verify the documentation.

Enabling/Disabling Redundancy

NOTICE:

Redundancy is not allowed in Proxy ATA mode.

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.

To disable Redundancy it is required to configure Node 1 and Node 2 separately as follows. First, configure a temporary IP in the Master node and uncheck the "Enable redundancy" checkbox. The system will restart with Redundancy disabled and the Backup node will now be unable to take 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. Configure a temporary IP and uncheck the "Enable redundancy" checkbox (system will restart). Now both systems are operating with Redundancy disabled and it is possible to revert the IP configuration.

Upgrading a redundant system

The GUI shows the upgrade progress only while upgrading the Master node. The upgrade completion on the Backup node must be verified by checking the software information (version).

The upgrade process is started on the Master node. Once the upgrade on the Master node is complete 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 to upgrade a redundant system is about 20 minutes.

- **Enable PRI/CAS redundancy** - This checkbox allows an OSB 500i to operate in redundant mode with PRI links. To use this feature, the PRI links on both nodes have to be connected to the corresponding ports of the splitter box.

For greater reliability of the system, a USB cable can be used to connect both nodes.

PRI redundancy is only available for Proxy, Proxy ACD and SBC Proxy modes. PRI redundancy can only be set when branch redundancy has been enabled.

- **Failed links threshold** - This parameter defines the number of failing PRI links on the Master node that will trigger a comparison with the status of the PRI links on the Backup node. If the Backup node has at least one link more in a non-failing state than the Master, then a switchover will be initiated. If switchover due to PRI link failure is not desired, this parameter should be set to 0. This parameter can only be adjusted when PRI redundancy has been enabled.
- **Switchover without Link Check** - In order to activate, the parameter **Failed links threshold** must be set to 0 and flag must be checked. When activated, the backup node will switch over if the master node is powered off and the links don't go into an alarm condition as would be normally expected. Warning: This flag should only be used when the PSTN provider does not report the Layer 1 alarms.
- **Test Default Gateway instead of subscribers during failover**- A Network Connectivity Test (NCT) is executed as part of the redundancy failover mechanism. This test normally verifies external connectivity by sending a Layer 2 Arping message to a few subscribers that are registered on the

system. When the checkbox is checked, the test will be applied against the Default Gateway rather than subscribers.

6.3.2 Network/Net Services > DNS

Client

- **Refresh DNS** - By clicking this button, the user can manually refresh the DNS client (restarting the service).
- **DNS server IP Address list** - List of DNS server IP addresses to be used by this client (maximum of 3 DNS servers). Enter an IP address in the **DNS server IP address** field and then click the **Add** button. The IP address will appear in the list. To remove a DNS server from the list, click it once in the list to select it and then click the **Delete** button.

NOTICE:

DNS supports both IPv4 and IPv6 addresses.

- **Alias list** - List of aliases to be used by this client. Enter an alias in the "Alias" field and then click the **Add** button. The alias will appear in the list. To remove an alias from the list, click it once in the list to select it and then click the **Delete** button.
-

Server

- **Enable DNS server** - Setting this checkbox enables the "DNS configuration" button, which, when clicked, opens a new screen that allows the user to configure the DNS server.
- **Enable customization** - Setting this checkbox enables the "Administer custom files" button, which, when clicked, opens a new screen that allows the user to upload files that will customize the DNS configuration.

NOTICE:

When this checkbox is enabled, custom configuration takes precedence, hence the "DNS configuration" button is disabled.

6.3.2.1 Network/Net Services > DNS Configuration

Zone Configuration

- **Enable OSEE v9 DNS zone splitting** - Support of DNS zone splitting by configuring and using a key for retrieving the assigned DNS zone file. This checkbox is disabled by default.

Click the **Add** button to add a new DNS zone entry. To delete an entry, first select the entry by clicking on it, and then click the **Delete** button.

- **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.

NOTICE:

IP masters/forwards accepts both IPv4 and IPv6 addresses.

- **File name** - The name to use for the file to store the cached information in (required field when zone type is slave). (usually the same as the Zone name).

Forward IP

Shows the list of IP addresses for the DNS server to forward queries to. It is 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.

NOTICE:

Forward IP supports both IPv4 and IPv6 addresses.

Click the **Add** button to add a new forwarding address entry. To delete an entry, first select the entry by clicking on it, and then click the **Delete** button.

6.3.2.2 Network/Net Services > DNS > Administer Custom Files

Administer Custom DNS Files

Click the "Browse and Upload" DNS Files

If using this facility, the named.conf file is mandatory and must be one of the uploaded files. See http://en.wikipedia.org/wiki/Zone_file for a description of DNS files.

NOTICE:

A custom DNS file may contain IPv6 addresses.#

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 Branch. Backup of the custom file will be included in the "Export all" function. After a re-installation of the Branch, the custom files must be restored to the Branch 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.

6.3.3 Network/Net Services > NTP > NTP Settings

NTP Settings

- **Region** - The Region drop list defines which region will be used in Branch, therefore being able to choose timezones by region (e.g. Europe, Africa, Asia, etc.), provided by the Region drop list.
- **Timezone** - The Timezone drop-down list defines which timezone will be used by the Branch. 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** - The Enable local NTP server checkbox is used to activate the local NTP server.
- **Manual configuration** - Manual configuration is used to set the Date and Time manually. Click the "Apply" button to set it up. This button is visible only if Manual configuration is selected. The timezone as well as the date and time are read from the system. In case no timezone is configured, then it is read from the system configuration file.
- **Synchronize with NTP server** - Synchronize with NTP server is the option used when an NTP server is available. In this case the server address must be entered in the NTP server field. Any IP address is valid, except 0.0.0.0 and 255.255.255.255.

NOTICE:

The **NTP Server** field accepts both IPv4 and IPv6 addresses.

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 an NTP Server (It does not set up anything, just uses the current ntp.conf).

When in "Manual configuration" mode, timezone changes are applied after clicking the "Apply" button and then confirming it by clicking "OK" followed by "Apply Changes".

When in "Synchronize with NTP server" mode, timezone changes are applied after clicking the "OK" and "Apply Changes" buttons.

Due to issues with Apache Session Timeout and Postgres database the Branch will reboot in case of changes that apply a new configuration manually or modify the NTP Server or timezone.

6.3.4 Network/Net Services > DHCP > General

General

- **Enable DHCP server** - This checkbox enables the internal DHCP Server service.
- **Enable customization** - This checkbox allows the user to upload files to customize the configuration of DHCP. Files are uploaded by clicking on the Administer custom files button. The custom file may include the DLS server configuration for the phones. In this case the DLS configuration must be manually set in the custom file.

IMPORTANT: The syntax and the contents of the file(s) will not be checked, so an incorrect configuration may cause the DHCP service to not start. When Customization is enabled, the DHCP server configuration through the GUI will be disabled. The custom file configuration will be preserved in case of upgrades.

IMPORTANT: The DHCP custom file must be backed up to survive a re-installation of the Branch. Backup of the custom file will be included in the "Export all" function. After a re-installation of the Branch, the custom files must be restored to the Branch 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.

- **Subnet** - The subnet IP address which will be served by this DHCP server.

IMPORTANT: DHCP accepts IPv4 addresses only. IPv6 is not currently supported.

- **Netmask** - The network mask associated with the subnet.
- **IP address from/to** - These fields configure the range of IP addresses that will be available.
- **Except IP address from/to** - These fields configure a exclusion range within the specified IP addresses range.
- **Static IP Address list configuration** - See Static IP address section below.
- **Lease time** - The default lease time (in seconds) of the DHCP leasing mechanism.

- **Max lease time** - The maximum lease time (in seconds) to be applied.
- **Interface** - The interface for the DHCP server to listen on.
- **Update style** - The update style scheme to be applied by this DHCP server to the Domain Name System.
- **DNS server list** - The list of DNS server IP addresses to be used. Add and Delete buttons are available to add and remove servers.
- **WINS server** - IP address of the WINS (Windows Internet Name Service) server to be used
- **Print server** - IP address of the Print server to be used
- **Broadcast address** - The broadcast IP address to be used
- **Domain name** - The domain name to be applied
- **Router** - The router IP address. If empty, the Branch default gateway IP address is used.
- **Enable NTP** - If enabled the NTP server address is offered to devices that make a DHCP request.
- **Disable 'Time Offset' Option** - When enabled, the configuration item "option time-offset" will not be added to dhcpd.conf file.

Deployment Service

The custom DHCP file may include the DLS server configuration for the phones. In this case the DLS configuration must be manually set in the custom file.

- **DLS server** - The IP address of the DLS server.
- **DLS port** - The port of the DLS server.
- **DCMP server** - The IP address of the DCMP server.
- **DCMP port** - The port of the DCMP server.

6.3.4.1 Network/Net Services > DHCP > Administer Custom Files

Administer Custom DHCP Files

Click the "Browse" button to locate the custom DHCP file on your local computer or network drive, and then click the "Upload" button to load it onto the Branch. A custom DHCP File can be deleted by first clicking it to select it and then clicking the "Delete" button.

If using this facility, the dhcpd.conf file is mandatory and must be one of the uploaded files.

IMPORTANT: The syntax and the contents of the file(s) will not be checked, so wrong configuration may cause the DHCP service to not start. When the Customization is enabled, the DHCP server configuration through the local management will be disabled. The custom files configuration will be preserved in case of upgrades.

IMPORTANT: IMPORTANT: The DHCP custom file must be backed up to survive a re-installation of the Branch. Backup of the custom file will be included in the "Export all" function. After

a re-installation of the Branch, the custom files must be restored to the Branch 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.

6.3.4.2 Network/Net Services > DHCP > Static IP Addresses

Static IP Address

A new static IP address entry is created by clicking the "Add" button. The static IP address can be configured in the corresponding row in the table. A static IP address is deleted from the table by first clicking on it to select it and then clicking the "Delete" button.

- **Hostname** - The hostname which applies for the configured IP.
- **MAC address** - The MAC address (in the format AA:BB:CC:DD:EE:FF) associated with the configured IP.
- **IP address** - The static IP address to configure.

6.3.5 Network/Net Services > Traffic Shaping

General

- **Enable traffic shaping** - To enable traffic shaping, the user has to set the checkbox.
- **traffic shaping table** - Clicking the "Add" button creates a new class of traffic row in the table. To delete a row from the table, first select the row by clicking on it, and then click the "Delete" button.
- **Parent class ID** - This is a hexadecimal number in the range 0000-FFFF, representing the ID for the traffic parent class.

Please note that there should be at least one row without the Parent Class ID set, because that row is the parent for others.

- **Class ID** - This is a hexadecimal number in range 0000-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 to.
- **Default class ID** - 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 a symbolic way.
- **Rate (Kbps)** - 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 Kbps.
- **Ceiling rate (Kbps)** - 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 (Kbytes)** - 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 (Kbytes)** - Also an optional parameter, that sets the maximum value of the burst. Values are defined in Kbytes (Example 1Kb).
- **MTU (bytes)** - 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 the number, the lower 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, packetFifo and byteFifo
- **SFQ quantum (bytes)** - This is an optional parameter that defines the amount of data, in bytes, that a stream is allowed to dequeue before the next queue gets a turn. The default is set to one MTU-sized packet. Do not set this parameter below the MTU!
- **SFQ perturbation (sec)** - 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.
- **Byte FIFO limit** - This is an optional parameter which defines the number of bytes that the queue can hold.
- **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 follows:

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 numbered 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.

6.3.6 Network/Net Services > QoS Settings

QoS Settings

- **Enable QoS** - Quality of Service is enabled using this checkbox.
- **DSCP for SIP** - DSCP value to be set in the IP packets of any SIP message sent by the Branch SIP Server.
- **DSCP for non Circuit RTP (Audio)** - DSCP value to be set in the IP packets of any RTP message sent by the Branch Media services, not through Circuit.
- **DSCP for Circuit RTP (Audio)** - DSCP value to be set in the IP packets of any RTP message sent by the Branch Media services, through Circuit.
- **QoS configuration table** - A new row in the QoS table is created by clicking the "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. A QoS rule is deleted

from the table by first clicking on the row to select it and then clicking the "Delete" button.

- The table fields are defined as follows:
 - 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:

The DSCP values of QoS configuration table rules can overwrite the values set by the SIP and RTP protocols when conflicting rules are set.

The DSCP field is a 6-bit field which is defined in RFC2474. Values between 0 and 64 should be used. 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
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

Name	Space	Reference	Decimal
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

6.4 VoIP

In this administrative area the user can configure the VoIP parameters.

Note that some configuration changes will cause the SIP Server to restart. Active and ongoing calls may fail.

6.4.1 VoIP > SIP Server Settings

General

- **Comm System Type** - The Comm System Type (mode) describes the Comm System node architecture. Simplex indicates a single node Comm System configuration. Collocated indicates that the Comm System has two nodes, with each connected to a separate LAN switch. The Branch is required to configure the addresses for each node. Geo-Separated indicates that the Comm System has two nodes, but they are in different physical locations. As with Collocated, the Branch is required to configure the addresses for each node. If the configuration is other than Simplex, the secondary and backup servers will be enabled.
- **OPTIONS source port** - The OPTIONS source port is used with Comm System V3.1 to bypass Digest Authentication for OPTIONS request.
It must be set to a value different from the UDP/TCP/TLS "SIP listening ports". This port must also be set as a trusted port on the endpoint representing the Branch in the Comm System.

- **IP Version Towards SIP Server** - indicates if the SIP servers (C-SBC or OSV) are being addressed via IPv4 or IPv6.

If the OSB with SSP via IPv6 is connected to the OSV via an OSB Proxy, the **Gateway Only** flag shall be enabled. So, if an OSB in SBC-Proxy is configured with an IPv6 address in the WAN interface the **Gateway Only** flag shall be available for configuration. On the other hand, if a 50i/500i is configured with the **Gateway Only** flag it shall be possible to change the operations mode to SBC-Proxy and to configure the WAN interface with an IPv6 address.

- **Enable outbound proxy** - Enables the configuration of an outbound proxy in case the Branch is in Proxy-ATA mode and is not connected directly to Comm System.
- **Outbound proxy** - The IP Address of the Branch to which the Proxy-ATA Branch will try to connect in case the "enable outbound proxy" flag is checked.
- **Outbound proxy port** - The IP port of the Branch to which the Proxy-ATA Branch will try to connect in case the "enable outbound proxy" flag is checked.
- **Enable path tagging** - Allows a Branch in Proxy-ATA mode to include a "Path" header in SIP messages and a Branch which has a connected ATA to handle the messages with this header.
- **Branch-behind SBC** - When checked, this flag indicates whether the Branch is behind a 3rd party Centralized Session Border Controller or, when not checked, directly connected to the Comm System or behind an OpenScape SBC. This is required by some third party SBCs to uniquely identify the subscribers/gateways behind the branch. If the OSB is configured with IP, the IP address will be visible using this flag.

Enabling this flag will change the port mapping handling for headers TO, FROM, CONTACT and VIA. If OSB is configured as SBC-Proxy, port mapping will not be performed when connected to an SBC which is connected to an OpenScape Voice.

NOTICE:

Flag is not required if OSB is configured behind OSSBC.

- **Branch behind NAT** - When checked, indicates whether the Branch is behind a NAT, whose IP address is not static but subject to dynamic changes. When checked, then the Branch shall use its "Logical Branch office ID" as "Logical-Endpoint-ID" to be encrypted in the OPTIONS sent to OSSBC.
- **Synch subscriber data** - When checked, the subscriber data synchronization is enabled.
- **Disable notification in survivable mode** -
- **Enforce Minimum Subscriber Transport Security**

- **Disable Basic Security Check for LAN** - Disabled by default.

The sanity check is used to prevent the system against corrupted, inconsistent or non-RFC compliant messages. The flag bypasses these tests for the LAN side.

NOTICE:

In most cases this kind of messages are not expected on the LAN side.

This flag can be used to increase the performance of OSB SIP server since the sanity check for SIP messages causes performance issues.

- **Send CANCEL on Unreplied Branches** - if this flag is enabled, CANCEL messages received by the Sip Server will be transmitted even on unreplied branches. Otherwise, the Sip Server will fake an internal **487** and the unreplied branches will be terminated immediately. This flag is disabled by default.
- **SDP ANAT Bypass** - ¹If enabled, the OSB checks in the presence of header **Require: sdp-anat** under SIP messages and if so, bypasses the SDP between endpoints, i.e., OSB does not anchor the media between IPv4 and IPv6 networks.

NOTICE:

This flag is only available for configuration when IPv6 support is enabled in the OSB.

- **Other trusted servers** - By pressing this button, you refer to the [VoIP > SIP Server Settings > Other Trusted Servers](#) tab
 - **Load Balance Mapping Table** - By pressing this button, you refer to the [VoIP > SIP Server Settings > Load Balance Mapping Table](#) tab
-

Node 1 and Node 2

The fields in these two sections configure the protocols and ports on the LAN where the Branch will be listening for incoming message traffic. A UDP listening port MUST be between 1 and 65535, and different from 5086, 5096, 5150 and 5160.

NOTICE:

IPv4 and IPv6 addresses are supported.

- **Target type** - If the configuration is "Binding" then the SRV Record field will be grayed-out and the user has to enter the Primary and Backup server IP address or FQDN (depending on the setting of Comm System Type), the Transport and the Port (the last fields are mandatory).

If the configuration is "SRV Record", a DNS SRV Record query will search the addresses automatically (SRV Record field) using the respective

¹ ANAT (Alternative Network Address Translation)

Transport (Transport field). The network administrator shall configure the priority of the SIP Server according to the network configuration.

- **Primary server** - The Primary server field identifies the preferred Comm System server to which the Branch is connected. In this field either an IP address or FQDN of the server is configured. The Transport field defines the SIP protocol used to communicate with the Comm System server, while Port is the SIP port used.

If TLS is used, the primary IP address should be pointed to SIPSM3.

IMPORTANT: OSB always uses TLS/MTLS on port 5061. Even configured as TLS, the connection is MTLS and port 5061 is used.

- **Backup server** - The Backup server field identifies the backup Comm System server to which the Branch will be connected in case of a Primary server failure. In this field either an IP address or FQDN of the server is configured. The transport field defines the SIP protocol used to communicate with the Comm System server, while Port is the SIP port used. Note that this field only applies when Comm System Type is set to "Geo-Separated".
 - **SRV record** - IP address or FQDN to retrieve the SRV (Service) record from. The transport field defines the transport protocol to be used in the SRV query.
-

Timers and Thresholds

- **Failure threshold (pings)** - This is the number of failure attempts that a Branch will count until it considers that it has detected a Comm System node failure.
- **Success threshold (pings)** - This defines the number of positive responses to wait until considering a Comm System node to be active again.
- **Transition mode threshold (pings)** - This is the number of failure attempts during Transition Mode that a Branch will count until it switches to Survivable Mode.
- **OPTIONS interval (sec)** - This box defines the time interval to send OPTIONS to the Comm System server(s).
- **OPTIONS timeout (sec)** - This box defines the timeout when waiting for a 200 OK message from a Comm System server.
- **Notification rate** - This is the number of notifications per second sent to phones after a state transition.

This field is disabled when the Branch is in Proxy ACD mode.

Clustered Nodes settings

- **Ping Method** - Available options: OPTIONS,INFO,REGISTER,NOTIFY,UPDATE.
- **OPTIONS interval (sec)** - This box defines the time interval to send OPTIONS to the Comm System server(s).
- **Failure threshold (pings)** -

6.4.1.1 VoIP > SIP Server Settings > Other Trusted Servers

This configuration screen allows the user to edit the list of trusted SIP Servers from which Requests can be accepted.

The list should include only IP addresses of 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.

NOTICE:

IPv4 and IPv6 addresses are supported, but they may not be a mix of IPv4 and IPv6.

- **Port** - This box is used to configure the SIP port of the trusted server.
- **Transport** - This drop-down box defines the SIP transport protocol to be used in communication with the trusted server. Available options are: TCP, UDP, and TLS.

NOTICE:

The sipism1 address should not be added to the list of trusted servers if the sipism3 (MTLS) address is being used.

6.4.1.2 VoIP > SIP Server Settings > Load Balance Mapping Table

This configuration screen provides routing/URL substitution information for systems that perform load balancing. The trusted servers table is also used for authentication (in a non-normal scenario where the OSB communicates with multiple OSVs) and for load balancing.

Incoming / Outgoing

When specifying the **Incoming** data, all fields are required, however port information will not be specified (and will be ignored) when the incoming string is an srv type address.

The **Outgoing** data is required. If any entry row is specified, all of the fields in that row must be specified (the exception is that if the address type is SRV, then no port is specified).

The OSB will be able to map the incoming URI to the correct destination and type. It will update the transport as well. The Outgoing fields (in general) should match the OSV addresses listed under **VOIP > Sip Server Settings**.

The **Outgoing** data should generally be **Node1** or **Node 2** of the primary OSV.

- **IP address or FQDN** - This is the configuration of the IP address or Fully Qualified Domain Name of the trusted server.

NOTICE:

IPv4 and IPv6 addresses are supported, but they may not be a mix of IPv4 and IPv6.

- **Type** - Possible values: Binding, SRV record
- **Port** - This box is used to configure the SIP port of the trusted server.
- **Transport** - This drop-down box defines the SIP transport protocol to be used in communication with the trusted server. Available options are: TCP, UDP, and TLS.

6.4.2 VoIP > Port and Signaling Settings

Port Range

- **RTP Ports** - These boxes define the RTP port range (minimum and maximum) to be used by RTP traffic, as well as the Time to live, which is the disconnection timer for non-RTP activity.

NOTICE:

These fields are always enabled in Branch SBC/SBC-Proxy (Session Border Controller) modes. The fields may also be used in Proxy and Proxy-ACD modes when Integrated Gateway feature or other B2BUA (Back-to-Back User Agent) provided feature is used (e.g. Automatic Call Distribution (ACD) Groups, Auto Attendant (AA), Multi Line Hunt Group (MLHG), Voicemail).

NOTICE:

The B2BUA application may not use the port range configuration used by the RTP Proxy when there is a match between negotiated media and the media profile used by the B2BUA (igw_features_lan). In this case, the RTP Port Range is fixed to 10000 - 19999 and the "RTP ports min/max" fields are ignored.

NOTICE:

Valid values for Port min and Port max are between 35000 and 65000. The port range should be within 2-48 ports.

NOTICE: The Time to live can range between 180 and 1200 seconds, while the default is 180. This field is valid for the Branch in the modes mentioned above when G729/sRTP is enabled.

- **Subscribers dynamic SIP ports** - These boxes define the SIP port range to be used in SIP messages.

NOTICE:

These boxes are only enabled in Branch SBC and SBC-Proxy modes.

NOTICE:

Valid values for Port min and Port max are between 10000 and 65000.

NOTICE:

Port range must be greater than or equal to 500 ports.

NOTICE: If the range is changed, the port mapping will be cleared and active calls will be affected. All subscribers must re-register.

- **Gateways/trunks static SIP ports** - These boxes define the SIP port range to be used by LAN gateways/trunks.

NOTICE:

These boxes are only enabled in Branch SBC and SBC-Proxy modes.

NOTICE:

Valid values for Port min and Port max are between 9000 and 9254.

NOTICE: Port range must be less than or equal to 255 ports.

Signaling and Transport Settings

- **INVITE No Answer timeout - NM (ms)** - Timer in milliseconds which applies if no reply for an INVITE arrives after the 100 Trying was received in Normal mode operation. This timer is valid for outgoing calls to external and internal gateways.
- **INVITE No Answer timeout - SM (ms)** - Timer in milliseconds which applies if no reply for an INVITE arrives after the 100 Trying was received in Survivable mode operation. This timer is valid for outgoing calls to external and internal gateways.
- **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 the case of two consecutive failures, the TCP connection will be terminated. The 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 and 1440 minutes with the default value set at 12 hours (720 min). The TCP/BFCP connection timer should be activated in order to avoid open TCP ports unintentionally.

NOTICE: BFCP as well as the other TCP timers are only valid on the Proxy-SBC mode

- **UDP-SIP keep -alives** - Enable the keep-alive mechanism if the connection was established by the OSB as a UDP client.

NOTICE:

Available only for the **SBC** mode.

- **Keep-alive time (sec)** - Determines the interval between sending the keep-alive requests.

NOTICE:

Available only for the **SBC** mode.

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. **This configuration is only available for OSB Branch SBC and applicable for all gateways and subscribers under it.**

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.

IMPORTANT: Check the **Enable the LAN-WAN media interworking** flag to activate this configuration.

- **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.

Same way as the "Open External Firewall Pinhole", the dummy RTP 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.

NOTICE:

This feature only applies to the addresses and ports used for the media streaming. It is not applicable to the SIP or MGCP protocols. Starting from V10R3.4.0, 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.

- **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. The total system memory usage may increase up to 1%. 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.

6.4.3 VoIP > Manipulation and Routing

Office Codes

A Branch can support subscribers spread across multiple Office Codes. It also supports defining dedicated trunk groups to be used for outgoing calls originated by subscribers within an Office Code. Extension dialling is still possible using Office Codes.

The table shows the set of office code/extension mappings. Click **Add** to create a new mapping. A new screen is displayed with the following fields to be defined:

- **Enable source-based routing in Normal Mode** - If an SN Range is entered with a Destination Prefix, it is possible to route external calls via a gateway that is chosen based on the calling party number. This is the definition of source-based routing. This feature is enabled by default in Survivability Mode. This field allows the feature to also be used in Normal mode.
- **SN Range** - This field defines the range of extension (subscriber) numbers that are assigned to the office code. The extension numbers can be entered either individually, or in ranges separated by a dash. Multiple extension numbers and/or SN ranges can also be entered, separated by a comma (e.g. 1000-1999, 2001). When entered as a range, the numbers must be separated by a dash. Only the digits 0 through 9, a space, a dash, and a comma are permitted in this field. Extension numbers should be defined with the same digit length for all office codes. The maximum number of digits in an extension number is 7. The user is not permitted to enter the same extension number against different office codes. This field is required.

- **Office Code** - This field defines the Office Code number that relates to all of the entries in the SN Range. Only the digits 0 through 9 are allowed. A maximum of 14 digits can be entered.
- **Destination Prefix** - The destination prefix identifies which outgoing trunk group or SSP in the gateway table will be used to route external calls from an extension within the Office Code. DIVERSION, REFERRED-BY or FROM headers (checked in that order) are used to look up the destination prefix that should be used. This field allows up to 100 characters. Only digits 0 through 9, '*', '#' or '+' are allowed.
- **Insert Office Code** - This checkbox, when set, causes the insertion of the Office Code of the called party into the R-URI. If the called party is an extension number, its office code is inserted into the R-URI of the INVITE message in order to complete the call. This functionality is bypassed if the checkbox is not set.

NOTICE:

Office codes are not allowed for Proxy ATA mode.

NOTICE: Either the Office code or the Destination prefix must be configured.

To delete a mapping, click to select it and then click **Delete**.

SIP Manipulation

This configuration allows changes in SIP headers (except from an Emergency Number) during **Survivability Mode** only.

NOTICE:

In **Normal Mode**, the OSV is responsible for SIP Manipulation, while the OSB handles gateway selection and Type of Number (TON) handling. The OSV will also be responsible for prefixing a dialed subscriber number with an office code.

NOTICE:

In **Survivable Mode**, the OSB is responsible for SIP Manipulation, Gateway selection, and Type of Number (TON) handling.

A new rule is added by clicking the **Add** button. To delete a rule, first click on the row in the table to select it then click the **Delete** button.

- **Match digits** - The matching digits are defined in this field. Only numerical digits and the characters *, # and + are supported.
- **Match position** - This field is used to define 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).

NOTICE: This field defines how many digits it will try to match, with the match position as a reference.

- **Header** - This field defines which SIP header the rule applies to. NOTE: For Proxy ACD mode, only R-URI and From headers are supported.
- **Delete/insert position** - This field defines from which digit position in the header the fields "Number of digits to delete" and "Insert digits at position" are applied. If the value of this field does not correspond to an effective position in 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. Only numerical digits and the characters *, # and + are supported.
- **Add prefix** - This field is used to set the prefix to be added to the digits in the header. Only numerical digits and the characters *, # and + are supported.
- **Replace all with** - The digits that will replace all header digits. Only numerical digits and the characters *, # and + are supported.
- **Call type** - This field is used to define to which calls the rule is applied: SIP-SIP, SIP-PSTN, PSTN-SIP or to All call types. NOTE: For Proxy ACD mode, only the All call type is supported.

If the header digits of a message match more than one rule, only the best matching rule is applied to the header. The best matching rule is the rule that matches the header digits and complies with the following criteria, from the higher priority to the lower priority:

- It has the longest "Match digits" length.
- It has the lowest "Match position" value.
- It has the highest "Match digits" value in lexicographical order.

For interaction with other manipulation rules: it should be noted that if "output digit strip" has been defined for the corresponding gateway, then first the gateway rule for stripping of digits is performed then the SIP manipulation rule is applied.

SIP manipulation rules do not apply to any GUI field. They apply only to SIP message headers.

NOTICE:

Office codes are not allowed in Proxy ATA mode.

IMPORTANT:

SIP Manipulation for SSP headers is valid only for outgoing calls.

From header manipulation may not be acceptable for some SIP Service Providers. For instance a service provider may need to have a business account number in the **From header**. Therefore manipulation of the **From header** would not make sense in this case.

OpenScape Branch supports the Sip Compact Headers.

IMPORTANT: Sending the SIP compacted messages directly to the **SipMgcpConverter** show a restriction on this component to parse these kind of messages. In survivable mode, an E-GW (or any other device) in the LAN by using SIP Compact Header, calling into the OSB without using transcoding (SSM) or B2B components, will not be able to contact the Media Server and therefore hearing announcements or start a conference. Possible workaround is to use set the B2B by using a different gateway type.

SIP Routing

This configuration allows the routing of SIP messages during Survivability Mode. Click **Add** to add a new rule.

- **Source IP** - This is the source IP address of the message to be routed. Subnet address in CIDR notation is also supported and can be set to route messages from any host in a subnet. This field can also be set with the LAN IP address in order to route messages from any host when the Destination type is set to Voice Mail.

NOTICE:

Source IP supports both IPv4 and IPv6 addresses.

- **Condition (error codes)** - The reply code list used to reroute the messages. The codes are separated using semicolons. If **Destination Type** is set to Voice Mail, codes from 640 to 690 may be used to set ringing timeout for calls whose original destination is a registered subscriber. The default timeout is 16 seconds for this case and it may be changed as follows: 16 + code - 650, or simply code - 634. For instance, a ringing timeout of 6 seconds can be set by adding the code 640 (640 - 634 = 6) to the list. Note that it is required to define at least one error code in the list. If more than one code from 640 to 690 is added, only the last one will take effect. If the destination of a call is a gateway or if the Destination Type is not Voice Mail, ringing timeout is always 180 seconds.
- **Destination IP or FQDN** - This is the configuration of the destination of the message to be routed.
- **Destination port** - This is the port to be used when routing messages to the destination.
- **Transport** - This defines the protocol to be used when routing messages to the destination.
- **Destination tag** - This box defines a tag to be added to re-routed SIP headers. The SIP manipulation rules do not apply to the Destination tag.
- **Destination type** - The destination type determines the type of route used for the rule. A route type can be of type Gateways or other SIP endpoints.

System Call Forwarding has precedence on rerouting configurations in the SIP Routing table. Refer to the Call Forwarding section.

NOTICE:

SIP Routing is not permitted in Proxy ATA mode

To delete a rule, first click on the rule to select it and then click **Delete**.

Source Based Manipulation

This configuration provides source-based routing (based on the Caller's number) for incoming gateway calls, to allow routing to different destinations.

NOTICE: For Integrated Gateways, **TON manipulation** will be executed before **Source Based Manipulation**. In Survivability mode, **SIP Manipulation** will be executed after **Source Based Manipulation**.

Click **Add** to add a new rule. To delete a rule, first click on the row in the table to select it then click **Delete**.

- **Matching Identity Header-** This field defines what **Identity Header** is searched for a match. It can be the headers FROM, P-AI, or P-AI that changes to FROM is P-AI is not present.
- **Source Match digits-** The matching digits are defined in this field. Only numerical digits and the characters *, # and + are supported.
- **Source Match position-** This field is used to define from which digit position the search is performed on the header. The first position is 0.
- **Source Min/Max Length-** Enter a valid value (format x, x/, or x/y). This field defines how many digits it will try to match, with the Source Match position as a reference.
- **Manipulation Header** - The header that will be manipulated. At this time, the only supported header is the R-URI.
- **Delete/insert position** - This field defines from which digit position in the header the fields **Number of digits to delete** and **Insert digits at position** are applied. If the value of this field does not correspond to an effective position in 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. Only numerical digits and the characters *, # and + are supported.
- **Add prefix** - This field is used to set the prefix to be added to the digits in the header. Only numerical digits and the characters *, # and + are supported.
- **Replace all with** - The digits that will replace all header digits. Only numerical digits and the characters *, # and + are supported.
- **Call type-** The only supported Call Type for this mode is PSTN-SIP.

6.4.4 VoIP > Error Codes

Error Code Settings

Survivable Mode

- **Enable routing for all codes** - If checked, the Enable routing in Survivable Mode column in the table will have all checkboxes checked.

IMPORTANT: Configuration for error codes 401 and 407 is not allowed in Normal Mode.

- **Disable routing for all codes** - If checked, the Enable routing in Survivable Mode column in the table will have all checkboxes checked.

NOTICE:

Error codes in SM are not allowed for Proxy ATA mode.

Normal Mode

- **Enable routing for all error codes** - If checked, the Enable routing in Normal Mode column in the table will have all checkboxes checked.
- **Disable routing for all error codes** - If checked, the Enable routing in Normal Mode column in the table will have all checkboxes unchecked.

Table

- **Error code** - Configurable SIP error codes. Gateway failover rerouting is blocked for all error codes that are not configured.

NOTICE:

Re-routing is granted for error codes enabled in the **VoIP->Error Codes** tab. The number of the error codes is specific for each installation, depending on the provider or on which error code you want to make a reroute (for example 503).

- **Description** - A brief description of the error code.
- **Enable routing in Survivable Mode** - If checked, the error code will be rerouted when the Branch is in Survivable Mode.
- **Enable routing in Normal Mode** - If checked, the error code will be rerouted when the Branch is in Normal Mode.

6.4.5 VoIP > Media

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.
- **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. 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 OSB 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.

LAN Media Configuration

- **Media profile** -Assign a media profile that has been created in the **Media profiles** tab under **VOIP**

Media Profiles

- **Profile name** - A unique profile name must be entered
- **Codecs** - Select a codec and add it to the list of codecs
- **Media protocol** - The user chooses between unsecure and secure RTP or if the payload is passed through. Possible values: 'Strict Pass-Thru', 'Best Effort SRTP', 'SRTP Only', 'RTP'. Default value: 'Strict Pass-thru'
- **Key exchange method** -Choose if between the key exchange methods
- **Mark sRTP Call leg as Secure** -Marks the FXS leg as secure independent of the actual payload security
- **Single m-line SRTP** -Indicates if the key exchange mechanism is negotiated with a single or dual m-line SDP

RTP

- **RTCP interval (ms)** - Represents the period of time in milliseconds between RTCP reports.
- **RTP protection** - It is used to enable/disable strict RTP protection.
- **Jitter buffer** - It is used to enable/disable the jitter buffer.
- **JB minimum delay (ms)** - Length of the jitter buffer in milliseconds. Range from 0 to 300. JB Minimum Delay cannot be higher than JB Maximum Delay. This field is configurable only if Jitter buffer is enabled.
- **JB maximum delay (ms)** - The maximum delay before the jitter buffer is resynchronized discarding the packets inside the jitter buffer. Range from 0 and 500. JB Maximum Delay must be higher than JB Minimum Delay. This field is configurable only if Jitter buffer is enabled.

- **Implementation** - This field is used to configure the jitter buffer implementation. The possible values are: Fixed, Adaptive, on fax detection, data always. It is enabled if Jitter buffer is enabled.

NOTICE:

Data transmission is very sensitive to timing issues. It was introduced as a means to buffering information and dealing with network jitter in the hardware drivers. This option is configured by setting the jitter buffer implementation to **Data Always**, which improves fax pass-through transmissions. Unfortunately, this option, as any jitter buffer implementation, adds a delay in the packets transmission, which causes some issues (voice delay, DTMF detection problems). Therefore, an option was also added, to use these buffers only for fax transmission, enabling the option **On Fax Detection**, which is recommended for use.

NOTICE:

Fixed and Adaptive Implementation are implemented in the application levels and are not indicated for timing constraint data transmissions, like fax or modem.

- **Packetization time (ms)** - The interval between the RTP packets. Allowed values are 10, 20 and 30 ms
- **Dtmf Forward Twist (dB)** - sets the maximum threshold in the forward twist for the DTMF to be detected by OSB. Dtmf Forward (positive) Twist is the difference in dB between row (lower frequency) and column (higher frequency) energies for dtmf frequencies, when column energy is greater than the row energy. This value should be adjusted only if DTMF is not being correctly detected or voice is being wrongly detected as DTMF.

Default value: 8 dB. Possible values: 4, 5, 6, 7, 8, 9, 10.

- **Dtmf Reverse Twist (dB)** - sets the maximum threshold in reverse twist for the DTMF to be detected by OSB. Dtmf Reverse (negative) Twist is the difference in dB between row (lower frequency) and column (higher frequency) energies for dtmf frequencies, when column energy is lower than the row energy. This value should be adjusted only if DTMF is not being correctly detected or voice is being wrongly detected as DTMF.

Default value: 4 dB. Possible values: 4, 5, 6, 7, 8, 9, 10.

If country is set to **United States/North America** or **United States Circa 1950/North America** the default value of DTMF Reverse Twist is 9 dB.

- **Dtmf Hits to Begin** - the amount of samples with specific DTMF frequency with energy enough to be considered a digit that will be considered to starting detecting a DTMF digit. The sample length in the OSB is 12,5ms. The default value is 2, which means a DTMF with minimum length of 38.5 ms would be detected, considering the digit is started at the middle of a sample. For short DTMF signals, e.g. lower than 50ms - usually used in caller identification DTMF sequences on analog trunks (FXO), in some cases if a sample is not considered a hit for any reason, the DTMF detection may fail, then this value may be tuned to 1.
- **Dtmf Hits to End** - the amount of samples not containing the current detected DTMF digit to consider the DTMF digit is finished. The default value is 3 (38.5ms).

- **Minimum Dtmf Duration (ms)** - The minimum DTMF signal length detected by OSB iGW. The value for silence interval between digits is 45msec and is fixed. Default value is set at 80 msec. Available range: 40-120msec.

IMPORTANT:

Minimum Dtmf Duration affects DTMF detection not only for CID, but the overall detection for calls.

IMPORTANT:

Some providers send short DTMFs to shorten the dialing duration. For that reason, **Minimum Dtmf Duration** needs to be tuned accordingly.

- **Enable RFC2833 support** - Enables RFC2833 support for sending DTMF digits. If the flag is enabled, the user of RFC will be negotiated between parties. If the flag is disabled, DTMF digits are transmitted inband.
-

NOTICE:

RTP configuration is enabled if Integrated Gateway is enabled.

- **Cancel DTMF transmission on reinvite** - Disabled by default. Stop an ongoing RTP Event, sending DTMF digit, if media renegotiation unhold is requested. This flag can only be set if **Enable RFC2833 Support** is set.
- **Send DTMF end using ptime** - When enabled, this flag will send the three DTMF END (final) packets using the ptime interval between them, otherwise the three DTMF end (final) packets will be sent in a burst at same time. Enable this flag if any DTMF end packets are being lost.
- **Use Restrict V29 FAX Frequency** - Changes V29 Fax carrier frequency tolerance from 2Hz to 1Hz. This flag must be set only if after a V29-9600 training or page transmission a V21 signal is wrongly detected as V29. This may happen because some fax machines have a V21 frequency close enough to the V29 frequency that it fits in OSB V29 detection tolerance.

Session Recording Client

The Session Recording Client (SRC) tab allows the configuration of SIP Recording Server, which will record RTP streams using SipRec protocol.

SipRec restrictions

- 1) Secure calls will not be recorded
 - 2) Only audio will be recorded
- **Enable recording** - This flag enables the Session Recording Server.
-

NOTICE: This flag must be enabled when the SIPREC based OpenScape Voice Call Recording solution is enabled.

- **Record All Calls** - When in **Survivable Mode**, this flag records every call. When in **Normal Mode**, this flag signals to OSV that this OSB is record-aware and supports recording.

NOTICE:

All calls will be anchored in both modes.

NOTICE: This flag must be enabled when the SIPREC based OpenScape Voice Call Recording solution is enabled.

In order to record only calls from specific Gateway/Trunk check **Record calls from this Gateway/Trunk** under **Gateway Configuration** (refer to [Features > Integrated Gateway](#))

- **Priority** - Recorder priority (Doesn't have effect for OSB - limited to one recorder).
- **Server Address** - IP or FQDN of the recorder.
- **Server Port**- Port in which the recorder should be listening for SIP messages.
- **Protocol** - Drop-down box with UDP/TCP/TLS option. If TLS is selected as protocol, it is expected to have mutual authentication between SRC and SRS. TLS is the recommended option.

NOTICE: When the SIPREC solution is enabled, the **Priority**, **Server Address**, **Server Port** and **Protocol** fields must be populated with the corresponding information of the SIPREC server.

6.4.5.1 VoIP > Media > Media Profile

General

- **Name** - Available options: default, igw_acd_aa_lan.
Media profile **igw_acd_aa_lan** is applied to calls involving integrated gateway as well as calls connected to Backup ACD and Auto-Attendant.
- **Media protocol** -The user chooses between unsecure and secure RTP or if the payload is passed through. Possible Values: 'Strict Pass-Thru', 'Best Effort SRTP', 'SRTP Only', 'RTP'. Default value: 'Strict Pass-Thru'
- **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:

This flag is available only when the **Enable LAN-SSP media interwork** flag is enabled.

NOTICE:

The **SDP Compatibility Mode** flag is disabled by default.

SRTP Configuration

- **Key exchange method** -Possible values: none, mikey, sdes, mikey+sdes, dtls(circuit only)
- **Mark sRTP Call leg as Secure** -Marks the FXS leg as secure independent of the actual payload security
- **Single m-line SRTP** -Indicates if the key exchange mechanism is negotiated with a single or dual m-line SDP

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** -If the received SDP offer contains codecs that are not configured in the media profile of the B-side these codecs shall be passed through to the B-side.

NOTICE:

This flag cannot be checked along with the **Enforce codec priority in profile** check box

- **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 OSB.
- **Use payload type 101 for telephony event/8000** - Disabled by default. This flag allows OSB 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 use to negotiate the telephone-event payload type sending in the SDP answer the payload type 101 for the telephone-event/8000 even if another payload type was used in the SDP offer. It may cause the DTMF tones not be recognized between the parties This flag should be enable in the Media Profile of the destination endpoint. The codec list of this Media profile MUST not be empty.
- **Enforce Packetization interval** - Each codec has its own packetization interval that can be selected from a drop 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.

NOTICE:

if the checkbox **Allow unconfigured codecs** 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** - This drop-down box presents a list of codecs that are available to be added to the profile. Selecting a codec and then clicking the **Add** button will result in the codec appearing in the table below.
- **Table** - This table presents the list of codecs that are assigned to the media profile. The "Priority" column indicates their relative priority to each other. The priority order can be adjusted by clicking the **Move up** or **Move down**

buttons. The delete a codec from the table first click it to select it and then click the **Delete** button.

6.5 Features

This screen provides access to all of the features of the Branch.

Features Available in Normal Mode and Survivable/Standalone Mode

- **Gateways and Trunks** - Checking this checkbox will enable the "Configure" button, which, when clicked, will open a new screen for configuring gateways and trunk groups.

NOTICE:

Because Gateways and Trunks are not allowed in Proxy ATA mode, this entry will not be visible on the screen in that mode.

- **Integrated Gateway** - Checking this checkbox will enable the "Configure" button, which, when clicked, will open a new screen for configuring the Integrated Gateway. The user can configure the various characteristics of the different types of PSTN interface board, depending on the type(s) of board(s) installed. Interfaces supported include PRI (T1 and E1), BRI (E1), FXS, and FXO. Integrated Gateway configuration applies to the OSB 50i and OSB 500i.

IMPORTANT:

For the 50i models, considering a migration to SIP, it is possible to increase the performance by disabling the integrated gateway feature, i.e., by keeping the **Enable integrated gateway** flag unchecked.

- **Ring down channels**- Table with the summary of E1 CAS channels configured as Ring Down.
 - **Enable**: Enabling/Disabling setting for the channel.
 - **Channel**: Shows Card, Port, and Channel Number (read-only).
 - **Trunk group**: Shows the trunk group name the channel is associated to (read-only).
 - **CAS signalling**: The signalling of the selected channels. It defines the protocol the Gateway is configured with the CO (read-only).
 - **CAS profile**: Select a profile from the available profile list.
 - **Own number**: Destination which will be notified in case of an incoming call. For MRD and Hoot-n-Holler, this is the exclusive extension, which can perform outgoing calls (only for Ring Down channels).
 - **Ring-down destination**: Destination which must be dialed after the PNAC to access the respective channel for an outgoing call (only for Ring Down channels).

NOTICE: This entry will be visible only for E1 PRI/CAS integrated gateway.

- **SIP Service Providers -**

NOTICE:

SIP Service Providers are only permitted in SBC Proxy and Branch SBC modes.

- **Auto Attendant** - Checking this checkbox will enable the "Configure" button, which, when clicked, will open a new screen for configuring the Auto Attendant.

NOTICE:

Because Auto Attendant is not allowed in Proxy ATA mode, this entry will not be visible on the screen in that mode.

- **Phone Software Management** - Checking this checkbox will enable the "Configure" button, which, when clicked, will open a new screen for configuring when phone software loads get pulled from a central server, as well as enabling the ability of phones to retrieve software from the Branch.
- **Media Server** - Checking this checkbox will enable the "Configure" button, which, when clicked, will open a new screen for configuring the Media Server.
- **LAN-WAN Media Interworking -**

NOTICE:

Only supported in SBC Proxy and Branch SBC modes.

- **Codec Support for Transcoding** - The Codec Support for Transcoding is enabled using the Enable Codec Support for the **Transcoding** check box. Clicking on the **Configure** button launches the **Codecs** window where various Codecs 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 OSB is always associated to the default media profile.
- **Backup Link** - Checking this checkbox will enable the drop-down box and the "Configure" button, which, when clicked, will open a new screen for configuring the Backup Link Client or the Backup Link Server, depending on the selection made in the drop-down box.

NOTICE:

Because Backup Link is not allowed in Proxy ATA mode, this entry will not be visible on the screen in that mode.

Features Available in Survivable/Standalone Mode Only

- **Multiline Hunt Groups** - Clicking the "Configure" button will open a new screen for configuring the Multiline Hunt Groups.

NOTICE:

Because Multiline Hunt Groups are not allowed in Proxy ACD mode or Proxy ATA mode, this entry will not be visible on the screen in these modes.

-
- **Automatic Call Distribution** - Clicking the "Configure" button will open a new screen for configuring the ACD Groups.

NOTICE:

Because ACD is only allowed in Proxy ACD mode, this entry will only be visible in that mode.

-
- **Emergency Calling** - Clicking the "Configure" button will open a new screen for configuring the emergency calling numbers and subnets.
 - **Call Forwarding** - Clicking the "Configure" button will open a new screen for configuring system-wide call forwarding.
 - **Call Detail Records** - Checking this checkbox will enable the "Configure" button, which, when clicked, will open a new screen for configuring how call detail records should be handled in Survivability Mode.
 - **Music on Hold** - Checking this checkbox allows the user to turn on system-wide music on hold for either gateways only, or for gateways and subscribers, applicable when the Branch is in Survivability mode. The drop-down box, which gets enabled when the checkbox is checked, is used to make the selection. If the checkbox is not checked, subscribers may still hear music on hold if their local device is capable of playing it.

NOTICE:

This setting applies to registered SIP subscribers only. It does not apply to FXS subscribers.

NOTICE:

This setting does not apply in Proxy ATA mode.

IMPORTANT: The negotiation with internal Media Server may delay the messages sent to the target endpoint (gateway or subscriber).

-
- **System Calling Number Suppression** - Checking this checkbox allows the user to turn on calling number suppression for outgoing calls that use

the Integrated Gateway. When activated it prevents the presentation of the calling party number (the Branch subscriber number) to the called party.

NOTICE:

This field applies to PRI, BRI, and FXO calls only.

NOTICE: This feature must be supported by the far-end CO.

NOTICE:

System Calling Number Suppression is not allowed for Proxy ATA mode.

The Calling Number Suppression Access Code allows the Branch subscriber to use the Calling Line Identification Restriction (CLIR) feature on a per-call basis.

This code can be configured with up to 24 digits, including * and #. To block the presentation of the calling party number to the called party, the calling party must enter the configured access code at the beginning of the dialing sequence, prior to any gateway routing prefix or the called party number.

6.5.1 Features > Gateways/Trunks Provisioning

General

A new gateway/trunk can be created by clicking the **Add** button. An existing gateway/trunk can be edited or deleted by first clicking the applicable row to select it and then clicking the **Edit** or **Delete** button respectively.

IMPORTANT:

In Standalone Mode, when adding gateways to the gateway table, the only gateway types allowed are **Integrated Gateway** (LAN interface) and **SIP Trunk" (WAN Interface)**.

- **DNS dynamic refresh interval (min)** - Minimum value in minutes to refresh DNS. The default value is 60 min.
- **Route to R-URI domain** - If enabled, OSB will honor the domain in the R-URI received from OSV, i.e., the call will be routed to the gateway addressed in the R-URI received if it is configured in the gateway table. The routing prefix will only be used to route the calls if the R-URI domain is not configured in the gateway table.

NOTICE:

Re-routing is granted for error codes enabled in the **VoIP->Error Codes** tab. The number of the error codes is specific for each

installation, depending on the provider or on which error code you want to make a reroute (for example 503).

The table provides an overview of some key parameters associated with the gateways and trunks. The fields are as follows:

- **Signaling address type**- Identifies how the **IP address/FQDN** parameter shall be used for addressing the Gateway/Trunk.

NOTICE:

The Signalling address type DNS SRV is allowed only if the Gateway is a SIP Trunk.

- **Remote URL** - Can be either IPv4 if it is configured in the LAN interface or IPv6 if configured on the WAN interface. If IPv6 is enabled the parameter Mapped Port shall be enabled and the option WAN shall be possible for the parameter Interface.
- **Port** - This box is used to configure the SIP port of the gateway/trunk.
- **Interface** - This box is used to configure the Gateway/Trunk Interface. WAN interface is valid only for SBC and Branch SBC-Proxy modes. LAN interface is also valid for OSB Proxy SBC and Branch SBC-Proxy ACD mode WANs.
- **Transport** - This combo defines the SIP transport protocol to be used in communication with the gateway/trunk. The supported Transport types are UDP, TCP and TLS.
- **Mapped port** - This box defines the gateway/endpoint mapped port for external IP addresses. The range of LAN gateways depends on the configured SIP ports range of Port Map. For WAN gateways, the valid mapped port range is from 21000 to 21255.
- **Routing prefix** - This box defines a valid Dial Number to be used in search for the gateways/trunks. When the Dialed Number matches the user part of Request-URI the corresponding gateway/trunk will be connected. Regular expressions may be used for matching. Only numerical digits and the characters *, # and + are supported as literals. The literal * and + must be inside of []. 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).
 - [^<list-of-characters>] Matches a character that is not contained within the brackets.

IMPORTANT: The “-“ suggests a range of numbers but can’t be used without []

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.

For further information refer to [Configuration of Gateways](#)

Special usage when Functional type = Emergency

The Routing Prefix has a special meaning: its first digits identify which dialed Emergency Number may address this gateway. For example, prefixes like "91122" or "91133" will restrict the gateway for outgoing emergency calls using a configured "911" Emergency Number.

The prefixes configured here will be later available at Emergency Subnet configuration pages.

- **Incoming Route Prefixes** - This table is used to route the calls in Normal & Survivability mode. It only shows if the gateway/trunk type is set to SIP Trunk.
- **Gateway/Trunk type** – This field defines the following types of gateways/trunks:
 - 3k/4k – HiPath 3000 or HiPath 4000 as gateway
 - RG – RG2700 and R8700 gateway
 - Mediatrix – Mediatrix gateways
 - Peer OSB – Another Branch used as gateway

NOTICE:

Peer OSB's will have the Functional Type set to **Survivability Mode Egress / Ingress** for OSB routing to the peers during Survivability Mode.

Peer OSB is not allowed in Normal mode since OSV handles all call routing decisions involving trunk access while the OSBs are in normal mode.

-
- SIP Trunk – Trunk using SIP protocol
 - Integrated Gateway – Integrated Gateway (50i/500i)
 - Backup Link Server – Backup Link Server
 - Voicemail
 - OSB with SSP – OSB with an IPv6 SSP as Gateway Only configured in the OSB

NOTICE:

This option shall only be presented if the **Gateway Only** flag is disabled

-
- Others

- **Functional type** – This field defines the following functionalities of gateways:
 - All Modes Egress/Ingress – Set the gateway to make outgoing calls and accept incoming calls in Normal or Survivability Mode.
 - All Modes Ingress – Set the gateway to accept incoming calls in Normal or Survivability Mode.
 - Normal Mode Egress/Ingress – Set the gateway to make outgoing calls and accept incoming calls only in Normal Mode.
 - Survivability Mode Egress/Ingress – Set the gateway to make outgoing calls and accept incoming calls only in Survivability Mode.
 - Emergency – If an emergency call in Survivability Mode is set, this route will be used to execute the call. If no emergency is found, the first egress route will be used.

Note: For SIP Trunk this field must be set as All Modes Egress/Ingress. Incoming and outgoing calls will be accepted in Normal or Survivability Mode.
- **Trunk profile**- Set the trunk profile, selecting a SIP Service Provider Profile. For gateways and Peer OSB this field must be set as Gateway. The SIP Trunk profile can either be type "Gateway" or a profile out of the SSP profile list. SSP and Gateway is valid for SBC and Branch SBC-Proxy modes.

NOTICE: If the flag **Registration required** is **enabled** in the Sip Service Provider profile, different Trunk profiles must be used for different Gateways/Trunks.

IMPORTANT: For SIP Trunk, this field must be a Sip Service Provider profile, trunk profile Gateway is not allowed for SIP trunk.

IMPORTANT: You may configure up to 2 Trunks and you can have up to 60 concurrent Trunk calls.

NOTICE:

In the Proxy-SBC mode (not Gateway only), OSB supports SIP Trunks using IPv6. IPv6 is only allowed in the WAN interface so the OSB will only be able to handle support SIP Trunks in the LAN using IPv4.

IMPORTANT: When the SIP Trunk is configured in terms of DNS SRV or FQDN, it is necessary to configure at least 2 mapped ports (max of 10 ports), in order to assign one mapped port to each IP resolved. If DNS SRV is set, the configured FQDN will also need a mapped port. If the Outbound Proxy address is set, it also needs one additional mapped port.

IMPORTANT: The SIP Trunk configured as DNS Server can use up to 10 mapped ports when the Outbound Proxy is set.

If the Outbound Proxy isn't set, the number of mapped ports will be 5.

- **Output digit strip** - The number of digits to be deleted of the destination URI. The digits are deleted from the beginning.
- **Output digit add** - This box configures a digit string to be added to digits of URI. The digits are added to the beginning.
- **Priority** - This combo defines which gateway/trunk will be used first if more than one matches. Lowest number has the highest priority. If a default gateway is required this gateway priority should be set to 0.
- **Operational Mode in OPTIONS Response** - This flag controls if the operational state will be returned as part of the response for OPTIONS messages sent by the gateway.

IMPORTANT: If using different PRIs on one single RG8700 as failover routes of each other then transport protocol must be set to TCP in survivability mode.

IMPORTANT: It is not allowed to configure the same IP or FQDN for different Gateway/Trunk types.

IMPORTANT:

Gateways must be of type **Others, Integrated Gateway, SIP Trunk or Peer OSB** when in **Proxy ACD** mode.

IMPORTANT: If there are two or more gateways with the same IP Address or FQDN, Operational Mode in OPTIONS Response flag must be enabled/disabled for all these gateways.

Signaling

- **INVITE No Answer timeout** - timeout until the party answers the call, otherwise will be dropped. Valid values: **120 to 360 seconds**.
- **INVITE No Reply timeout** - timeout to wait for a 100 Trying being responded after the INVITE. Valid values: **1 to 32 seconds**.

TLS

- **TLS mode** - Allows the selection between Server Authentication, Mutual Authentication and Client Mode. All the parameters are valid only if the transport type is configured as TLS.
 - Server Authentication - In this case only the server is being authenticated by the client.
 - Mutual Authentication - In this case the server and the client authenticate each other.
 - Client Mode - Prevents 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 Branch as a TLS client.

- **Keep-alive interval (seconds)** - Determines the interval between sending the keep-alive requests. Valid values: 60 - 3000 seconds, default: 120.
- **Keep-alive timeout (seconds)** - 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** - Assign a media profile that has been created in the **Media profiles** tab under **VOIP**.
- **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.

- **Media realm subnet mask** - Subnet mask used for media negotiation.
- **Anchoring media** - Choose between forced and auto media anchoring. If set to automatic, the media optimization will be used whenever possible. If set to forced media, it will be always be anchored by the OSB.

Possible values: **forced,auto**. Default value: **forced**

- **Force media optimization on transcoding** - Enables media optimization when media is not anchored & transcoding is active. This checkbox is disabled if **Anchoring Media** is set to **forced**.

WAN Media Configuration

- **Media profile** - Assign a media profile that has been created in the **Media profiles** tab under **VOIP**
- **Anchoring media** - Choose between forced and automatic media anchoring. Possible values: 'forced', 'auto'. Default value: 'forced'
 - **Force media optimization on transcoding** - Enables media optimization when media is not anchored and transcoding is active. This checkbox is disabled if **Anchoring Media** is set to 'forced'
 - **Record calls from this Gateway/Trunk** - Enables recording using SIPREC protocol for this specific gateway. Default is unchecked.

NOTICE: This flag interacts with flag "Voip-> Media-> Record All Calls". Please refer to the help section for the complete description.

NOTICE: This flag must be enabled when the SIPREC based OpenScape Voice Call Recording solution 'proxy mode' is enabled.

- **Allow Asymmetric RTP** - In the case of Gateway on the WAN or Sip Trunk on LAN or on WAN side, the RTP flow is always set as symmetric in the OSB. Therefore, the RTP packets must be received from the same port negotiated in the SDP, in which the OSB will be sending the RTP packets. If this is not true, the OSB will automatically start sending the packets to the source port of RTP packets received from the remote side. To change this behavior the flag **Allow Asymmetric RTP** may be

enabled. In this case, the OSB will not update the destination port based on the source port of the RTP flow. The default is disabled. This flag is applicable only for Gateway on the WAN or Sip Trunk on LAN or WAN, in which the media is anchored by the OSB.

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.

Miscellaneous

NOTICE:

The following configuration is available only for SIP trunks.

- **UDP-SIP keep -alives** - Enable the keep-alive mechanism if the connection was established by the OSB as a UDP client.

- **Keep-alive time (sec)** - Determines the interval between sending the keep-alive requests.
- **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 is only available for OSB Branch SBC and Proxy-SBC modes & SIP Trunks.

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.

Same way as the "Open External Firewall Pinhole", the dummy RTP 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.

NOTICE:

This feature only applies to the addresses and ports used for the media streaming. It is not applicable to the SIP or MGCP protocols. Starting from V10R3.4.0, 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.

6.5.2 Features > Integrated Gateway

Country Configuration

- The country field is read-only on this screen. To change it, refer to the "System" / "Settings" screen. When the Country is set, various parameters such as hookflash timers, ring cadence and tone frequencies are set up accordingly. Click the "Country configuration" button to see a read-only list of the full set of parameters. This setting applies to the Integrated Gateway and to the ACD and Auto Attendant features.

Gateway Configuration

- **Card 1 and Card 2** - These fields show the type of PCI card(s) that is(are) installed in the Branch. Supported card types are: FXS, FXO, BRI, and PRI.
- **Configure...** - For the OSB 50i, there is a separate "Configure..." button for each card, whereas for the OSB 500i there is a single button that applies

to one or both of the installed PRI cards. When this button is clicked, a new screen opens that has card-specific configuration parameters.

- **Trunk group...** - Trunk groups can be configured for FXO, BRI and PRI cards. When this button is clicked, a new screen opens that allows the user to set up the various per-trunk group parameters.
- **Per card clock source** - This checkbox applies for the OSB 500i only. For the OSB 500i with a single PRI card, the checkbox is set and disabled. For the OSB 500i with two PRI cards, when set the Clock Source Priority is split between each card. In other words, the PRI clock information is not transmitted from one card to the other. If not set, the user can use any of 8 ports as the clock source for the system by setting the Clock Source Priority field for the various PRI links from 1 to 8. A special Timing Cable must be installed to be able to utilize this capability.
- **Disable FXO audit** - This checkbox manages to disable the 12 hours audit for all FXO ports. In the OSB, all FXO calls have by default an audit that disconnect the call after 12 hours. This checkbox changes this behavior and if enabled, the call is not disconnected.

QoS Monitoring

- **Enable QoS monitoring** - Checking this checkbox will enable the "QoS monitoring configuration" button, which, when clicked, will open a new screen that permits the user to set up the QoS monitoring parameters.

Local Toll Tables

NOTICE:

These fields are only applicable when the country is United States / North America or United States Circa 1950 / North America.

- **Local Toll Tables** - Show which LTTs have been imported to the OSB, as well as offering the ability to view and delete the LTTs from the OSB.

Clicking this button refers to [Features > Integrated Gateway > Local Toll Table Configuration](#)

6.5.2.1 Features > Integrated Gateway > BRI Configuration

Card Configuration

- **Access type** - Sets the BRI Access Type. It can be PP - Point-to-Point or PMP - Point-to-Multi-Point. Default value is PP.
- **MSN** - A list of up to 10 MSN that are handled by the Branch. The MSN are from 1 to 24 digits long. The list can be empty and this configuration item is only available for BRI in mode PMP.

- **HW Echo Cancellation** - Enable hardware echo cancellation on BRI ports. If this flag is disabled, software echo cancellation will be used.

Fax T.38

- **Fax T.38** - Enables BRI card T.38 negotiation for fax. It is enabled using the enable check box.
- **CNG Detection** - Enables detecting CNG tone for T.38 fax negotiation. It is enabled using the enable check box. The activation of the flag "CNG detection" will only take effect if T.38 flag is also enabled.

NOTICE:

T.38 fax calls always start as a voice call and then switch to the T.38 codec.

Port Configuration

- **Enable** - Enable or disable the BRI physical port.
- **Physical port** - The port number of the BRI port. It is a ready-only field.
- **Clock source priority** - It sets the clock source priority. The priorities must be different between the BRI ports, except for priority 0. Priority 0 means that this port will not be used as a clock source for the card / system.
- **Echo tail(ms)** - Echo tail for Hardware Echo Cancellation. Available values: "none", 16 msec, 32 msec, 64 msec, 128 msec (VPM based)
- **Switch type** - It sets the protocol by a combo box. Only euroisdn is supported at this time.
- **Exclusive channel** - It is set to enable/disable exclusive channel.
- **Idle Reset interval** - It sets the time in seconds between restart of unused B-channels. If the field is empty, the functionality is disabled.
- **Receive Gain** - It sets the Gain of payload for receive. A negative value decreases the gain, and a positive value increases the gain.
- **Transmit Gain** - It sets the Gain of payload for transmit. A negative value decreases the gain, and a positive value increases the gain.
- **Default destination** - It is the destination number if no called party number is received for ISDN incoming calls. The default destination is also used if just one digit is received and there is no rule to handle it in the Specific Overlap Dialing Patterns table.
- **T302 timer** - It is the timer to wait for digits.
- **Far end disconnect with inband announcement** - It is set to enable/disable disconnect with inband announcement.
- **B-channel parallel restart** - if flag is enabled RESTART message for each individual b-channel is sent simultaneously for all b-channels. If flag is disabled RESTART is sent for first b-channel and RESTART ACKNOWLEDGE is required for this b-channel before sending RESTART to next b-channel.
- **Always Send PI8 in Alerting** - if flag is enabled the Branch sends ALERTING with PI8 (progress indicator: In-band information or an appropriate pattern is now available) whenever a 180 Ringing (without SDP)

is received. Otherwise PI8 will be sent only when a 180 Ringing with SDP is received."

IMPORTANT: For in band announcements, PI=1 and PI=8 are supported in PROGRESS, ALERTING and CALL PROCEEDING messages. When one of these messages is received with PI=1 or PI=8, voice path is open and inband tones could be heard by the caller if available. Additionally, PI=8 can be supported in DISCONNECT message if flag "Far end disconnect with inband announcement" is enabled

- **Setup progress indicator** - Configures the Progress Indicator in SETUP message. If the received INVITE does not contain any SDP, no progress indicator is sent, regardless of the configuration. The following options are supported:
 - Call is not end-to-end, ISDN further call progress information may be available in-band.
 - Destination address is non ISDN.
 - Origination address is non ISDN.
 - None.
- **Start early media on CALL PROCEEDING** - This command will cause the Branch to raise a SIP 183 Session Progress message with an SDP Answer as soon as it receives the ISDN CALL PROCEEDING message. The SIP 183 Session Progress response will contain a "P-Early-Media" header field (RFC5009) with a new proprietary value ("fast-connect"). If an ALERTING is received afterwards, the Branch will send back a SIP 180 Ringing response with SDP Answer and without the "P-Early-Media" header. This flag will be ignored if INVITE received does not contain SDP.
- **183 Session Progress without SDP** - Comm System sends a 183 Session Progress response code without SDP (i.e, without inband announcement) in some situations (for ex, call processing delayed and no information about the called party is available till this point). This configuration item allows choosing how this response code must be informed to the PSTN caller according to the carrier requirements. This action intends to stop timer T309 avoiding the disconnection of call by the caller side. Possible values:
 - Progress: response code is converted to ISDN PROGRESS message including the Progress Indicator #2 - called party is non-ISDN (Default for PRI switch types: NI-2, 4ESS and 5ESS)
 - Progress and Alerting: response code is converted to ISDN PROGRESS message including the Progress Indicator #2 (destination is non-ISDN) followed by an ISDN ALERTING message.
 - Alerting: response code is converted to ISDN ALERTING message. (Default for PRI switch type EuroISDN and BRI interfaces)
 - None: response code is discarded.
- **Disable far end restart** - In scenarios in which 50i is connected to a CO switch that does not accept RESTART message during BRI span bring up. The flag is recommended for use in BRI PMP systems.

NOTICE:

If the parameter 183 Session Progress without SDP is set to Progress and Alerting, it will supersede the parameter "Always Send PI8 in Alerting". So, if the parameter 183 Session Progress

without SDP is set to Progress and Alerting and flag Always Send PI8 in Alerting is enabled the Alerting will be sent without PI8 as determined by the parameter 183 Session Progress without SDP. In this case, if a 183 Session Progress without SDP is received a Progress and an Alerting are sent. When the 180 Ringing is received on the SIP side, no further Alerting shall be sent because the Alerting message had already been sent.

NOTICE: If the parameter 183 Session Progress without SDP is set to Alerting, it will also supersede the parameter "Always Send PI8 in Alerting", so the Alerting will be sent without PI8. If 183 Session Progress without SDP is set to None, the Alerting will result from 180 Ringing and it will contain a PI8 if the "Always Send PI8 in Alerting" is enabled.

6.5.2.2 Features > Integrated Gateway > FXO Configuration

Fax T.38

- **Fax T.38** - Enables FXO card T.38 negotiation for fax. It is enabled using the enable check box.
 - **CNG Detection** - Enables detecting CNG tone for T.38 fax negotiation. It is enabled using the enable check box. The activation of the flag "CNG detection" will only take effect if T.38 flag is also enabled.
-

NOTICE:

T.38 fax calls always start as a voice call and then switch to the T.38 codec.

Port Configuration

- **Enable** - Enable or disable the FXO physical port.
- **Physical port** - The port number of the FXO port. It is a read-only field.
- **Signaling mode** - It configures the signaling mode. Only Loopstart is available.
- **Answer by polarity reversal** - Configuring the gateway to enable/disable the detection of answer via silent reversal.
- **Disconnect by polarity reversal** - Configuring the gateway to enable/disable the detection of disconnection via silent reversal.
- **Polarity reversal delay hang up (ms)** - The minimum time interval between the answer polarity switch and hang up polarity switch and only used if Answer and Disconnect by polarity reversal are enabled.
- **Loop supervision** - It is set to enable/disable loop supervision. If enabled, the signaling mode is set to Kewlstart.
- **Echo cancellation** - Echo cancellation for Hardware Echo Cancellation. Available values: "none", 16 msec, 32 msec (OSLEC based)
- **Receive gain(dB)** - It sets the Gain of payload for receive. A negative value decreases the gain, and a positive value increases the gain.

- **Transmit gain(dB)** - It sets the Gain of payload for transmit. A negative value decreases the gain, and a positive value increases the gain.
- **Ring detection timeout(sec)** - Timer in seconds indicating the amount of time after which incoming FXO calls would timeout if they remain in ringing state. Note: Care should be taken in reducing this timer to a low value as it would have an impact on features also using the ring no answer timers e.g. Call forward no answer, Voice Mail, etc.
- **Caller ID** - It is set to enable/disable Caller ID detection for FXO lines.
- **Pre answer delay for CID (ms)** - Delay before the call is answered for FXO and only used if Caller ID is enabled. This timer should be long enough to receive all caller id incoming digits. Available range: 200-1800 msec
- **CID signaling** - The user can select the protocol via a drop-down box. Only used if caller ID is enabled. The values available are: Bell (US), V23 (UK), V23 (Japan) and DTMF (some providers in Denmark, Sweden, Holland, Brazil, India, etc). If DTMF is used, please also see "Minimum DTMF Duration" and other DTMF detection configuration parameters like "DTMF Reverse Twist".
- **CID start** - The user can select the indication of the start of caller ID via a drop-down box. The values available are: Ring, Polarity Reversal, Polarity Reversal for India and DTMF Before Ring. Only used if caller ID is enabled.
 - **Ring**: Start receiving CID at Ring signal.
 - **Popularity Reversal**: Polarity reversal indicates the CID start.
 - **Popularity Reversal for India**: Polarity reversal indicates the CID start, at India DTMF tone detection.
 - **DTMF before Ring**: Channel is always monitoring signal activity on the line, and upon signal detection, it will start receiving DTMF caller id and start call afterwards. The level of signal detection is configured by the "DTMF Caller ID Level" parameter. This option is available only for license V9R1 and higher.

NOTICE:

The **DTMF Before Ring** option must be set if DTMF CID is received before any ring or polarity reversal signal. It enables a continuous monitoring of signal on the line, starting the CID detection upon any signal received over DTMF Caller ID Level. This option is valid only if CID Signalling is set to DTMF.

India finds itself in a unique situation. It has several telephone line providers, and they are not all using the same CID signaling; and the CID signaling is not like other countries. There is the need to test some permutations of CID Signaling and CID Start for India. These are some configuration that should be used with specific providers:

- Provider: MTNL, old BSNL Config: **CID Signaling**= v23, **CID start** = ring
- Provider: TATA Config: **CID signaling** = DTMF, **CID start** = polarity reversal for India
- **DTMF CID Level** - DTMF Caller ID Level.

If caller ID signalling is set to **DTMF** and Caller ID Start is set to **DTMF before Ring**, the energy level on the line must be tuned to properly identify the DTMF tones. The specified value is compared to the average over a

packet of audio level of the absolute value of 16 bit signed linear samples. It must be set high enough to prevent false detections, while low enough to ensure no dtmf spills are missed.

Default value set at 400. Available range:128-2048

- **Busy/Congestion Tone disconnect** - Enable/disable the disconnection of line upon detection of busy or congestion tone.

If busy/congestion tone detection is enabled, enter how many tone cycles the system shall wait before disconnecting the call in the Minimum busy detect count field.
- **Pattern 1 disconnect** - Enable/disable the disconnection of line upon detection of Pattern 1 tone and silence configured in advanced section. It will be necessary detection of same number of cycles configured in Minimum Tone Detect Count.
- **Pattern 2 disconnect** - Enable/disable the disconnection of line upon detection of Pattern 2 tone and silence configured in advanced section. It will be necessary detection of same number of cycles configured in Minimum Tone Detect Count.
- **Minimum tone detect count** - It sets how many busy tones you have to wait before hanging up. It is only used when busy detect disconnect is enabled. Valid values are 4-14 or 1-14 if **Use Frequency to detect Busy/Congestion Tone Disconnect** is enabled.
- **Default destination** - It is the destination number data for Incoming calls.
- **FXO Hoot Line** - Enable this flag for the FXO port that needs to have E&M (**Ear & Mouth** or **Listen & Talk**, also known as **recEive & transMit**) hoot. Disabled by default.

Advanced

- **Use Frequency to detect Busy/Congestion Tone Disconnect**- If this flag is enabled, the tone frequency will be used to detect tones for disconnecting the call if **Busy/Congestion Tone Disconnect** is enabled. In such case, the values for **busy pattern**, **congestion pattern**, **pattern1** and **pattern2** will be ignored. For Argentina, tone frequency is 425Hz, default tone size is 300ms. Beside these system parameters, the **Minimum Tone Detect Count** will be considered to disconnect the call. If **Use Frequency to detect Busy/Congestion Tone Disconnect** flag is enabled, the **Minimum Tone Detect Count** range will also support 1 and 2 values.

NOTICE:

This flag is available only for the Argentina country.

- **Pattern 1 Tone (ms)** - Configure the tone within a cycle to be considered for disconnection when Pattern1 Tone disconnect is enabled.
- **Silence (ms)** - Configure the silence length within a cycle to be considered for disconnection when Pattern1/2 Tone disconnect is enabled.
- **Pattern 2 Tone (ms)** - Configure the tone within a cycle to be considered for disconnection when Pattern 2 Tone disconnect is enabled.
- **Silence (ms)** - Configure the silence length within a cycle to be considered for disconnection when Pattern 2 Tone disconnect is enabled.

6.5.2.3 Features > Integrated Gateway > FXS Configuration

Card Configuration

- **Loop current (mA)** - It is the loop current for the analog FXS phones.
- **Manual ring settings** - If this checkbox is set, the Ring Frequency and Ring Voltage can be configured manually, otherwise the country defaults are used.
 - **Ring frequency** - It is the ring frequency for analog FXS phones. The default value is 20, please adjust manually accordingly to the desired value.
 - **Ring voltage** - It is the ring voltage peak value for analog FXS phones. The default value is 75, please adjust manually accordingly to the desired value.
- **Hook flash** - turns on or off hook flash capabilities for all ports.
 - **Hook flash duration** - choose between a Long (200ms to 1250ms) or Short (80ms to 200ms) duration hook flash.
- **CLIP** - Calling line identification presentation.
- **Enable path tagging** - Allows a Branch (not in Proxy-ATA mode) to include a "Path" header in SIP messages from the FXS.
- **Allow compression codecs over FAX lines** - When this checkbox is set, whichever codecs have been negotiated for a call can be used, even when it is a FAX call. When the checkbox is not set, then the G.711 codec will be used exclusively for FAX calls.
- **FXS Invalid Voltage Audit** - Enable/disable FXS Invalid Voltage Audit.
- **Boost Onhook Voltage** - this flag is relevant only for Proxy ATA systems. In some cases, the nominal 48V onhook voltage is not reached. In such cases, if necessary, this flag can be enabled to increase onhook voltage. Note that as the power is the same, the current provided will be reduced proportionally.
- **Spare flag 3** - Enable/disable Spare flag 3.

NOTICE:

Loop current, Manual ring settings, Ring frequency, Ring voltage, Hook flash, & Hook flash duration values must be the same for both FXS cards of the OSB 50i ATA (48-Port version).

NOTICE: For Brazil, setting the **Hook Flash Duration** as "Long" will be considered to be from 200ms to 400ms.

Endpoint Service Profile

- **Endpoint service profile** - Clicking this button brings up the Endpoint Service Profiles screen.
-

Port Configuration

- **All ports (enabling only ports with subscriber number)** - Enabling/Disabling all ports.
- **Echo cancellation** - Enabling/Disabling echo cancellation for all ports.
- **Echo training(ms)** - Enabling echo training will cause the OSB to briefly mute the channel before opening the audio channel, send an impulse with the configured duration in milliseconds, and use the impulse response to pre-train the echo canceller. Available values are: **none**(default), **400-1200 msec** (granularity of 100 msec).
- **Enable** - Enable or disable an FXS physical port.
- **Physical port** - Number of the FXS port. It is a read-only field.
- **Subscriber number** - Subscriber directory number.
- **Subscriber name** - This is the subscriber's name used in the display on the device.
- **Registration interval timer** - Phone registers every Registration Interval Timer seconds.
- **Receive gain** - It sets the Gain of payload for receive. A negative value decreases the gain, and a positive value increases the gain.
- **Transmit gain** - It sets the Gain of payload for transmit. A negative value decreases the gain, and a positive value increases the gain.
- **Digest authentication realm** - This is the 'realm' parameter sent in the header when challenging a request. Typically it is some kind of URL.
- **Digest authentication user ID** - The User Name is a string that uniquely identifies a user within a given realm. This name can be different from the Subscriber name.
- **Digest authentication password** - A password to be used in the Digest Authentication.
- **Fax device** - Enables fax for this interface. It is enabled using the enable check box.

NOTICE:

When this flag is enabled: - Call Waiting is disabled for the port. - End of dial time is changed to 8sec(with flag disabled, time is 3sec)

-
- **Check hook state before dialing** - Check the hook state for an interface before dialing on it, if the other side is off, hook call cannot be completed and the user will hear busy tone.

IMPORTANT: Certain devices will assume they are always out of service, so it is highly recommended not to use this feature unless it is necessary.

-
- **Fax T.38** - Enables FXS interface T.38 negotiation for fax. It is enabled using the enable check box.
 - **CNG detection** - Enables detecting CNG tone for T.38 fax negotiation. It is enabled using the enable check box. The activation of the flag "CNG detection" will only take effect if T.38 flag is also enabled.
 - **FXS hoot line** - Enable this flag for the FXS port that needs to have E&M (Ear & Mouth or Listen & Talk, also known as **recEive & transMit**) hoot. Disabled by default.

- **Hotline/Warmline** - Enable the Hotline or Warmline feature for an FXS port. Disabled by default.

NOTICE:

Hotline/Warmline cannot be enabled if FXS Hoot Line is enabled, and vice versa. Hotline/Warmline is incompatible with FXS Hoot Line, hence one or the other can be selected.

- **Endpoint service profile** - Associate an endpoint service profile to a FXS subscriber.

NOTICE: T.38 fax calls always start as voice call and then switches to T.38 codec.

6.5.2.4 Features > Integrated Gateway > FXS Configuration > Endpoint Service Profiles

This screen presents a summary of the already created endpoint service profiles. Endpoint service profiles are used to associate Dial Restriction rules to FXS ports. A new endpoint service profile can be created by clicking the "Add" button. An existing endpoint service profile can be changed or deleted by first clicking on the item to select it and then clicking the "Edit" or "Delete" button respectively. It is possible to create up to 10 Endpoint Service Profiles.

After clicking "add" or "Edit" a new screen opens, as described below.

General

- **Name** - This is the name of the Endpoint Service Profile.
- **Blocked call disconnection** - This field indicates the way the blocked call shall be disconnected: either with an announcement and disconnection after a timeout, or by being disconnected.

Blocked Calls

This section shows a table with the configuration of dial restriction rules. The table allows the creation of up to 20 rules. The digit sequence is checked against the rules in the table before the INVITE with the digit sequence is sent to Comm System in normal mode or before any SIP manipulation or route analysis is performed in Survivable mode.

NOTICE:

The digit sequence will only be verified if the FXS dials itself. In case the FXS is involved in calls in which a SIP Subscriber defects, blind transfers or forwards, the dialed number will not be verified.

- **Denied number** - A regular expression that allows the entering of dial patterns, which are not accepted for the endpoints associated to this endpoint service profile.

NOTICE:

The Regular Expression is evaluated in the same way as Routing Prefix in the Gateway/Trunk table.

- **Operational mode** - This field indicates if the rule is enabled for Survivable mode or for both Normal and Survivable modes.

6.5.2.5 Features > Integrated Gateway > PRI Configuration

Card Configuration

- **Method** - Possible values "E1" or "T1". This is a read only field only for the OSB 50i DP14 hardware. The default value for new systems is "T1".

NOTICE:

If the PRI Method is changed, you shall receive a warning message stating **"The PRI Method will be changed. The interfaces will be reset according to the default values for the newly selected Method. All PRI B-channels will be removed from all trunk groups. Click OK to continue."**

- **Channel maintenance** - Clicking this button redirects the user to the channel maintenance window, where the user can configure individual PRI links or B-channels. This button applies to the OSB 500i only.

Fax T.38

- **Fax T.38** - Enables PRI card T.38 negotiation for fax. It is enabled using the enable check box.
- **CNG Detection** - Enables detecting CNG tone for T.38 fax negotiation. It is enabled using the enable check box. The activation of the flag "CNG detection" will only take effect if T.38 flag is also enabled.

NOTICE:

T.38 fax calls always start as voice calls and then switch to the T.38 codec.

Port Configuration

The table shows basic information for PRI ports. A more complete set of configuration options are available by first selecting a PRI link by clicking on its row in the table, and then clicking the "Edit" button.

- **Enable** - Use this check box to enable or disable the port.

- **Physical port** - Indicates Port position in the span card.
- **Framing (T1)/Signaling method (E1)** - Framing configured for this port. To edit this value click "Edit" button.
- **Clock source priority** - Clock Source priority used for this port.
- **Coding** - Coding used for this port. To edit this value click "Edit" button.
- **Switch type** - Switch Type configured for this port. To edit this value click "Edit" button (only PRI).
- **Line build out** - Line Build Out used for this port. To edit this value click "Edit" button.
- **Terminal mode** - If this check box is enabled this port will work as TE - Terminal Equipment (user side). Otherwise the role of this port is NE - Network Equipment (network side, only PRI).

Due to the internal clock accuracy, PRI links configured in the Branch as network side role cannot be used. Already existing configurations may work, however if issues are occurring (even in previous OSB versions or builds), the environment must be reconfigured on the OSB links as user side role.

CAS Advanced Settings

- **Enable CAS advanced settings** - Enabling/Disabling CAS Table Configuration Timers. To configure the timer values click the "CAS Advanced Settings" button. Only recommended for advanced users.
- **CAS profile** - Configure CAS Telco general parameters.

Advanced SIP to ISDN Cause Mode Mapping

Adds new option to customize which ISDN cause code will be sent upon receiving specific SIP error status.

- **500/503** - Map SIP status to the following available options:.
 - (38) Network Out of Order (default)
 - (41) Temporary Failure

6.5.2.6 Features > Integrated Gateway > PRI Configuration > PRI Interface > CAS Profiles

Default CAS Profiles

Default CAS Profiles - There are several pre-defined CAS profiles that can be used on a Branch. The profiles that have been chosen and/or defined for a Branch are shown in the table in the "CAS Profile Configuration" section. To utilize one of the pre-defined profiles on the Branch, first select it in the drop-down box, and then click the "Add profile" button. The selected profile will appear in the table. See the section below for details of each of the fields in the profile, and how to edit a profile.

NOTICE: These profiles should be configured to match the OSB Country setting.

CAS Profile Configurations

Profile parameters can be edited in the table. A new, blank, profile can be created by clicking the "Add" button and filling in the fields accordingly. A profile can be deleted by first clicking on its row to select it and then clicking the "Delete" button.

- **Name** - Name of the CAS profile.
- **ANI before DNIS** - Get or not ANI before DNIS.
- **Maximum amount of ANI** - Maximum amount of ANI (calling party number) expected digits.
- **Maximum amount of DNIS** - Maximum amount of DNIS (called party number) expected digits.
- **Maximum waiting time of MF back tone** - How much time our backward MF can last.
- **Metering pulse timeout** - Timer to wait for metering pulse detection
- **Skip category** - Skip the category request and go directly to Group II and Group B signals.
- **Immediate accept** - Bypass the use of Group II and Group B signals.
- **Charge calls** - Allow charge of calls.
- **Enable forced release** - Send backward forced release.

6.5.2.7 Features > Integrated Gateway > PRI Configuration > PRI Interface > CAS Advanced Settings

NOTICE:

This section changes the CAS timer values. All timer values are in milliseconds (ms). It is not recommended to change them if you are not an advanced user.

- **Timeout for backward request to resume cycle** - Resume the MF digit on DNIS timeout timer. Default value is 150ms.
- **Call forward safety** - Forward Safety Timer. Default value is 30000 ms.
- **Wait for seize acknowledge** - How much time it is waited for a response to our SEIZE signal. Default value is 8000ms.
- **Wait for answer** - How much time it is waited when the call has been accepted. Default value is 60000ms.
- **Double answer** - When double answer is in effect, it is the interval between the ANSWER, CLEARBACK and ANSWER again. Default value is 400 ms.
- **Answer delay** - Short delay before answering to give the other end an additional time to detect the tone off condition. Default value is 150 ms.
- **Persistence check** - How much time it is waited for CAS signaling before handling the new signal. Default value is 500 ms.
- **DTMF start dialing** - DTMF Start Dialing Timer. Default value is 500 ms.
- **MF threshold time** - Time that an MF tone should last before being handled. Default value is 0 ms.

6.5.2.8 Features > Integrated Gateway > PRI Configuration > PRI Interface

General

- **Physical port** - Number of PRI port. It is a ready only field.
- **Framing (T1)/Signaling method (E1)** - line formatting options ESF (Extended Super Frame) or D4 (Superframe) for T1, ISDN (ccs - common channel signaling) CAS (channel associated signaling) for E1. The type of framing used is determined by your Telco.

NOTICE:

ISDN or CAS-MFCR2 or CAS Ring Down are Supported.

- **Line build out (LBO)** - each number in the combo box corresponds the following value:
 - 0 = 0 db (CSU) / 0-133 feet (DSX-1)
 - 5 = -7.5db (CSU)
 - 6 = -15db (CSU)
 - 7 = -22.5db (CSU)
- **Coding** - Line encoding method options AMI (Alternate Mark Inversion) or B8ZS (Bipolar 8 with Zero Substitution) for T1, AMI or HDB3 (High Density Bipolar 3). The line coding used is determined by your Telco.
- **Switch type** - sets protocol by a combo box. Only euroisdn is supported for E1. T1 card supports NI2 for 50i and NI2/4ESS/5ESS for 500i.
- **Receive gain (dB)** - It sets the Gain of payload for receive. A negative value decreases the gain, and a positive value increases the gain (mandatory).
- **Transmit gain (dB)** - It sets the Gain of payload for transmit. A negative value decreases the gain, and a positive value increases the gain (mandatory).
- **Default destination** - It is the destination number if no called party number received for ISDN incoming calls. The default destination is also used if just one digit is received and there is not a rule to handle it in the Specific Overlap Dialing Patterns table.
- **Clock source priority** - This parameter determines whether the clock signal from the far end of this T1/E1 port will be used as the master source of clock timing for this card or system. Available values are 1-4 for one card or 1-8 for two cards and should be uniquely assigned. The value 1 is the highest priority. The value 0 indicates that this port will never be used as a source of clock timing for this card. If all ports are set to 0 then the clock will be derived internally.
- **Exclusive channel** - If enabled, indicates only the channel offered in the SETUP message is accepted, otherwise channel is preferred (only PRI). This field is editable only if port is configured as terminal mode (user side), otherwise it will be always enabled.
- **CRC** - enable/disable CRC4 checking (only E1). Remote interface and local configuration must match, otherwise the interface may not work properly, e.g. port may remain down, background humming noise may be heard on calls, etc.
- **BCAS** - enable B-channel Availability Signaling Procedures. Only available for 4ESS and 5ESS. If this parameter is enabled the user will be able to

Block/Unblock an individual B-channel in Channel Maintenance screen. Only when BCAS is enabled Branch will answer isdn SERVICE messages.

NOTICE:

If BCAS is activated and NI2 trunk is used, then Restart Channel must be used.

- **BCAS service message after restart** - selects behavior upon receiving isdn RESTART/RESTART ACKNOWLEDGE messages when BCAS is enabled:
 - None: no SERVICE message is sent.
 - In service: send SERVICE message with change status "In Service" for those b-channels that are enabled and not blocked (MANOOS/NE or MANOOS/FE).
 - Out of service: send SERVICE message with change status "Out of Service" for those b-channels that are enabled and not blocked (MANOOS/NE or MANOOS/FE).
- **Echo cancellation** - enables the echo cancellation parameter.

NOTICE:

Echo cancellation may affect DTMF detection.

- **Echo tail(ms)** - Echo tail for Hardware Echo Cancellation. Available values are: 16, 32, 64 and 128 (msec).
- **Echo training(ms)** - Enabling echo training will cause the OSB to briefly mute the channel before opening the audio channel, send an impulse with the configured duration in milliseconds, and use the impulse response to pre-train the echo canceller. Available values are: **none**(default), **400-1200 msec** (granularity of 100 msec).
- **Extended Echo Cancellation** - Since the OSB50i DP14 uses SW-DSP OSLEC process, the echo cancelation on high number of simultaneous E1/T1 channels requires high dynamic processing that may affect the system performance.

This effect is compensated by the **Extended Echo Cancellation** functionality but with a possible perception of the audio quality level, depending on the phone (e.g. lower on OpenStages or higher on CP phones). This function can now be disabled, in order to improve voice quality.

This flag applies only for DP14 and E1/T1 Port and it is enabled by default.

IMPORTANT: The Echo Cancellation feature is performed by software at OSB 50i DP14 models and at some cases it can generate noise in the calls. If you are experiencing audio/noise issues, check the [OpenScape Branch Configuration Guide](#) for some configurations examples that may assist you.

Timers (does not apply for CAS)

- **T302 timer** - timer to wait for digits for overlap dialing (mandatory on E1).

- **T305 timer** - timer to wait for DISCONNECT ACK once DISCONNECT is sent out, if this timer expires RELEASE is sent and T308 is started (mandatory).
 - **T308 timer** - timer to wait for RELEASE COMPLETE once RELEASE is sent out, if this timer expires RELEASE retransmitted and T308 is restarted. If this timer expires twice the B-channel is placed in maintenance condition and call reference is released (mandatory).
 - **T309 timer** - maintain active calls on layer 2 disconnection, calls are cleared if connection is not established before T309 timer expires.
 - **T313 timer** - wait for CONNECT ACK once CONNECT is sent out, if this timer expires DISCONNECT is sent. Used only if port is configured as terminal mode (user side).
-

Advanced (does not apply for CAS)

- **Sending complete** - add Sending Complete information element in SETUP messages. For 4ESS/5ESS this parameter is not allowed.
- **Far end disconnect with inband announcement** - if enabled upon receiving a DISCONNECT with PI-8 the call is not released, sending a 183 PROGRESS to open channel to send a disconnection message. If disabled, the call is released upon receiving a DISCONNECT ignoring PI-8 (only PRI).
- **Calling name delay** - indicates that the Calling Name will be provided in a separate ISDN message. In this case, the SIP INVITE message will be postponed until the Facility with Calling Name is received or after a fixed 2 seconds timer expires. For 4ESS/5ESS this parameter is not allowed.
- **Second screening indicator** - if enabled the second screening indicator will be used in incoming setup message.
- **Send calling party name** - enable/Disable the sending of the Calling Name information in outgoing calls. This configuration is useful when destination side does not support the Calling Name Delivery feature.
- **Calling party name** - Indicates in which Information Element the Calling Party Name information should be delivery in outgoing calls. For EuroISDN switch type, two options are available:
 - Facility IE (Calling Name Operation) (Default)
 - Display IE

Switch types NI-2, 4ESS and 5ESS, only support delivery of Calling Party Name in the Facility IE (Calling Name Operation). Send Calling Party Name configuration item must be enabled to change this configuration.

- **Data calls allowed** - allow or not calls with clearmode to be done.
- **Setup progress indicator** - Configures the Progress Indicator in SETUP message (New Zealand). The following options are supported:
 - Call is not end-to-end, ISDN further call progress information may be available in-band.
 - Destination address is non ISDN.
 - Origination address is non ISDN.
 - None.
- **Send redirecting number** - Enable/Disable the sending of the Redirecting Number in outgoing calls to integrated gateway. This configuration is useful when destination side does not support the Redirecting Number feature.

- **Redirecting number** - Indicates in which Information Element the Redirecting Number information should be delivery in outgoing calls. For EuroISDN switch type, two options are available:
 - Facility IE (DivertingLegInformation2 Operation) (Default)
 - Redirecting Number IE

Switch types NI-2, 4ESS and 5ESS, only support delivery the redirecting number in the Redirecting Number IE. Send Redirecting Number configuration item must be enabled to change this configuration.
- **183 session progress without SDP** - Comm System sends a 183 Session Progress response code without SDP (i.e, without inband announcement) in some situations (for ex, call processing delayed and no information about the called party is available till this point). This configuration item allows choosing how this response code must be informed to the PSTN caller according to the carrier requirements. This action intends to stop timer T309 avoiding the disconnection of call by the caller side. Possible values:
 - Progress: response code is converted to ISDN PROGRESS message including the Progress Indicator #2 - called party is non-ISDN (Default for PRI switch types: NI-2, 4ESS and 5ESS)
 - Progress and Alerting: response code is converted to ISDN PROGRESS message including the Progress Indicator #2 (destination is non-ISDN) followed by an ISDN ALERTING message.
 - Alerting: response code is converted to ISDN ALERTING message. (Default for PRI switch type EuroISDN and BRI interfaces)
 - None: response code is discarded.
- **Always send PI8 in ALERT** - if flag is enabled, the Branch sends ALERTING with PI8 (progress indicator: In-band information or an appropriate pattern is now available) whenever a 180 Ringing (without SDP) is received. Otherwise PI8 will be sent only when a 180 Ringing with SDP is received."

IMPORTANT:

For in band announcements, PI=1 and PI=8 are supported in PROGRESS, ALERTING and CALL PROCEEDING messages. When one of these messages is received with PI=1 or PI=8, voice path is open and inband tones could be heard by the caller if available. Other PI's are ignored, although when using switch type QSIG or CorneN-Q, in Normal Mode, these Progress Indicators are passed transparently to the OSV. The OSV may handle it accordingly. Additionally, PI=8 can be supported in DISCONNECT message if **Far end disconnect with inband announcement** flag is enabled.

- **Channel mapping** - Only available for QSIG and CORNET switch types. Possible values: Logical/Physical

Physical: b-channels from 1-15, 17-31, channel 16 is used as a signalling channel.

Logical: b-channels from 1-30, channel 16 is used as a "pseudo" b-channel. This is default for Qsig/CorneN-Q switch types.
- **QSIG ringback** - If disabled, do not play ringback for QSIG/CORNET
- **Restart link at start-up** - if enabled send PRI restart message after link start-up.

- **Start early media on CALL PROCEEDING** - This command will cause the Branch to raise a SIP 183 Session Progress message with an SDP Answer as soon as it receives the ISDN CALL PROCEEDING message. The SIP 183 Session Progress response will contain a "P-Early-Media" header field (RFC5009) with a new proprietary value ("fast-connect"). If an ALERTING is received afterwards, the Branch will send back a SIP 180 Ringing response with SDP Answer and without the "P-Early-Media" header. This flag will be ignored if INVITE received does not contain SDP.
- **L3 trunk restart type** - depending on the selected option the OSB50i/ OSB500i will send the Q931 RESTART message accordingly:
 - **Restart Channel** - A RESTART message is sent for each channel, if the channel is enabled and assigned to any trunk group. The channel will be considered IN SERVICE if the respective RESTART ACKNOWLEDGE response is received for that channel.

Restart Channel is default value for NI2/EuroISDN for 50i.
 - **Restart Interface** - One RESTART message is sent with Restart indicator information element set to "All Interfaces", if following conditions apply:
 - OSB50i: "All Interfaces?" is sent if all channels for that port are enabled and assigned to any trunk group, otherwise, a RESTART for each channel will be sent just for the enabled and assigned channels.
 - OSB500i: "All Interfaces?" is sent if all channels for that port are enabled, otherwise, a RESTART for each channel will be sent just for the enabled channels.

If a RESTART ACKNOWLEDGE is received with Restart indicator information element set to "All Interfaces" all the channels for that E1/T1 will be considered IN SERVICE.

Restart Interface is default value for NI2/EuroISDN for 500i.

For 5ESS/4ESS Restart Interface is not allowed.
- **Disable far end restart** - In scenarios in which 50i/500i is connected to a CO switch like MUNDRA that does not accept RESTART message during PRI span bring up. The flag is for use only with NET5 type switch and specific CO such as MUNDRA in India.
- **B-channel parallel restarts** - if flag is enabled RESTART message for each individual b-channel is sent simultaneously for all b-channels. If flag is disabled RESTART is sent for first b-channel and RESTART ACKNOWLEDGE is required for this b-channel before sending RESTART to next b-channel.
- **Idle reset interval** - It sets the time in seconds between restart of unused B channels. If the field is empty, the functionality is disabled.
- **Group restarted b-channels in channel identification IE** -

NOTICE:

On the OSB 500i, the "B-channel parallel restarts" flag setting is used during both the link start-up process and the PRI enabling process, but it is not used for Restart actions initiated from the Channel Maintenance tab. Any Restart action on the Channel Maintenance tab will always result in B-channel parallel restarts.

- **Do not send ISDN Status Message** -If this flag is set, OSB will never send an ISDN Status Message out. Do not send Status if configured as Network and Call proc received without channel id – similar behavior as setup
- **Screening Indicator** - The Screening Indicator is information sent to indicate whether the number information was provided by the user or the network. Usually, for PBX operation, if the calling number received from the calling user is determined to be correct, the network shall set the screening indicator to “user-provided, verified and passed”. If the screening function fails the network shall note that the screening is failed and shall use a default number associated with the calling user. The network shall set the screening indicator to “network provided”. In the OSB, which works as a gateway and not as a PBX, this information is configurable and the same value is sent for all calls according to the “Screening Indicator” parameter configured in PRI Interface. Possible values:
 - **0x0 number not screened, user-provided number**
 - **0x1 number passed network screening, user-provided number**
 - **0x2 number failed network screening, user-provided number**
 - **0x3 network-provided number**

Default value: **0x0 number not screened, user-provided number.**

If Terminal Mode is clear, i.e., if the port is configured as network side, the only possible value is 0x3 network-provided number

NOTICE:

Number Presentation (allowed / prohibited) is not determined by the screening indicator, but by the Presentation Indication value, also included in the Calling Party Number ISDN information element.

IMPORTANT:

If the parameter 183 Session Progress without SDP is set to Progress and Alerting, it will supersede the parameter "Always Send PI8 in Alerting". So, if the parameter 183 Session Progress without SDP is set to Progress and Alerting and flag Always Send PI8 in Alerting is enabled the Alerting will be sent without PI8 as determined by the parameter 183 Session Progress without SDP. In this case, if a 183 Session Progress without SDP is received a Progress and an Alerting are sent. When the 180 Ringing is received on the SIP side, no further Alerting shall be sent because the Alerting message had already been sent.

IMPORTANT: Wireshark is not able to interpret the Facility IEs in the ISDN messages, because it uses the QSIG standards (ECMA standards) to interpret them. The definition of the Facility IEs by ECMA (QSIG) is different from the definition by ETSI (ISDN). For the interpretation of the Facility in ISDN, the ETSI standard ETS 300 196-1 Generic functional protocol for the support of supplementary services shall be used. For

Redirecting Party being carried in the Facility IE the standard ETS 300 207-1 Diversion supplementary services shall be used.

IMPORTANT: The limitations on feature interactions between PRI and CAS Ring Down are consequence of CAS RD calls restrictions; Own number is an example. Call transfer, forwarding and other features will only work if the own number matches the calling number of the feature call. Feature calls that generate outgoing calls through PRI port won't show this restrictions.

Channels

- **All channels** - Enabling/Disabling all B-channels.
- **Enable** - Enabling/Disabling a B-Channel for this PRI interface.
- **Number** - The B-Channel number.
- **CAS initial state** - ABCD bit position during startup, only for CAS for each channel. When not using CAS, the Branch shows Idle state.

6.5.2.9 Features > Integrated Gateway > Trunk Group Configuration

This screen displays a table that shows a summary of configured Trunk Groups.

A new Trunk Group is created by clicking the "Add" button, which will open the Trunk Group Configuration screen.

An existing Trunk Group can be edited by first clicking it to select it and then clicking the "Edit" button.

An existing Trunk Group can be deleted by first clicking it to select it and then clicking the "Delete" button. If a PRI trunk group is deleted, its B- channels will be in OOS state.

- **Type** - This field shows the port type: FXO, BRI or PRI. It is a read-only field.
- **FQDN** - It is the Fully Qualified Domain Name of the trunk group.
- **Trunk group name** - It is the name of the Trunk Group.
- **Trunk selection** - It configures the trunk selection by a drop down box. The values are Top to bottom and Bottom to top.
- **Hunt type** - It configures the hunt type by a drop down box. The values are Linear and Circular.

6.5.2.10 Features > Integrated Gateway > Trunk Group Configuration > General

Configuration

- **Type** - This field shows the port type: FXO, BRI or PRI. It is a read only data.

NOTICE:

For 500i, only 'PRI/CAS' is displayed.

- **FQDN** - It is the Fully Qualified Domain Name of the trunk group.
- **Trunk group name** - It is the name of the Trunk Group.
- **Restart trunk group channels** - Restart the enabled channels from selected list. Note that trunkgroup hunting does not get restarted.
- **Trunk selection** - It configures the trunk selection by a drop down box. The values are Top to bottom and Bottom to top.
- **Hunt type** - It configures the hunt type by a drop down box. The values are Linear and Circular.
- **Direction** - Specifies the direction of traffic flow supported on the trunk group:
 - Both - Originating and terminating traffic is permitted.
 - Originating - Only traffic that is originated on this trunk group is permitted.
 - Terminating - Only traffic that is terminated on this trunk group is permitted.
- **Mark sRTP call-leg as secure** - if a secure media is negotiated for a trunk (FXO, BRI or PRI), the call will be indicated as secure (ST-Siemens-Call-Type: secure).
- **Voice bearer capability** - Speech or 3.1 kHz audio.

Incoming Calls

- **Max overlap digit length** - Maximum number of digits that can be received in an overlap dialing incoming call. When the number of incoming digits matches this configuration, the called number is considered complete even no sending complete information is received. Possible values are within the range 1-24 digits.
- **Specific overlap dialing patterns** - Replaces "Max overlap digit length" value. Indicates that the system must process incoming digits in accordance with the patterns defined in the table. If this parameter is enabled "Max Overlap Digit Length" is ignored and the table must have at least one entry. Not applicable for CAS, FXO, T1 and BRI Point to Multiple Point.
 - Dialing pattern: accepts numeric values and the percent character '%' only. Used in combination with the Maximum digit length field to determine if sufficient incoming digits have been dialed to permit the call to continue processing. No match will result in the call waiting for the next digit to be received.
 - Maximum digit length: specifies the maximum overlap digit length for the row. Possible values are within the range 1-24 digits. If Dialing Pattern is just numbers without '%', the length will filled or corrected automatically.
- **Connected line identification presentation incoming** - Default value is unchecked. Only visible when the PRI Method is E1, or it is a BRI trunk group.

NOTICE:

This flag must not be visible when configuring T1 PRIs on both the OSB 50i and OSB 500i.

- **Called Name Incoming** - Enable called name for incoming calls (ISDN-SIP). If name received in PAI header in sip 180 ringing, and Privacy: id not present, called name facility will be sent in ISDN Alerting.

- **Answer Supervision Timer-Incoming Call (sec)** - Default value is 360 sec. Range: 120 to 3600 sec.

NOTICE:

This flag doesn't apply to calls from FXS ports.

- **Match prefixes for Unknown numbers** - If set, the leading digits of the incoming calling or called party number with Unknown Type of Number is matched against (in this order) the International Prefix, National Prefix and Subscriber Prefix. The prefix field must have a non-empty value to match. In case a number remains Unknown after the prefix check, the default Type of Number of Subscriber is taken.
- **Force FQDN in Contact Header for Incoming Calls in NM** -
Options: Incoming calls made in Normal Mode: Force FQDN in contact header, otherwise branch IP will be used.

NOTICE:

This flag will not take effect over QSIG trunk groups. The FQDN is always added to the contact header when SIP-Qv2 is used to establish the calls.

- **Blacklist profile** - Blacklisting incoming calls based on Calling Party Number. Blacklist profiles shall apply only for integrated gateway trunks (S0,S2,FXO), on both NM and SM. In the case of FXO, it is only possible if the CLIP is supported. Patterns can be defined with special character %, i.e., %9232473 (suffix) or 561923% (prefix) using the same match pattern as in the trunkgroup match.
- **Enable IPC Redundancy** - Enable IPC Redundancy delay control (used for CAS-ARD systems). This checkbox is disabled by default.
- **Call Delay in ms** - Delay to be applied on the Incoming call processing when the IPC Redundancy flag is activated. Available values: 100-3000 msec. Default value set at 0msec.

IMPORTANT:

On QSIG/SIP-Q, the OpenScape Branch works as a end-to-end tunnel transporting the QSIG messages inside the SIP body. Therefore features such as (but not limited to) **Connected Line Identification Presentation, TON, SIP Manipulation** et al. are not covered because of the SIPQ end-to-end transparent connection. All features are sent in the SDP MIME body and should be handled by the OSV side. During survivability mode, the QSIG features are handled in the same way as ISDN features, including CLIR, TON and SIP Manipulation.

Outgoing Calls

- **Set numbering plan to ISDN** - When the Number Type is Unknown, it will set the Numbering Plan to ISDN. Otherwise, it will set to Unknown (only PRI).

NOTICE:

This flag applies only to **Called Party Number**

- **Pre dial delay for DTMF** - When an analog trunk is seized, it takes some time until the DTMF receiver is allocated by CO. If DTMF digits are dialed before the DTMF receiver is allocated, the first digits can be lost. It shall be possible to configure a delay to start sending the DTMF digits.
- **Send Redirect Number instead of calling number for redirected calls** -
The calling number shall be replaced by the redirecting number in case of call forwarding (immediate, on no reply, on busy and on call deflect) to PSTN. The calling number shall also be replaced by the redirecting number in the case of system call forward. The calling number shall not be replaced in case of transferred calls. For SIP Service Providers, the replacement of the original caller by the redirecting party number is already configurable by means of the SIP Service Provider profiles.
- **Calling Party Number Presentation Restricted**- Set calling party number presentation restricted to all outgoing call. Not supported for CAS.
- **Connected line identification presentation outgoing** -Default value is unchecked. Only visible when the PRI Method is E1, or it is a BRI trunk group.

NOTICE:

This flag must not be visible when configuring T1 PRIs on both the OSB 50i and OSB 500i.

- **Called Name Outgoing** - Enable called name for outgoing calls (SIP-ISDN). If called name facility received in ISDN Alerting, with presentation allowed, it will be sent in PAI header in sip 180 ringing.
 - **Answer Supervision Timer - Outgoing Call (sec)**
-

Collect Calls (only for CAS)

- **Collect call control** - who will check the permission for collect calls, choose between Server (will check on normal mode and Branch in survivable mode) or Gateway (Branch will check the permission). Only works for CAS and Brazil.
 - **Permission for receiving Collect calls by category** - if Branch will check the permission for collect call by category. If this flag is not checked, the call with the indication of collect call will be rejected.
 - **Permission for receiving Collect calls by double Answer** - if Branch will check the permission for collect call by double answer. If this flag is not checked, the call is double answered, which causes the release of the collect calls.
-

CAS (only for CAS)

- **CAS profile** - Select any of the created CAS profiles in CAS profiles table.
- **CAS Answer for Early Media** - If set allows answer in CAS calls to play announcements. Otherwise, send the appropriate backward tone.

6.5.2.11 Features > Integrated Gateway > Trunk Group Configuration > Channels List

Configuration

- **Filter** - this drop-down box is used to filter the list of available channels to a specific Port on a specific card. Selecting the blank entry in the drop-down list will display all channels of all ports of all cards.
- **Trunk ports** - The left-hand list shows the list of PRI, BRI, or FXO channels that are available. Any channel that is already in use on this or another trunk group will not be shown here.

To add a channel to the "Selected Channel" list, first click it to select it, and then click the double-right chevron button. Multiple channels can be selected by holding down the Ctrl key while selecting them.

- If a channel needs to be removed from a "Selected Channel" list, first click on it to select it, and then click the double-left chevron button.

6.5.2.12 Features > Integrated Gateway > Trunk Group Configuration > Network Specific Facilities (T1 only)

Configuration

The network specific facilities is an information element used in the NI2 protocol to provide the call-by-call service.

If this service is provided by the carrier network, the following fields should be set accordingly (1).

In the outgoing calls, the information element NSF will be included in the SETUP message.

In the incoming calls, NSF should be received in the SETUP message and all configured parameters should match. Otherwise, the call is rejected (2).

(1) Other settings maybe the required for the call-by-call service such as specific called/calling Type of Number, bearer capabilities etc. Please, consult the carrier network documentation.

(2) Extension bit 8 of Facility Coding Value is not checked by the Branch. Call will be not rejected in case of wrong value of this bit.

- **Send NSF** - enabling/disabling sending the NSF.
- **Facility coding value** - Indicates the service/feature requested to the carrier network. Please, consult the carrier network documentation to check which services/features are provided. Only services are supported by the Branch. The services used are:
 - none
 - ATT_SDN_SDDN_GSDN
 - MCI_VNET_Vision

- SPRINT_VPN
- ATT_tollFreeMegacom
- MCI_800_888_877
- SPRINT_800_888_877
- ATT_Megacom
- MCI_PRISMI_PRISMII_WATS
- SPRINT_UltraWATS
- accunet
- longDistance
- internationalTollFree
- ATT_multiquest
- inwatts
- MCI_900
- outwatts
- foreignExchange
- tieTrunk
- hotelMotel
- selectiveClassOfCall
- callRedirection
- **Network ID** - A Four-digit code that indicates the carrier network which the service/feature will be requested. If empty, it indicates the local service provider.
- **Service parameters** - Up to five digits that provide additional information to the service/feature requested. Not all services requires service parameters.
- **Ignore incoming NSF** - If this flag is enabled, the NSF information on incoming calls will not be checked. If this flag is disabled, incoming calls will be only accepted if configured NSF matches with received NSF information, i.e., incoming calls are disconnected if:
 - System is not configured to send NSF information and the Branch receives the NSF information from C.O.
 - System is configured to send NSF information and it does not match received NSF information from C.O. Incoming calls without NSF information are always accepted by the Branch.

6.5.2.13 Features > Integrated Gateway > Trunk Group Configuration > Number Modification

Definitions

- **Country code** - It is the configuration of the country code (L2).
- **Area code** - It is the configuration of the Local Area Code (L1).
- **National number length** - If the Digit length check is enabled and a match for PNAC and/or Prefix is found the length of the number will be performed, after stripping PNAC and/or Prefix if the remaining length is equal to the National number length the TON will be set to National.
- **Subscriber number length** - If the Digit length check is enabled and a match for PNAC and/or Prefix is found the length of the number will be performed, after stripping PNAC and/or Prefix if the remaining length is equal to the Subscriber number length the TON will be set to Subscriber.

Prefixes

- **International PNAC** - It is the configuration of the international Public Network Access Code (PNAC).
 - **International prefix** - It is the configuration of the international prefix.
 - **National PNAC** - It is the configuration of the national PNAC.
 - **National prefix** - It is the configuration of the national prefix.
 - **Subscriber PNAC** - It is the configuration of the subscriber PNAC.
 - **Subscriber prefix** - It is the configuration of the subscriber prefix.
-

Incoming Calls

- **TON-IN Settings**

Calling Party Number

- **Match prefixes for Unknown numbers**- If set, the leading digits of the incoming calling or called party number with Unknown Type of Number is matched against (in this order) the International Prefix, National Prefix and Subscriber Prefix. The prefix field must have a non-empty value to match. In case a number remains Unknown after the prefix check, the default Type of Number of Subscriber is taken.
- **TON via length check** - If set and if number lengths are specified in National Number Length and/or Subscriber Number Length, the length of the incoming number is checked against these lengths and if a length match is found the appropriate Type of Number is assumed for the incoming number.

Called Party Number

- **Match prefixes for Unknown numbers** - If set, the leading digits of the incoming calling or called party number with Unknown Type of Number is matched against (in this order) the International Prefix, National Prefix and Subscriber Prefix. The prefix field must have a non-empty value to match. In case a number remains Unknown after the prefix check, the default Type of Number of Subscriber is taken.
- **TON via length check** - If set and if number lengths are specified in National Number Length and/or Subscriber Number Length, the length of the incoming number is checked against these lengths and if a length match is found the appropriate Type of Number is assumed for the incoming number.

Connected Number

- **Copy configuration from OUTGOING calling party number** - If enabled, the configuration of the outgoing calling party number is copied.
- **Match PNACs and/or prefixes** - If enabled, the leading digits of the incoming calling or called party number with Unknown Type of Number is matched against (in this order) the International Prefix, National Prefix and Subscriber Prefix. The prefix field must have a non-empty value to match. In case a number remains Unknown after the prefix check, the default Type of Number of Subscriber is taken.

- **TON via length check** - If set and if number lengths are specified in National Number Length and/or Subscriber Number Length, the length of the incoming number is checked against these lengths and if a length match is found the appropriate Type of Number is assumed for the incoming number.
- **Default TON from SIP**- Available options:

Unknown: the number is treated as a number of which the type of number is not known

International: the incoming number is treated as an International number

National: the incoming number is treated as a National number.

Subscriber: the incoming number is treated as a Subscriber number.

- **TON-OUT Settings**

Calling Party Number

- **Preferred TON to SIP (Normal Mode)** -Available options:

Same as TON-IN: the input TON is the preferred output TON

International: an output TON of International means that the number is normalized to an International number if the input TON is national or subscriber using the country code and/or area code.

- **Preferred TON to SIP (Survivable Mode)** - Available options:

Same as TON-IN: the input TON is the preferred output TON

International: an output TON of International means that the number is normalized to an International number if the input TON is national or subscriber using the country code and/or area code

National: an output TON of National means that the number is either upgraded from a subscriber number to a national number using the area code defined in Req. 2040 or that an international number is downgraded by stripping the country code if it starts with the country code.

Subscriber: an output TON of Subscriber means that an international number is downgraded by stripping the country code if it starts with the country code. If the resulting national number or any incoming national number starts with the area, then the area code is stripped as well.

- **Use Local Toll Table** - This checkbox is used to perform an LTT lookup on an incoming call. It is applicable ONLY for T1 systems. The results of

the lookup won't affect the Type of Number (TON) settings, but it will be used later in the call. The default value for this field is 'unchecked'.

Called Party Number

- **Preferred TON to SIP (Normal Mode)** -Available options:

Same as TON-IN: the input TON is the preferred output TON

International: an output TON of International means that the number is normalized to an International number if the input TON is national or subscriber using the country code and/or area code

- **Preferred TON to SIP (Survivable Mode)** -Available options:

Same as TON-IN: the input TON is the preferred output TON

International: an output TON of International means that the number is normalized to an International number if the input TON is national or subscriber using the country code and/or area code

National: an output TON of National means that the number is either upgraded from a subscriber number to a national number using the area code defined in Req. 2040 or that an international number is downgraded by stripping the country code if it starts with the country code.

Subscriber: an output TON of Subscriber means that an international number is downgraded by stripping the country code if it starts with the country code. If the resulting national number or any incoming national number starts with the area, then the area code is stripped as well.

Connected Number

- **Preferred TON to PSTN** - Available options:

Same as TON-IN: the input TON is the preferred output TON

International: an output TON of International means that the number is normalized to an International number if the input TON is national or subscriber using the country code and/or area code

National: an output TON of National means that the number is either upgraded from a subscriber number to a national number using the area code defined in Req. 2040 or that an international number is downgraded by stripping the country code if it starts with the country code.

Subscriber: an output TON of Subscriber means that an international number is downgraded by stripping the country code if it starts with the country code. If the resulting national number or any incoming national number starts with the area, then the area code is stripped as well.

- **Post Manipulation Settings**

- **Normal Mode** - Available options:

None: the number is sent on the SIP interface without adding PNACs and prefixes or converting an international number to GNF – this setting is not

recommended unless the Preferred TON to SIP in Normal Mode is set to International.

Add PNAC and Prefixes: the number is sent on the SIP interface prefixed with the PNAC and prefix appropriate for the TON determined by the Preferred TON to SIP in Normal Mode setting.

GNF: an international number is prefixed with a '+' before being sent on the SIP interface without adding the international PNAC and prefix. Other types of number are also sent without adding PNAC and prefixes. It is expected that this setting is used with Preferred TON to SIP in Normal Mode set to International.

- **Survivable Mode** -Available options:

None: the number is sent on the SIP interface without adding PNACs and prefixes or converting an international number to GNF – this setting is not recommended unless the Preferred TON to SIP in Survivable Mode is set to International.

Add PNAC and Prefixes: the number is sent on the SIP interface prefixed with the PNAC and prefix appropriate for the TON determined by the Preferred TON to SIP in Survivable Mode setting.

Outgoing Calls

• TON-IN Settings

Calling Party Number

- **Match PNACs and/or prefixes-** If set, the leading digits of the incoming calling or called party number with Unknown Type of Number is matched against (in this order) the International Prefix, National Prefix and Subscriber Prefix. The prefix field must have a non-empty value to match. In case a number remains Unknown after the prefix check, the default Type of Number of Subscriber is taken.
- **TON via length check** - If set and if number lengths are specified in National Number Length and/or Subscriber Number Length, the length of the incoming number is checked against these lengths and if a length match is found the appropriate Type of Number is assumed for the incoming number.
- **Default TON from SIP** - Available options:

Unknown: the number is treated as a number of which the type of number is not known

International: the incoming number is treated as an International number

National: the incoming number is treated as a National number.

Subscriber: the incoming number is treated as a Subscriber number.

Called Party Number

- **Match PNACs and/or prefixes-** If set, the leading digits of the incoming calling or called party number with Unknown Type of Number is matched against (in this order) the International Prefix, National Prefix and Subscriber Prefix. The prefix field must have a non-empty value to match. In case a number remains Unknown after the prefix check, the default Type of Number of Subscriber is taken.

- **TON via length check** - If set and if number lengths are specified in National Number Length and/or Subscriber Number Length, the length of the incoming number is checked against these lengths and if a length match is found the appropriate Type of Number is assumed for the incoming number.
- **Default TON from SIP** - Available options:
 - Unknown:** the number is treated as a number of which the type of number is not known
 - International:** the incoming number is treated as an International number
 - National:** the incoming number is treated as a National number.
 - Subscriber:** the incoming number is treated as a Subscriber number.

Connected Number

- **Copy configuration from INCOMING calling party number** - If enabled, the configuration of the incoming calling party number is copied.
- **Match prefixes for Unknown numbers** - If enabled, the leading digits of the incoming calling or called party number with Unknown Type of Number is matched against (in this order) the International Prefix, National Prefix and Subscriber Prefix. The prefix field must have a non-empty value to match. In case a number remains Unknown after the prefix check, the default Type of Number of Subscriber is taken.
- **TON via length check** - If enabled, and if number lengths are specified in National Number Length and/or Subscriber Number Length, the length of the incoming number is checked against these lengths and if a length match is found the appropriate Type of Number is assumed for the incoming number.

• TON-OUT Settings

Calling Party Number

- **Preferred TON to PSTN** - Available options:
 - Same as TON-IN:** the input TON is the preferred output TON
 - International:** an output TON of International means that the number is normalized to an International number if the input TON is national or subscriber using the country code and/or area code
 - National:** an output TON of National means that the number is either upgraded from a subscriber number to a national number using the area code defined in Req. 2040 or that an international number is downgraded by stripping the country code if it starts with the country code.
 - Subscriber:** an output TON of Subscriber means that an international number is downgraded by stripping the country code if it starts with the

country code. If the resulting national number or any incoming national number starts with the area, then the area code is stripped as well.

Called Party Number

- **Preferred TON to PSTN** - Available options:

Same as TON-IN: the input TON is the preferred output TON

International: an output TON of International means that the number is normalized to an International number if the input TON is national or subscriber using the country code and/or area code

National: an output TON of National means that the number is either upgraded from a subscriber number to a national number using the area code defined in Req. 2040 or that an international number is downgraded by stripping the country code if it starts with the country code.

Subscriber: an output TON of Subscriber means that an international number is downgraded by stripping the country code if it starts with the country code. If the resulting national number or any incoming national number starts with the area, then the area code is stripped as well.

Connected Number

- **Preferred TON to SIP (Normal Mode)** - Available options:

Same as TON-IN: the input TON is the preferred output TON

International: an output TON of International means that the number is normalized to an International number if the input TON is national or subscriber using the country code and/or area code

National: an output TON of National means that the number is either upgraded from a subscriber number to a national number using the area code defined in Req. 2040 or that an international number is downgraded by stripping the country code if it starts with the country code.

Subscriber: an output TON of Subscriber means that an international number is downgraded by stripping the country code if it starts with the country code. If the resulting national number or any incoming national number starts with the area, then the area code is stripped as well.

- **Preferred TON to SIP (Survivable Mode)** - Available options:

Same as TON-IN: the input TON is the preferred output TON

International: an output TON of International means that the number is normalized to an International number if the input TON is national or subscriber using the country code and/or area code

National: an output TON of National means that the number is either upgraded from a subscriber number to a national number using the area code defined in Req. 2040 or that an international number is downgraded by stripping the country code if it starts with the country code.

Subscriber: an output TON of Subscriber means that an international number is downgraded by stripping the country code if it starts with the

country code. If the resulting national number or any incoming national number starts with the area, then the area code is stripped as well.

- **Use Local Toll Table** - This checkbox is used to perform an LTT lookup on an incoming call. It is applicable ONLY for T1 systems. The results of the lookup won't affect the Type of Number (TON) settings, but it will be used later in the call. The default value for this field is 'unchecked'.
- **Post-Manipulation Settings**
 - **Normal/Survivable Mode** -

None: the number is sent on the PSTN interface without adding a prefix or setting the Type of Number to Unknown.

Add Prefix+ Unknown TON: the number is sent on the PSTN interface prefixed with the prefix appropriate for the TON determined by the Preferred TON to PSTN setting.

Unknown TON: the number is sent on the PSTN interface after setting the Type of Number to Unknown.

6.5.2.14 Features > Integrated Gateway > QoS Monitoring

Configuration

- **Send traps** - it is set to enable/disable the send traps.
- **Reporting mechanism** - Selecting the criteria for reporting the QoS parameters by a drop down box. The values must be threshold crossing or Collection of each call session.
- **QCU IP address** - It configures the QCU IP address.

NOTICE:

QoS Monitoring supports both IPv4 and IPv6 addresses.

- **QCU port** - It configures the QCU Port address.
- **Maximum jitter threshold** - Setting the Threshold for maximum jitter in the RTP stream.
- **Average round trip delay threshold** - Setting the Threshold for maximum round trip delay in the RTP stream.
- **Lost packets threshold compressing** - it configures the Threshold for count of lost packets in the RTP stream for compressed codecs.
- **Lost packets threshold not compressing** - Setting the Threshold for count of lost packets in the RTP stream for non-compressed codecs.

6.5.2.15 Features > Integrated Gateway > Local Toll Table Configuration

Local Toll Tables Imported to OSB

This tab shows which LTTs are already imported to the OSB. This list is populated from the master XML configuration file. You can either view or delete the selected LTT(s).

- **Local Toll Table Name** - Filename of Local Table Name.
- **Related to** -.
- **Extracted from OSV** -.

Upload a new Local Toll Table

- **Upload Local Toll Table from OSV-** By clicking this button you refer to [Features > Integrated Gateway > Local Toll Tables Configuration > Upload Local Toll Table](#)

IMPORTANT:

The LTT itself is not editable on the OSB. Therefore, if an LTT needs to be updated, then a new OSV file version must be created and uploaded to the OSB. The action of importing an LTT to the OSB will result in the old data first getting deleted and then recreated.

IMPORTANT: Any time that a new LTT is imported to the OSB, or any time that an existing LTT is updated, the Kamailio SIP server will be restarted. This will result in the loss of ongoing calls.

6.5.2.16 Features > Integrated Gateway > Local Toll Tables Configuration > Upload Local Toll Table

Upload Local Toll Table

Upload a Local Toll Table file (LTT) to the OSB, which the OSB will then parse and extract the LTT components from it. The extracted LTTs will be listed for the user, who can then select the LTTs that must be imported to the OSB.

- **Filename** : - Local Toll Table filename. The Filename field will store the full path and filename of the LTT file that was previously created by the soapExport command on the OSV.
 - **Browse** - Clicking the 'Browse...' button will bring up a standard file browser dialog box.
 - **Upload** - After clicking the "Upload" button, the 'Local Toll Tables Available for Importing to OSB' section will be populated with the list of LTTs that are discovered in the OSV file.
-

Local Toll Tables available for uploading to OSB

- **Local Toll Table Name** - Filename of Local Table Name.
- **Related to** -.
- **Extracted from OSV** -.

Select the entries that you want to use on this Branch and then click **OK**.

You may view an LTT prior to importing by clicking the **View** button after setting the applicable checkbox(es).

IMPORTANT: If you select an LTT that has previously been uploaded, the existing entry in the XML file will be overwritten with the new data.

6.5.3 Features > SIP Service Provider Configuration

General

Configuration Item	Description	Possible Values	Operational Mode	Direction
SSP name	SSP name	--	-	-
SSP Default Profile	List of default SIP Service Providers (SSP) profiles available. If one profile is selected certain options/flags are enabled/checked/made required automatically. Field is optional.	• AT&T Flex Reach • AT&T Toll-Free • BT • COLT Telecom • DTAG/T-Systems (Sonus) • Level 3 Communications • Lync Mediation Server • Orange • Qwest • Skype-IP Auth • Telefonica • Vodafone/Arcor • Verizon-EMEA IP Trunking • Verizon-IPCC Trunking • Verizon-US IP Trunking • Sip Connect • DTAG/NGN Registration Mode	-	-
Allow sendind of insecure Referred-By header	If selected (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 scenario, 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) and the transferring party identity is in the Referred-By header field.	Enabled/Disabled. Default value: Disabled for all SSPs.	SM	Call transfer to SSP

Configuration Item	Description	Possible Values	Operational Mode	Direction
Send P-Preferred-Identity rather than P-Asserted-Identity	If selected (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.	Enabled/Disabled. Default value: Disabled for all SSPs.	SM	To SSP
Do not send Diversion header	If selected (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.	Enabled/Disabled. Default value: According to the SSP profile. See SSP Default profiles for details.	SM	Call diverted to SSP
Send URI in telephone-subscriber format	If selected (enabled), "+" is inserted only in front of the 'R-URI' and 'TO' headers (not the FROM, PAI, or Diversion headers).	Enabled/Disabled. Default value: According to the SSP profile. See SSP Default profiles for details.	NM	To SSP
Send authentication number in Diversion header	If selected (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 SP, the calling party number may not be a subscriber that belongs in that SP. In this case, the SP needs to authenticate the call based on the number of the redirecting subscriber, i.e., the number contained in the Diversion header.	Enabled/Disabled. Default value: According to the SSP profile. See SSP Default profiles for details.	NM	Call diverted to SSP

Configuration Item	Description	Possible Values	Operational Mode	Direction
Send authentication number in P-Asserted-Identity header	If selected (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.	Enabled/Disabled. Default value: According to the SSP profile. See SSP Default profiles for details.	NM	To SSP
Send authentication number in From header	If selected (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.	Enabled/Disabled. Default value: According to the SSP profile. See SSP Default profiles for details.	NM	To SSP
Include restricted numbers in From header	If selected (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)	Enabled/Disabled. Default value: Disabled for all SSPs.	SM	To SSP
Use SIP Service Address for all identity headers	If enabled, for both normal and survivability modes, identity header fields are modified to include the SIP Service Address network domain field. Applies to the SIP REGISTER (if registration used), INVITE, ACK, and BYE request methods. This parameter can be configured for all SSP profiles. By default, the following headers are modified to include the SIP Service Address: R-URI, From, To, P-Asserted-Identity and Diversion.	Enabled/Disabled. Default value: According to the SSP profile. See SSP Default profiles for details.	NM/SM	To SSP

Configuration Item	Description	Possible Values	Operational Mode	Direction
Sip Service Address	FQDN or IP address identifying the network domain for the SIP Service Provider.	--	SM	To SSP
Use SIP Service Address in Request-URI header	Modifies Request-URI header to include the SIP Service Address network domain.	Enabled/Disabled. Default value: According to the SSP profile. See SSP Default profiles for details.	NM/SM	To SSP
Use SIP Service Address in From header	Modifies From header to include the SIP Service Address network domain.	Enabled/Disabled. Default value: According to the SSP profile. See SSP Default profiles for details.	NM/SM	To SSP
Use SIP Service Address in To header	Modifies To header to include the SIP Service Address network domain.	Enabled/Disabled. Default value: According to the SSP profile. See SSP Default profiles for details.	NM/SM	To SSP
Use SIP Service Address in P-Asserted-Identity header	Modifies P-Asserted-Identity header to include the SIP Service Address network domain.	Enabled/Disabled. Default value: According to the SSP profile. See SSP Default profiles for details.	NM/SM	To SSP
Use SIP Service Address in Diversion header	Modifies Diversion header to include the SIP Service Address network domain.	Enabled/Disabled. Default value: According to the SSP profile. See SSP Default profiles for details.	NM/SM	To SSP
Use SIP Service Address in Contact header	Modifies Contact header to include the SIP Service Address network domain.	Enabled/Disabled. Default value: Disabled for all SSPs.	NM/SM	To SSP
Use SIP Service Address in Via header	Modifies Via header to include the SIP Service Address network domain.	Enabled/Disabled. Default value: Disabled for all SSPs.	NM/SM	To SSP
Use SIP Service Address in P-Preferred-Identity header	Modifies P-Preferred-Identity header to include the SIP Service Address network domain.	Enabled/Disabled. Default value: Disabled for all SSPs.	NM/SM	To SSP

Configuration Item	Description	Possible Values	Operational Mode	Direction
Privacy	Define Branch behavior in respect to receiving/sending /ignoring PAI (or PPI) header. - If Privacy Support is set to Basic, the OpenScape Branch SHALL NOT send a P-Asserted-Identity header field in the messages (requests or responses) to the endpoint. The OpenScape Branch SHALL also ignore any received P-Asserted-Identity header fields. - If Privacy Support is set to Full, the OpenScape Branch SHALL send a P-Asserted-Identity (or a P-Preferred-Identity) header field in the messages (requests and responses) to the endpoint. The OpenScape Branch 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 Branch SHALL send a P-Asserted-Identity (or a P-Preferred-Identity) header field in the messages to the endpoint. However, the OpenScape Branch 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 Branch SHALL NOT send a P-Asserted-Identity header field in the messages (requests and responses) to the endpoint. However, the OpenScape Branch SHALL accept any received P-Asserted-Identity header fields.	• Basic • Full • Full Send • Full Receive Default value: According to the SSP profile. See SSP Default profiles for details.	SM	To/From SS

Home DN

Configuration Item	Description	Possible Values	Operational Mode	Direction
Mandatory default home DN	If selected (enabled), the default home DN will always be used as the authentication number.	Enabled/Disabled. Default value: According to the SSP profile. See SSP Default profiles for details.	SM	To SSP
Mandatory default home DN - Normal Mode	If selected (enabled), the default home DN will always be used as the authentication number in Normal Mode.	Enabled/Disabled. Default value: According to the SSP profile. See SSP Default profiles for details.	NM	To SSP
Default home DN	Number required by SSP. It shall be configured accordingly to the phone number blocks provided by the provider to the SIP-PBX. This parameter is used in the following situations: - The Mandatory Default Home DN parameter is enabled. In this case the Default Home DN will always be used as the authentication id in Survivability mode. - In Survivability Mode when the Calling party is not an OpenScape Branch subscriber and there is no redirecting or transferring party (ex. GW to GW call). - In Survivability Mode when the redirecting or transferring party is not an OpenScape Branch subscriber (ex. GW to GW call). - The parameter Registration Required is enabled. Once the Registration required is set, the Default home DN becomes mandatory. The Default home DN is used to populate the "To:" and "From:" headers of the REGISTER request.	--	NM/SM	To SSP

Registration

Configuration Item	Description	Possible Values	Operational Mode	Direction
Registration required	If selected (enabled), the OSB will send registrations to SSP. If Business Identity Required is checked the Business Identity DN is used as the registration Address of Record in the From: and To: address fields allowing the Default Home DN to be used in OpenScape Branch Survivability Mode to identify a default Caller ID. NOTICE: If Registration required is enabled, different Trunk profiles must be used for different configured Gateways/Trunks.	Enabled/Disabled. Default value: According to the SSP profile. See SSP Default profiles for details.	NM/SM	Register to SSP
Registration interval (sec)	Registration interval in seconds	60 - 7200 seconds	NM/SM	Register to SSP

Business Identity

Configuration Item	Description	Possible Values	Operational Mode	Direction
Business Identity required	If enabled, requires the caller identified in the From header field contain the Business Identity DN.	Enabled/Disabled. Default value: According to the SSP profile. See SSP Default profiles for details.	NM/SM	To SSP
Business Identity DN	Contains the Business DN. Parameter takes precedence over: - Default Home DN if both are configured for the From Header - Include restricted numbers in From header which means the From header field will contain the Business Identity DN when caller Id is restricted. If Registration Required is set the Business Identity DN is used as the registration AoR in the SIP REGISTER message From: and To: header fields.	--	NM/SM	To SSP

Manipulation

Configuration Item	Description	Possible Values	Operational Mode	Direction
Insert Anonymous caller ID for blocked Caller-ID	If checked, and the INVITE sent by OpenScape Voice includes a Privacy header field with value of 'id', or the user identifies the call is to be made private (Privacy:user), OpenScape Branch overwrites the P-Asserted-Identity URI with the anonymous URI of anonymous@anonymous.invalid . In OpenScape Branch Survivable mode, Caller ID blocking feature is unavailable since the OSV equivalent of Calling Identity Delivery and Suppression (CIDS) is not an available feature to toggle delivery or suppression of the calling identity.	Enabled/Disabled. Default value: Disabled for all SSPs.	NM/SM	To SSP
Use single via header	When enabled, the mapped OSV Via header will be removed and it would not work anymore as proxy for the Via header point of view.	Enabled/Disabled. Default value: Disabled.	NM/SM	To SSP
Manipulation	Opens the Outgoing SIP Manipulation configuration window allowing creation/modification/deletion of specific SIP manipulation rules.	--	NM/SM	To SSP

Flags

Configuration Item	Description	Possible Values	Operation Mode	Direction
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. This flag is only valid if the entry in the Gateways / Trunks table to which the SSP Profile is configured with FQDN	Enabled/Disabled. Default value: According to the SSP profile. See SSP Default profiles for details.	SM	To SSP
REFER supported by SSP	This parameter indicates if the SSP supports REFER request. In Survivability Mode, when this parameter is not set, B2BUA entity is used to establish all calls with SSPs.	Enabled/Disabled. Default value: Disabled for all SSPs.	SM	To/From SSP
FQDN in Request-URI to SSP	If enabled the FQDN is sent in the R-URI of SIP Requests. This flag is only valid if the entry in the Gateways / Trunks table entry to which the SSP Profile is configured with a FQDN.	Enabled/Disabled. Default value: Disabled for all SSPs.		To SSP

Configuration Item	Description	Possible Values	Operation Mode	Direction
Use To DN to populate the RURI	Enable if the SIP Service Provider is sending the Account information in the Request URI and the destination information in the To header.	Enabled/Disabled. Default value: Disabled for all SSPs.	NM/SM	From SSP
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.	Enabled/Disabled. Default value: Disabled for all SSPs.	NM/SM	To SSP
Request-URI user in TO header to SSP	If enabled, To header user matches the Request-URI user in a new call to SSP.	Enabled/Disabled. Default value: Disabled for all SSPs.	NM/SM	To SSP
SSP does not accept long Record-Route headers	This flag indicates that the SSP does not accept long Record-Route headers.	Enabled/Disabled. Default value: Disabled.	NM/SM	To SSP
Remove the clearmode parameter from SDP towards SSP	Activate this flag to remove the clearmode parameter from SDP towards SSP.	Enabled/Disabled. Default value: Disabled.	NM/SM	To SSP
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. In this case, SSM takes control of this information and fix the SDP sent to the SSP partner endpoint.	Enabled/Disabled. Default value: According to the SSP profile. See SSP Default profiles for details.	NM/SM	From SSP
Do not send INVITE with sendonly media attribute	Do not send INVITE with sendonly media attribute to SSP. In this case, SSM removes the attribute from the SDP towards the SSP.	Enabled/Disabled. Default value: Disabled for all SSPs.	NM/SM	To SSP
Do not send INVITE with inactive media attribute	Do not send INVITE with video media line to SSP. In this case, SSM removes the video media line from the SSP towards the SSP.	Enabled/Disabled. Default value: Disabled for all SSPs.	NM/SM	To SSP
Do not send INVITE with video media line	Do not send INVITE with video media line to SSP. In this case, SSM removes the video media line from the SSP towards the SSP.	Enabled/Disabled. Default value: Disabled for all SSPs.	NM/SM	To SSP

Configuration Item	Description	Possible Values	Operation Mode	Direction
Do not send Invite without SDP	Do not send INVITE without SDP to SSP. When enabled, the OSB 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.  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 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. NOTICE: 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.	Enabled/Disabled. Default value: Disabled for all SSPs.	NM/SM	To SSP

Configuration Item	Description	Possible Values	Operation Mode	Direction
Do not send Invite without SDP	NOTICE: To use the flag, LAN-WAN or LAN-SSP interworking must be enabled. NOTICE: Starting from V10R3.03.00.	Enabled/Disabled. Default value: Disabled for all SSPs.	NM/SM	To SSP
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). SSM handles the re-invite locally.	Enabled/Disabled. Default value: Disabled for all SSPs.	NM/SM	To SSP
Do not send Re-Invite	Do not send re-invite at all to the SSP. SSM handles the re-invite locally.  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.	Enabled/Disabled. Default value: Disabled for all SSPs.	NM/SM	To SSP

Configuration Item	Description	Possible Values	Operation Mode	Direction
Do not send Re-Invite	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. NOTICE: To use the flags, LAN-WAN or LAN-SSP interworking must be enabled.	Enabled/Disabled. Default value: Disabled for all SSPs.	NM/SM	To SSP
Remove Silence Suppression Parameter on SDP	If enabled, removes the silence suppression parameter from SDP towards SSP.	Enabled/Disabled. Default is disabled for all SSPs.	NM/SM	To SSP
Enable local MOH in Survivable Mode and Force direction attribute to sendrcv	When checked, the OSB provides local MOH, i.e., no re-INVITE is sent to destination endpoint for media negotiation. Activate this flag when MOH is enabled and the target SSP does not re-INVITES or re-INVITES without SDP.	Enabled/Disabled. Default is disabled for all SSPs.	NM/SM	To SSP
Force direction attribute to sendrcv	This flag indicates if the SDP Media Attribute will be maintained, added or changed to sendrcv. This configuration is recommended for providers that do not accept to receive SDP without direction attribute. IMPORTANT: This configuration only applies for SIP responses.	Enabled/Disabled. Default is disabled for all SSPs.	NM/SM	To SSP

Digest Authentication

Configuration Item	Description	Possible Values	Operational Mode	Direction
Digest Authentication Supported	Enables Digest Authentication support. If enabled, the OpenScape Branch or OpenScape SBC will accept being challenged by the SIP SP and will respond with the credentials.	Enabled/Disabled. Default value: According to the SSP profile. See SSP Default profiles for details.	NM/SM	To SSP
Digest authentication realm	Configures Digest Authentication realm. A realm can be specified with an IP address, a FQDN or in format user@domain.	--	NM/SM	To SSP
Digest authentication user ID	Configures Digest Authentication user.	--	NM/SM	To SSP
Digest authentication password	Configures Digest Authentication password.	--	NM/SM	To SSP

TLS Support

Configuration Item	Description	Possible Values	Operational Mode	Direction
TLS Signalling	This item is used to configure how TLS as a transport type will be signaled in the SIP messages of remote endpoint calls. - Pass-Thru: Accept or Send transport=tls or SIPS in SIP Message. - 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 • Transport=tls • Sips Scheme • Endpoint Config Default value: According to the SSP profile. See SSP Default profiles for details.	NM/SM	To/From SSP

SIP Connect

Configuration Item	Description	Possible Values	Operational Mode	Direction
Use tel URI	When the SSP requires the use of tel URIs, the user must check this checkbox, in which case the OSB shall convert all SIP URIs to Tel URIs towards the SSP and vice versa.	Enabled/Disabled. Default value: Disabled for all SSPs.	NM/SM	To/From SSP
Send user=phone in SIP URI	When checked, the OSB adds "user=phone" in SIP URIs towards SSP.	Enabled/Disabled. Default value: According to the SSP profile. See SSP Default profiles for details.	NM/SM	To SSP
Registration Mode	This flag represents the Sip Connect registration mode support.	Enabled/Disabled. Default value: According to the SSP profile. See SSP Default profiles for details.	NM/SM	To SSP
TR118				

XML Flags

The following flags are configured via XML only. There is no graphical user interface available.

Configuration Item	Description	Possible Values	Operational Mode	Direction
Flag 12	If enabled, removes the clearmode parameter from SDP towards SSP. Applies to Verizon profiles only.	Enabled/Disabled. Default value: Disabled for all SSPs.	NM/SM	To SSP
Flag 14	If enable, this flag indicates the SSP does not accept long Record-Route headers. To complies with this type of SSP, OSB uses shorter form of private parameters added to the Record-Route header as: - bob instead of b2bua-ob-caller - etc.and also, remove some others such as fwan and twan indications, storing them internally by using the Kamailio's hash table.	Enabled/Disabled. Default value: Disabled for all SSPs.	NM/SM	To SSP

6.5.3.1 Features > SIP Service Providers Profiles

- **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** -Specifies the Remote Directory.
- **User name** - User name.Default: administrator

- **Password** - Up to 8 numerical characters are allowed.
- **Download New Default profile List** - Download new default profile list from an external SFTP (Secure File Transfer Protocol) server. The files will be downloaded in **.csv** format.

The list must be synchronized with SW deliverable, so as long a new provider is certified, the internal and external list are updated.

A new SIP Service Provider is configured using **Add** button. An existing SIP Service Provider can be changed using **Edit** button and deleted using **Delete** button.

- **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 home DN** - number required by SSP.
- **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.

6.5.4 Features > Auto Attendant

NOTICE:

Auto attendant is not allowed for Proxy ATA mode.

Time Information

- **Date** - It shows the date when the screen has been opened. It is a read only field.
- **Week day** - It shows the week day when the screen has been opened. It is a read only field.
- **Time** - It shows the time when the screen has been opened. It is a read only field.

General

- **Interdigit timer** - It is the time the system will wait for more digits when digits were already dialed. On the timer expiry, the system will process the dialed digits. Possible values are within the range 3-15 seconds.
- **Wait to go to menu** - It is a delay to get connected to announcements. Possible values are within the range 1 - 3 seconds.

- **Record access code** - It is the code to record the user's announcements. It is allowed a value up to 24 digits.

IMPORTANT: The aforementioned parameters (Interdigit timer, Wait to go to menu) can be modified & applied without the Asterisk restart mechanism, which causes the disconnection of all established calls.

Routing

- **Name** - Name of the Auto Attendant route. It is allowed a value up to 20 characters.
- **Routing method** - Method used to route a call to the Auto Attendant. The values available are:
 - 1) FQDN/IP: Domain name in the R-URI of incoming SIP calls.
It is also possible to route Integrated Gateway calls to the Auto Attendant by this routing method using the FQDN configured for the PRI/BRI/FXO port in the Trunk Group table.
 - 2) DN: Called destination number (user name in the R-URI of SIP call or called party number of BRI/PRI calls).
To route calls from an FXO port to the Auto Attendant using a DN, use the Default Destination configured in the FXO Port Configuration table.
- **FQDN/IP or DN** - FQDN/IP or DN that this routing table shall serve. The FQDN/IP or DN configured in this field must also be configured in the Comm System in order to route the calls to the Auto Attendant in Normal Mode.

NOTICE:

IPv4 and IPv6 addresses are supported.

- **Routing code** - In the case of Forced Announcement, it is necessary to manipulate the original dialed number by adding a routing code. This allows the Comm System to correctly route the call to the Auto-Attendant so that the initial greeting can be played to the caller. This routing code must be configured in the Comm System. It is allowed a value up to 24 digits.
- **Menu 1** - Select one of the created menus.
- **Menu 2** - Select one of the created menus.
- **Menu 3** - Select one of the created menus.
- **Initial greeting** - This greeting will be played when the caller reaches the Auto Attendant.
- **Forward to original destination** - This flag enables the Forced Announcement feature. If this flag is set, the initial greeting is played to the caller and the call is immediately routed to the original destination. When it is disabled, Menu 1 is a required field.
- **Default destination** - It is the default destination for calls when there is no menu associated or active for the called Auto Attendant route. The default destination number can be an extension number or an external number. It is recommended to use full extension number when configuring this parameter.

NOTICE:

When associating menus to an Auto Attendant route in the routing table, it is recommended to verify that there are no overlapping date/time intervals between the menus. If an overlap exists and it is desired to keep the configuration, the precedence of menus will be Menu1->Menu2->Menu3.

IMPORTANT: The aforementioned parameters (Name, Menu1/2/3, Initial Greeting, Forward to Original Destination, Default Destination) can be modified & applied without the Asterisk restart mechanism, which causes the disconnection of all established calls.

Menus

Displays a table with a summary of the configured Auto Attendant menus.

A new Menu is created by clicking the "Add" button, which opens the Auto Attendant Menu Configuration screen.

A previously configured menu can be changed by first clicking on it to select it and then clicking the "Edit" button.

A previously configured menu can be deleted by first clicking on it to select it and then clicking the "Delete" button.

Announcements

- **Browse** - Click the "Browse" button to locate an announcement file on your local computer or server that you want to upload to the Branch.
 - **Upload** - Once you have browsed to the file that you want to upload, click the "Upload" button.
 - **Delete** - A previously uploaded announcement can be deleted by first clicking on it to select it and then clicking the "Delete" button.
-

NOTICE:

Announcement files must conform to the following specification:

NOTICE:

- Bit rate = 128 kbps
 - Audio sample size = 16 bits
 - Channels = mono
 - Sampling rate = 8 kHz
 - Audio format = PCM
-

6.5.4.1 Features > Auto Attendant Menu

General

- **ID** - It is the Menu ID. It is a read only field.
- **Name** - It is the name of the Menu. It is allowed a value up to 20 characters.
- **Activation mode** - It is used to set the activation mode of the menu. The modes available are:
 - 1) Automatic - This menu is automatic activated if the current weekday and time is within the weekday/time range configured for the menu.
 - 2) Manual - This menu is manually enabled / disabled via access code. When activated, this menu has precedence over other menu types.
 - 3) Both - the menu can be activated/deactivated manually by access code or automatically by weekday/time interval.
- **Weekday start** - Weekday when the menu will start working. This option is only valid if Activation mode is set to automatic or both.
- **Weekday stop** - Weekday when the menu will stop working. This option is only valid if Activation mode is set to automatic or both.
- **Time 1 start and Time 2 start** - Time of the day when the menu will start working. This option is only valid if Activation mode is set to automatic or both.
- **Time 1 stop and Time 2 stop** - Time of the day that menu will stop working. The stop time cannot be earlier than the corresponding start time. This option is only valid if Activation mode is set to automatic or both.
- **Activation code** - Access code to manually activate a menu. This option is only valid if Activation mode is set to Manual.
- **Deactivation code** - Access code to manually deactivate a menu. This option is only valid if Activation mode is set to Manual.
- **Time out** - Time in seconds the user has to enter the first digit. In the first expiry of this timer, the Destination Selection Greeting is played again; in the next expiry, the call is forwarded to Default Destination, if configured. Otherwise, the call is disconnected. Possible values are within the range 3-15 seconds.
- **Destination selection greeting file** - Announcement to be played. This announcement should guide the caller to select a destination. Default file: vm-enter-num-to-call.wav. Text of announcement: "Please enter the number you wish to call"
- **Failure prompt file** - The prompt which is presented to the caller when the chosen destination is invalid. Default file: privacy-incorrect.wav. Text of announcement: "I'm sorry, that number is not valid."
- **Final prompt file** - The prompt which is presented to the caller when the chosen destination is invalid and the default destination could not answer the call for some reason or it is not configured. Default file: vm-goodbye.wav. Text of announcement: "Goodbye"
- **Default destination prompt file** - The prompt which is presented to the caller when the call is transferred to the default destination. Default file: priv-introsaved.wav. Text of announcement: "Thank you. Please hold, while I attempt to connect you with your party!"
- **Transfer prompt file** - The prompt which is presented to the caller when the call is transferred to the chosen destination. Default file: transfer.wav. Text of announcement: "Please hold while I try that extension."

- **Extension dialing** - When this parameter is set, the caller will be able to dial the desired extension number. The digit entering process is finished by timeout or by pressing '#'. Digits '*' and '#' can be configured in the Destination Table.
- **Default destination** - It is the escape destination. This field is mandatory when Extension dialing and Digit selection are not selected.
- **Number of extension dialing digits** - This is the maximum number of digits that can be dialed for an extension when extension dialing is selected.

IMPORTANT: The aforementioned parameters (Name, Activation Mode, Weekday Start/Stop, Time 1 Start, Time 1 Stop, Time 2 Start, Time 2 Stop, Time out, Destination Selection Greeting File, Failure Prompt File, Final Prompt File, Default Destination Prompt File, Transfer Prompt File, Extension Dialing, Default Destination, Digit Selection) can be modified & applied without the Asterisk restart mechanism, which causes the disconnection of all established calls.

Digits

- **Digit selection** - When this checkbox is checked, a table is available to configure the behavior for each digit that can be dialed. For each digit, the following parameters will be defined.
 - **Digit** - It is the digit number.
 - **Name** - Indicative name for the dial rule. It is allowed a value up to 20 characters.
 - **File** - Announcement file to be played if this digit is dialed. Default file: menu[menu ID]_digit[digit number].wav.
 - **Repeat this menu** - Repeats the Destination selection greeting file when this digit is dialed. If the checkbox is set, then the "File", "Destination", and "Allow recording" fields are ignored.
 - **Destination** - Destination number to which the call will be routed.
 - **Allow recording** - enable / disable announcement recording for that destination.

NOTICE: The default File may be empty.

NOTICE: The activation of the AA Automatic menu may take a minute more or less than the time set.

6.5.5 Features > Voice Mail Service

The VoiceMail Feature provides the capability of sending an E-Mail with & without Voice attachment as well as MWI notification and LED signalling on the OpenStage phones in Normal and Survivability mode.

General

- **VoiceMail Destination** - Default value set at 1234. It is allowed a value up to 30 digits.
- **VoiceMail Greeting** - The mailbox user shall be able to manage (record and change) his/her own Greeting Message. Default value: "vm-welcome.wav".
- **Maximum Number of Messages** - System max messages. Refer to following table:

OSB type	Max Messages default	Max Messages range
OSB 50i/250	30	10-500
OSB 1000	100	300-2000
OSB6000	300	100-9999
OSB 500i	60	20-1000
ATA, GW only	-	-

- **Maximum Message Length (sec)** - Default value set at 30 sec. Range: 10-90 sec.
- **Silence Time Before Ending Recording (sec)** - Default value set at 10 sec. Range: 5-20 sec
- **VoiceMail Retrieve Destination (From Own Ext.)** - Default value set at 2345.
- **VoiceMail Retrieve Prompt (From Own Ext.)** - Default value: "vm-welcome.wav".
- **VoiceMail Retrieve Destination (From Other Ext.)** - It is the code to record the user's announcements. It is allowed a value up to 24 digits.
- **VoiceMail Retrieve Prompt (From Other Ext.)** - Default value: "vm-welcome.wav"
- **Maximum Login Attempts Allowed** - The mailbox user shall have configurable maximum login attempts for message retrieval. The retrieval call shall be disconnected after maximum (configurable) failed logins. Range: 3-10 attempts

VoiceMail Boxes

- **Enabled** - Checkbox for enabled/disabled VoiceMail Box
- **Name** - VoiceMail Box name
- **MailBox Number** - MailBox Serial Number
- **PIN** - PIN number length: 4 numeric digits (valid field value)
- **Max Msg length(sec)** - Default value: 30 sec. Range: 10-90 sec
- **Announce CID** - This checkbox is enabled by default.
- **Send MWI** - This checkbox is enabled by default.
- **Email Address** - IP or FQDN.
- **Send Email** - This checkbox is disabled by default
- **Attach Msg to Email** - This checkbox is disabled by default.
- **Del Msg after Snd/Synch** - This checkbox is disabled by default
- **VoiceMail Default Box** - If no configured VoiceMail box for the dialed DN is found, the Message will be placed here. Number of digits to match can be configured as "Full" or "Last Digit" match.

- **VoiceMail Box Match** - VoiceMail message can be left for that particular DN if this DN was dialed and VM Box is configured for that DN.Exact Number match is required.
-

Maintenance

- **Keep Retrieved Messages** - This checkbox is disabled by default.
 - **VoiceMail Storage Time (weeks)** - The VoiceMail storage time can be configured. The default value is 1 Week. The possible values are 1, 2, 3 weeks or blank. After this time all the recorded messages will be removed, including the unread ones. Default value:1 week.
 - **E-Mail Server**- In order to be able to send email notifications, an email server account shall be configured for the voicemail. User and Password are optional.
 - **E-Mail Server Type** - e.g POP3
 - **Synchronize VoiceMail Messages** - Disabled by default.
 - **Clear VoiceMail Folder** - Enabled by default.
-

Announcements

- **Browse** - Click the "Browse" button to locate an announcement file on your local computer or server that you want to upload to the Branch.
- **Upload** - Once you have browsed to the file that you want to upload, click the "Upload" button.
- **Delete** - A previously uploaded announcement can be deleted by first clicking on it to select it and then clicking the "Delete" button.
- **VoiceMail Retrieve Prompt** - default: "Please enter a Mailbox Number"
- **VoiceMail Retrieve PIN** - no naming restrictions
- **VoiceMail Retrieve Wrong PIN**-default: "MailBox or login incorrect please check the number and try again"
- **VoiceMail Retrieve Change PIN** - default: "Please enter your new password"
- **VoiceMail Retrieve Change PIN failed** - default: "The password your entered did not match, please re-enter..."
- **VoiceMail Retrieve Wrong Box Number** -default: "vm-incorrect-mailbox.wav"="MailBox or login incorrect please check the number and try again"

The user can upload the files into the `/opt/siemens/openbranch/var/mngmt/vmgreetings` directory and upon selecting it in the GUI, the file will be copied into the `/var/lib/asterisk/sounds/VM-OSBbase-en` directory and renamed to the right name.

6.5.6 Features > Phone Software Management

Periodic Branch Pulling Software from Central Server

- **Enable software pulling** - The checkbox enables or disables the downloading of phone load images from the server.

- **Start time** - The time of day when the downloading of phone images will begin.
- **Stop time** - The stop time to end the downloading of phone images, if not completed already.
- **Central phone software server URL** - The URL points to the central server that contains the phone load images.

NOTICE:

IPv4 and IPv6 addresses are supported.

- **Start software pulling** - Clicking the button starts manual software pulling of phone software images from the central server.
-

Phone Pulling Software from Branch

This section allows the Branch to provide phone load images to phones.

- **Enable image provisioning** - The checkbox enables or disables the provisioning of load images to phone.
- **Maximum parallel access** - The drop-down box specifies the maximum number of parallel upload sessions that are allowed.
- **Available phone software images** - A list of available phone load images. Load images can be delete from the list by first left-clicking on the image to highlight it, and then left-clicking the "Delete" button.

6.5.7 Features > Media Server/Streaming

The Media Server/Streaming provides announcements and station controlled conference for the subscribers. The Streaming Feature provides the capability of Streaming content for Music On Hold based on an Internet radio stream (e.g Web Radio) or a local Wave file in Normal & Survivable Mode invoked by MGCP Message.

The supported codecs are G711 a-law and G711 u-law.

In order to ensure support of secure media exchange (SRTP) with the Media Server, Branch and phone real-time clocks should be synchronized through NTP.

General

- **Media server listen port** - The port the Media Server uses for communication with the Call Agent.
- **Use system FQDN** - If enabled, instead of the system IP address, the system FQDN is used on media transactions.
- **Language** - It is used to select the preferential language.
- **Enable whisper Mode** - Whisper mode is a media server capability that allows a supervisor agent to whisper to a monitored agent. Checking this box will enable this capability on the media server.
- **Advanced...** - Click this button to bring up an additional screen with advanced configuration options.

Conference

- **Number of conference / whisper cells** - The maximum number of ports/cells that are opened for providing conferences.
- **Maximum conference time (sec)** - The maximum time, in seconds, a conference is allowed to be active.

The **unlimited** check box will disable this configuration.

- **Conference prefix access code** - Prefix in SIP R-URI required to access a Media Server conference.

Announcements

- **Number of announcement ports** - The maximum amount of ports that are opened for providing announcements.
- **Maximum announcement time (sec)** - The maximum time, in seconds, an announcement session is allowed to be active for an inactive connection.

The **unlimited** check box will disable this configuration.

- **Stop announcement on DTMF** - If it is enable, the announcement will stop when the Media Server receives a DTMF.

Streaming Source

IMPORTANT: This tab requires Base License V9 or greater.
Streaming is a V9 license based feature.

- **Enable Music On Hold Streaming** - Enables the MOH streaming feature.
- **Use HTTP proxy** - Enables the HTTP proxy usage for accessing the Streaming Source.Disabled by default.
- **HTTP proxy FQDN or IP** - IP address format check - **IPv4** only (for now)
- **HTTP proxy port** - Possible values: **80, 8080**
- **Local FQDN or IP** - Local Steaming Interface, length is limited to 32 characters. Default value: LAN-IP If no WAN available/WAN-IP if WAN available
- **Streaming buffer size (sec)** - Possible values: 0-60 sec.Default value:30 sec
- **Streaming Source URL (first)** - Length is limited to 40 characters.

The **Status** green if Streaming server is connected + steaming source (link to Internet radio or local file, or ERROR).

- **Streaming Source URL (fallback)** - Length is limited to 40 characters

6.5.7.1 Features > Media Server Advanced Configuration

MS Adapter

The MS Adapter is used for NAT traversal of the MGCP communication between the local Media Server and the Call Agent when the Branch is in Branch SBC or SBC-Proxy modes.

- **Transaction time-to-live** - It is used to configure the maximum duration, in seconds, of an MGCP transaction in Branch SBC or SBC-Proxy modes.
-

Languages

- **Installed languages** - This area lists all installed Media Server languages. To delete a language, select the language and then click the Uninstall button.
- **Install Language** - A new language can be installed by browsing to the applicable language file on your local computer or server and then clicking the Install button.

6.5.8 Features > Backup Link Client Configuration

This window is available only when Backup link mode is set to Backup Link Client.

NOTICE:

Backup Link Client is not allowed for Proxy ACD mode.

General

- **Primary DID number** – Standard E164 number used for setting up a clearmode call to the Primary Backup Link Server (E.164 number type - maximum 15 digits).
- **Secondary DID number** – Standard E164 number used for setting up a clearmode call to the Secondary Backup Link Server (E.164 number type - maximum 15 digits).
- **Packetization interval** – Specifies the interval for RTP packetization on the clearmode call. Allowed values are 10, 20, 30, 40, 50 and 60 ms.
- **PPP authentication** – This is the PPP authentication method used by Backup Link Client and Backup Link Server. Note that this authentication must be same at both ends. The supported authentication methods are None, PAP (Password Authentication Protocol) or MSCHAP-V2 (MS Challenge Handshake Authentication Protocol V2).
- **Username** – This is the username used when authentication method is PAP or MSCHAP-v2.
- **Password** – This is the password used when authentication method is PAP or MSCHAP-v2.
- **RTP port minimum** – Base local port for RTP communication.
- **RTP port maximum** – Maximum local port for RTP communication.
- **Congestion delay (seconds)** – In case of backup link congestion, the SIP Server shall generate 503 responses with Retry-After for new requests. The

Congestion Delay specifies the Retry-After time value sent to the phones, after which they should send again their requests.

Multi-Link

- **Minimum number of B-channels** – Minimum number of B-Channels to use.
 - **Minimum bandwidth (kbps)** – Minimum bandwidth used by B-Channels. It is the result of maximum number of B-Channels * 64 kbit/s. It is a read-only data.
 - **Maximum number of B-channels** – Maximum number of B-Channels to use. Maximum B-Channels are immediately started when Survivable Mode is reached.
 - **Maximum bandwidth (kbps)** – Maximum bandwidth used by B-Channels. It is the result of maximum number of B-Channels * 64 kbit/s. It is a read-only data.
 - **Initial number of B-channels** – Initial number of B-Channels to be initially established when Backup Link is started at normal mode.
 - **Initial bandwidth (kbps)** – Initial bandwidth used by B-Channels. It is the result of initial number of B-Channels * 64 kbit/s. It is a read-only data.
 - **High watermark (%)** – High watermark that indicates when a new tunnel must be added to the bundle.
 - **Low watermark (%)** – Low watermark that indicates when a new tunnel must be removed from bundle.
 - **High watermark detection window (sec)** – Amount of time (seconds) that the Backup Link usage will stay over the High Watermark before adding a new tunnel to the bundle.
 - **Low watermark detection window (sec)** – Amount of time (seconds) that the Backup Link usage will stay below the Low Watermark before removing an existing tunnel from the bundle.
-

Routing

- **IP address** – IP addresses that will also be routed through the Backup Link in addition to the regular Backup Link Server IP address.
 - **Description** – Simple description text for documenting the reason the current entry has been added.
-

Backup Link Client configuration restrictions

Some parameters at "VOIP/Comm System" need special configuration for avoiding Transition Mode when link is already up:

- **OPTIONS timeout (sec)** must be at least 10s
- **Failure threshold (pings) multiplied by OPTIONS timeout (sec)** must be at least 30s

Furthermore, the following configuration restriction is necessary to avoid the link entering in Survivable Mode upon construction:

$$Mtt \leq Tt * Oi + (Tt - 1) * Ot$$

Where:

- Mtt = Maximum time in transition mode = 60s if only Primary link is configured or 120s if also Secondary link is configured;
 - Tt = Transition Mode threshold
 - Oi = OPTIONS interval
 - Ot = OPTIONS timeout

Backup Link Client configuration tables

To calculate the bandwidth requirements for the backup link, the administrator needs to know the number of registered SIP users (note that each line of a keyset is a registered SIP user). With this number, the initial bandwidth requirements can be derived from the following table.

Number of registered Users	Initial / Minimum number of B-Channels
0 - 50	1
51 - 250	1
251 - 1000	2
1001 - 3000	3
3001 - 6000	4

The Maximum number of B-Channels shall be chosen according to the time to transition the branch office from survivable mode to normal and to the number of registered users. The following table displays the required number of backup links for a given set of transition times and registered users.

6.5.9 Features > Backup Link Server Configuration

Configuration for all clients in a Backup Link Server. This window is available only when Backup link mode is set to Backup Link Server.

NOTICE:

Backup Link Server is allowed only for Proxy or SBC-Proxy modes.

General

- **Max backup links** – This is the maximum number of Backup Links that a Server may accept. After achieving this limit, the Server will drop links based on priority evaluation. Note: This field shall be configured based on the availability of channel in the gateway at data center for backup link connection.
- **Max B-channels** – Maximum number of B-Channels that Backup Link Server may set up among all bundles.

- **Packetization interval** – Specifies the interval for RTP packetization on a clearmode call. Allowed values are 10, 20, 30, 40, 50 and 60 ms.
 - **RTP port minimum** – Base local port number for RTP communication.
 - **RTP port maximum** – Maximum local port number for RTP communication.
 - **PPP subnet** (IP address/netmask bits) – The fields "PPP Local IP Address" and "PPP Remote IP Address" must be removed from the Client configuration. PPP Subnet will be used for all clients.
 - **LSM IP Address** – This is the IP address for LSM in Comm System.
-

Clients

- **Tunnel name** – BLS tunnel name informed on SNMP trap sent to Comm System to set up CAC policy. Special characters < > \ , ' " are not allowed.
 - **BLC hostname** – Hostname of the Branch that hosts the Backup Link Client.
 - **Priority** – This is the priority used for accepting or rejecting an incoming tunnel construction request. When the maximum number of backup links is achieved, the Server will drop the link with lowest priority. New incoming tunnels with the same priority of existing tunnels will be dropped in favor of the existing ones. Priority 0 (zero) is the highest priority.
 - **PPP authentication** – This is the PPP authentication method used by Backup Link Client and Backup Link Server. Note that this authentication must be the same at both ends. The supported authentication methods are None, PAP (Password Authentication Protocol) or MSCHAP-V2 (MS Challenge Handshake Authentication Protocol V2).
 - **Username** – This is the username used when the authentication method is PAP or MSCHAP-v2.
 - **Password** – This is the password used when the authentication method is PAP or MSCHAP-v2.
 - **Retry after** – This is the timeout sent to Backup Link Client upon Backup Link rejection due to priority evaluation, when the maximum number of Backup Links is reached. See also the Priority description. The Backup Link Client will retry the Backup Link establishment after this time.
-

Routing

- **IP address** – IP address that will also be routed through the Backup Link in addition to the regular Backup Link Server IP address.
- **Description** – Simple description text for documenting the reason the current entry has been added.
- **Tunnel name** – Enter one of the Backup Link Server tunnel names from the Clients table.

6.5.10 Features > Multi Line Hunt Groups

NOTICE:

Multi Line Hunt Groups (MLHG) are not allowed for Proxy ATA mode.

NOTICE: MLHGs apply to Survivability mode only.

NOTICE: The MLHG Loop detection is triggered after the fourth time overflowing between MLHGs in Survivability mode.

A new MLHG is created by clicking the **Add** button. The MLHG can then be configured in the corresponding row in the table. An MLHG is deleted from the table by first clicking on the relevant row and then clicking the "Delete" button.

- **Enable** - Enable or disable this MLHG.
- **Pilot number** - This box defines the MLHG access code. Must be a full DN.
- **Pilot type** - has two options:
 - pilot: must be a full DN referring to an existing subscriber that is registered on this OpenScape Branch. The pilot DN will be the first group member.
 - non pilot: can be any valid DN but must not be an existing subscriber DN or gateway that is registered on this OpenScape Branch.
- **Hunt type** - has 4 different types:
 - linear: the hunting will begin with the first group member, as defined in the group member list.
 - cyclic: the hunting will begin with the first group member immediately following the last group member that answered a call.
 - parallel: all members will ring simultaneously.
 - UCD: UCD hunting is similar to cyclic hunting but the call will be presented to the members until a disconnection or answer. It will not be disconnected after the first cycle for the group members. A call to a UCD type MLHG will be forwarded to the overflow destination, if it is configured, and the number of calls waiting for answer in the group is greater than the number of members. If the overflow destination is not configured, the call will be disconnected.
- **No answer advance timer** - this timer represents the period (in seconds) that each group member will ring before the next group member is called. The default value is 30 seconds and the range is 5 to 3600 seconds.

Note: In the case of parallel hunting it is recommended to set this timer to 0.
- **Overflow destination** - in case none of the MLHG members answer the call, the overflow destination is called. The overflow destination can be a subscriber DN, another MLHG, or a PSTN number.
- **Overflow timer** - Configurable timer set for the Overflow destination.

Default value set at 0 and the range expands to 120 seconds.

- **Members** - a comma-separated list of member DNs. Note that only full DNs are permitted. The order of the members in the list dictates the order that they will be selected by the various hunting types.

NOTICE:

If a Pilot number has been defined, and the Pilot type is "pilot", then the Pilot number is the first member of the list.

IMPORTANT: The aforementioned parameters (Enable, Pilot Number, Pilot Type, Hunt Type, No Answer Advance Time, Overflow Destination, Members) can be modified & applied without the Asterisk restart mechanism, which causes the disconnection of all established calls.

Configuration for All Multi Line Hunt Groups

- **Member Advance Timer / sec** - Configurable Timer set to advance to the next Member if the current Member is unavailable or busy.

Default value =1

Range = 0 - 10 seconds (0 - 100 msec)

6.5.11 Features > Automatic Call Distribution (ACD)

In this screen the user can configure the Automatic Call Distribution parameters.

General

- **Agents log On service access code** - defines the log on access code for all agents. The value must be different from the Agents log Off service access code. Valid digits are 0-9 and "*".
- **Agents log Off service access code** - defines the log off access code for all agents. The value must be different from the Agents log On service access code. Valid digits are 0-9 and "*".
- **Agents timeout** - defines how long an agent will ring before the agent is considered unavailable and is logged off from the queues. The agent will need to log on again. It will not have effect if the advance timeout is greater than the Queue advance timeout.
- **Support keyset toggle key** - determines if the availability of the agents is updated using the keyset-toggle Make Busy key on the Agent's device
- **Keyset toggle service access code** - defines the keyset toggle access code for all agents. Valid digits are 0-9 and "*". if enabled, then Log On/Off Access codes are disabled. Availability of agent is determined by using the keyset-toggle Make Busy Key on the Agents device.

IMPORTANT: The aforementioned parameters (Agent Log On / Off Service Access Code, Agents Timeout, Support Keyset Toggle Key, Keyset Toggle Access Code) can be modified & applied without the Asterisk restart mechanism, which causes the disconnection of all established calls.

IMPORTANT: ACD currently uses the rmemory hunt mechanism (round robin with memory, remember where we left off last ring pass)

Queues

This section displays a table with a summary of the defined ACD queues.

A new ACD queue can be created by clicking the "Add" button, which will open the ACD queue screen with the full set of configuration options.

Up to 100 ACD queues can be configured. The "Add" button is disabled when this limit is reached.

An existing ACD queue can be edited by first clicking it to select it, and then clicking the "Edit" button.

An existing ACD queue can be deleted from the table by first clicking it to select it, and then clicking the "Delete" button.

- **Queue ID** - Internal ID which identifies the queue. It is used for profile assignment and is not configurable.
- **Queue name** - Name of the queue.
- **DID list** - List of DID numbers to access the queue from gateway or SIP server.
- **Destination (overflow, voice mail)** - Destination number of a queued call when the limit of calls in the queue is reached or the timeout for a call in the queue is elapsed. Alternately, a Voice Mail Server number where a call is immediately diverted when there are no agents available in the queue.
- **Assigned agent IDs** - The list of assigned agent IDs is displayed clicking on the "show" link.

Profiles

This section displays a table with a summary of the defined ACD profiles.

A new ACD profile can be created by clicking the "Add" button.

Up to 100 ACD profiles can be configured. The "Add" button is disabled when this limit is reached.

The profile names and queue IDs are edited directly in this table. To assign more than one queue ID to the same profile, enter the queue IDs separated by commas.

An existing ACD profile can be deleted from the table by first clicking it to select it, and then clicking the "Delete" button.

Agents

- **Configure** - This button opens a new screen where it is possible to configure the ACD agents.

- **Show agent status** - This button opens a new screen which presents the status of all agents.

Files

- **Prompt language** - Select the language of the audio prompts used by the Backup ACD. By default, the language will be selected according to the country settings. The following languages are available: **English - US, English – British, Portuguese – Brazil, Spanish, Italian, German, French.**

The default value of the language according to the country is defined as following:

Country	Language
Argentina	Spanish
Australia	English-US
Austria	German
Belgium	French
Brazil	Portuguese-Brazil
Bulgaria	English-US
Chile / Chile 2	Spanish
China	English-US
Colombia, Colombia Claro, Colombia Telefonica	Spanish
Czech Republic	English-US
Denmark, Estonia, Finland	English-US
France	French
Germany	German
Greece, Hong Kong, Hungary, India, Israel	English-US
Italy	Italian
Japan, Korea, Lithuania, Malaysia	English-US
Mexico	Spanish
Netherlands, New Zealand, Norway	English-US
Panama	Spanish
Philippines, Poland, Portugal, Russian Federation, Singapore, South Africa	English-US
Spain	Spanish
Sweden	English-US
Switzerland	German
Taiwan, Thailand, Turkey	English-US

Country	Language
United Kingdom	English-British
United States / North America, United States Circa 1950 / North America	English-US
Venezuela	Spanish
Other countries	English-US

- **Music on hold files** - A new Music on hold file is uploaded to the system using "Upload" button. The available music on hold files are shown in this box and can be used in one or more queues. A music on hold file is deleted from the system using "Delete" button.
- **Announcement files** - A new announcement file is uploaded to the system using "Upload" button. The available announcement files are shown in this box and can be used in one or more queues for queue join, queue waiting or agent announcement selection. An announcement file is deleted from the system using "Delete" button.

NOTICE:

Only WAV audio files (.wav) that comply with the following requirements can be uploaded:

NOTICE:

- Bit Rate: 128 kbps
- Audio Sample size: 16 bit
- Channels: Mono
- Sampling Rate: 8 kHz
- Audio Format: PCM
- Available space in the system. For Systems with 2GB of flash memory this is critical. It is not recommended to upload more than 20 MB of WAV files to the system.

Logs

Get logs - Using this button, the user can download a tar file containing the log files for all queues. This file contains the queue logs that can be used by an external application to generate call, agent and queue statistics.

Each of these files will contain log information for events that occurred in the last 24 hours.

6.5.11.1 Features > ACD > Queues**General**

- **ID** - Internal ID which identifies the queue. It is used for profile assignment and is not configurable.

- **Name** - Queue name.
- **Destination (overflow, voice mail)** - Destination number of a queued call when the limit of calls in the queue is reached or the timeout for a call in the queue is elapsed. Alternately, a Voice Mail Server number where a call is immediately diverted when there are no agents available in the queue.
- **Queue advance timeout** - Time to advance the call to the next available agent position if the current ringing agent does not pick up the call. If the Agent timeout is elapsed before the Queue advance timeout, this value will never be reached because the agent will be logged off automatically, and the call will be advanced to the next available agent.
- **Agents wrap up time** - Time to keep the agent unavailable after he/she hangs up on a call. This time allows the agent to do post-call processing.
- **Play ring tone instead of music on hold** - This check box specifies that the calls are receiving ringing tone instead of music on hold. This can be useful for queues for which the average holding time is very low.
- **Music on hold** - This box allows the selection of uploaded music on hold files which will be played to callers in the ACD queue.
- **Generate diversion header** - This box allows the addition of a SIP Diversion header when a call is diverted to the number in the Destination (overflow, voice mail) box.
- **DID list** - This box allows entering the DID numbers that need treatment by a backup ACD queue. There is no limit on the DID numbers. A DID number is created using "Add" button, and deleted from table using "Delete" button. During transition to normal mode, Branch de-queues queued calls to Comm System using the same DID number that was used to dial to ACD group.

IMPORTANT: The aforementioned parameters (Queue ID / Queue Name, DID List, Overflow, Queue Advance timeout, Agents Wrap up Time, Play ring tone instead of music on hold, Music on Hold, Generate Diversion Header) can be modified & applied without the Asterisk restart mechanism, which causes the disconnection of all established calls.

Agent timeout versus Queue advance timeout behavior

If the Agent timeout is greater than the Queue advance timeout, when the ACD call rings on the agent until the Queue advance timeout expiration, the agent will stop ringing (but not logging off) and the next available agent will be called.

If the Agent timeout is lower or equal than the Queue advance timeout, when the ACD call rings on the agent until the Agent timeout expiration, the agent will stop ringing, will be logged off and the next available agent will be called.

The difference between the timeouts shall be at least 5 seconds in order to avoid delays caused by, for instance, cell calls.

Caller Parameters

- **Overflow to voice mail server** - This box allows the immediate diversion of a call to the Voice Mail Server number entered the Destination (overflow,

voice mail) box when there are no agents available in the queue. When selected, the following boxes are disabled: Queue advance timeout, Play ring tone instead of music on hold and Music on hold.

- **Maximum waiting time** - This box defines the maximum time that a caller can be in a queue before being transferred to the Destination (overflow, voice mail).
- **Maximum callers** - This box defines the maximum number of calls that can be queued in the ACD queue. When reached, the call will be further treated by the Destination (overflow, voice mail). The unlimited check box will disable this configuration.

Agent Overview

- **Show agent status** - This button opens a new screen which presents the status of agents configured for the selected queue.

Announcements

- **Queue join announcement** - This announcement is played when a call is entered in the queue. The announcement file is selected from the uploaded announcement file list.
- **Queue waiting announcement** - This announcement is periodically played to the caller. The announcement file is selected from the uploaded announcement file list.
- **Agent announcement** - This announcement is played to the agent before the call is connected. The announcement file is selected from the uploaded announcement file list.
- **Announce position to caller** - When this check box is selected an announcement informing the position in queue is periodically played to the caller.
- **Announce estimated hold time to caller** - When this check box is selected an announcement informing the estimated hold time is periodically played to the caller.
- **Announce hold time to agent** - When this check box is selected an announcement informing the time the caller has been waiting in the queue is played to the agent before the call is connected.
- **Position/hold time announcement frequency** - This box defines (in seconds) how often the announcements of position and estimated hold time are played to the caller.
- **Interval between queue join and queue waiting announcements** - This box defines (in seconds) how often the queue waiting announcement is played to the caller after the queue join announcement.

Announcement playback is provided on this screen. Next to each drop-down box used to choose the announcement file, there is a Play button for playback. When clicked, this button will start the reproduction of the selected file.

IMPORTANT: The queue timeout starts counting only after the join announcement has ended.

6.5.11.2 Features > ACD > Agents

A new ACD agent is created using the **Add** button. The ACD agent is deleted from table using "Delete" button. The maximum number of allowed agents depends on hardware platform, please consult the configuration guide. The "Add" button is disabled when this limit is reached.

IMPORTANT: For OSB 500i, the maximum number of Backup ACD Agents is 250. For OSB 1000/ 6000, the limit is 500.

- **Agent ID** - the agent identifier used in logon/logoff procedures. Agent IDs can't be duplicated. Only numerical values are allowed. Up to 15 numerical characters are allowed.
- **Agent name** - a name to identify the agent.
- **Password** - a password used in logon/logoff procedures. Up to 8 numerical characters are allowed.
- **Confirm password** - the same password used in Password field.
- **Assigned profile** - Queue profile assigned to the agent. The profiles must be configured previously in the Profile table.
- **Auto-Logon** - Allow ACD agents to be configured in such a way that login is not required to turn active. If the auto-login is set to **Yes**, then it's mandatory that the agent login be the same as the AOR used by the agent. The agent ID must correspond to the DN used for registration.

IMPORTANT:

The OSB supports only 3 queues per profile, if the registries are simultaneous. In case you close the Desktop Client and don't logout, the call will ring in until the timer expires. After that, it will be redirected to another user. (The register will be present till the timer expires). After the registry expires, this user will not be called anymore.

IMPORTANT:

The aforementioned parameters (Agent ID, Agent Name and Password) can be modified & applied without the Asterisk restart mechanism, which causes the disconnection of all established calls.

NOTICE:

The Circular Round Robin mechanism is applied, in order to offer calls to agents.

NOTICE:

The following features should not be used in ACD agents:

NOTICE:

- Do Not Disturb;
 - Call Refuse,
 - Call Deflect,
 - Call Forwarding (all types),
 - Large Conference,
 - Keysets/Line Appearances,
 - Call Waiting
 - Hot/Warm Line.
-

6.5.12 Features > Emergency Calling

Emergency Calling Subnets

The table lists the currently configured emergency calling subnets. For a definition of the fields in the table, refer to the "Emergency Calling Subnets" help page.

- **Add** - To add a new entry to the table, click the "Add" button. Refer to the "Emergency Calling Subnets" help page for details regarding how to define a subnet.
 - **Edit** - To edit an entry in the table, first select it by clicking it and then click the "Edit" button. Refer to the "Emergency Calling Subnets" help page for details regarding how to edit a subnet.
 - **Delete** - To delete an entry in the table, first select it by clicking it and then click the "Delete" button.
-

Emergency Calling Number

An Emergency number can be added to the list by entering the number or a regular expression rule (to set a specific range of numbers) in the **Emergency numbers** field and then clicking **Add**. To remove an Emergency number from the list, first click it to select it, and then click **Delete**.

IMPORTANT: The rules for the regular expressions are the same described for the Routing Prefix on Gateways/Trunks configuration. For further information refer to [Features > Gateways/Trunks Provisioning](#) on page 540.

The list of Emergency numbers, when dialed, will allow the Branch to identify an Emergency Call.

A call to a number in this list will trigger the server to try to establish an outgoing call to an available gateway (highest priority).

The search for an emergency destination is performed as follows:

- Try a gateway configured with Functional type set to "Emergency".
- If no emergency gateway is available, try to use the lowest priority gateway by checking 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 the local attendant configured in the 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 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, which means that both are associated to that subnet. For this reason, you will not be permitted to delete the 9 or the 911.

NOTICE:

Emergency Calling menu is not available for configuration for OSB Gateway Only and OSB Proxy ATA.

6.5.12.1 Features > Emergency Call Routing

General

- **Subnet based routing** - Checking this flag (selected by default) will enable the Subnet based routing (Using IP address or subnet and Subnet mask), in this case once selected it will gray out the DN list settings.
- **DN list based routing** - Checking this flag will enable the DN numbers list. When checked, the Subnets settings are grayed out.
- **IP address or subnet** - This configures the IP address (or range of IP addresses) of the subscriber(s).

NOTICE:

IPv4 and IPv6 addresses and subnet masks are supported.

- **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.
- **DN numbers** - List of DN numbers. Up to 10 entries, numbers can be entered using regular expressions.
- **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.

INFO: If the gateway is required to make Emergency as well as normal calls, select **None**.

- **Description** - An arbitrary string used for description in symbolic way.
- **Default destination** - It is a fully registered and callable local SIP phone number. When the emergency call to the PSAP fails, the emergency call is

redirected to this default destination (attendant) which may have a PSTN land line to call the PSAP directly to report the emergency for the original caller.

- **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.

When the query doesn't match any subnet corresponding to the contact IP then the query based on DN is invoked.

LIN

This table is where the list of LIN numbers is constructed or edited. 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 that the emergency services are not constrained.

- **LIN** - This is the Location Identification Number used to associate a subscriber with their physical location. Only numerical digits or the character + are supported.
 - **Callback number** - It is a callable phone number registered at the PSAP. If an outgoing emergency call is unintentionally interrupted, the remote operator may place a callback call at this number. The Branch will then redirect the call to the original phone which started the emergency call.
 - **Default callback number** - It is a callable phone number to which the callback call will be redirected if the checkbox is enabled.
 - **Use default callback number** - If enabled, redirect any callback call to Default callback number instead of the original caller.
-

NOTICE:

Please note that when a 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 15 minutes, 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 Branch supports transparent conveyance of location information (i.e. the GeoLocation header field and the PIDF-LO) from the phone towards the OpenScape Voice. The OpenScape Branch Proxy ATA and OpenScape Branch as Gateway Only will only be able to include Location information data for their Analog Subscribers (FXS ports)

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
- 4) The INVITE will not be directly routed to Asterisk (survivable mode)
- 5) The IP address of the originator is part of a subnet which is configured in the Emergency Calling Subnet of the OSB

- **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

NOTICE:

For an OSB 50i or OSB Proxy ATA, the location information shall be configurable for FXS ports

6.5.13 Features > Call Forwarding

In this screen it is possible to configure the Call Forwarding parameters for survivability mode.

System Call Forwarding is valid for calls originally addressed to subscribers who are registered on the Branch.

The Following parameters may be used in Call Forwarding (depending on which "Activate" flag(s) is(are) checked):

- **Error codes** (only for Forward On Error) - A sequence of SIP error codes separated by semicolons. The error codes 408 and 486 may not be used here since they are covered by the other Call Forwarding options.
- **Redirect number** - A digit string with up to 24 digits to be used as a DN.
- **Ring duration** (Forward No Reply Only) - A range from 1 to 60 seconds (Default: 24 sec). This timer defines how long a subscriber will ring before the call is forwarded.
- **Source IP address** - Defines the host IP address or Subnet, IP address and mask in CIDR format, of the calling party.

NOTICE:

IPv4 and IPv6 addresses are supported.

The Call Forward calls are redirected to the Branch IP, so the routing rules of the Branch will be used to determine the final destination of the call.

Recommendation - if System Call Forwarding is to be enabled in a Branch, all subscribers in that Branch shall be configured to use the same Voice Mail server.

In case of forward to external voicemail the Redirect Number should be configured with the corresponding match digit(s) of a gateway with the Gateway type parameter set to voicemail in the gateway table.

NOTICE:

It is the user's responsibility to avoid conflicts in re-routing.

NOTICE:

System Call Forward is not permitted for Proxy ATA mode.

6.5.14 Features > Call Detail Records

General

- **Billing File Settings**

- Maximum number of records - this defines the maximum number of CDR records stored in a single billing file.
- Maximum time interval (min) - this parameter defines the time when the billing files will be stored in the permanent storage device (FLASH memory or DISK)
- Maximum file size (kbytes) - this box is used to set the maximum size in kbytes of the billing file.
- Allow file overwrite - this checkbox enables or disables the cdr files overwrite, older files are overwritten if the checkbox is checked.

NOTICE:

The billing file will be stored in the /cdr folder.

- **SFTP Settings**

- Transfer method - this defines the method used to transfer the files to Billing Server. In Push mode Branch will send the billing files to the billing server. In Pull mode Branch stores the billing files and the billing server is responsible for retrieving the billing files via SFTP. Default value is Pull.
- Port - this parameter defines the port used for SFTP when accessing the remote billing server
- Re-attempt timer (min) - the amount of time in minutes Branch shall wait before re-attempting an SFTP transfer in push mode. Allowed min value=1, Allowed max value=1440 (1 day), Default value=5.

- **E.164 Translation**

If the E.164 translation checkbox is enabled, CDR tickets will generate the called number with modified digits that match with the dialed number prefix.

A new translation rule can be configured using the "Add" button and deleted using the "Delete" button.

- Matching digits - digits that are used to match with the starting digits of the called number.
- Translation - defines the digits that will be used to substitute "Matching Digits".

Primary Billing Server

- **Hostname** - The hostname or its IP address.

NOTICE:

Both IPv4 and IPv6 addresses are supported.

- **User name** - the user name for the account to access, e.g. root.
 - **Password** - the password for the account.
-

Secondary Billing Server

- **Hostname** - The hostname or its IP address.

NOTICE:

Both IPv4 and IPv6 addresses are supported.

-
- **User name** - the user name for the account to access, e.g. root.
 - **Password** - the password for the account..

6.6 Security

In this administrative area the user can configure the security parameters.

6.6.1 Security > General

Certificates

- **Shared secret files** - This button opens a new window where it is possible to configure the Shared Secret files.
- **Certificate management** - This button opens a new window where it is possible to choose and manage the TLS Certificates.

Administrator Accounts

Administrator Accounts can be created by pressing the **Add** button and the existing ones can be edited or deleted using the **Edit** and **Delete** buttons. Adding or editing launches the [Administrator Account](#) configuration window.

PKI Configuration

Public keys allow automatic access without passwords. Keys can be used for SSH access.

This feature allows external users logged into a Branch to execute scripts or other commands, without having to explicitly log into the OSB using a password.

This will be done by storing the external user's public key on the Branch.

The certificate files for the WEB server (hereafter called "https") interface can now be conveniently changed.

Once installed, it is possible to connect to the local GUI over https as this tells the server to establish a secure connection with the browser.

Once a secure connection is established, all web traffic between the web server and the web browser will be secure.

The certificate also authenticates the server to the browser avoiding identity theft.

- **Enable PKI** - This check box enables PKI usage.

- **PKI Configuration** - This button will open a window to add, delete and upgrade Keys for allowed users
-

Secure Web Management

- If the Secure web management flag is enabled, the Apache web server will only accept TLS connections. If the flag is disabled, Apache will also accept SSLv3.
-

Passwords

- To change a password, select a User name, enter the current password, enter the new password, confirm the new password and click the "Change" button.
 - To reset a password, select a user then click the "Reset" button. A confirmation window will commit the changes. This feature is only allowed for users root and administrator.
-

Digest Authentication

- **Digest Authentication** - When checked, indicates the configuration of Digest Authentication as part of the Security settings.
- **Server Quality of Protection (QoP)** - This is any combination of the options Auth, Auth-int. These options have the following meanings: Auth - authentication and Auth-int - authentication with message body integrity protection.
- **Nonce** - A numeric value in the range 0-1800 seconds. This means the nonce life in seconds. Default value is 300 seconds.
- **Max Retries** - A numeric value in the range 0-100 with a default value of 5. This determines the maximum number of times the OSB will permit a client to try to authenticate itself in a given session. The value of 0 means an infinite number of tries is permitted.

6.6.1.1 Security > General > Shared Secret Files

In this window it is possible to configure the Shared secret files.

- **Shared secret files** - This field lists all shared secret files loaded in the system. To delete a file, click on the file to select it and then click the "Delete" button. Shared secret files must have the .key file extension.
- **Upload Shared Secret File** - A new shared secret can be added by browsing to the applicable file and then clicking the "Upload" button.
- **Create New Shared Secret File** - A new shared secret file can be created by entering the name and then clicking the "Create" button.

6.6.1.2 Security > General > Certificate Management

System Certificate

System SIP over TLS certificate profile - This box selects the default certificate profile to be used for SIP TLS connections.

HTTPS certificate profile - Possible values: HTTPS System Default.

Certificate Profiles

This is the list of certificate profiles. A new certificate profile can be created by clicking the "Add" button and existing entries can be edited or deleted by first clicking on an entry to select it and then clicking the "Edit" or "Delete" button as appropriate.

The Proxy ATA, OSB 50, OSB 50i, and OSB 250 have an upper limit of 5 Certificate Profiles.

The OSB 500i, OSB 1000, and OSB 6000 have an upper limit of 10 Certificate Profiles.

Log entries will be written when creating, modifying and deleting certificate profiles. These logs are available in the System Log on the local GUI and written to the /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.
 - **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.

6.6.1.3 Security > General > Certificate Management > Certificate Profile

Certificate Profile Configuration

- **Certificate profile name** - Name of the certificate profile.
- **Certificate service** - Parameter used to indicate if the certificate profile service is SIP-TLS, HTTPS or VPN. Note: For the default profile, only SIP-TLS is allowed. In addition, this field cannot be changed once the profile is created.

- **Local client certificate file** - Local client certificate file is an optional field. This is used when establishing a TLS connection as a TLS client (only for Mutual Authentication). If the Local client certificate is not configured, the Local server certificate shall be used.
- **Local server certificate file** - Certificate file to be used when establishing a TLS connection as a 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.

Pressing the **Show** button near each certificate/CA file opens a screen with a view of the certificate parameters.

- **Subject**
- **Issuer**
- **Validity**
- **Fingerprints**

Select **OK** to temporarily store changes. Make your changes permanent by selecting **Apply Changes** on the **General** page.

Validation

- **Certificate validation** - Enables the validation of the CA chain and CA signature, Validity Period, and Critical Extensions.
- **Revocation status** - Enables the verification of revoked certificates according to the CRL of the CA.
- **Identity 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 for in a TLS connection. Valid values: 15 - 1440 minutes.
-

TLS version

- **TLS version** - Select the supported TLS version. The options are: TLSv1.0, TLSv1.1 and TLSv1.2.

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.

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.

6.6.1.4 Security > General > 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.
- **CRL issuer** - Issuer name loaded from the CRL.
- **CRL status** - Status of the CRL list (Removed, Installed, Expired, Downloading).
- **This update** - Date and time of the CRL update (loaded from the CRL).
- **Next update** - Date and time of next CRL update (loaded from the CRL).
- **Last CRL update** - Date and time of the last update.

6.6.1.5 Administrator Account

Administrator accounts configuration for the firewall /routing settings for the OSB.

Administrator Profile

- **Account enabled** - This flag is used to grant login rights (**SSH** and **Management Portal**) to users. Enabled by default.

IMPORTANT: The flag is disabled & grayed out for assistant & redundancy users.

- **User Name** - User name of the Administrator account.
- **Password** - The password for the Administrator account user name.

- **Confirm Password** - Confirm & verify the Administrator account user name password.
- **Privilege** - Administrative privileges. Possible values: Administrator, Network Administrator, Security Administrator, Network and Security Administrator, Read Only.
- **Expires (days)** - The password expiration timeslot. Possible values: 7 -99999.
- **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.
- **Change password in first login** - When adding a new user, the **Change Password in first login** is enabled by default, & 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 by providing the current and the new password.

6.6.1.6 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.
 - **Browse** - 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.
-

HTTPS PKI Configuration

The **HTTPS Profile** drop-down field allows you to select from a list of HTTPS profiles that have been created using the Certificate Management capability.

6.6.2 Security > Firewall Overview

This screen presents an overview of how the internal firewall has been configured for the LAN and WAN interfaces. The interface settings can be edited by first clicking on the relevant row in the table and then clicking the **Edit** button.

6.6.2.1 Security > Firewall > Firewall Configuration

General

NOTICE:

For established connections, blocking will not apply until those connections are considered closed, and the process for this to happen is protocol specific. However, if the machine is rebooted, all past connections are cleared so any new blocking rule takes places immediately.

NOTICE:

If the WAN interface is configured with an IPv6 address, the firewall for the WAN interface shall be configured with IPv6 addresses.

IMPORTANT: OpenScape Branch does not block outgoing packets as their respective responses. Firewall acts only in incoming packets (excepting the responses for OSB requests)

- **Enable IP masquerading** - IP masquerading will mask the LAN addresses in the WAN, this will hide the entire internal address space which will appear as a single IP address in another, often public address space.
This parameter is only applicable when configuring the WAN interface.
- **Enable port forwarding** - When checked, click the **Configure** button to set up the port forwarding details.
This parameter is only applicable when configuring the WAN interface.
- **Port Forwarding Configuration** - The button opens a new window where it is possible to configure Port forwarding. A new rule is added by clicking the **Add** button. In this case a new row is created in the table and it is possible

to configure the incoming port (In port) number, the outgoing IP (Out IP address) to be used, the outgoing port (Out port) number and the protocol.

To delete a rule first select it by clicking it and then click 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 the **Apply Changes** button.

NOTICE:

Port forwarding from IPv6 to IPv4 and from IPv4 to IPv6 and IP masquerading will not be supported this time. now. These parameters will not be presented for Proxy with IPv6.

- **Incoming Network Connections** - These settings are used 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 the Branch. The **Allow all network connections** flag will disable the firewall for these protocols.

Some services like Telnet and FTP are not provided by the Branch but firewall configuration is possible for cases where devices connected to the Branch LAN require those connections.

Blocking SIP or TLS will drop network packages coming from sources that are not configured in the system, and this includes the requests coming from subscribers. The IP range of subscribers must be added to the firewall white list.

Blocking RTP/sRTP will block requests for all ports configured for RTP/ RTCP (media) as consequence the voice path will not be established when these ports are blocked.

Blocking MGCP will block requests for the local media server so local announcements/media streaming and large conferences will not work with MGCP blocked.

- **Incoming VoIP Connections** - These settings are used to disable VoIP protocols from accessing the WAN interface.
- **White List** - Allow Incoming network connections for a specific IP/Port. If the Port field is empty, all ports will be allowed.

NOTICE:

The **White List** and **Black List** parameters accept both IPv4 and IPv6 addresses.

- **Black List** - Block Incoming network connections for a specific IP/Port. If the Port field is empty, all ports will be blocked.

NOTICE:

Message Rate Control (if enabled) will be restarted if the firewall rules are changed.

External Firewall

NOTICE:

This section applies to the WAN interface only.

- **External Firewall** - When checked, indicates the configuration of an external firewall for the selected interface.
- **SIP ALG** - When checked, indicates the setting SIP Application Level Gateway option.
- **Profile** - This is the profile designation for the external firewall being configured.
- **External IP Address** - This field is the external IP address identity of the external firewall.
- **Internal IP Address** - This field is the internal IP address identity of the external firewall.

6.6.3 Security > Message Rate Control

Message Rate Control Settings

Message Rate Control is a Network Intrusion Prevention System (NIPS) and Network Intrusion Detection System (NIDS), which performs packet logging and real-time traffic analysis on IP networks.

- **Enable Message Rate Control** - This checkbox 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.

Setting the Message Rate Threshold to the minimum value could cause RTP packages to be dropped, especially in Branch SBC installations.

- **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 the 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:

White List supports both IPv4 and IPv6 addresses.

6.6.4 Security > RADIUS

RADIUS Settings

- **Enable RADIUS** - This check box enables the RADIUS Server feature.
- **Address** - Two RADIUS Server IP addresses or FQDNs can be configured in the fields "Server 1" and "Server 2". Server 2 is not required. The use of an IP address is preferred over an FQDN.

NOTICE:

RADIUS supports both IPv4 and IPv6 addresses.

- **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. Note that the port number for RADIUS 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** - The '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** - Indicates how long the Branch will wait for a response from a Radius Server (1 - 10 seconds, 3 seconds recommended). A timeout of 1 or 2 seconds must be avoided in networks with high delays. In case of a timeout or other network problem then local authentication will be used.
- The check boxes **"Enable RADIUS Authentication"** and **"Enable RADIUS Accounting"** together with the check boxes **"WEB"**, **"CLI"** and **"SSH"** can be used to select which services 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).

NOTICE:

When RADIUS is enabled, the Authentication service or Accounting service (or both) must be selected and, for each selected service, at least one application must be enabled.

6.6.5 Security > Tunnel Connections

VPN

To create a new VPN tunnel, click the "Add" button. To delete a VPN 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 VPN connection name. A unique name should be used for each connection.
- **Partner** - This box defines the partner. It can be a remote IP address or a remote name.
- **Routing** - This box adds a route (partner network) to routing table after connection is established.
- **Routing mask** - This box defines the mask for the route.
- **Local IP** - This box defines the local IP address for the VPN connection.
- **Remote IP** - This box defines the remote IP address (partner) for the VPN connection.
- **Port** - This box defines the port used for the VPN connection. Each connection must use a different port.
- **Auth type** - This box defines the type of authentication.
- **Secret key file** - This box defines the shared secret key file for the connection, when the type of authentication is defined as secret.
- **Certificate profile** - This box defines the certificate profile for the VPN connection. It must be configured only when X.509 certificates are used.
- **Enable LZO compression** - This flag enables the LZO real-time compression algorithm in VPN connections. With LZO the data is compressed in an adaptive manner. In other words, compression only occurs when the data on the VPN really can be compressed.

VPN configuration applies only when the WAN interface is enabled.

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.

6.6.6 Security > Denial of Service Mitigation

Dynamic Blacklist

- **Block unauthorized users** - if enabled, upon receiving a “401 unauthorized” response from the OSV, the response is forwarded to the SIP UA. If three (fixed) successive failure attempts occur it is flagged as an “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. This checkbox is disabled by default.

IMPORTANT:

The **Block unauthorized users** only applies for subscribers connected to the WAN which is only possible if WAN is configured to IPV6 and LAN to IPV4 or vice-versa.

- **Unauthorized user quarantine interval (sec)** - Default value is 300 seconds; integer with range 60-36000.
- **Block unknown users** - if enabled, upon receiving a “404 Not Found” response from OSV to a SIP REGISTER message, a “403 Forbidden” response is returned to the offending endpoint instead of forwarding the “404 Not Found” response. This checkbox is disabled by default.

IMPORTANT:

The **Block unknown users** only applies for subscribers connected to the WAN which is only possible if WAN is configured to IPV6 and LAN to IPV4 or vice-versa.

- **Unknown user quarantine interval (sec)** - Default value is 300 seconds; integer with range 60-36000.
- **Subscriber garbage collector** - Default value is 300 seconds; integer with range 60-90000.

IMPORTANT:

The **Subscriber garbage collector** only applies for subscribers connected to the WAN which is only possible if WAN is configured to IPV6 and LAN to IPV4 or vice-versa.

- **Subscriber garbage collector interval (sec)** - Default is 60 seconds; integer with range 30-120.
- **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

- **Minimal (sec)** - default is 60 seconds; integer of range 60-3600.

- **Medium (sec)** - 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 List Allowed

// text to be added //

6.7 Diagnostics and Logs

The Diagnostics and Logs screen allows you to:

- View the log files of various system processes.
- Activate debugging tools and view or export their output.
- Set up parameters for controlling continuous and on-demand tracing.
- View statistics for the Media Server and SIP Server, as well as to view the change history of the system.

6.7.1 Diagnostics and Logs > Logs

Log Viewer

The Log data drop-down box allows the user to select which application to retrieve the log for. After selecting the log to be viewed, click the **Show** button to view the log in a new window. The **Clear** button is used to clear the log file that is selected in the **Log data** field. Note that the **Log Settings** section allows the user to choose how much information to capture in a log.

While viewing a log, it is possible to clear the file, export it to a local file, or close the window. See the Note below for details regarding log files that cannot be cleared.

Possible choices for log data viewing are:

- **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.
- **B2BUA** – B2BUA is an Asterisk running in the system. It has three main functions: work as a B2BUA for gateways and SSPs in Survivability Mode; provide some functionalities like ACD, Auto Attendant, MLHG and Voicemail; provide the Integrated Gateway functionality for PRI, BRI, FXS and FXO boards. This log is useful for debugging all these functions, regarding the Integrated Gateway it is necessary to investigate call processing, DTMF detection, FAX T.38, voice quality issues, etc.
- **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.

- **CAS FMC R2** – Log of the CAS MFC R2 signaling. This signaling is applicable only for E1 interface. This log is useful to debug all CAS MFC R2 call establishment and features issues.
- **CAS E&M/Ring Down** – Log of the CAS E&M/Ring Down signaling. This signaling is applicable for both T1 and E1 interfaces. This log is useful to debug all CAS E&M/Ring Down call establishment issues
- **CDR** – Logs from Call Detail Recording that is the application that records in a ticket the information regarding caller, called parties call duration etc., for a call that was done during the survivable mode. The tickets are internally stored until the external server retrieved them.
- **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 Branch.
- **DAHDI** – Log of the DAHDI driver. Applies to the OSB 50i and OSB 500i only. This log is useful to debug problem in the PRI, BRI, FXS and FXO ports alarms. It is also useful to debug FXO and FXS signaling, along with B2BUA logs.
- **Firewall & Msg Rate Control** – This log contains the details of packets that are blocked by the Firewall and Msg Rate control.
- **ISDN** – Log of the ISDN Layer 2 and Layer 3 ISDN messages (BRI and PRI ports). This log is also included in the B2BUA logs when set to level INFO or DEBUG. Level INFO includes Layer 3 messages and it is useful to debug call processing issues, along with B2BUA logs. Level DEBUG includes Layer 3 and Layer 2 messages. This level is very verbose and must only be activated to debug Layer 2 issues, like link establishment and BRI PTMP issues.
- **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.
- **Phone Software Management** – These are the logs from Phone Software Management application that is used to store, control and allow the upload and download of Phone software images.
- **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.
- **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.
- **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 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.
- **Survivability Provider** – Log of the Survivability provider application. This application is responsible for the OPTIONS heartbeat functionality, that indicates the system operational mode (SM, NM, etc.). This application is also responsible for SSP registration and BCF Notifications functionalities.
- **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.
- **Denial of service**-The log will show hosts that sent DoS messages and are blocked by the system.
- **Symptom Collector**-This log contains the logs of the process used to send high priority logs direct to another server in the network. Useful only when kernel logs and very low level errors must be checked.

The "Show" button opens a new window or tab to present the log information.

The "Clear" button clears the selected log file. The "Alarm History", "Boot", "Current processes" and "Web Server" logs cannot be cleared.

The "Clear All Logs" button clears all logs, except for "Alarm History", "Boot", "Current processes" and "Web Server".

NOTICE:

The "Alarm History", "Boot", "Current processes" and "Web Server" logs cannot be cleared.

NOTICE:

From V10R2, the BLC and BLS have been removed.

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.

NOTICE:

Syslog Server supports both IPv4 and IPv6 addresses.

- **Log Levels**

- 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 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.

NOTICE: Setting the log level to Debug, Info, Notice or Warning may affect the system performance and will generate several log files. In addition, some features may not work properly, such as Media Server conferencing and announcements.

The user can set the log level for each application individually. The levels are defined as follows:

- For ISDN only, two levels are available: INFO (Q931) which is ISDN layer 3 messages, and DEBUG (Q931+Q921), which will enable the logging of layer 2 and layer 3 ISDN message.
 - MF Trace reports the MFC tones that are sent or received.
 - Trace reports the line signaling.
 - Stack reports the stack messages.
 - All reports all log levels.
 - None does not report any message.
 - Error, warning, notice and debug are the same as above.
- **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:

- 1) Add a start line with the text of the **Signature Key** box.
- 2) Remove the last line with the MD5 result.
- 3) Calculate the MD5 of the result file: it must be equal to the last line removed.

Fallback

- **Fallback to default log level** - If changes have been made to the log level of one or more applications, and the changes need to be reverted back by a certain time, then this checkbox must be checked and the Fallback time must be specified.
- **Fallback time (hh:mm)** - The time of day when the Branch resets the trace configuration back to its default values.

6.7.2 Diagnostics and Logs > Debugging

Debugging Tools

- **Tool** - This drop-down list selects the tool to be used: ICMP will start ping, Traceroute shows the hops from origin to the given destination, and Network Tracer captures and decodes IP packages to/from the network.
- **Options** - ICMP and Traceroute can have their own options entered in the "Options" box. In these cases 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.

NOTICE:

IPv4 and IPv6 addresses are supported.

- **Interface** - For the Network Tracer, there is a drop-down list that allows the user to select the interface:
 - All Interfaces
 - SIP/MGCP/Q931 Trace
 - SIP/MGCP/Q931/InterworkingRTP Trace

NOTICE:

The number of interfaces presented is dependent on how the Branch is configured.

NOTICE: All Interfaces - The network trace capture (wireshark) may not be able to capture all network packets in all traffic load conditions. This is a limitation on the Wireshark application.

The SIP/MGCP/Q931 trace option is used to capture a network trace at the application level. (SIP and MGCP protocols are shown as UDP messages. Q931 is shown as TCP and is only applicable for the Integrated Gateway.)

- The original protocol information is stored in the TTL field (time to live) of the IP header. The new meanings of the TTL field are:
 - UDP = 101 (decimal number)
 - TCP = 102
 - TLS = 103

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 an input field where the user enters the capture maximum file size. In case the maximum size is reached the file starts to rewrite itself starting from the first entries. The range for this field is 1MB to 100MB.

- **Debug tool buttons**

- The "Start" button is used to execute the tool operation.
- The operation is stopped by clicking the "Stop" button.
- For ICMP and Traceroute the results can be seen in a new window by clicking on the "View" button or by exporting the data using the "Export" button.
- To get the Network Tracer results use the "Export" button.

Rapid Stat

Rapid Stat is a tool that collects system information in order to aid with 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 the integrated gateway HW types.

NOTICE:

In level 5, due to the amount of information collected, Rapid Stat file generation can take several minutes.

6.7.3 Diagnostics and Logs > Trace

Continuous Tracing and On Demand tracing are supported.

Continuous Tracing

- **Enable** - Flag used to enable Continuous Tracing.
- **IP address** - IP address of the Trace Manager server.

NOTICE:

Trace Manager supports both IPv4 and IPv6 addresses.

- **System name** - The System name configured on the Trace Manager server.

- Log and trace files are stored in the Trace Manager server "`\Tracedata\<System Hostname>\OpenBranch`" directory. The "`\Tracedata\`" directory must be the home directory of the SFTP user.
 - **File size threshold (kbytes) / Time interval threshold (mins)** - The log/trace files are sent to Trace Manager 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 has elapsed (valid values are between 1 and 60 mins).

The polling time is about 10 seconds, so file sizes may vary if the amount of log data is increasing quickly.
 - **SFTP username/password** - Login information used to connect to the SFTP server on the Trace Manager server.
 - **SIP/Q931 trace** - Flag used to enable the SIP/Q931 trace capture.
 - **MGCP trace** - Flag used to enable the MGCP trace capture.
-

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 previous configuration. The Continuous Tracing file size and time parameters still control when files are sent (via SFTP).

The "Start" button is used to execute the tool operation. The operation can be stopped using the "Stop" button.

- **Log type** - Selects the application for which 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. The time range is from 1 to 1440 minutes, with the default being 5 minutes.

6.7.4 Diagnostics and Logs > Statistics

View statistics for the Media Server and SIP Server.

Media Server

- Total number of ports used - the total number of ports opened by the Media Server.
- Current conference port usage - the number of ports currently opened by the Media Server for conferencing.
- Current port usage - the number of ports currently opened by the Media Server.

SIP

- Active dialogs - the number of currently active SIP dialogs.
- Requests out - represents the number of SIP requests sent since the SIP Server started.

- Requests in - represents the number of SIP requests received since the SIP Server started.
- Responses out - represents the number of SIP responses sent since the SIP Server started.
- Responses in - represents the number of SIP responses received since the SIP Server started.

6.8 Alarms

In this administration area the user can configure the alarms / SNMP traps.

6.8.1 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 describes 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.

6.8.2 Alarms > SNMP Configuration

A new SNMP trap configuration is created by clicking the **Add** button. The SNMP details can be configured in the corresponding row in the table. A Trap is deleted from the table by first clicking on the relevant row to select it, and then clicking the **Delete** button. You are able to configure up to 5 SNMP v2c and SNMP v3 trap destinations for the OSB.

General

- **SNMP v2c Read-Only Community Name** - Enter the community name. The length of the field must not exceed 32 characters, with a minimum length of 1. The setting must be stored in the system XML file. The Community Name is used for the discovery process per network manager. The content of this parameter shall not be presented for users which are not in the same group as the root user, e.g. the guest user is not in the same group as the root user.
- **SNMP v2c Read-Only IP** - IP address (supports both IPv4 and IPv6)

SNMP v2c Trap Destinations

- **IP address**- The IP Address and Port identify the unique key for the table. The user must be allowed to enter multiple rows in the table with the same IP address so long as the port number is different for each row.

NOTICE:

The **SNMP v2c Trap Destinations** field accepts both IPv4 and IPv6 addresses.

- **Port** - The IP Address and Port identify the unique key for the table. The user must be allowed to enter multiple rows in the table with the same IP address so long as the port number is different for each row.
- **Community Name** - This is a required field when an IP address and port have been entered. The content of this parameter shall not be presented for users which are not in the same group as the root user, e.g. the guest user is not in the same group as the root user. The name must have a minimum of 6 and a maximum of 32 characters.
- **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. P address.
- **Type** - The default for this field when a new row is added to the table is "Alarm". The field must be disabled.

SNMP v3 EngineID Configuration

- **Current SNMP Engine ID**- Display only field.

- **Generate automatically**- 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. The IP Address and Port identify the unique key for the table. You are allowed to enter multiple rows in the table with the same IP address so long as the port number is different for each row.
- **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 checked, the drop-down box next to it must be enabled, otherwise the drop-down box is disabled. The drop-down box must offer the list of available NIC ports on the system. The default value is "eth0". Notice that only the active NIC ports are offered.
- **Text entry (max 27 chars)** - When checked, the text entry field next to it must be enabled, otherwise the text entry field must be disabled. You 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 checked the text entry field next to it must be enabled, otherwise the text entry field must be disabled. You may enter a regular hex string, up to a maximum of 27 bytes. The default for this field is an empty string. You may 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 accepted.

SNMP v3 GET Configuration

- **Enable** - This checkbox allows the snmp v3 gets of linux default MIB. It is disabled by default.
- **Read-Only user name** - User configuration.
Min: 6 characters & max: 32 characters. Default value: `snmpv3user`
- **Security level** - Default value: `authPriv` (hardcoded - grayed out)
- **Auth protocol** - Default value: `SHA-1` (hardcoded - grayed out)
- **Auth password** - At least 8 characters must be entered, with a maximum of 32. Default value: `snmpv3authPass`
- **Priv protocol** - Default value: `AES` (hardcoded - grayed out).
- **Priv password** - At least 8 characters must be entered, with a maximum of 32. Default value: `snmpv3encPass`

You must click **OK** and then **Apply Changes** for changes to take effect.

SNMP v3 Trap Destinations

- **IP address**- The IP address of the far-end system to which traps are to be sent.

NOTICE:

The **SNMP v3 Trap Destinations** field accepts both IPv4 and IPv6 addresses.

- **Port** - 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** - This is the equivalent of the v2c Community Name. A text field. Duplicate entries in this column are permitted. This is a required field when an IP address and port have been entered.
- **Security Level** - This is a required field when an IP address and port have been entered. This field is a drop-down box offering 3 choices:
 - 1) **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.
 - 2) **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.
 - 3) **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 box offering 2 choices: "SHA-1" or "MD5" in that order. 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 you select "MD5", a pop-up message shall appear that says: "Note that the MD5 protocol has been deprecated and is not recommended for use." There must be an "OK" button to dismiss the message.
- **Auth password** - When creating a new row in the table, you enter the password in clear text. At least 8 characters must be entered, with a maximum of 32. Once the changes have been applied, this field must display the password as a sequence of mask characters (typically the bullet symbol). This is a required field when "Security Level" is set to "Auth Only" or "Auth+Priv".
- **Priv protocol** - This field is a drop-down box offering 2 choices: "AES" or "DES" in that order. The default value for a new record in the table is an empty string. You must select "AES" or "DES" when "Security Level" is set to "Auth+Priv". If you select "DES", a pop-up message shall appear that says: "Note that the DES protocol has been deprecated and is not recommended for use.". There must be an "OK" button to dismiss the message.
- **Priv password** - When creating a new row in the table, you enter the password in clear text. At least 8 characters must be entered, with a maximum of 32. Once the changes have been applied, this field must display the password as a sequence of mask characters (typically the bullet symbol). 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". The field must be disabled.

You must click **OK** and then **Apply Changes** for changes to take effect.

6.9 Maintenance

In this administrative area the user can change system configuration by loading or importing an XML configuration file, backup the system configuration by exporting a single XML configuration file or export all XML configuration files as a tar file (latest 10 files), or install the system using install, upgrade or update procedures.

The user can also proceed with bulk configurations (Delta XML) of OSB, configuration queries and configuration comparisons.

IMPORTANT: The maximum number of XML configuration files stored on your system is 100. In case this amount exceeds 100, the older files will be deleted until the compact flash is full with 100 files.

6.9.1 Maintenance > Import/Export

This screen allows the user to import (upload) new configuration files, re-load existing configuration files, or export configuration files as part of a backup strategy, as well as importing and exporting files / configuration components that have been customized by the user. The importing of legacy files is also supported.

IMPORTANT: The maximum number of XML configuration files stored on your system is 100. In case this amount exceeds 100, the older files will be deleted until the compact flash is full with 100 files.

- **Configuration file in use** - This is a read-only field that shows which system configuration file is in use on the Branch.

Load

- **Select a Configuration file** - Choose which file to load. The drop-down box lists all .xml and .psw files. The sort order of the drop-down list is descending, showing the latest available .xml file at the top of the list.

The default selection on opening the screen must be the latest available .xml file.

- **Load** - The Load function allows the user to choose a "config....xml" file that is already on the OSB disk drive and then make it the current configuration for the OSB by loading it. This action typically requires a restart of the OSB.

NOTICE:

The Load function can also be used for .psw files. The .psw file must be at the bottom of the list.

Import

The **Import** function allows the user to import (upload) a previously exported .xml file to the OSB from a location on the user's disk drive. The imported file will be immediately loaded into the OSB memory. This action typically requires a restart of the OSB.

NOTICE:

NOTICE: The **Import** function can also be used for .psw files. The .psw file must be at the bottom of the list.

- **Select an exported file** - An exported file is selected for importing.

Three legacy file types are supported for importing:

- 1) .xml: These files are single copies of the system configuration XML file.
- 2) .psw: These files contain all of the user passwords for the OSB.
- 3) .tar: These files are containers for multiple XML files and any custom DHCP or custom DNS files. The .tar file was created using the legacy **Export all** button.

A legacy tar file has the following format:

- .xml files are in the root folder
- There is a "custom" folder, where there is a "dhcp" folder, a "dhcp" folder & the "dhcp" and "dns" folders contain the custom DHCP and custom DNS files.
- **Browse** - Clicking the 'Browse...' button will bring up a standard file browser dialog box.
- **Upload** - Select a valid configuration file on their local computer or network, then click the "Upload" button to upload the file to the Branch. The configuration will be loaded to the Branch and the page will be reloaded.
- **Select file group(s) to import** - Select groups of files to export by setting the checkboxes.
 - Branding
 - Configuration
 - Custom DHCP
 - Custom DNS
 - License
 - Local Toll Table
 - Media (AA/ACD)
 - Media Server Languages
 - Packet Filter Rules
 - Passwords
 - Security certificates and keys
 - XML
- **Select individual file(s) to import** - When a legacy .tar file is detected, the "File Group" checkboxes will all be disabled, and you will see the files contained in the .tar file in the right-hand side of the Import section on the GUI. You can then select which files to import using individual file/folder

checkboxes and click "Import Selected", or they can click "Import All" to import all files in the .tar file.

- **Import Selected** - Choose to import the selected file.
- **Import All** - Choose to import all files that are contained in the .tar file being imported. Any file(s) being imported will overwrite existing files of the same name.

Export

- **Select file group(s) to export** - Select groups of files to export by setting the checkboxes. File groups cannot be exported if a single XML file is being exported. File groups will be combined into a single tar file, except if only **Passwords** is selected, in which case the file will be of .psw type. If File group **XML** is selected for export, only .xml files will be exported. Zipped compressed .xml files will not be part of the export.

The format of the .tar file :

- No files will be stored in the root folder
- Branding
- Configuration
- Custom DHCP
- Custom DNS
- License
- Local Toll Table
- Media
- Media Server Languages
- Packet Filter Rules
- Passwords
- Security certificates and keys
- XML

Folders only need to be created for the File groups that are being exported

- **Select individual file(s) to export** - T
- **Single XML File** - Select a single system configuration XML file. When this option is selected, all File group checkboxes will be disabled. The output file will have a .xml file extension.
- **Export Selected** - Clicking this button will export the selected file to a location of your choosing. It is your choice whether to save or open the file. Clicking "Cancel" closes the screen with no changes.
- **Export all** - Clicking this button creates a tar file with the last 10 XML configuration files. It is your choice whether to save or open the file. Clicking "Cancel" closes the screen with no changes.

Change History

- **Last configuration time** - This field indicates the last date and time when the Branch configuration was changed.
- **User** - This field indicates which user made the last change.
- **User IP address** - This field indicates the IP address of the user who made the last change

- **Show last changes** - Clicking this button brings up a new screen that shows the differences between the current configuration and the prior configuration. Differences are highlighted in yellow and they can be quickly located and navigated by clicking the "<< Prev diff" and "Next diff >>" buttons.
- **Compare with previous version** - By selecting a previous system configuration file, the user can compare it with the immediately preceding version. As with the "Show last changes" button, differences are highlighted in yellow and they can be quickly located and navigated by clicking the "<< Prev diff" and "Next diff >>" buttons.

6.9.2 Maintenance > Install/Upgrade

The user can install a system from a USB stick, or upgrade a system from various source locations. In the latter case, the upgrade load is stored on the backup partition and the old load is then preserved in case fallback is required.

Installation

By clicking the "Install" button, the user can perform a full installation. The installation erases both the backup and the active partitions and overwrites them with the new software that is on the USB stick. The database can be preserved if it was previously stored on the USB stick.

This option is only available if the USB stick is plugged in and the system is booting from the USB stick.

Upgrade

Clicking the "Upgrade" button means that a full version will be installed on the backup partition and the active partition will be preserved in case of failure.

Upgrade is possible using a USB stick, local files stored on a PC, over an HTTPS link, or via an SFTP link.

When using a USB stick, the version stored on the stick will become the new active partition. When upgrading from local files, the user chooses which files to upload, depending on the version desired. For the other methods (HTTPS and SFTP), the user has to fill in the access authorization credentials and then click the "List Versions" button to select from the Software version available to use.

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.

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.

6.9.3 Maintenance > Bulk Configuration (Delta XML)

The Delta XML Feature targets the support of bulk configurations of OSBs.

The user is able to use for individual configurations of OSBs and for bulk configuration the same set of GUI's residing locally in the OSB.

One OSB system, preferably the same type (e.g. 50iD44, ...), will be 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 OSBs will take the Delta file and merge, after checking the Version, OSB 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 will be 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 as Master chosen OSB.

- 1) In the first step mark the fields to be changed in the regular GUI against the currently used XML file, either with the already valid entry or just to mark it. After pushing the **Create Diff** button the diff between the currently used XML file and the changes will be presented in the GUI.
- 2) In the second step the deltas can be fine tuned and if accepted the changes will be verified and the Delta file will be created. By pressing the **Upload** button the Delta file will be 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 with **Browse** and press **Upload**. **Apply Changes** is used to activate the changes.

NOTICE:

Before **Apply Changes** it is possible to see the changes 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 at once

Edit Delta XML

- **Please Validate Configuration Before Edition**- Clicking this button will validate the selected configuration file.

If successful, the new configuration will be kept and a positive response file will be send to the SFTP server to complete the process.

If applying is not successful the OSB falls back to the previous configuration and negative response file will be send to the SFTP server to complete the process.

NOTICE:

Changes done on configuration after validating will only be detected when reloading the **Bulk Configuration (Delta XML)** tab

- **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 the <<**Prev diff** ,**Current diff** and **Next diff** >> buttons.
- **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 the <<**Prev diff** ,**Current diff** and **Next diff** >> buttons
- **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 shall turn green. The exported Delta XML, when applied, will replace 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 check box is unmarked.

- **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 following is shown: " **Accept/Drop operation will be applied to all diffs. Please review the accepted changes before exporting**"

- **Validate Accepted Changes**- When pressed, **Validate Accepted Changes** is replaced by the **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** will not be possible. CMP demands `deltaXml.xml` as the name of the Delta XML file, other name will be ignored.

6.9.4 Maintenance > Restart

- **Restart** - This button is used to reboot the system. The user will be prompted to confirm the system restart.
- **Restart to backup** - This button is used to reboot the system and use the software stored in the backup partition.
- **File system repair** - This button calls the check and repair tool for all disk drives in the Branch. All problems found are automatically fixed.
- This option is only available if the USB stick is plugged in and the system is booting from the USB stick.

6.9.5 Scheduled Maintenance

If the Google Cloud Load Balancer is used, it is possible to select the maintenance date or set the system as maintenance state immediately, under **Scheduled Maintenance**. Once you apply the maintenance configuration by selecting the options **Auto**, **Now** or **Schedule**, a warning pop-up will inform that some essential services will be disabled and the system will not be able to make calls.

Maintenance Schedule Options

- **Maintenance State**

It is the current state of the server and the text inside the () describe how the server enter in this state. Available options:

- **out of service (auto)**: operated by the server itself
- **forced**: operated by an administrator
- **schedule**: operated an administrator using a define date and time period

- **System in maintenance**

Select what type of maintenance state will be applied when the button **Apply** button is pressed. Available options:

- **Auto**: The **Auto** mode will only use the server software decisions to control if the server is in maintenance.
- **Now**: The **Now** option will force the server to enter in maintenance at once.
- **Schedule**: the **Schedule** option will use the time in the boxes below to select when the server will enter in maintenance.

NOTICE:

The server can enter in maintenance state even before the date and time defined if the server thinks that it the right decision.

- **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 it 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.

7 OpenScape Branch CDR Overview

7.1 OSB CDR File Structure

OSB CDR File Structure

OSB CDR File Structure	
TAG	Description
FILENAME:	The FILENAME tag is used to identify the name of the file when it was created. (An adjunct processor may have subsequently changed the file).
DEVICE:	The DEVICE tag identifies the device that created the file.
HOSTNAME:	The HOSTNAME tag identifies the configured IP Hostname of the device that created the file.
FILETYPE:	The FILETYPE tag identifies the type of file (Call Records).
VERSION:	The VERSION tag specifies the version of the file format, enabling future enhancements to the file format.
<NL>	An extra new line is inserted.
CREATE:	The CREATE tag is used to indicate the start of the call record information and additionally specifies the date / time stamp when the file was initially created (unless changed, it should mirror the date / time stamp in the file name).
<NL>	An extra new line is inserted.
RECORD:	Individual Data Records numbered sequentially and ending with a new line <NL> are located between the CREATE and CLOSE tags. Each record is composed of number of fields in an ASCII comma delimited format.
<NL>	An extra new line is inserted.
CLOSE:	The CLOSE tag is used to indicate the end of the call record information and additionally specifies the date / time stamp when the file was closed.

OSB CDR File Structure
FILENAME: /cdr/OSBIP169-20111108T090005+0500000004.bf --> Name/Path of CDR record
DEVICE: OpenScape Branch --> Device Type
HOSTNAME: OSBIP169 --> Configured OSB Hostname
FILETYPE: CALL RECORDS --> CDR file
VERSION: V2R0.06.00 --> SW version running on Active Partition
CREATE: 2011-11-08T09:00:05+0500 --> File Creation Date
0,Std,OSBIP169,607b4e345ae75cd,10,5558885226,5558885256,orig,term,,,,,10.234.1.70,10.234.1.101,2011-08-11T08:58:01.0+0500,2011-08-11T08:58:04.0+0500,5256,200,OK,,0, 0x010104
CLOSE: 2011-11-08T09:00:05+0500 --> File Close Date

7.2 OSB CDR Record Structure

OSB CDR Record Structure

OSB CDR Structure		
0,Std,OSBIP169,607b4e345ae75cd,10,5558885226,5558885256,orig,term,,,,,10.234.1.70,10.234.1.101,2011-08-11T08:58:01.0+0500,2011-08-11T08:58:04.0+0500,5256,200,OK,,0, 0x010104		
Field Number	Name/Description	From Example Above
1	Sequence Number: written CDR+1. ex. 1, 2, 3 ... etc	0
2	CDR type (standard Or half-call release record).	Std
3	OSB ID: Hostname of the Branch.	OSBIP169
4	SIP Call ID.	607b4e345ae75cd
5	Call Duration in Seconds.	10
6	Calling party number.	5558885226
7	Called party number	5558885256
8	Calling party identifier (orig, term, inc, outg, unknown)	orig

9	Called party identifier (orig, term, inc, outg, unknown)	term
10	Transferring party number	
11	Forwarding party number	
12	MLHG member number	
13	Location Identification Number	
14	IP or FQDN Ingress side address	10.234.1.70
15	IP or FQDN Egress side address	10.234.1.101
16	Answer time UTC format:	2011-08-11T08:58:01.0+0500 Note: The "time portion" of a timestamp is in 24-hour format and represents the local time at the OSB. The addition or subtraction of the offset yields a final time calculated in UTC.
17	Release time UTC format:	2011-08-11T08:58:04.0+0500 Note: The "time portion" of a timestamp is in 24-hour format and represents the local time at the OSB. The addition or subtraction of the offset yields a final time calculated in UTC.
18	Original Dialed Digits	5256
19	SIP response Status Code 1xx, 2xx, 3xx, 4xx, 5xx, 6xx	200
20	SIP response Reason Phrase ex. OK, Busy here, etc	OK
21	PSTN Gateway Side - Codec Used	
22	Secure RTP Indicator (0,1)	0

23	Integrated GW only. -> 0xaabbcc	0x010104
	Where:	
	aa - slot position - 01	
	bb - port - 01	
	cc - channel - 04	

7.3 OSB CDR Field Structure

OSB CDR Field Structure

No.	Field Data Type Description		
Field Number	Name/Description	Data Type	Description
1	Sequence Number:	INT	
2	CDR type (standard Or half-call release record).	ENUM	CDR Record type (Values: std Or half-call release record)
3	OSB ID: Hostname of the Branch.	STRING	Hostname of the Branch.
4	SIP Call ID.		
5	Call Duration in Seconds.	INT	
6	Calling party number.	DIGITS	This field displays a string of up to 20 characters that associates the initiator of a call.
7	Called party number	DIGITS	This field displays a string of up to 20 characters that associates the called party number.
8	Calling party identifier	STRING	Calling party identifier - (Values : orig, term, inc, outg, unknown)
9	Called party identifier	STRING	Called party identifier - (Values : orig, term, inc, outg, unknown)

10	Transferring party number	DIGITS	This field displays a string of up to 20 characters that associates the transferring party number.
11	Forwarding party number	DIGITS	This field displays a string of up to 20 characters that associates the forwarding party number.
12	MLHG member number	DIGITS	
13	Location Identification Number		
14	IP or FQDN Ingress side address		
15	IP or FQDN Egress side address		
16	Answer time UTC format	DATE	This data type is an 26 long ASCII string representing a date and time stamp. DATE has the format described in FDD052 and which is reproduced here for convenience: YYYY-DD-MMThh:mm:ss.s/+HHMM Note: The "time portion" of a timestamp is in 24-hour format and represents the local time at the OSB. The addition or subtraction of the offset yields a final time calculated in UTC.

17	Release time UTC format	DATE	This data type is an 26 long ASCII string representing a date and time stamp. DATE has the format described in FDD052 and which is reproduced here for convenience: YYYY-DD-MMThh:mm:ss.s/+HHMM Note: The "time portion" of a timestamp is in 24-hour format and represents the local time at the OSB. The addition or subtraction of the offset yields a final time calculated in UTC.
18	Original Dialed Digits		
19	SIP response Status Code 1xx, 2xx, 3xx, 4xx, 5xx, 6xx		
20	SIP response Reason Phrase ex. OK, Busy here, etc		
21	PSTN Gateway Side - Codec Used		
22	Secure RTP Indicator (0,1)		
23	Integrated GW only. - > 0xaabbcc		
	Where:		
	aa - slot position - 01		
	bb - port - 01		
	cc - channel - 04		

8 Appendix - Overview

The information in this section provides additional information for Maintenance and Configuration.

8.1 Alarm Information - Overview

The Alarms Information details section provides additional information on specific alarms for OpenScape Branch.

Alarm information includes but is not limited to the following:

- Alarm List
- Descriptions
- Maintenance Procedure
- Alarm Group
- Severity

8.1.1 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.

8.1.2 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.

8.1.3 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

8.1.4 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.

8.1.5 Alarm Groups

Each alarm is mapped to an alarm group. The 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

8.1.5.1 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 verification
- Installation failure (media, ACD, Attendant servers)

8.1.5.2 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)

8.1.5.3 Alarm Group: Ethernet

An Ethernet port becomes unavailable is reported as an Ethernet alarm.

8.1.5.4 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)

8.1.5.5 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

8.1.5.6 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

8.1.5.7 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

8.1.5.8 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

8.1.6 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.

8.1.6.1 +1.5V high voltage

+1.5V high voltage.

Associated Device: OSB, SBC

Group Name: Hardware:

Severity: critical

Default Threshold: x3250: 1.650;

Faulty Object: HW-Sensors

Maintenance Procedure:

8.1.6.2 +1.5V low voltage

+1.5V low voltage.

Associated Device: OSB, SBC

Group Name: Hardware:

Severity: critical

Default Threshold: x3250: 1.350;

Faulty Object: HW-Sensors

Maintenance Procedure:

8.1.6.3 +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;

Faulty Object: HW-Sensors

Maintenance Procedure:

8.1.6.4 +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;

Faulty Object: HW-Sensors

Maintenance Procedure:

8.1.6.5 +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;

Faulty Object: HW-Sensors

Maintenance Procedure:

8.1.6.6 +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;

Faulty Object: HW-Sensors

Maintenance Procedure:

8.1.6.7 +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;

Faulty Object: HW-Sensors

Maintenance Procedure:

8.1.6.8 +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;

Faulty Object: HW-Sensors

Maintenance Procedure:

8.1.6.9 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;

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.

8.1.6.10 B2BUA not running

B2BUA 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;

Faulty Object: B2BUA

Maintenance Procedure: Process Manager has a mechanism to restart automatically the applications that are not running. If the B2BUA is still not running after several restarts by PM check the b2bua logs to see the root cause. As last resource proceed to a restart to backup.

8.1.6.11 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;

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 observed then Message Rate Control functionality should be enabled. Otherwise a network assessment is recommended.

8.1.6.12 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;

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 observed then Message Rate Control functionality should be enabled. Otherwise a network assessment is recommended.

8.1.6.13 Bandwidth ethernet port 3

Bandwidth ethernet port 3

Associated Device: OSB, SBC

Group Name: Resource

Severity: major

Default Threshold: rx200: 90; x3250: 90; x3550: 90;

Faulty Object: Resource

Maintenance Procedure: Flooding TCP/IP packages on Ethernet port 3, this could indicate an excessive traffic of SIP/MGCP messages or an attack. If a kind of attack is being observed then SNORT functionality should be enabled. Otherwise a network assessment is recommended.

8.1.6.14 Bandwidth ethernet port 4

Bandwidth ethernet port 4

Associated Device: OSB, SBC

Group Name: Resource

Severity: major

Default Threshold: rx200: 90; x3250: 90; x3550: 90;

Faulty Object: Resource

Maintenance Procedure: Flooding TCP/IP packages on Ethernet port 3, this could indicate an excessive traffic of SIP/MGCP messages or an attack. If a kind of attack is being observed then SNORT functionality should be enabled. Otherwise a network assessment is recommended.

8.1.6.15 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;

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.

8.1.6.16 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;

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.

8.1.6.17 Snort not running

Snort 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: Snort

Maintenance Procedure: Process Manager has a mechanism to restart automatically the applications that are not running. If the Snort is still not running after several restarts by PM check the Snort logs to see the root cause. As last resource proceed to a restart to backup.

8.1.6.18 IPsec not running

IPsec 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: IPsec

Maintenance Procedure: Process Manager has a mechanism to restart automatically the applications that are not running. If IPsec 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.

8.1.6.19 Unsupported Hardware Platform

Unsupported Hardware Platform

Associated Device: OSB,SBC

Group Name: Software

Severity: critical

Default Threshold: advantech250: 0;d945:0;

Faulty Object: System Software

Maintenance Procedure: Software version is incompatible with the Hardware model. Upgrade of the Hardware is required.

8.1.6.20 Branch is operating in Backup Link Mode

Branch is operating in Backup Link Mode

Associated Device: OSB

Group Name: Communication

Severity: major

Default Threshold: rx200: 0; rx330: 0; advantech250: 0; advantech50i: 0; advantech500i: 0; x3250: 0; x3550: 0;

Faulty Object: BLC

Maintenance Procedure: When standard connection to OSV is reestablished the BackupLink will be terminated, then this alarm will be automatically cleared.

8.1.6.21 Card 1 failure

Card 1 failure

Associated Device: OSB

Group Name: Hardware:

Severity: major

Default Threshold: advantech50i: 0; advantech500i: 0;

Faulty Object: HW-Sensors

Maintenance Procedure:

8.1.6.22 Card 1 port 1 failure

Card 1 port 1 failure

Associated Device: OSB

Group Name: Hardware:

Severity: major

Default Threshold: advantech50i: 0; advantech500i: 0;

Faulty Object: HW-Sensors

Maintenance Procedure:

8.1.6.23 Card 1 port 2 failure

Card 1 port 2 failure

Associated Device: OSB

Group Name: Hardware:

Severity: major

Default Threshold: advantech50i: 0; advantech500i: 0;

Faulty Object: HW-Sensors

Maintenance Procedure:

8.1.6.24 Card 1 port 3 failure

Card 1 port 3 failure

Associated Device: OSB

Group Name: Hardware:

Severity: major

Default Threshold: advantech50i: 0; advantech500i: 0;

Faulty Object: HW-Sensors

Maintenance Procedure:

8.1.6.25 Card 1 port 4 failure

Card 1 port 4 failure

Associated Device: OSB

Group Name: Hardware:

Severity: major

Default Threshold: advantech50i: 0; advantech500i: 0;

Faulty Object: HW-Sensors

Maintenance Procedure:

8.1.6.26 Card 1 port 5 failure

Card 1 port 5 failure

Associated Device: OSB

Group Name: Hardware:

Severity: major

Default Threshold: advantech50i: 0;

Faulty Object: HW-Sensors

Maintenance Procedure:**8.1.6.27 Card 1 port 6 failure**

Card 1 port 6 failure

Associated Device: OSB

Group Name: Hardware:

Severity: major

Default Threshold: advantech50i: 0;

Faulty Object: HW-Sensors

Maintenance Procedure:

8.1.6.28 Card 1 port 7 failure

Card 1 port 7 failure

Associated Device: OSB

Group Name: Hardware:

Severity: major

Default Threshold: advantech50i: 0;

Faulty Object: HW-Sensors

Maintenance Procedure:

8.1.6.29 Card 1 port 8 failure

Card 1 port 8 failure

Associated Device: OSB

Group Name: Hardware:

Severity: major

Default Threshold: advantech50i: 0;

Faulty Object: HW-Sensors

Maintenance Procedure:

8.1.6.30 Card 1 port 9 failure

Card 1 port 9 failure

Associated Device: OSB

Group Name: Hardware:

Severity: major

Default Threshold: advantech50i: 0;

Faulty Object: FXS

Maintenance Procedure:Change FXS card to fix the problem

8.1.6.31 Card 1 port 10 failure

Card 1 port 10 failure

Associated Device: OSB

Group Name: Hardware:

Severity: major

Default Threshold: advantech50i: 0;

Faulty Object: FXS

Maintenance Procedure:Change FXS card to fix the problem

8.1.6.32 Card 1 port 11 failure

Card 1 port 11 failure

Associated Device: OSB

Group Name: Hardware:

Severity: major

Default Threshold: advantech50i: 0;

Faulty Object: FXS

Maintenance Procedure:Change FXS card to fix the problem

8.1.6.33 Card 1 port 12 failure

Card 1 port 12 failure

Associated Device: OSB

Group Name: Hardware:

Severity: major

Default Threshold: advantech50i: 0;

Faulty Object: FXS

Maintenance Procedure:Change FXS card to fix the problem

8.1.6.34 Card 1 port 13 failure

Card 1 port 13 failure

Associated Device: OSB

Group Name: Hardware:

Severity: major

Default Threshold: advantech50i: 0;

Faulty Object: FXS

Maintenance Procedure:Change FXS card to fix the problem

8.1.6.35 Card 1 port 14 failure

Card 1 port 14 failure

Associated Device: OSB

Group Name: Hardware:

Severity: major

Default Threshold: advantech50i: 0;

Faulty Object: FXS

Maintenance Procedure:Change FXS card to fix the problem

8.1.6.36 Card 1 port 15 failure

Card 1 port 15 failure

Associated Device: OSB

Group Name: Hardware:

Severity: major

Default Threshold: advantech50i: 0;

Faulty Object: FXS

Maintenance Procedure:Change FXS card to fix the problem

8.1.6.37 Card 1 port 16 failure

Card 1 port 16 failure

Associated Device: OSB

Group Name: Hardware:

Severity: major

Default Threshold: advantech50i: 0;

Faulty Object: FXS

Maintenance Procedure:Change FXS card to fix the problem

8.1.6.38 Card 1 port 17 failure

Card 1 port 17 failure

Associated Device: OSB

Group Name: Hardware:

Severity: major

Default Threshold: advantech50i: 0;

Faulty Object: FXS

Maintenance Procedure:Change FXS card to fix the problem

8.1.6.39 Card 1 port 18 failure

Card 1 port 18 failure

Associated Device: OSB

Group Name: Hardware:

Severity: major

Default Threshold: advantech50i: 0;

Faulty Object: FXS

Maintenance Procedure:Change FXS card to fix the problem

8.1.6.40 Card 1 port 19 failure

Card 1 port 19 failure

Associated Device: OSB

Group Name: Hardware:

Severity: major

Default Threshold: advantech50i: 0;

Faulty Object: FXS

Maintenance Procedure:Change FXS card to fix the problem

8.1.6.41 Card 1 port 20 failure

Card 1 port 20 failure

Associated Device: OSB

Group Name: Hardware:

Severity: major

Default Threshold: advantech50i: 0;

Faulty Object: FXS

Maintenance Procedure:Change FXS card to fix the problem

8.1.6.42 Card 1 port 21 failure

Card 1 port 21 failure

Associated Device: OSB

Group Name: Hardware:

Severity: major

Default Threshold: advantech50i: 0;

Faulty Object: FXS

Maintenance Procedure:Change FXS card to fix the problem

8.1.6.43 Card 1 port 22 failure

Card 1 port 22 failure

Associated Device: OSB

Group Name: Hardware:

Severity: major

Default Threshold: advantech50i: 0;

Faulty Object: FXS

Maintenance Procedure:Change FXS card to fix the problem

8.1.6.44 Card 1 port 23 failure

Card 1 port 23 failure

Associated Device: OSB

Group Name: Hardware:

Severity: major

Default Threshold: advantech50i: 0;

Faulty Object: FXS

Maintenance Procedure:Change FXS card to fix the problem

8.1.6.45 Card 1 port 24 failure

Card 1 port 24 failure

Associated Device: OSB

Group Name: Hardware:

Severity: major

Default Threshold: advantech50i: 0;

Faulty Object: FXS

Maintenance Procedure:Change FXS card to fix the problem

8.1.6.46 Card 1 port 1 recovering

Card 1 port 1 recovering

Associated Device: OSB

Group Name: Hardware:

Severity: major

Default Threshold: advantech50i: 0; advantech500i: 0;

Faulty Object: HW-Sensors

Maintenance Procedure: Wait for the link recovery

8.1.6.47 Card 1 port 2 recovering

Card 1 port 2 recovering

Associated Device: OSB

Group Name: Hardware:

Severity: major

Default Threshold: advantech50i: 0; advantech500i: 0;

Faulty Object: HW-Sensors

Maintenance Procedure: Wait for the link recovery

8.1.6.48 Card 1 port 3 recovering

Card 1 port 3 recovering

Associated Device: OSB

Group Name: Hardware:

Severity: major

Default Threshold: advantech50i: 0; advantech500i: 0;

Faulty Object: HW-Sensors

Maintenance Procedure: Wait for the link recovery

8.1.6.49 Card 1 port 4 recovering

Card 1 port 4 recovering

Associated Device: OSB

Group Name: Hardware:

Severity: major

Default Threshold: advantech50i: 0; advantech500i: 0;

Faulty Object: HW-Sensors

Maintenance Procedure: Wait for the link recovery

8.1.6.50 Card 1 port 5 recovering

Card 1 port 5 recovering

Associated Device: OSB

Group Name: Hardware:

Severity: major

Default Threshold: advantech50i: 0; advantech500i: 0;

Faulty Object: HW-Sensors

Maintenance Procedure: Wait for the link recovery

8.1.6.51 Card 1 port 6 recovering

Card 1 port 6 recovering

Associated Device: OSB

Group Name: Hardware:

Severity: major

Default Threshold: advantech50i: 0; advantech500i: 0;

Faulty Object: HW-Sensors

Maintenance Procedure: Wait for the link recovery

8.1.6.52 Card 1 port 7 recovering

Card 1 port 7 recovering

Associated Device: OSB

Group Name: Hardware:

Severity: major

Default Threshold: advantech50i: 0; advantech500i: 0;

Faulty Object: HW-Sensors

Maintenance Procedure: Wait for the link recovery

8.1.6.53 Card 1 port 8 recovering

Card 1 port 8 recovering

Associated Device: OSB

Group Name: Hardware:

Severity: major

Default Threshold: advantech50i: 0; advantech500i: 0;

Faulty Object: HW-Sensors

Maintenance Procedure: Wait for the link recovery

8.1.6.54 Card 2 failure

Card 2 failure

Associated Device: OSB

Group Name: Hardware:

Severity: major

Default Threshold: advantech50i: 0; advantech500i: 0;

Faulty Object: HW-Sensors

Maintenance Procedure:

8.1.6.55 Card 2 port 1 failure

Card 2 port 1 failure

Associated Device: OSB

Group Name: Hardware:

Severity: major

Default Threshold: advantech50i: 0; advantech500i: 0;

Faulty Object: HW-Sensors

Maintenance Procedure:

8.1.6.56 Card 2 port 2 failure

Card 2 port 2 failure

Associated Device: OSB

Group Name: Hardware:

Severity: major

Default Threshold: advantech50i: 0; advantech500i: 0;

Faulty Object: HW-Sensors

Maintenance Procedure:**8.1.6.57 Card 2 port 3 failure**

Card 2 port 3 failure

Associated Device: OSB

Group Name: Hardware:

Severity: major

Default Threshold: advantech50i: 0; advantech500i: 0;

Faulty Object: HW-Sensors

Maintenance Procedure:

8.1.6.58 Card 2 port 4 failure

Card 2 port 4 failure

Associated Device: OSB

Group Name: Hardware:

Severity: major

Default Threshold: advantech50i: 0; advantech500i: 0;

Faulty Object: HW-Sensors

Maintenance Procedure:

8.1.6.59 Card 2 port 5 failure

Card 2 port 5 failure

Associated Device: OSB

Group Name: Hardware:

Severity: major

Default Threshold:

Faulty Object: HW-Sensors

Maintenance Procedure:

8.1.6.60 Card 2 port 6 failure

Card 2 port 6 failure

Associated Device: OSB

Group Name: Hardware:

Severity: major

Default Threshold:

Faulty Object: HW-Sensors

Maintenance Procedure:

8.1.6.61 Card 2 port 7 failure

Card 2 port 7 failure

Associated Device: OSB

Group Name: Hardware:

Severity: major

Default Threshold:

Faulty Object: HW-Sensors

Maintenance Procedure:

8.1.6.62 Card 2 port 8 failure

Card 2 port 8 failure

Associated Device: OSB

Group Name: Hardware:

Severity: major

Default Threshold:

Faulty Object: HW-Sensors

Maintenance Procedure:

8.1.6.63 Card 2 port 9 failure

Card 2 port 9 failure

Associated Device: OSB

Group Name: Hardware:

Severity: major

Default Threshold: advantech50i: 0;

Faulty Object: FXS

Maintenance Procedure:Change FXS card to fix this problem

8.1.6.64 Card 2 port 10 failure

Card 2 port 10 failure

Associated Device: OSB

Group Name: Hardware:

Severity: major

Default Threshold: advantech50i: 0;

Faulty Object: FXS

Maintenance Procedure:Change FXS card to fix this problem

8.1.6.65 Card 2 port 11 failure

Card 2 port 11 failure

Associated Device: OSB

Group Name: Hardware:

Severity: major

Default Threshold: advantech50i: 0;

Faulty Object: FXS

Maintenance Procedure:Change FXS card to fix this problem

8.1.6.66 Card 2 port 12 failure

Card 2 port 12 failure

Associated Device: OSB

Group Name: Hardware:

Severity: major

Default Threshold: advantech50i: 0;

Faulty Object: FXS

Maintenance Procedure:Change FXS card to fix this problem

8.1.6.67 Card 2 port 13 failure

Card 2 port 13 failure

Associated Device: OSB

Group Name: Hardware:

Severity: major

Default Threshold: advantech50i: 0;

Faulty Object: FXS

Maintenance Procedure:Change FXS card to fix this problem

8.1.6.68 Card 2 port 14 failure

Card 2 port 14 failure

Associated Device: OSB

Group Name: Hardware:

Severity: major

Default Threshold: advantech50i: 0;

Faulty Object: FXS

Maintenance Procedure:Change FXS card to fix this problem

8.1.6.69 Card 2 port 15 failure

Card 2 port 15 failure

Associated Device: OSB

Group Name: Hardware:

Severity: major

Default Threshold: advantech50i: 0;

Faulty Object: FXS

Maintenance Procedure:Change FXS card to fix this problem

8.1.6.70 Card 2 port 16 failure

Card 2 port 16 failure

Associated Device: OSB

Group Name: Hardware:

Severity: major

Default Threshold: advantech50i: 0;

Faulty Object: FXS

Maintenance Procedure:Change FXS card to fix this problem

8.1.6.71 Card 2 port 17 failure

Card 2 port 17 failure

Associated Device: OSB

Group Name: Hardware:

Severity: major

Default Threshold: advantech50i: 0;

Faulty Object: FXS

Maintenance Procedure:Change FXS card to fix this problem

8.1.6.72 Card 2 port 18 failure

Card 2 port 18 failure

Associated Device: OSB

Group Name: Hardware:

Severity: major

Default Threshold: advantech50i: 0;

Faulty Object: FXS

Maintenance Procedure:Change FXS card to fix this problem

8.1.6.73 Card 2 port 19 failure

Card 2 port 19 failure

Associated Device: OSB

Group Name: Hardware:

Severity: major

Default Threshold: advantech50i: 0;

Faulty Object: FXS

Maintenance Procedure:Change FXS card to fix this problem

8.1.6.74 Card 2 port 20 failure

Card 2 port 20 failure

Associated Device: OSB

Group Name: Hardware:

Severity: major

Default Threshold: advantech50i: 0;

Faulty Object: FXS

Maintenance Procedure:Change FXS card to fix this problem

8.1.6.75 Card 2 port 21 failure

Card 2 port 21 failure

Associated Device: OSB

Group Name: Hardware:

Severity: major

Default Threshold: advantech50i: 0;

Faulty Object: FXS

Maintenance Procedure:Change FXS card to fix this problem

8.1.6.76 Card 2 port 22 failure

Card 2 port 22 failure

Associated Device: OSB

Group Name: Hardware:

Severity: major

Default Threshold: advantech50i: 0;

Faulty Object: FXS

Maintenance Procedure:Change FXS card to fix this problem

8.1.6.77 Card 2 port 23 failure

Card 2 port 23 failure

Associated Device: OSB

Group Name: Hardware:

Severity: major

Default Threshold: advantech50i: 0;

Faulty Object: FXS

Maintenance Procedure:Change FXS card to fix this problem

8.1.6.78 Card 2 port 24 failure

Card 2 port 24 failure

Associated Device: OSB

Group Name: Hardware:

Severity: major

Default Threshold: advantech50i: 0;

Faulty Object: FXS

Maintenance Procedure:Change FXS card to fix this problem

8.1.6.79 Card 2 port 1 recovering

Card 2 port 1 recovering

Associated Device: OSB

Group Name: Hardware:

Severity: major

Default Threshold: advantech500i: 0;

Faulty Object: HW-Sensors

Maintenance Procedure: Wait for the link recovery

8.1.6.80 Card 2 port 2 recovering

Card 2 port 2 recovering

Associated Device: OSB

Group Name: Hardware:

Severity: major

Default Threshold: advantech500i: 0;

Faulty Object: HW-Sensors

Maintenance Procedure: Wait for the link recovery

8.1.6.81 Card 2 port 3 recovering

Card 2 port 3 recovering

Associated Device: OSB

Group Name: Hardware:

Severity: major

Default Threshold: advantech500i: 0;

Faulty Object: HW-Sensors

Maintenance Procedure: Wait for the link recovery

8.1.6.82 Card 2 port 4 recovering

Card 2 port 4 recovering

Associated Device: OSB

Group Name: Hardware:

Severity: major

Default Threshold: advantech500i: 0;

Faulty Object: HW-Sensors

Maintenance Procedure: Wait for the link recovery

8.1.6.83 Card 2 port 5 recovering

Card 2 port 5 recovering

Associated Device: OSB

Group Name: Hardware:

Severity: major

Default Threshold: advantech500i: 0;

Faulty Object: HW-Sensors

Maintenance Procedure: Wait for the link recovery

8.1.6.84 Card 2 port 6 recovering

Card 2 port 6 recovering

Associated Device: OSB

Group Name: Hardware:

Severity: major

Default Threshold: advantech500i: 0;

Faulty Object: HW-Sensors

Maintenance Procedure: Wait for the link recovery

8.1.6.85 Card 2 port 7 recovering

Card 2 port 7 recovering

Associated Device: OSB

Group Name: Hardware:

Severity: major

Default Threshold: advantech500i: 0;

Faulty Object: HW-Sensors

Maintenance Procedure: Wait for the link recovery

8.1.6.86 Card 2 port 8 recovering

Card 2 port 8 recovering

Associated Device: OSB

Group Name: Hardware:

Severity: major

Default Threshold: advantech500i: 0;

Faulty Object: HW-Sensors

Maintenance Procedure: Wait for the link recovery

8.1.6.87 D-channel down on Card 1 port 1

D-Channel down on Card 1 port 1, due to physical layer or configuration problems

Associated Device: OSB

Group Name: Communication

Severity: major

Default Threshold: advantech500i: 0;advantech50i:0;

Faulty Object: ISDN

Maintenance Procedure: This may indicate a failure with physical layer. Configuration mismatches may also trigger this alarm, for example, configuring both sides as user (terminal mode) or network. Loss of synchronization or timing slips could cause the d-channel not coming up, this may be fixed disabling and enabling the port locally/remotely, or rebooting the system.

8.1.6.88 D-channel down on Card 1 port 2

D-Channel down on Card 1 port 2, due to physical layer or configuration problems

Associated Device: OSB

Group Name: Communication

Severity: major

Default Threshold: advantech500i: 0;advantech50i:0;

Faulty Object: ISDN

Maintenance Procedure: This may indicate a failure with physical layer. Configuration mismatches may also trigger this alarm, for example, configuring both sides as user (terminal mode) or network. Loss of synchronization or timing slips could cause the d-channel not coming up, this may be fixed disabling and enabling the port locally/remotely, or rebooting the system.

8.1.6.89 D-channel down on Card 1 port 3

D-Channel down on Card 1 port 3, due to physical layer or configuration problems

Associated Device: OSB

Group Name: Communication

Severity: major

Default Threshold: advantech500i: 0;advantech50i:0;

Faulty Object: ISDN

Maintenance Procedure: This may indicate a failure with physical layer. Configuration mismatches may also trigger this alarm, for example, configuring both sides as user (terminal mode) or network. Loss of synchronization or timing slips could cause the d-channel not coming up, this may be fixed disabling and enabling the port locally/remotely, or rebooting the system.

8.1.6.90 D-channel down on Card 1 port 4

D-Channel down on Card 1 port 4, due to physical layer or configuration problems

Associated Device: OSB

Group Name: Communication

Severity: major

Default Threshold: advantech500i: 0;advantech50i:0;

Faulty Object: ISDN

Maintenance Procedure: This may indicate a failure with physical layer. Configuration mismatches may also trigger this alarm, for example, configuring both sides as user (terminal mode) or network. Loss of synchronization or timing slips could cause the d-channel not coming up, this may be fixed disabling and enabling the port locally/remotely, or rebooting the system.

8.1.6.91 D-channel down on Card 2 port 1

D-Channel down on Card 2 port 1, due to physical layer or configuration problems

Associated Device: OSB

Group Name: Communication

Severity: major

Default Threshold: advantech500i:0;

Faulty Object: ISDN

Maintenance Procedure: This may indicate a failure with physical layer. Configuration mismatches may also trigger this alarm, for example, configuring both sides as user (terminal mode) or network. Loss of synchronization or timing slips could cause the d-channel not coming up, this may be fixed disabling and enabling the port locally/remotely, or rebooting the system.

8.1.6.92 D-channel down on Card 2 port 2

D-Channel down on Card 2 port 2, due to physical layer or configuration problems

Associated Device: OSB

Group Name: Communication

Severity: major

Default Threshold: advantech500i:0;

Faulty Object: ISDN

Maintenance Procedure: This may indicate a failure with physical layer. Configuration mismatches may also trigger this alarm, for example, configuring both sides as user (terminal mode) or network. Loss of synchronization or timing slips could cause the d-channel not coming up, this may be fixed disabling and enabling the port locally/remotely, or rebooting the system.

8.1.6.93 D-channel down on Card 2 port 3

D-Channel down on Card 2 port 3, due to physical layer or configuration problems

Associated Device: OSB

Group Name: Communication

Severity: major

Default Threshold: advantech500i: 0;

Faulty Object: ISDN

Maintenance Procedure: This may indicate a failure with physical layer. Configuration mismatches may also trigger this alarm, for example, configuring both sides as user (terminal mode) or network. Loss of synchronization or timing slips could cause the d-channel not coming up, this may be fixed disabling and enabling the port locally/remotely, or rebooting the system.

8.1.6.94 D-channel down on Card 2 port 4

D-Channel down on Card 2 port 4, due to physical layer or configuration problems

Associated Device: OSB

Group Name: Communication

Severity: major

Default Threshold: advantech500i: 0;

Faulty Object: ISDN

Maintenance Procedure: This may indicate a failure with physical layer. Configuration mismatches may also trigger this alarm, for example, configuring both sides as user (terminal mode) or network. Loss of synchronization or timing slips could cause the d-channel not coming up, this may be fixed disabling and enabling the port locally/remotely, or rebooting the system.

8.1.6.95 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;

Faulty Object: Resource

Maintenance Procedure:

8.1.6.96 CDRHandler 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;

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.

8.1.6.97 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;

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.

8.1.6.98 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;

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.

8.1.6.99 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;

Faulty Object: TLS Certificate

Maintenance Procedure: A new certificate shall be generated.

8.1.6.100 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;

Faulty Object: TLS Certificate

Maintenance Procedure: Update the certificate immediately.

8.1.6.101 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;

Faulty Object: TLS Certificate

Maintenance Procedure: A new certificate shall be generated.

8.1.6.102 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;

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.

8.1.6.103 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;

Faulty Object: TLS Certificate

Maintenance Procedure: Update the certificate as soon as possible.

8.1.6.104 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;

Faulty Object: TLS Certificate

Maintenance Procedure: Contact the Certification Authority that issued the CRL to resolve the invalid CRL.

8.1.6.105 Subscriber synchronization failure

Either the Subscriber Data or the Digest Authentication Data or both have not been correctly synchronized.

Associated Device: OSB, SBC

Group Name: Security

Severity: critical

Default Threshold: rx200: 0; rx330: 0; advantech250: 0; advantech50i: 0; advantech500i: 0; x3250: 0; x3550: 0;d945:0;

Faulty Object: SIP Server Subscriber Authentication

Maintenance Procedure: Check if the OpenScape Voice supports digest authentication and the subscriber data synchronization. Synchronize the configuration. This alarm must be manually cleared.

8.1.6.106 Event Name Wrong Digest Authentication exchange key

The key used for digest authentication on OSV doesn't match with the one used on OSB.

Associated Device: OSB, SBC

Group Name: Security

Severity: critical

Default Threshold: rx200: 0; rx330: 0; advantech250: 0; advantech50i: 0; advantech500i: 0; x3250: 0; x3550: 0;d945:0;

Faulty Object: SIP Server Subscriber Authentication

Maintenance Procedure : The alarm should be cleared automatically after OSB resends the key to OSV and a successful digest authentication is completed.

8.1.6.107 CPU Vcore HT high voltage

CPU Vcore HT high voltage.

Associated Device: OSB

Group Name: Hardware:

Severity: critical

Default Threshold: rx330: 1.26;

Faulty Object: HW-Sensors

Maintenance Procedure:

8.1.6.108 CPU Vcore HT low voltage

CPU Vcore HT low voltage.

Associated Device: OSB

Group Name: Hardware:

Severity: critical

Default Threshold: rx330: 1.13;

Faulty Object: HW-Sensors

Maintenance Procedure:

8.1.6.109 CPU VDD HT high voltage

CPU VDD HT high voltage.

Associated Device: OSB

Group Name: Hardware:

Severity: critical

Default Threshold: rx330: 2.633;

Faulty Object: HW-Sensors

Maintenance Procedure:

8.1.6.110 CPU VDD HT low voltage

CPU VDD HT low voltage.

Associated Device: OSB

Group Name: Hardware:

Severity: critical

Default Threshold: rx330: 2.397;

Faulty Object: HW-Sensors

Maintenance Procedure:

8.1.6.111 CPU VLDT HT 1.2V high voltage

CPU VLDT HT 1.2V high voltage.

Associated Device: OSB

Group Name: Hardware

Severity: critical

Default Threshold: rx330: 1.26;

Faulty Object: HW-Sensors

Maintenance Procedure:**8.1.6.112 CPU VLDT HT 1.2V low voltage**

CPU VLDT HT 1.2V low voltage.

Associated Device: OSB

Group Name: Hardware

Severity: critical

Default Threshold: rx330: 1.13;

Faulty Object: HW-Sensors

Maintenance Procedure:

8.1.6.113 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;

Faulty Object: HW-Sensors

Maintenance Procedure:

8.1.6.114 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;

Faulty Object: HW-Sensors

Maintenance Procedure:

8.1.6.115 CPU1 +2.5V high voltage

CPU1 +2.5V high voltage.

Associated Device: OSB

Group Name: Hardware:

Severity: critical

Default Threshold: rx330: 2.6;

Faulty Object: HW-Sensors

Maintenance Procedure:

8.1.6.116 CPU1 +2.5V low voltage

CPU1 +2.5V low voltage.

Associated Device: OSB

Group Name: Hardware:

Severity: critical

Default Threshold: rx330: 2.4;

Faulty Object: HW-Sensors

Maintenance Procedure:

8.1.6.117 CPU1 VRM CPU1 high voltage

CPU1 VRM CPU1 high voltage.

Associated Device: OSB

Group Name: Hardware:

Severity: critical

Default Threshold: rx330: 13.008;

Faulty Object: HW-Sensors

Maintenance Procedure:

8.1.6.118 CPU1 VRM CPU1 low voltage

CPU1 VRM CPU1 low voltage.

Associated Device: OSB

Group Name: Hardware:

Severity: critical

Default Threshold: rx330: 11.055;

Faulty Object: HW-Sensors

Maintenance Procedure:

8.1.6.119 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:

8.1.6.120 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:

8.1.6.121 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:

8.1.6.122 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:

8.1.6.123 CPU2 +2.5V high voltage

CPU2 +2.5V high voltage.

Associated Device: OSB

Group Name: Hardware:

Severity: critical

Default Threshold: rx330: 2.6;

Faulty Object: HW-Sensors

Maintenance Procedure:

8.1.6.124 CPU2 +2.5V low voltage

CPU2 +2.5V low voltage.

Associated Device: OSB

Group Name: Hardware:

Severity: critical

Default Threshold: rx330: 2.4;

Faulty Object: HW-Sensors

Maintenance Procedure:

8.1.6.125 CPU2 Vtt high voltage

CPU2 Vtt high voltage.

Associated Device: OSB

Group Name: Hardware:

Severity: critical

Default Threshold: rx330: 1.000;

Faulty Object: HW-Sensors

Maintenance Procedure:

8.1.6.126 CPU2 Vtt low voltage

CPU2 Vtt low voltage.

Associated Device: OSB

Group Name: Hardware:

Severity: critical

Default Threshold: rx330: 0.790;

Faulty Object: HW-Sensors

Maintenance Procedure:**8.1.6.127 CPU2 VRM CPU2 high voltage**

CPU2 VRM CPU2 high voltage.

Associated Device: OSB

Group Name: Hardware:

Severity: critical

Default Threshold: rx330: 13.008;

Faulty Object: HW-Sensors

Maintenance Procedure:

8.1.6.128 CPU2 VRM CPU2 low voltage

CPU2 VRM CPU2 low voltage.

Associated Device: OSB

Group Name: Hardware:

Severity: critical

Default Threshold: rx330: 11.055;

Faulty Object: HW-Sensors

Maintenance Procedure:

8.1.6.129 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;

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.

8.1.6.130 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;

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.

8.1.6.131 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;

Faulty Object: TLS Certificate

Maintenance Procedure: Verify if there is enough disk space to store the CRL file.

8.1.6.132 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;

Faulty Object: TLS Certificate

Maintenance Procedure: Resolve the network problem that prevented the CRL download.

8.1.6.133 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;

Faulty Object: TLS Certificate

Maintenance Procedure: Update the expired CRL.

8.1.6.134 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;

Faulty Object: TLS Certificate

Maintenance Procedure: Contact the Certification Authority that issued the CRL to resolve the invalid CRL.

8.1.6.135 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;

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.

8.1.6.136 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;

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.

8.1.6.137 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;

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.

8.1.6.138 Error writing a CDR billing file

Error writing a CDR billing file

Associated Device: OSB

Group Name: Usage

Severity: major

Default Threshold: rx200: 0; rx330: 0; advantech250: 0; advantech50i: 0; advantech500i: 0; x3250: 0; x3550: 0;

Faulty Object: CDR

Maintenance Procedure: There is no free space in cdr path, this is most probably caused by a connection loss with billing server. Either delete manually files or check connectivity to billing server, otherwise CDR tickets will be lost.

8.1.6.139 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;

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.

8.1.6.140 Failed to add Backup Link channel

Failed to add Backup Link channel.

Associated Device: OSB

Group Name: Communication

Severity: major

Default Threshold: rx200: 0; rx330: 0; advantech250: 0; advantech50i: 0; advantech500i: 0; x3250: 0; x3550: 0;

Faulty Object: BLC

Maintenance Procedure: Check BLC/BLS configuration. Problem may also be on PSTN call routing.

8.1.6.141 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;

Faulty Object: BLC

Maintenance Procedure: Check why BackupLink calls are failing or taking too much to complete.

8.1.6.142 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;

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.

8.1.6.143 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;

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.

8.1.6.144 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;

Faulty Object: phone sw repository

Maintenance Procedure: The system is in backup link mode, see alarm (groupId='5' eventId='14').

8.1.6.145 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;

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.

8.1.6.146 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;

Faulty Object: phone sw repository

Maintenance Procedure: The system is in survivable mode, see alarm (groupId='5' eventId='4').

8.1.6.147 Far End Alarm on Card 1 port 1: AIS signal received

Far End Alarm on Card 1 port 1: AIS signal received

Associated Device: OSB

Group Name: Hardware:

Severity: major

Default Threshold: advantech50i: 0; advantech500i: 0;

Faulty Object: PRI

Maintenance Procedure: A received Alarm Indication Signal means that an alarm is occurring on the line upstream of the PSTN connected to the port. Check if the framing format configured on the port matches the framing format of the line. If not, change the framing format on this port to match that of the line. Contact the service provider to check for misconfiguration within the PSTN.

8.1.6.148 Far End Alarm on Card 1 port 2: AIS signal received

Far End Alarm on Card 1 port 2: AIS signal received

Associated Device: OSB

Group Name: Hardware:

Severity: major

Default Threshold: advantech500i: 0;

Faulty Object: PRI

Maintenance Procedure: A received Alarm Indication Signal means that an alarm is occurring on the line upstream of the PSTN connected to the port. Check if the framing format configured on the port matches the framing format of the line. If not, change the framing format on this port to match that of the line. Contact the service provider to check for misconfiguration within the PSTN.

8.1.6.149 Far End Alarm on Card 1 port 3: AIS signal received

Far End Alarm on Card 1 port 3: AIS signal received

Associated Device: OSB

Group Name: Hardware:

Severity: major

Default Threshold: advantech500i: 0;

Faulty Object: PRI

Maintenance Procedure: A received Alarm Indication Signal means that an alarm is occurring on the line upstream of the PSTN connected to the port. Check if the framing format configured on the port matches the framing format of the line. If not, change the framing format on this port to match that of the line. Contact the service provider to check for misconfiguration within the PSTN.

8.1.6.150 Far End Alarm on Card 1 port 4: AIS signal received

Far End Alarm on Card 1 port 4: AIS signal received

Associated Device: OSB

Group Name: Hardware:

Severity: major

Default Threshold: advantech500i: 0;

Faulty Object: PRI

Maintenance Procedure: A received Alarm Indication Signal means that an alarm is occurring on the line upstream of the PSTN connected to the port. Check if the framing format configured on the port matches the framing format of the line. If not, change the framing format on this port to match that of the line. Contact the service provider to check for misconfiguration within the PSTN.

8.1.6.151 Far End Alarm on Card 1 port 5: AIS signal received

Far End Alarm on Card 1 port 5: AIS signal received

Associated Device: OSB

Group Name: Hardware:

Severity: major

Default Threshold:

Faulty Object: PRI

Maintenance Procedure: A received Alarm Indication Signal means that an alarm is occurring on the line upstream of the PSTN connected to the port. Check if the framing format configured on the port matches the framing format of the line. If not, change the framing format on this port to match that of the line. Contact the service provider to check for misconfiguration within the PSTN.

8.1.6.152 Far End Alarm on Card 1 port 6: AIS signal received

Far End Alarm on Card 1 port 6: AIS signal received

Associated Device: OSB

Group Name: Hardware:

Severity: major

Default Threshold:

Faulty Object: PRI

Maintenance Procedure: A received Alarm Indication Signal means that an alarm is occurring on the line upstream of the PSTN connected to the port. Check if the framing format configured on the port matches the framing format of the line. If not, change the framing format on this port to match that of the line. Contact the service provider to check for misconfiguration within the PSTN.

8.1.6.153 Far End Alarm on Card 1 port 7: AIS signal received

Far End Alarm on Card 1 port 7: AIS signal received

Associated Device: OSB

Group Name: Hardware:

Severity: major

Default Threshold:

Faulty Object: PRI

Maintenance Procedure: A received Alarm Indication Signal means that an alarm is occurring on the line upstream of the PSTN connected to the port. Check if the framing format configured on the port matches the framing format of the line. If not, change the framing format on this port to match that of the line. Contact the service provider to check for misconfiguration within the PSTN.

8.1.6.154 Far End Alarm on Card 1 port 8: AIS signal received

Far End Alarm on Card 1 port 8: AIS signal received

Associated Device: OSB

Group Name: Hardware:

Severity: major

Default Threshold:

Faulty Object: PRI

Maintenance Procedure: A received Alarm Indication Signal means that an alarm is occurring on the line upstream of the PSTN connected to the port. Check if the framing format configured on the port matches the framing format of the line. If not, change the framing format on this port to match that of the line. Contact the service provider to check for misconfiguration within the PSTN.

8.1.6.155 Far End Alarm on Card 1 port 1: RAI signal received

Far End Alarm on Card 1 port 1: RAI signal received

Associated Device: OSB

Group Name: Hardware:

Severity: major

Default Threshold: advantech50i: 0; advantech500i: 0;

Faulty Object: PRI

Maintenance Procedure: A received Remote Alarm Indication means that the PSTN has a problem with the signal that it is receiving from OSB. Firstly, check the cabling. Then check the settings at the remote end and verify that they match OSB port settings. Try to connect this port to another PSTN line. If the new connection clears the alarm, then the problem may occur in the previous PSTN line and the PSTN provider must be contacted.

8.1.6.156 Far End Alarm on Card 1 port 2: RAI signal received

Far End Alarm on Card 1 port 2: RAI signal received

Associated Device: OSB

Group Name: Hardware:

Severity: major

Default Threshold: advantech500i: 0;

Faulty Object: PRI

Maintenance Procedure: A received Remote Alarm Indication means that the PSTN has a problem with the signal that it is receiving from OSB. Firstly, check the cabling. Then check the settings at the remote end and verify that they match OSB port settings. Try to connect this port to another PSTN line. If the new connection clears the alarm, then the problem may occur in the previous PSTN line and the PSTN provider must be contacted.

8.1.6.157 Far End Alarm on Card 1 port 3: RAI signal received

Far End Alarm on Card 1 port 3: RAI signal received

Associated Device: OSB

Group Name: Hardware:

Severity: major

Default Threshold: advantech500i: 0;

Faulty Object: PRI

Maintenance Procedure: A received Remote Alarm Indication means that the PSTN has a problem with the signal that it is receiving from OSB. Firstly, check the cabling. Then check the settings at the remote end and verify that they match OSB port settings. Try to connect this port to another PSTN line. If the new connection clears the alarm, then the problem may occur in the previous PSTN line and the PSTN provider must be contacted.

8.1.6.158 Far End Alarm on Card 1 port 4: RAI signal received

Far End Alarm on Card 1 port 4: RAI signal received

Associated Device: OSB

Group Name: Hardware:

Severity: major

Default Threshold: advantech500i: 0;

Faulty Object: PRI

Maintenance Procedure: A received Remote Alarm Indication means that the PSTN has a problem with the signal that it is receiving from OSB. Firstly, check the cabling. Then check the settings at the remote end and verify that they match OSB port settings. Try to connect this port to another PSTN line. If the new connection clears the alarm, then the problem may occur in the previous PSTN line and the PSTN provider must be contacted.

8.1.6.159 Far End Alarm on Card 1 port 5: RAI signal received

Far End Alarm on Card 1 port 5: RAI signal received

Associated Device: OSB

Group Name: Hardware:

Severity: major

Default Threshold:

Faulty Object: PRI

Maintenance Procedure: A received Remote Alarm Indication means that the PSTN has a problem with the signal that it is receiving from OSB. Firstly, check the cabling. Then check the settings at the remote end and verify that they match OSB port settings. Try to connect this port to another PSTN line. If the new connection clears the alarm, then the problem may occur in the previous PSTN line and the PSTN provider must be contacted.

8.1.6.160 Far End Alarm on Card 1 port 6: RAI signal received

Far End Alarm on Card 1 port 6: RAI signal received

Associated Device: OSB

Group Name: Hardware:

Severity: major

Default Threshold:

Faulty Object: PRI

Maintenance Procedure: A received Remote Alarm Indication means that the PSTN has a problem with the signal that it is receiving from OSB. Firstly, check the cabling. Then check the settings at the remote end and verify that they match OSB port settings. Try to connect this port to another PSTN line. If the new connection clears the alarm, then the problem may occur in the previous PSTN line and the PSTN provider must be contacted.

8.1.6.161 Far End Alarm on Card 1 port 7: RAI signal received

Far End Alarm on Card 1 port 7: RAI signal received

Associated Device: OSB

Group Name: Hardware:

Severity: major

Default Threshold:

Faulty Object: PRI

Maintenance Procedure: A received Remote Alarm Indication means that the PSTN has a problem with the signal that it is receiving from OSB. Firstly, check the cabling. Then check the settings at the remote end and verify that they match OSB port settings. Try to connect this port to another PSTN line. If the new connection clears the alarm, then the problem may occur in the previous PSTN line and the PSTN provider must be contacted.

8.1.6.162 Far End Alarm on Card 1 port 8: RAI signal received

Far End Alarm on Card 1 port 8: RAI signal received

Associated Device: OSB

Group Name: Hardware:

Severity: major

Default Threshold:

Faulty Object: PRI

Maintenance Procedure: A received Remote Alarm Indication means that the PSTN has a problem with the signal that it is receiving from OSB. Firstly, check the cabling. Then check the settings at the remote end and verify that they match OSB port settings. Try to connect this port to another PSTN line. If the

new connection clears the alarm, then the problem may occur in the previous PSTN line and the PSTN provider must be contacted.

8.1.6.163 Far End Alarm on Card 2 port 1: AIS signal received

Far End Alarm on Card 2 port 1: AIS signal received

Associated Device: OSB

Group Name: Hardware:

Severity: major

Default Threshold: advantech500i: 0;

Faulty Object: PRI

Maintenance Procedure: A received Alarm Indication Signal means that an alarm is occurring on the line upstream of the PSTN connected to the port. Check if the framing format configured on the port matches the framing format of the line. If not, change the framing format on this port to match that of the line. Contact the service provider to check for misconfiguration within the PSTN.

8.1.6.164 Far End Alarm on Card 2 port 2: AIS signal received

Far End Alarm on Card 2 port 2: AIS signal received

Associated Device: OSB

Group Name: Hardware:

Severity: major

Default Threshold: advantech500i: 0;

Faulty Object: PRI

Maintenance Procedure: A received Alarm Indication Signal means that an alarm is occurring on the line upstream of the PSTN connected to the port. Check if the framing format configured on the port matches the framing format of the line. If not, change the framing format on this port to match that of the line. Contact the service provider to check for misconfiguration within the PSTN.

8.1.6.165 Far End Alarm on Card 2 port 3: AIS signal received

Far End Alarm on Card 2 port 3: AIS signal received

Associated Device: OSB

Group Name: Hardware:

Severity: major

Default Threshold: advantech500i: 0;

Faulty Object: PRI

Maintenance Procedure: A received Alarm Indication Signal means that an alarm is occurring on the line upstream of the PSTN connected to the port.

Check if the framing format configured on the port matches the framing format of the line. If not, change the framing format on this port to match that of the line. Contact the service provider to check for misconfiguration within the PSTN.

8.1.6.166 Far End Alarm on Card 2 port 4: AIS signal received

Far End Alarm on Card 2 port 4: AIS signal received

Associated Device: OSB

Group Name: Hardware:

Severity: major

Default Threshold: advantech500i: 0;

Faulty Object: PRI

Maintenance Procedure: A received Alarm Indication Signal means that an alarm is occurring on the line upstream of the PSTN connected to the port. Check if the framing format configured on the port matches the framing format of the line. If not, change the framing format on this port to match that of the line. Contact the service provider to check for misconfiguration within the PSTN.

8.1.6.167 Far End Alarm on Card 2 port 5: AIS signal received

Far End Alarm on Card 2 port 5: AIS signal received

Associated Device: OSB

Group Name: Hardware:

Severity: major

Default Threshold:

Faulty Object: PRI

Maintenance Procedure: A received Alarm Indication Signal means that an alarm is occurring on the line upstream of the PSTN connected to the port. Check if the framing format configured on the port matches the framing format of the line. If not, change the framing format on this port to match that of the line. Contact the service provider to check for misconfiguration within the PSTN.

8.1.6.168 Far End Alarm on Card 2 port 6: AIS signal received

Far End Alarm on Card 2 port 6: AIS signal received

Associated Device: OSB

Group Name: Hardware:

Severity: major

Default Threshold:

Faulty Object: PRI

Maintenance Procedure: A received Alarm Indication Signal means that an alarm is occurring on the line upstream of the PSTN connected to the port. Check if the framing format configured on the port matches the framing format of the line. If not, change the framing format on this port to match that of the line. Contact the service provider to check for misconfiguration within the PSTN.

8.1.6.169 Far End Alarm on Card 2 port 7: AIS signal received

Far End Alarm on Card 2 port 7: AIS signal received

Associated Device: OSB

Group Name: Hardware:

Severity: major

Default Threshold:

Faulty Object: PRI

Maintenance Procedure: A received Alarm Indication Signal means that an alarm is occurring on the line upstream of the PSTN connected to the port. Check if the framing format configured on the port matches the framing format of the line. If not, change the framing format on this port to match that of the line. Contact the service provider to check for misconfiguration within the PSTN.

8.1.6.170 Far End Alarm on Card 2 port 8: AIS signal received

Far End Alarm on Card 2 port 8: AIS signal received

Associated Device: OSB

Group Name: Hardware:

Severity: major

Default Threshold:

Faulty Object: PRI

Maintenance Procedure: A received Alarm Indication Signal means that an alarm is occurring on the line upstream of the PSTN connected to the port. Check if the framing format configured on the port matches the framing format of the line. If not, change the framing format on this port to match that of the line. Contact the service provider to check for misconfiguration within the PSTN.

8.1.6.171 Far End Alarm on Card 2 port 1: RAI signal received

Far End Alarm on Card 2 port 1: RAI signal received

Associated Device: OSB

Group Name: Hardware:

Severity: major

Default Threshold: advantech500i: 0;

Faulty Object: PRI

Maintenance Procedure: A received Remote Alarm Indication means that the PSTN has a problem with the signal that it is receiving from OSB. Firstly, check the cabling. Then check the settings at the remote end and verify that they match OSB port settings. Try to connect this port to another PSTN line. If the new connection clears the alarm, then the problem may occur in the previous PSTN line and the PSTN provider must be contacted.

8.1.6.172 Far End Alarm on Card 2 port 2: RAI signal received

Far End Alarm on Card 2 port 2: RAI signal received

Associated Device: OSB

Group Name: Hardware:

Severity: major

Default Threshold: advantech500i: 0;

Faulty Object: PRI

Maintenance Procedure: A received Remote Alarm Indication means that the PSTN has a problem with the signal that it is receiving from OSB. Firstly, check the cabling. Then check the settings at the remote end and verify that they match OSB port settings. Try to connect this port to another PSTN line. If the new connection clears the alarm, then the problem may occur in the previous PSTN line and the PSTN provider must be contacted.

8.1.6.173 Far End Alarm on Card 2 port 3: RAI signal received

Far End Alarm on Card 2 port 3: RAI signal received

Associated Device: OSB

Group Name: Hardware:

Severity: major

Default Threshold: advantech500i: 0;

Faulty Object: PRI

Maintenance Procedure: A received Remote Alarm Indication means that the PSTN has a problem with the signal that it is receiving from OSB. Firstly, check the cabling. Then check the settings at the remote end and verify that they match OSB port settings. Try to connect this port to another PSTN line. If the new connection clears the alarm, then the problem may occur in the previous PSTN line and the PSTN provider must be contacted.

8.1.6.174 Far End Alarm on Card 2 port 4: RAI signal received

Far End Alarm on Card 2 port 4: RAI signal received

Associated Device: OSB

Group Name: Hardware:

Severity: major

Default Threshold: advantech500i: 0;

Faulty Object: PRI

Maintenance Procedure: A received Remote Alarm Indication means that the PSTN has a problem with the signal that it is receiving from OSB. Firstly, check the cabling. Then check the settings at the remote end and verify that they match OSB port settings. Try to connect this port to another PSTN line. If the new connection clears the alarm, then the problem may occur in the previous PSTN line and the PSTN provider must be contacted.

8.1.6.175 Far End Alarm on Card 2 port 5: RAI signal received

Far End Alarm on Card 2 port 5: RAI signal received

Associated Device: OSB

Group Name: Hardware:

Severity: major

Default Threshold:

Faulty Object: PRI

Maintenance Procedure: A received Remote Alarm Indication means that the PSTN has a problem with the signal that it is receiving from OSB. Firstly, check the cabling. Then check the settings at the remote end and verify that they match OSB port settings. Try to connect this port to another PSTN line. If the new connection clears the alarm, then the problem may occur in the previous PSTN line and the PSTN provider must be contacted.

8.1.6.176 Far End Alarm on Card 2 port 6: RAI signal received

Far End Alarm on Card 2 port 6: RAI signal received

Associated Device: OSB

Group Name: Hardware:

Severity: major

Default Threshold:

Faulty Object: PRI

Maintenance Procedure: A received Remote Alarm Indication means that the PSTN has a problem with the signal that it is receiving from OSB. Firstly, check the cabling. Then check the settings at the remote end and verify that they match OSB port settings. Try to connect this port to another PSTN line. If the new connection clears the alarm, then the problem may occur in the previous PSTN line and the PSTN provider must be contacted.

8.1.6.177 Far End Alarm on Card 2 port 7: RAI signal received

Far End Alarm on Card 2 port 7: RAI signal received

Associated Device: OSB

Group Name: Hardware:

Severity: major

Default Threshold:

Faulty Object: PRI

Maintenance Procedure: A received Remote Alarm Indication means that the PSTN has a problem with the signal that it is receiving from OSB. Firstly, check the cabling. Then check the settings at the remote end and verify that they match OSB port settings. Try to connect this port to another PSTN line. If the new connection clears the alarm, then the problem may occur in the previous PSTN line and the PSTN provider must be contacted.

8.1.6.178 Far End Alarm on Card 2 port 8: RAI signal received

Far End Alarm on Card 2 port 8: RAI signal received

Associated Device: OSB

Group Name: Hardware:

Severity: major

Default Threshold:

Faulty Object: PRI

Maintenance Procedure: A received Remote Alarm Indication means that the PSTN has a problem with the signal that it is receiving from OSB. Firstly, check the cabling. Then check the settings at the remote end and verify that they match OSB port settings. Try to connect this port to another PSTN line. If the new connection clears the alarm, then the problem may occur in the previous PSTN line and the PSTN provider must be contacted.

8.1.6.179 Far End Loopback Activated on Card 1 port 1

Far End Loopback Activated on Card 1 port 1

Associated Device: OSB

Group Name: Hardware:

Severity: major

Default Threshold: advantech500i: 0;

Faulty Object: PRI

Maintenance Procedure: Loopback is a test operation mode. Disable Loopback in PSTN. If the alarm persists, contact the service provider.

8.1.6.180 Far End Loopback Activated on Card 1 port 2

Far End Loopback Activated on Card 1 port 2

Associated Device: OSB

Group Name: Hardware:

Severity: major

Default Threshold: advantech500i: 0;

Faulty Object: PRI

Maintenance Procedure: Loopback is a test operation mode. Disable Loopback in PSTN. If the alarm persists, contact the service provider.

8.1.6.181 Far End Loopback Activated on Card 1 port 3

Far End Loopback Activated on Card 1 port 3

Associated Device: OSB

Group Name: Hardware:

Severity: major

Default Threshold: advantech500i: 0;

Faulty Object: PRI

Maintenance Procedure: Loopback is a test operation mode. Disable Loopback in PSTN. If the alarm persists, contact the service provider.

8.1.6.182 Far End Loopback Activated on Card 1 port 4

Far End Loopback Activated on Card 1 port 4

Associated Device: OSB

Group Name: Hardware:

Severity: major

Default Threshold: advantech500i: 0;

Faulty Object: PRI

Maintenance Procedure: Loopback is a test operation mode. Disable Loopback in PSTN. If the alarm persists, contact the service provider.

8.1.6.183 Far End Loopback Activated on Card 1 port 5

Far End Loopback Activated on Card 1 port 5

Associated Device: OSB

Group Name: Hardware:

Severity: major

Default Threshold:

Faulty Object: PRI

Maintenance Procedure: Loopback is a test operation mode. Disable Loopback in PSTN. If the alarm persists, contact the service provider.

8.1.6.184 Far End Loopback Activated on Card 1 port 6

Far End Loopback Activated on Card 1 port 6

Associated Device: OSB

Group Name: Hardware:

Severity: major

Default Threshold:

Faulty Object: PRI

Maintenance Procedure: Loopback is a test operation mode. Disable Loopback in PSTN. If the alarm persists, contact the service provider.

8.1.6.185 Far End Loopback Activated on Card 1 port 7

Far End Loopback Activated on Card 1 port 7

Associated Device: OSB

Group Name: Hardware:

Severity: major

Default Threshold:

Faulty Object: PRI

Maintenance Procedure: Loopback is a test operation mode. Disable Loopback in PSTN. If the alarm persists, contact the service provider.

8.1.6.186 Far End Loopback Activated on Card 1 port 8

Far End Loopback Activated on Card 1 port 8

Associated Device: OSB

Group Name: Hardware:

Severity: major

Default Threshold:

Faulty Object: PRI

Maintenance Procedure: Loopback is a test operation mode. Disable Loopback in PSTN. If the alarm persists, contact the service provider.

8.1.6.187 Far End Loopback Activated on Card 2 port 1

Far End Loopback Activated on Card 2 port 1

Associated Device: OSB

Group Name: Hardware:

Severity: major

Default Threshold: advantech500i: 0;

Faulty Object: PRI

Maintenance Procedure: Loopback is a test operation mode. Disable Loopback in PSTN. If the alarm persists, contact the service provider.

8.1.6.188 Far End Loopback Activated on Card 2 port 2

Far End Loopback Activated on Card 2 port 2

Associated Device: OSB

Group Name: Hardware:

Severity: major

Default Threshold: advantech500i: 0;

Faulty Object: PRI

Maintenance Procedure: Loopback is a test operation mode. Disable Loopback in PSTN. If the alarm persists, contact the service provider.

8.1.6.189 Far End Loopback Activated on Card 2 port 3

Far End Loopback Activated on Card 2 port 3

Associated Device: OSB

Group Name: Hardware:

Severity: major

Default Threshold: advantech500i: 0;

Faulty Object: PRI

Maintenance Procedure: Loopback is a test operation mode. Disable Loopback in PSTN. If the alarm persists, contact the service provider.

8.1.6.190 Far End Loopback Activated on Card 2 port 4

Far End Loopback Activated on Card 2 port 4

Associated Device: OSB

Group Name: Hardware:

Severity: major

Default Threshold: advantech500i: 0;

Faulty Object: PRI

Maintenance Procedure: Loopback is a test operation mode. Disable Loopback in PSTN. If the alarm persists, contact the service provider.

8.1.6.191 Far End Loopback Activated on Card 2 port 5

Far End Loopback Activated on Card 2 port 5

Associated Device: OSB

Group Name: Hardware:

Severity: major

Default Threshold:

Faulty Object: PRI

Maintenance Procedure: Loopback is a test operation mode. Disable Loopback in PSTN. If the alarm persists, contact the service provider.

8.1.6.192 Far End Loopback Activated on Card 2 port 6

Far End Loopback Activated on Card 2 port 6

Associated Device: OSB

Group Name: Hardware:

Severity: major

Default Threshold:

Faulty Object: PRI

Maintenance Procedure: Loopback is a test operation mode. Disable Loopback in PSTN. If the alarm persists, contact the service provider.

8.1.6.193 Far End Loopback Activated on Card 2 port 7

Far End Loopback Activated on Card 2 port 7

Associated Device: OSB

Group Name: Hardware:

Severity: major

Default Threshold:

Faulty Object: PRI

Maintenance Procedure: Loopback is a test operation mode. Disable Loopback in PSTN. If the alarm persists, contact the service provider.

8.1.6.194 Far End Loopback Activated on Card 2 port 8

Far End Loopback Activated on Card 2 port 8

Associated Device: OSB

Group Name: Hardware:

Severity: major

Default Threshold:

Faulty Object: PRI

Maintenance Procedure: Loopback is a test operation mode. Disable Loopback in PSTN. If the alarm persists, contact the service provider.

8.1.6.195 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;

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.

8.1.6.196 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:

8.1.6.197 FXS Ring Voltage Lost on Card 1

FXS Ring Voltage Lost on Card 1

Associated Device: OSB

Group Name: Hardware

Severity: critical

Default Threshold: advantech50i: 0;

Faulty Object: FXS

Maintenance Procedure: Verify if the FXS power cable is not connected. If so, reconnect it again and restart the system. If it does not work, open the OSB box and verify if the source cable is connected to the FXS board. If not, connect them.

8.1.6.198 FXS Ring Voltage Lost on Card 2

FXS Ring Voltage Lost on Card 2

Associated Device: OSB

Group Name: Hardware

Severity: critical

Default Threshold: advantech50i: 0;

Faulty Object: FXS

Maintenance Procedure: Verify if the FXS power cable is not connected. If so, reconnect it again and restart the system. If it does not work, open the OSB box and verify if the source cable is connected to the FXS board. If not, connect them.

8.1.6.199 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.

8.1.6.200 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.

8.1.6.201 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.

8.1.6.202 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

8.1.6.203 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;

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.

8.1.6.204 High CPU temperature

High CPU temperature

Associated Device: OSB, SBC

Group Name: Hardware

Severity: critical

Default Threshold: advantech250: 60; advantech50i: 60; advantech500i: 60;

Faulty Object: HW-Sensors

Maintenance Procedure: Change CPU to fix this problem.

8.1.6.205 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;

Faulty Object: Voice channels

Maintenance Procedure:

8.1.6.206 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;

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.

8.1.6.207 High system board temperature

High system board temperature.

Associated Device: OSB, SBC

Group Name: Hardware:

Severity: critical

Default Threshold: rx200: 65; rx330: 65;

Faulty Object: HW-Sensors

Maintenance Procedure:

8.1.6.208 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;

Faulty Object: HW-Sensors

Maintenance Procedure:

8.1.6.209 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:

8.1.6.210 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;

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.

8.1.6.211 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;

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.

8.1.6.212 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.

8.1.6.213 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;

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 than 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.

8.1.6.214 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;

Faulty Object: License

Maintenance Procedure: The system is running without license. To solve this enter a valid license.

8.1.6.215 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;

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.

8.1.6.216 Could not contact license server

License server is either not configured or not reachable

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: Verify that the license server address is correctly configured in the system. If correctly configured, check the connectivity between the system and the license server.

8.1.6.217 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;

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.

8.1.6.218 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;

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.

8.1.6.219 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;

Faulty Object: License

Maintenance Procedure:

8.1.6.220 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;

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.

8.1.6.221 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;

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.

8.1.6.222 Loss of Clock on Card 1 port 1

Loss of Clock on Card 1 port 1

Associated Device: OSB

Group Name: Communication

Severity: major

Default Threshold: advantech500i: 0;

Faulty Object: PRI Interface

Maintenance Procedure: Clock with a higher priority was lost on OSB port. Check if the port has any other alarms. If so, try to correct the other alarms. If the problem persists, contact PSTN service provider.

8.1.6.223 Loss of Clock on Card 1 port 2

Loss of Clock on Card 1 port 2

Associated Device: OSB

Group Name: Communication

Severity: major

Default Threshold: advantech500i: 0;

Faulty Object: PRI Interface

Maintenance Procedure: Clock with a higher priority was lost on OSB port. Check if the port has any other alarms. If so, try to correct the other alarms. If the problem persists, contact PSTN service provider.

8.1.6.224 Loss of Clock on Card 1 port 3

Loss of Clock on Card 1 port 3

Associated Device: OSB

Group Name: Communication

Severity: major

Default Threshold: advantech500i: 0;

Faulty Object: PRI Interface

Maintenance Procedure: Clock with a higher priority was lost on OSB port. Check if the port has any other alarms. If so, try to correct the other alarms. If the problem persists, contact PSTN service provider.

8.1.6.225 Loss of Clock on Card 1 port 4

Loss of Clock on Card 1 port 4

Associated Device: OSB

Group Name: Communication

Severity: major

Default Threshold: advantech500i: 0;

Faulty Object: PRI Interface

Maintenance Procedure: Clock with a higher priority was lost on OSB port. Check if the port has any other alarms. If so, try to correct the other alarms. If the problem persists, contact PSTN service provider.

8.1.6.226 Loss of Clock on Card 2 port 1

Loss of Clock on Card 2 port 1

Associated Device: OSB

Group Name: Communication

Severity: major

Default Threshold: advantech500i: 0;

Faulty Object: PRI Interface

Maintenance Procedure: Clock with a higher priority was lost on OSB port. Check if the port has any other alarms. If so, try to correct the other alarms. If the problem persists, contact PSTN service provider.

8.1.6.227 Loss of Clock on Card 2 port 2

Loss of Clock on Card 2 port 2

Associated Device: OSB

Group Name: Communication

Severity: major

Default Threshold: advantech500i: 0;

Faulty Object: PRI Interface

Maintenance Procedure: Clock with a higher priority was lost on OSB port. Check if the port has any other alarms. If so, try to correct the other alarms. If the problem persists, contact PSTN service provider.

8.1.6.228 Loss of Clock on Card 2 port 3

Loss of Clock on Card 2 port 3

Associated Device: OSB

Group Name: Communication

Severity: major

Default Threshold: advantech500i: 0;

Faulty Object: PRI Interface

Maintenance Procedure: Clock with a higher priority was lost on OSB port. Check if the port has any other alarms. If so, try to correct the other alarms. If the problem persists, contact PSTN service provider.

8.1.6.229 Loss of Clock on Card 2 port 4

Loss of Clock on Card 2 port 4

Associated Device: OSB

Group Name: Communication

Severity: major

Default Threshold: advantech500i: 0;

Faulty Object: PRI Interface

Maintenance Procedure: Clock with a higher priority was lost on OSB port. Check if the port has any other alarms. If so, try to correct the other alarms. If the problem persists, contact PSTN service provider.

8.1.6.230 Redundant system not reachable via alternate interface

The redundant system is not reachable via alternate interface cable connection

Associated Device: OSB,SBC

Group Name: Communication

Severity: major

Default Threshold: advantech500i: 0;

Faulty Object: Alternate Interface for the PRI Redundancy

Maintenance Procedure: This may indicate a failure in the redundant system partner (e.g. hardware failure, power off, etc). Also this may indicate a problem in either the USB network adapters or in the network cable.

8.1.6.231 Switchover due to PRI threshold

Switchover due to PRI threshold-This node is switching over to backup because it reached the threshold of failing PRI links

Associated Device: OSB,SBC

Group Name: Communication

Severity: major

Default Threshold: advantech500i: 0;

Faulty Object: Number of active PRI links on node

Maintenance Procedure: This may indicate a failure with the cable(s) of the splitter box or a failure on the the hardware of the line card(s).

8.1.6.232 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;

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.

8.1.6.233 Loss of communication with billing server

Loss of communication with billing 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;

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.

8.1.6.234 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;

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.

8.1.6.235 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;

Faulty Object: File server link

Maintenance Procedure:

8.1.6.236 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;

Faulty Object: GATEWAY link

Maintenance Procedure: This alarm indicates that the network gateway is not reachable. Check the network gateway configuration and network connections.

8.1.6.237 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;

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.

8.1.6.238 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;

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.

8.1.6.239 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;

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.

8.1.6.240 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;

Faulty Object: Node2 Primary OSV link

Maintenance Procedure:

8.1.6.241 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;

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.

8.1.6.242 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;

Faulty Object: Redundancy

Maintenance Procedure:

8.1.6.243 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;

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.

8.1.6.244 Loss of communication with surveillance system

Loss of communication with surveillance 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;

Faulty Object: Surveillance system link

Maintenance Procedure:

8.1.6.245 Loss of Signal on Card 1 port 1

Loss of Signal on Card 1 port 1

Associated Device: OSB

Group Name: Hardware:

Severity: major

Default Threshold: advantech50i: 0; advantech500i: 0;

Faulty Object: PRI

Maintenance Procedure: Firstly, make sure that the cable between the OSB PRI port and the PSTN service provider is connected correctly. Check to see if the cable is hooked up to the correct ports. If necessary, correct the cable connections. Then, check cable integrity. There could be breaks or other physical abnormalities in the cable. Ensure that the pinouts are set correctly. A cable replacement, may be needed if necessary. Check the cable connectors. If transmit and receive pairs are reverse, they can cause errors.

8.1.6.246 Loss of Signal on Card 1 port 2

Loss of Signal on Card 1 port 2

Associated Device: OSB

Group Name: Hardware:

Severity: major

Default Threshold: advantech50i: 0; advantech500i: 0;

Faulty Object: PRI

Maintenance Procedure: Firstly, make sure that the cable between the OSB PRI port and the PSTN service provider is connected correctly. Check to see if the cable is hooked up to the correct ports. If necessary, correct the cable connections. Then, check cable integrity. There could be breaks or other physical abnormalities in the cable. Ensure that the pinouts are set correctly. A cable replacement, may be needed if necessary. Check the cable connectors. If transmit and receive pairs are reverse, they can cause errors.

8.1.6.247 Loss of Signal on Card 1 port 3

Loss of Signal on Card 1 port 3

Associated Device: OSB

Group Name: Hardware:

Severity: major

Default Threshold: advantech50i: 0; advantech500i: 0;

Faulty Object: PRI

Maintenance Procedure: Firstly, make sure that the cable between the OSB PRI port and the PSTN service provider is connected correctly. Check to see if the cable is hooked up to the correct ports. If necessary, correct the cable connections. Then, check cable integrity. There could be breaks or other physical abnormalities in the cable. Ensure that the pinouts are set correctly. A cable replacement, may be needed if necessary. Check the cable connectors. If transmit and receive pairs are reverse, they can cause errors.

8.1.6.248 Loss of Signal on Card 1 port 4

Loss of Signal on Card 1 port 4

Associated Device: OSB

Group Name: Hardware:

Severity: major

Default Threshold: advantech50i: 0; advantech500i: 0;

Faulty Object: PRI

Maintenance Procedure: Firstly, make sure that the cable between the OSB PRI port and the PSTN service provider is connected correctly. Check to see if the cable is hooked up to the correct ports. If necessary, correct the cable connections. Then, check cable integrity. There could be breaks or other physical abnormalities in the cable. Ensure that the pinouts are set correctly. A cable replacement, may be needed if necessary. Check the cable connectors. If transmit and receive pairs are reverse, they can cause errors.

8.1.6.249 Loss of Signal on Card 1 port 5

Loss of Signal on Card 1 port 5

Associated Device: OSB

Group Name: Hardware:

Severity: major

Default Threshold: advantech50i: 0; advantech500i: 0;

Faulty Object: PRI

Maintenance Procedure: Firstly, make sure that the cable between the OSB PRI port and the PSTN service provider is connected correctly. Check to see if the cable is hooked up to the correct ports. If necessary, correct the cable connections. Then, check cable integrity. There could be breaks or other physical abnormalities in the cable. Ensure that the pinouts are set correctly. A cable replacement, may be needed if necessary. Check the cable connectors. If transmit and receive pairs are reverse, they can cause errors.

8.1.6.250 Loss of Signal on Card 1 port 6

Loss of Signal on Card 1 port 6

Associated Device: OSB

Group Name: Hardware:

Severity: major

Default Threshold: advantech50i: 0; advantech500i: 0;

Faulty Object: PRI

Maintenance Procedure: Firstly, make sure that the cable between the OSB PRI port and the PSTN service provider is connected correctly. Check to see

if the cable is hooked up to the correct ports. If necessary, correct the cable connections. Then, check cable integrity. There could be breaks or other physical abnormalities in the cable. Ensure that the pinouts are set correctly. A cable replacement, may be needed if necessary. Check the cable connectors. If transmit and receive pairs are reverse, they can cause errors.

8.1.6.251 Loss of Signal on Card 1 port 7

Loss of Signal on Card 1 port 7

Associated Device: OSB

Group Name: Hardware:

Severity: major

Default Threshold: advantech50i: 0; advantech500i: 0;

Faulty Object: PRI

Maintenance Procedure: Firstly, make sure that the cable between the OSB PRI port and the PSTN service provider is connected correctly. Check to see if the cable is hooked up to the correct ports. If necessary, correct the cable connections. Then, check cable integrity. There could be breaks or other physical abnormalities in the cable. Ensure that the pinouts are set correctly. A cable replacement, may be needed if necessary. Check the cable connectors. If transmit and receive pairs are reverse, they can cause errors.

8.1.6.252 Loss of Signal on Card 1 port 8

Loss of Signal on Card 1 port 8

Associated Device: OSB

Group Name: Hardware:

Severity: major

Default Threshold: advantech50i: 0; advantech500i: 0;

Faulty Object: PRI

Maintenance Procedure: Firstly, make sure that the cable between the OSB PRI port and the PSTN service provider is connected correctly. Check to see if the cable is hooked up to the correct ports. If necessary, correct the cable connections. Then, check cable integrity. There could be breaks or other physical abnormalities in the cable. Ensure that the pinouts are set correctly. A cable replacement, may be needed if necessary. Check the cable connectors. If transmit and receive pairs are reverse, they can cause errors.

8.1.6.253 Loss of Signal on Card 2 port 1

Loss of Signal on Card 2 port 1

Associated Device: OSB

Group Name: Hardware:

Severity: major

Default Threshold: advantech50i: 0; advantech500i: 0;

Faulty Object: PRI

Maintenance Procedure: Firstly, make sure that the cable between the OSB PRI port and the PSTN service provider is connected correctly. Check to see if the cable is hooked up to the correct ports. If necessary, correct the cable connections. Then, check cable integrity. There could be breaks or other physical abnormalities in the cable. Ensure that the pinouts are set correctly. A cable replacement, may be needed if necessary. Check the cable connectors. If transmit and receive pairs are reverse, they can cause errors.

8.1.6.254 Loss of Signal on Card 2 port 2

Loss of Signal on Card 2 port 2

Associated Device: OSB

Group Name: Hardware:

Severity: major

Default Threshold: advantech50i: 0; advantech500i: 0;

Faulty Object: PRI

Maintenance Procedure: Firstly, make sure that the cable between the OSB PRI port and the PSTN service provider is connected correctly. Check to see if the cable is hooked up to the correct ports. If necessary, correct the cable connections. Then, check cable integrity. There could be breaks or other physical abnormalities in the cable. Ensure that the pinouts are set correctly. A cable replacement, may be needed if necessary. Check the cable connectors. If transmit and receive pairs are reverse, they can cause errors.

8.1.6.255 Loss of Signal on Card 2 port 3

Loss of Signal on Card 2 port 3

Associated Device: OSB

Group Name: Hardware:

Severity: major

Default Threshold: advantech50i: 0; advantech500i: 0;

Faulty Object: PRI

Maintenance Procedure: Firstly, make sure that the cable between the OSB PRI port and the PSTN service provider is connected correctly. Check to see if the cable is hooked up to the correct ports. If necessary, correct the cable connections. Then, check cable integrity. There could be breaks or other physical abnormalities in the cable. Ensure that the pinouts are set correctly. A cable replacement, may be needed if necessary. Check the cable connectors. If transmit and receive pairs are reverse, they can cause errors.

8.1.6.256 Loss of Signal on Card 2 port 4

Loss of Signal on Card 2 port 4

Associated Device: OSB

Group Name: Hardware:

Severity: major

Default Threshold: advantech50i: 0; advantech500i: 0;

Faulty Object: PRI

Maintenance Procedure: Firstly, make sure that the cable between the OSB PRI port and the PSTN service provider is connected correctly. Check to see if the cable is hooked up to the correct ports. If necessary, correct the cable connections. Then, check cable integrity. There could be breaks or other physical abnormalities in the cable. Ensure that the pinouts are set correctly. A cable replacement, may be needed if necessary. Check the cable connectors. If transmit and receive pairs are reverse, they can cause errors.

8.1.6.257 Loss of Signal on Card 2 port 5

Loss of Signal on Card 2 port 5

Associated Device: OSB

Group Name: Hardware:

Severity: major

Default Threshold: advantech50i: 0; advantech500i: 0;

Faulty Object: PRI

Maintenance Procedure: Firstly, make sure that the cable between the OSB PRI port and the PSTN service provider is connected correctly. Check to see if the cable is hooked up to the correct ports. If necessary, correct the cable connections. Then, check cable integrity. There could be breaks or other physical abnormalities in the cable. Ensure that the pinouts are set correctly. A cable replacement, may be needed if necessary. Check the cable connectors. If transmit and receive pairs are reverse, they can cause errors.

8.1.6.258 Loss of Signal on Card 2 port 6

Loss of Signal on Card 2 port 6

Associated Device: OSB

Group Name: Hardware:

Severity: major

Default Threshold: advantech50i: 0; advantech500i: 0;

Faulty Object: PRI

Maintenance Procedure: Firstly, make sure that the cable between the OSB PRI port and the PSTN service provider is connected correctly. Check to see

if the cable is hooked up to the correct ports. If necessary, correct the cable connections. Then, check cable integrity. There could be breaks or other physical abnormalities in the cable. Ensure that the pinouts are set correctly. A cable replacement, may be needed if necessary. Check the cable connectors. If transmit and receive pairs are reverse, they can cause errors.

8.1.6.259 Loss of Signal on Card 2 port 7

Loss of Signal on Card 2 port 7

Associated Device: OSB

Group Name: Hardware:

Severity: major

Default Threshold: advantech50i: 0; advantech500i: 0;

Faulty Object: PRI

Maintenance Procedure: Firstly, make sure that the cable between the OSB PRI port and the PSTN service provider is connected correctly. Check to see if the cable is hooked up to the correct ports. If necessary, correct the cable connections. Then, check cable integrity. There could be breaks or other physical abnormalities in the cable. Ensure that the pinouts are set correctly. A cable replacement, may be needed if necessary. Check the cable connectors. If transmit and receive pairs are reverse, they can cause errors.

8.1.6.260 Loss of Signal on Card 2 port 8

Loss of Signal on Card 2 port 8

Associated Device: OSB

Group Name: Hardware:

Severity: major

Default Threshold: advantech50i: 0; advantech500i: 0;

Faulty Object: PRI

Maintenance Procedure: Firstly, make sure that the cable between the OSB PRI port and the PSTN service provider is connected correctly. Check to see if the cable is hooked up to the correct ports. If necessary, correct the cable connections. Then, check cable integrity. There could be breaks or other physical abnormalities in the cable. Ensure that the pinouts are set correctly. A cable replacement, may be needed if necessary. Check the cable connectors. If transmit and receive pairs are reverse, they can cause errors.

8.1.6.261 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:

8.1.6.262 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:

8.1.6.263 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:

8.1.6.264 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:

8.1.6.265 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:

8.1.6.266 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:

8.1.6.267 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:

8.1.6.268 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:

8.1.6.269 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:

8.1.6.270 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:

8.1.6.271 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:

8.1.6.272 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:

8.1.6.273 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:

8.1.6.274 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:

8.1.6.275 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:

8.1.6.276 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:

8.1.6.277 Low fan speed PSU 1(S7)

Low fan 1 speed PSU 1(S7)

Associated Device: OSB, SBC

Group Name: Hardware:

Severity: major

Default Threshold: rx200: 400;

Faulty Object: HW-Sensors

Maintenance Procedure: Change fan to fix this problem

8.1.6.278 Low fan speed PSU 2(S7)

Low fan 1 speed PSU 2(S7)

Associated Device: OSB, SBC

Group Name: Hardware:

Severity: major

Default Threshold: rx200: 400;

Faulty Object: HW-Sensors

Maintenance Procedure: Change fan to fix this problem

8.1.6.279 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:

8.1.6.280 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:

8.1.6.281 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:

8.1.6.282 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:

8.1.6.283 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:

8.1.6.284 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:

8.1.6.285 Media Server not running

Media Server 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;

Faulty Object: Media Server

Maintenance Procedure: Process Manager has a mechanism to restart automatically the applications that are not running. If the Media Server is still not running after several restarts by PM check the mediaserver logs to see the root cause. As last resource proceed to a restart to backup.

8.1.6.286 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;

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.

8.1.6.287 Near End Alarm on Card 1 port 1: LOF/LFA

Near End Alarm on Card 1 port 1: LOF/LFA

Associated Device: OSB

Group Name: Hardware:

Severity: major

Default Threshold: advantech50i: 0; advantech500i: 0;

Faulty Object: PRI

Maintenance Procedure: Check if the framing format configured on OSB port matches the framing format of the PSTN line. Try to modify the framing format. Change the line build out configuration on the OSB port.

8.1.6.288 Near End Alarm on Card 1 port 2: LOF/LFA

Near End Alarm on Card 1 port 2: LOF/LFA

Associated Device: OSB

Group Name: Hardware:

Severity: major

Default Threshold: advantech50i: 0; advantech500i: 0;

Faulty Object: PRI

Maintenance Procedure: Check if the framing format configured on OSB port matches the framing format of the PSTN line. Try to modify the framing format. Change the line build out configuration on the OSB port.

8.1.6.289 Near End Alarm on Card 1 port 3: LOF/LFA

Near End Alarm on Card 1 port 3: LOF/LFA

Associated Device: OSB

Group Name: Hardware:

Severity: major

Default Threshold: advantech50i: 0; advantech500i: 0;

Faulty Object: PRI

Maintenance Procedure: Check if the framing format configured on OSB port matches the framing format of the PSTN line. Try to modify the framing format. Change the line build out configuration on the OSB port.

8.1.6.290 Near End Alarm on Card 1 port 4: LOF/LFA

Near End Alarm on Card 1 port 4: LOF/LFA

Associated Device: OSB

Group Name: Hardware:

Severity: major

Default Threshold: advantech50i: 0; advantech500i: 0;

Faulty Object: PRI

Maintenance Procedure: Check if the framing format configured on OSB port matches the framing format of the PSTN line. Try to modify the framing format. Change the line build out configuration on the OSB port.

8.1.6.291 Near End Alarm on Card 1 port 5: LOF/LFA

Near End Alarm on Card 1 port 5: LOF/LFA

Associated Device: OSB

Group Name: Hardware:

Severity: major

Default Threshold: advantech50i: 0; advantech500i: 0;

Faulty Object: PRI

Maintenance Procedure: Check if the framing format configured on OSB port matches the framing format of the PSTN line. Try to modify the framing format. Change the line build out configuration on the OSB port.

8.1.6.292 Near End Alarm on Card 1 port 6: LOF/LFA

Near End Alarm on Card 1 port 6: LOF/LFA

Associated Device: OSB

Group Name: Hardware:

Severity: major

Default Threshold: advantech50i: 0; advantech500i: 0;

Faulty Object: PRI

Maintenance Procedure: Check if the framing format configured on OSB port matches the framing format of the PSTN line. Try to modify the framing format. Change the line build out configuration on the OSB port.

8.1.6.293 Near End Alarm on Card 1 port 7: LOF/LFA

Near End Alarm on Card 1 port 7: LOF/LFA

Associated Device: OSB

Group Name: Hardware:

Severity: major

Default Threshold: advantech50i: 0; advantech500i: 0;

Faulty Object: PRI

Maintenance Procedure: Check if the framing format configured on OSB port matches the framing format of the PSTN line. Try to modify the framing format. Change the line build out configuration on the OSB port.

8.1.6.294 Near End Alarm on Card 1 port 8: LOF/LFA

Near End Alarm on Card 1 port 8: LOF/LFA

Associated Device: OSB

Group Name: Hardware:

Severity: major

Default Threshold: advantech50i: 0; advantech500i: 0;

Faulty Object: PRI

Maintenance Procedure: Check if the framing format configured on OSB port matches the framing format of the PSTN line. Try to modify the framing format. Change the line build out configuration on the OSB port.

8.1.6.295 Near End Loopback activated on Card 1 port 1

Near End Loopback activated on Card 1 port 1

Associated Device: OSB

Group Name: Hardware:

Severity: major

Default Threshold: advantech50i: 0; advantech500i: 0;

Faulty Object: PRI

Maintenance Procedure: Loopback is a test operation mode. Disable loopback on OSB port.

8.1.6.296 Near End Loopback activated on Card 1 port 2

Near End Loopback activated on Card 1 port 2

Associated Device: OSB

Group Name: Hardware:

Severity: major

Default Threshold: advantech50i: 0; advantech500i: 0;

Faulty Object: PRI

Maintenance Procedure: Loopback is a test operation mode. Disable loopback on OSB port.

8.1.6.297 Near End Loopback activated on Card 1 port 3

Near End Loopback activated on Card 1 port 3

Associated Device: OSB

Group Name: Hardware:

Severity: major

Default Threshold: advantech50i: 0; advantech500i: 0;

Faulty Object: PRI

Maintenance Procedure: Loopback is a test operation mode. Disable loopback on OSB port.

8.1.6.298 Near End Loopback activated on Card 1 port 4

Near End Loopback activated on Card 1 port 4

Associated Device: OSB

Group Name: Hardware:

Severity: major

Default Threshold: advantech50i: 0; advantech500i: 0;

Faulty Object: PRI

Maintenance Procedure: Loopback is a test operation mode. Disable loopback on OSB port.

8.1.6.299 Near End Loopback activated on Card 1 port 5

Near End Loopback activated on Card 1 port 5

Associated Device: OSB

Group Name: Hardware:

Severity: major

Default Threshold: advantech50i: 0; advantech500i: 0;

Faulty Object: PRI

Maintenance Procedure: Loopback is a test operation mode. Disable loopback on OSB port.

8.1.6.300 Near End Loopback activated on Card 1 port 6

Near End Loopback activated on Card 1 port 6

Associated Device: OSB

Group Name: Hardware:

Severity: major

Default Threshold: advantech50i: 0; advantech500i: 0;

Faulty Object: PRI

Maintenance Procedure: Loopback is a test operation mode. Disable loopback on OSB port.

8.1.6.301 Near End Loopback activated on Card 1 port 7

Near End Loopback activated on Card 1 port 7

Associated Device: OSB

Group Name: Hardware:

Severity: major

Default Threshold: advantech50i: 0; advantech500i: 0;

Faulty Object: PRI

Maintenance Procedure: Loopback is a test operation mode. Disable loopback on OSB port.

8.1.6.302 Near End Loopback activated on Card 1 port 8

Near End Loopback activated on Card 1 port 8

Associated Device: OSB

Group Name: Hardware:

Severity: major

Default Threshold: advantech50i: 0; advantech500i: 0;

Faulty Object: PRI

Maintenance Procedure: Loopback is a test operation mode. Disable loopback on OSB port.

8.1.6.303 Near End Alarm on Card 2 port 1: LOF/LFA

Near End Alarm on Card 2 port 1: LOF/LFA

Associated Device: OSB

Group Name: Hardware:

Severity: major

Default Threshold: advantech50i: 0; advantech500i: 0;

Faulty Object: PRI

Maintenance Procedure: Check if the framing format configured on OSB port matches the framing format of the PSTN line. Try to modify the framing format. Change the line build out configuration on the OSB port.

8.1.6.304 Near End Alarm on Card 2 port 2: LOF/LFA

Near End Alarm on Card 2 port 2: LOF/LFA

Associated Device: OSB

Group Name: Hardware:

Severity: major

Default Threshold: advantech50i: 0; advantech500i: 0;

Faulty Object: PRI

Maintenance Procedure: Check if the framing format configured on OSB port matches the framing format of the PSTN line. Try to modify the framing format. Change the line build out configuration on the OSB port.

8.1.6.305 Near End Alarm on Card 2 port 3: LOF/LFA

Near End Alarm on Card 2 port 3: LOF/LFA

Associated Device: OSB

Group Name: Hardware:

Severity: major

Default Threshold: advantech50i: 0; advantech500i: 0;

Faulty Object: PRI

Maintenance Procedure: Check if the framing format configured on OSB port matches the framing format of the PSTN line. Try to modify the framing format. Change the line build out configuration on the OSB port.

8.1.6.306 Near End Alarm on Card 2 port 4: LOF/LFA

Near End Alarm on Card 2 port 4: LOF/LFA

Associated Device: OSB

Group Name: Hardware:

Severity: major

Default Threshold: advantech50i: 0; advantech500i: 0;

Faulty Object: PRI

Maintenance Procedure: Check if the framing format configured on OSB port matches the framing format of the PSTN line. Try to modify the framing format. Change the line build out configuration on the OSB port.

8.1.6.307 Near End Alarm on Card 2 port 5: LOF/LFA

Near End Alarm on Card 2 port 5: LOF/LFA

Associated Device: OSB

Group Name: Hardware:

Severity: major

Default Threshold: advantech50i: 0; advantech500i: 0;

Faulty Object: PRI

Maintenance Procedure: Check if the framing format configured on OSB port matches the framing format of the PSTN line. Try to modify the framing format. Change the line build out configuration on the OSB port.

8.1.6.308 Near End Alarm on Card 2 port 6: LOF/LFA

Near End Alarm on Card 2 port 6: LOF/LFA

Associated Device: OSB

Group Name: Hardware:

Severity: major

Default Threshold: advantech50i: 0; advantech500i: 0;

Faulty Object: PRI

Maintenance Procedure: Check if the framing format configured on OSB port matches the framing format of the PSTN line. Try to modify the framing format. Change the line build out configuration on the OSB port.

8.1.6.309 Near End Alarm on Card 2 port 7: LOF/LFA

Near End Alarm on Card 2 port 7: LOF/LFA

Associated Device: OSB

Group Name: Hardware:

Severity: major

Default Threshold: advantech50i: 0; advantech500i: 0;

Faulty Object: PRI

Maintenance Procedure: Check if the framing format configured on OSB port matches the framing format of the PSTN line. Try to modify the framing format. Change the line build out configuration on the OSB port.

8.1.6.310 Near End Alarm on Card 2 port 8: LOF/LFA

Near End Alarm on Card 2 port 8: LOF/LFA

Associated Device: OSB

Group Name: Hardware:

Severity: major

Default Threshold: advantech50i: 0; advantech500i: 0;

Faulty Object: PRI

Maintenance Procedure: Check if the framing format configured on OSB port matches the framing format of the PSTN line. Try to modify the framing format. Change the line build out configuration on the OSB port.

8.1.6.311 Near End Loopback activated on Card 2 port 1

Near End Loopback activated on Card 2 port 1

Associated Device: OSB

Group Name: Hardware

Severity: major

Default Threshold: advantech50i: 0; advantech500i: 0;

Faulty Object: PRI

Maintenance Procedure: Loopback is a test operation mode. Disable loopback on OSB port.

8.1.6.312 Near End Loopback activated on Card 2 port 2

Near End Loopback activated on Card 2 port 2

Associated Device: OSB

Group Name: Hardware

Severity: major

Default Threshold: advantech50i: 0; advantech500i: 0;

Faulty Object: PRI

Maintenance Procedure: Loopback is a test operation mode. Disable loopback on OSB port.

8.1.6.313 Near End Loopback activated on Card 2 port 3

Near End Loopback activated on Card 2 port 3

Associated Device: OSB

Group Name: Hardware

Severity: major

Default Threshold: advantech50i: 0; advantech500i: 0;

Faulty Object: PRI

Maintenance Procedure: Loopback is a test operation mode. Disable loopback on OSB port.

8.1.6.314 Near End Loopback activated on Card 2 port 4

Near End Loopback activated on Card 2 port 4

Associated Device: OSB

Group Name: Hardware

Severity: major

Default Threshold: advantech50i: 0; advantech500i: 0;

Faulty Object: PRI

Maintenance Procedure: Loopback is a test operation mode. Disable loopback on OSB port.

8.1.6.315 Near End Loopback activated on Card 2 port 5

Near End Loopback activated on Card 2 port 5

Associated Device: OSB

Group Name: Hardware

Severity: major

Default Threshold: advantech50i: 0; advantech500i: 0;

Faulty Object: PRI

Maintenance Procedure: Loopback is a test operation mode. Disable loopback on OSB port.

8.1.6.316 Near End Loopback activated on Card 2 port 6

Near End Loopback activated on Card 2 port 6

Associated Device: OSB

Group Name: Hardware

Severity: major

Default Threshold: advantech50i: 0; advantech500i: 0;

Faulty Object: PRI

Maintenance Procedure: Loopback is a test operation mode. Disable loopback on OSB port.

8.1.6.317 Near End Loopback activated on Card 2 port 7

Near End Loopback activated on Card 2 port 7

Associated Device: OSB

Group Name: Hardware

Severity: major

Default Threshold: advantech50i: 0; advantech500i: 0;

Faulty Object: PRI

Maintenance Procedure: Loopback is a test operation mode. Disable loopback on OSB port.

8.1.6.318 Near End Loopback activated on Card 2 port 8

Near End Loopback activated on Card 2 port 8

Associated Device: OSB

Group Name: Hardware

Severity: major

Default Threshold: advantech50i: 0; advantech500i: 0;

Faulty Object: PRI

Maintenance Procedure: Loopback is a test operation mode. Disable loopback on OSB port.

8.1.6.319 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.

8.1.6.320 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;

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.

8.1.6.321 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;

Faulty Object: BLC

Maintenance Procedure: Check why no BackupLink call is completing.

8.1.6.322 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;

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.

8.1.6.323 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:

8.1.6.324 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;

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'.

8.1.6.325 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.

8.1.6.326 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;

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.

8.1.6.327 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;

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.

8.1.6.328 Port 3 failure

Port 3 failure

Associated Device: OSB, SBC

Group Name: Ethernet

Severity: major

Default Threshold: rx200: 0; x3250: 0; x3550: 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.

8.1.6.329 Port 4 failure

Port 4 failure

Associated Device: OSB, SBC

Group Name: Ethernet

Severity: major

Default Threshold: rx200: 0; x3250: 0; x3550: 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.

8.1.6.330 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:

8.1.6.331 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:

8.1.6.332 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;

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.

8.1.6.333 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.

8.1.6.334 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:

8.1.6.335 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:

8.1.6.336 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;

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.

8.1.6.337 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;

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.

8.1.6.338 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;

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.

8.1.6.339 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;

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.

8.1.6.340 Rejected to add Backup Link channel

BLS rejected to add Backup Link channel. The limit of links or channels has been achieved on BLS.

Associated Device: OSB

Group Name: Communication

Severity: major

Default Threshold: rx200: 0; rx330: 0; advantech250: 0; advantech50i: 0; advantech500i: 0; x3250: 0; x3550: 0;

Faulty Object: BLC

Maintenance Procedure: Check BLS configuration. Consider increasing number of links or channels. Also consider increasing BLC priority.

8.1.6.341 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;

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.

8.1.6.342 SBC Session denied due to license

SBC Session denied 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;

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.

8.1.6.343 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.

8.1.6.344 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;

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.

8.1.6.345 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;

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.

8.1.6.346 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;

Faulty Object: SIP Server

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.

8.1.6.347 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.

8.1.6.348 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;

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.

8.1.6.349 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;

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.

8.1.6.350 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;

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.

8.1.6.351 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;

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.

8.1.6.352 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:

8.1.6.353 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;

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.

8.1.6.354 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:

8.1.6.355 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:

8.1.6.356 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;

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.

8.1.6.357 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;

Faulty Object: VRRPD

Maintenance Procedure:

8.1.6.358 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;

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.

8.2 Replacing OSB Voice Prompts

OpenScape Branch provides three features that use sound files:

- Automatic Call Distribution Groups
- Auto Attendant
- Voice Mail

NOTICE:

By default, OSB only supports the English language for those features. All three features provide mechanism to upload customized announcements, however it is not allowed for all sound files used in the feature.

NOTICE: If desired to change the language used for those features, it shall be done manually.

Example: **BCD Travel Brazilian Portuguese Voice Prompt**

8.2.1 Language Files

Automatic Call Distribution (ACD) Groups, Auto Attendant (AA) and Voice Mail (VM) are OSB features executed by the Asterisk software. Many language packages for Asterisk can be found in the internet, see <http://www.voip-info.org/wiki/view/Asterisk+sound+files+international> for details.

Usually the voice prompts have the same name in all languages so they can be easily replaced.

NOTICE:

Asterisk language packages cannot be directly installed in the OSB. The RPMs provided in the internet create a different directory structure not used by the OSB. The files shall be replaced manually.

8.2.2 Directory Structure

Asterisk voice prompts are stored in the OSB in the following directory structure:

```
/var/lib/asterisk/sounds
/var/lib/asterisk/sounds/dictate
/var/lib/asterisk/sounds/digits
/var/lib/asterisk/sounds/silence
/var/lib/asterisk/sounds/ann( link to /opt/siemens/
openbranch/mngmt/announcements)
/var/lib/asterisk/sounds/ann( link to /opt/siemens/
openbranch/mngmt/greetings)
/var/lib/asterisk/sounds/ann( link to /opt/siemens/
openbranch/mngmt/vm-osb-en)
/var/lib/asterisk/sounds/ann( link to /opt/siemens/
openbranch/mngmt/vmgreetings)
```

8.2.3 General Purpose Voice Prompts

The files under the sounds directory and in the subdirectories dictate, digits and silence are general purpose voice prompts and can not be changed via local GUI.

```
/var/lib/asterisk/sounds
/var/lib/asterisk/sounds/dictate
/var/lib/asterisk/sounds/digits
/var/lib/asterisk/sounds/silence
```

The voice prompts in these directories are the Asterisk default ones, excepting:

```
/var/lib/asterisk/sounds/agent-alreadyoff-simple.wav
/var/lib/asterisk/sounds/agent-alreadon-simple.wav
/var/lib/asterisk/sounds/agent-incorrect-literal.wav
/var/lib/asterisk/sounds/agente-user-logoff.wav
/var/lib/asterisk/sounds/queue-minute.wav
```

They are not found in the default Asterisk sound package. They were created based on other available English voice prompts specially to OSB.

For other languages, these files can be also created based on other voice prompts in a specific language or recorded according to the customer decision. The file names shall be preserved to replace them in the OSB.

8.2.4 ACD Announcements

Customized ACD announcements are stored under `/opt/siemens/openbranch/var/mngmt/announcements`

This directory stores the voice prompts for **queue join**, **queue wait** or **agent announcement** selection.

New voice prompts can be copied directly to this directory or uploaded via local GUI.

If desired to have the default voice prompts in other language, they can be also created based on other voice prompts in a specific language or recorded according to the customer decision. The file names shall be preserved to replace them in the OSB.

The default files are:

```
/opt/siemens/openbranch/var/mngmt/announcements/queue-
periodic-announce.wav
/opt/siemens/openbranch/var/mngmt/announcements/queue-
thankyou.wav
/opt/siemens/openbranch/var/mngmt/announcements/pri-
introsaved.wav
```

8.2.5 Auto Attendant Announcements

Customized AA announcements are stored under `/opt/siemens/openbranch/var/mngmt/greetings`

This directory stores the voice prompts for AA **Destination selection greeting**, **Failure prompt**, **Final prompt**, **Default destination prompt** or **Transfer prompt** selection.

New voice prompts can be copied directly to this directory or uploaded via local GUI.

If desired to have the default ones in other language, they can be also created based on other voice prompts in a specific language or recorded according to the customer decision. The file names shall be preserved to replace them in the OSB.

The default files are:

`/opt/siemens/openbranch/var/mngmt/greetings/goodbye.wav`

`/opt/siemens/openbranch/var/mngmt/greetings/transfer.wav`

`/opt/siemens/openbranch/var/mngmt/greetings/num-not-valid.wav`

`/opt/siemens/openbranch/var/mngmt/greetings/enter-num-to-call.wav`

`/opt/siemens/openbranch/var/mngmt/greetings/connect-to-party.wav`

8.2.6 VoiceMail Announcements

Customized VM announcements are stored under `/opt/siemens/openbranch/var/mngmt/vmgreetings`

This directory stores the voice prompts for selection of:

- VoiceMail Greeting
- VoiceMail Retrieve Prompt (From Own Extension)
- VoiceMail Retrieve Prompt (From Other Extension)
- VoiceMail Retrieve Wrong PIN
- VoiceMail Retrieve Change PIN
- VoiceMail Retrieve Change PIN failed
- VoiceMail Retrieve Wrong Box Number

New voice prompts can be copied directly to this directory or uploaded via local GUI.

If desired to have the default ones in other language, they can be also created based on other voice prompts in a specific language or recorded according to the customer decision. The file names shall be preserved to replace them in the OSB.

The default files are:

`/opt/siemens/openbranch/var/mngmt/vm-osb-en/vm-incorrect-mailbox.wav`

```

/opt/siemens/openbranch/var/mngmt/vm-osb-en/vm-login.wav
/var/lib/asterisk/sounds/vm-mismatch.wav
/var/lib/asterisk/sounds/vm-newpassword.wav
/opt/siemens/openbranch/var/mngmt/vm-osb-en/vm-password.wav
/opt/siemens/openbranch/var/mngmt/vmgreetings/vm-
welcome.wav

```

8.2.7 Replacing Files

The osb-pt_br-sounds.zip file was created based on voice prompts provided by the Disc-OS project (http://downloads.sourceforge.net/disc-os/Disc-OS-Sounds-1.0-pt_BR.tar.gz?use_mirror=osdn)

The files in there are organized following the OSB directory structure to make the installation easier:

```

/sounds
/sounds/digits
/sounds/ann
/sounds/greet
/sounds/vmgreet
/sounds/vm-osb-en

```

In order to export the voice prompts:

- 1) GSSH to OSB using WinSCP or another tool. Ensure that you have the root access to the OSB.
- 2) Under `/var/lib/asterisk/sounds/` replace the voice prompts by the ones in the sounds directory of the zip file.
- 3) Under `/var/lib/asterisk/sounds/digits` replace the voice prompts by the ones in the sounds/digits directory of the zip file.
- 4) In order to replace feature specific voice prompts, do the same for:

```

/var/lib/asterisk/sounds/ann
/var/lib/asterisk/sounds/greet
/var/lib/asterisk/sounds/vmgreet
/var/lib/asterisk/sounds/vm-osb-en

```

8.2.8 V9 Backup/Restore Custom Files

NOTICE:

This procedure needs to take place only once after OSB V9R0 release. Once installed, the modified voice prompts can be

exported and imported easily via local GUI. The files can be preserved in case of a new installation.

To export the voice prompts:

- 1) Go to **Maintenance>Import/Export**
- 2) Under **Export** section, select file group **Media (AA/VM/ACD/MOH)**
- 3) Click on **Export**
- 4) A tar file will be generated with voice prompts used for the features.

To import the voice prompts:

- 1) Go to **Maintenance>Import/Export**
- 2) Under **Import** section, select the tar file to be uploaded.
- 3) Click on **Upload**
- 4) Select the files/groups to be restored in the system and click on **Import**.

Index

A

ACD Configuration [352](#)
ACD:Agent display [362](#)
ACD:Agent status [357](#)
ACD:Agents [365](#)
ACD:General settings [354](#)
ACD:Log files [358](#)
ACD:Profiles [363](#)
ACD:Queue [359](#)
Activate software [81](#)
Agent [354](#), [365](#)
Alarm Details [51](#)
Alarm settings [158](#), [159](#), [162](#), [438](#)
Alarms [49](#), [158](#), [438](#), [661](#), [665](#), [665](#), [665](#), [666](#), [666](#), [666](#), [666](#), [667](#), [667](#), [667](#), [668](#), [668](#), [668](#), [669](#), [669](#), [669](#), [670](#), [670](#), [670](#), [671](#), [671](#), [671](#), [672](#), [672](#), [672](#), [672](#), [673](#), [673](#), [673](#), [674](#), [674](#), [674](#), [674](#), [675](#), [675](#), [675](#), [676](#), [676](#), [676](#), [677](#), [677](#), [677](#), [677](#), [678](#), [678](#), [678](#), [678](#), [679](#), [679](#), [680](#), [680](#), [680](#), [680](#), [681](#), [681](#), [681](#), [681](#), [682](#), [682](#), [682](#), [683](#), [683](#), [683](#), [684](#), [684](#), [684](#), [684](#), [685](#), [685](#), [685](#), [686](#), [686](#), [686](#), [686](#), [687](#), [687](#), [687](#), [688](#), [688](#), [688](#), [689](#), [689](#), [689](#), [690](#), [690](#), [690](#), [691](#), [691](#), [691](#), [692](#), [692](#), [692](#), [693](#), [693](#), [693](#), [694](#), [694](#), [694](#), [695](#), [695](#), [695](#), [696](#), [696](#), [696](#), [696](#), [697](#), [697](#), [697](#), [697](#), [698](#), [698](#), [698](#), [699](#), [699](#), [699](#), [700](#), [700](#), [700](#), [700](#), [701](#), [701](#), [701](#), [702](#), [702](#), [702](#), [703](#), [703](#), [703](#), [704](#), [704](#), [705](#), [705](#), [705](#), [706](#), [706](#), [706](#), [707](#), [707](#), [707](#), [708](#), [708](#), [709](#), [709](#), [709](#), [710](#), [710](#), [710](#), [711](#), [711](#), [712](#), [712](#), [712](#), [713](#), [713](#), [713](#), [714](#), [714](#), [714](#), [715](#), [715](#), [715](#), [716](#), [716](#), [716](#), [717](#), [717](#), [718](#), [718](#), [718](#), [719](#), [719](#), [719](#), [719](#), [720](#), [720](#), [720](#), [721](#), [721](#), [721](#), [722](#), [722](#), [722](#), [723](#), [723](#), [723](#), [723](#), [724](#), [724](#), [724](#), [725](#), [725](#), [725](#), [726](#), [726](#), [726](#), [727](#), [727](#), [727](#), [727](#), [728](#), [728](#), [728](#), [729](#), [729](#), [729](#), [730](#), [730](#), [730](#), [731](#), [731](#), [731](#), [732](#), [732](#), [732](#), [733](#), [733](#), [733](#), [734](#), [734](#), [734](#), [735](#), [735](#), [735](#), [736](#), [736](#), [737](#), [737](#), [737](#), [738](#), [738](#), [738](#), [739](#), [739](#), [740](#), [740](#), [740](#), [741](#), [741](#), [741](#), [742](#), [742](#), [743](#), [743](#), [743](#), [744](#), [744](#), [744](#), [745](#), [745](#), [745](#), [745](#), [746](#), [746](#), [746](#), [747](#), [747](#), [747](#), [748](#), [748](#), [748](#), [748](#), [749](#), [749](#), [749](#), [749](#), [750](#), [750](#), [751](#), [751](#), [751](#), [752](#), [752](#), [752](#), [752](#), [753](#), [753](#), [754](#), [754](#), [754](#), [754](#), [755](#), [755](#), [755](#), [756](#), [756](#), [756](#), [757](#), [757](#), [757](#), [758](#), [758](#), [758](#), [758](#), [759](#), [759](#), [759](#), [760](#), [760](#), [760](#), [760](#), [761](#), [761](#), [761](#), [762](#), [762](#), [762](#), [763](#), [763](#), [763](#), [764](#), [764](#), [764](#), [765](#), [765](#), [765](#), [766](#), [766](#), [766](#), [767](#), [767](#), [767](#), [768](#), [768](#), [768](#), [769](#), [769](#), [769](#), [770](#), [770](#), [770](#), [771](#), [771](#), [771](#), [772](#), [772](#), [772](#), [772](#), [773](#), [773](#)
Announcement for ACD [359](#)
Audience [18](#)
Automated Attendant [419](#)
Automated Attendant:Basic settings [422](#), [423](#)
Automated Attendant:Menus [426](#)

Automated Attendant:Routing [424](#)

B

Backup [19](#)
Backup data channel [304](#), [310](#), [313](#)
Backup link [310](#), [313](#)
Backup link client [304](#)
Backup link server [304](#)
Batch job [82](#), [84](#), [85](#)
Batch jobs [83](#)
Black List [236](#), [458](#)
Branch office [37](#)
Branch office:Create and Delete [38](#), [41](#), [103](#)
Branch office:Display [39](#)
BRI card [382](#)
bSBC mode [19](#)
Business group [37](#)

C

Call Forwarding for Survivable Mode [301](#), [302](#)
Central SBC [19](#)
Certificates [215](#)
Clock source [406](#)
Codec Priority list [342](#)
Codecs [374](#)
Common Management Platform (CMP) [19](#)
Communication system [272](#), [336](#), [338](#), [387](#), [396](#)
Configuration file [77](#), [78](#), [79](#)
Continuous tracing [175](#), [177](#), [446](#), [448](#)
Country configuration [272](#), [274](#)
Custom [461](#)

D

Dashboard [46](#)
Debugging [172](#)
Debugging:Tools [173](#)
Default gateway address [193](#)
Deployment mode [275](#), [279](#), [430](#)
DHCP server [209](#), [210](#)
Disabling Redundancy [196](#)
DNS server [204](#), [452](#)
DNS:Forward IPs [206](#)
DNS:Server list [206](#)
DNS:Settings [206](#), [453](#)
DNS:Zone [206](#)

E

E1 PRI [387](#), [396](#), [406](#)
Enabling Redundancy [196](#)

End of Dial [375](#)
Error codes [297](#), [473](#)

F

File system [74](#)
Firewall [235](#), [236](#), [457](#), [458](#)
FXO card [380](#)
FXS card [375](#)

G

Gateways [315](#), [319](#), [476](#)
General [64](#)

H

Hardware Platforms [19](#), [32](#)
Header manipulation [283](#), [290](#), [468](#)
Health Check [52](#)

I

Integrated gateway:BRI configuration [382](#)
Integrated gateway:Codecs [374](#)
Integrated gateway:FXO configuration [380](#)
Integrated gateway:FXS configuration [375](#)
Integrated gateway:General settings [370](#)
Integrated gateway:Media [372](#)
Integrated gateway:PRI Configuration [387](#), [396](#), [406](#)
Integrated gateway:QoS monitoring [371](#)
Integrated gateway:Trunk group [408](#)
Integrated gateway:Trunk group 500i [413](#)
Interface [189](#), [190](#), [191](#), [450](#), [450](#)
Introduction [18](#), [19](#)
IP security [240](#), [241](#)

J

Job Manager [82](#)

L

License server location [263](#)
License type:base license [132](#), [135](#)
License type:dynamic user license [133](#)
License type:evaluation license [132](#)
License type:OpenScape Branch Auto Attendant license [134](#)
License type:OpenScape Branch Backup ACD Feature license [134](#)
License type:OpenScape SBC Session license [135](#)
License type:OSB base license [132](#), [135](#)
License type:regular license [125](#)
License type:software subscription license [126](#), [127](#)
License type:upgrade license [135](#)
List of jobs [83](#)

Log files [60](#), [62](#)
Logging [167](#), [441](#)
Logging:Settings [170](#), [444](#)

M

MAC address [210](#)
Mark filters [199](#)
Media [372](#)
Media server [180](#)
Media Server Profiles [449](#)
Media server:Adapter [187](#)
Media server:Announcement settings [186](#)
Media server:Conference settings [184](#)
Media server:Connectivity [183](#)
Media server:Converter [188](#)
Media server:Enable [182](#)
Media server:Language file [188](#)
Menu [34](#)

N

Navigation [34](#)
Network services [190](#), [450](#)
Node [338](#)
Node redundancy [336](#)
NTP settings [202](#), [204](#), [451](#)

O

Office Code Mapping [285](#)
On demand trace [175](#), [179](#), [446](#)
OpenScape Branch Assistant [90](#)
Operating Modes [19](#)

P

Packet shaping [199](#)
Password [44](#), [244](#), [264](#), [266](#), [268](#)
Password management [87](#)
Periodic Synchronization [91](#)
Phone Software Storage [119](#)
Port configuration [474](#)
Port forwarding [235](#), [238](#), [457](#)
Port mapping [300](#)
PRI [387](#), [396](#), [406](#)
Profile [363](#)
Profiles [430](#), [430](#), [435](#), [436](#), [437](#)
Proxy [275](#), [430](#)
Proxy ACD [275](#), [430](#)
Proxy ACD mode [19](#)
Proxy ATA [275](#), [430](#)
Proxy mode [19](#)

Q

QoS [331](#), [333](#), [482](#)

QoS monitoring [371](#)
Queue [359](#)

R

Rapidstat [46](#), [52](#)
Redundancy [19](#)
Registered subscribers [67](#), [68](#), [300](#)
Restart [76](#)
Routing [190](#), [194](#), [450](#)
Routing rules [293](#), [295](#), [469](#), [472](#)
RTP settings [343](#), [344](#)
Rule filters [199](#)

S

SBC [275](#), [430](#)
SBC Proxy [430](#)
SBC Proxy mode [19](#)
SBC-Proxy [275](#)
Schedule [82](#), [84](#), [85](#)
Schedules [83](#)
Secure transfer [91](#)
Security [214](#), [455](#)
Serviceability [73](#)
Services status [55](#), [57](#)
Shared secret files [215](#)
Simplified Installation [88](#), [88](#), [92](#), [95](#), [97](#), [100](#), [101](#), [114](#), [117](#)
SIP error codes [297](#), [473](#)
SIP header manipulation [283](#), [290](#), [468](#)
SIP header manipulation [281](#), [466](#)
SIP routing rules [293](#), [295](#), [469](#), [472](#)
SIP Service Provider Profiles [322](#), [476](#), [477](#)
SIP settings [298](#), [475](#)
SNORT [233](#), [234](#), [456](#), [457](#)
Software [81](#), [86](#)
Software activation [82](#)
Software Information [53](#)
Static IP [210](#)
Status [42](#)
Subnet [210](#)
Subscribers [300](#)
Survivability [19](#), [246](#)
Survivability:CDR handling [258](#), [463](#)
Survivability:MoH handling [464](#)
Survivability:Multiline Hunt Groups [250](#)
Survivability:Music on Hold handling [260](#)
Synchronization [91](#)
System information [54](#)
System settings [261](#), [465](#)

T

T1 PRI [387](#), [396](#), [406](#)
Threshold [340](#), [483](#)
Timer [340](#), [483](#)

TLS settings [217](#), [219](#), [223](#), [225](#), [228](#), [229](#)
Tracing [175](#), [177](#), [179](#), [446](#), [448](#)
Traffic class [199](#)
Traffic shaping [199](#), [199](#)
Transport Layer Security [215](#)
Trap destinations [158](#), [164](#), [165](#), [438](#), [439](#), [440](#)
Troubleshooting [117](#)
Trunk group [408](#), [413](#)
Trusted addresses [336](#)

U

Update [81](#), [86](#)
Update OSB status [42](#)
Upgrade [81](#), [86](#)
Upgrade Manager [74](#)
Upgrading a redundant system [196](#)

V

VLAN settings [191](#)
Voice over IP Profiles [465](#)
VoIP configuration [269](#)
VRRP settings [196](#)

W

White List [236](#), [458](#), [461](#)

