



A MITEL
PRODUCT
GUIDE

Unify OpenScape Branch

OpenScape Branch V10

Configuration Guide
July 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

Table of Contents	
History of Changes	7
1 Disclaimer	9
2 Software Installation.....	9
2.1 Boot sequence setup.....	9
2.1.1 Configure BIOS for IBM/Lenovo 3250M3/M5/M6 and 3550M4/M5	11
2.1.2 Boot device for one time use: for IBM 3250M3/M5/M6 and 3550M3/M4/M5, Lenovo SR250/SR250 V2 and SR530 and SR630 V2	11
2.1.3 System Boot Mode - Legacy Mode or UEFI Mode	12
2.1.3.1 Lenovo x3250M6 and x3550 M5 platforms	13
2.1.3.2 Lenovo SR530, SR630 V2 and Lenovo SR250/SR250 V2 platforms	13
2.1.4 RAID (Redundant array of independent disks) information	13
for IBM3550, RX200 and SR530	13
3. USB Stick Setup tool	14
4 Full Installation	18
5 Branding.....	21
6 OpenScape Voice (OSV) Configuration	23
7 OpenScape Branch Configuration	25
8 Network Services	26
8.1 Ethernet Interface Bonding.....	29
9 OSB IPV6 for Administration	34
10 IPV6 Support for SIP Devices	34
11 OSB IPV6 support for SIP trunks	34
12 Users/Password Recovery/Change.....	36
12.1 Users/Passwords	36
13 Administration Accounts	37
14 Radius.....	38
15 SSH with PKI and Certificate files for WEB Server	38
16 Utilities(Reboot+VersionInformation)	40
17 Time Settings/NTP	41
18 VOIP Configuration.....	42
18.1. PROXY Mode	42
18.2. SIP Server Configuration	42
18.3. Codecs Configuration.....	46
18.4. RTP Configuration.....	49
18.5. Timers and Thresholds	50
18.6. SIP Manipulation, Office Code Mapping and Gateways.....	51
18.7. SIP Manipulation Provisioning	51
18.8. Office Code Mapping	53
18.9. Extension Dialing Across Office Codes	53
18.10. Source-Based Routing.....	54
18.11. SIP Routing Provisioning	55
18.12. Gateway Provisioning	56
18.13. SIP Manipulation Provisioning	60
19 Call Forward (Voice Mail)	62
20 Local Voice Mail Service.....	63
21 MOH.....	68
22 QOS	69
23 DHCP	70
24 PhoneSoftwareManagement	71
24.1. Feature Description- Prerequisites	71
24.2. Central HTTPS server	71

24.3.	Phones	72
24.4.	Branch Office	72
24.5.	OSB Configuration	73
24.6.	DLS Configuration.....	75
24.7.	Configure Central HTTPS Server	75
24.8.	Obtain Branch Office Data.....	76
24.9.	Synchronize with OpenScape Server.....	78
24.10.	Location	78
24.11.	Phone Deployment	80
24.12.	Deploy Workpoints.....	81
24.13.	Manage Rules.....	81
25	Auto Attendant (AA).....	83
26	Message rate control	85
27	Digest Authentication Credentials synchronization between OSB and OSV	86
28	Emergency Calling.....	87
29	NG911 support for Emergency Calling.....	92
30	CDR	96
30.1	CDR Record Details.....	97
32.	DNS	98
32.1	Slave DNS	98
32.2	Forward DNS	100
32.3	Master DNS	101
33.	DNS SRV	102
34.	Multi Line Hunting Groups (MLHG)	105
34.1	Synchronization for OSB MLHG and Emergency Calling Subnets	106
35.	OSB Redundancy	107
35.1	Upgrading Redundant System	107
35.2	Disabling Redundant System	108
35.3	Master Status Check.....	108
35.4	Backup Status Check.....	109
36.	Phone Configuration for Proxy.....	110
37.	OSB Status information	111
37.1	System Status (Checking if OSB is in SM or NM)	111
37.2	Services Status	113
37.3	Registered Subscribers	113
38.	Backup/Restore and XML Configurations	119
38.1	Load Config (DB XML File)	120
38.2	Import Config (DB XML File).....	120
38.3	Export Config (DB XML File).....	121
38.4	Backup/Restore of custom configuration files.....	122
38.4.1	Export.....	122
38.4.2	Import.....	123
39.	How to install / upgrade a file.....	124
39.1	How to configure Bulk Configuration (Delta XML)	134
40.	How to Restart	139
40.1	How to configure Scheduled Maintenance	142
41	Creating Delta XML	144
42	Upgrade	151
43	Debug/Tracing	154
43.1	Log settings (Log Size, Log Level and Syslog)	154
43.2	Log data	155
43.3	Rapidstat	158
43.4	Debugging Tools (ICMP, Trace Route, Network Tracer).....	158

43.5 Continuous Tracing	162
43.6 On Demand Trace	162
43.7 Advanced (Enabling the System Collector Logs)	163
44 Port and Signaling Settings	165
45 Branch SBC Mode	167
46 Media Server (MS)	177
46.1 Configuring OSB as main Media Server in OSV	179
46.2 Configuring OSB in the OSV as Branch Media Server	146
46.2.1 Enable Media Server Audit in the OSV	150
46.2.2 Upload of Customized Media Server Announcements	152
47. TLS Configuration	154
47.1 Create TLS Certificate	154
47.2 Submit the Certificate Sign Request file to the Certificate Authority	154
47.3 Download the Certificate from the Certificate Authority	155
47.4 Upload TLS Certificates for OpenScapeBranch	155
48 . Minimum TLS Version	158
48.1 Configuration of TLS in OpenScapeBranch/OSV	160
48.2 Configuration of MTLS in OpenScapeBranch/OSV	162
48.3 Configuration of TLS in Phones	164
48.4 Tracing with TLS	166
49 Certificate verification process compliant with Baseline Security Policy	167
50 Special characters in P-Preferred Identity of SIP INVITE	168
51 OpenScape Branch SRTP Interworking and Codec Transcoding Configuration	169
52 Media Transcoding	174
53 Security enhancements	176
54 Support of near end NAT Firewall	178
55. External Firewall - Pinhole	183
55.1 Open External Firewall – Pinhole	183
55.2 Send RTP dummy packets	184
56 OpenScape Branch 50i	192
56.1 Integrated GW Configuration (Advantech 50i)	192
56.2 Enable Integrated GW and Discover card configuration	194
56.3 FXS and FXO Configuration	195
56.4 BRI Configuration	207
56.4.1 Configure OSB 50i D44 to be used as BRI NT (Network)	210
56.4.2 BRI - Trunk Group Configuration	212
56.4.3 PRI - Trunk Group Configuration	227
56.5 Integrated Gateway – General Settings	233
56.5.1 Gateway/Trunk Configuration	233
56.5.2 SIPQ V2	233
56.5.3 Blacklist	233
56.5.4 Codec Configuration	238
56.5.5 CID Suppression	239
56.5.6 Number Modification	240
56.5.7 Local Toll Table	250
57 OpenScape Branch 500i	251
57.2 Enable Integrated GW and Discover card configuration	252
57.3 PRI Configuration	255
57.3.1 PRI - Trunk Group Configuration	265
57.4 500i - General Settings	270
57.4.1 Redundancy	270
57.4.2 Gateway/Trunk Configuration	273
57.5 CID Suppression	278

57.6	Number Modification	278
57.6.1	Incoming Calls	281
57.6.2	Outgoing Calls	283
57.6.3	OSB 50i/500i Gateway Number Modification Implementation.....	285
57.7	Local Toll Table	289
57.7.1	Creation of LTT	289
58	OpenScape Branch 50i/500i as GW Only	290
58.1	OpenScape Voice	290
58.2	OpenScape Branch Main.....	296
58.2.1	VoIP	296
58.2.2	Gateway	298
58.2.3	Media Server	298
58.2.4	Auto Attendant	298
58.2.5	Survivable Mode features	299
58.2.6	Redundancy	299
58.2.7	BackupLink	299
58.2.8	DNS.....	299
58.2.9	NTP	299
58.2.10	Digest Authentication	299
58.2.11	Licensing.....	299
58.2.12	Caller Number Suppression	299
58.3	OpenScape 50i/500i Gateway	300
58.3.1	Gateway Only Configuration	300
58.3.2	Licensing.....	303
59	OSB 50i DP24 and OSB 500i DP4/8 as standalone PRI Adapters to SIP Trunking.....	306
60	Proxy ATA	307
60.1	Configuration Options.....	307
60.1.1	Proxy ATA behind OSB Proxy (ex. OSB500i) connected to OSV.....	307
60.1.2	Proxy ATA connected directly to OSV.....	310
60.1.3	General Proxy ATA Configuration	312
60.2	System Status	320
61	Multiple OSBs in a Branch	323
61.1	Configuration in the OSV:	323
61.2	Configuration in the OSB:	323
62	Simplified Installation.....	327
62.1	Common Management Portal and OSB Assistant configuration:.....	327
62.2	Option 1 - Zero Touch Installation	330
64.2.1	Zero Touch Installation Steps	331
64.3	Option 2 – Simplified Installation Using Logical ID and DHCP Option 43.....	332
64.3.1	USB Stick preparation.....	332
64.3.2	DHCP Configuration	332
64.3.3	Option 2 Installation Steps	333
64.4	Option 3 – Simplified Installation Using Logical ID with DHCP not providing Option 43	334
64.4.1	USB Stick preparation.....	334
64.4.2	DHCP Configuration	334
64.4.3	Option 3 Installation Steps	334
64.5	Option 4 – Simplified Installation Using Existing Configuration File	336
64.5.1	USB Stick preparation.....	336
64.5.2	DHCP Configuration	336
64.5.3	Option 4 Installation Steps	337
64.6	Option 5 – Secured Simplified Installation Using VPN	337
64.6.1	USB Stick preparation.....	337
64.6.2	DHCP Configuration	339

64.6.3	Option 5 Installation Steps	340
64.6.4	Error Conditions	341
65	Back Up Data Link	342
65.1	Network and Connectivity Requirements.....	342
65.1.1	Media Server.....	342
65.1.2	Network Services	342
65.1.3	Gateways	342
65.1.4	Data Center Router	342
65.1.5	IPSec VPN	342
65.1.6	PPP Network.....	342
65.2	Known Restrictions.....	343
65.2.1	General	343
65.2.2	OSB V1R4.....	343
65.2.3	OSB V1R3.....	343
65.3	Configuration for OpenScape Branch with OpenScape VoiceIntegrated Simplex or Collocated	343
65.3.1	Configuring the OpenScape Voice for Backup Data Link Support	343
65.3.2	Subscriber Rerouting Configuration.....	346
65.3.3	Configuration of Voice Mail Rerouting (optional)	357
65.4	Configuring the OpenScape Branch for Backup Data Link Support	358
65.4.1	Backup Link Server (BLS) Configuration	358
65.4.2	Backup Link Client (BLC) Configuration	361
65.4.3	Survivability Mode Avoidance	364
65.5	Configuration for OpenScape Branch with OpenScape Voice Geo Separated	365
65.5.1	Configuring the OpenScape Voice for Backup Data Link Support	365
65.5.2	Configuration of Voice Mail Rerouting (optional)	378
65.5.3	Configuring the OpenScape Branch for Backup Data Link Support.....	379
65.5.4	Survivability Mode Avoidance	386
66	Data Center Router Settings for Geo Separated Configuration	387
66.1	SNMP Configuration.....	387
66.2	WAN Monitoring	387
66.2.1	Configuration on Data Center Router 1	387
66.2.2	Configuration on Data Center Router 2	388
66.3	Configuration on Branch Router	389
66.4	Alternate routing to Backup Link Server.....	389
66.4.1	Configuration on Data Center Router 1	390
66.5	Configuration on Data Center Router 2.....	390
67	SIP Service Provider Provisioning.....	391
67.1	Enable the WAN interface	391
67.2	Create SIP Service ProviderProfile	392
67.3	Create SIP Trunk.....	398
67.4	Create Routing Map	400
67.5	Do not send invite without SDP and MOH in Survivability Mode	400
67.5.1	No MOH to SSP in Survivability Mode.....	400
67.5.2	Providing MOH to the SSP in Survivability Mode	401
67.6	Point to Service Provider or Publix DNS (If Applicable)	401
67.7	Cseq updates for Digest Authentication	401
68	Licensing.....	402
68.1	Supported License Types	403
68.2	Central License Server (CLS)	405
68.3	Common Management Portal License Configuration.....	405
68.4	Stand Alone License Configuration.....	407
68.5	Subscription License	410
69	Automatic Call Distribution (ACD).....	411

69.1	General Configuration	411
69.2	ACD Queues.....	411
69.3	ACD Profiles	414
69.4	ACD Agents	415
69.5	ACD Audio Files	417
69.6	Configuration for Toggle Key.....	418
70	Virtualized OpenScape Branch Solution	419
70.1	OSB iso image.....	419
70.2	ISO Image for fresh installation	420
70.3	ISO Image for migration of native hardware	424
70.4	Virtual Machine (VM).....	425
70.5	Creating the VM.....	425
70.6	Deploying OSB vApp	425
70.7	Creating VM manually	432
70.8	Virtual OSB Installation	450
70.9	VM version	460
70.10	OpenScape Branch and SBC distribution via OVA	461
70.11	VLAN configuration for OSB VM.....	462
71	Hosted OpenScape Branch with Secured Management Network	462
71.1	Network Requirements.....	462
71.1.1	VPN Concentrator Options	462
71.1.2	Firewall.....	462
71.1.3	Network Configuration.....	462
71.2	Configuration for OpenScape Branch	462
71.2.1	Configuring the VPN using IPSec.....	462
71.3	Certificate Profile	464
71.4	Configuration for OpenScape Voice.....	466
71.5.1	Configuring Management IP for the Endpoint.....	466
72	Replacing OSB Voice Prompts (Features)	467
72.1	Language File	467
72.2	Directory Structure	467
72.3	General Purpose Voice Prompts	468
72.4	ACD Announcements.....	468
72.5	Auto Attendant Announcements	469
72.6	Voice Mail Announcements	470
72.7	Replacing files	471
72.8	Steps to Install	472
72.9	V9 Backup/Restore Custom Files	474

History of Changes

Issue	Date	History of Changes
9.00.00	26/08/16	<ul style="list-style-type: none"> Creation of the V9R0 based on V8
9.00.00.01	22/11/16	<ul style="list-style-type: none"> Inclusion of Delta FRNs for V9R0
9.00.00.02	03/03/17	<ul style="list-style-type: none"> Inclusion of Delta FRNs for V9R1
9.00.00.03	03/04/17	<ul style="list-style-type: none"> Support of SNMP V3 GET Configuration
9.00.00.04	25/05/17	<ul style="list-style-type: none"> ACD Proxy Select language for ACD Agent logon/logoff
9.00.00.05	01/09/17	<ul style="list-style-type: none"> Minor modifications & enhancements
9.00.00.06	29/09/17	<ul style="list-style-type: none"> OSB Support of SIP Connect V1.1 Registration Mode
9.00.00.07	29/09/17	<ul style="list-style-type: none"> OSB: Allow SIP trunks from LAN side
9.00.00.08	19/03/18	<ul style="list-style-type: none"> OpenScape Branch distribution via OVA
9.00.00.09	27/04/18	<ul style="list-style-type: none"> Minor modifications & enhancements
9.00.00.10	11/05/18	<p>New Hardware Type: Lenovo SR530 (Replacement for IBM x3550 M5)</p> <p>Open External Firewall – Pinhole feature</p>
9.00.00.11	17/08/18	<ul style="list-style-type: none"> Enable Firewall on OS Branch LAN
9.00.00.12	28/09/18	<ul style="list-style-type: none"> BCF Event Handling Protocol Administration Accounts
9.00.00.13	14/12/18	<ul style="list-style-type: none"> Allow SIP trunks from LAN side activation Instructions
9.00.00.14	06/02/19	<ul style="list-style-type: none"> Updated Table D: Operating Modes Diagram Minor enhancements & modifications
9.00.00.15	01/03/19	<ul style="list-style-type: none"> Redesign of Time Zone configuration
9.00.00.16	03/04/19	<ul style="list-style-type: none"> DTAG SSP configuration for OSB
9.00.00.17	05/07/19	<ul style="list-style-type: none"> Digest Authentication Credentials synchronization between OSB and OSV
9.00.00.18	15/11/21	<ul style="list-style-type: none"> Documentation Enhancements and updates
9.00.00.19	10/12/21	<ul style="list-style-type: none"> Documentation Enhancements and updates
9.00.00.20	06/04/22	<ul style="list-style-type: none"> Documentation Enhancements and updates
9.00.00.21	16/06/22	<ul style="list-style-type: none"> Documentation Enhancements and updates
9.00.00.22	02/02/23	<ul style="list-style-type: none"> Documentation enhancements and updates
9.00.00.23	01/02/23	<ul style="list-style-type: none"> Documentation enhancements and updates TOC and headings troubleshooting
9.00.00.24	09/03/23	<ul style="list-style-type: none"> Updated Chapter <u>67.2 Create SIP Service Provider Profile</u>
9.00.00.25	21/04/23	<ul style="list-style-type: none"> Minor updates and enhancements

9.00.00.26	27/06/23	<ul style="list-style-type: none"> • Minor updates and enhancements
9.00.00.27	01/08/23	<ul style="list-style-type: none"> • Added Lenovo SR630 V2 server
9.00.00.28	20/09/23	<ul style="list-style-type: none"> • Updated Chapter 51 OpenScape Branch SRTP Interworking and Codec Transcoding Configuration
9.00.00.28	24/07/2024	<ul style="list-style-type: none"> • Rebranded to the Mitel layout

1 Disclaimer

This document has been elaborated along the OpenScapeBranch development as a guide and manual of configuration best practices.

However the descriptions and configurations in this document are based, and limited, to a very specific deployment scenario: the Development Laboratory. Most cases, setups and networks found on the real deployment are unique and may require a proper adequacy or necessary configuration changes to work correctly.

2 Software Installation

2.1 Boot sequence setup

Some BIOS configuration changes may be required if you are using an OpenScape Branch 50/250, OpenScape Branch 50i, OpenScape Branch 500i, Lenovo/IBM or Fujitsu server. (Not required for OpenScape Branch 50i A024/48).

Before installation, if you are using IBM/Lenovo or Fujitsu hardware then some BIOS configuration changes may be required:

- Set the boot sequence for some servers adding the USB storage as first option and the Hard Disk as second.

Verify Automatic Power Restore Policy to “Always ON” for IBM 3250 servers.

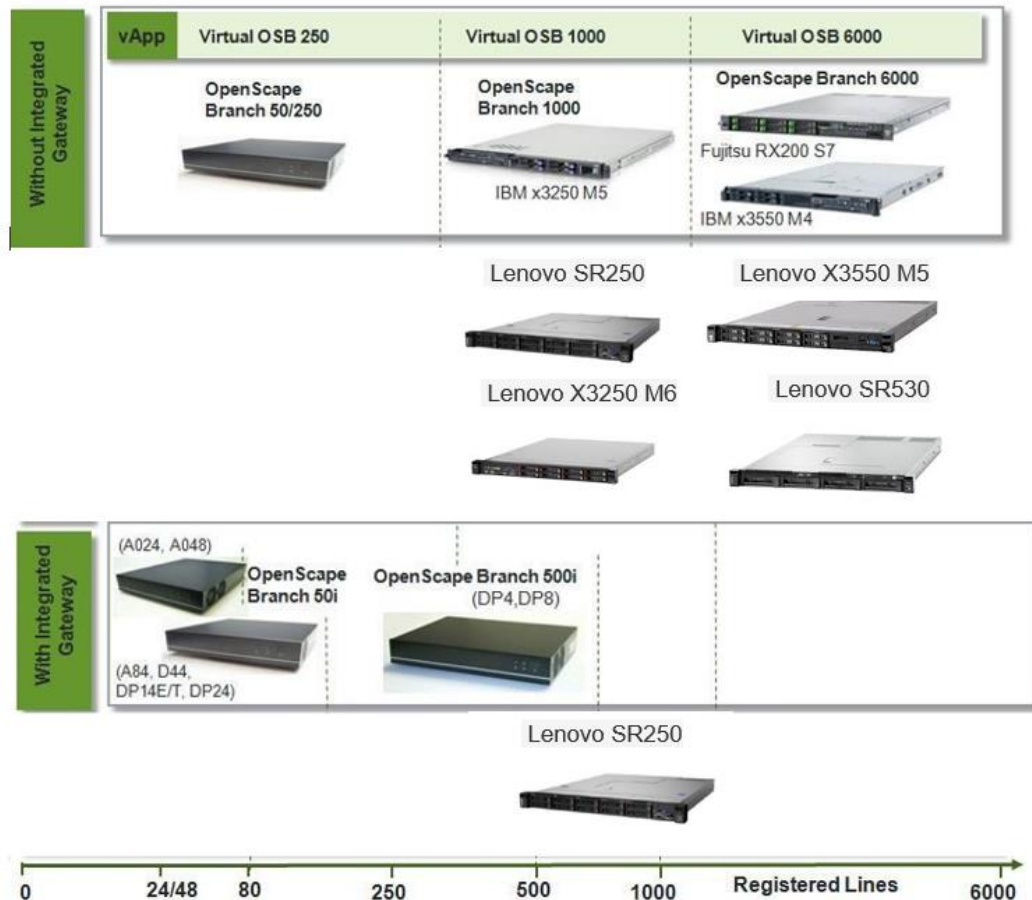
- OpenScape Branch 500i: Boot sequence. First device should be set to “USB Hard Disk”, and second set to Hard Disk.

BIOS change steps for making the USB device the primary boot device will be added and a change request has been submitted to Fujitsu.

- OpenScape Branch 50/250/50i: Verify Auto Power on is Enabled. (Advanced > APM Configuration > Restore On ACPower Loss > Power On.)

Note: if problems detecting USB stick on OpenScape Branch 50/250, OpenScape Branch 50i shows then BIOS update is required. Contact service if this is needed (Work around is to unplug/plug USB stick while OSB is turned on).

Note: After software installation, for security issue, it is recommended to start the boot from Hard Disk option.



Software image: image provided for customer on SWS.

- image_osb-10.02.*.*.tar – Software image file for upgrade or install.
- usbsticksetup_osb-10.02.*.*.zip - Contains the USB Stick Wizard, it is optional and is included when changes in installation scripts or changes in GUI that affect installations procedures were done.
- misc_osb-10.02.*.*.tar.gz - contains the configuration and the data structure to be used in the OpenScape Branch MIB.
- image_osb-10.02.*.*.spa - File for use when uploading to CMP only.
- vApps_osb-10.02.*.*.zip – Virtual deployments specific.
- sw-metadata-osb-10.02.*.*.json – this file is used with OS Composer application.

Additional file used in SFTP and HTTPS

List - Text file for external server along with software image in case of SFTP/HTTPS installation/ upgrade. File must be created manually.

Example: To install image_osb-10.2.*.*.tar, place "list" file in the same directory (of the HTTPS/SFTP server) where tar file is located.

Note: If your server is Linux, store the image file in an empty directory.

2.1.1 Configure BIOS for IBM/Lenovo 3250M3/M5/M6 and 3550M4/M5

1. Power on the server.
2. At boot up wait and press **F1** to enter the BIOS setup when the option "<F1> Setup" is available.
3. Once in the "System Configuration and Boot Management" window with the arrow key, navigate to "Boot Manager" and press **Enter**.
4. Once in the "Boot Manger" window select **Add Boot Option** and press **Enter**.
5. Select "USB Storage" and press **Enter**.
6. Press **Esc** to exit and go back to the "Boot Manager" window.
7. Select **Change Boot Order** and press **Enter**.
8. Press **Enter** again to change the order.
9. The order should be:
 - USB Storage
 - Hard Disk 0
10. Press **Enter**.
11. Select **Commit Changes** to save.
12. Press **Esc** to exit from all the windows.
13. Select **Y** when asked "Do you want to exit the Setup Utility?".

2.1.2 Boot device for one time use: for IBM 3250M3/M5/M6 and 3550M3/M4/M5, Lenovo SR250/SR250 V2 and SR530 and SR630 V2

2.1.2.1 IBM x3250M3/M5/M6, x3550M3/M4/M5 platforms

1. Plug in the USB stick to be used for the boot.
2. Power on or reboot the server.
3. When prompted, select **F12** to select Boot Device option.
4. In "Boot Devices Manager", select the **USB Storage** option.
5. Press **Esc** to exit.

2.1.2.2 Lenovo SR530, SR630 V2 and Lenovo SR250/SR250 V2 platforms

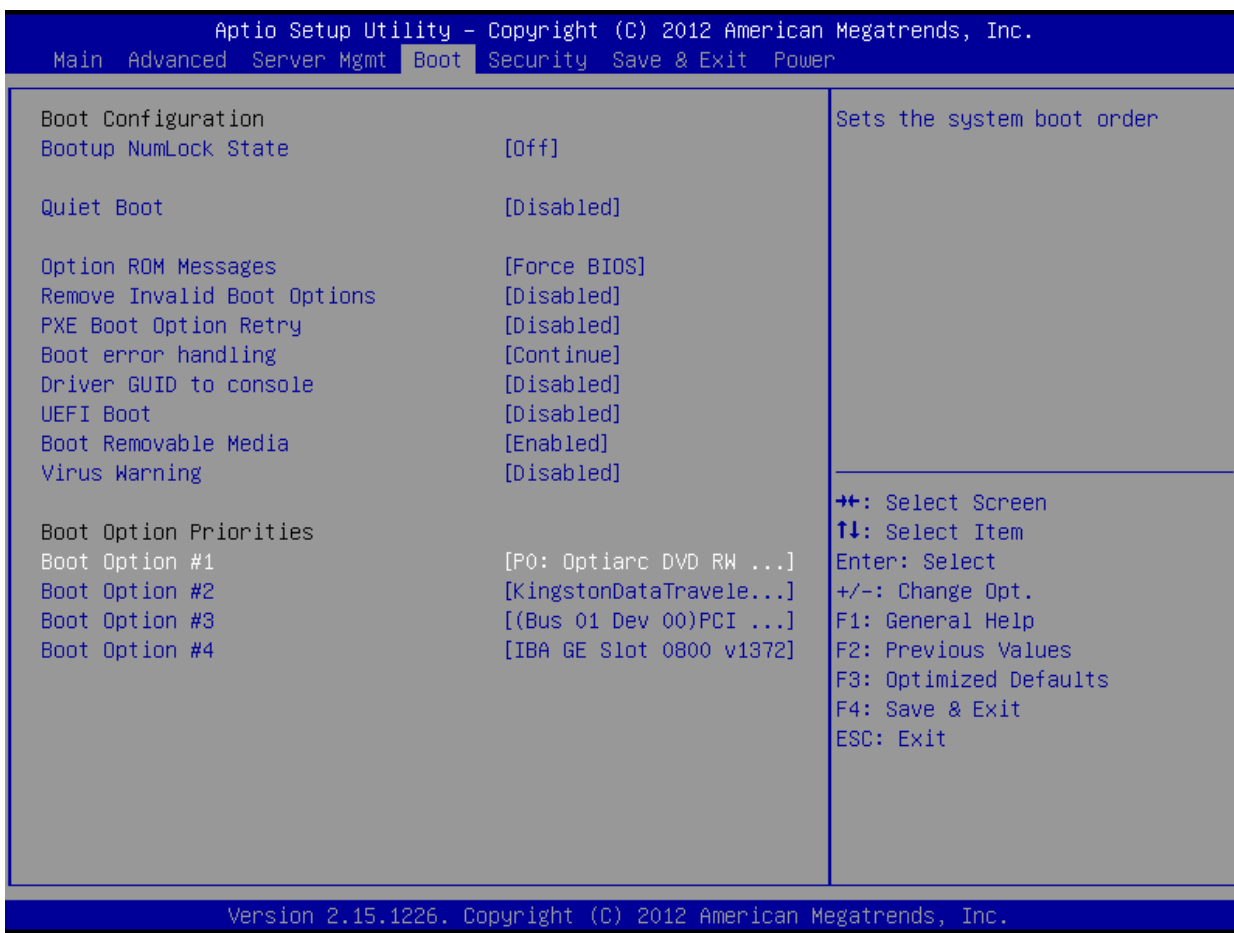
1. Plug in the USB stick to be used for the boot.
2. Power on or reboot the server.
3. When prompted, select **F12** "One Time Boot Device" option.
4. In "Boot Devices Manager", select **USB Storage** option.
5. Press **Enter** to exit.

2.1.2.3 Fujitsu RX200 platforms

1. Plug in the USB stick to be used for the boot.
2. Power on or reboot the server.
3. At boot up wait and Press **F2** to enter setup.
4. Use the right arrow to select the boot tab.
5. Select the USB as the boot option #1.
6. Exit setup.

7. Continue with the system boot.

You can not select USB as a boot option since there are multiple USBs on the system, and picking a specific port would be problematic. The best solution is to plug a USB in (as shown below: a Kingston Data Traveler USBstick) and you can then select.



2.1.3 System Boot Mode - Legacy Mode or UEFI Mode

NOTE: Lenovo SR250 V2 is available starting from V10R3.3.0

NOTE: Lenovo SR630 V2 is available starting from V10R3.3.0

Before V10R2, only the Legacy Mode was available for system boot. Now, it is possible to choose the UEFI Mode to system boot.

The System Boot Mode must be configured correctly, otherwise the Server will not boot from the Hard Drive.

2.1.3.1 Lenovo x3250M6 and x3550 M5 platforms

- LEGACY MODE: Select **F1** to enter in System Setup, choose Boot Manager option, the Boot Modes must be configured as Legacy Mode.
- UEFI MODE: Select **F1** to enter in System Setup, choose Boot Manager option, the Boot Mode must be changed to UEFI mode. In System Settings, the Legacy Support must be disabled.

2.1.3.2 Lenovo SR530, SR630 V2 and Lenovo SR250/SR250 V2 platforms

LEGACY MODE:

1. Select F1 to enter in System Setup.
2. Choose the UEFI Setup option.
3. Select System Settings and enable the Legacy BIOS.
4. Configure the Boot Manager/Boot Modes as Legacy Mode.

UEFI MODE:

1. Select F1 to enter in System Setup.
2. Choose the UEFI Setup option.
3. Disable the Legacy BIOS in System Settings.

IMPORTANT:

The following servers do not support UEFI Boot Mode, only Legacy Mode:

- Fujitsu Rx 200 S6
- Fujitsu Rx 200 S7
- 50i
- 500i

For virtual machines, it is recommended to use Legacy Mode.

2.1.4 RAID (Redundant array of independent disks) information for IBM3550, RX200 and SR530

Please refer to Chapter 3 of the following document for instructions:

[OpenScape Voice V10, Service Manual: Installation and Upgrades, Installation Guide.](#)



Note: Only RAID 1 is supported.

3. USB Stick Setup tool

This application is distributed with the following files from SWS

- **osb-10.02.*.*.zip**, that contains:
 - **image_osb-10.02.*.*.tar** – Software image file for upgrade or install.
 - **image_osb-10.02.*.*.spa** – File contains the compatibility information from the old release to new release for use by the CMP.
 - **usbsticksetup_osb-10.02.*.*.zip** - Contains the USB Stick Wizard.
- **misc_osb-10.02.*.*.tar.gz** - has the default XML configuration files and the MIBS
- **vApps_osb-10.02.*.*.zip** - Contains the OVF templates to create and deploy a virtual machine for the various models of Virtual OSB.
- **sw-metadata-osb-10.02.*.*.json** – this file is used with OS Composer application.

The USB Stick Wizard (usbsticksetup.exe) is a Windows application used to generate a USB Stick (pen drive) for OpenScape Branch Installation.

Name	Type	Size
image_osb-10.02.00.00-2.spa	SPA File	1 KB
image_osb-10.02.00.00-2.tar	TAR File	730,990 KB
misc_osb-10.02.00.00-2.tar.gz	GZ File	157 KB
osb-10.02.00.00-2.bz2	BZ2 File	254,947 KB
osb-10.02.00.00-2	Compressed (zipped) Folder	752,962 KB
sw-metadata-osb-10.02.00.00-2.json	JSON File	1 KB
usbsticksetup_osb-10.02.00.00-2	Compressed (zipped) Folder	753,170 KB
vApps_osb-10.02.00.00-2	Compressed (zipped) Folder	8 KB

1) Unzip the file “usbsticksetup_oss-*.*.*.zip”. The files will unzip into a folder called “usbsticksetup”. The contents of the “usbsticksetup” folder will look like:

Name	Type	Size
ob	File folder	
syslinux	File folder	
systemd-boot	File folder	
Readme	Text Document	1 KB
usbsticksetup	Application	2,220 KB
usbsticksetup.exe.manifest	MANIFEST File	2 KB

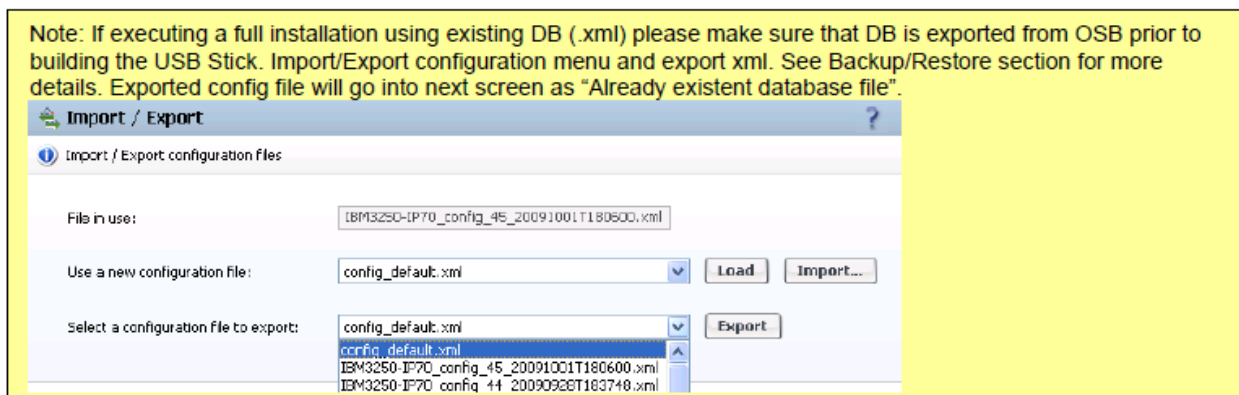
2) Copy the software image *.tar file into the ob folder. The ob folder will then look like:

Name	Type	Size
image_osb-10.02.00.00-2.tar	TAR File	730,990 KB
initrd.gz	GZ File	12,091 KB
vmlinuz	File	8,838 KB

3) The “syslinux” folder will look like:

Name	Type	Size
COPYING	File	18 KB
isolinux.bin	BIN File	44 KB
ldlinux.c32	C32 File	120 KB
ldlinux.e64	E64 File	137 KB
mkisofs	Application	378 KB
syslinux.cfg	CFG File	1 KB
syslinux.efi	EFI File	196 KB
syslinux	Application	26 KB

4) Proceed to the USB stick creation running usbsticksetup.exe application.



Up to V10R1:

USB Stick Setup

Media Select
G:\ (3,73 GB) Refresh

WARNING: all partitions of Removable Medias will be deleted and a single FAT32 partition will be created. Therefore, all data of the removable media will be erased.

Installation Method

☐ Generate node.cfg file

☒ Already existent database file J:\RD-OSB-OSSBC\OpenBranch ...

☐ Already existent node.cfg file ...

☐ Automated ☐ PreInstall ☐ Net boot ☐ DHCP

Branch Network Configuration

Hardware type: ...

Hostname: IPv6-Proxy-PRI-T1 System Name

Interface: LAN Interface

☐ Disable interface ☐ Enable IPv6

IPv4 address: 21 . 21 . 0 . 77

IPv4 netmask: 255 . 255 . 0 . 0

IPv6 address:

IPv6 netmask:

IPv4 gateway: 21 . 21 . 0 . 1

IPv6 gateway: fad0:26::1

Logical ID: WoWarcrafft:BG_RD_OSB_OSSBC:Proxy

CMP URL 1: 10.100.123.84

CMP URL 2:

Note: DB (xml) can not be used for different hardware types.

Note: DHCP, Logical ID, CMP URL, Automated, PreInstall, and Net Boot Options are covered on Simplified installation Appendix section. Fields can only be edited/clear when Automated or Net boot are selected.

Note: Partitioned USB Stick must be checked for IBM 3550 M3/ M4, IBM3250 M3/M5/ M6 and Lenovo SR250. If creating USB stick with existing DB for M3 servers, then partitioned flag must

Change Branding Names and Logo

☐ Partitioned USB Stick

OK Cancel

Min 2GB USB Stick Required

Option to create new Config File. Network interfaces configuration is required with this option.

USB Stick will be created with existing DB file (*.xml). If option is selected then Server Name and Interfaces are grayed out.

USB Stick will be created with existing Config file (*.cfg). If option is selected then Server Name and Interfaces are grayed out.

Configure LAN and WAN (If applicable/SBC). Note that each interface must be on separate subnets. Configure WAN/LAN if SBC Mode is used. Configure LAN only if proxy mode is used, and WAN when on the SBC-Proxy or IPV6-Proxy modes.

"Change Branding Names and Logo" is covered on Branding section.

Starting from V10R2:

Min 2GB USB Stick Required

Option to create new Config File. Network interfaces configuration is required with this option.

Note: DB (xml) can not be used for different hardware types.

Note: DHCP, Logical ID, CMP URL, Automated, PreInstall, and Net Boot Options are covered on Simplified installation Appendix section.

Fields can only be edited/clear when Automated or Net boot are selected.

System Name

Note: USB Stick will be created with existing DB file (*.xml). If option is selected then Server Name and Interfaces are grayed out.

Note: USB Stick will be created with existing Config file (*.cfg). If option is selected then Server Name and Interfaces are grayed out.

From V10R2, the new flag was added to set the System Boot as UEFI Mode.

“Change Branding Names and Logo” is covered on Branding section.

Note: Partitioned USB Stick must be checked for IBM/LENOVO/FUJITSU HW servers.

USB Stick Setup

Media Select: F:\ (14,3 GB)

WARNING: all data of the removable media will be erased.

Configuration database:

- ☐ Generate node.cfg file
- ☒ Already existent database file: C:\Users\user\Downloads\IPv6-Proxy-PRI-T1-osb-confl
- ☐ Already existent node.cfg file

Branch Network Configuration:

Hardware type: [Empty]

Hostname: IPv6-Proxy-PRI-T1

Interface: LAN Interface [Dropdown]

☐ Disable interface

IPv4 address: 21 . 21 . 0 . 77

IPv4 netmask: 255 . 255 . 0 . 0

IPv4 gateway: 21 . 21 . 0 . 1

☐ Enable IPv6

IPv6 address: [Empty]

IPv6 netmask: [Empty]

IPv6 gateway: fad0:26::1

Installation Method:

- ☐ Automated
- ☐ PreInstall
- ☐ Net boot
- ☐ DHCP

☐ UEFI Bootloader

General:

DNS 1: 192 . 168 . 100 . 4

DNS 2: . . .

Logical ID: 192.168.96.82

CMP URL 1: WoWarcraft:BG_RD_OSB_OSSBC:Proxy_PRI_T1

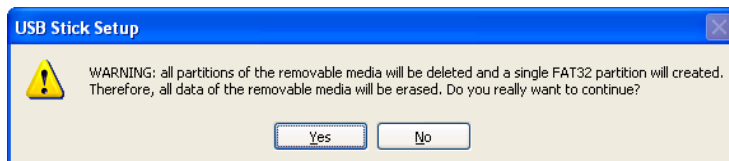
CMP URL 2: [Empty]

Change Branding Names and Logo

☐ Partitioned USB Stick

OK Cancel

5. After filling in the required information press OK to create the USB Stick.



6. After the process is concluded the USB Stick can be removed and it will be ready for installation.

Note: log from USB Stick setup tool is available on PC by selecting “Start”, “Run”, and “%TEMP%”. Log name shows as “usbsticksetup_(date).log”.

4 Full Installation

Installation erases both backup and active partitions and overwrites them with existent SW in USB. The database can be preserved if previously stored in USB stick. This option is only available if the USB stick is plugged in and the system is booting from the USBstick.

Note: Option can be done from Local GUI only. (Not supported from CMP).

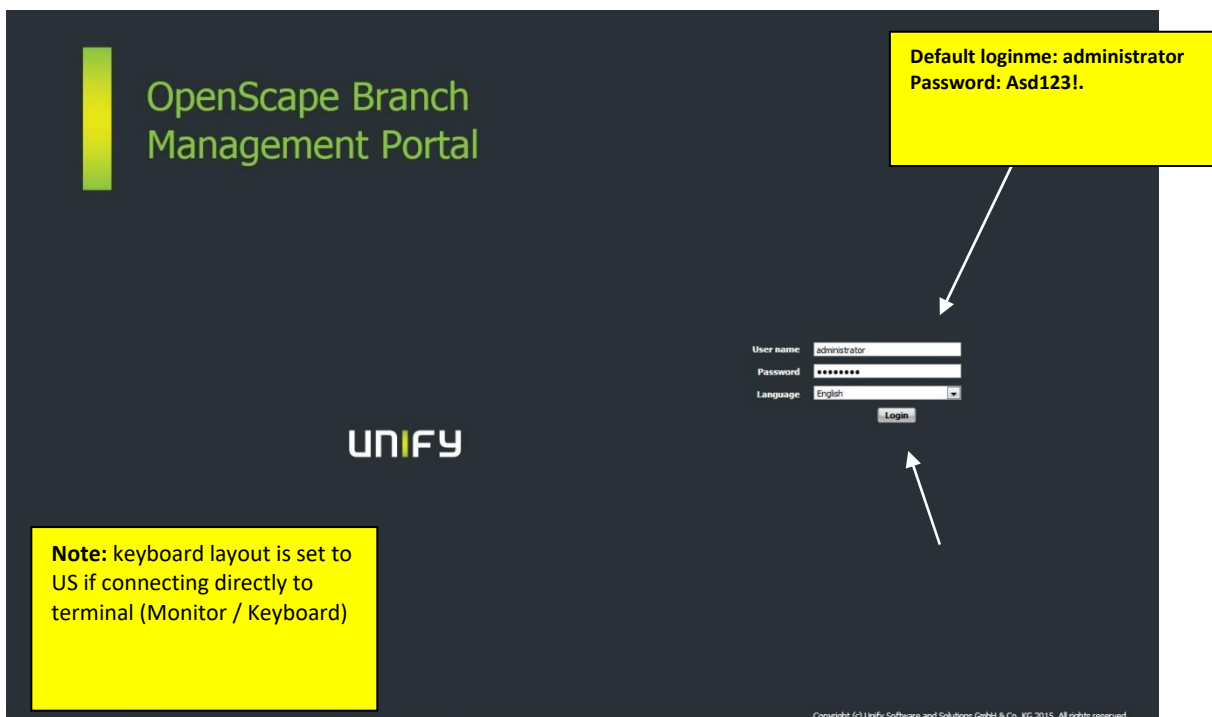
1. Restart OSB with USB connected.
2. Select the USB as the boot device during the power up sequence (F12).
3. Open the internet browser to the LAN IP (defined in the previous steps) via https:// and login as:
 - i. Username: **administrator**
 - ii. Password: **Asd123!.**

After login OSB will alert the user that OSB is running with USB stick.

Note: From V10R2, the Local GUI is optimized for current versions of Chrome, Edge and Firefox. Please note that using IE or other browsers may lead to rendering errors and/or limited functionality.

Important: The **OpenScape Branch platform** is available in following languages: **English, German and French** (starting from V10R2.1.0). You may choose the language of preference (English, German or French) before login.

- **Up to V10R1**



- Starting from V10R2

Username: administrator

Password: Asd123!.

Unify OpenScape Branch

Management Portal

User name

Password

Language

Unify Software and Solutions GmbH & Co. KG 2024. All rights reserved.

4. Go to Maintenance > Install/Upgrade tab > Full "Install" option appears
(Note that option only shows when booting from USB stick).

Maintenance

Select OK to temporarily store changes. Make your changes permanent by selecting 'Apply Changes' on the General page.

Install/Upgrade

Installation

☐ UEFI Bootloader (UEFI Bios NOT detected)

Number of Code Partitions (2-5)

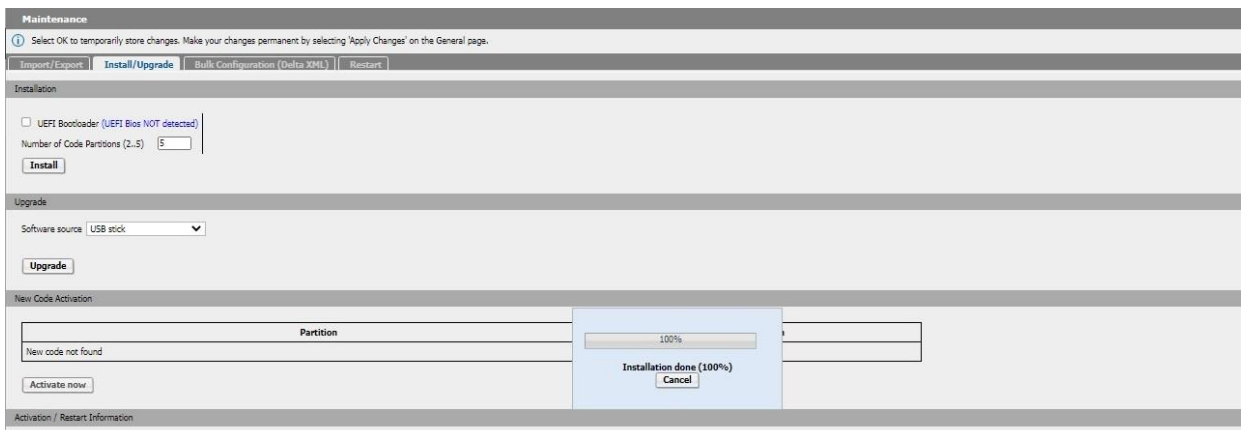
Upgrade

Software source

Note: From V10R1, there is a new option to select the number of code partitions to be created. The default is 2 (one for the active version and other for the backup version). From now on, it is possible to have until 5 partitions of code. Despite the number of partitions selected, the number created can be below due to the disk size limitations. For instance: you can select 5, but just 3 will be created.

Note: From V10R2, the UEFI bootloader flag is available in the installation option. “UEFI Bios detected” or “UEFI Bios NOT detected” message is displayed.
The UEFI bootloader flag could be activated in the USBsticksetup.
Please, pay attention to choose this option. **The System Boot Mode must be configured correctly, otherwise the Server will not boot from the Hard Drive.**

5. Press the **Install** button to perform a full installation. All previous data in the system will be lost. If the USB stick has been created with a Config/DB file then that will be applied during the installation. During the installation a progress bar indicates the progressing of tasks.



6. Once finished, a popup window is displayed indicating that the installation is completed. A request to remove the USB Stick is displayed.

21.21.10.180 says

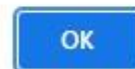
System installed. Press OK to reboot the system now.



7. Remove the USB stick and click **OK**. The system boots in about 3 minutes.

21.21.10.180 says

Please remove the USB stick before continuing.



8. Open the internet browser to the IP (defined in the previous steps) via **https://** and login as shown:

-User Name: “administrator”
-Password: “Asd123!”

Note: No configuration changes are allowed for about 5-10 minutes while process manager checks if the system is stable. If the check of installation fails, the system reboots to backup partition. In case of a full installation and if both partitions are failing, a re-installation following the same procedure is required.

21.21.142.143 says

The process manager is working to ensure that the system is stable.
Please wait a few minutes and try again.

OK

If the check of installation fails, the system will reboot to backup partition; in case of a full installation and both partitions are failing then a re-installation using same procedure is required.

Note: Administration for a standalone OpenScape Branch without CMP can be performed by the OpenScape Branch Management Portal (Local GUI). Since the OpenScape Branch is normally protected by a firewall, a tunnel must be created to allow administrative access. This tunneling capability is supported for V7 and later releases of the OpenScape Branch. To allow access to the Local GUI, a SSDP plug-in resides in the server software and can be enabled, disabled and be monitored via the Local GUI. SSDP provides a tunnel to the Local GUI from the OpenScape Branch device to the service technician's workplace. The service technician work in a Secure Infrastructure for Remote Access (SIRA) environment.

How to activate it: Login to Local GUI > Maintenance & Diagnostics Tab > Enable SSDP > Apply Changes.

It may be necessary to configure the SSDP plug-in with an HTTP proxy server via the Axeda Deployment Utility so the SSDP plug-in can contact the SSDP Enterprise Server.

9. If the configuration database has not been part of the USB stick, restore the configuration either by using the import function and a saved configuration database (Local GUI > Maintenance > Import/Export > Import) or by entering the database manually.

5 Branding

Feature allows updating the Company Name, Product Name, TLA, and Logo.

Note: Feature applies to local GUI only.

System

Select OK to temporarily store changes. Make your changes permanent by selecting 'Apply Changes' on the General page.

SettingsLicenseBranding

Branding Settings

Company nameUnify Software and Solutions

Product nameOpenScape Branch

TLACopyright (c) Unify Software and Solutions GmbH & Co. KG 2021. All rights reserved

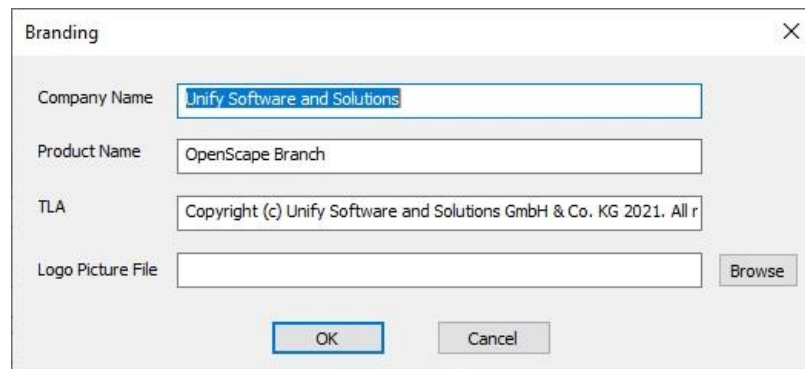
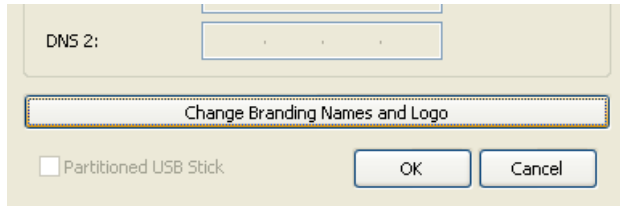
Logo picturedefaultImportDelete

Company Name: changes the Company Name that is presented on Local GUI. **Product Name:** changes the Product Name that is presented on Local GUI. **TLA:** changes the Trademark License Agreement that is presented on Local GUI.

Logo picture: changes the Logo Picture that is presented on Local GUI for the login screen and title bar. The file must be a valid image (png, jpg, gif) and should use the recommended dimension (160x40) for proper display and can not be larger than 50KB. After importing logo, it is required to "Apply Changes" so that new logoshow.

Note regarding browser cache: Any changing user interface element may not be immediately visible on all versions of all supported browsers. Browser reload discarding cache (usually Ctrl-F5) may be needed for updating the pages accordingly. Even clearing the browsing history may beneeded.

USB can be created using the updated Company Name, Product Name, TLA, and Logo so that Customized Branding parameters can be used during Full Installation.



6 OpenScape Voice (OSV) Configuration

Following configuration required in the OSV. All signaling will go through proxy.

1. OSB SIP Endpoint Configuration: create Sip Endpoint using CMP.

Configuration OpenScape Voice > BG > Members > Endpoints > Add

Note: If there is a GW behind the OSB Endpoint, then the OSB Endpoint must be set as an **Associated Endpoint** in the GW.

The image shows two screenshots of the OpenScape Voice configuration interface. The top screenshot shows the 'General' tab of the 'Endpoint' configuration page. It includes fields for Name, Remark, Registered (checked), Profile (EP227), Branch Office, Associated Endpoint, and Default Home DN. A yellow callout box notes: 'Note: End Point Profile must be created before adding End Points. OpenScape Voice > BG > Profiles > Add'. Another yellow callout box points to the 'Registered' checkbox and says 'Static Registered.'.

The bottom screenshot shows the 'Attributes' tab of the 'Endpoint' configuration page. It includes a list of attributes with checkboxes: Supports SIP UPDATE Method for Display Updates, UPDATE for Confirmed Dialogs Supported, Send Provisional response during session updates, Survivable Endpoint, SIP Proxy, Route via Proxy, Allow Proxy Bypass, Public/Offnet Traffic, Accept Billing Number, and Allow Sending of Insecure Referred-By Header. A yellow callout box notes: 'Required flags for Proxy Functionality. Note: "Do not Send Invite without SDP" attribute must NOT be selected on OSB50i/OSB500i Integrated Gateway End Point.'.

The right side of the bottom screenshot shows the 'Aliases' tab. It includes a table with columns 'Name' and 'IP Address'. A yellow callout box notes: 'OSB IP address must be configured for alias (Port is optional. Ex 10.234.1.70:5060). Note: if using OSB with Redundancy then Alias should include Redundant IP and Physical IP addresses for both OSB nodes.'.

The top right screenshot shows the 'General' tab of the 'Endpoint' configuration page. It includes fields for Type (Static), Signaling Address Type (IP Address or FQDN), Endpoint Address (10.234.1.70), Port (5060), Transport protocol (TCP), Best Effort SRTP support (MIKEY, SDES), and ANAT Support (Enabled). A yellow callout box notes: 'Note: On v6 or v7 OSV, the OSB endpoint should NOT be configured as Trusted. The only need for having this set to Trusted was for responding to OPTIONS requests. With CQ207173 (V6 PS23) and CQ207180 (V7 PS08) the OPTIONS requests are not challenged anymore regardless whether digest authentication is turned on or not.'.

Configure Endpoint as trusted if Digest Authentication is used in the OSV and OSV version is older than (OSV6 PS23) or (OSV7 PS08).

1) "Scenario where Digest Authentication is enabled in the OSV but challenges are NOT desired for SIP requests on this OSB endpoint to the OSV". Configure the Endpoint as "Trusted" for all ports. OSV parameter Srx/Sip/AuthTraverseViaHdrs can be set to "RtpFalse" since the Endpoint is configured as "Trusted" for all ports and no challenges for requests on this Endpoint will be issued from the OSV with Digest Authentication enabled.

2) "Scenario where Digest Authentication is enabled in the OSV and challenges are desired for SIP requests on this OSB endpoint to the OSV". On the Endpoint, configure as "Trusted" only the specific SIP OPTIONS port which will be used to communicate with the OSV. OSV parameter Srx/Sip/AuthTraverseViaHdrs is set to "RtpTrue" to traverse the header for the trusted port being used by OPTIONS. OSV will issue challenges for all SIP requests on this Endpoint for ports which are not trusted (all except for the port using OPTIONS). Also make sure in the OSB configuration the SIP OPTIONS are set to use this specific port as well (refer to Page 16).

2. Discover/Add Branch Office

Configuration > openScape Voice > Business Group > Branch Office List > Add

- 1) Select Add to discover Branch Office.
- 2) Setup Branch Office Name
- 3) Select SIP endpoint created in step 1 of OSV Configuration.
- 4) Select Appropriate NP and Office Code.
- 5) Check OpenScape Branch Flag.

[OSVCLUSTERV6] - BGLoad - Add Branch Office

Here you can create a Branch Office. Representative Endpoint is mandatory.

General | DID Pool | Access Control List

General

Branch Office Name IBM3250-IP70

Representative Endpoint IBM3250IP70 ...

Numbering Plan NP_BGLoad ...

Office Code (555) 888 ...

Routing Area ...

This is a Branch Office of type OpenScape Branch ☒

Select OSB
Endpoint

Note: Branch Office Flag
must be checked.

7 OpenScape Branch Configuration

OpenScape Branch tab is used to configure Branches running on OpenScape Branch Hardware. OSB 6000 (Lenovo/IBM) Supports 6000 registered subscribers; OSB 1000 (Lenovo/IBM) supports 1000 registered subscribers; OSB500i (Advantech 500i) supports 500 registered subscribers; OSB 50/250 supports 250 registered subscribers; OSB50i supports 80 subscribers; while OSB 50i A024/48 supports 24/48 FXS ports.

Select Branch Office from Branch Office list.

OpenScape Branch Overview - OSVCLUSTERV6

Use the Refresh selected button to update the status of selected OpenScape Branch appliances. To update the status of all OpenScape Branch appliances use the Refresh all button.

Filter: for Branch Office

Sel:0 | Items:100 | Page:1 | All:34

<input type="checkbox"/>	Branch Office	IP Address	Comm System	Business Group	Version	Status	Mode	Last Update
<input type="checkbox"/>	Advantech_1.56	10.234.1.56	OSVCLUSTERV6	BG_MarkP	V2R0.01.00 Build 11	Normal	Proxy	2011/07/23 09:53:37
<input type="checkbox"/>	aicharlotteosb1	10.238.16.10	OSVCLUSTERV6	EDMC				
<input type="checkbox"/>	bocaOB20_TL5	10.234.1.20	OSVCLUSTERV6	TL5galo				
<input type="checkbox"/>	bocaOB21_BL5	10.234.1.20	OSVCLUSTERV6	BGCA				
<input type="checkbox"/>	bocaOB22_OS500i	20.20.1.22	OSVCLUSTERV6	BGCA				
<input type="checkbox"/>	bocaOB23_OS500i	20.20.4.23	OSVCLUSTERV6	BGCA				
<input type="checkbox"/>	bocaOB_20	10.234.1.20	OSVCLUSTERV6	BGCA	V2R0.01.00 Build 11	Normal	Proxy	2011/07/23 09:53:37

After selecting the Branch Office user has access to Statistics, Registered Subscribers, Backup link Status (if enabled), and Link Status (OSB 50i/500i only). License Information is covered on License section.

General - OSVCLUSTERV6 - OSBIP170

Aggregated information and...

Statistics

SIP Server	Active Dialogs:	0
	Requests In:	18622
	Requests Out:	5107
	Responses In:	724
	Responses Out:	13462

System Info

Registered subscribers:

Backup link status:

Link status:

Licensing Information

First updated: --- Last updated: ---

Logical ID: OSVCLUSTERV6:BGLoad:OSBIP170 Hw ID: N/A

License type	Configured	Locally Configured	Usage
OpenScape Branch Base	0	0	0
OpenScape Branch Users	0	0	0
Auto Attendant feature	0	0	0
Backup ACD feature	0	0	0
SBC sessions	0	0	0

User can apply configuration changes by using "ApplyChanges".

Note: Depending on the changes made some processes or even the entire system will restart. GUI will alert user when restart is required.

Selecting "Cancel Changes" will revert back all changes since the last "Apply Changes"

8 Network Services

User can configure network services using this menu. A pre-defined configuration of interfaces and default gateway can be done using USB Stick Wizard.

Configuration > OpenScape Branch > Branch Office > Configuration > Network/Net Services > Settings



Network/Net Services

Select OK to temporarily store changes. Make your changes permanent by selecting 'Apply Changes' on the General page.

Settings

DNS

NTP

DHCP

Traffic Shaping

QoS

Physical Network Interface

Interface	Enabled	MTU	Speed (Mbps)	Duplex mode
eth0	<input checked="" type="checkbox"/>	1500	Auto	Auto
eth1	<input checked="" type="checkbox"/>	1500	Auto	Auto

2) Window shows Interface IP.

Note: Each subsection provides Help Links.

Note: changes to Interface Network Services will require a system restart.Eth0 cannot be disabled.

Interface Configuration

LAN configuration

Type	Interface	IP address	Subnet mask	VLAN tag	UDP port	TCP port	TLS port	MTLS port
Main IPv4	eth0	30.30.0.45	255.255.0.0	0	5060	5060	5061	5161

Add

Delete

WAN configuration

Type	Interface	IP address	Subnet mask	VLAN tag	UDP port	TCP port	TLS port	MTLS port
Main IPv4	eth1	25.25.0.45	255.255.255.0	0	5060	5060	5061	C

Add

Delete

VLAN: it is possible to configure VLAN by editing the interfaces.

1 - Routers should be already configured to use VLAN TAG

2 - The LAN address (interface 1) should not share the same subnet which VLAN is using. 3 – LAN interface requires a dummy IP when VLAN is active.

Ex...

```

openbranch_lan: 10.90.0.253 255.255.240.0
openbranch_vlan: 10.200.0.29 255.255.240.0 200
openbranch_wan: 0.0.0.0 0.0.0.0
openbranch_gw: 10.200.0.1

```

Network/Net Services

Select OK to temporarily store changes. Make your changes permanent by selecting 'Apply Changes' on the General page.

Settings | DNS | NTP | DHCP | Traffic Shaping | QoS

Physical Network Interface

Interface	Enabled	MTU	Speed (Mbps)	Duplex mode
eth0	<input checked="" type="checkbox"/>	1500	Auto	Auto
eth1	<input checked="" type="checkbox"/>	1500	Auto	Auto

☐ Interface bonding

Interface Configuration

LAN configuration

Add **Delete**

Type	Interface	IP address	Subnet mask	VLAN tag	UDP port	TCP port	TLS port	MTLS port
Main IPv4	eth0	192.168.108.198	255.255.255.224	0	5060	5060	5061	5

OK **Cancel**

Window shows Interface IP.
 Note: Each subsection provides Help Links.
 Note: changes to Interface Network Services will require a system restart.Eth0 cannot be disabled.

Interface Bonding –
 checkbox for enabling the creation of bonding groups composed of multiple (at least two) Ethernet interfaces.

8.1 Ethernet Interface Bonding

Ethernet Bonding provides the OSB user with the ability to create bonding groups composed of multiple (at least two) Ethernet interfaces. Bonding groups are useful for providing 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.

Model	Mode	# Eth	# Bond	Notes
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)

Model	Mode	# Eth	# Bond	Notes
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) AND/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
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) AND/OR bond1=eth1+(eth3 or eth2)

Example 1 - OSB with 2 ethernet ports (eth0, eth1))

Note:Bonding is allowed only when WAN is not configured or required (SBC modes).

Note:Bonding is restricted to the LAN (bond0). eth1 must be enabled before selecting it to be part of a bonding group (bond0).

Physical Network Interface

Interface	Enabled	MTU	Speed (Mbps)	Duplex mode
eth0	<input checked="" type="checkbox"/>	1500	Auto	Auto
eth1	<input checked="" type="checkbox"/>	1500	Auto	Auto

1 ☒ Interface bonding

Bond interface	Enabled	Type	eth0	eth1
bond0	<input checked="" type="checkbox"/>	Redundancy	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

Interface Configuration

LAN configuration

Add Delete

Type	Interface	IP address	Subnet mask	VLAN tag	UDP port	TCP port
Main IPv4	bond0	10.200.0.111	255.255.240.0	0	5060	

Network/Net Services

Select OK to temporarily store changes. Make your changes permanent by selecting 'Apply Changes' on the General page.

Settings DNS NTP DHCP Traffic Shaping QoS

Routing

Default gateway address 10.200.0.1

Default gateway IPv6 address

Routing configuration

Add Delete

Row	Destination	Gateway	Netmask	Interface
1	10.201.35.78	10.200.0.34	255.255.240.0	bond0

Network/Net Services

Select OK to temporarily store changes. Make your changes permanent by selecting 'Apply Changes' on the General page.

Settings DNS NTP DHCP Traffic Shaping QoS

General

☒ Enable traffic shaping

Add Delete

Row	Parent class ID	Class ID	Interface	Default class ID	Description	Rate (Kbps)	Ceiling rate (Kbps)	Burst (Kbytes)	Ceiling burst (Kbytes)	mtu	Priority
1		3ff	bond0	0	traffic 1	60					

Network/Net Services

Select OK to temporarily store changes. Make your changes permanent by selecting 'Apply Changes' on the General page.

Settings DNS NTP DHCP Traffic Shaping QoS

QoS Settings

☒ Enable QoS

DSCP for SIP 26

DSCP for RTP 46

Add Delete

Row	Protocol	In interface	Out interface	Port	DSCP	Mark
1	All	bond0	all			

Example 2 - OSB with 4 ethernet ports (eth0, eth1,eth3,eth4))

Note: If OSB is configured in one of the SBC modes, a second bond group (bond1) will be available.

Note: If bond1 is available, eth1 will not be allowed on LAN bond group (bond0). eth0 is not allowed on bond1 (if present).

Note: eth2 and eth3 interfaces are enabled automatically when selected on bond group.

Network/Net Services

Select OK to temporarily store changes. Make your changes permanent by selecting 'Apply Changes' on the General page.

Settings | DNS | NTP | DHCP | Traffic Shaping | QoS

Physical Network Interface

Interface	Enabled	MTU	Speed (Mbps)	Duplex mode
eth0	<input checked="" type="checkbox"/>	1500	Auto	Auto
eth1	<input checked="" type="checkbox"/>	1500	Auto	Auto
eth2	<input type="checkbox"/>	1500	Auto	Auto
eth3	<input checked="" type="checkbox"/>	1500	Auto	Auto

☒ **Interface bonding** 1

Bond interface	Enabled	Type	eth0	eth1	eth2	eth3
bond0	<input checked="" type="checkbox"/> 3	Redundancy	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/> 2

Interface Configuration

LAN configuration

Add **Delete**

Type	Interface	IP address	Subnet mask	VLAN tag	UDP port	TCP
Main IPv4	bond0	21.21.0.150	255.255.0.0	0	5060	

WAN configuration

Add **Delete**

Type	Interface	IP address	Subnet mask	VLAN tag	UDP port	TCP
Main IPv4	eth1	21.22.0.151	255.255.0.0	0	5060	

Network/Net Services

Select OK to temporarily store changes. Make your changes permanent by selecting 'Apply Changes' on the General page.

Settings DNS NTP DHCP Traffic Shaping QoS

Routing

Default gateway address 21.21.0.1

Default gateway IPv6 address

Routing configuration

Add Delete

Row	Destination	Gateway	Netmask	Interface
1	10.198.67.36	21.21.0.45	255.255.240.0	bond0

eth1

bond0

Network/Net Services

Select OK to temporarily store changes. Make your changes permanent by selecting 'Apply Changes' on the General page.

Settings DNS NTP DHCP Traffic Shaping QoS

General

☒ Enable traffic shaping

Add Delete

Row	Parent class ID	Class ID	Interface	Default class ID	Description	Rate (Kbps)	Ceiling rate (Kbps)	Burst (Kbytes)	Ceiling burst (Kbytes)	mtu	Priorit
1			eth1								

eth1

bond0

Network/Net Services

Select OK to temporarily store changes. Make your changes permanent by selecting 'Apply Changes' on the General page.

Settings DNS NTP DHCP Traffic Shaping QoS

QoS Settings

☒ Enable QoS

DSCP for SIP: 26

DSCP for RTP: 46

Add Delete

Row	Protocol	In interface	Out interface	Port	DSCP	Mark
1	All	All	all			

all
eth1
bond0

Network/Net Services

Select OK to temporarily store changes. Make your changes permanent by selecting 'Apply Changes' on the General page.

Settings DNS NTP DHCP Traffic Shaping QoS

Physical Network Interface

Interface	Enabled	MTU	Speed (Mbps)	Duplex mode
eth0	<input checked="" type="checkbox"/>	1500	Auto	Auto
eth1	<input checked="" type="checkbox"/>	1500	Auto	Auto
eth2	<input checked="" type="checkbox"/>	1500	Auto	Auto
eth3	<input checked="" type="checkbox"/>	1500	Auto	Auto

☒ Interface bonding

Bond interface	Enabled	Type	eth0	eth1	eth2	eth3
bond0	<input checked="" type="checkbox"/>	Redundancy	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
bond1	<input checked="" type="checkbox"/>	Load sharing	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>

Interface Configuration

LAN configuration

Add Delete

Type	Interface	IP address	Subnet mask	VLAN tag	UDP port	TCP port	TLS port
Main IPv4	bond0	21.21.0.150	255.255.0.0	0	5060	5060	5061

WAN configuration

Add Delete

Type	Interface	IP address	Subnet mask	VLAN tag	UDP port	TCP port	TLS port
Main IPv4	bond1	21.22.0.151	255.255.0.0	0	5060	5060	5061

Network/Net Services

Select OK to temporarily store changes. Make your changes permanent by selecting 'Apply Changes' on the General page.

Settings DNS NTP DHCP Traffic Shaping QoS

Routing

Default gateway address 21.21.0.1

Default gateway IPv6 address

Routing configuration

Add Delete

Row	Destination	Gateway	Netmask	Interface
1				bond0

Network/Net Services

Select OK to temporarily store changes. Make your changes permanent by selecting 'Apply Changes' on the General page.

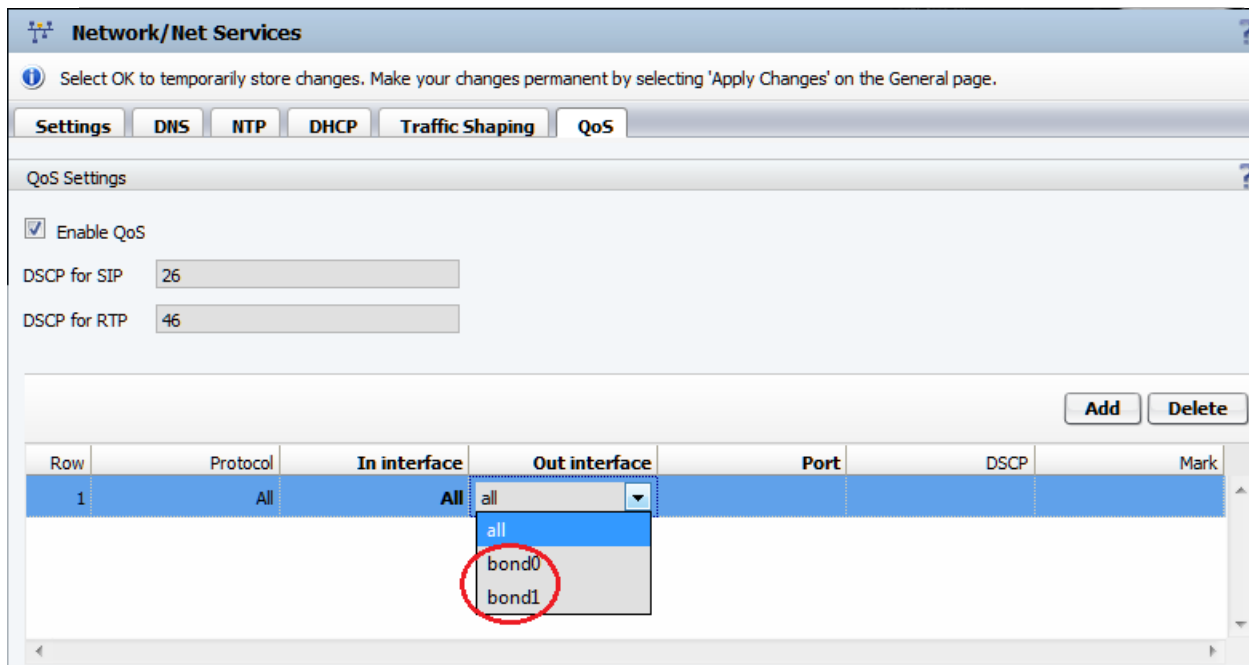
Settings DNS NTP DHCP Traffic Shaping QoS

General

☒ Enable traffic shaping

Add Delete

Row	Parent class ID	Class ID	Interface	Default class ID	Description	Rate (Kbps)	Ceiling rate (Kbps)	Burst (Kbytes)	Ceiling burst (Kbytes)	mtu	Priorit
1			bond0								



Terminal (OSB with 4 ethernet ports (eth0, eth1, eth2, eth3) in SBC mode

```
lenovo:/home/administrator # cat /etc/sysconfig/network/ifcfg-eth0
BONDING_MASTER=yes
BONDING_MODULE_OPTS="mode=active-backup miimon=100"
BONDING_SLAVE0=seth0
BONDING_SLAVE1=seth2
BOOTPROTO=static
MTU=1500
IPADDR=21.21.0.150
NETMASK=255.255.0.0
STARTMODE=auto
USERCONTROL=no
lenovo:/home/administrator # cat /etc/sysconfig/network/ifcfg-eth1
BONDING_MASTER=yes
BONDING_MODULE_OPTS="mode=balance-rr miimon=100"
BONDING_SLAVE0=seth1
BONDING_SLAVE1=seth3
BOOTPROTO=static
MTU=1500
IPADDR=21.22.0.151
NETMASK=255.255.0.0
STARTMODE=auto
USERCONTROL=no
lenovo:/home/administrator
```

```

lenovo:/home/administrator # ifconfig
eth0      Link encap:Ethernet  HWaddr 40:F2:E9:BB:E5:D0
          inet addr:21.21.0.150  Bcast:21.21.255.255  Mask:255.255.0.0
          inet6 addr: fe80::42f2:e9ff:febb:e5d0/64 Scope:Link
          UP BROADCAST RUNNING MASTER MULTICAST  MTU:1500  Metric:1
          RX packets:3006 errors:0 dropped:0 overruns:0 frame:0
          TX packets:559 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:266010 (259.7 Kb)  TX bytes:56598 (55.2 Kb)

eth1      Link encap:Ethernet  HWaddr 40:F2:E9:BB:E5:D1
          inet addr:21.22.0.151  Bcast:21.22.255.255  Mask:255.255.0.0
          inet6 addr: fe80::42f2:e9ff:febb:e5d1/64 Scope:Link
          UP BROADCAST RUNNING MASTER MULTICAST  MTU:1500  Metric:1
          RX packets:2696 errors:0 dropped:0 overruns:0 frame:0
          TX packets:4 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:271177 (264.8 Kb)  TX bytes:536 (536.0 b)

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:65536  Metric:1

RX packets:2498 errors:0 dropped:0 overruns:0 frame:0
TX packets:2498 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:0
RX bytes:1507596 (1.4 Mb)  TX bytes:1507596 (1.4 Mb)

seth0     Link encap:Ethernet  HWaddr 40:F2:E9:BB:E5:D0
          UP BROADCAST RUNNING SLAVE MULTICAST  MTU:1500  Metric:1
          RX packets:3006 errors:0 dropped:0 overruns:0 frame:0
          TX packets:559 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:266010 (259.7 Kb)  TX bytes:56598 (55.2 Kb)
          Interrupt:16

seth1     Link encap:Ethernet  HWaddr 40:F2:E9:BB:E5:D1
          UP BROADCAST RUNNING SLAVE MULTICAST  MTU:1500  Metric:1
          RX packets:2696 errors:0 dropped:0 overruns:0 frame:0
          TX packets:4 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:271177 (264.8 Kb)  TX bytes:536 (536.0 b)
          Interrupt:17

seth2     Link encap:Ethernet  HWaddr 40:F2:E9:BB:E5:D0
          UP BROADCAST SLAVE MULTICAST  MTU:1500  Metric:1

RX packets:0 errors:0 dropped:0 overruns:0 frame:0
TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:1000
RX bytes:0 (0.0 b)  TX bytes:0 (0.0 b)
Interrupt:16

seth3     Link encap:Ethernet  HWaddr 40:F2:E9:BB:E5:D1
          UP BROADCAST SLAVE MULTICAST  MTU:1500  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:0 (0.0 b)  TX bytes:0 (0.0 b)
          Interrupt:17

```

lenovo:/home/administrator #

Network/Net Services

Select OK to temporarily store changes. Make your changes permanent by selecting 'Apply Changes' on the General page.

Settings | DNS | NTP | DHCP | Traffic Shaping | QoS

Routing

Default gateway address: 25.25.0.1

Default GW IP Address for OSB

Routing configuration

Add Delete

Row	Destination	Gateway	Netmask	Interface
-----	-------------	---------	---------	-----------

3) Routing Configuration allows user to configure IP routes. Routing table is created and is possible to configure the destination IP address, gateway IP address, network mask and choose which interface will be used to route the IP packets.

Redundancy

☒ Enable redundancy ☐ Enable PRI/CAS redundancy Failed links threshold: [dropdown] ☐ Switchover without Link Check

☐ Test Default Gateway instead of subscribers during failover

Interface	IP address	Backup IP address	Virtual IP Address
-----------	------------	-------------------	--------------------

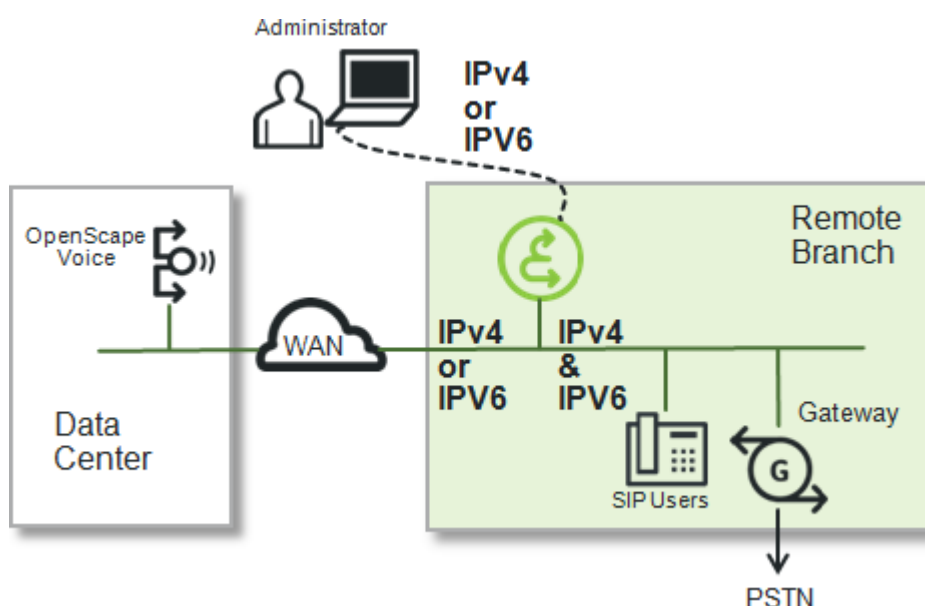
Enable Redundancy – This flag enables the redundancy and will be detailed in another section

OK Cancel

9 OSB IPV6 for Administration

OpenScope Branch can also support the OSB Administration Interface to be IPv6.

- IPv6 and IPv4 to Gateways and SIP users
 - IPv4 or IPv6 connection to the data center
 - IPv4 or IPv6 for administration services
-
- OSB can be used as a GW-only for IPv6-SSP's No dual Stack Support
(Interfaces LAN=IPv4 and WAN=IPv6)



10 IPV6 Support for SIP Devices

This feature introduced the support of IPv6 from OSB **only** in Proxy Mode (LAN > IPv4 and WAN > IPv6) or SBC-Proxy modes. First step is to enable WAN interface with the support of IPv6 on Settings Tab (under Network/Net Services).

Configuration > OpenScope Branch > Branch Office > Configuration > Network/Net Services > Settings

WAN configuration

Type	Interface	IP address	Subnet mask	VLAN tag	UDP port	TCP port	TLS port	MTLS port	Message r.
Main IPv6	eth1	fd00:10:10:200::10	ffff:ffff:ffff:ffff::	0	5060	5060	5061	5161	
Main IPv4									
VLAN IP									
Main IPv6									
Main admin									

Second step is to determine the kind of connection with OSV, either IPv4 or IPv6 on Sip Server Settings (under VOIP tab).

Configuration > OpenScope Branch > Branch Office > Configuration > VoIP > Sip Server Settings

The screenshot shows the 'Sip Server Settings' configuration window. The 'General' tab is selected. The 'Comm System Type' is set to 'geo-separated'. The 'OPTIONS source port' is set to '5060'. The 'IP Version Towards SIP Server' is set to 'IPv4'. There are two checkboxes: 'Enable path tagging' and 'Branch behind SBC', both of which are unchecked.

Please note the following table that indicates the phone configuration whether it is operating with IPv4 or IPv6.

IP version from phone to OSB	IP version Towards SIP Server		
		IPv4	IPv6
	IPv4	SIP Gateway = OSB SIP Server = OSV SIP Registrar = OSV Proxy failure – fallback to OSV*	SIP Gateway = OSB SIP Server = OSB SIP Registrar = OSB Proxy failure – no fallback to OSV*
	IPv6	SIP Gateway = OSB SIP Server = OSB SIP Registrar = OSB Proxy failure – no fallback to OSV*	SIP Gateway = OSB SIP Server = OSV SIP Registrar = OSV Proxy failure – fallback to OSV*

Note: It is not possible to configure both IPV6 and IPV4 for the same interface and no IPV6 administration is supported at the moment.

*OSV/OSS fallback would be possible, for instance on a IPV6 phone and IPV4 OSV with fallback, the phone configuration would be: SIP Server -> OSS OPv6/FQDN address, SIP Registrar -> OSSIPv6/FQDN address.

Notes: Check the OSS fallback configuration for further details and for duplex, use DNS SRV accordingly.


OSB Proxy IP version to Data Center			
IP version from GW Only/ATA to OSB	OSB Proxy IP version to Data Center		
	IPv4	IPv4	IPv6
		Outbound Proxy = OSB Proxy Node 1 Primary = OSV Node 1 Node 1 Backup = OSV Node 2 Node 2 Primary = OSV Node 2 Node 2 Backup = OSV Node 1 Proxy	Outbound Proxy = OSB Proxy Node 1 Primary = OSB Proxy Node 1 Backup = <empty> Node 2 Primary = <empty> Node 2 Backup = <empty> Proxy failure – no fallback

The only way to get fallback in case of OSB Proxy failure is by means of an alternative route through an OS SBC. In this case, the Node 1 Backup shall be configured with the OS SBC WAN IP address which shall also be using IPv4.

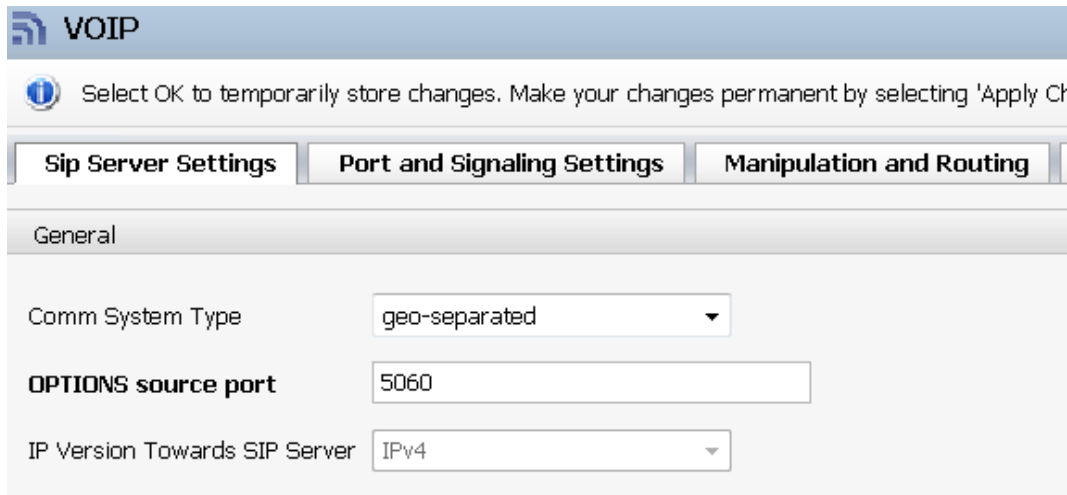
11 OSB IPv6 support for SIP trunks

This feature introduces the communication with SIP Service Providers via IPv6. So additionally to Proxy Mode, SBC Proxy supports IPv6 on its WAN side.

First step is the configuration of WAN interface with IPv6 (already mentioned above).

The flag "IP Version towards SIP server" will be grayed out with content value IPv4 (under VOIP  SIP Server Settings).

Configuration  OpenScope Branch  Branch Office  Configuration  VoIP  Sip Server Settings



VOIP

Select OK to temporarily store changes. Make your changes permanent by selecting 'Apply Changes'.

Sip Server Settings | Port and Signaling Settings | Manipulation and Routing

General

Comm System Type: geo-separated

OPTIONS source port: 5060

IP Version Towards SIP Server: IPv4


According to the requirements, three topologies are supported for connection to IPv6 SSP. For this reason it is allowed from now on to configure an SBC Proxy with IPv6 support as Gateway only.


Topology 1: OSB in SBC Proxy Mode (LAN IPv4, WAN IPv6) , SSP IPv6 , OSV IPv4

Topology 2: OSB_1 in SBC Proxy Mode (LAN IPv4, WAN IPv6) and Gateway Only, SSP IPv6 connected to OSB_1, OSB_2 Proxy Mode (LAN IPv4, WAN IPv6) connected to OSB_1, OSV IPv6 connected to OSB_2, external IPv4 phones

Topology 3: OSB_1 in SBC Proxy Mode (LAN IPv4, WAN IPv6) and Gateway Only, SSP IPv6 connected to OSB_1, OSB_2 Proxy Mode (LAN IPv4, WAN IPv6) connected to OSB_1, OSV IPv4 connected to OSB_2, external IPv6 phones

by SSP" (SSP configuration) flag will be grayed out and the available Gateway/Trunk rules will be the following:
 LAN – Integrated Gateway (only if 50i/500i HW).
 WAN – SIP Service Provider
 Furthermore the second OSB (OSB_2) mentioned on topologies 1 and 2 above will have a new option on Gateway/Trunk Type "OSB with SSP".

 **Gateway Configuration**

 Gateway configuration provisioning.

General

Signaling address type

IP address or FQDN

Remote URL

Port

5060

Interface

LAN

Transport

TCP

Mapped port

9001

Routing prefix

Gateway/Trunk type

RG

Functional type

3k/4k
Backup Link Server
Dynamic Video Peer
Mediatrrix
OSB 50i/500i
OSB with SSP
Others

Trunk profile

Output digit strip

Output digit add

Priority

Peer OSB
Proxy ATA
RG
SIP Trunk
VoiceMail

☐ Operational Mode in OPTIONS Response

12 Users/Password Recovery/Change

Configuration > OpenScape Branch > Branch Office > Configuration > Security > General > Passwords

Passwords

User name: administrator

Current password:

New password:

Confirm new password:

Change Reset

Passwords section allows user to change Password. Reset password defaults administrator password back to **Asd123!**.
Note: password change applies immediately. It is not required to select "Apply Changes" on main OSB screen.

12.1 Users/Passwords

Default users/passwords for OSB:

User: **administrator**, Password: **Asd123!**.
User: **service**, Password: **BF0bpt@x**
User: **cdr**, Password: **MNY9\$dta**
User: **ACD**, Password: **3jMp!ee9**

User: **root**, Password: **T@R63dis**
User: **guest**, Password: **1clENtk=**
User: **assistant**, Password: **2GwN!gb4**

Note: SSH access for root is disabled by default.

Default users rights/groups for OSB:

User	Assistant	Local GUI	ssh/sftp	Groups	Rights to Change/Reset Passwords
guest	No access	Read only	No access	user	guest
assistant	Read and Write	No access	sftp only	assistant, sshlogin	All users.
cdr	No access	No access	sftp only	cdr, sshlogin	cdr
ACD	No access	Read only (Read and Write for ACD parameters)	ssh only	user, sshlogin	ACD
administrator	No access	Read and Write	ssh/sftp (Read only)	user, sshlogin	All users.
service	No access	Read and Write	ssh/sftp (Read and Write)	www, user, admin, sshlogin, assistant	All users.
root	No access	Read and Write	ssh/sftp (Read and Write)	root	All users.

13 Administration Accounts

Administration accounts configuration for the firewall/routing settings of OSB.

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.

The screenshot shows the 'Security' configuration window with the 'Administrator Accounts' tab selected. The window has a title bar 'Security' and a subtitle 'Select OK to temporarily store changes. Make your changes permanent by selecting 'Apply Changes' on the General page.' Below the subtitle are tabs: 'General', 'Firewall', 'Message Rate Control', 'RADIUS', 'Tunnel Connections', and 'Denial of Service Mitigation'. The 'Administrator Accounts' section is active, showing a table of accounts and buttons for 'Add', 'Edit', and 'Delete'.

	User name	Administrative privilege	Change Password in first login	Expires (days)	Enabled
1	administrator	Administrator	<input type="checkbox"/>	99999	<input checked="" type="checkbox"/>
2	service	Administrator	<input type="checkbox"/>	99999	<input checked="" type="checkbox"/>
3	guest	Read Only	<input type="checkbox"/>	99999	<input checked="" type="checkbox"/>
4	assistant	Administrator	<input type="checkbox"/>	99999	<input checked="" type="checkbox"/>
5	redundancy	Read Only	<input type="checkbox"/>	99999	<input checked="" type="checkbox"/>
6	newUser1	Network and Security Administrator	<input checked="" type="checkbox"/>	99999	<input checked="" type="checkbox"/>

The screenshot shows the 'Administrator Account' configuration window. It has a title bar 'Administrator Account' and a subtitle 'Select OK to temporarily store changes. Make your changes permanent by selecting 'Apply Changes' on the General page.' The 'Administrator Profile' section is active, showing fields for 'Account Enabled', 'User name', 'Password', 'Confirm password', 'Privilege', 'Expires (days)', 'SSH login', and 'Change Password in first login'. A dropdown menu for 'Privilege' is open, showing options: 'Administrator', 'Network Administrator', 'Security Administrator', 'Network and Security Administrator', and 'Read Only'.

☒ Account Enabled

User name:

Password:

Confirm password:

Privilege: (dropdown menu open)

Expires (days):

☐ SSH login

☒ Change Password in first login

Privilege dropdown options: Administrator, Network Administrator, Security Administrator, Network and Security Administrator, Read Only

Buttons: OK, Cancel

Administrator Profile

Account enabled - This flag is used to grant login r Management Portal) to users. Enabled by default.
The flag is disabled & grayed out for assistant & redundancy u

User Name - User name of the Administrator account. **Password** - The password for the Administrator account user **Confirm Password** - Confirm & verify the Administrator ac password.

Privilege - Administrative privileges. Possible values: **Network Administrator, Security Administrator, Networ Administrator, Read Only**.

Expires (days) - The password expiration timeslot. Possible v **SSH login** - Login to the Linux open source application that exchanged using a secure channel between two networked d by default.

Change password in first login - When adding a new u **Password** in first login is enabled by default, & the Expires p 99999, meaning the password will not expire.

NOTE:

Only user root has the privilege to change the password of other users without knowing the current password.

Users with privileges "Administrator", "Security Administrator" and "Network and Security Administrator" are able to define the password of other users only when adding the user.

After that, only the user itself can change the password providing the current and new password.

14 Radius

OpenScape Branch supports Radius Authentication and Accounting which provides a way of identifying a user before allowing access to aclient.

Note: RADIUS is supported with redundant OSBs. Users on each physical OSB are authenticated via RADIUS so the physical IP addresses of each of the OSBs (not the Virtual IP) must be configured in the RADIUS servers.

Configuration > OpenScape Branch > Branch Office > Configuration > Security > Radius

Note: different applications allow different numbers of characters in a username. CLI allows 44, while SSH and HTTPS allow 254. It is recommended that the customer limits his/her usernames to 44 characters on all three applications.

15 SSH with PKI and Certificate files for WEB Server

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 using a password. This is done by storing the external user's public key on the OpenScape Branch.

To configure a PKI for SSH the following steps shall be executed:

- Enable PKI Configuration;
- Open the PKI Configuration screen;
- Click on the Add button;
- Select the internal user (administrator or service) to which the key will be associated;
- Select the public key file and click to import it;
- Apply the configuration.

Security
Select OK to temporarily store changes. Make your changes permanent by selecting 'Apply Changes' on the General page.

General Firewall Message Rate Control **RADIUS** Tunnel Connections Denial of Service Mitigation

RADIUS Settings

☒ Enable RADIUS

Address: Port: Secret: Timeout (sec):

Server 1: 10.234.2.230 radius: 3

Server 2: 10.234.2.231 radius: 3

☒ Enable RADIUS Authentication

Apply To: ☒ CLI ☒ SSH ☒ WEB

☒ Enable RADIUS Accounting

Apply To: ☒ CLI ☐ SSH ☐ WEB

Note: internal accounts "assistant" and "redundant" users must not be created on Radius server.

Note: Use of the 'su' command performs local authentication (CLI and SSH only).

Enable Radius: enables RADIUS Server feature.
IP Address/FQDN: Two RADIUS Servers IPs/FQDNs can be configured in the fields "Server 1" and "Server2". Server 2 is optional.
Port: 0-65535 or radius (1812/1813).
Note: Port number for accounting is hard-coded to be the next value up from the authentication port number (ex. 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: used to authenticate radius requests. 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: ~!@#\$%^&*()_+|=~'{}[]:~";<>?/.,
Note: secret 2 must be configured if Server2 IP/FQDN is configured.
Timeout: how long the OpenScape Branch will wait for a response from Server. Note: 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 the local authentication will be used

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 Client and
 WEB - controls the users using an Internet Browser.

Security
Select OK to temporarily store changes. Make your changes permanent

General Firewall Message Rate Control **RADIUS** Tunnel Connections Denial of Service Mitigation

Certificates
Shared secret files Certificate management

PKI Configuration
☒ Enable PKI configuration PKI configuration

Administrator Accounts

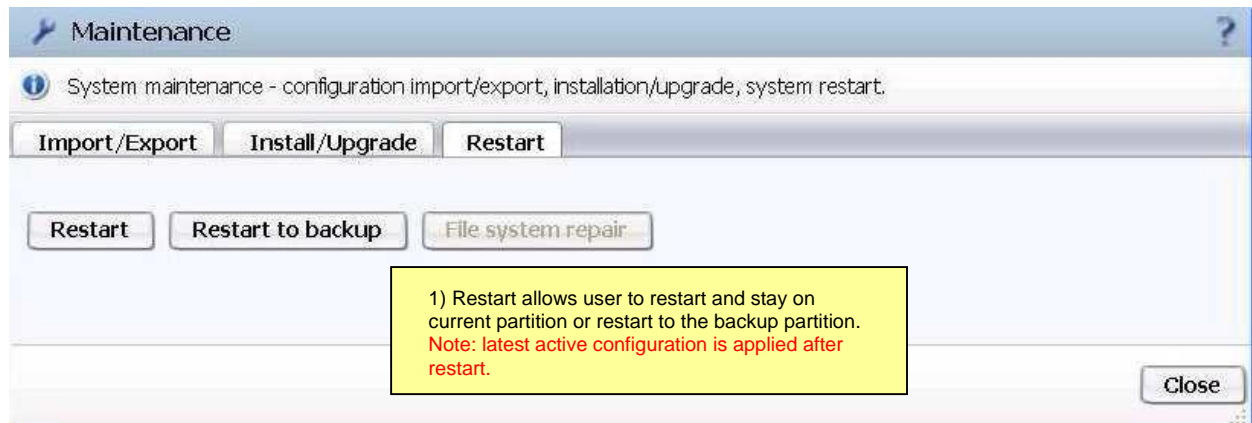
	User name	Administrative privilege
1	administrator	Administrative privilege
2	service	Administrative privilege
3	guest	Read Only
4	assistant	Administrative privilege
5	redundancy	Read Only
6	ACD	ACD Administrative privilege
7	cdr	Read Only

RD-OSB-50i-20 - Add/Update Public Key - Google Chrome
 Not secure | https://21.21.0.9/AddUpdatePki.html?writeCounter=1
Add/Update Public Key
 Select OK to temporarily store changes. Make your changes permanent by selecting 'Apply Changes' on the General page.
Add Public Key
 Associated Internal User Name:
 Public Key File:
 Choose File No file chosen Import

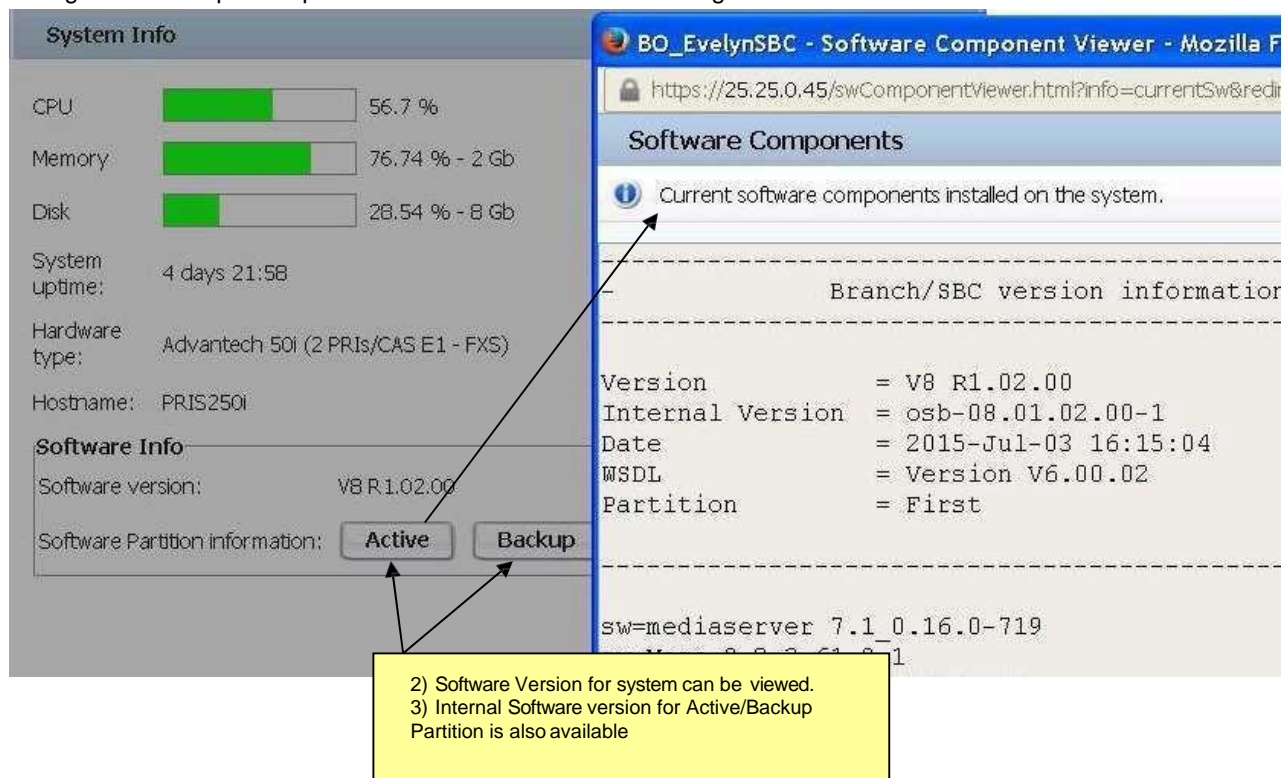
16 Utilities (Reboot + Version Information)

User can restart system to current or backup partition. It is also possible to show software information. (Health Check and Configuration Export/Import is covered later on)

Configuration > OpenScape Branch > Branch Office > Configuration > Maintenance > Restart



Configuration > OpenScape Branch > Branch Office > Configuration > local Dashboard



17 Time Settings/NTP

User can configure NTP server and time settings under Network Services. Configuration > OpenScope Branch > Branch Office > Configuration > Network/Net Services > NTP.

The screenshot shows the 'Network/Net Services' configuration page with the 'NTP' tab selected. The page includes a header with a warning icon and text: 'Select OK to temporarily store changes. Make your changes permanent by select'. Below the header are tabs for 'Settings', 'DNS', 'NTP', 'Traffic Shaping', and 'QoS'. The 'NTP Settings' section contains a 'Region' dropdown menu set to 'Asia' and a 'Timezone' dropdown menu set to '(GMT +07:00) Jakarta'. There are three radio buttons: 'Enable local NTP server' (checked), 'Manual configuration', and 'Synchronize with NTP server'. The 'Manual configuration' section has fields for 'Date' (02.26.2019) and 'Time' (16:20), with an 'Apply' button. The 'Synchronize with NTP server' section has an 'NTP server' text field, an 'Add' button, a list box containing '192.168.100.4', a 'Delete' button, and a 'Synchronize now' button. Annotations include: a yellow box at the top right stating 'NTP tab provides Date & Time Settings as well as Local NTP Server'; a yellow box pointing to the Region dropdown stating 'Drop list with the available Regions that relates to the Timezones in the selected region.'; a yellow box at the bottom left stating 'Enable Local NTP Server - SBC will act as NTP server for the Branch'; and a yellow box at the bottom right containing instructions for Time Zone, Manual Configuration, Synchronize with NTP server, and NTP Server, along with a note about system restarts.

NTP tab provides Date & Time Settings as well as **Local NTP Server**

Drop list with the available **Regions** that relates to the **Timezones** in the selected region.

Enable Local NTP Server - SBC will act as NTP server for the Branch

Time Zone: select Time Zone from Drop down menu.
Manual Configuration - Date/Time: set the Date/Time manually.
Synchronize with NTP server: will define a server for automatic adjustments
NTP Server: IP address for NTP Server.

Note: Some changes will require a system restart.

NOTE: Up to three DNS Servers can be configured.
If IPV6 is enabled, NTP Server can be an IPV6 address.

NOTE: If Redundancy is active, system will use physical IP for NTP queries. So, for slave synchronization the physical IP of both Master and Slave OpenScope SBC must be added to NTP Server firewall list.

18 VOIP Configuration

User can configure VOIP parameters. Some configuration changes will cause the SIP server to restart, active and ongoing calls may fail.

Configuration > OpenScape Branch > Branch Office > Configuration > VoIP

18.1. PROXY Mode

18.2. SIP Server Configuration

User has to configure OpenScape Branch mode under System configuration: **Note: changes to OpenScape Branch mode require a system restart.**

Configuration > OpenScape Branch > Branch Office > Configuration > System > Settings

StandAlone mode Activation - is under the System Tab, "Enable StandAlone Mode" flag will reboot the system and check for the proper license

50IDP245A - System - Google Chrome

https://25.25.0.45/systemConfiguration.html?tabId=systemTab

System

Select OK to temporarily store changes. Make your changes permanent by selecting 'Apply Changes' on the General page.

Settings | License | Branding

General

Branch mode SBC-Proxy ← SBC-Proxy Only - This is the only mode supported for the standalone

Hostname 50IDP245A

Domain name unify.com

☐ Gateway only

☒ Enable Standalone Mode ← Set the Standalone Mode to configure this operation mode.

Country configuration

Country Brazil Country configuration

Administration

Session expiry timer 3 hours

Default language English

Watchdog Configuration

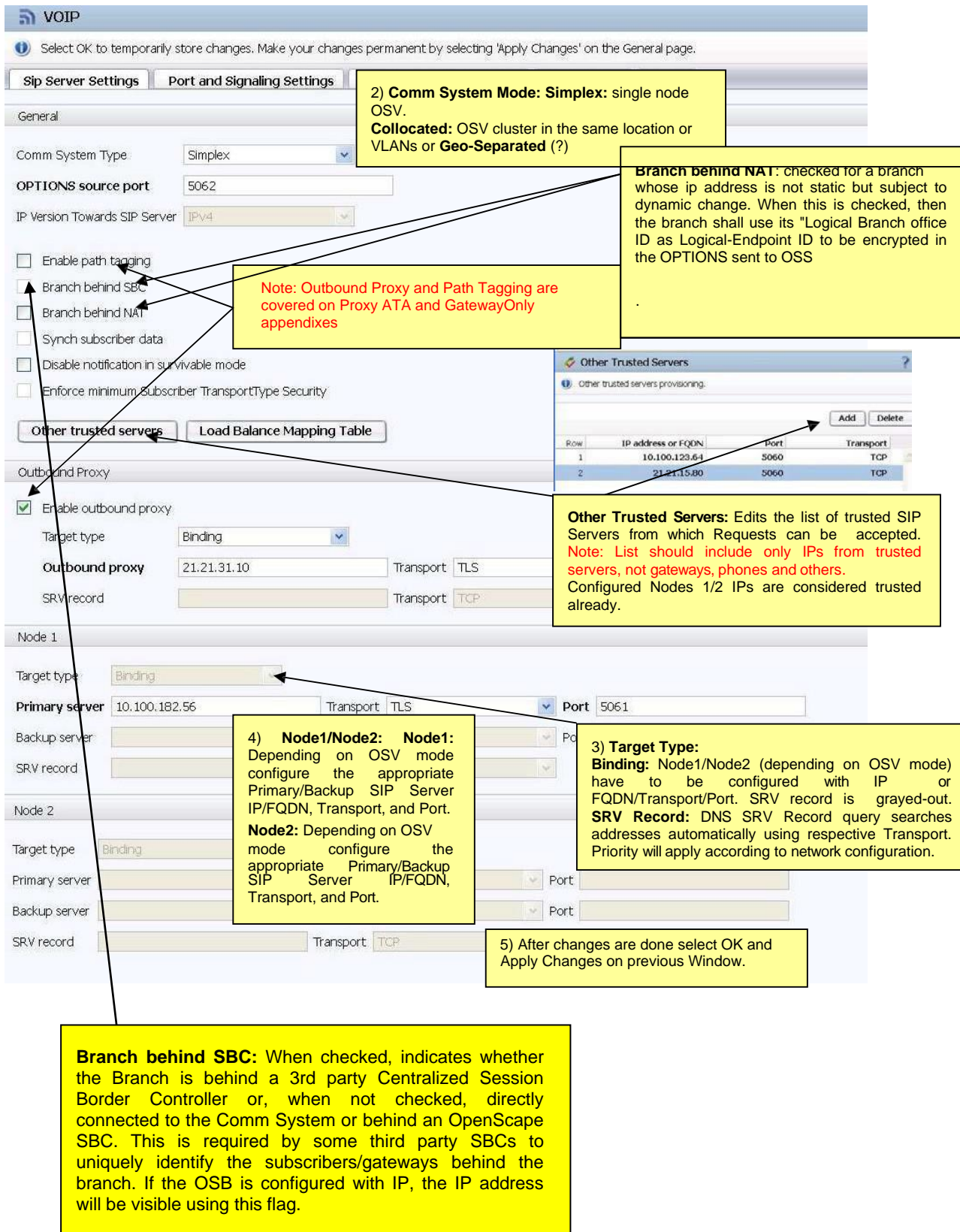
☒ Watchdog expiry timer Watchdog information

Watchdog expiry timer 1 min

OK Cancel

And OSV nodes will be configured under VOIP/general.

Configuration  OpenScope Branch  Branch Office  Configuration  VoIP  Sip Server Settings



VOIP

Select OK to temporarily store changes. Make your changes permanent by selecting 'Apply Changes' on the General page.

Sip Server Settings | Port and Signaling Settings

General

Comm System Type: Simplex

OPTIONS source port: 5062

IP Version Towards SIP Server: IPv4

☐ Enable path tagging

☐ Branch behind SBC

☐ Branch behind NAT

☐ Synch subscriber data

☐ Disable notification in survivable mode

☐ Enforce minimum Subscriber TransportType Security

Other trusted servers | Load Balance Mapping Table

Outbound Proxy

☒ Enable outbound proxy

Target type: Binding

Outbound proxy: 21.21.31.10 | Transport: TLS

SRV record: | Transport: TCP

Node 1

Target type: Binding

Primary server: 10.100.182.56 | Transport: TLS | Port: 5061

Backup server: | Transport: | Port: |

SRV record: | Transport: | Port: |

Node 2

Target type: Binding

Primary server: | Transport: | Port: |

Backup server: | Transport: | Port: |

SRV record: | Transport: TCP | Port: |

Other Trusted Servers

Other trusted servers provisioning.

Row	IP address or FQDN	Port	Transport
1	10.100.123.64	5060	TCP
2	21.21.15.80	5060	TCP

2) Comm System Mode: Simplex: single node OSV.
Collocated: OSV cluster in the same location or VLANs or Geo-Separated (?)

Branch behind NAT: checked for a branch whose ip address is not static but subject to dynamic change. When this is checked, then the branch shall use its "Logical Branch office ID as Logical-Endpoint ID to be encrypted in the OPTIONS sent to OSS

Note: Outbound Proxy and Path Tagging are covered on Proxy ATA and GatewayOnly appendices

Other Trusted Servers: Edits the list of trusted SIP Servers from which Requests can be accepted. **Note:** List should include only IPs from trusted servers, not gateways, phones and others. Configured Nodes 1/2 IPs are considered trusted already.

3) Target Type:
Binding: Node1/Node2 (depending on OSV mode) have to be configured with IP or FQDN/Transport/Port. SRV record is grayed-out.
SRV Record: DNS SRV Record query searches addresses automatically using respective Transport. Priority will apply according to network configuration.

4) Node1/Node2: Node1: Depending on OSV mode configure the appropriate Primary/Backup SIP Server IP/FQDN, Transport, and Port.
Node2: Depending on OSV mode configure the appropriate Primary/Backup SIP Server IP/FQDN, Transport, and Port.

5) After changes are done select OK and Apply Changes on previous Window.

Branch behind SBC: When checked, 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 OpenScope 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.

TCP/UDP/TLS	OSV Mode	MTLS
	Simplex	
sipsm1_vip	Node 1	sipsm3_vip
	Collocated	
sipsm1_vip	Node 1	sipsm3_vip
sipsm2_vip	Node 2	sipsm4_vip
	Geo-Separated	
sipsm1_vip	Node 1 Primary Server	sipsm3_vip
sipsm2_vip	Node 1 Secondary Server	sipsm4_vip
sipsm2_vip	Node 2 Primary Server	sipsm4_vip
sipsm1_vip	Node 2 Secondary Server	sipsm3_vip

Note: In case the OSV is configured with the same IP address for TLS and MTLS (sipsm1_vip = sipsm3_vip, sipsm2_vip = sipsm4_vip) then use the MTLS port 5161 instead of 5061

18.3. Codecs Configuration

Configuration > OpenScape Branch > Branch Office > Configuration > Features > Codecs

The support of different codecs for Integrated gateway and Media server calls require the following configurations:

In this first section user has to select which codecs will be available under “Enable Codec Support for Transcoding”

Features

Enable/Disable desired Feature:

Features Available in Normal Mode and Survivability Mode

- ☐ Enable gateways/trunks Configure
- ☐ Enable auto attendant Configure
- ☒ Enable phone software management Configure
- ☒ Enable Media Server Configure
- ☒ Enable Codec Support for transcoding Configure
- ☐ Enable Backup Link Client Configure
- Emergency Calling Configure

Features Available in Survivability Mode Only

- Multi-line Hunt Groups Configure
- Call Forwarding Configure
- ☐ Enable Call Detail Records Configure
- ☐ Enable Music On Hold for Gateways
- ☐ System calling number suppression access code

Available Codecs

Select codecs.

Enable	Codecs
<input checked="" type="checkbox"/>	G711A 8 kHz - 64 kbps
<input checked="" type="checkbox"/>	G711U 8 kHz - 64 kbps
<input type="checkbox"/>	G722 8 kHz - 64 kbps
<input type="checkbox"/>	G7221 16 kHz - 24Kbps
<input type="checkbox"/>	G7221 16 kHz - 32Kbps
<input type="checkbox"/>	G7221C 32 kHz - 24Kbps
<input type="checkbox"/>	G7221C 32 kHz - 32Kbps
<input checked="" type="checkbox"/>	G729 8 kHz - 8 kbps
<input type="checkbox"/>	OPUS 48 kHz - Variable
<input type="checkbox"/>	ILBC 8 kHz - Variable
<input type="checkbox"/>	ISAC 16 kHz - Variable

By default the Codecs G711A, G711U and G729 are enabled

The codecs G711A, G711U cannot be disabled

Codecs: List applies when OSB is acting as B2BUA (Ex. AA, ACD, MLHG,) During normal operation, the SDP is negotiated between endpoints so other codecs (ex. 729) are supported. Also valid for SBC modes and LAN-WAN transcoding.

Second step is to add these codecs on Media profiles. Please note that only codecs that are enabled appear as an option on Media Profile configuration.

In this section user will enable the profiles and select the codecs and order of codecs that will be used.

Media Profile in use and media profiles available.

User has to Edit the profiles and select the codecs priorities

Profile name	Codecs	Media protocol	Key exchange method	Mark sRTP Call-leg as Secure	Single m-line SRTP
default		Strict Pass-Thru	none		
lgw_jan	G711U,G711A,G729	Strict Pass-Thru	none		
b2bua_profile	G711U,G711A	RTP only	none		

Media Profile

Select OK to temporarily store changes. Make your changes permanent by selecting 'Apply Changes' on the General page.

General

Name

Media protocol Strict Pass-Thru

SRTP configuration

SRTP crypto context negotiation none

☐ Mark SRTP Call-leg as Secure

☐ Single m-line SRTP

☐ Enable DTLS

Codec configuration

☐ Allow unconfigured codecs

☐ Enforce codec priority in profile

☐ Send Telephony Event in Invite without SDP

Packetization interval auto

Codec G722 8 kHz - 64 kbps Add

G722 8 kHz - 64 kbps
 G7221 16 kHz - 24Kbps
 G7221 16 kHz - 32Kbps
 G7221C 32 kHz - 24Kbps
 G7221C 32 kHz - 32Kbps

Priority	Codec Name
1	G711U 8 kHz - 64 kbps
2	G711A 8 kHz - 64 kbps

Flags:

Allow Unconfigured Codecs: If enabled, even when a codec is not in the list of supported codecs on the igw_profile, the OSB will accept it and use it for transcoding.

Note: The "Enable Codec Support for Transcoding" flag was originally used for codec transcoding between the LAN/WAN from a Branch-SBC or SBC Proxy, but it is also needed to support the transcoding for Integrated Gateway and Media Server.

18.4. RTP Configuration

Administration -> VoIP -> Media -> RTP

RTP configuration is enabled if Integrated Gateway is enabled.

RTP	
RTCP interval (ms)	5000
<input type="checkbox"/> RTP protection	
<input type="checkbox"/> Jitter buffer	
JB minimum delay (ms)	20
JB maximum delay (ms)	150
Implementation	Fixed
Packetization time (ms)	20
Dtmf Forward Twist (dB)	8
Dtmf Reverse Twist (dB)	4
<input checked="" type="checkbox"/> Enable RFC 2833 support	
<input type="checkbox"/> Cancel DTMF transmission on reinvite	
<input type="checkbox"/> Use Restrict V29 FAX Frequency	

RTCP interval(ms): Represents the period of time in milliseconds between RTCP reports.

RTP protection: enable/disable strict RTP protection.

Jitter buffer: 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 or Adaptive. It is enabled if Jitter buffer is enabled.

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 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 are not being correctly detected or voice is being wrongly detected as DTMF.

Available options:4,5,6,7,8,9,10
Default value:8 dB

Dtmf reverse Twist (dB): Sets the maximum threshold in reverse twist for the DTMF to be detected by OSB. Dtmf Reverse Twist is the difference in dB between row (lower frequency) and column (higher frequency) energies for dtmf frequencies, when row energy is greater than the column energy. This value should be adjusted only if DTMF are not being correctly detected or voice is being wrongly detected as DTMF.

Available options:4,5,6,7,8,9,10
Default value:4 dB

NOTE: If country is United States/North America or United States Circa 1950/North America the default value of DTMF Reverse Twist is 9dB

Enable RFC 2833 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. This flag can only be set if "Enable RFC2833 Support" is set. Default is disabled.

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. Set 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

18.5. Timers and Thresholds

User can configure Timers & Thresholds to detect OSV node failures.

Timers & Thresholds: Survivability Provider settings to determine how fast the OSB detects and reacts to a node failure, and how often it checks the connection.

Configuration > OpenScope Branch > Branch Office > Configuration > VoIP > Sip Server Settings

Failure Threshold (pings): number of failure attempts counted before considering a node failure (Range 1-10)

Success Threshold (pings): number of positive responses before considering node is active (Range 1-10).

Transition Mode Threshold: number of failure attempts counted before switching to Survivability Mode (Set transition mode threshold to 0 if this mode is not required).

Options Interval (sec): keep alive interval to send options to SIP Server. (Range 10 - 300).

Options Timeout (sec): timeout when waiting for 200OK from SIP Server (Range 1 - 32).

Notification Rate: Number of notifications per sec after state transition. Disabled in Proxy ACD Mode.

Timers and Thresholds			
Failure threshold (pings)	<input type="text" value="2"/>	OPTIONS interval (sec)	<input type="text" value="20"/>
Success threshold (pings)	<input type="text" value="1"/>	OPTIONS timeout (sec)	<input type="text" value="4"/>
Transition mode threshold (pings)	<input type="text" value="1"/>	Notification rate (per sec)	<input type="text" value="10"/>

Clustered Nodes settings	
Ping Method	<input type="text" value="OPTIONS"/>
Failure threshold (pings)	<input type="text" value="2"/>

OSV Timer/Threshold Examples

Settings:

Failure Threshold = 2 (pings)

OPTIONS interval = 60 (sec)

OPTIONS request Timeout = 4 (sec) Transition Mode Threshold = 1 (pings)

Scenario1 (Going to Survivability Mode): normal OPTIONS 4s (first timeout/fail) OPTIONS fast ping 4s OPTIONS fast ping 4s (failure threshold - 2 fast pings) TRANSITION 60s (ping interval) OPTIONS transition 4s (transition threshold)

Total: 76seconds

Going to Normal Mode: Any time between 0 to 64 (Options + timeout) seconds OSB will go back to NM

Settings:

Failure Threshold = 2 (pings)

OPTIONS interval = 60 (sec)

OPTIONS request Timeout = 4 (sec) Transition Mode Threshold = 2 (pings)

Scenario2 (Going to Survivability Mode): normal OPTIONS 4s (first timeout/fail) OPTIONS fast ping 4s OPTIONS fast ping 4s (failure threshold - 2 fastpings) TRANSITION 60s (ping interval) OPTIONS transition 4s (transition threshold) TRANSITION 60s (ping interval) OPTIONS transition 4s (transition threshold)

Total: 140seconds

Going to Normal Mode: Any time between 0 to 64 (Options + timeout) seconds OSB will go back to NM

Note for going to Survivability Mode scenarios: Timer Total example shows from the time Option is sent and not responded. Transition time could be longer depending when last Option was responded by OSV.

18.6. SIP Manipulation, Office Code Mapping and Gateways

Configuration for SIP Manipulation (Survivability Mode), Office Code Mapping (Survivability Mode and Normal Mode) and Routing (Survivability Mode) are located under VOIP Menu and Manipulation and Routing Tab.

Configuration > OpenScape Branch > Branch Office > Configuration > VoIP > Manipulation and Routing

18.7. SIP Manipulation Provisioning

Allows user to change SIP headers during Survivability Mode (except from an Emergency Number). Rules priority applies for best match from left to right.

Note: after save in Sip Manipulation Window user has to Apply Changes for them to commit. Apply Changes for Sip Manipulation requires SipServer to be restarted. Call processing will be affected temporarily.

Match Digits: digits dialed (called number) will be compared against.
Match Position: start compare of Match Digits at this position.

Header: SIP Header used for digit manipulation (R-URI /From/PAI/PPI/Diversion).
Delete/Insert Position: position where to make change

Add Prefix: place digits in front on Header.
Replace All With: All digits will be replaced on Header.

Row	Match digits	Match position	Match length	Header	Delete/insert position	Number of digits to delete	Insert digits	Add prefix	Replace all with	Call type
1	53	4		R-URI					5558880000	All
2	561719	0		R-URI		6				All
3	305	0		R-URI	1	2	44			All
4	555888	0		R-URI		6				SIP-SIP

Delete Digits: Number of digits to be removed.
Insert Digits: place digits at position.

Note: Call type different than "All" can only be configured for FROM Header.

- a) **Row1:** match 53 to the called number starting on digits position 4 (Count 0 through 4 from the left of the called number). If match replace all digits with 5558880000
Dial 7777535000 → match (Position 4), after Translation 5558880000.
- b) **Row2:** match 561719 to the called number starting on digit position 0. If match delete 6 digits and prefix 555888.
Dial 5617195200 → match (Position 0), after Translation 5558885200
- c) **Row3:** match 305 to the called number starting on digit position 0. If match delete 2 digits from position 1 and then append 44. User Dials 3053333240 → match (Position 0), after Translation 3443333240.
- d) **Row4:** match 555888 to the calling number starting on digit position 0. If match, delete 555888 for SIP to SIP only. User Calling Number 5558885246 → match (Position 0), after Translation 5246 if a SIP-SIP call was made.

Note: is possible to add a + in the From Header (if needed for certain GWs, ex. HiPath 3000). Example: Match digits: 4, Match position: 0, Header: From, Add prefix: +. This configuration is needed for HiPath 3000/4000 so that the Gateway is able to interpret the called party number as international number. + on R-URI should be removed as well.

A new field called “Match length” is added.

SIP Manipulation

Row	Match digits	Match position	Match length	Header	Delete/insert position	N
1	2	0	1/	R-URI From P-PI P-AI Diversion P-AI (or FROM if no P-AI exists)		

New field "Match length" was added.
Possible configured values are:
• x: number from 1 to 23.
The number of digits being matched is equal to x.
If a user dials fewer or more digits than x, then the rule is ignored. If a user dials exactly x digits, then the rule is checked.
• x/: number from 1 to 23.
The number of digits being matched is at least x.
If a user dials x or more digits, then the rule is checked.
• x/y: where x and y can be a number from 1 to 23.
y is greater than or equal to x.
The number of digits being matched is not less than x and not more than y.
If a user dials fewer digits than x or more digits than y, then the rule is ignored.
If a user dials between x and y digits, then the rule is checked.
NOTE: This field will also apply to SSP SIP Manipulation.

New Header entries were added:
• P-PI: P-Preferred Identity
• P-AI: P-Asserted Identity
• Diversion
• P-AI (or FROM if no P-AI exists)
When both headers exist in the message then the P-AI header will be modified, otherwise the FROM header will be modified.

18.8. Office Code Mapping

Configuration allows a customer to set up extension dialing across office codes defined on the same branch (Survivability Mode), and to establish source-based routing whereby a calling party number is used as the key for determining which outgoing gateway is used (Survivability Mode or Survivability/Normal Modes).

Configuration > OpenScope Branch > Branch Office > Configuration > VoIP > Manipulation and Routing

VOIP

Select OK to temporarily store changes. Make your changes permanent by selecting 'Apply Changes' on the General page.

Sip Server Settings Port and Signaling Settings Manipulation and Routing Error Codes Media

Office Codes:

☒ Enable source-based routing in Normal Mode

Enable Source Based Routing in Normal Mode: flag enables source based routing for Normal Mode (Survivability is enabled by default if match is found on Office Code Mapping table).

Add Edit Delete

Row	SN range	Office code	Destination prefix	Insert office code
1	6800 - 7000	55113817	*89	On

SN Range: subscriber numbers can be added as a range using a dash (ex. 3100 – 3350) or as a single number (ex. 3388).
Note1: duplicate subscriber numbers within the same or different ranges are not allowed.
Office Code: maximum of 14 digits [0-9] can be entered (Country Code, Area Code, and Exchange Code grouped together). **This field is only used in Survivability Mode.**
Destination Prefix: stores a single destination prefix that identifies which outgoing GW/TKG/SSP should be used to route external calls from an extension (Routing Prefix on GW Provisioning Table).
Insert Office Code: when set, will cause the new "Office Code" function to insert the office code of the called party into the R-URI. This field gives the user the ability to choose between using the Office Code function or SIP Manipulation to adjust the R-URI. **This field is only used in Survivability mode.**
Note: Office Code and/or Destination Prefix are required.

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.

18.9. Extension Dialing Across Office Codes

Feature support of multiple office codes on a single OSB while allowing the subscribers in the different office codes to dial each other by using an extension number. This is useful in cases where a customer has multiple physical branches that only have a few subscribers using different office codes.

Normal Mode

In Normal mode, extension dialing across office codes is accomplished by configuring Prefix Access Codes in the OSV for each extension number. The rules for each PAC entry will result in the applicable Office Code being inserted into the called party number (R-URI). This is necessary to ensure that the full called party number is available for destination handling.

Survivable Mode

In Survivable Mode, the Office Code table is used to look up the Office Code associated with a called party number, when that called party number is dialed as an extension. OSB performs a lookup of the called party number to determine if the number can be found in the Office Code table. If the number is found, then the office code that applies to it is copied from the Office Code table and inserted into the R-URI. If the table lookup yields no matching entry then processing will continue without any modification to the R-URI (this corresponds with current behavior).

18.10. Source-Based Routing

Feature supports routing of outgoing calls to the PSTN over facilities that are associated with the calling party, rather than the called party (Regular OSB mechanism). This is useful in cases where a customer has multiple physical branches that only have a few subscribers. The physical branches may be in geographically dispersed locations, hence requiring different trunk facilities to carry the PSTN traffic.

Normal Mode

While the OSV has its own concept of source-based routing based on Rate Areas (the description of this capability is outside the scope of this document), the OSB version of this capability is also supported on the OSB in Normal mode, in case the customer prefers to configure it in one place only. Setting the checkbox labeled "Enable source-based routing in Normal Mode" will result in the Office Code table contents (SN Range and Destination Prefix fields) being used to determine which outgoing gateway to use for calls to external destinations. Note that the calling party number is used for the lookup in the SN Range field.

Survivable Mode

OSB performs a lookup in the SN Range field using the calling party number to get the Destination Prefix. The prefix is then used by the function that looks at the Gateway table to determine which outgoing facility to utilize for the call. source-based routing.

If no match is found the traditional OSB outgoing call routing, which is based on the called party number, is used.

18.11. SIP Routing Provisioning

Allows rerouting of messages during SM.

Configuration > OpenScope Branch > Branch Office > Configuration > VoIP > Manipulation and Routing

The screenshot shows the 'SIP Routing' configuration page within the 'VOIP' section. At the top, there's a message: 'Select OK to temporarily store changes. Make your changes permanent by selecting 'Apply Changes' on the General page.' Below this are tabs for 'Sip Server Settings', 'Port and Signaling Settings', 'Manipulation and Routing' (which is active), 'Error Codes', and 'Media'. The 'SIP Routing' section has an 'Add' button and a 'Delete' button. A table lists the routing rules:

Row	Source IP	Condition (error codes)	Destination IP or FQDN	Destination port	Transport	Destination tag	Destination type
1	10.234.1.170	408;690;486	bgloadnational227.rg8700.si	5060	TCP	9305333240	Voice Mail

Source IP: source IP of the message to be routed (Subnet address in CIDR notation is also supported)

Error codes: reply code list used to reroute the messages. 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. (ex. timeout of 6s can be set by adding the code 640 (640 - 634 = 6) to the list. Note that it is required to set at least an error code at 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 180s.

Destination IP/FQDN: This is the configuration of the destination of the message to be routed.

Destination tag: defines a tag to be added to re-routed SIP headers. SIP manipulation rules do not apply to destination tag.

Destination type: determines the type of route used for the rule

18.12. Gateway Provisioning

Configuration > OpenScope Branch > Branch Office > Configuration > Features > Enable gateways/trunks Feature allows user to configure Gateways for Normal Mode and Survivability Mode.

Note: user has to Apply Changes after saving GW provisioning changes. Apply Changes requires SipServer and SSM processes to be restarted. Call processing will be affected temporarily.

Note: Mapped Port parameter 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 (Only Applies to Branch SBC/SBC- Proxy or IPV6-Proxy Modes).

Gateways/Trunks provisioning

DNS dynamic refresh interval (min): 60

☐ Route to R-URI domain

Row	Signaling address type	Remote URL	Port	Interface	Transport	Mapped port	Routing prefix	Gateway/Trunk type	Functional type	Trunk profile	Output digit strip	Output digit add	Priority
1	IP address or FQDN	25.25.0.40	5060	LAN	TCP	9000	5511381728%	Peer OSB	Survivability Mode Egress/Ingress	Gateway	0		1
2	IP address or FQDN	25.25.0.40	5060	LAN	TCP	9000	28%	Peer OSB	Survivability Mode Egress/Ingress	Gateway	0	55113817	1
3	IP address or FQDN	pr15062.unow.k	5096	LAN	UDP	9001	8%	Integrated Gateway	All Modes Egress/Ingress	Gateway	0		1
4	IP address or FQDN	pr15062.unow.k	5096	LAN	UDP	9001	320%	Integrated Gateway	All Modes Egress/Ingress	Gateway	1		1
5	IP address or FQDN	rg08d.unow.k	5060	LAN	TCP	9002	209%	RG	All Modes Egress/Ingress	Gateway	0		2
6	IP address or FQDN	21.21.4.21	5060	LAN	TCP	9003	4%	RG	All Modes Egress/Ingress	Gateway	0	55113817	1
7	IP address or FQDN	25.25.0.40	5060	LAN	TCP	9000	120%	Peer OSB	Survivability Mode Egress/Ingress	Gateway	1		1
8	IP address or FQDN	pr15062.unow.k	5096	LAN	UDP	9001	[*]44	Integrated gateway	All Modes Egress/Ingress	Gateway	3	20902	1

Note: When using OSB with Mediatrix, the "Gateway/Trunk Type" must be set to "Others" for GW Provisioning if the Mediatrix gateway is running version DGW 2.X or higher. For earlier Mediatrix versions the "Gateway/Trunk Type" must be set to "Mediatrix".

Priority 0 GW (OPTIONAL): should be used only on specific cases. OSB will attempt to route calls using Default GW only when it can not route to other GWs or SIP End Points. (Ex. Invalid number dialed). Only 1 GW can be configured as default and no prefix can be configured. For fail over route priority 0 is not taken into consideration.

Gateway Configuration

Gateway configuration provisioning.

General

Signaling address type: IP address or FQDN

Remote URL: pri50is2.unow.net5.cwb

Port: 5096

Interface: LAN

Transport: UDP

Mapped port: 9001

Routing prefix: 8%

Gateway/Trunk type: Integrated Gateway

Functional type: All Modes Egress/Ingress

Trunk profile: Gateway

Output digit strip: 0

Output digit add:

Priority: 1

☐ Operational Mode in OPTIONS Response

Signaling

INVITE no answer timeout - Normal Mode (sec): 360

INVITE no answer timeout - Survivable Mode (sec): 180

INVITE no reply timeout - Normal Mode (sec): 3

INVITE no reply timeout - Survivable Mode (sec): 3

TLS

TLS mode: Server authentication

Certificate profile: OSV Solution

☐ TLS keep-alive

Keep-alive interval (seconds): 120

Keep-alive timeout (seconds): 10

Media Configuration

Media profile: default

Media realm subnet IP address:

Media realm subnet mask:

Anchoring media: Forced

☐ Force media anchoring on transcoding

OK Cancel

IP Address/FQDN/DNS Srv: configuration for GW IP, FQDN, or DNS Srv. Only one can be configured. FQDN is resolved via DNS or /etc/host.

Port/Transport: SIP Port and Transport Protocol for communication with GW. **Interface:** SBC and **SBC-Proxy only.**

Type: 3K/4K/Backup Link Server/ Mediatix/ Others/Peer OSB, RG/SIP Trunk/ VoiceMail. (In ProxyACD mode only "Others", "Peer OSB", or "Integrated Gateway" can be used).
Output digit strip: delete digits (from Beginning)
Output digit add: add digits (from Beginning).
Priority: lowest has highest priority.

-All Modes: Normal Mode and SurvivabilityMode.
-Egress: Outgoing Calls **-Ingress:** Incoming Calls
-Emergency: Emergency GW for SM (It must be configured only if supported. When Emergency call fails to reach the PSAP, call is re routed to configured local Destination (ex. Local Attendant) which has land line to call PSAPdirectly.

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 modeWANS.

The items in that section are only configurable when the **Enable LAN-SSP media interwork** flag is set and the gateway is in the WAN.

Once the **Enable LAN-SSP media interwork** flag is set, the **Media Configuration** will be allowed when a SIP Trunk is added to the gateway table

Note: Routing Prefix expressions may be used for matching. Expressions available do not necessarily comply with POSIX Regular Expression rules. Nevertheless, POSIX Regular Expressions are a good reference to build matching rules. Expressions:

Expression	Description	Example
%	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	99% --> Match on 99 followed by any digits
-	Matches any single character	[9][3-6]% --> Match on 9, followed by a digit between 3-6, followed by any digits.
+	Denotes repetition of the previous item one or more times	93+1% --> Match on 931, 9331, 93331, etc followed by anydigits
*	Denotes repetition of the previous item zero or more times	93*1% --> Match on 91, 931, 9331, 93331, etc. followed by any digits.
	Denotes alternation (either of two alternatives).	9% 8% --> Match on 9 or 8 followed by any digits.
[^<list-of-characters>]	Matches a character that is not contained within the brackets	Match on 3 followed by any digits except digit 8 (match on 30,31,32,33,34,35,36,37,39)

Note: GW provisioning routing prefix matches on "[" first instead of Digits for best match. Ex. Rules "9011%" and "[2-9]%" are created. If user dials 9011XXXX 📞 Best match is "[2-9]%".

18.12.1 Gateway Configuration as a SIP trunk in LAN side

OpenScape Branch provides the option of having a SIP trunk in LAN.

- Create an SSP profile. Do not configure anything in the profile, just give a name to it. **Save & apply.**
- Change the gateway type to **SIP Trunk** & associate the profile created to it. **Save & apply.**

Note: The B2BUA is used by default in SM in SSP calls. The REFER will be handled locally by the B2BUA.

- If step b does not work, configure the gateway type as **3k/4k**.

It will make the calls in SM be routed through B2BUA then the REFER will be handled locally.

OSB: Allow SIP trunks from LAN side activation Instructions

Proxy and Proxy-ACD Modes

- Features: click on Sip Service Provider profiles and create an SSP profile (default settings)

Features

Select OK to temporarily store changes. Make your changes permanent by selecting 'Apply Changes' on the General page.

Features Available in Normal Mode and Survivability Mode

<input checked="" type="checkbox"/> Enable gateways/trunks	Configure	
<input checked="" type="checkbox"/> Enable integrated gateway	Configure	Ring down channels
Sip Service Provider profiles	Configure	SIP Service Provider profiles can be created
<input checked="" type="checkbox"/> Enable auto attendant	Configure	
<input checked="" type="checkbox"/> Enable Voice Mail Service	Configure	
<input type="checkbox"/> Enable phone software management	Configure	
<input checked="" type="checkbox"/> Enable Media Server / Streaming	Configure	
<input type="checkbox"/> Enable LAN-SSP media interwork	Configure	Media Profiles can be created and associated to the SSPs in the gateway table
<input checked="" type="checkbox"/> Enable Codec Support for transcoding	Configure	
<input type="checkbox"/> Enable Backup Link Client	Configure	
Emergency calling	Configure	

- Features --> Gateway/Trunks --> Gateway Configuration

Gateway Configuration

Select OK to temporarily store changes. Make your changes permanent by selecting 'Apply Changes' on the General page.

General

Signaling address type	IP address or FQDN	
Remote URL	provider.com	
Port	5060	
Interface	LAN	Only LAN interface is allowed
Transport	TCP	
Routing prefix	01%	
Gateway / Trunk type	SIP Trunk	SIP Trunk can be selected
Functional type	All Modes Egress/Ingress	
Trunk profile	SP	SSP Profile can be assigned to the SIP Trunk
Output digit strip	0	
Output digit add		
Priority	1	
<input type="checkbox"/> Operational Mode in OPTIONS Response		

18.13 SIP Manipulation Provisioning

1) DNS Server List: DNS server can be configured in the OSB in order to resolve FQDNs configured. OSB will act as DNS client. Up to three DNS Servers can be configured. IF IPV6 is enabled, the NTP address can be an IPV6 address.

Configuration > OpenScape Branch > Branch Office > Configuration > Network/Net Services > DNS

The screenshot shows the 'Network/Net Services' configuration window with the 'DNS' tab selected. The window has a title bar and a help icon. Below the title bar is a message: 'Select OK to temporarily store changes. Make your changes permanent by selecting 'Apply Changes' on the General page.' The 'DNS' tab is active, and other tabs like 'Settings', 'NTP', 'DHCP', 'Traffic Shaping', and 'QoS' are visible. The 'Client' section contains a 'Refresh DNS' button and a list of DNS server IP addresses. One IP address, '192.168.100.4', is already entered. There are 'Add' and 'Delete' buttons for the IP address list. An 'Alias' field with an 'Add' and 'Delete' button is also present. The 'Server' section has two checkboxes: 'Enable DNS server' and 'Enable customization', each with a corresponding button ('DNS configuration' and 'Administer custom files' respectively). At the bottom right are 'OK' and 'Cancel' buttons. A yellow callout box points to the 'Add' button for the IP address list, containing the text: 'DNS Server List (configure): Enter IP address of DNS servers (If OSB is acting as DNS Client) Note: other DNS functionality is covered on DNS section'.

Network/Net Services

Select OK to temporarily store changes. Make your changes permanent by selecting 'Apply Changes' on the General page.

Settings DNS NTP DHCP Traffic Shaping QoS

Client

Refresh DNS

DNS server IP address

192.168.100.4

Add Delete

Alias

Add Delete

Server

☐ Enable DNS server DNS configuration

☐ Enable customization Administer custom files

OK Cancel

DNS Server List (configure): Enter IP address of DNS servers (If OSB is acting as DNS Client)
Note: other DNS functionality is covered on DNS section

```
# Syntax:
#
# IP-Address  Full-Qualified-Hostname  Short-Hostname
#
127.0.0.1      localhost

# special IPv6 addresses
::1           localhost ipv6-localhost ipv6-loopback

fe00::0       ipv6-localnet

ff00::0       ipv6-mcastprefix
ff02::1       ipv6-allnodes
ff02::2       ipv6-allrouters
ff02::3       ipv6-allhosts

127.0.0.1      OB-IBM3250-IP70

#OB#
10.234.1.70    OB-IBM3250-IP70.siemens.com  OB-IBM3250-IP70
#OB#

10.234.3.87    RG1Nat.rg8700.com
10.234.3.87    RG1Loc.rg8700.com
10.234.3.87    RG1Int.rg8700.com
10.234.3.87    RG1Unk.rg8700.com
10.234.3.227   RG2Nat.rg8700.com
10.234.3.227   RG8700Incoming.rg8700.com
```

Host file: if no DNS server is available, FQDNs can be resolved using OSB host file /etc/hosts **Note: Limit of 5 SSH sessions (Idle expiration timer is 60 minutes)**

19 Call Forward (Voice Mail)

Allows rerouting of messages to Voice Mail during SM. Feature was introduced in V1R4 and can be used instead of SIP Routing to route calls to Voice Mail in SM. Configuration

 OpenScape Branch  Branch Office  Configuration  Features  Call Forwarding

Call Forward

Call Forward provisioning.

Call Forward No Reply

Activate: ☒

Redirect Number:

Ring Duration:

Source IP address:

Call Forward on Busy

Activate: ☒

Redirect Number:

Source IP address:

Call Forward On Do not Disturb

Activate: ☒

Redirect Number :

Source IP address:

Error Codes

Redirect number: digit string with up to 24 digits to be used as DN. (ex. Xpression number if connected on SIP side or PSTN number to be routed to Xpressions on Data Center).

Ring duration (only in No Reply Forward): range from 1 to 60 seconds (Default: 24 sec). Timer while the subscriber will receive ring before the call is forwarded. It should be configured higher value that phone call forward in order to avoid conflicts.

Source IP address: host IP address or Subnet, IP address and mask in CIDR format. If source IP is exactly OSB IP then CFcan apply to all callers.

Note: if a call is routed to Voice Mail server via PSTN (public network) please verify that CO/GWs support diversion header information.

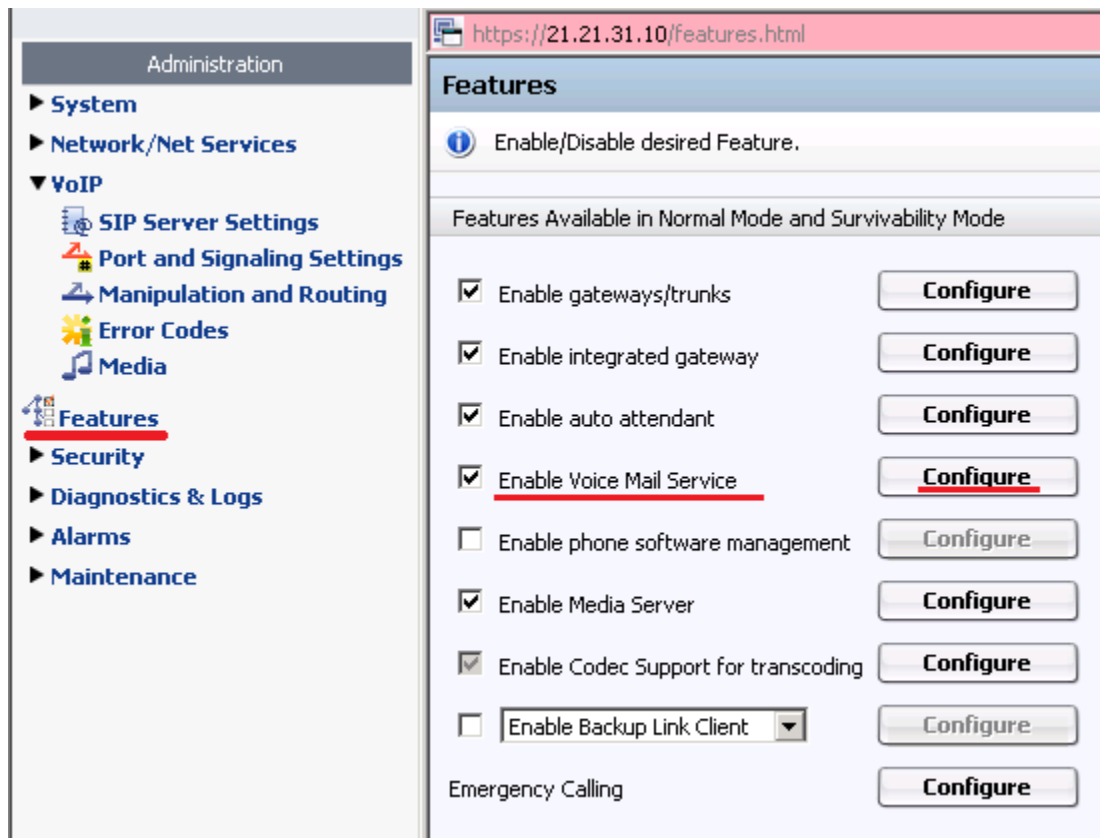
Error Codes: Error Codes (only in On Error Forward) that will trigger forwarding to voice mail.

Error Codes	
Error Codes	
Error codes : <input type="text" value="300"/>	<input type="button" value="Add"/> <input type="button" value="Delete"/>
Sel:0 Items/Page: <input type="text" value="10"/> All:3	
<input type="checkbox"/>	Error codes
<input type="checkbox"/>	606
<input checked="" type="checkbox"/>	403
<input type="checkbox"/>	302

20 Local Voice Mail Service

Provides for OSB's a simple Voice Mail capability in normal and survivable mode.

Administration -> Features -> Enable Voice Mail Service



For MWI functionality during normal mode operation:

- Subscriber: needs to be enabled the Feature "Call Forwarding to Voice Mail" in the OSV
- OSV: the parameter "Srx/Main/MwiNatureOfAddress" should be set to "2".

Note: MWI notification capability is NOT supported for analog subscribers (FXS ports).

80-BG01-50iA - Features - Windows Internet Explorer
https://21.21.31.10/features.html

Features

Enable/Disable desired Feature.

Features Available in Normal Mode and Survivability Mode

<input checked="" type="checkbox"/> Enable gateways/trunks	<input type="button" value="Configure"/>
<input checked="" type="checkbox"/> Enable integrated gateway	<input type="button" value="Configure"/>
<input checked="" type="checkbox"/> Enable auto attendant	<input type="button" value="Configure"/>
<input checked="" type="checkbox"/> Enable Voice Mail Service	<input type="button" value="Configure"/>
<input type="checkbox"/> Enable phone software management	<input type="button" value="Configure"/>

VoiceMail Service

VoiceMail Service provisioning.

General

VoiceMail Destination	<input type="text" value="043111"/>	VoiceMail Retrieve Destination (From Own Ext.)	<input type="text" value="043111"/>
VoiceMail Greeting	<input type="text" value="vm-welcome.wav"/>	VoiceMail Retrieve Prompt (From Own Ext.)	<input type="text" value="vm-welcome.wav"/>
Maximum Number Of Messages	<input type="text" value="30"/>	VoiceMail Retrieve Destination (From Other Ext.)	<input type="text" value="043113"/>
Maximum Message Length (sec)	<input type="text" value="60"/>	VoiceMail Retrieve Prompt (From Other Ext.)	<input type="text" value="vm-welcome.wav"/>
Silence Time Before Ending Recording (sec)	<input type="text" value="10"/>	Maximum Login Attempts Allowed	<input type="text" value="3"/>

General

VoiceMail Destination: voicemail dial number destination (up to 24 characters). This is the number used to call forward the calls to Voicemail.

VoiceMail Greeting: Select the greeting message that is played when a forwarded call is answered by voicemail.

VoiceMail Retrieve Destination (From Own Ext.): number that user dials to access his own mailbox (up to 24 characters).

VoiceMail Retrieve Prompt (From Own Ext.): Select the greeting message that is played when user access his own mailbox.

VoiceMail Retrieve Destination (From Other Ext.): number that user dials to access his mailbox from other destination (up to 24 characters). This number must be different from VoiceMail Destination and VoiceMail Retrieve Destination.

VoiceMail Retrieve Prompt (From Other Ext.): Select the greeting message that is played when user access his mailbox from other destination.

Maximum Number of Messages: configure the maximum number of messages. It depends on the OSB Server type.

Maximum Message Length (sec): configure maximum message length allowed in the system. Range: 10-90 seconds.

Silence Time Before Ending Recording (sec): Time of silence before disconnect the call from Voicemail. Range: 2-10.

Maximum Login Attempts Allowed: Maximum login attempts for message retrieval. Call is disconnected after maximum failed logins. Range: 1-5

VoiceMail Boxes ?

Search for in

	Enabled	Name	MailBox Number	PIN	Max Number of Msgs	Max Msg length (sec)	Announc CID	Send MWI	Email Address	Send Email	Attach Msg to Email	Del Msg after Snd
1	<input checked="" type="checkbox"/>	sip5007	551138175007	••••	3	30	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
2	<input checked="" type="checkbox"/>	sip5008	551138175008	••••	3	30	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
3	<input checked="" type="checkbox"/>	sip5009	551138175009	••••	3	30	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
4	<input checked="" type="checkbox"/>	sip5010	551138175010	••••	3	30	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

VoiceMail Default Box:

VoiceMail Box Match:

VoiceMail Boxes

Enabled: checkbox for enable/disable Voicemail box

Name: voicemail box name

MailBox Number: mailbox number

PIN: PIN number – 4 numeric digits

Max Number of Msgs: maximum number of messages for mailbox. Sum of all Max Number of Msgs must be lower than Maximum Number of Messages configured under General tab.

Max Msg length (sec): maximum message length for mailbox. This value must be lower than Maximum Message Length configured under General tab.

Announce CID: enable/disable the announcement of CID before play the recorded message.

Send MWI: enable/disable to send the MWI when a new message is recorded to the mailbox.

Email Address: mailbox email address

Send Email: enable/disable to send an email to configured address when a new message is recorded.

Attach Msg to Email: enable/disable if the E-Mail is sent with or without recorded message attached

Del Msg after Snd: if flag is enabled, the message is deleted from OSB after sending to email destination. If disable, message is kept.

VoiceMail Default Box: if no configured VoiceMail box for the dialed DN is found, the Message will be placed on this default mailbox.

VoiceMail Box Match: Defines when the number received to leave messages belongs to a voicemail mailbox number

Maintenance

Keep Retrieved Messages

☐

VoiceMail Storage Time (weeks)

1

E-Mail Server

Address

User

Password

Email

Clear VoiceMail Folder

Maintenance

Keep Retrieved Messages: xxx

VoiceMail Storage Time (weeks): Recorded VoiceMails will be stored for a configurable amount of time. After this time all the recorded messages will be removed, including the unread ones.

E-Mail Server Configuration

In order to be able to send email notifications, an email server account shall be configured for the voicemail.

Address: email server address (IP or FQDN)

User: user of email account that will be used to send email notifications when a new message is recorded.

Password: password of email account

Email: email account.

Clear VoiceMail Folder: Clear All VoiceMail Messages and Recorded Greetings.

Announcements

Announcement files

Browse...

Upload

Delete

vm-incorrect-mailbox.wav

vm-login.wav

vm-mismatch.wav

vm-newpassword.wav

vm-password.wav

vm-welcome.wav

VoiceMail Retrieve Prompt

vm-login.wav

VoiceMail Retrieve PIN

vm-password.wav

VoiceMail Retrieve Wrong PIN

vm-incorrect-mailbox.wav

VoiceMail Retrieve Change PIN

vm-newpassword.wav

VoiceMail Retrieve Change PIN Failed

vm-mismatch.wav

VoiceMail Retrieve Wrong Box Number

vm-incorrect-mailbox.wav

Announcements

A fresh delivered OSB will contain default prompts for the VoiceMail service.

All VoiceMail relevant prompts can be customized and uploaded/deleted by Administrator.

The VoiceMail box user will be able to record his own VoiceMail prompt.

21 MOH

OpenScape Branch supports Music On Hold while running in Survivability Mode using local Media Server.

Note: OSB Media Server must be enabled for this feature.

Configuration > OpenScape Branch > Branch Office > Configuration > Features > Enable Music On Hold

Features

Enable/Disable desired Feature.

Features Available in Survivability Mode Only:

Multi-line Hunt Groups Configure

Call Forwarding Configure

☒ Enable Call Detail Records Configure

☒ Enable Music On Hold for Gateways & Subscribers ▼

☐ Enable Music On Hold for Gateways

☐ Enable Music On Hold for Gateways & Subscribers

☐ System calling number suppression access code:

OK Cancel

Enable Music On Hold for Gateways: OSB plays MOH to non registered callers (ex. GW callers) if enabled.

Enable Music On Hold for Gateways & Subscribers: OSB will play MOH to any caller.

Note: If phone is configured with SRTP then "SDP negotiation" should be configured as "RTP- SRTP".

22 QOS

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. OSB allows QoS configuration if required by network switches and routers (this configuration is only valid for: the RTP traffic with RTP bridging/anchoring). RTP via RTPproxy.

QoS Settings

☐ Enable QoS Configuration

DSCP for SIP: 26

DSCP for non-Circuit RTP (Audio): 46

DSCP for Circuit RTP (Audio): undefined

Table:

Row	Protocol	In interface	Out interface	Port	DSCP	Mark
Add Delete						

Callouts:

- Note: if QoS is disabled (Or enabled but not configured) OSB will mark SIP packets with 12 (AF12).
- Note: after applying configuration you can collect Wireshark (All Interfaces) from OSB or external trace in order to verify packet marking.
- Configure QoS for SIP/RTP (Range 1- 63 for SIP/RTP)
- Configure Port or range of ports (ex. 0:65535)
- Note: The DSCP field is a 6-bit field which is defined in the RFC2474. Should be used values from 0 to 63
- If more specific configuration is needed then table configuration is available. Note: configured values in this table will over write values from Top (DSCP for SIP and DSCP for RTP) of the Window if conflicting rules exist

Name	Decimal
CS0	0
CS1	8
CS2	16
CS3	24
CS4	32
CS5	40
CS6	48
CS7	56
AF11	10
AF12	12
AF13	14
AF21	18
AF22	20
AF23	22
AF31	26
AF32	28
AF33	30
AF41	34
AF42	36
AF43	38
EF PHB	46

23 DHCP

OSB can be configured to act as a DHCP server for devices within the Branch.

Note: DLS and NTP (Network Services Menu, NTP Tab) information will be provided to DHCPclients.

Configuration > OpenScape Branch > Branch Office > Configuration > Network/Net Services > DHCP

The screenshot shows the 'Network/Net Services' configuration window with the 'DHCP' tab selected. The 'General' section includes checkboxes for 'Enable DHCP server' (checked) and 'Enable customization' (unchecked), with an 'Administer custom files' button. Below are fields for 'Subnet' (21.21.0.0), 'Netmask' (255.255.0.0), 'IP address from' (21.21.10.0), and 'to' (21.21.25.240). There is an 'Except IP address from' field and a 'Static IP address list configuration' button. The 'Lease time' is set to 86400 and 'Max lease time' to 604800. The 'Interface' is set to 'LAN Interface' and 'Update style' is 'None'. There is a 'DNS server IP address' field with 'Add' and 'Delete' buttons. The 'WINS server' field is empty, and 'Print server' is unchecked. The 'Broadcast address' is 21.21.255.255, and 'Domain name' is empty. The 'Router' field is empty. The 'Enable NTP' checkbox is checked, and 'Disable 'Time Offset' Option' is unchecked. The 'Deployment Service' section includes 'DLS server' and 'DLS port' (18443) fields, and 'DCMP server' and 'DCMP port' (18080) fields.

Enable Customization: allows user to upload its own configuration of DHCP server. The syntax and contents of the file(s) will not be checked, so wrong configuration may cause the DHCP service to not start. When the checkbox is checked, the general DHCP configuration will be disabled. The configuration will be preserved in case of upgrades.

Note: customized files must be uploaded to both nodes if redundant OSBs are used.

Static IPs can be configured for certain devices from range of the Range of IPs specified.

Hostname: the hostname which applies for the configured IP.

MAC address: MAC address (in the format AA:BB:CC:DD:EE:FF) associated with the configured IP.

General

IP address from-to: configure the range of IP addresses that will be available for clients.

Except IP address from-to: IPs from range that will not be provided to clients. Lease time: default lease time (in seconds) of the DHCP leasing mechanism. Max lease time: maximum lease time (in seconds) to be applied.

WINS/Print Server: IPs to be provided to DHCP clients.

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

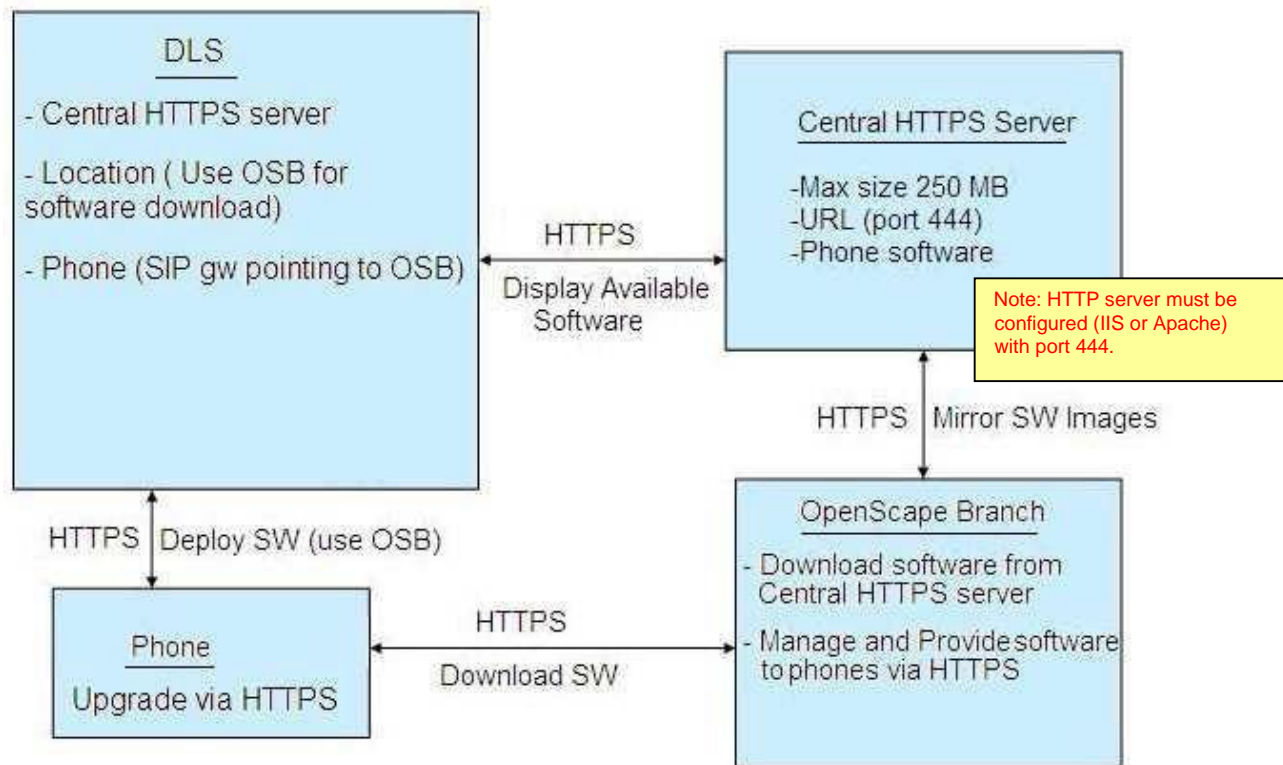
DLS Server/Port: IP address/Port to be provided to DHCP clients. DHCP is only for IPV4.

If OSB is Master DNS (DNS-SRV only), then it must be at the top of the list.

24 Phone Software Management

24.1. Feature Description- Prerequisites

Area in OSB disk is reserved for phone SW so that phones can upgrade application from OSB within the Branch instead of connecting to main HTTPS server in Data Center. With this capability a software load is only downloaded once to the branch instead of having multiple downloads for each of the phones at the branch. It is very useful when limited bandwidth is available to the branch. DLS informs devices accordingly to use OSB appliance for phone software upgrade. OSB pulls phone software from the configured HTTPS server. For this implementation, all phones belonging to a branch, must be assigned to a DLS location. DLS location must be set to use OSB for software deployment and may include more than one branch.

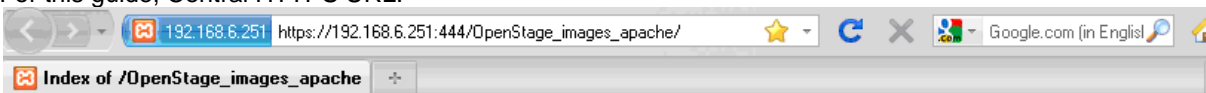


- Branch Office has been created on the OSV with OSB (only OSB is supported)
- HTTP server configured (IIS or Apache) with port 444 and administrator must check not to exceed 250 MB of software
- OSB mirrors with the Central HTTP phone SW Server (port 444). Both must be configured with port 444
- Central HTTPS server URL: server where the phone software is uploaded (<https://server/path>)

24.2. Central HTTPS server

HTTPS server is configured (IIS or Apache) with port 444 and administrator must check not to exceed 250 MB of software. This URL must be accessible from the network where the OSB resides. The HTTPSServer should allow Directory Listing in order to be able to scan subfolder contents. Additionally, copy dls_directory_reader.asp or dls_directory_reader.php file (depending on the HTTPS server implementation followed), from within the installer DLS folder \Tools into the root directory of the HTTPSServer.

For this guide, Central HTTPS URL:



Index of /OpenStage_images_apache

- [Parent Directory](#)
- [OS_HI_SIP_V2_R2_47_4.img](#)
- [OS_HI_SIP_V3_R0_73_0.img](#)
- [OS_HI_SIP_V3_R1_26_0.img](#)
- [OS_LO_SIP_V2_R2_47_4.img](#)
- [OS_LO_SIP_V3_R0_73_0.img](#)
- [OS_LO_SIP_V3_R1_26_0.img](#)
- [dls_directory_reader.asp](#)
- [dls_directory_reader.php](#)

Apache/2.2.21 (Win32) mod_ssl/2.2.21 OpenSSL/1.0.0e PHP/5.3.8 mod_perl/2.0.4 Perl/v5.10.1 Server at 192.168.6.251 Port 444

24.3. Phones

Only OpenStage phones are supported. Only Openstage phones are supported. Optipoints do not support functionality to retrieve phone software from HTTPserver.

Phone sip gateway must always be set and point to OSB. In case of FQDN or DNS SRV usage, DLServer must be able to resolve these entries.

24.4. Branch Office

For the purposes of this guide, the Branch Office setup on the OSV is displayed OSV : grp1016c

BG: BG Manual testing Branch Office : RX200_Goliath

Subscribers : (4) 2105007001, 2105007002, 2105007003, 2105007004

Representative endpoint : 192.168.6.88 (OSBip)

24.5. OSB Configuration

Enable Phone Software Management on OSB.

Configuration > OpenScope Branch > Branch Office > Configuration > Features > Enable Phone Software Management.

The screenshot shows the 'Phone Software Management' configuration window. It is divided into two main sections: 'Periodic Branch Pulling Software from Central Server' and 'Phone Pulling Software from Branch'.

Periodic Branch Pulling Software from Central Server:

- ☒ Enable software pulling
- Start time (hh:mm): 02:00
- Stop time (hh:mm): 06:00
- Central phone software server URL: https://192.168.6.214:444/OpenStag
- Start software pulling button

Phone Pulling Software from Branch:

- ☒ Enable image provisioning
- Maximum parallel access: 3
- Available phone software images: (empty list box)
- Delete button

Callout Box 1 (Top Right):

- Enable:** enables/disables the download of phone software from the HTTPS server.
- Start time:** defines when download of phone SW will begin.
- Stop time:** defines when download of phone SW will stop if download not completed yet.
- Central phone software server URL:** server where the phone software is uploaded.
- Start software pulling:** immediately begins the download of phone software from the HTTPS server.

Callout Box 2 (Bottom Right):

- Enable:** enables or disables the provisioning of SW to phones.
- Maximum Parallel Access:** sets the maximum allowed parallel upload sessions for phones.
- Note:** After mirroring with HTTPS server all phone software loads are transferred to /osb/var/PhoneSwDownload. All these images are moved to /osb/var/PhoneSwRepository and are available to phones for upgrade. Links to the file will be made in the PhoneSwDownload directory. Available Phone SW Images are displayed and can be deleted manually.

OK Cancel

After Phone Software Management setup has been completed and OSB has completed the download (scheduled or immediate) of phone images, administrator can check that OSB provides http server functionality by opening any browser and selecting one of the following URLs:

https://<osb_ip>:4560/opt/siemens/openbranch/var/PhoneSwRepository or https://<osb_ip>:4560/



Index of /

Icon	Name	Last modified	Size	Description
[]	OS HI SIP V2 R2 47 4.img	05-Dec-2012 12:58	24M	
[]	OS HI SIP V3 R0 73 0.img	05-Dec-2012 12:58	22M	
[]	OS HI SIP V3 R1 26 0.img	05-Dec-2012 12:58	24M	
[]	OS LO SIP V2 R2 47 4.img	05-Dec-2012 12:58	13M	
[]	OS LO SIP V3 R0 73 0.img	05-Dec-2012 12:58	14M	
[]	OS LO SIP V3 R1 26 0.img	05-Dec-2012 12:58	14M	

At this point, OSB has mirrored successfully the phone software from the Central HTTP server and OSB is able to provide this software to the branchphones

24.6. DLS Configuration

All branch phones must be assigned to one location. One location can be set to include more than one branch office.

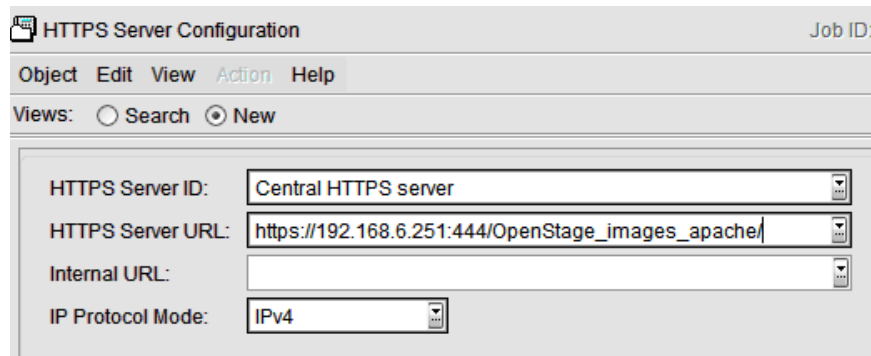
It is assumed that phones are already registered with DLS, either DLS IP has been provided to phones via DHCP option or DLS scan feature has been used.

Please note that once configuration is completed, for each branch subscriber, the corresponding location will be set only if phone is registered with DLS

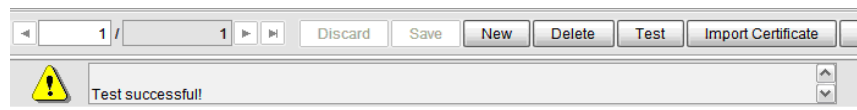
24.7. Configure Central HTTPS Server

Configure HTTPS Server ID and URL, and then save.

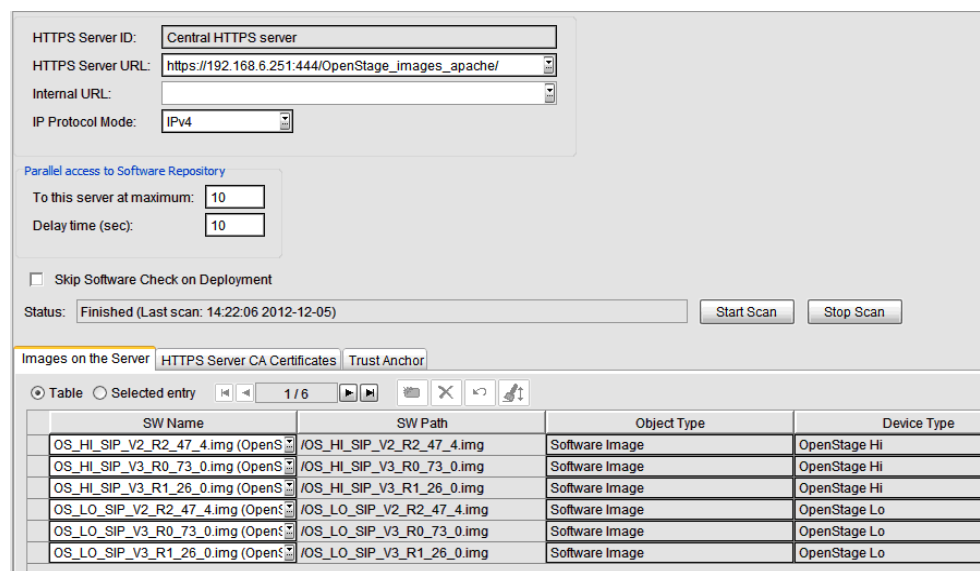
Deployment Service > Administration > Server Configuration > HTTPS Server Configuration.



Use “Test” functionality to correct and check full communication

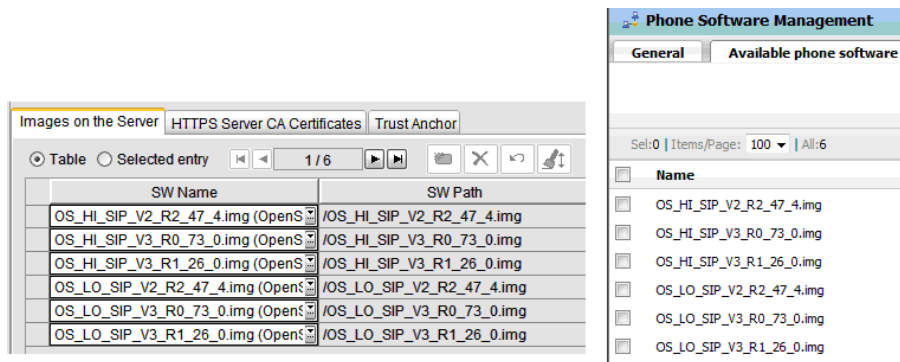


Start scan to check sw available on the server. After scanning is completed, DLS entry “Central HTTPS server” will display phone images.



SW Name	SW Path	Object Type	Device Type
OS_HI_SIP_V2_R2_47_4.img (OpenS...	/OS_HI_SIP_V2_R2_47_4.img	Software Image	OpenStage Hi
OS_HI_SIP_V3_R0_73_0.img (OpenS...	/OS_HI_SIP_V3_R0_73_0.img	Software Image	OpenStage Hi
OS_HI_SIP_V3_R1_26_0.img (OpenS...	/OS_HI_SIP_V3_R1_26_0.img	Software Image	OpenStage Hi
OS_LO_SIP_V2_R2_47_4.img (OpenS...	/OS_LO_SIP_V2_R2_47_4.img	Software Image	OpenStage Lo
OS_LO_SIP_V3_R0_73_0.img (OpenS...	/OS_LO_SIP_V3_R0_73_0.img	Software Image	OpenStage Lo
OS_LO_SIP_V3_R1_26_0.img (OpenS...	/OS_LO_SIP_V3_R1_26_0.img	Software Image	OpenStage Lo

Based on the setup so far, DLS is aware of the phone software that the OpenscapeBranch contains since it scanned the Central HTTPS server which the Openscape Branch used to download images from



24.8. Obtain Branch Office Data

Branch Office data to be retrieved are Switch name, BG name and Branch name. **PFR must be set on OSV**

a) Create Packet Filter Rule to allow DLS to communicate with OSV

Packet Filter Rule Name: DLS_Sync

Description: Allow soap call from DLS to bond node IP Remote FQDN:

Remote IP Address: 192.168.6.251

<dls server ip> Remote NetMask: 255.255.255.255

Remote Port Begin: 0 Remote Port End: 0 Direction: InComing

Local Host : bond_node_alias Local Port Begin: 8769

Local Port End: 0 Transport Protocol: TCP Action: Allow

Note: PFR does not apply for onboard DLS servers.

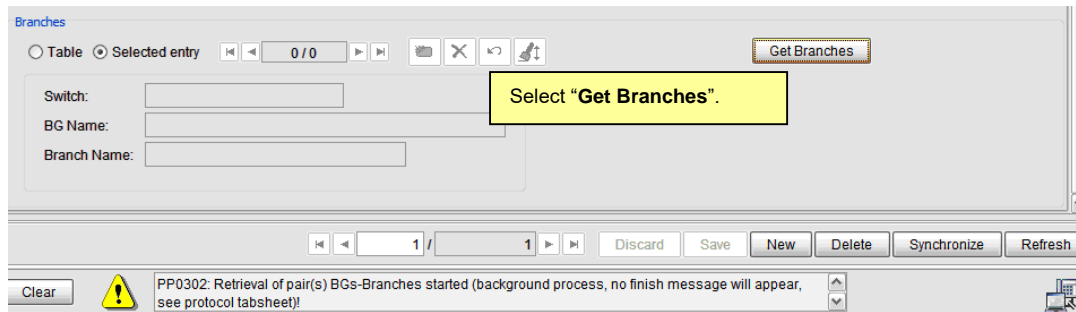
b) Create Element Manager and Get Branches

Deployment Service > Element Manager > Element Manager Configuration > Create a new element manager. Select Element Manager Type: OpenScape Voice and port 8769 and Save.

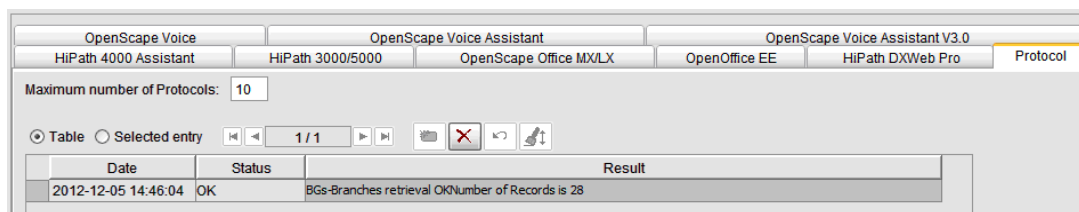
Note: Element Manager address is the admin ip of node 1 (only for geographic separated osv cluster complete the 2nd EM address with node 2 ip).

The screenshot shows the 'Element Manager' configuration window. It has a 'Job ID' field and an 'Exec Time' dropdown set to 'asap'. The 'Views' section has 'Search' and 'New' options. The main configuration area includes fields for 'Element Manager ID' (set to 'Openscape Voice v6'), 'Element Manager Address' (set to '10.10.162.10'), '2nd EM Address' (empty), 'Port' (set to '8769'), 'Protocol' (set to 'http'), 'Account' (empty), 'Password' (empty), 'E.164 Prefix' (empty), and 'Remark' (empty). The 'Element Manager Type' is set to 'OpenScape Voice'. There are checkboxes for 'On Synchronization update registered workpoints as soon as possible' (checked), 'Allow just 1 workpoint per E.164' (unchecked), 'Add new subscribers as IP Clients' (unchecked), and 'Add new subscribers as IP Phones' (checked). The 'Synchronization interval [min]' is set to '0' with a note '(0 = no automatic synchronization)'.

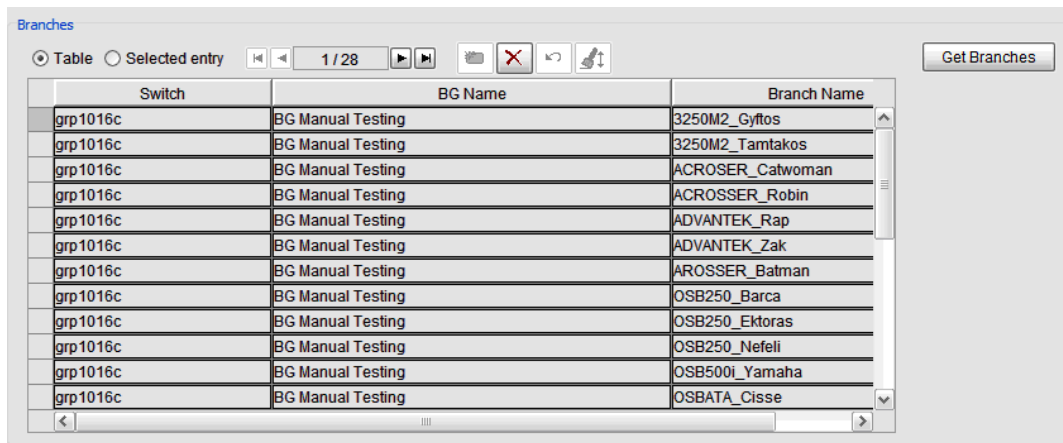
After selecting Save, admin must scroll down, select OpenScape Voice tab and then click the “Get Branches” button. As stated in the bottom message area, admin must see protocol tabsheet to check status



Select Protocol tab and then refresh to verify.



Selecting refresh at this point in OpenScape Voice tab, will display the Branch Offices configured on the Openscape Voice server (only the ones that are type OpenScapeBranch)



24.9. Synchronize with OpenScope Server

Synchronization will get subscriber data (E164DN, Switch, BG, Branch Office).

Deployment Service > Element Manager > Element Manager Configuration. Select the element manager already created in step 3.2 and select to Synchronize

Element Manager configuration window showing the 'OpenScope Voice' tab. The configuration includes fields for Element Manager ID, Address, Port, and Protocol. The 'Synchronize' button is highlighted in the bottom right corner.

As stated in the bottom message area, admin must see protocol tab to check status.

Date	Status	Result
2012-12-05 15:40:32	OK	Synchronization of Plug&Play Data with Elementmanager started at 'Wed Dec 05 15:36:14 EET 2012'*****...
2012-12-05 14:46:04	OK	BGs-Branches retrieval OK Number of Records is 28

24.10. Location

Location is the parameter that binds the phones with the OSB and the phone software on the OSB with the phone software on the Central HTTPServer.

Deployment Service > Administration > Server Configuration > Location Name: Enter the Name for the Location.

HTTPS Server: Select the previously configured HTTPS server that the OSB is mirroring from.

Use OSBranch for Software Deployment: select the checkbox to use OSB to provide software to the phones. “OSBranch path” and “OSBranch port” values will be set and active (not grayed out anymore) Business groups (tab): add the Branch Office (one or more).

Note: Restrictions can be configured on “SW Deployment Restrictions” tab.

Location

Job ID: Exec Time:

Object Edit View Help

Views: ☐ Search ☒ Object ☐ Table

Name: ☐ PKI Connector enabled

Parent Location:

FTP Server:

HTTPS Server:

Network Drive:

☒ Use OSBranch for Software Deployment

OSBranch path: OSBranch port:

Remark:

Default values (informational only)
 OSBranch path : /opt/siemens/openbranch/var/PhoneSwRepository
 OSBranch port : 4560
 Note: It is possible to configure many Branch Offices in one location. Each phone belonging to a specific Branch Office will only contact its own corresponding OSB.

Infrastructure Policies P&P Number Pool SW Deployment Restrictions Certificate Deployment Restrictions

IP Ranges Reg-Addresses E.164-Patterns Business Groups

1 / 1

Switch	BG Name	Branch Name
grp1016c	BG Manual Testing	RX200_Goliath

Verification: OSB subscribers must be configured with location “OSB Location” at the DLS server (phones already registered with DLS server as mentioned previously)

- Switch: grp1016c (OSV)
- BG Name: BG Manual testing (BG)
- Branch Name: RX200_Goliath (Branch Office)
- Branch subs: 2105007001, 2105007002, 2105007003, 2105007004
- DLS location: OSB Location

Search by location (pop up list should include configured location)

IP Device Configuration

Job ID: Exec Time:

Object Edit View Action Help

Views: ☐ Search ☐ Object ☐ Table

IP Address: IP Address 2: IP Protocol Mode:

Device ID: SW Version: Device Family:

Device Type: SW Type: Windows Account:

E.164: Reg-Address:

Basic E.164: Last Registration:

Remarks:

General ☒ Synchronization ☐ Profile ☐ DLS-Connectivity ☐ Security State Protocol ☐ OCMP ☐ Autoconfig IP Phone ☐ Autoconfig IP Client ☐ Autoconfig IP Gateway ☐ Archives Data

☐ Administration disabled

☐ Autodeployment disabled

☐ Automatic Certificate Deployment disabled

☐ Preconfigured IP Device

IP Device Update:

Autoconfiguration

☐ Activate Plug&Play

☐ Delete after Plug&Play

☐ Use for HFA Mobility with HPATH 3000

☐ Apply Default Profiles at IP Device Registration

Location:

Find in Table

Search:

OSB Location Location

1 / 1

OK Cancel

Close Window Search

Results: Please note that if phones are registered with DLS, then a valid IP address will be displayed in the corresponding column field.

Service V6								
IP Device Configuration								
Job ID: <input type="text"/>								
Object Edit View Action Help								
Views: <input type="radio"/> Search <input type="radio"/> Object <input checked="" type="radio"/> Table								
	● E.164 ▲	Element Manager ID	System Type	Switch	Business Group	Branch Office	Location	IP Address
2105007001		OSV v6	OpenScape Voice	grp1016c	BG Manual Testing	RX200_Goliath	OSB Location	192.168.6.203
2105007002		OSV v6	OpenScape Voice	grp1016c	BG Manual Testing	RX200_Goliath	OSB Location	192.168.6.200
2105007003		OSV v6	OpenScape Voice	grp1016c	BG Manual Testing	RX200_Goliath	OSB Location	192.168.6.202
2105007004		OSV v6	OpenScape Voice	grp1016c	BG Manual Testing	RX200_Goliath	OSB Location	192.168.6.205

24.11. Phone Deployment

DLS offers two ways to deploy phonesoftware.

1. Deployment Service > Software Deployment > Deploy Workpoints
2. Deployment Service > Software Deployment > Manage Rules

OpenScape Deployment Service V6

- DeploymentService
 - Administration
 - IP Devices
 - Mobile Users
 - Gateways
 - Software Deployment
 - Deploy Workpoints
 - Manage Rules
 - Element Manager
 - Profile Management
 - XML Applications
 - Job Coordination
 - Help
 - Logoff admin

Deploy Workpoints

Object Edit View

Views: ☒ Search

IP Address:

Device ID:

Device Type:

E.164:

Basic E.164:

Remarks:

Software Deployment

Configuration data for

Note: phones have been grouped to locations so admin can use "SW Deployment Restrictions" in order to schedule phone software deployments (e.g. Off Hours)

Select the already configured location on the DLSServer.
Select and configure the options on "SW Deployment Restrictions" tab

Location

Job ID:

Object View Help

Views: ☐ Search ☒ Object ☐ Table

OSBranch path: OSBranch port:

Remark:

IP Ranges Reg-Addresses E.164-Patterns Business Groups Infrastructure Policies P&P Number Pool **SW Deployment Restrictions** Certificate Deployment Restrictions

☒ Monday

☐ Whole day
☒ Between and

☒ Tuesday

☐ Whole day
☒ Between and

☒ Friday

☐ Whole day
☒ Between and

☐ Saturday

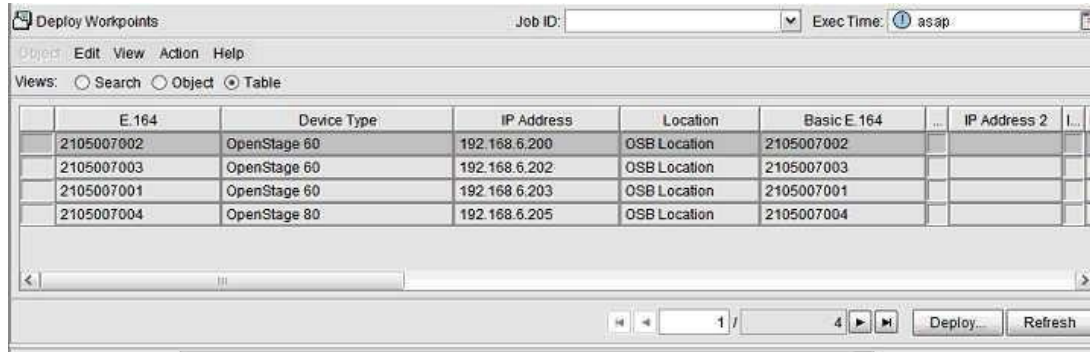
☐ Whole day
☒ Between and

24.12. Deploy Workpoints

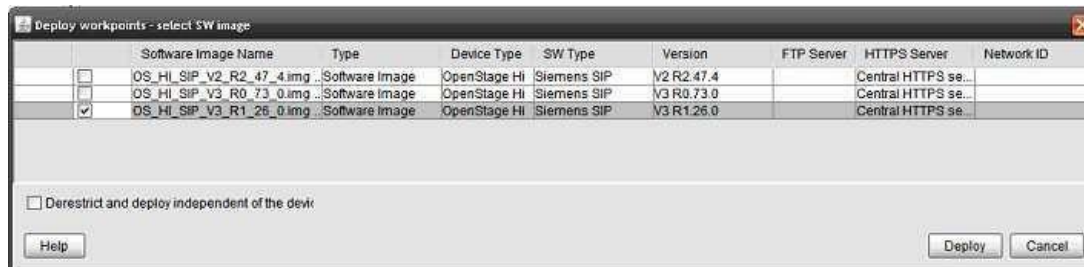
Deployment Service > Software Deployment > Deploy Workpoints

Admin can search by location (click on the drop down button in the location field to select location from a list).

Select table view to view all phones



Select phone software and press "Deploy"



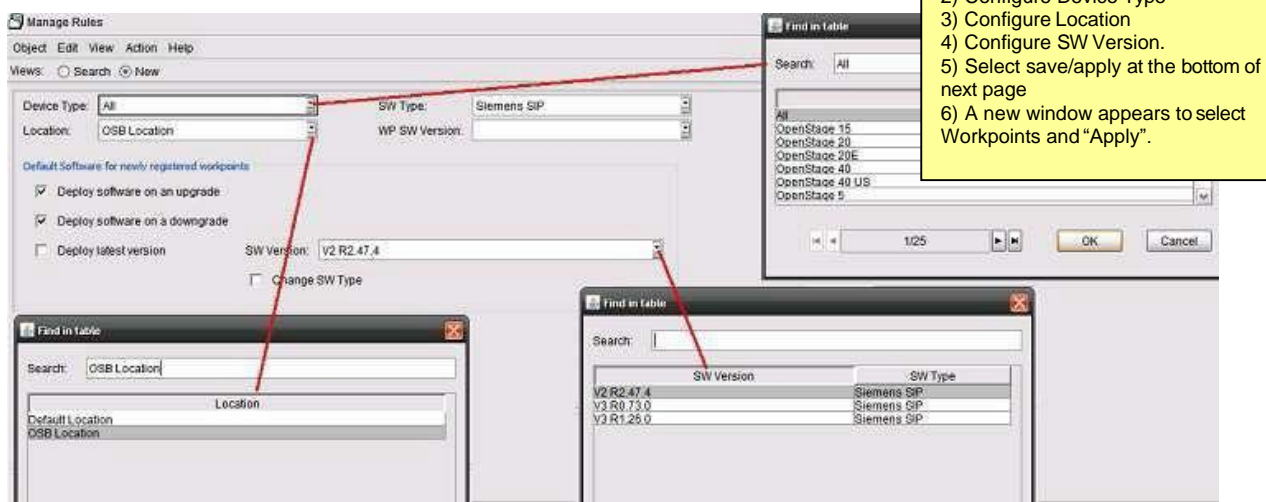
Select deployment options:

- Enforce deployment if phone is busy

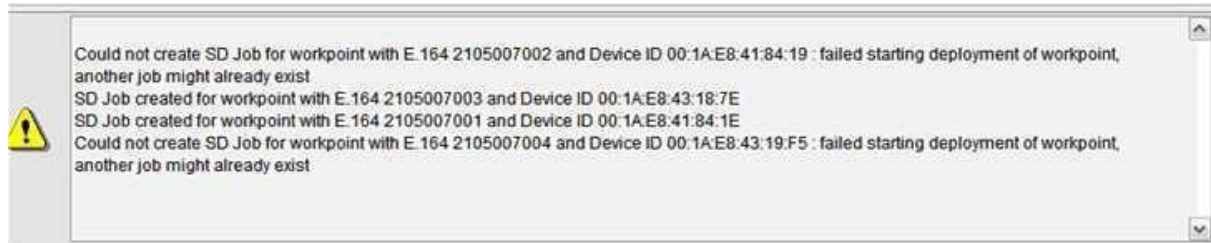
- Overwrite deployment restrictions and then confirm, by pressing "OK" Second option refers to the restrictions set when configuring the location.

24.13. Manage Rules

Deployment Service > Software Deployment > Manage Rules



After the last step is completed, info will appear on the bottom message area regarding the last actions that took place.



Verification: Navigate to Job Control for verification. This applies for both ways of software deployment (Deploy Workpoints and Manage Rules)

Deployment Service Job Coordination Job Control. Select table view

	E.164	IP Address	IP Address 2	Device ID	Action Type	Action Status	Device Type
	2105007001	192.168.6.203		00:1A:E8:41:84:1E	Software Deployment	active			OpenStage 60
	2105007003	192.168.6.202		00:1A:E8:43:18:7E	Software Deployment	active			OpenStage 60
	2105007002	192.168.6.200		00:1A:E8:41:84:19	Software Deployment	active			OpenStage 60
	2105007004	192.168.6.205		00:1A:E8:43:19:F5	Software Deployment	active			OpenStage 80

As stated above there are 4 jobs active, including the two devices that DLS could not create SD Job for in the previous step. Admin can select any job to check execution time and deployment data.

IP Address: 192.168.6.203 IP Address 2: Location: OSB Location

Device ID: 00:1A:E8:41:84:1E SW Version: V3 R0.68.0

Device Type: OpenStage 60 SW Type: Siemens SIP

E.164: 2105007001 Action Type: Software Deployment

Reg-Address: 10.10.161.16 Action Status: active

Remarks:

Basic Data | Deployment Data | Configuration Data | XML Application Data

Activation Time: 2012-12-10 16:23:53 Repository: <https://192.168.6.88:4560/opt/siemens/openbranch/var/PhoneSwRepository>

Execution Time: File Path: /

Planned Execution Time: 2012-12-10 21:59:51 File Name: OS_HI_SIP_V2_R2_47_4.img

End Time: File Type: APP Port: SW Type: Siemens SIP

Connection Attempts: 0 Username:

Note: DLS instructed the phone to download the phone image from the OSB and SW deployment is scheduled at a later time.

25 Auto Attendant (AA)

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.

Note: If Auto Attendant is used with IGW then Phones/GWs must not be configured with G.729A only, G.711 codec is also required.

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 routing instances. Each instance must be associated to a destination number.

Configuration > OpenScape Branch > Branch Office > Configuration > Features > Enable Auto Attendant

Time Information: Configured time or from NTP server.

Inter digit timer: time the system will wait for more digits when digits were already dialed (3-15).
Record Access Code: code used to record user's announcements
Wait to go to menu: delay to get connected to Menu Announcements.

Auto Attendant Menus can be added, edited, or deleted here

Announcements: list of WAV files that can be used for AA configuration/menus. WAV files can be uploaded/deleted.
Note: Only WAV audio files (.wav) with: Bit Rate: 128kbps, Audio Sample size: 16 bit, Channels: Mono, Sampling Rate: 8 kHz, Audio Format: PCM are allowed for announcements.

Note: if using 50i and uploading a large WAV file then pipe message could show on B2BUA log.

Note: Endpoint profile Xfer service must be enabled in OSV for AA feature

Name: Auto Attendant route.
Routing method: 1) FQDN/IP: Domain name in the R-URI of incoming SIP calls. 2) DN: Called destination number (user name in the R-URI of SIP call or called party number of BRI calls).
FQDN/IP or DN: FQDN/IP and DN configured in this field must also be configured in the OSV in order to route the calls to the Auto Attendant in Normal Mode (Routing code required for FQDN/IP routing).
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 1/2/3: Menus can be assigned to Routing route.
Initial Greeting: played when the caller reaches the Auto-Attendant.
Forward to Original Destination: 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 disabled, Menu 1 is a required field.
Default Destination: default destination for calls when there is no menu associated or active for the called Auto Attendant route.
Note: default destination number can be an extension number or an external number. It is recommended to use full extension number when configuring this parameter.
Note: routing DN must not be a registered subscriber.

Auto attendant menu

Auto attendant menu provisioning.

General

ID
1
Name

Activation mode
Automatic

Weekday start
Monday
Weekday stop
Monday

Time1 start (hh:mm)
Time1 stop (hh:mm)

Time2 start (hh:mm)
Time2 stop (hh:mm)

Activation code
Deactivation code

Time out (sec)
10

Destination selection greeting file
enter-num-to-call.wav
Failure prompt file
num-not-valid.wav

Final prompt file
goodbye.wav
Default destination prompt file
connect-to-party.wav

Transfer prompt file
transfer.wav

Extension dialing
☐
Default destination

Number of extension dialing digits
7

Digits

☒ Digit selection

Row	Digit	Name	File	Repeat this menu	Destination	Allow recording
1	1	SalesDept	menu1_digit1.wav	<input type="checkbox"/>	5558885200	<input checked="" type="checkbox"/>
2	2	CustomerService	menu1_digit2.wav	<input type="checkbox"/>	5558885300	<input checked="" type="checkbox"/>
3	3	Billing	menu1_digit3.wav	<input type="checkbox"/>	5558885400	<input checked="" type="checkbox"/>
4	4		menu1_digit4.wav	<input type="checkbox"/>		
5	5		menu1_digit5.wav	<input type="checkbox"/>		
6	6		menu1_digit6.wav	<input type="checkbox"/>		
7	7		menu1_digit7.wav	<input type="checkbox"/>		
8	8		menu1_digit8.wav	<input type="checkbox"/>		
9	9		menu1_digit9.wav	<input type="checkbox"/>		
10	0		menu1_digit0.wav	<input type="checkbox"/>		
11	*	Repeat Menu	menu1_digit*.wav	<input checked="" type="checkbox"/>		
12	#		menu1_digit#.wav	<input type="checkbox"/>		

Digit: selection number.

Name: name for the dial rule.

File: Announcement played if digit is dialed.

Destination: Destination number to which the call will be routed. **Allow Recording:** enable / disable announcement recording for that destination (**E164 number required**).

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.

Name: name for Menu.

Time Out: timer before call is routed to default destination.

Activation Mode:

- Automatic: enabled/disabled automatically by configuredtime.
- Manual: enabled/disabled via access code.
- Both: Automatic and Manual enabled/disabled is allowed.

WeekDay/Time configuration: configuration when menu will be enabled/disabled automatically. Only applies if Activation mode is Automatic or Both.

Activation Code: Code used to enable menu (Manual and Both modes only)

Deactivation Code: Code used to disable menu (Manual and Both modes only)

Destination selection greeting: announcement guides caller to select a destination.

Failure prompt: announcement presented to caller when chosen destination is invalid.

Default destination prompt: announcement presented before xfer to default destination.

Final prompt file: announcement presented to caller when chosen destination is invalid and the default destination could not answer the call for some reason or it is not configured.

Transfer prompt file: announcement presented to caller when call is transferred to the chosen destination.

Extension dialing.... caller will be able to dial the desired extension number.

Default Destination: escape destination for Menu if a valid option is not selected.

Number of Extension Dialing Digits: maximum number of digits that can be dialed for an extension Extension Dialing is activated

Digit Selection: This shall allow a customer to route all calls to a particular DN to an announcement and then forward on to a destination.

Note: To record an announcement (only one Welcome message/subscriber) dial the RA-Code (ex. *98) directly from one of the subscribers that has Recording Enabled (ex.5558885200). The FROM header should correspond to the Subscriber number format. A called party then routed to the Record Enabled Auto Attendant Destination will first get that Welcome message before being transferred to that subscriber.

26 Message rate control

In previous version this was named SNORT (Network Intrusion Prevention System (NIPS)) and Network Intrusion Detection System(NIDS), which performs packet logging and real-time traffic analysis on IP networks. It checks for networks packets and tries to find a “signature” in suspect packets. When the feature is enabled and Message Rate Threshold is reached, the Snort (now the IP Tables) will configure a Firewall rule to block the IP that generated such traffic. This IP will be monitored, if no more traffic comes from this IP the Firewall rule will be removed when block period expires. Otherwise, the block period will be renewed.

Note: OSB IP as well as PC for OAM should be configured in IP addresses to avoid packet lost.

Configuration > OpenScape Branch > Branch Office > Configuration > Security > Message rate control

Security

Select OK to temporarily store changes. Make your changes permanent by selecting 'Apply Changes' on the General page.

General **Firewall** **Message Rate Control** **RADIUS** **Tunnel Cor**

Message Rate Control Settings:

☐ Enable Message Rate Control

Message rate threshold: 20000

Block period (sec): 60

White list:

Enable Message Rate Control: Enable/Disable the feature.
Message Rate Threshold: number of messages per sec which will block an IP address (100-256000).
Block Period: blocking time of IP address in seconds (1-2048).
IP Address: list all IPs which will not be blocked by the IP Tables.

NOTE: SNORT has been replaced by the IP Tables since V8R0.

27 Digest Authentication Credentials synchronization between OSB and OSV

During the SIP registration process, OSB requests for the Subscriber Data and for the Digest Authentication Credentials if these feature is enabled in the OSB.

Note: The OSB's FQDN (<hostname>.<domain name>) must be configured as an alias for the branch endpoint in the OSV.

Configuration > OpenScape Branch > Branch Office > Configuration > Security > General > Digest Authentication Tab

The screenshot displays the 'Security' configuration window with the 'General' tab selected. Below the tabs, there is a table of user credentials and a 'Digest Authentication' section.

	User name	Administrative privilege	Change Password in first login	SSH login	Expires (days)	Enabled
1	administrator	Administrator	<input type="checkbox"/>	<input checked="" type="checkbox"/>	99999	<input checked="" type="checkbox"/>
2	service	Administrator	<input type="checkbox"/>	<input checked="" type="checkbox"/>	99999	<input checked="" type="checkbox"/>
3	guest	Read Only	<input type="checkbox"/>	<input type="checkbox"/>	99999	<input checked="" type="checkbox"/>
4	assistant	Administrator	<input type="checkbox"/>	<input type="checkbox"/>	99999	<input checked="" type="checkbox"/>
5	redundancy	Read Only	<input type="checkbox"/>	<input type="checkbox"/>	99999	<input checked="" type="checkbox"/>
6	ACD	ACD Administrator	<input type="checkbox"/>	<input type="checkbox"/>	99999	<input checked="" type="checkbox"/>
7	cdr	Read Only	<input type="checkbox"/>	<input type="checkbox"/>	99999	<input checked="" type="checkbox"/>

Digest Authentication

☒ Digest authentication

Server quality of protection (QOP)

Nonce life (sec)

Max retries

Buttons: Add, Edit, Delete, OK, Cancel

Provides the access to Emergency Services.

As a general rule the emergency calls should be forwarded to PSTN gateway which supports CAMA functionality in US or for other PSTN gateway in cases where CAMA is not used. A call to the Emergency Number triggers the server to try to establish an outgoing call to an Emergency gateway (highest priority). When an Emergency call fails to reach the PSAP, call is re-routed to the configured local Destination (ex. Local Attendant) which has land line to call PSAP directly.

The Emergency calling menu is located under **Features** (Features Available in **Normal Mode** and **Survivability Mode**) and there are two sections available for configuration: Emergency Call Routing and Emergency Calling Numbers.

OpenScape Branch >Branch Office >Configuration> Features > Emergency Calling

Emergency Call Routing can be configured based on Subnet or DN list

Emergency Call Routing

Select OK to temporarily store changes. Make your changes permanent by selecting 'Apply Changes' on the General page.

General

☒

Subnet based routing

☐

DN list based routing

IP address or subnet

Subnet mask

DN numbers

Add

Delete

Routing prefix

None

Description

Default destination

Send LIN instead of CPN

☐

Two options available to configure Emergency Call Routing:
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: IP or range of IPs – Usually subscribers IP addresses for Survivability Mode and OSV's IP for Normal mode. – For NM using OSV, mask should be 255.255.255.255.
Subnet mask: IP subnet of the range of subscribers /OSV defined by IP configuration.
DN numbers: List of DN numbers. Up to 10 entries, numbers can be entered using regular expressions.
Routing prefix: configures preferred GW to be used, First digits of each prefix links the subnet/DN list to a dialed Emergency Number. – refer to Configuration Guide Session 63.2 “Configuration in the OSB” for additional information on routing prefix. If the gateway is required to make **Emergency as well as normal calls**, select the option **None**.
Description: description of emergency routing.
Default destination: if emergency call to the PSAP fails, the call is redirected to this local default destination (attendant).
Send LIN instead of CPN: send Calling Party Number (CPN) or Location Identification Number (LIN) on Q931

LIN				
Row	LIN	Callback number	Default callback number	Use default callback number
1	5558882810	5558882810		<input type="checkbox"/>

Emergency Calling Subnet - LIN

LIN: Local Identification Number used to associate a subscriber to its physical location
 CallBack Number: phone number registered at the PSAP. If an outgoing emergency call is unintentionally interrupted, then the remote operator may call back at this number

Notes :

"IP Address or Subnet" "255.255.255.255" and "Subnet Mask" "255.255.255.254" parameters are used when the IP address of calling SIP phone cannot be matched
 Routing prefix values will show only after GW entry is configured on GW provisioning table and flagged as emergency route

For OSB Proxy ATA and OSB Gateway Only, the Location Information and Emergency Calling Numbers are available under the FXS configuration menu (Features > Configure integrated gateway > Configure FXS > FXS Configuration) since the Emergency Calling feature is not available under Features.
 For any FXS subscriber, specific location information values can be set to override general values.

Location Information	
Building	<input type="text"/>
Floor	<input type="text"/>
Room	<input type="text"/>

FXS port configuration – Location Information

Each FXS port can be set with different value for Building, Floor & Room

(Features > Integrated Gateway > FXS Configuration > FXS Port configuration > Location Information).

If any parameter is not set for a specific FXS port, general values shall be used. If a parameter is configured for a specific FXS port, this value will supersede the general.

Emergency Calling Numbers

Emergency numbers

- 123
- [+]123
- [1][2|3]

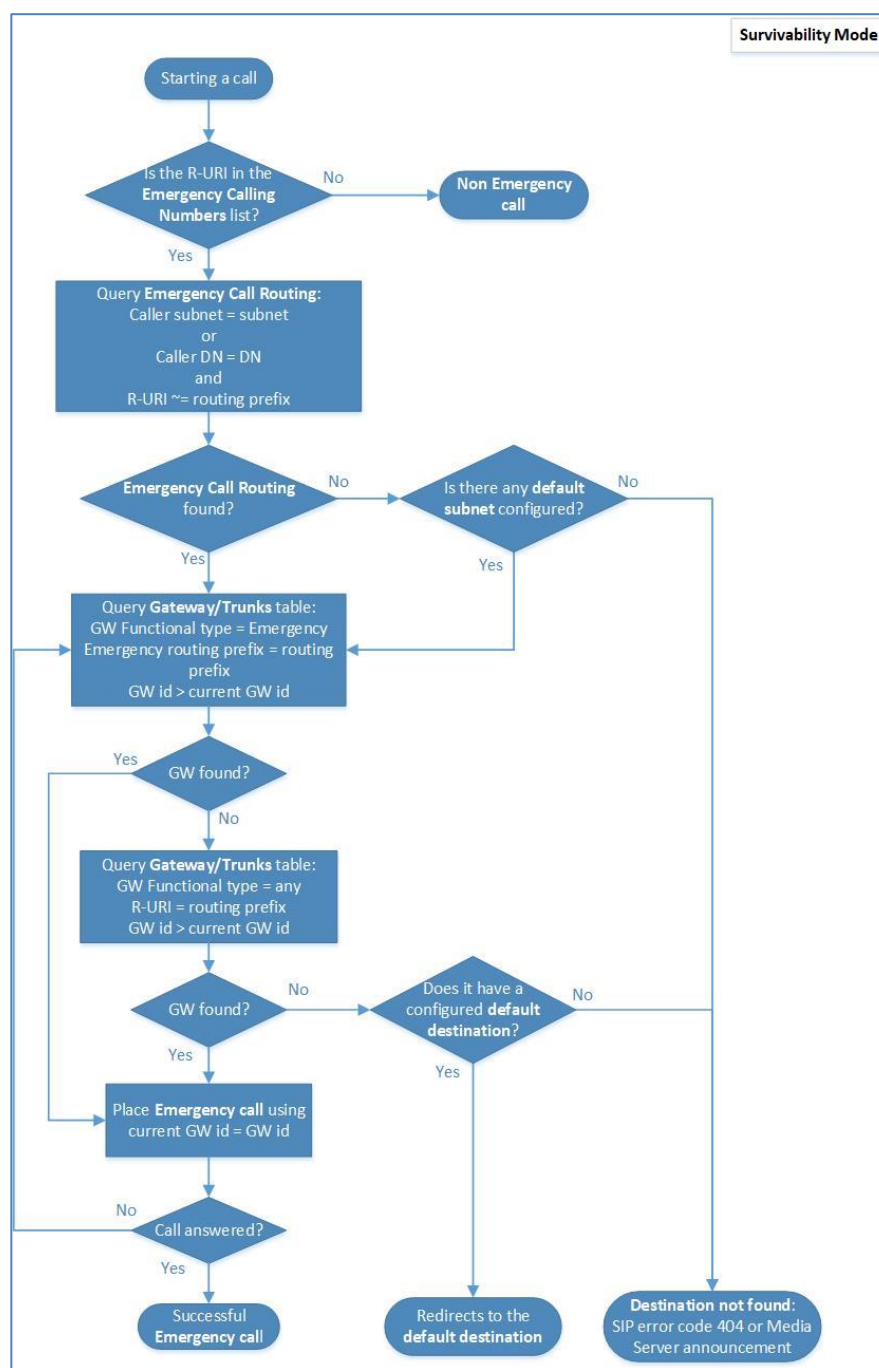
Emergency Calling Numbers:

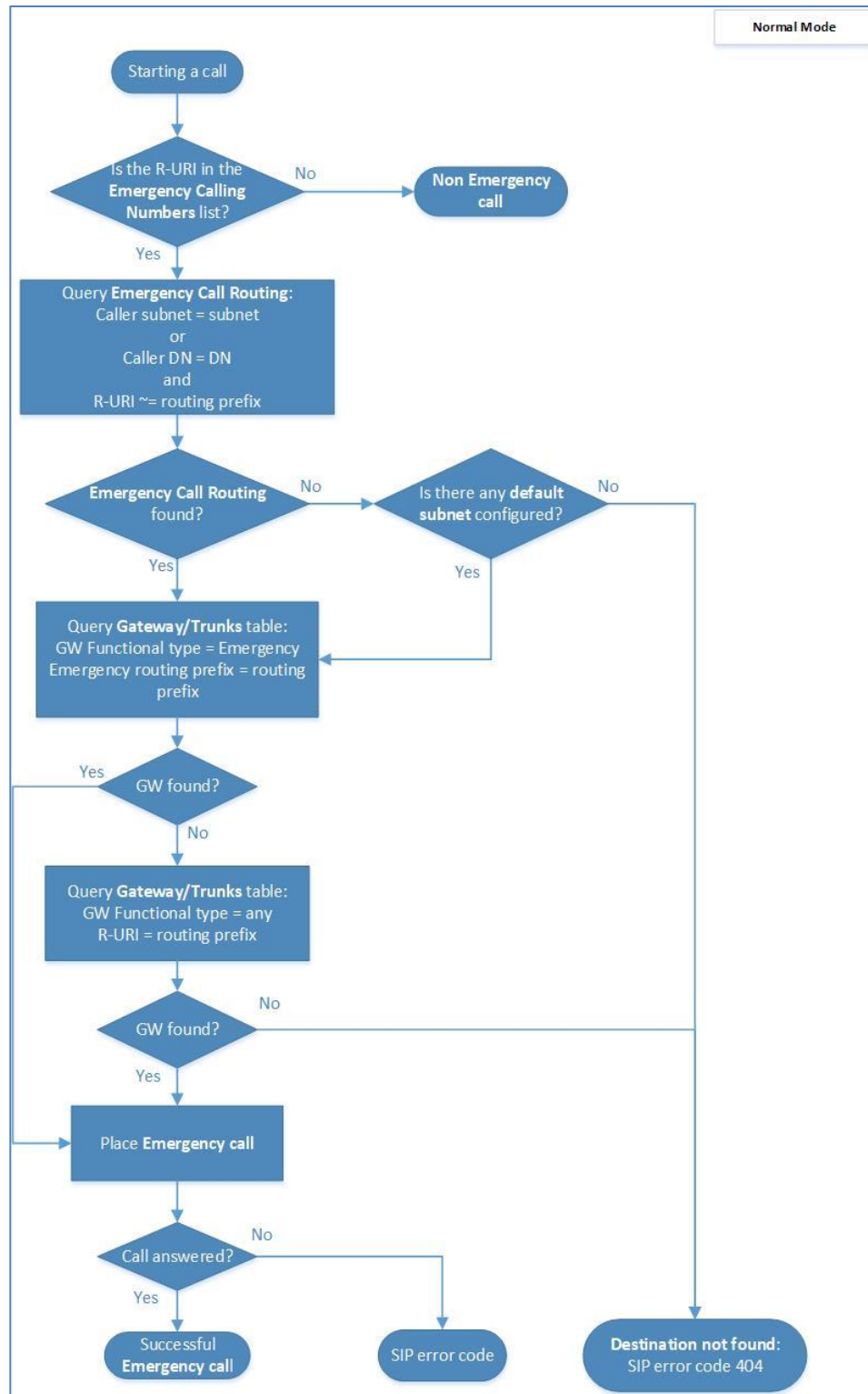
If a number from the list is dialed, OpenScape Branch identifies it as an "Emergency Call" (for USA this represents the 911 emergency calls). A call to a number from the emergency number list will trigger the server to try to establish an outgoing call to an available gateway (highest priority).

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. Only numerical digits and the characters *, # and + are supported as literals. The literals * and + must be inside of []. Expressions available do not necessarily comply with POSIX Regular Expression rules. Nevertheless, POSIX Regular Expressions are a good reference to build matching rules

The rules for the regular expressions are the same described for the Routing Prefix on Gateways/Trunks configuration. For further information refer to **18.12. Gateway Provisioning**.

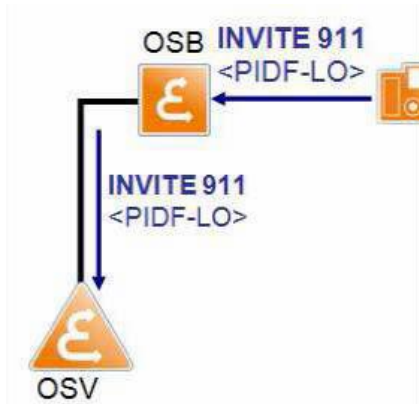
The following flowcharts illustrate how an emergency call works for Survivability and Normal modes.





29 NG911 support for Emergency Calling

Pass transparently the PIDF-LO and Geo-location header fields (NG911) - OSB shall support the transparent conveyance of location information (GeoLocation header fields and the PIDF-LO in the SIP message body)
 OSB: NG911 support for emergency calling - OSB shall be able to include a GeoLocation header field and a pre-defined PIDF-LO into an outgoing emergency call for location unaware phones.



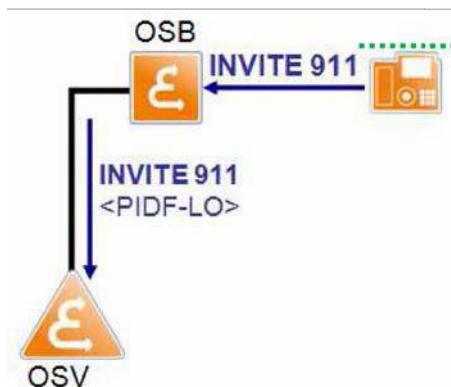
Location information for phones : ➤ DLS
 ➤ LLDP-MED

OSB in Normal Mode
 All operation modes are supported
 (Proxy, SBC-Proxy, Branch SBC)

Emergency call is transparently passed through

Location unaware phone

Mandatory parameters




Location Information	
Enable geo-location support <input checked="" type="checkbox"/>	
Country	Greece
State or region or province	ATT
County or parish or district	ATHENS
City	HRAKLEIO
Street	LEOFOROS HRAKLEIOU 455
Leading street direction	NORTH
Street type suffix	STR
Address number	155
Postal code	141 22
Postal community name	UNIFY
Building	MAIN
Floor	GROUND
Room	1.01

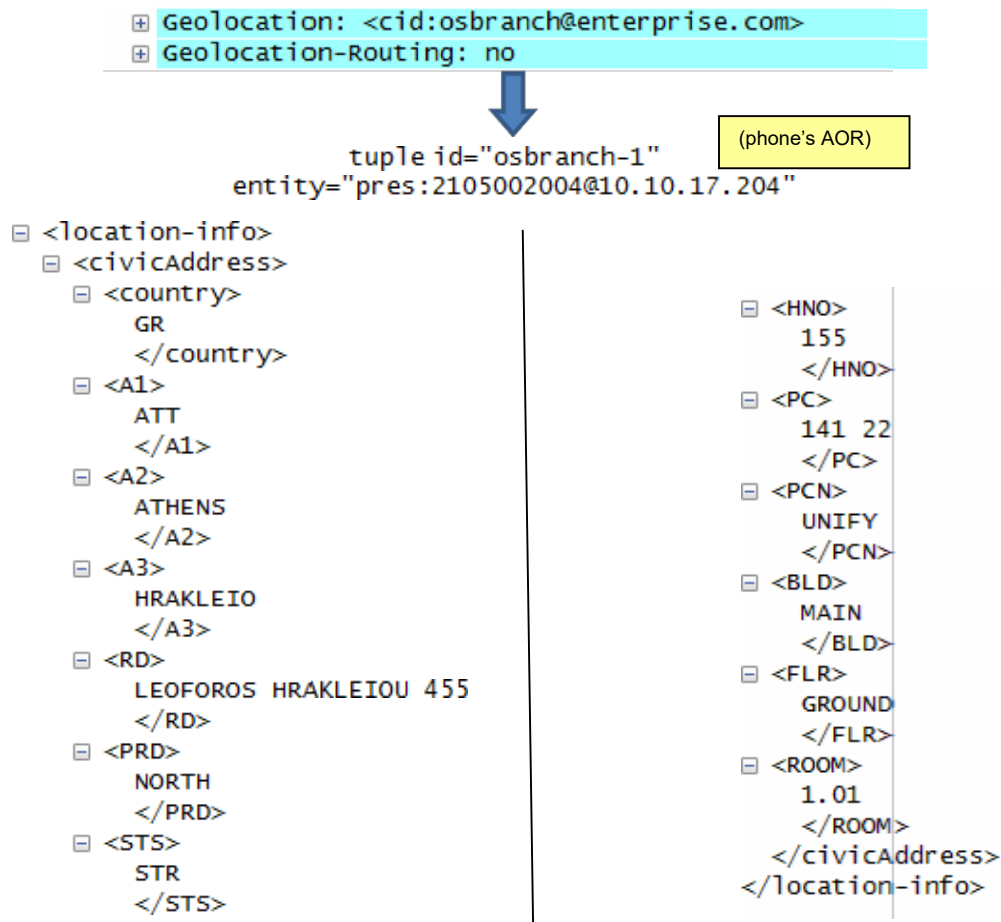
Configuration: Geo-location support must be enabled
 Features > Emergency Calling >
 Emergency Calling Subnet

OSB will add the Location information only when:

- 📞 OSB in Normal Mode
- 📞 INVITE request received from a SIP subscriber
- 📞 DN part of the R-URI corresponds to the routing prefix

 Geo-Location must be enabled

- OSB Gateway Only
- OSB Proxy ATA



Geo-location support for FXS (OSB 50i & OSB Proxy ATA)

Features > Integrated Gateway > FXS Configuration

Each FXS port can be set with different value for Building, Floor & Room

The screenshot shows the "FXS port Configuration" interface. It includes a section for "FXS Port provisioning" with a "Repeat interval (sec)" field set to 5. Below this is the "Location Information" section with fields for "Building" (FXS), "Floor" (2), and "Room" (Jupiter). A yellow box on the right contains the following text: "If any of the parameters are empty for a specific FXS port, general values shall be used. If a parameter is configured for a specific FXS port, this value will supersede the general value".

- Emergency number must be configured to identify that the dialed number corresponds to an emergency

-
- If an emergency number is configured for a subnet which includes the OSB LAN IP address on the Emergency Calling screen, the configured emergency number is automatically filled in the FXS emergency number

Notes:

- OSB continues to support Regular Emergency calls and Emergency Gateways (PSTN) in all supported modes
- NG911 Emergency calls to SIP Service Providers through the OpenScape Branch SBC-Proxy / Branch SBC will not be supported on this 1st step.
- If an NG911 emergency call is done in survivable mode the call will be handled as a regular Emergency call and route the call to the configured Emergency Gateway (PSTN)
- OSB shall provide NG911 support in SM with FRN5498

30 CDR

OpenScape Branch supports Call Detail Records while running in Survivability mode. While running in Normal mode this is done by the OSV.

Note: CDR Allocated space

-400 MB small systems (<3550/Fujitsu).

-512MB for 3550/Fujitsu.

Configuration > OpenScape Branch > Branch Office > Configuration > Features > Enable Call Detail Records

Note: CDR uses the Contact information included in 200OK for storing FQDN or IP information for called party on Outgoing GW/SSP calls.

Call Detail Records

Select OK to temporarily store changes. Make your changes permanent by selecting 'Apply Changes' on the General page.

General

Billing File Settings

Maximum number of records: 100

Maximum time interval (min): 60

Maximum file size (K):

☐ Allow file overwrite

☒ E.164 translation

Matching digits	Translation
9011305	305
011305	305

Add **Delete**

SFTP Settings

Transfer method: Push

Port: 22

Note: CDRs will only be pushed to billing server if /cdr folder exists in billing server.

Allow File Overwrite: CDRs will be over written if CDR space fills up and push/pull method was not done.
Note: alarm will be created if CDR space runs low or CDRs can not be created.

E.164 Translation: If enabled, CDR tickets will generate the called number with modified digits that matches with the dialed number prefix.
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".

Max Number Of Records: max number of records per single billing file.
Max Time Interval: max time for billing file to close.
Max File Size: max size for billing size.
Transfer Method: Push method (send CDR files to billing server using "General & SFTP Billing File Settings"). Pull Mode (billing server gets CDR files. "General & SFTP settings" not used in this mode).
Port: port for push method.
Re Attempt Timer: wait time before re attempting another SFTP transfer in push mode.

Primary Billing Server

Hostname: 10.100.123.92

User name: root

Password:

Pri/Sec Billing Servers: IP address, User Name, and Password for billing servers. Settings are only used while in Push Transfer Method.






Secondary Billing Server

Hostname: 25.25.0.40

User name: root

Password:

30.1 CDR Record Details

FILENAME: /OSBIP169-20111108T090005+0500000004.bf  Name of CDR record
 DEVICE: OpenScape Branch  Device Type HOSTNAME: OSBIP169  Configured OSB Hostname
 FILETYPE: BILLING  CDR file
 VERSION: V7R0.02.00  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,,,,,10.234.1.70,10.234.1.101,20
 11-8-11 T08:58:01.0+0500,2011-08-11T08:58:04.0+0500,5256,200,OK,,0,0x010104 CLOSE: 2011-11-

08T09:00:05+0500  File Close Date

Field Number	From Example Above	Name/Description
1	0	Sequence Number: written CDR+1. ex. 1, 2, 3 ...etc
2	Std	CDR type (standard Or half-call releaserecord).
3	OSBIP169	Openbranch ID: Hostname of the Branch.
4	607b4e345ae75cd	SIP Call ID.
5	10	Call Duration in Seconds.
6	5558885226	Calling party number.
7	5558885256	Called party number
8	orig	Calling party identifier (orig, term, inc, outg, unknown)
9	term	Called party identifier (orig, term, inc, outg,unknown)
10		Transferring party number
11		Forwarding party number
12		MLHG member number
13		Location Identification Number
14	10.234.1.70	IP or FQDN Ingress side address
15	10.234.1.101	IP or FQDN Egress side address
16	2011-08-11T08:58:01.0+0500	Answer time UTC format Note: "time portion" of a timestamp is the localtime at the OSB. The addition or subtraction of the offset yields a final time calculated in UTC.
17	2011-08-11T08:58:04.0+0500	Release time UTC format Note: "time portion" of a timestamp is the localtime at the OSB. The addition or subtraction of the offset yields a final time calculated in UTC.
18	5256	Original Dialed Digits
19	200	SIP response Status Code 1xx, 2xx, 3xx, 4xx, 5xx,6xx
20	OK	SIP response Reason Phrase ex. OK, Busy here, etc
21		Codec Used(not Used)
22	0	Secure RTP Indicator (0,1)
23	0x010104	Integrated GW only. -> 0xaabbcc Where: aa - slot position - 01 bb - port - 01 cc - channel - 04

32.DNS

Handling of domain names using OpenScope Branch DNS Server can be done in three different ways: Slave, Forward and Master (Service only).

Configuration > OpenScope Branch > Branch Office > Configuration > Network/Net Services > DNS

The screenshot shows the 'Network/Net Services' configuration window with the 'DNS' tab selected. The 'Client' section is active. A yellow callout box explains the 'Refresh DNS' button: 'Refresh DNS: Allows user to manually refresh DNS client (Restarting the Service)'. Another yellow callout box explains the 'DNS Server List (configure)' field: 'Enter IP address of DNS servers (If OSB is acting as DNS client)'. The 'DNS server IP address' field contains '192.168.100.4'. A third yellow callout box explains the 'Alias' field: '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 OSB. -If phone is configured with DNS SRV record for "Gateway". Note: Missing alias configuration could cause calls towards OSB to be rejected with 403 loose routing reject and/or registrations toward OSB being rejected with 483.' The 'Alias' field contains 'pri50is2.unow.net5.cwb'.

32.1 Slave DNS

OSB as a Slave DNS gets its zone data using a zone transfer operation (typically from a master DNS) and it 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 screenshot shows the 'Network/Net Services' configuration window with the 'DNS' tab selected. The 'Server' section is active. A yellow callout box explains the 'Enable DNS server' checkbox: 'Flag To Enable/Disable DNS Server Functionality.' The 'Enable DNS server' checkbox is checked. The 'DNS configuration' button is visible. The 'Enable customization' checkbox is unchecked. The 'Administer custom files' button is visible. The 'OK' and 'Cancel' buttons are at the bottom right.

Enable OSEE v9 DNS zone splitting-
 Support of DNS zone splitting by configuring and using a key for retrieving the assigned DNS zone file. Disabled by default.

If reverse lookup is desired, then the reverse zone must be added as shown in the example.

IP masters/forwards: IP address of the Master DNS.

Type: must be configured as slave.
Zone Name must contain a valid name for the zone which has to be defined in the Master DNS.
 Note: zone names with underscores "_" are not allowed and are not RFC compliant.

File Name: valid name for the zone which has to be defined in the Master DNS (usually the same as the Zone name).

Note: Zone file will be used to store the zone information that DNS Server gets from master. Any request not found on slave will be forwarded if Forward IP list is configured.

Forward IP list: IP address of the DNS master which would be used to solve all FQDNs which are not covered by the configured slave zones.

Row	Type	Zone name	IP masters/forwards	File name
1	Slave			
2	Slave			
3	Slave			

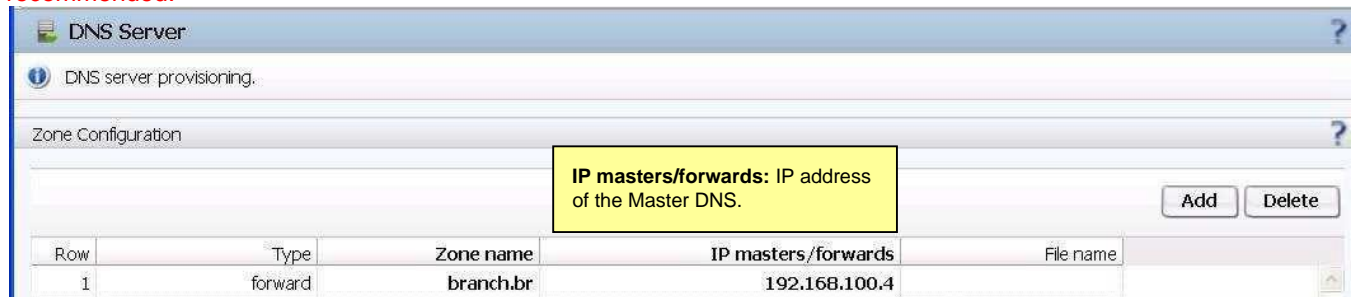
The master DNS for each zone allows slaves to refresh their zone record when the 'expire' parameter of the SOA Record is reached. The "expire" value should be longer than the longest time that you require the slave DNS server to function without contacting the master DNS server. Often the "refresh" value will be 30 minutes or so and the "expire" value will be 1 week.

Note: If Redundancy is active, system will use physical IP for DNS queries. So, for slave synchronization the physical IP of both Master and Slave OpenScape Branches must be added to DNS Server firewall list.

32.2 Forward DNS

OSB as a Forward DNS will forward requests to an external DNS server and caches the results.

Note: Forward DNS should only be used if Master DNS is trustable and reachable. Otherwise, slave configuration is recommended.



The screenshot shows the 'DNS Server' configuration window. The 'Zone Configuration' section contains a table with the following data:

Row	Type	Zone name	IP masters/forwards	File name
1	forward	branch.br	192.168.100.4	

Annotations in the image:

- A yellow box points to the 'IP masters/forwards' column header with the text: **IP masters/forwards:** IP address of the Master DNS.
- Buttons 'Add' and 'Delete' are visible to the right of the table.

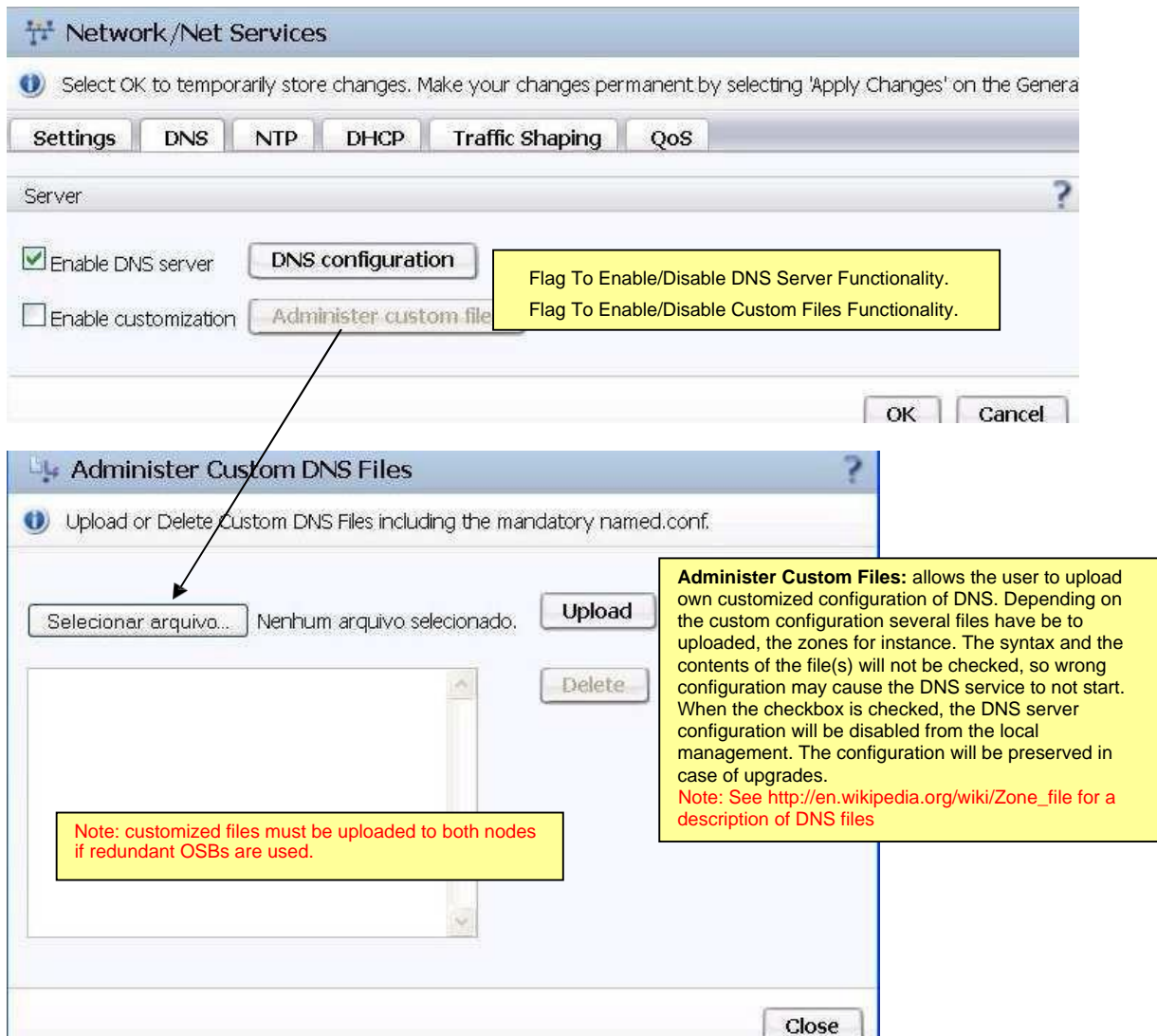
Type: must be configured as forward.

Zone Name must contain a valid name for the zone which has to be defined in the Master DNS.

32.3 Master DNS

OSB acts as Master DNS server. For this case, no DNS Master Server is configured. The flag DNS Server is activated and Custom DNS files can be uploaded. All zones have to be manually configured.

NOTE: Other DNS configuration is grayed out when customization is enabled.



33.DNS SRV

DNSSRV will be used when you need OpenScape Branch and phones to receive several addresses in order to have forwarding options in case of a failure of OpenScape Voice node or Network outages.

Note: For more information on configuring the DNS Server and the OSV Solution with DNS-SRV, please refer to the [OSV Test Configuration and Connectivity Solutions Manual](#) available inG-DMS.

For DNS-SRV it is necessary to create different SRV zones (domains) for OSV node 1, OSV node 2 (only for geographical separation between nodes) and one zone for each Branch (if you use only TCP, UDP and TLS) or two zones for each Branch if you use MTLS (one for TCP, UDP and TLS and one forMTLS).

Note: The priority of the proxy in the DNS server configuration has to be a lower number (higher priority) than the OSV. Configuration > OpenScape Branch > Configuration > System > Settings

The screenshot shows the 'System' settings page in the OpenScape Branch configuration interface. At the top, there is a blue header bar with the 'System' title and a sub-header with a warning icon and text: 'Select OK to temporarily store changes. Make your changes permanent by selecting 'Apply Changes' on the General page.' Below this are three tabs: 'Settings', 'Licenses', and 'Branding'. The 'Settings' tab is active, showing a 'General' section. In the 'General' section, there are fields for 'Branch Mode' (set to 'Proxy'), 'Hostname' (set to 'FUJITSU-S7-Evelyn'), and 'Domain name' (set to 'unify.com'). A yellow callout box with an arrow points to the 'Domain name' field, containing the text: 'Domain Name: Enter the DNS SRV zone for the Branch.' Below these fields is a checkbox labeled 'Gateway only' which is unchecked. Further down is a 'Country Configuration' section with a 'Country' dropdown menu set to 'United States / North America' and a 'Country configuration' button. At the bottom of the page is an 'Administration' section. A second yellow callout box with red text is positioned to the right of the 'Country Configuration' section, containing the text: 'Note: For correct DNS configuration see section above.'

Configuration OpenScape Branch Configuration VoIP SIP Server Settings

VOIP

Select OK to temporarily store changes. Make your changes permanent by selecting 'Apply Changes' on the General page.

Sip Server Settings

Port and Signaling Settings

Manipulation and Routing

Error Codes

Media

☐ Synch subscriber data
☐ Disable notification in survivable mode
☐ Enforce minimum Subscriber TransportType Security

Other trusted servers

Load Balance Mapping Table

Node 1

Target type

SRV Record

Primary server

Transport

TLS

Backup server

Transport

TCP

SRV record

branch.br

Transport

TCP

Node 2

Target type

SRV Record

Primary server

Transport

TLS

Port

Backup server

Transport

TCP

Port

SRV record

branch.br

Transport

TCP

Enter the SRV record for the OSV. It must be entered for both nodes in Geo-Separated Mode. Zone name cannot be the same for the 2 nodes. Note: port numbers are automatically taken from SRV response.

Note: User can check IPs were received correctly from DNS server in the main status page

103

P31003-H81A0-M101-18-76A9, 20/09/2023
OpenScope Branch V10, Configuration Guide

OpenStage/Optipoint :

- 4) Ports configured with 0 since port is taken from SRV response.
- 5) DNS SRV records are configured for Server, Registrar, and Gateway addresses.
- 6) Update Domain Name under phone Network Settings.

Registration	
SIP Addresses	
SIP server address	<input type="text" value="osvnode1.us"/>
SIP registrar address	<input type="text" value="osvnode1.us"/>
SIP gateway address	<input type="text" value="obranchnode1.us"/>

Port configuration	
SIP server	<input type="text" value="0"/>
SIP registrar	<input type="text" value="0"/>
SIP gateway	<input type="text" value="0"/>
SIP local	<input type="text" value="5060"/>
Backup proxy	<input type="text" value="0"/>
RTP base	<input type="text" value="5010"/>
Download server (default)	<input type="text" value="21"/>
LDAP server	<input type="text" value="389"/>
HTTP proxy	<input type="text" value="0"/>
LAN port speed	<input type="text" value="Automatic"/>
PC port speed	<input type="text" value="Automatic"/>
PC port mode	<input type="text" value="disabled"/>
PC port autoMDIX	<input type="checkbox"/>
<input type="button" value="Submit"/> <input type="button" value="Reset"/>	

SIP details:

SIP routing: <input type="text" value="Server"/>	
Registrar IP address or DNS name:	<input type="text" value="osvnode1.us"/>
Server IP address or DNS name:	<input type="text" value="osvnode1.us"/>
Gateway IP address or DNS name:	<input type="text" value="obranchnode1.us"/>
SIP port:	<input type="text" value="5060"/>
RTP Base port:	<input type="text" value="5004"/>

34. Multi Line Hunting Groups (MLHG)

Stand alone feature which operates in survivability mode with no relation with OpenScape Voice MLHG groups. In order to have a similar functionality while in Survivability Mode the user has to set MLHG parameters accordingly.

Note: feature is not available in Proxy ACDmode.

Configuration > OpenScape Branch > Branch Office > Configuration > Features > Multi-line Hunt Groups

Hunt Type: Linear: hunting will always be done in the same sequence according to the group members order. Cyclic: hunting will be done based on the last subscriber that answered the call and then the next one will be called. Parallel: all members will ring simultaneously. UCD: hunting similar to cyclic type 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.

Row	Enable	Pilot number	Pilot type	Hunt type	No answer advance timer (sec)	Overflow destination	Overflow timer
1	<input checked="" type="checkbox"/>		pilot	Cyclic	30		0

Pilot Number: defines the MLHG access code.

Pilot Type: 1) Pilot: must refer to an existent subscriber DN. The pilot DN will be the first group member.

2) Non pilot: can be any code and must not be related to an existent subscriber DN.

Members: The order of the members will be relevant according to the hunt strategy. Members are separated using a comma.

Note: It is required to use international number format for Pilot Numbers, Overflow Destination, and Members. External DNs can also be used as MLHG members.

No Answer Advance Timer: Period that each member will ring before the next member is called.

Overflow Destination: in case of none of members answer the call then the overflow is called. The overflow can be a subscriber, 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.

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)

34.1 Synchronization for OSB MLHG and Emergency Calling Subnets

It is possible to enable periodic synchronization of data between the OpenScape Branch Assistant and the OpenScape Branch servers for Multiline Hunt Group and Emergency Calling subnets.

Note: feature is not supported for peer OSBcluster.

Configuration > OpenScape Voice > Administration > General Settings > OSB Synchronization

The screenshot shows the 'OSVCLUSTERV7 - OSB synchronization' window. It contains the following elements:

- Header: [OSVCLUSTERV7] - OSB synchronization
- Info icon and text: Here you can set up the OSV Assistant to OSB Assistant synchronization.
- Section: Toggle synchronization and choose the time it will be executed on a daily basis
- Enable daily synchronization: ☒
- Perform synchronization at: 00 : 00
- Section: Choose Business Groups and Open Branches where OSV-OSB synchronization will be performed
- All Business Groups: ☒ Business Group: [text field]
- All Open Branches: ☒ Open Branch: [text field]
- Buttons: Perform synchronization now, Save, Cancel

Note: Daily synchronization can be enabled at specified time for Selected OpenScape Branch servers. When "enabled" the following data is sent from the OpenScape Branch Assistant to the OpenScape Branch servers:

- Multiline Hunt Group
- Emergency Calling subnets

Note: profile only MLHGs are not configurable for synchronization.

Configuration > OpenScape Branch > Administration > General Settings > OSB Synchronization

The screenshot shows the 'General Settings' window with the 'Synchronization' tab selected. It contains the following elements:

- Header: General Settings
- Info icon and text: Configure general settings
- Tabs: Installation, Synchronization
- Info icon and text: Due to the synchronization, services will be restarted. Active and ongoing calls may fail
- Section: Periodic synchronization
- Enable: ☒
- Start Date: 3/12/12 Time: 00 : 02
- Frequency: 24 (hours)
- Section: Trigger synchronization
- Info icon and text: Select branch office to synchronize now
- Branch Office: All
- Button: Synchronize
- Buttons: Save, Cancel

Note: Enable synchronization on the OpenScape Branch tab. It is possible to perform manual synchronization as well. **Note:** B2BUA service is restarted in OSB during synchronization.

35.OSB Redundancy

Redundancy uses a non-proprietary protocol which is used to increase the availability of the Branch. This is based on a virtual IP address in the same subnet of the OpenScope Branch used for redundancy. During switchovers, calls remain active if connected between Endpoints.

Note: Files changed manually (ex. /etc/hosts), customized DHCP/DNS files and CDRs are not synchronized between nodes. TLS related files (certificates, key files, CRL lists) and Passwords are synchronized. Other DB parameters (including Hostname) are synchronized and identical between nodes.

For OSB V2/V1R4: Passwords, files changed manually (ex. /etc/hosts), TLS Certificates, and CDRs are not synchronized between. Passwords must match between both nodes. Other DB parameters (including Hostname) are synchronized and identical between nodes.

Configuration > OpenScope Branch > Branch Office > Configuration > Network/Net Services > Settings

Enable Redundancy flag.
Note1: Phones will register to Redundant IP.
Note2: Enabling/disabling feature requires a system restart.
Note3: Same HW type and SW level must be used between nodes. Latency for one leg must not exceed 100 milliseconds. Round Trip Latency must not exceed 200 milliseconds.

☒ Enable redundancy ☒ Enable PRI/CAS redundancy Failed links threshold: 0 ☒ Switchover without Link Check

☒ Test Default Gateway instead of subscribers during failover

Interface	IP address	Backup IP address	Virtual IP Address
LAN	21.21.25.10	21.21.25.11	21.21.25.15

Virtual IP: virtual IP address for redundant System.
IP Address/Backup IP address: physical IP for each node.
Note: it is required to configure 3 OSV End Points for redundant system (1 for Redundant and 1 for each physical IP address of each node). 3 Branch offices must be added for configuration and maintenance.

Redundant OSB can be managed via the Virtual IP address; active node synchronizes the DB/XML to the standby node.

OK Cancel

Note: IPs for Master, Backup, Virtual must be on the same network.

Please note that when enabling the Redundancy and configuring IPs in OSB1, the database is copied in the second node if available so it would not be required to enable it on OSB2.

35.1 Upgrading Redundant System

User interaction is only on Master Node.

- 1.Go to Software Repository on Maintenance tab and upload image. tar and spa file
- 2.Go to OpenBranch Assistant tab and select Job Management
- 3.In the List of Jobs, select Add Job. Select as Action Transfer, the Target version (version previously uploaded in the Software Repository).
- 4.In the Start Time and Date field either select immediate or schedule the action for a specific time and date
- 5.From the List of nodes select the virtual node and press OK
- 6.Once Transfer action is Complete proceed with the Activation of the software. The user can either Add a new Job in the List of Jobs or clone the Transfer action and change the Action to Activation...Activation of the Software is started
- 7.Activation of software is Complete and Master node restarts.
- 8.Standby Node becomes Active temporarily.
- 9.Once running again, after about 5 minutes, previous Active Node becomes Master Node again and uploads SW image to Original Standby Node.
- 10.Upload/Upgrade completes, Standby Node restarts. Both Nodes are now upgraded.

Note: a few alarms will show during upgrade procedure since nodes will restart. Alarms should clear automatically when upgrade completes.

35.2 Disabling Redundant System

Following steps must be done to disable the feature:

1. Select the Master Node from Menu in the OpenBranch Assistant tab->Networkservices->Edit Interface.
2. Delete the entries for node 2, virtual node and change the IP Address Node 1 to a temporary IP.
3. Go to the Redundancy Tab and Disable Redundancy. Press OK and Apply changes

At this point system gets restarted. When the box comes up with the new temporary IP address, in order for the user to be able to administer the box, he will have to edit the corresponding Endpoint in the OSV (either change the IP of the Endpoint or create a new dummy one). The box now is a standalone box and Previously Backup node has now become Master.

4. Repeat the above steps for the Backup Node (which is now Master)

35.3 Master Status Check

Redundant or physical IP of first node can be used to check node status (Master Node in this case).
Configuration > OpenScape Branch > Branch Office > Configuration > Local Dashboard

Dashboard - BOCast1 - OBBocaIP40VRRP

Aggregated information and data for selected Branch Office.

System status

Operational status: normal Redundancy state: Master

Alarm summary Critical: 0 Major: 0

Buttons: Show active alarms...

Servers

Primary: 10.234.3.109 Active

Backup:

WAN outage:

Note: Synchronization of the operational mode/DB is done by a polling process (Every 5 minutes). So in case of switchover, the backup (new master) must send the NOTIFY's to all phones with the respective operational mode.

Note: If Redundant System is not available OSB Master will show an alarm. Alarms are reported using physical IP address of each node.

Active alarms - OBBocaIP40VRRP						
Information about current list of alarms.						
Alarm ID	Severity	Managed Resource	Alarm Type	Last Occurred	Acknowledged Status	User Hit Count
13512	Major	OBBocaIP40VRRP_10.234.1.40	[Communication][Loss of Communication with Redundant System]	2009/06/24 11:54:34	False	1

IMPORTANT Note: In an OSB redundant environment where OSB is in survivability mode, If OSB Master is down causing switching of master/slave-node, then:

RTP flow between the PSTN and the MLHG agent will stay up, but the SIP call will be lost.

All calls that were in queue (e.g. in ringing state) will be lost. Note that the backup OSB1000 does not know anything about these calls.

35.4 Backup Status Check

Physical IP address of second node can be used to check node status (Backup Node in this case).

Note: backup node only allows read access.

Configuration > OpenScope Branch > Branch Office > Configuration > Local Dashboard > Services Status (Show)

Services Status							
Current status of available services.							
B2BUA	not running	RTP Proxy	not running	SSM	not running	SNORT	running
VPN	not running	Interface4	not running	Syslog	running	Cron	running
Survivability Provider	not running	Interface3	not running	DBMS	running	NTP	running
M5 Converter	not running	DHCP	not running	Audit	running	SSH	running
M5 Adapter	not running	IPsec	not running	Process Manager	running	Web Server	running
DNS	not running	BLS	not running	SNMP	running	Redundancy	Active
SIP Server	not running			Interface1	running	CDR	stand-by
BLC	not running			Alarm Manager	running	Continuous Tracing	stand-by

Verify Redundancy service shows running

36. Phone Configuration for Proxy

Check outbound proxy flag

The screenshot displays the configuration interface for the OpenScape Branch V10, specifically the 'SIP interface' and 'Registration' sections. The interface is divided into 'Administrator Pages' and 'User Pages' tabs. The left sidebar lists various configuration categories: Admin Login, Applications, Bluetooth, Network, System, Features, File transfer, Local functions, Date and time, and Speech. The main content area shows the 'SIP interface' configuration, which includes fields for 'Outbound proxy' (checked), 'Default OBP domain', 'SIP transport' (set to TCP), and 'Response timer (ms)' (set to 32000). A yellow callout box highlights the 'SIP interface' section with the following text: 'Sip Server/Sip Registrar points to OSV SIPSM1 (Also If TLS is used) Sip Gateway Points to OSB Note: sipsm1 can be used with TLS for Proxy mode if sipsm3 is added in trusted IP list on OpenScape branch configuration.' Below the 'SIP interface' section, the 'Registration' section is visible, containing 'SIP Addresses' (SIP server address, SIP registrar address, SIP gateway address), 'SIP Session' (Session timer enabled, Session duration, Registration timer, Server type, Realm, User ID, Password), and 'SIP Survivability' (Backup registration allowed, Backup proxy address, Backup registration timer, Backup transport, Backup OBP flag). The 'Submit' and 'Reset' buttons are located at the bottom of the 'Registration' section.

Administrator Pages | **User Pages**

Admin Login
Applications
Bluetooth
Network
System
System Identity
SIP interface
Registration
SNMP
Features
Security
File transfer
Local functions
Date and time
Speech

SIP interface

Outbound proxy ☒
Default OBP domain
SIP transport
Response timer (ms)
Connect

Sip Server/Sip Registrar points to OSV
SIPSM1 (Also If TLS is used)
Sip Gateway Points to OSB
Note: sipsm1 can be used with TLS for Proxy mode if sipsm3 is added in trusted IP list on OpenScape branch configuration.

Administrator Pages | **User Pages**

Admin Login
Applications
Bluetooth
Network
System
System Identity
SIP interface
Registration
SNMP
Features
Security
File transfer
Local functions
Date and time
Speech
General information
Authentication
Ringer setting
Mobility
Diagnostics
Maintenance

Registration

SIP Addresses

SIP server address
SIP registrar address
SIP gateway address

SIP Session

Session timer enabled ☐
Session duration (seconds)
Registration timer (seconds)
Server type
Realm
User ID
Password

SIP Survivability

Backup registration allowed ☐
Backup proxy address
Backup registration timer (seconds)
Backup transport
Backup OBP flag ☐
Submit Reset

37. OSB Status information

It is possible to get OSB System Status, System Information, Registered Subscribers, Logs (See Logging Section), Service Status and Subscriber Data.

37.1 System Status (Checking if OSB is in SM or NM)

Connectivity and System state in relation to the SIP server as well as active alarms (See AlarmSection). GW only systems have specific status data. Configuration OpenScape Branch Branch Office Configuration Local Dashboard

Connectivity to the SIP server **"Normal"** indicates full connectivity to Primary/Backup server. **"Survivable"** indicates no connectivity to Primary/ Backup server. System is operating in limited mode. **"Transition"** system is in the process of switching mode.

Alarm Summary: shows counters for active alarms (more details under alarm section).

Note: No note added for this node

Only Applicable to Redundancy

Addresses/FQDN of SIP servers. Green / red Box associated indicates state of the server.
"Active" full connectivity with server.
"In Penalty Box" no connectivity with server.
"NotRunning" Survivability Provider not running. "OK" binding has lower Priority than active binding.

Note: The user can check IPs were received correctly from DNS server in the main status page.

System Info: CPU / Memory / Disk Usage, System Date / time, Up time, System Name, OS and HW type are available.

Alarm summary		System Info	
OpenScape Branch	Critical 0	CPU:	7.94%
	Minor 0	Memory:	20.24%
		Disk Usage:	18.15%
		Date/Time:	Monday, July 26, 2010 11:03:46 AM EDT
		System Uptime:	2 days 1 min
		Hostname:	OSB50I-BRI-169
		Operating System:	SUSE Linux 10.3 (i586)
		Hardware:	

Status	
Operational Status:	normal
Redundancy State:	Not active

Servers	
Primary:	10.234.3.50
Penalty Box state:	Active

Actions	
Rapidstat:	Start
Version:	Show
Services status:	Show
Log files:	Show

System Info	
CPU	2.92 % - 4 x 2667 MHz (10000 MHz Reserved in VM)
Memory	13.87 % - 4 Gb (4 Gb Reserved in VM)
Disk	17.2 % - 42 Gb
System uptime	25 min
Hardware type	Virtual OSB 1000
Hostname	VMOSB
Software Info	
Software version	V10 R3.01.01
Software Partition information	Active Backup

Note: Starting from V10R3.1.1, the VMWare reservation settings (CPU and Memory Reserved in VM) have been added in the System Info in Dashboard.

This information has also been added in the **vmsettings.txt** file which is in info.tar in rapidstat.

50i-DP24-StandAlone Mode

https://25.25.0.45/maintenance.html#

UNIFY 50i-DP24-StandAlone Mode Management Portal

User name: administrator | Help | Logout

50i-DP24-StandAlone Mode

Administration

System

Network/Net Services

VoIP

Port and Signaling Settings

Manipulation and Routing

Error Codes

Media

Features

Security

Diagnostics & logs

Alarms

Maintenance

General - 50iDP24SA

Branch aggregated information and data.

Alarms

Alarm summary: Critical: 1 Major: 0 Minor: 0 Show alarm details

System Status

Branch mode SBC-Proxy Auto refresh timer 30 seconds

Operational state Standalone

Services status Show Registered subscribers Show

Link Status Show Dynamic port mapping Show

Backup link status Show Subscriber data Show

Denial of Service Mitigation Show

System Info

CPU 43.61 %

Memory 24.27 % - 2 Gb

Disk 24.84 % - 8 Gb

System uptime 6 days 30 min

Hardware type Advantech 50i (2 PRIs/CAS E1 - FXS)

Hostname 50iDP24SA

Software Info

Software version V9 R0.06.00

Software Partition information Active Backup

Apply Changes Cancel Changes

37.2 Services Status

Window shows state of OpenScope Branch Services.

Note: some Services require configuration/activation in order to go into running state (ex. DNS, DHCP, etc). Other services only apply to SBC mode (Ex. RTP Proxy) and will always show not running in Proxymode.

Services Status			
Current status of available services.			
Alarm Manager	running	MS Converter	not running
Audit	running	Media Server	not running
B2BUA	running	NTP	not running
CDR	stand-by	Process Manager	running
Continuous Symptom Collector	not running	RTP Proxy	not running
Continuous Tracing	stand-by	Redundancy	stand-by
Cron	not running	SIP Server	running
DBMS	running	SNMP	running
DHCP	not running	SSH	running
DNS	not running	SSM	running
Eth0	running	Streaming Server	not running
Eth1	not running	Survivability Provider	running
IPsec	not running	Syslog	running
Kernel Console Collector	not running	VPN	not running
MS Adapter	not running	Web Server	running

37.3 Registered Subscribers

Window shows all devices registered to the OpenScope Branch. Configuration > OpenScope Branch > Branch Office > Configuration > Local Dashboard > Registered Subscribers

Registered Subscribers			
Registered Subscribers			
It is possible to filter by specific subscriber/contact.			
Search for: <input type="text"/> in: Username Search Show All			
Items/Page: 10 << 1 >> All: 497 CSV Export			
Username	Contact	Expires (seconds)	
552133594002	sip:552133594002@21.21.25.5:5060;transport=udp	49	
552133594003	sip:552133594003@21.21.25.5:5062;transport=udp	3054	
552133594004	sip:552133594004@21.21.25.5:5064;transport=udp	2823	
552133594005	sip:552133594005@21.21.25.5:5066;transport=udp	2128	
552133594006	sip:552133594006@21.21.25.5:5068;transport=udp	926	
552133594007	sip:552133594007@21.21.25.5:5070;transport=udp	1732	
552133594008	sip:552133594008@21.21.25.5:5072;transport=udp	2737	
552133594009	sip:552133594009@21.21.25.5:5074;transport=udp	903	
552133594011	sip:552133594011@21.21.25.5:5076;transport=udp	2245	
552133594012	sip:552133594012@21.21.25.5:5078;transport=udp	3064	

Username: Registered number/name.
Contact: IP address and transport Protocol.
Expires: Registration ExpirationTimer.

Note Keysets: support in Survivability Mode is limited to basic operations. No support for SUBSCRIBE/NOTIFY messages, in this case LEDs belonging to line appearances are not updated. Calls are forked to all registered contacts insurvivability. No configuration in Management Portal is needed. Keypset example: 5558885256 registered from 10.234.1.132 and 10.234.1.101 (two appearances)
Each Keypset line appearance counts as one subscriber in Registered Subscriber list. (Ex. 2 Devices with 2 line appearances, including primary line, will count as 4 subscribers in Registered Subscriber list).

38. Alarms

38.1 Alarm Configuration

OSB allows user to activate/deactivate/configure alarm thresholds as well as check alarm status/History.
Configuration > OpenScape Branch > Branch Office > Configuration > Alarms > Alarm Settings

Alarms

Select OK to temporarily store changes. Make your changes permanent by selecting 'Apply Changes' on the General page.

Alarm SettingsSNMP Configuration

Row	Group ID	Event ID	Group name	Event name	Active	Threshold	Trigger	Severity	Flow timer	Reporting class	Faulty object	Event type
1	1	1	Hardware	High temperature core 0	<input checked="" type="checkbox"/>	70	Greater than	Critical	0	1	HW-Sensors	Equipment
2	1	2	Hardware	High temperature	<input checked="" type="checkbox"/>	70	Greater than	Critical	0	1	HW-Sensors	Equipment
3	1	6										
4	1	7										
5	1	8										
6	1	9										
7	1	23										
8	1	24										
9	1	25										
10	1	26										
11	1	27										
12	1	28										
13	1	60										
14	1	61	Hardware	Card 2 failure	<input checked="" type="checkbox"/>	0	Greater than	Major	0	1	HW-Sensors	Equipment

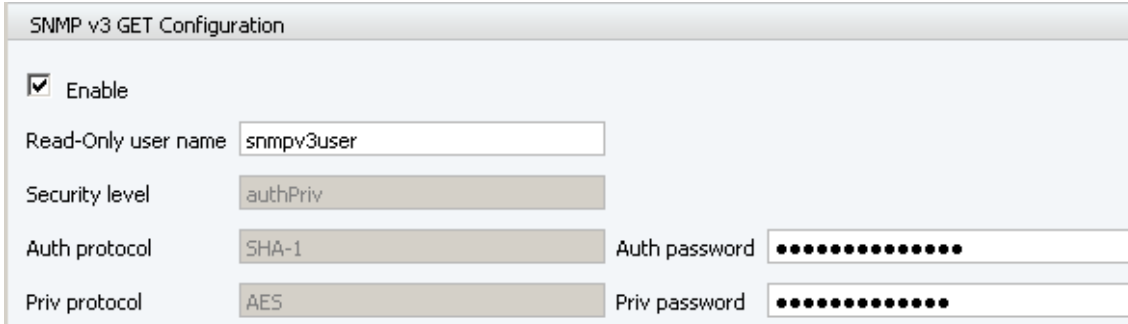
When configuring flow timer as 0, then alarm traps to clear an alarm are reported every time. If configured as 60, then same alarm trap to clear alarm is repeated only after timer expires.

1- **GroupID** and **EventId** correspond to the SNMP trap OID (last 2 numbers of the OID).
2- **GroupName** name of the GroupID. It groups together system status information of similar kind.
3- **EventName** character string that describes the alarm. Closely related to the trap name as defined in the OSB SNMP MIB.
4- **Active** determines if the alarm will be generated or not.
5- **Threshold** value that needs to be checked by monitor for an alarm to be generated.
6- **Trigger** shows the condition where the alarm will be generated. Trigger is a comparison with alarm value.
7- **Severity** alarm severity assigned to that particular alarm (warning, minor, major, critical). The Severity is fixed per Fault-Id.
8- **Flow Timer** indicates the minimal time to wait before generating a next occurrence of the same alarm.
9- **ReportingClass** 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.
10- **FaultyObject** character string that defines the object that is at fault.
11- **Event Type** classifies alarms into: communications, environmental, equipment, processingError, and qualityOfService.

38.2 SNMP V3 GET Configuration

Local GUI Alarms SNMP Configuration SNMP v3 GET Configuration

The Management portal of OSB allows the configuration of snmp v3 gets of linux default MIB.



The image shows a configuration window titled "SNMP v3 GET Configuration". It contains several settings:

- Enable:** A checkbox that is checked.
- Read-Only user name:** A text field containing "snmpv3user".
- Security level:** A dropdown menu showing "authPriv".
- Auth protocol:** A dropdown menu showing "SHA-1".
- Auth password:** A text field with masked characters (dots).
- Priv protocol:** A dropdown menu showing "AES".
- Priv password:** A text field with masked characters (dots).

SNMP v3 GET Configuration:

Enabled: checkbox for enable/disable the snmp v3 gets of linux default MIB. 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).

Priv protocol: Default value: AES (hardcoded - grayed out).

Auth password: min: 8 characters & max: 32 characters. Default value: snmpv3authPass

Priv password: min: 8 characters & max: 32 characters. Default value: snmpv3encPass.

38.3 Trap Destinations

Configuration > OpenScape Branch > Branch Office > Configuration > Alarms > SNMP Configuration

Alarms can be routed to a remote device using SNMP v2c or SNMP v3.

To allow SNMP manager discovery, SNMP v2c read-only community name and SNMP v2c read-only IP have to be configured. Note: if read-only community name is configured in the SNMP v2c trap destinations table for an IP, general configuration will not be used for that IP.

Alarm Settings **SNMP Configuration**

General ?

SNMP v2c Read-Only Community Name SNMP v2c Read-Only IP

SNMP v2c Trap Destinations ?

Add Delete

Row	IP address	Port	Trap community name	Blocked	Reporting class set	Type	Read-Only community name
1	10.200.0.50	162	public	<input type="checkbox"/>	1;2;3;4;5;6;7	alarm	
2	10.200.0.51	162	public	<input type="checkbox"/>	1;2;5;6;7	alarm	test789
3	10.200.0.51	169	public	<input type="checkbox"/>	7	alarm	
4	10.200.0.52	162	public	<input type="checkbox"/>	7	alarm	
5	10.200.0.53	162	public	<input type="checkbox"/>	1;2;3;4;5;6;7	alarm	0123test

For SNMP v2c trap destination table:
IP address: Defines the IP used where trap is sent.
Port: Internal port used to send the trap.
Trap community name: Community name of the trap.
Blocked: Trap will not be sent (if checked).
Reporting class set: list of Alarm Reporting Classes that will be reported via SNMP trap.
The values must be separated using semi-colons.
Example: When setting this field to "1;2;5;6;7" the alarms with 1, 2, 5, 6 and 7 Reporting Classes will be reported. **Note: MIBs are located in OSB /usr/share/snmp/mibs**
Read-only community name: (when configured) replaces general read-only community name.

Note: up to 5 trap destinations can be configured.

SNMP v3 EngineId Configuration ?

Current SNMP Engine ID

☒ Generate from IP address

☐ Generate from MAC address

☐ Text entry (max 27 chars)

☐ Hex string entry (max 27 bytes)

Engine ID: Unique identifier of a SNMP v3 engine.
It can be generated via IP address, MAC address...
or...
It can be configured via a text entry or hex string.

Important: It is NOT possible to configure the same IP and port for trap destination in both SNMP v2c and SNMP v3 destination tables!!!

SNMP v3 Trap Destinations ?

Add Delete

Row	IP address	Port	Security name	Security level	Auth protocol	Auth password	Priv protocol	Priv password	Blocked	Reporting class set	Type
1	10.200.0.50	162	OSFM	authPriv	sha1	aes	<input type="checkbox"/>	1;2;3;4;5;6;7	alarm
2	10.200.0.51	162	OSFM	authPriv	sha1	aes	<input type="checkbox"/>	1;2;3;4;5;6;7	alarm
3	10.200.0.52	162	OSFM	none					<input type="checkbox"/>	1;2;3;4;5;6	alarm
4	10.200.0.52	165	OSFM	auth	md5			<input type="checkbox"/>	7	alarm
5	10.200.0.53	162	OSFM	auth	sha1			<input type="checkbox"/>	7	alarm

Note: up to 5 trap destinations can be configured.

For SNMP v3 trap destination table.

IP address: Defines the IP used where trap is sent.

Port: Internal port used to send the trap.

Security name: SNMP v3 security name.

Security level: authPriv (traps sent with authentication and privacy), auth (traps sent with authentication only), none.

Auth protocol: Authentication protocol (md5 or sha1).

Auth password: Authentication password.

Priv protocol: Privacy/Encryption protocol (des or aes).

Priv password: Privacy/Encryption password.

Blocked: Trap will not be sent (if checked).

Reporting class set: list of Alarm Reporting Classes that will be reported via SNMP TRAP.

38.4 Alarm Status/History

It is possible to check the status of alarms to see if any are active. User can also go back and check on alarm History to see alarms that occurred and cleared automatically.

Maintenance > Inventory > Nodes > Branch Office

The screenshot shows the 'Alarm summary' section at the top, displaying counts for Critical (0), Major (1), and Minor (0) alarms. A 'Show Active Alarms' button is visible. Below this is the 'Status' section, which includes details like 'Operational Status: normal', 'Redundancy State: Not active', and 'Penalty Box state: Active'. A yellow callout box explains that the 'Alarm Summary' shows the number of active Critical, Major, and Minor Alarms, and that the number of active alarms increases or decreases automatically as alarms are cleared. Below the status section is the 'Active alarms - OSB50i-169' window. A yellow callout box states that details about active alarms are displayed in this window, and users can see details for each alarm or close the window. At the bottom, a table lists the active alarms.

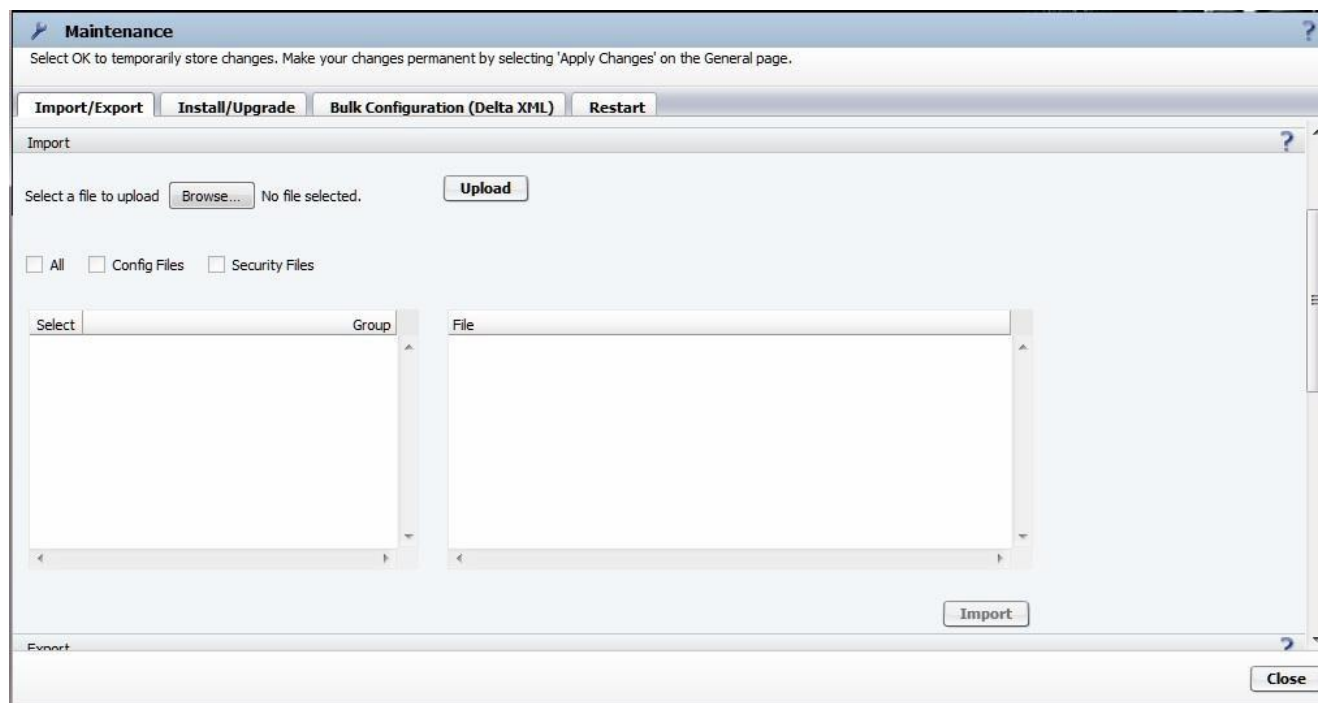
Alarm ID	Severity	Managed Resource	Alarm Type	Last Occurred	Acknowledged Status	User	Hit Count
13310	Major	OSB50i-169_10.234.1.169	[Resource][CDR disk space running low]	2010/07/26 11:41:55	false		1

38. Backup/Restore and XML Configurations

User can change system configuration by loading, importing or exporting xml configuration files.

Note: configuration done from CLI (ex. /etc/hosts, Manual DNS config, etc) will have to be backed up manually as it is not part of the XML.

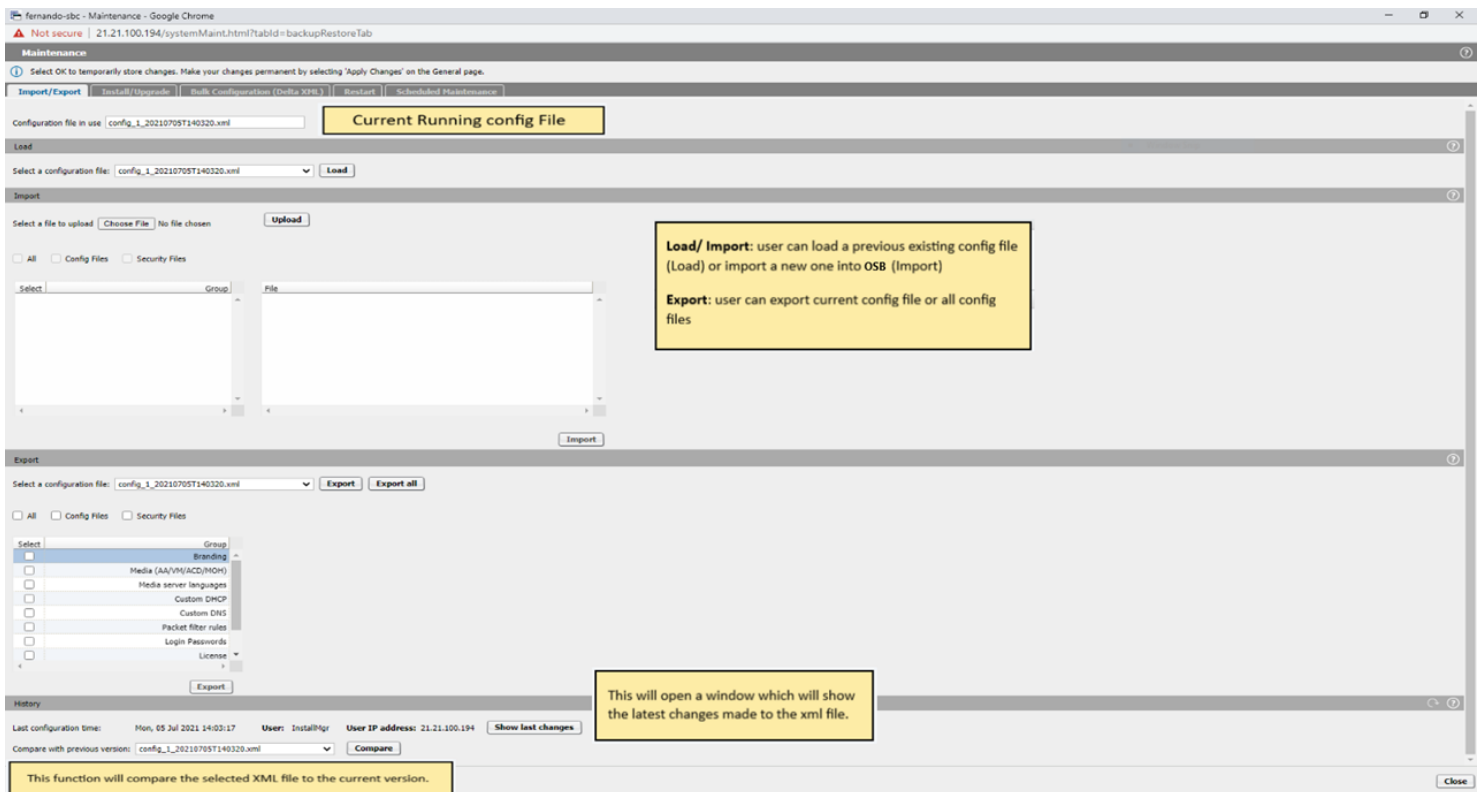
- Configuration > OpenScape Branch > Branch Office > Maintenance > Import/Export



Note: The maximum number of .xml configuration files a system can store at the same time is reduced. When the user tries to save 25 files or more, all except the newest 10 will be compressed on a .tar.gz.

38.1 Load Config (DB XML File)

Read, store, and apply xml config files settings.



- 1) In the **Load** field, select a configuration file from the drop down menu and press **Load**.

A new configuration file is loaded. Changes are applied permanently by selecting **Apply Changes** on the General page.

Note: after applying changes the loaded config file will be incremented by 1 (e.g. **Config_1_.xml** is configured as **Config_2_.xml**).

38.2 Import Config (DB XML File)

Import Config (DB XML File) prompts user for a valid xml config file. The file is imported as the newest xml config file and a version number is displayed.

- 1) In the **Import** field, select **Choose file** and browse for the file you want to upload on a new window.

A new configuration file is loaded. Changes are applied permanently by selecting **Apply Changes** on the General page.

Note: after applying changes the loaded config file will be incremented by 1. (e.g. **Config_1_.xml** is configured as

Config_2_.xml).

38.3 Export Config (DB XML File)

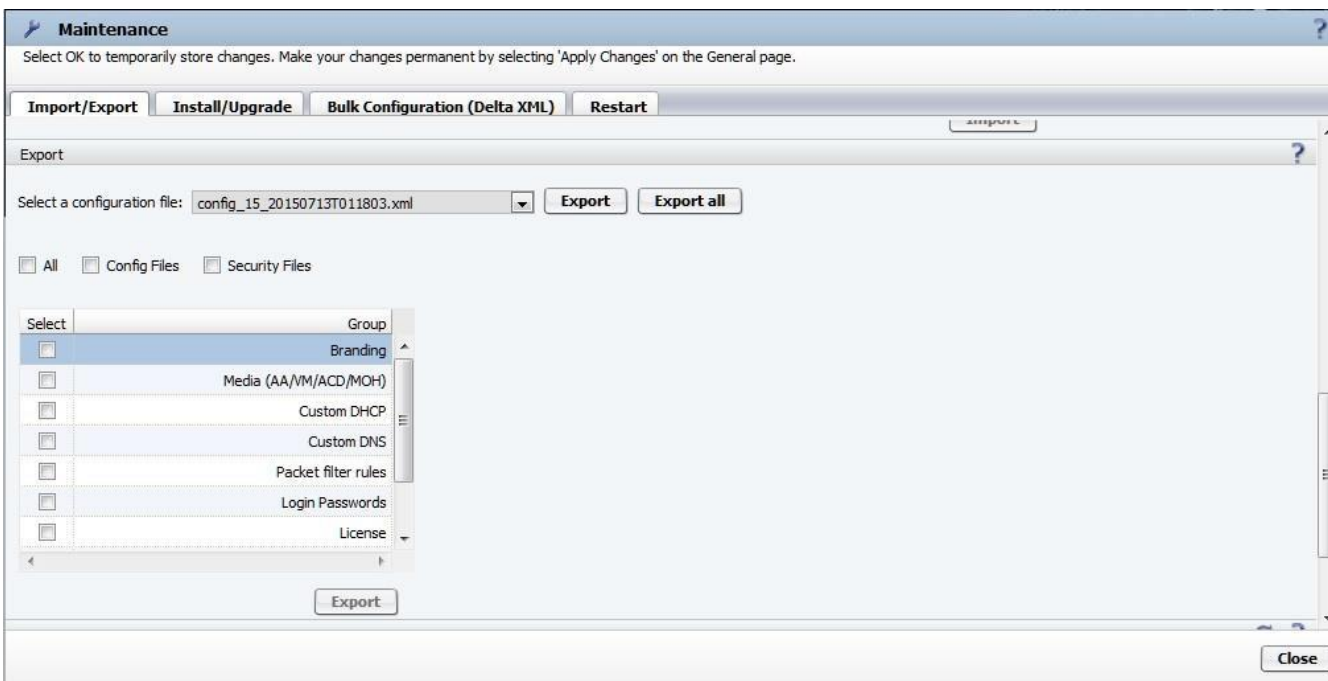
The **Export** button shows two options: **Save** or **Open** the selected xml config file.

- 3) Select a configuration file to export and **Save** or **Open** file. By default the latest config file is selected.

Note: The maximum number of .xml configuration files a system can store at the same time is reduced. When the user tries to save 25 files or more, all except the newest 10 will be compressed on a .tar.gz.

38.4 Backup/Restore of custom configuration files

38.4.1 Export



The available file groups are listed in the scroll box. Select groups to export by selecting the checkboxes aside the group name. Any number of groups can be selected and exported.

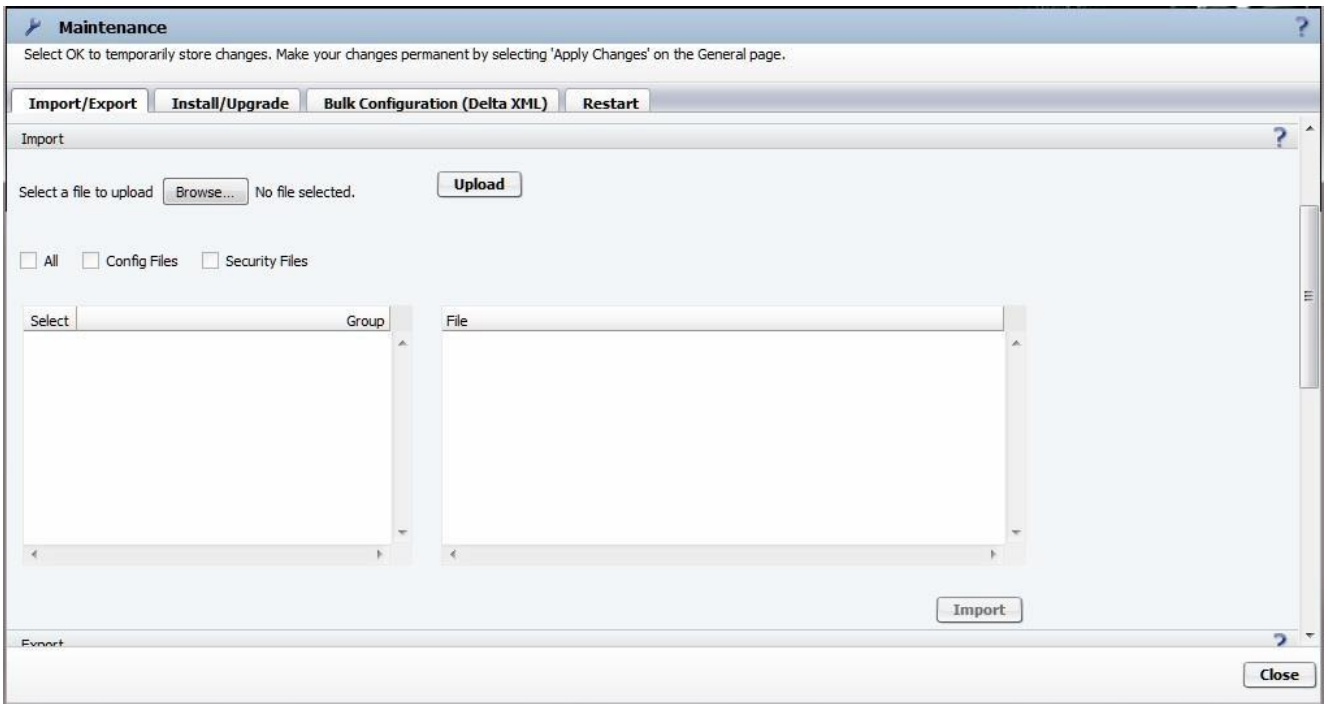
Shortcut checkboxes can be accessed just above the scroll box. There it is possible to select **All** groups, **Config Files** (XML group) or **Security Files** (Security certificates and keys group).



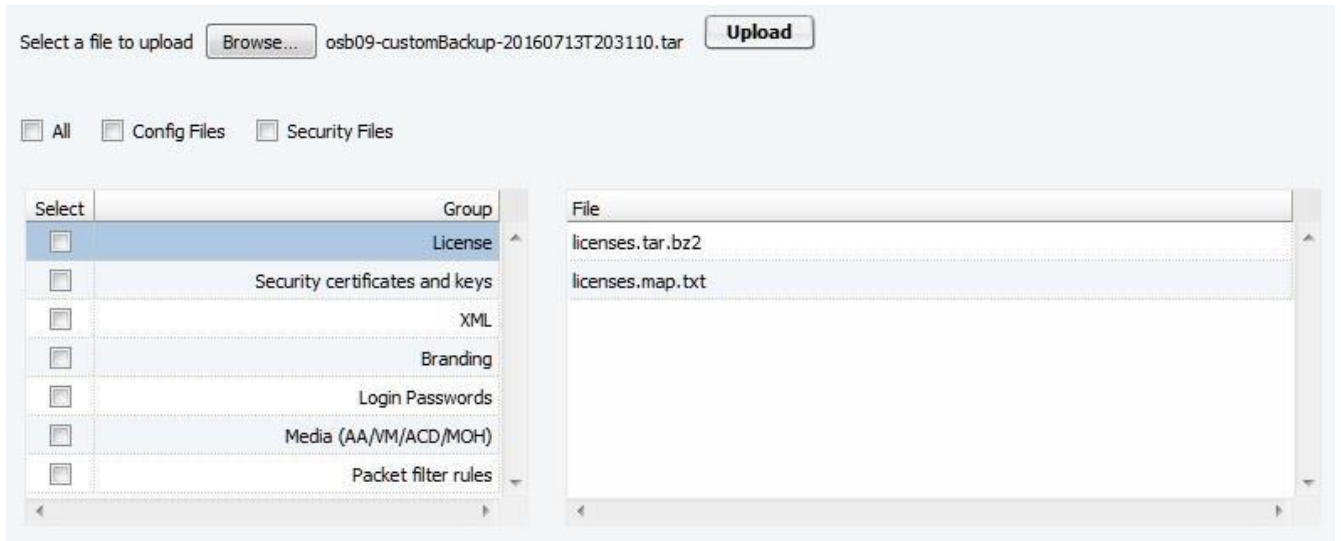
A password will be required when selecting **All**, **Security Files** or **Security certificates and keys**. This password is used to encrypt the sensitive data and will be required only when importing those files.

Press **Export** just below the scroll area to save a tar file with all the files related to the selected groups. The tar file is named <hostname>-customBackup-<date>.tar.

38.4.2 Import



Select the tar file by pressing the **Upload** button. If the file is valid, the left scroll area is populated with the non empty group directories. The right scroll area shows the contents of the currently selected group.



Select groups to import by selecting the checkboxes aside the group name. Any number of groups can be selected and imported.



As in the export section, a password will be required when selecting **All**, **Security Files** or **Security certificates and keys**. This password is used to decrypt the sensitive data and is required to import those files.

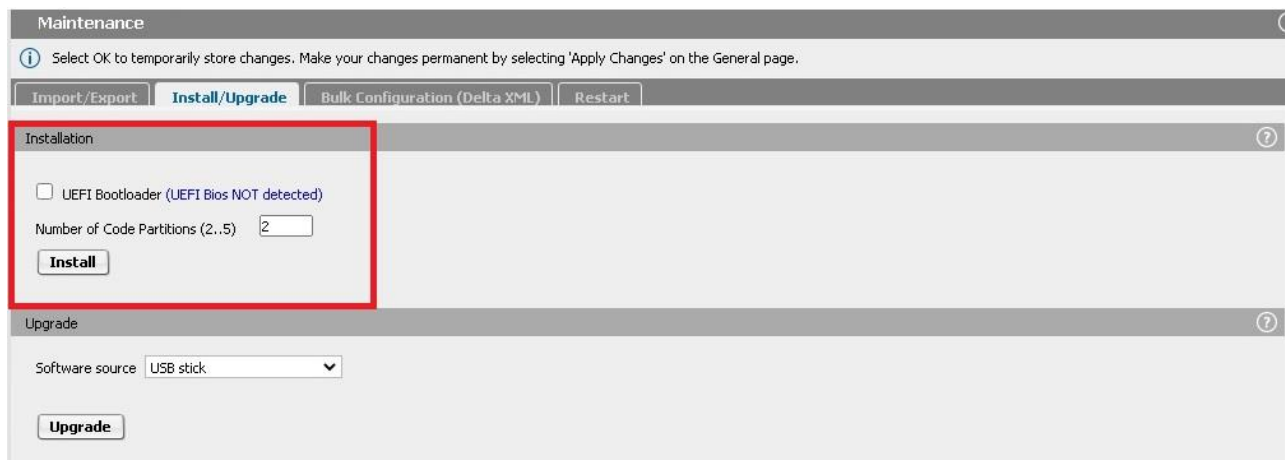
Depending on which groups are selected, pressing **Apply Changes** may be required to complete the import process.

Error messages may appear at the end of import operation. Details about the error may be found on "Web Server" log.

39. How to install / upgrade a file

Install / Upgrade Tab under Maintenance allows you to start the OSB software installation or upgrade.

Install



The **Install** option is available only the first time you perform the full installation.

Installation erases both backup and active partitions and overwrites the existent software version in USB. The database can be preserved if previously stored in USB stick.

Starting from V10R2, the **UEFI bootloader flag** is available in the installation option. “**UEFI Bios detected**” or “**UEFI Bios NOT detected**” message is also shown, depending on the boot mode configured in the server.

For Legacy Mode, this flag should be deactivated and for UEFI Mode this flag should be activated.

The UEFI bootloader flag could be also activated in the USBsticksetup.

Please, attention to choose this option. The System Boot Mode must be configured correctly, otherwise the Server will not boot from the Hard Drive.

INFO: For virtual machines, it is recommended to use Legacy Mode, then this flag should be not used.

INFO:

Using physical hardware, this option is available only if the USB stick is plugged and the system is booting from the USB stick. For virtual machines, this option is also available in full installation.

- **Partitioning**



By default, the system disk has 2 partitions:

1. Partition “A” is used to hold one copy of the uncompressed OpenScape Branch software.
2. 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 performing the first upgrade after the initial installation, the new software is stored on the “B” partition and the boot loader is modified, so that the “B” partition is designated as holding the “active” file system which is loaded into RAM whenever the OpenScape Branch 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.

In case the previous upgrade is successful, a subsequent upgrade replaces the software on the “A” partition and the bootloader is 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 becomes the backup software.

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

- **More partitions**

During the full installation it is possible to request the creation of more code partitions. You can create until 5 partitions, **and this number is only limited by the size of the used disk**. For instance, it is possible to select 5, but the system permits only 4 partitions. The explanation about the partitions “A” and “B” are still valid, but now they will rotate over an extra number of partitions:

After a full installation

- **Partition 0 => “Active”**
- **Partition 1 => “Backup” of “Active”**
- Partition 2 => “empty”
- Partition 3 => “empty”

An upgrade will use the next “empty” or “avail” partition in numeric order. In this case the “Partition 2” is selected and the result is:

- **Partition 0 => “Backup” of “Active”**
- Partition 1 => “Backup” of “Partition 0”
- **Partition 2 => “Active”**
- Partition 3 => “empty”

As shown, the partition 2 becomes the new “Active” partition and the Partition 0 is the new “Backup” of “Active” partition. If a new upgrade is done, then the result is:

- Partition 0 => “Backup” of “Partition 2”
- Partition 1 => “Backup” of “Partition 0”
- **Partition 2 => “Backup” of “Active”**
- **Partition 3 => “Active”**

As shown, the partition 3 becomes the new “Active” partition and the Partition 2 is the new “Backup” of “Active” partition. In case a new upgrade takes place, then the result is:

- **Partition 0 => “Active”**
- Partition 1 => “Valid software but it is not backup of any partition”
- Partition 2 => “Backup” of “Partition 3”
- **Partition 3 => “Backup” of “Active”**

The process continues as described. An administrator can change the “Active” partition to any valid software partition and its backup partition is automatically selected if it is still available. This is done at code partitions under the restart tab.

Code partitions					
Name	Version	State	Status	Unblock all	Refresh
P0	bcf-10.09.00.00-91	ready		Block/Unblock	Restart from P0
P1	bcf-10.09.00.00-92	ready		Block/Unblock	Restart from P1
P2	bcf-10.09.00.00-94	ready	backup	Block/Unblock	Restart from P2
P3	bcf-10.09.02.00-80	ready	next-boot,running	Block/Unblock	Restart from P3

Note: An Administrator can block any partition to avoid an upgrade over it. This is a way to keep a running and know version to be used at any moment.

Note: Database files are related to a version. In case of a fallback to an older version it is possible that the last configurations will be not used. These configurations can be redone if the old version allows them.

Upgrade

Upgrade option includes the fields shown in the image below:

Maintenance

Select OK to temporarily store changes. Make your changes permanent by selecting 'Apply Changes' on the General page.

Import/Export **Install/Upgrade** **Bulk Configuration (Delta XML)** **Restart** **Scheduled Maintenance**

Upgrade

Software source: **USB stick** (selected)
Local file
SFTP
HTTPS

Upgrade

New Code Activation

Partition	Version
New code not found	Unknown

☐ Reboot only when all calls are disconnected

Time to wait for all calls be disconnected (between 1 to 72 hours)

Activate now

Activate at date: **+1 Day** **+1 Hour** **Now**

Activation / Restart Information

Running: To partition: **Activation/Restart cancel**

Waiting calls by: Number of calls:

Time left:

Scheduled upgrade at: Will wait calls by: **Schedule cancel**

Close

- **Upgrade** field

The Upgrade means that a full version is installed in an available partition and the active partition is preserved in case of failure or to return to an older version.

The upgrade and activation of the new software are separated actions. The activation can be performed at a specific date or right after the upgrade. Until a reboot operation takes place, the system informs that a new software is available at each login.

When performing an upgrade, by any means other than **USB stick**, make sure the IP address of the sending device is in the "white list" of the Message Rate control function. Navigate to Local GUI > Security > Message Rate Control.

It is recommended to use the **Local File** option when possible by getting the image onto a local computer or network. This could prevent problems related with the timeout of the file transfer caused by long propagation delays.

Upgrade full version is installed on the backup partition and the active partition is preserved in case of failure.

Prerequisites

Software image *.tar file is required for all upgrade's types. Tar files contains 3 files:

- image*.ob
- image*.key
- image*.sig.

Note: Upgrade process is interrupted if Web Page is Closed during the copy / sftp of the software. DB is not modified during Upgrades.

Upgrade is possible via the following four ways:

1. USB stick

The version stored in the USB stick is used.

- a) Select **USB Stick** from Menu.
- b) Click **Upgrade**.
- c) When the upgrade process is completed, remove USB and confirm restart.

Note: in case of a redundant system both nodes are upgraded. Master first then backup.

2. Local file

The user chooses which local file to upload, depending on the version desired.

The screenshot shows the 'Maintenance' section of a web interface, specifically the 'Install/Upgrade' tab. At the top, there is a message: 'Select OK to temporarily store changes. Make your changes permanent by selecting 'Apply Changes' on the General page.' Below this, there are five tabs: 'Import/Export', 'Install/Upgrade' (which is active), 'Bulk Configuration (Delta XML)', 'Restart', and 'Scheduled Maintenance'. The 'Upgrade' section contains a 'Software source' dropdown menu set to 'Local file'. Below this, there is a 'File' section with a 'Choose File' button and the text 'No file chosen'. Underneath, a list of files is shown with the entry 'C:\image_osb-10.02.00.00-2.tar' and a 'Remove' button next to it. At the bottom of the section is an 'Upgrade' button.

- a) Browse to select the "tar" file to be used for the update.
- b) Click **Upgrade**.
- c) When files are copied confirm restart.

Note: In case of a redundant system both nodes are upgraded. Master node first and after that the backup node.

3. HTTPS

The screenshot shows the 'Maintenance' section of a configuration interface. At the top, there is a header 'Maintenance' and a message: 'Select OK to temporarily store changes. Make your changes permanent by selecting 'Apply Changes' on the General page.' Below this is a navigation bar with buttons: 'Import/Export', 'Install/Upgrade' (highlighted), 'Bulk Configuration (Delta XML)', 'Restart', and 'Scheduled Maintenance'. The main area is titled 'Upgrade' and contains the following fields: 'Software source' (dropdown menu set to 'HTTPS'), 'Hostname' (text box with '10.80.0.20'), 'Remote directory' (text box with '\sbc'), a 'List Versions' button, 'Software version' (dropdown menu set to 'osb-10.02.00.00-2'), and an 'Upgrade' button.

- Provide the hostname (IP address) and remote directory of a https server which contains the software image.
- Add the *.tar and *.spa files in this directory. The file named "**list**" must be added in the same directory. This file should contain the name related to the software image, e.g. image_osb-10.02.00.00-2.tar.
- Click **List Versions** and select the available software version to upgrade.

4. SFTP

The screenshot shows the 'Maintenance' section of a configuration interface. At the top, there is a header 'Maintenance' and a message: 'Select OK to temporarily store changes. Make your changes permanent by selecting 'Apply Changes' on the General page.' Below this is a navigation bar with buttons: 'Import/Export', 'Install/Upgrade' (highlighted), 'Bulk Configuration (Delta XML)', 'Restart', and 'Scheduled Maintenance'. The main area is titled 'Upgrade' and contains the following fields: 'Software source' (dropdown menu set to 'SFTP'), 'Hostname' (text box with '21.21.100.1'), 'Port' (text box with '22'), 'Remote directory' (text box with '/root/upgrade'), 'User name' (text box with 'root'), 'Password' (text box with masked characters '*****'), a 'List Versions' button, 'Software version' (dropdown menu set to 'osb-10.02.00.00-2'), and an 'Upgrade' button.

- Provide the hostname (IP address), port and remote directory of SFTP server which contains the software image.
- Supply a username and password to login to the server.
- Add the *.tar file in this remote directory. The file named “**list**” must be added in the same directory. This file should contain the name related to the software image, e.g. image_osb-10.02.00.00-2.tar.
- Click **List Versions** and select the available software version to upgrade.

- **New code activation** field

New Code Activation

Partition	Version
P1	P1 - osb-10.02.00.00-2

☐ Reboot only when all calls are disconnected
Time to wait for all calls be disconnected (between 1 to 72 hours)

Activate now

Activate at date

10/20/2021

04:04 PM

+1 Day

+1 Hour

Now

Activation / Restart Information

Running:

NO

To partition:

ACTIVE

Activation/Restart cancel

Waiting calls by:

disabled

Number of calls:

0 / 0

Time left:

0 days 00h00m

Scheduled upgrade at:

Will wait calls by:

disabled

Schedule cancel

Blocking Calls Information

Blocking State:

NO

Cancel wait for backup upgrade

After the upgrade process, the new code must be activated. The activation can be requested using **Activate now** option or **Activate at date**. In case you select **Activate at date**, it is necessary to schedule a specific day and time.

It is also possible to request the system to wait for running calls before reboot to activate the new code.

For redundant system, when the flag **Reboot only when all calls are disconnected** is selected and upgrade is activated, the calls will be blocked until the end of upgrade process in both nodes (master and backup). The option for **Time to wait for all calls to be disconnected** is from 1 to 72 hours and the default value is 24 hours.

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 all the upgrade/activation is completed. In case of redundant systems this also includes the upgrade of the backup node. If the calls rejected by this process cannot be diverted to other servers, they will be lost. In this case, the administrator is responsible to redirect the traffic to another OSB.

By activating the upgrade, a warning message is displayed indicating the upgrade.

- **Activation / Restart Information** field

This area shows if a reboot process is running. If the process is not in final steps, it is possible to cancel it using the buttons **Activation / Restart cancel** and **Schedule cancel**.

It is also possible to request the system to wait for running calls before reboot to a partition. The use of the option to wait calls will also reject new calls. If the calls rejected by this process cannot be diverted to other servers, they will be lost.

Note: This information is also available on the restart tab.

5. Blocking Calls information

Maintenance

Select OK to temporarily store changes. Make your changes permanent by selecting 'Apply Changes' on the General page.

Import/Export Install/Upgrade Bulk Configuration (Delta XML) Restart Scheduled Maintenance

Upgrade

Software source: Local file

File: Choose File No file chosen

Files: C:\fakepath\image_osb-10.02.00.00-2.tar Remove

Upgrade

New Code Activation

Partition	Version
P2	osb-10.02.00.00-2

☒ Reboot only when all calls are disconnected

Time to wait for all calls be disconnected (between 1 to 72 hours) 24

Activate now

Activate at date: 12/06/2021 11:35 PM +1 Day +1 Hour Now

Activation / Restart Information

Running: NO To partition: ACTIVE Activation/Restart cancel

Waiting calls by: disabled Number of calls: 0 / 0

Time left: 0 days 00h00m

Scheduled upgrade at: Will wait calls by: disabled Schedule cancel

Blocking Calls Information

Blocking State: NO Cancel wait for backup upgrade

For redundant system, when the flag **Reboot only when all calls are disconnected** is selected and upgrade is activated, the calls will be blocked until the end of upgrade process in both nodes (master and backup). When activating the upgrade, a warning message is displayed.

Maintenance

Select OK to temporarily store changes. Make your changes permanent by selecting 'Apply Changes' on the General page.

Import/Export Install/Upgrade Bulk Configuration

Upgrade

Software source: Local file

File: Choose File No file chosen

Files: C:\fakepath\image_osb-10.02.00.00-2.tar Remove

Upgrade

New Code Activation

Partition	Version
P2	osb-11

☒ Reboot only when all calls are disconnected

Time to wait for all calls be disconnected (between 1 to 72 hours) 24

Activate now

Activate at date: 12/06/2021 11:35 PM +1 Day +1 Hour Now

Activation / Restart Information

Running: NO To partition: ACTIVE Activation/Restart cancel

Waiting calls by: disabled Number of calls: 0 / 0

Time left: 0 days 00h00m

Scheduled upgrade at: Will wait calls by: disabled Schedule cancel

Blocking Calls Information

Blocking State: NO Cancel wait for backup upgrade

21.21.142.144 says

Do you want to reboot the system and activate the software now?

WARNING!!!! - It could wait for active calls be disconnected by 24 hour(s)

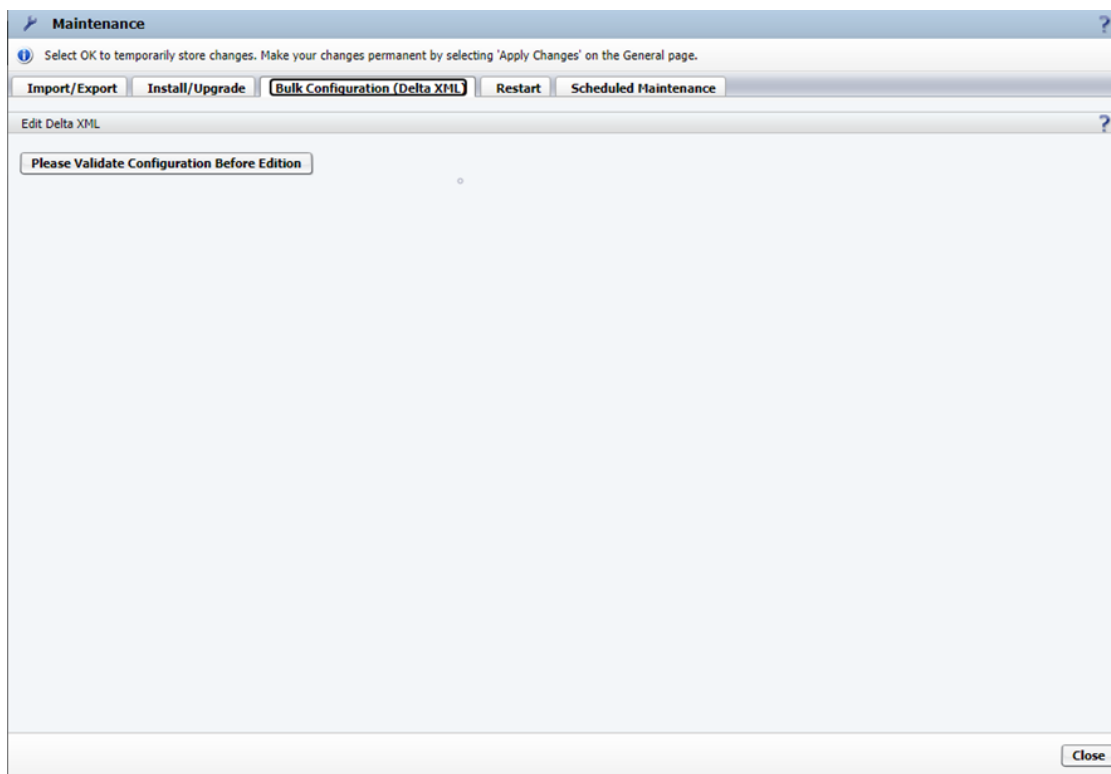
All new calls will be refused.

WARNING!!!! The calls will be blocked until the upgrade of backup node be finished.

OK Cancel

During this period, 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 has 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 "pmc block" command.

39.1 How to configure Bulk Configuration (Delta XML)



Prior to the creation of a Delta XML file, it is necessary to change all the data to be included. In the following example the NTP client (NTP tab) is disabled and new entries have been added to "DNS server IP address" and "Alias" (DNS tab).

Note: Do not **Apply Changes**. Changes are detected by differing the not applied changes with the last saved config xml file.

After the changes, navigate to **Configuration > OpenScape Branch > Branch Office > Maintenance > Bulk Configuration**.

Validate the changes that have not been applied by clicking **Please Validate Configuration Before Edition**. Once the validation takes place, the edition area is presented.

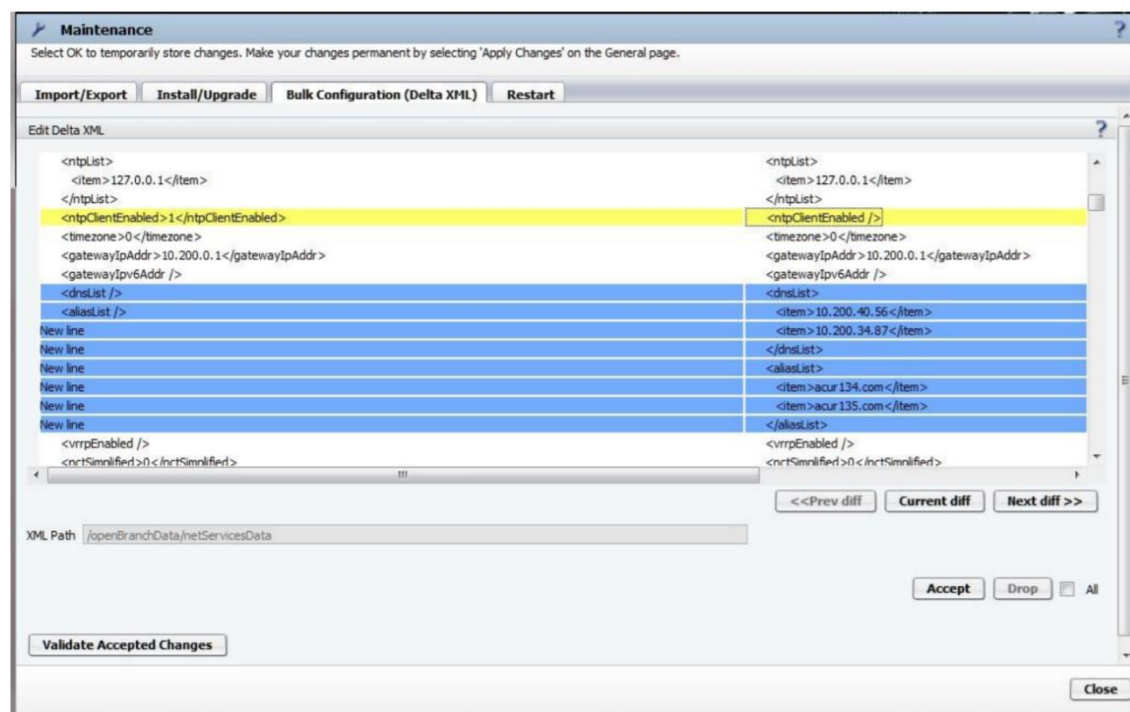
Note: Changes done on configuration after this step are detected only when reloading the "Bulk Configuration (Delta XML)" tab.

Now it is possible to navigate through the individual changes. Use the buttons **Prev diff** and **Next diff** to jump from one diff to the previous or next ones. **Current diff** focuses the diff area on the current selected change.

XML Path indicates, on the xml structure, the position of the currently selected change.

All operations are done over the currently selected change (visually observed as surrounded by a dotted frame).

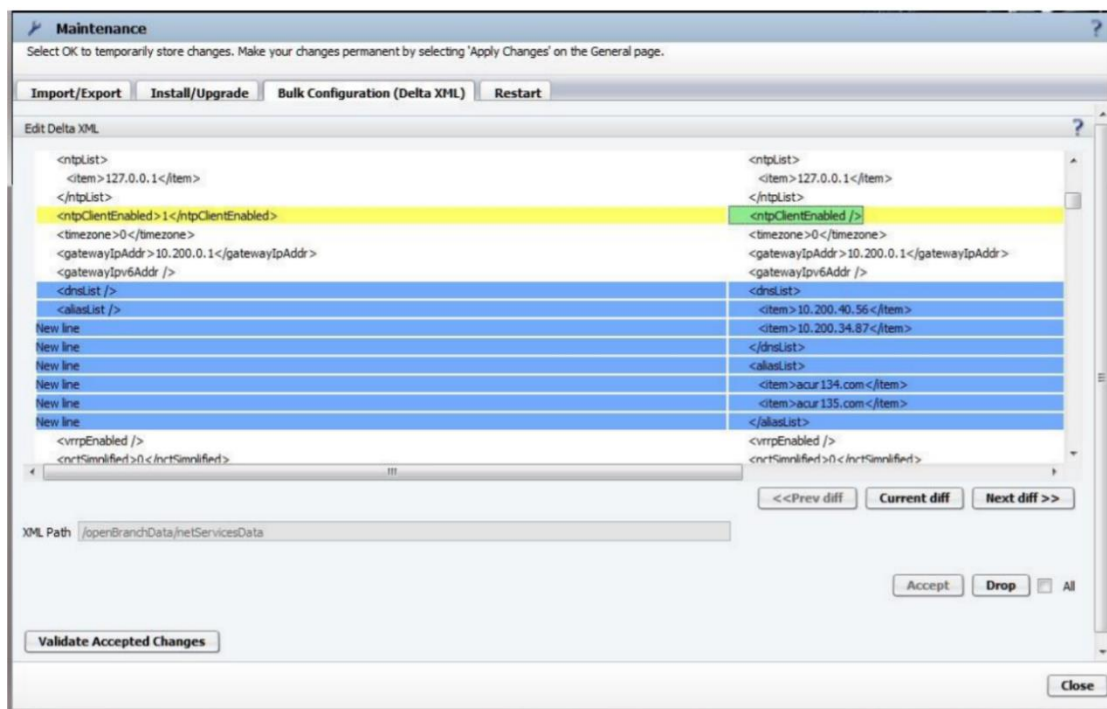
Note: In normal configuration task this feature can be used to have a preview of modifications on xml before the **Apply Changes**.



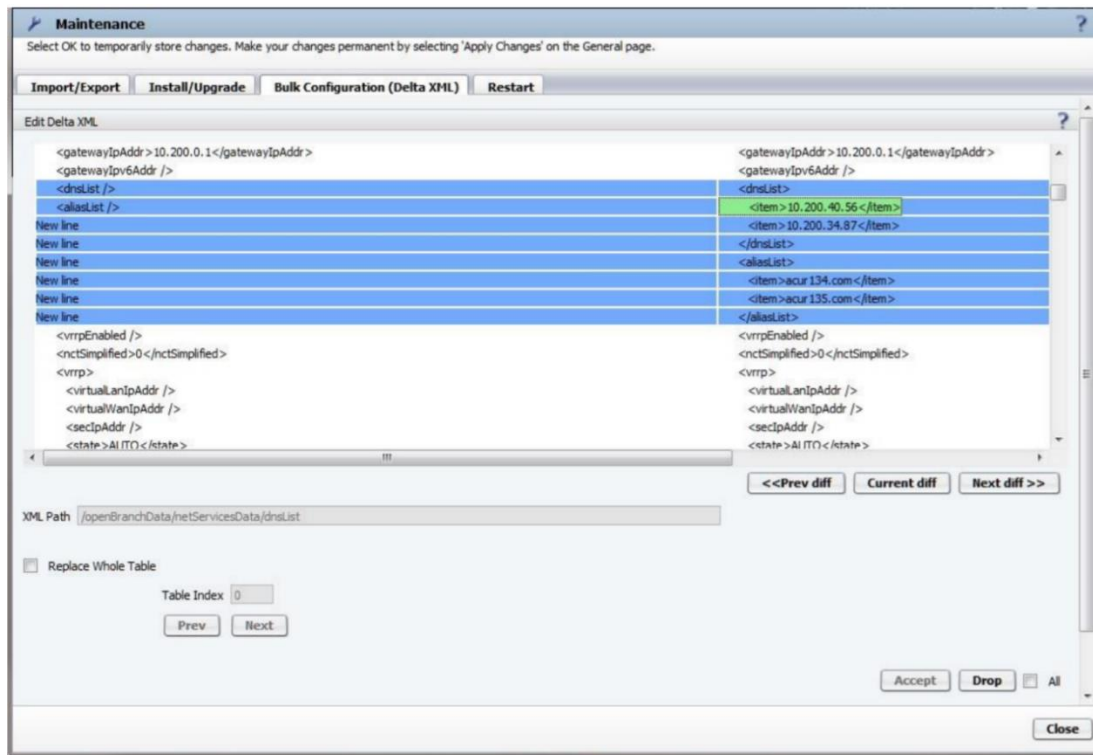
Only "accepted" changes are included on Delta XML files. It is possible to include/exclude changes on Delta XML file individually or in groups ("item" elements (lists or tables)).

Accept and **Drop** acts over currently selected change (checkbox **All** unchecked).

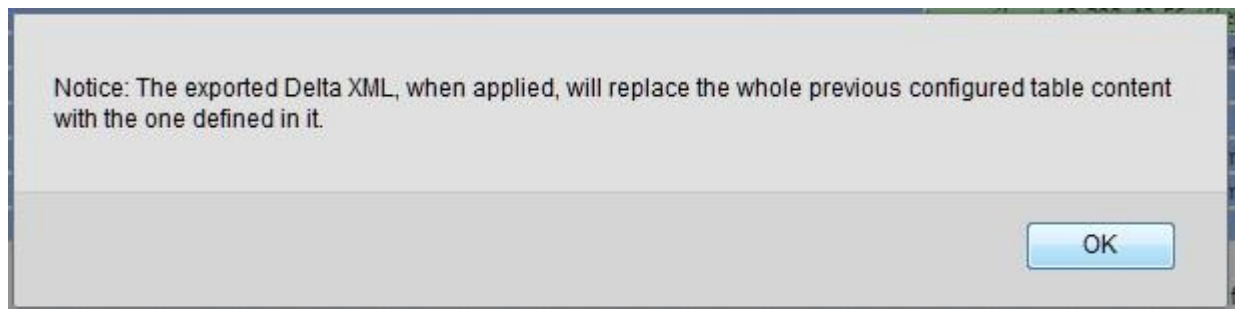
Accepted changes are marked with a green background. Dropping an accepted change returns its background to the original color. Original background colors are the same ones used on the **Compare** on **Import / Export** tab.



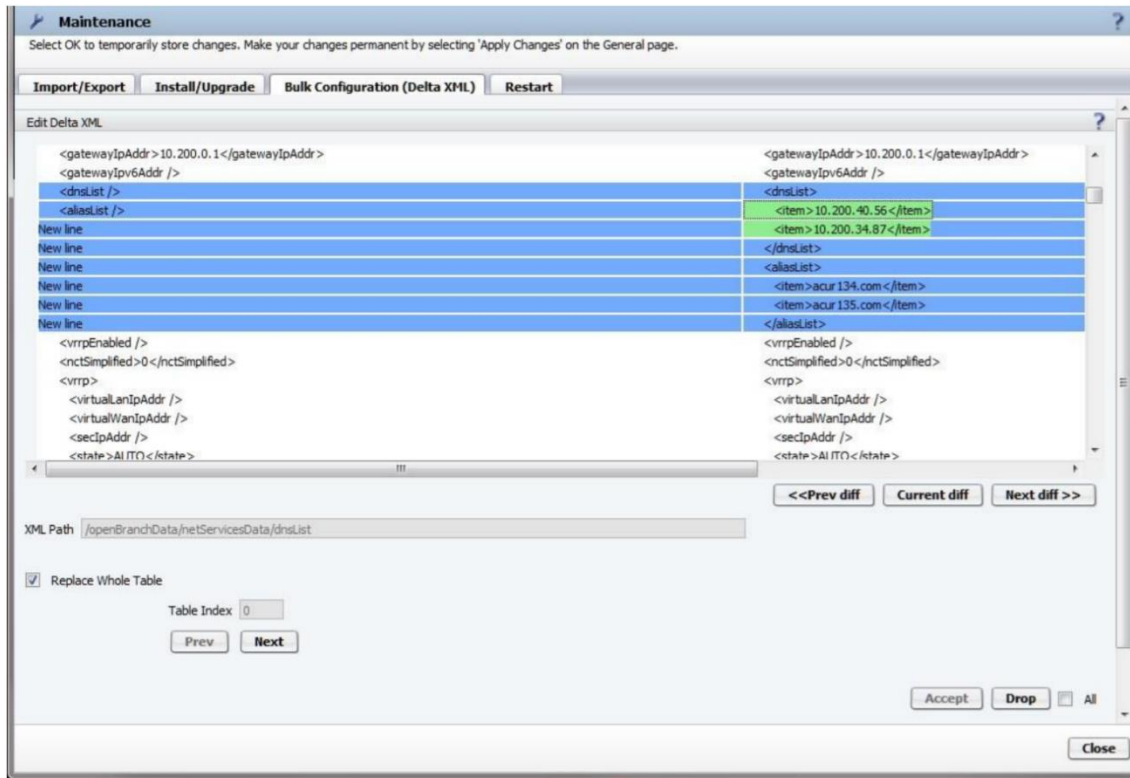
For lists and tables ("item" elements) there are additional operations shown at the left area below the "XML Path".



This Notice is presented the first time **Replace Whole Table** is checked:



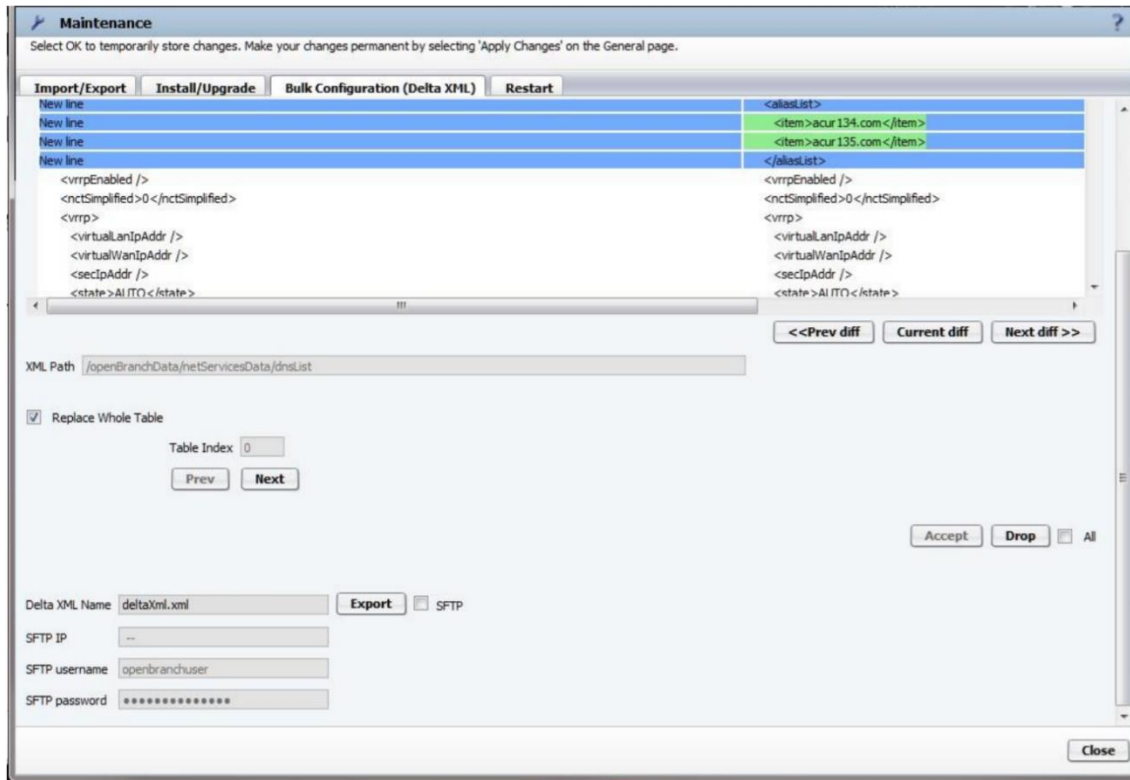
If the **Replace Whole Table** is checked, all "item" elements in the same level are colored in green. The exported Delta XML, when applied, replaces the whole previous configured table content by the one in green. **Table Index** informs the position of the "item" element (starts with 0). **Prev** and **Next** navigates inside the table selecting "item" elements individually. **Accept/Drop** applies to them.



The following is presented when **All** is checked for the first time. When checked the **Accept / Drop** acts over all the changes. Be aware that unpredictable results may occur when exporting the Delta XML file.



After all desired changes are accepted, press **Validate Accepted Changes**. Export area is presented.



Delta XML file can be exported through the browser or SFTP.

If local GUI is accessed through CMP, changing "Delta XML Name" is not possible. CMP demands deltaXml.xml as the name of the Delta XML file. Any other name is ignored.

All xml tags inside the following xml tags are ignored for the purpose of generating Delta XML file:

- alarmList
- saveUser
- saveRUser
- saveTime
- clientIpAddr
- swVersion
- hwType
- product
- hostname
- logicalBranchOfficeId
- hwId
- saveCounter
- openBranchNetwork
- mode
- voipData.

40.How to Restart

Restart Tab under Maintenance includes the following areas:

Maintenance

Select OK to temporarily store changes. Make your changes permanent by selecting 'Apply Changes' on the General page.

Import/Export Install/Upgrade Bulk Configuration (Delta XML) **Restart** Scheduled Maintenance

Restart Restart from backup File system repair

☐ Reboot only when all calls are disconnected

Time to wait for all calls be disconnected (between 1 to 72 hours)

Minimal number of calls

Code partitions

Name	Version	State	Status	Unblock all	Refresh
P0	P0 - osb-10.02.01.00-1	ready	next-boot,running	Block/Unblock	Restart from P0
P1	P1 - osb-10.02.00.00-2	ready	new	Block/Unblock	Restart from P1
P2	P2 - osb-10.02.01.00-1	ready		Block/Unblock	Restart from P2
P3	P3 - osb-10.02.01.00-1	ready	backup	Block/Unblock	Restart from P3

Activation / Restart Information

Running: To partition: Activation/Restart cancel

Waiting calls by: Number of calls:

Time left:

Scheduled upgrade at: Will wait calls by: Schedule cancel

- **Restart** button

This button is used to reboot the system and use the active partition.

The user is prompted to confirm the system's restart.

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

Note: When the node that is restarted is acting as Master the other node might take over the Master function.

- **Restart from backup** button

This button is used to reboot the system and use the software stored in backup partition of the current partition. If the backup partition is not available (code was removed or overwritten), this button is disabled.

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

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

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

- **File system repair** button

This button calls the check and repair tool for all Branch disks. All problems found are automatically fixed.

Note: This option is only available if the USB stick is plugged and the system is booting from the USB stick.

- **Code partitions** field

The available code partitions are listed in a table with buttons to control them.

The State column will inform the states:

- Blocked – the partition cannot be used by an upgrade process.
- Ready – the partition is available for an upgrade and has a valid software.
- Empty - the partition is avail but has no valid software.

The Status column will inform the status:

- Next-boot – the partition that runs in case of restart.
- Running – Is the partition currently being executed.
- Backup – this is the backup partition of the running partition.
- New – this partition is changed by an upgrade (it will keep this status until it is validated, checked against problems).

The buttons **Block / Unblock** and **Unblock all** are used to block the partitions against upgrades. It does not block the partition that is selected to run. Using the buttons **Restart from X**, all valid partitions can be selected to run.

Read more about the behavior of partitions in Partitioning under [How to Install / Upgrade a file](#).

- **Activation / Restart information** field

This area shows if a reboot process is running. If the process has not been completed yet, it is possible to cancel it using the buttons **Activation / Restart** cancel and **Schedule Cancel**.

Note: This information is also available on the install / upgrade tab.

It is also possible to request the system to wait for running calls before reboot to a partition. The use of the option to wait calls also rejects new calls. If the calls rejected by this process cannot be diverted to other servers, they get lost.

40.1 How to configure Scheduled Maintenance

This section shows the server Scheduled Maintenance state. The server can enter in a maintenance state either by a user or by internal conditions. The user can decide to put a server in maintenance at a specific time or immediately.

Note: The server can enter in maintenance state even before the date and time defined if the server thinks that is the right decision.

Maintenance mode in OSB is a way to set the OSB call processing in an out of service state, so the traffic can be handled by another server, without shutting down the server. In that way, the upgrade and configuration functionalities can still be done.

When in a maintenance state, a server does not accept any calls and must be ready for administration procedures like updates and configurations. In case of a scheduled Maintenance administrators are responsible to redirect traffic to another OSB (in case the topology of the network does not support rerouting automatically) during maintenance window. After this new implementation there is the possibility of scheduling automatically the maintenance mode only when there are no active calls in the system.

Additionally, in case of scheduled Maintenance mode if flag **In Maintenance only after all calls are disconnected** is set, active calls are not affected at any way before **Time to wait for all calls be disconnected (between 1 to 72 hours)** is reached. Ongoing calls can be monitored in the Management Portal in Diagnostics & Logs Menu and in Statistics Tab.

All new calls are rejected until Maintenance mode is activated. Statistics work in maintenance mode and ongoing calls can be monitored in the Management Portal in Diagnostics & Logs Menu and in Statistics Tab.

Maintenance

Select OK to temporarily store changes. Make your changes permanent by selecting 'Apply Changes' on the General page.

Import/Export Install/Upgrade Bulk Configuration (Delta XML) Restart Scheduled Maintenance

Maintenance Schedule Options

Maintenance State: In service (auto)

System in maintenance: Auto Apply

Current Date/Time: 03/19/2021 10:59 AM

Start Date/Time: 03/19/2021 01:05 AM +1 Day +1 Hour Now

End Date/Time: 03/19/2021 01:05 AM +1 Day +1 Hour Now

☐ In Maintenance only after all calls are disconnected

Time to wait for all calls be disconnected (between 1 to 72 hours) 24

Response Codes sent when in Maintenance, Upgrading or Restarting

Response Code/Message for Core Side: 503 easyobinstall reboot

Response Code/Message for Access Side: 503 easyobinstall reboot

Close

The following fields are available:

- **Maintenance Schedule Options** field

Maintenance State: It is the current state of the server and the text inside the () describes how the server enters in this state.

Select what type of maintenance state will be applied when the button **Apply** button is pressed.

Available options:

- **Auto:** When the server enters in maintenance by itself (normally associated with software or hardware problems).
The Auto mode only uses the server software decisions to control if the server is in maintenance.

- **Now:** When requested by a user's administrator.
The Now option will force the server to enter in maintenance immediately.

- **Schedule:** When requested by an administrator using a define date and time period.
The Schedule option uses the time in the boxes below to select when the server will enter in maintenance.

- **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 starting the maintenance.

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 all the maintenance is completed. In case of redundant systems this also includes the maintenance of the backup node. If the calls rejected by this process cannot be diverted to other servers, they will be lost.

- **Response Codes sent when in Maintenance, Upgrading or Restarting field**

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.

41 Creating Delta XML

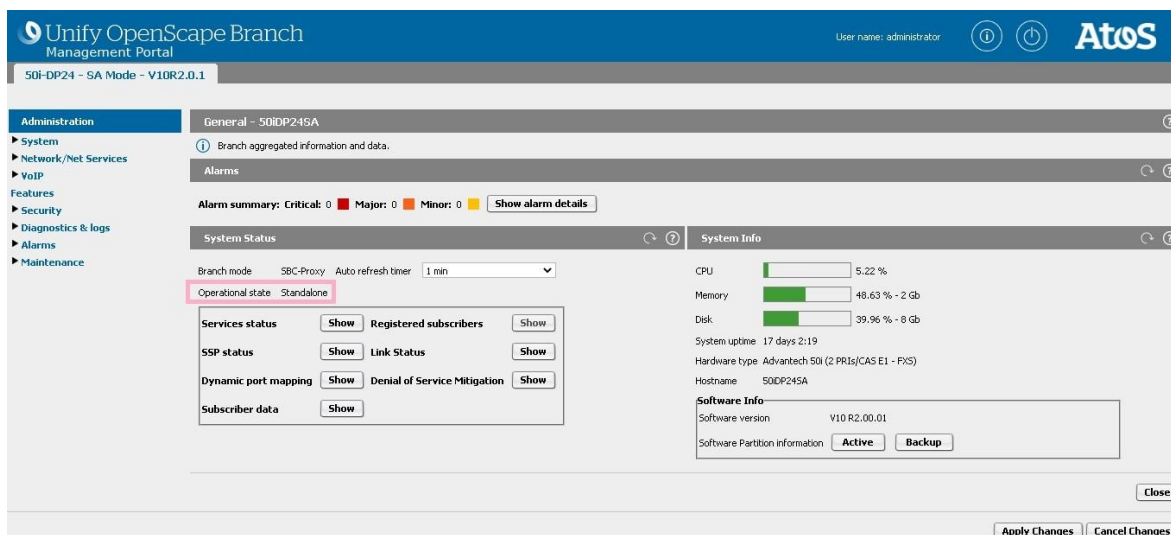
Prior to the creation of Delta XML file it is necessary to change all data to be included.

Please refer to the **OpenScape Branch V9 Admin Guide**, section 3.2.3.2 ["How to Create a New Batch Job"](#)

In the following example the NTP client (NTP tab) is disabled and new entries have been added to "DNS server IP address" and "Alias" (DNS tab).

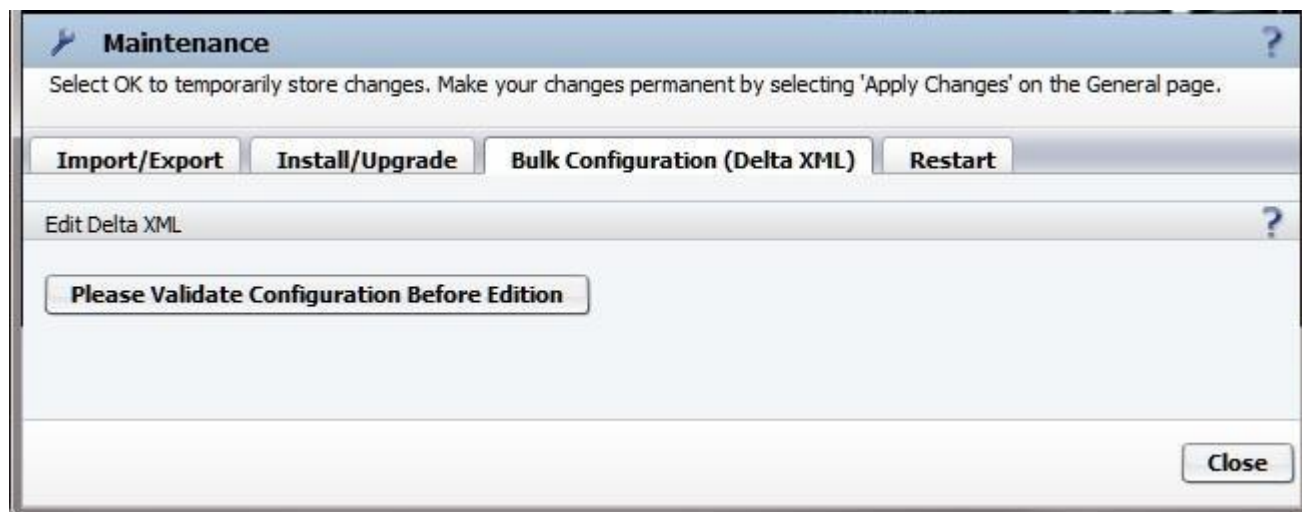
Note: Do not **Apply Changes**. Changes are detected by differing the not applied changes with the last saved config xml file.

After the changes, navigate to **Configuration > OpenScape Branch > Branch Office > Maintenance > Bulk Configuration**



Validate the changes that have not been applied by clicking the "**Please Validate Configuration Before Edition**". Once the validation takes place, the edition area will be presented.

Note: Changes done on configuration after this step will only be detected when reloading the "Bulk Configuration (Delta XML)" tab.



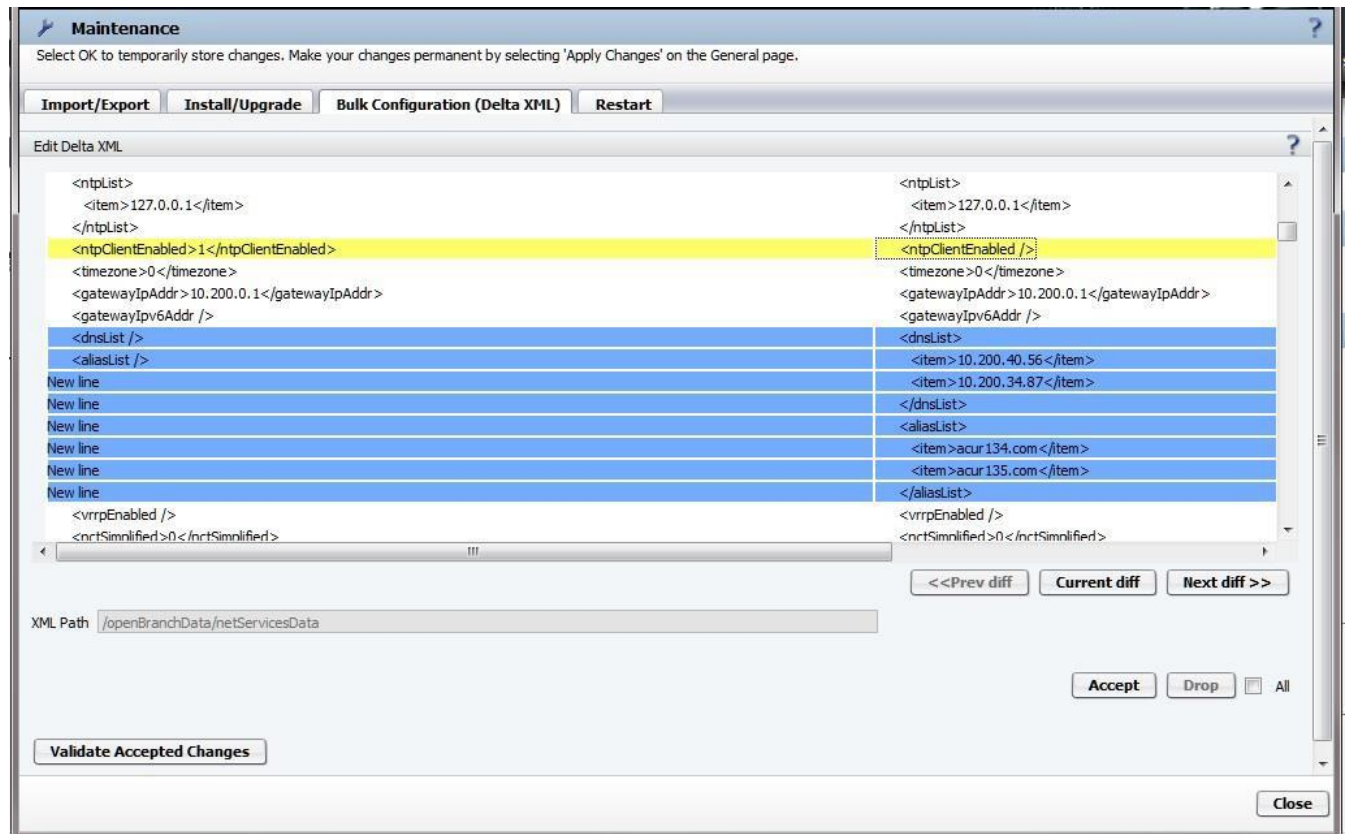
Now it is possible to navigate through the individual changes. Use the buttons **Prev diff** and **Next diff** to jump from one diff to the previous or next ones. **Current diff** focus the diff area on the current selected change.

XML Path indicates, on the xml structure, the position of the currently selected change.

All operations are done over the currently selected change (visually observed as surrounded by a dotted frame).

Hint: In normal configuration task this feature can be used to have a preview of modifications on xml before the

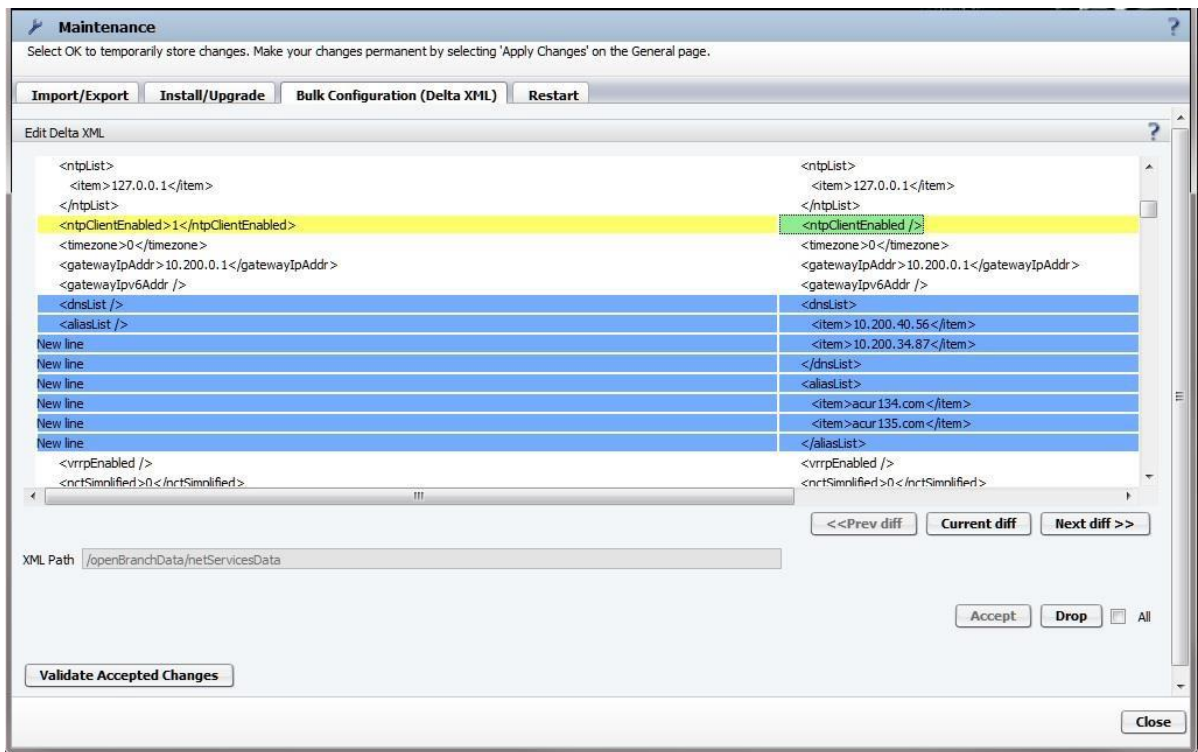
Apply Changes.



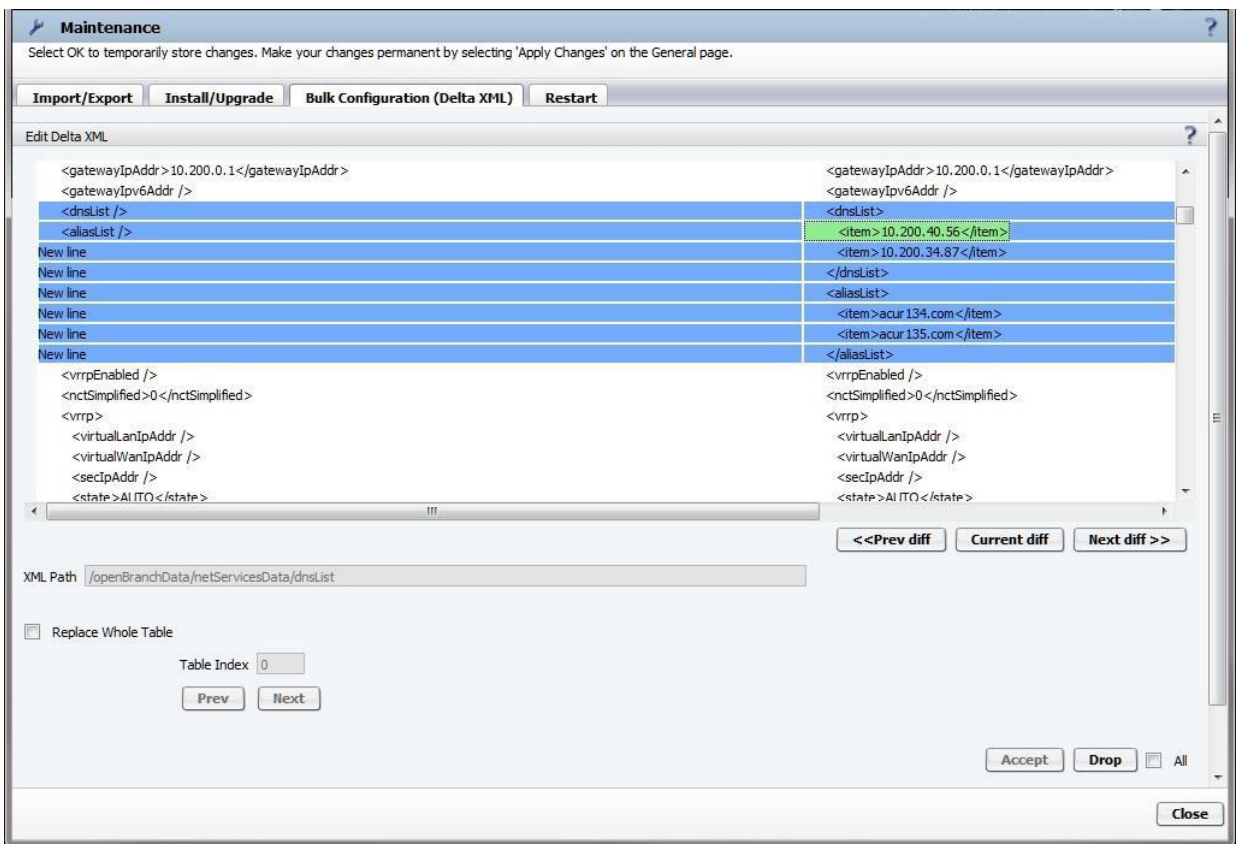
Only "accepted" changes are included on Delta XML files. It is possible to include/exclude changes on Delta XML file individually or in groups ("item" elements (lists or tables)).

Accept and **Drop** acts over currently selected change (checkbox **All** unchecked).

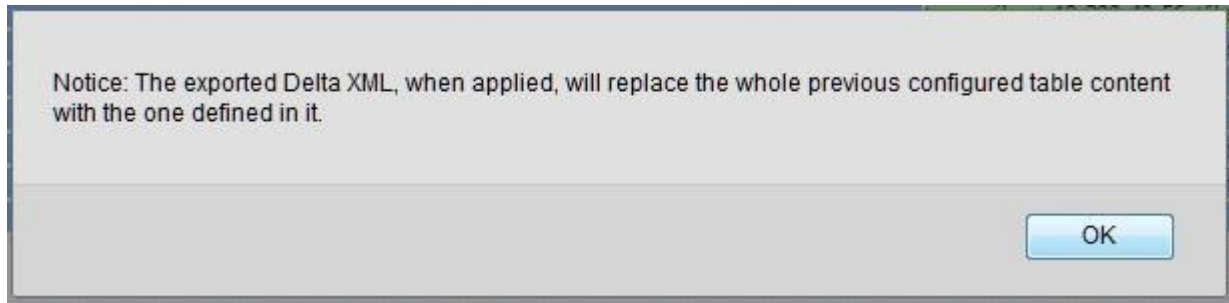
Accepted changes are marked with a green background. Dropping an accepted change returns its background to the original color. Original background colors are the same ones used on the **Compare** on **Import/Export** tab.



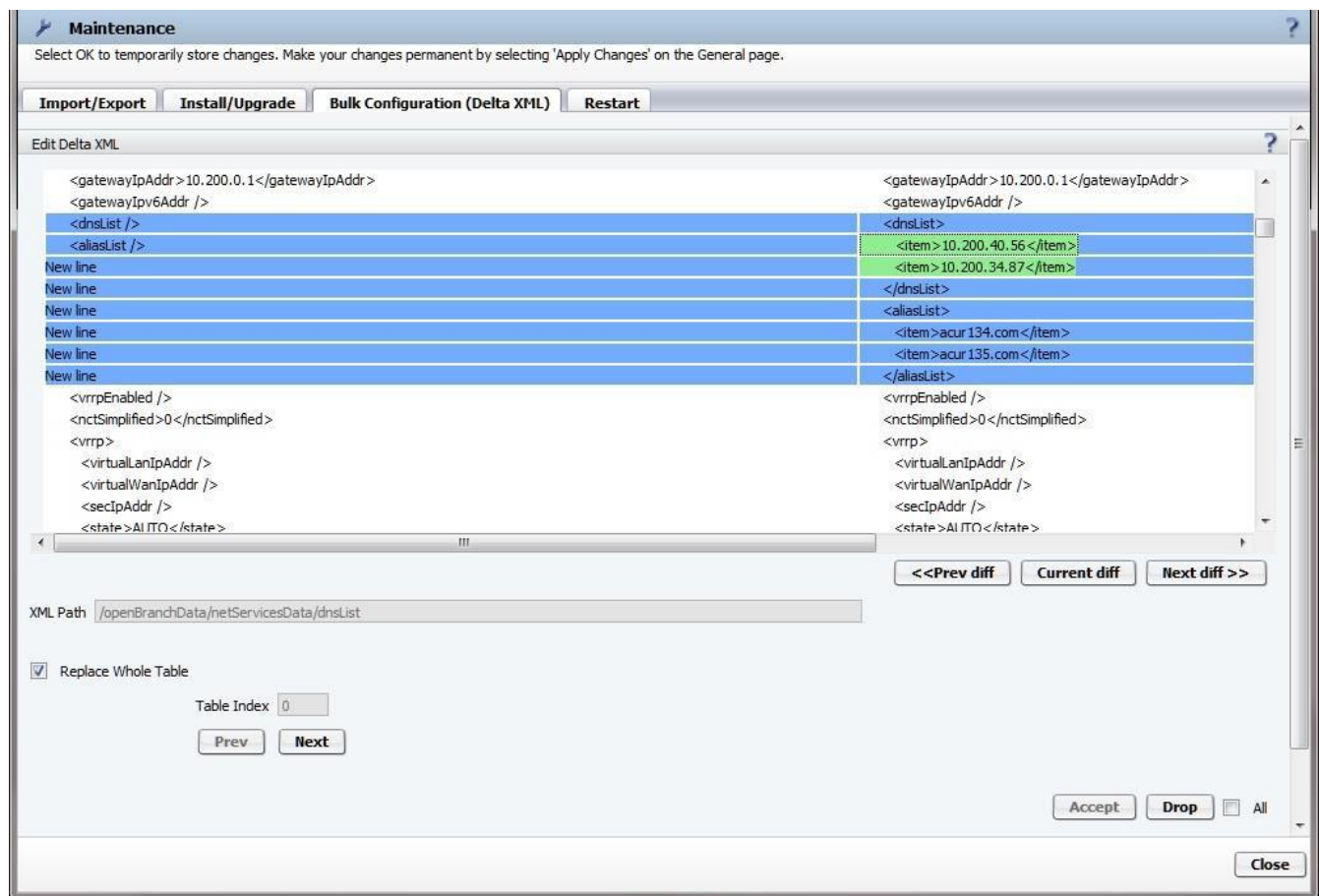
For lists and tables ("item" elements) we have additionally operations at left below the "XML Path".



This Notice is presented the first time **Replace Whole Table** is checked.



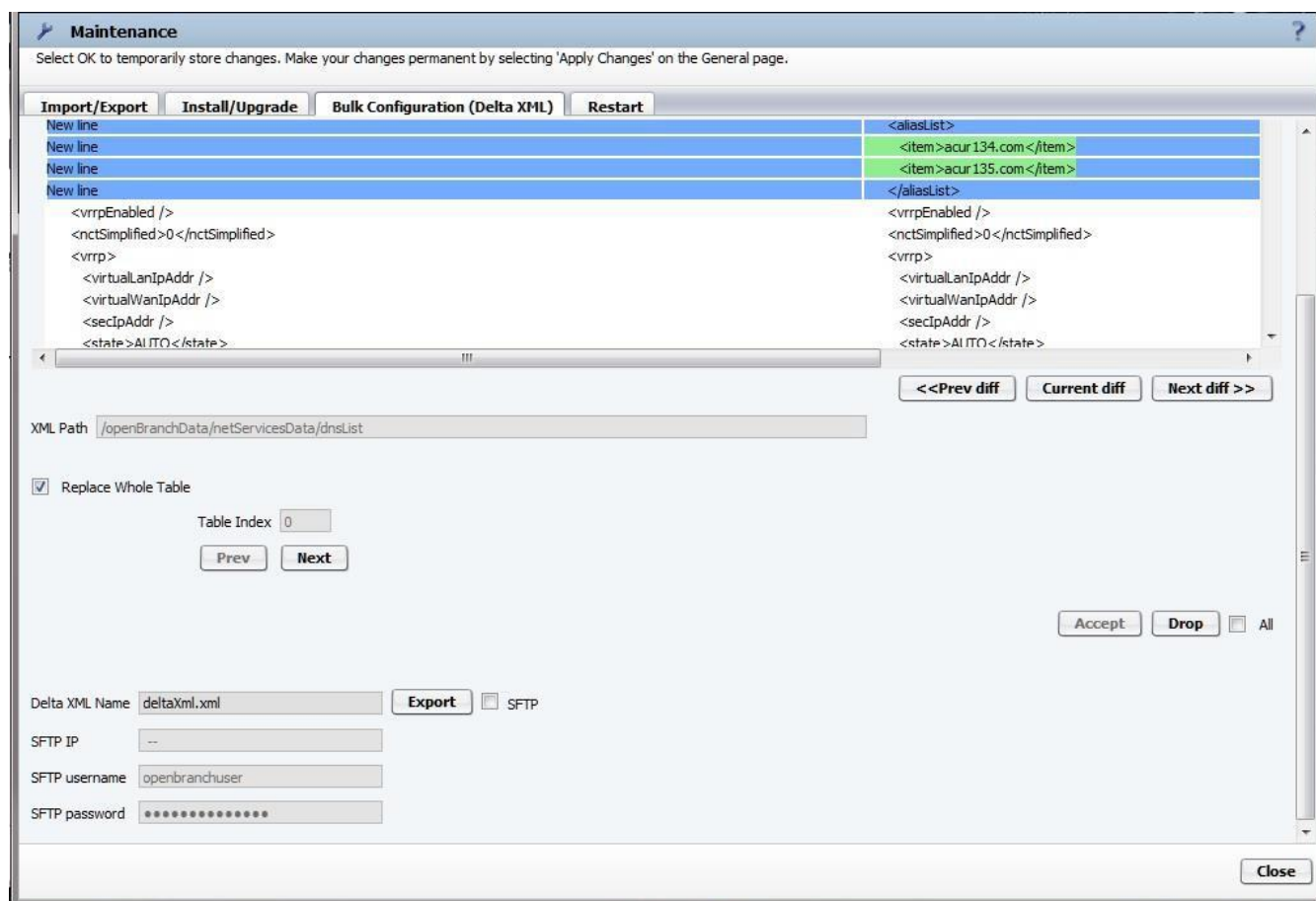
If the **Replace Whole Table** is checked, will turn green all "item" elements in the same level. The exported Delta XML, when applied, will replace the whole previous configured table content by the one in green. **Table Index** informs the position of the "item" element (starts with 0). **Prev** and **Next** navigates inside the table selecting "item" elements individually. **Accept/Drop** applies to them.



The following is presented when **All** is checked for the first time. When checked the **Accept/Drop** acts over all the changes. Be aware that unpredictable results may occur when exporting the Delta XML file.



After all desired changes are accepted, press **Validate Accepted Changes**. Export area is presented.



Delta XML file can be exported through the browser or SFTP.

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.

All xml tags inside the following xml tags are ignored for the purpose of generating Delta XML file:

alarmList, saveUser, saveRUser, saveTime, clientIpAddr, swVersion, hwType, product, hostname, logicalBranchOfficeId, hwId, saveCounter, openBranchNetwork, mode, voipData.

42 Upgrade

Full version will be installed on the backup partition and the active partition will be preserved in case of failure. Upgrade is possible using USB stick, local files stored in PC/network, HTTPS and SFTP. In USB stick the version stored in stick will be used, while in other methods the user has to choose which version will be used. In HTTPS or SFTP, the list is retrieved from the server of SW supplier. Software image *.tar file is required for all upgrades types. Tar files contains 3 files: image*.ob, image*.key, and image*.sig.

Note: Upgrade process will be interrupted if Web Page is Closed during the copy/sftp of the software(Local GUI). DB is not modified during Upgrades.

The screenshot shows the OpenScope GUI with the 'Inventory' tab selected. The 'Software Repository' section displays a table with columns: Product Name, Version, and Size. A yellow callout box points to the 'Add...' button, stating: "Under Maintenance Inventory, Image can be added to the Software Repository."

Below the repository list is the 'Add to software repository' section. It contains a list of files being uploaded: File 1 (image_ob-01.03.01.26.t), File 2 (image_ob-01.03.01.26.s), File 3, and File 4. A yellow callout box points to the 'Browse...' buttons, stating: "Browse/Add Image Upgrade and SPA file".

At the bottom, the 'Applications' menu is shown. A yellow callout box points to the 'Software activation' button, stating: "Select Software Activation from Applications menu."

Type	Active version	Node	IP address/Hostname
OpenScape Branch	V2R0.01.00 Build 12	MOB52	10.234.5.2
OpenScape Branch	---	OSBIP170-Node 1, OSBIP170-Node 2	10.234.1.170, 10.234.1.170
OpenScape Branch	---	BOAdvantec51	10.234.1.51
OpenScape Branch	V2R0.01.00 Build 3	bocaOB_21	10.234.1.21
OpenScape Branch	---	bocaOB22_OS850i	20.20.1.22
OpenScape Branch	---	FujitsuRed65-Node 1, FujitsuRed65-Node 2	10.234.1.67, 10.234.1.66
OpenScape Branch	---	bocaOB23_OS850i	20.20.4.23
OpenScape Branch	---	IBMIP58	10.234.1.58
OpenScape Branch	---	BO_JG_x3250M2	10.234.4.88
OpenScape Branch	---	IBM3250_IP70	10.234.1.70

1. USB Stick Copy image*.tar into USB stick and select Upgrade in GUI. USB stick needs to be selected for

Location source in drop down menu. Note: only one image must be copied to USB stick.

Name	Size	Type	Date Modified
image_ob-10.10.1.17.tar	282,890 KB	WinZip File	2/2/2009 5:19 PM

Note: "Assuming drive cache: write through" message shows on system/syslog when USB is connected to OSB.

1) Select **USB Stick** from Menu.
 2) Select Full Image Type
 3) Click on Activate
 4) When Upgrade Completes Remove USB and confirm restart.

Verify following OSV default firewall rule exists if experiencing problems upgrading/updating where error is related to CMP not being able to SFTP to SB.

Packet Filter Rule Name:
oLcal_Init_TCP_Node_IP
Description:
Remote FQDN:
Remote IP Address:
Remote NetMask:
Remote Port Begin: 0
Remote Port End: 0
Direction: InComing
Local Host : bond_node_alias
Local Port Begin: 0
Local Port End: 0
Transport Protocol: TCP
Action : Allow

System Information

Product name: OpenScale Branch

Node name: IBM3250-IP70

IP address: 10.234.1.70

Active version: V1R2.01.00

Software Updates

Location: USB stick [Configure...]

Version Image type

USB Full

USB Delta

2. Local File Copy image*.tar into local PC/Network. Common Repository needs to be selected for location source in drop down menu. Follow same steps as USB upgrade.

Software activation

Select software location and press 'Configure' if applicable to proceed with activation.

System Information

Product name: OpenScale Branch

Node name: IBM3250-IP70

IP address: 10.234.1.70

Active version: V1R2.01.00

Software Updates

Location: Common Repository [Configure...]

1) Select **Common Repository** from Menu.
 2) Select Version and Click on Activate.
 3) Close Window when Upgrade Completes.

Current status: RUNNING

Progress: 11.0%

Information:

Manually update status: Refresh

3. SFTP/HTTPS: only available from Local GUI. Contact Service if this is required.

43 Debug/Tracing

43.1 Log settings (Log Size, Log Level and Syslog)

User can configure log size and log level for each log type in the Utilities tab. It is also possible to configure a syslog server.

Note: setting the log levels to Warning, Notice, Info, or Debug may affect system performance and/or call processing and should only be done during maintenance windows. Please note that even in a maintenance window Basic functionality can be affected if high level of tracing is done. Tracing should only be enabled if requested by service.

Configuration > OpenScape Branch > Branch Office > Configuration > Diagnostics & Logs > Settings

Diagnostics & logs

Select OK to temporarily store changes. Make your changes permanent by selecting 'Apply Changes' on the General page.

Settings | Debugging | Continuous Tracing | On Demand Trace | Statistics

Settings

Log size (kbytes) Syslog server

Log Levels

SIP Server	Error	Process Manager	Notice
B2BUA	Error	Survivability Provider	Error
Media Server	Error	Alarm Manager	Error
CDR	Error	RTP Proxy	Error
Continuous Tracing	Error	ISDN	None
CAS MFC R2	None	SSM	Error
Redundancy	Notice	DAHDI	Error
CAS E&M/Ring Down	Error	SIP Service Provider	Error

☐ Signature on Log Files

Signature Key

Fallback

☒ Fallback to default log level

Fallback time (hh:mm)

Log Size: maximum size of each log file (32-1024).

Log Server: syslog server IP address.

Log Level: log level for each application can be configured individually.

Note: Default setting Log level is Error for most services (PM level is default "Notice").

Note: ISDN and Continuous Tracing log information will not be sent to Syslog Server.

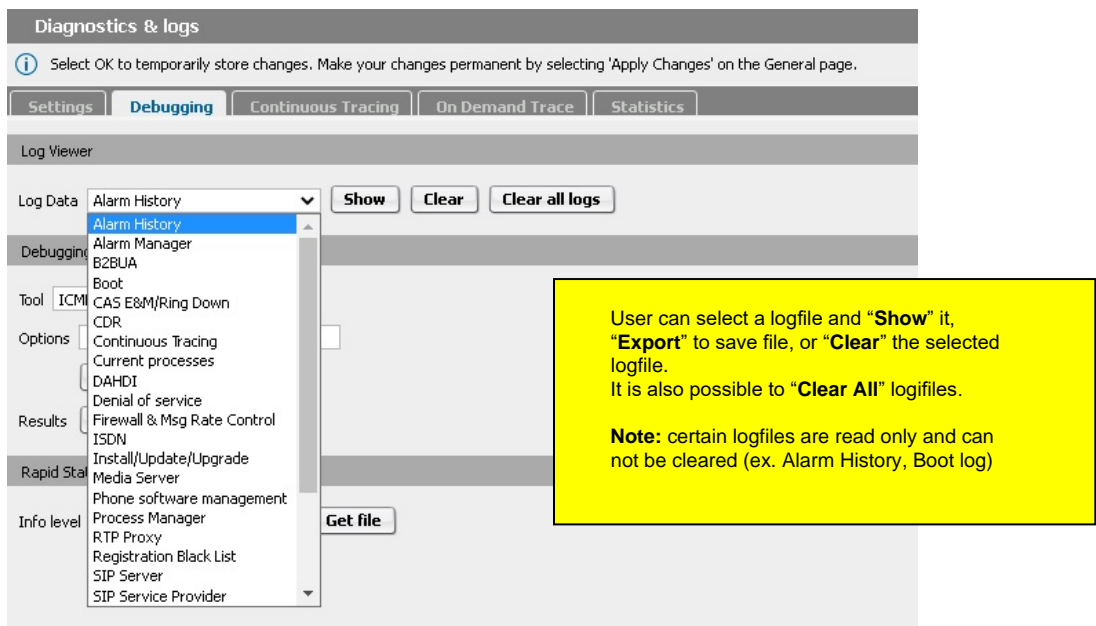
Note: SIP Server Info and Debug level will produce the same output

Flag used to return all category levels to default (Error) at time specified. It is the absolute time when the system will fallback the log levels. Option is useful to make sure that traces are set to default during normal hours in case specific tracing was done during maintenance window.

Log Level	Description
Emergency	Panic condition report.
Alert	Reports a condition that should be corrected immediately, such as failure.
Critical	Report of device failures.
Error	Level used for applications to report internal errors.
Warning	Level to be used to report application instability.
Notice	Report conditions that are not errors, but should require some attention.
Info	Used for Informational messages.
Debug	Level used for debugging applications.
Note: CAS and ISDN log levels include other log level categories (50i/500i only).	

43.2 Log data

Log data is available under the main OpenScape Branch Dashboard under Configuration > OpenScape Branch > Branch Office > Configuration >Diagnostics & Logs > Debugging



Application	Description
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 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 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.
Denial of service	The log will show hosts that sent DoS messages 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.
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 MFC 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, callee parties call duration and 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 provide logs for the initial installation via usbstick 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 RTPProxy 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.

43.3 Rapidstat

Tool that collects system information for systemdebugging.

Up to five levels of information can be retrieved. Result will be a compressed file containing the information. By default the info level is set to 2.

Note: Recommendation is to collect Level5 which includes information of all 5 categories.

Level 1 – System configuration, template files, boot and system log, process manager log, installed packages, cpu load, security, snmp, memory usage and disk usage.

Level 2 – Sip server logs, b2bua logs, sp logs and cdr logs + Level1

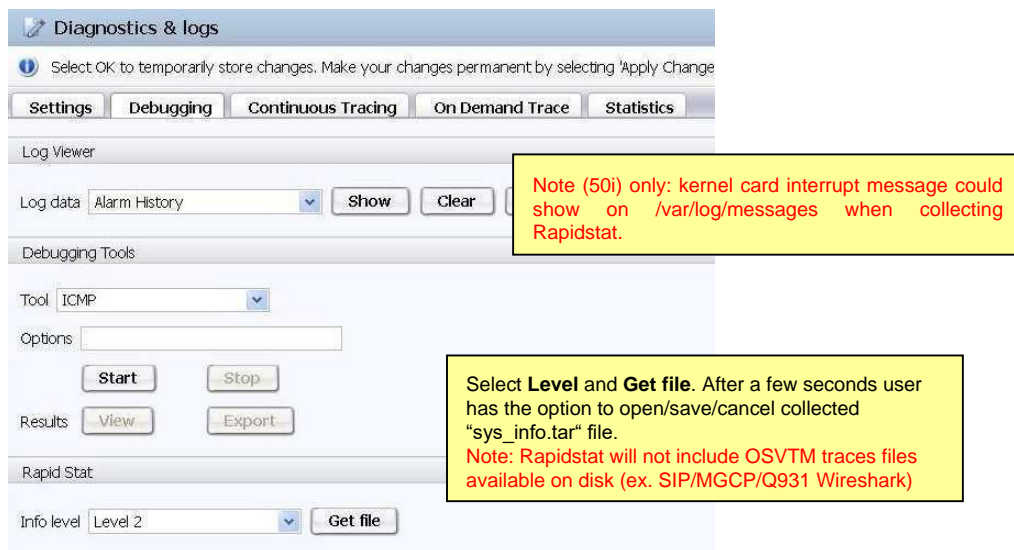
Level 3 – SNORT and audit logs + Level1/2

Level 4 – Management logs + Level 1/2/3

Level 5 – Media server logs, B2BUA channels and PRI/BRI information (50i/500i) + Rapidstat Level 1/2/3/4

Note: Level5 could take a few minutes to collect depending on traffic/usage (50i/500i)

Configuration OpenScape Branch Branch Office Configuration Diagnostics & Logs Debugging



43.4 Debugging Tools (ICMP, Trace Route, Network Tracer)

Under Logging user has access to ICMP, Traceroute, and Network Tracer debugging capabilities.

Configuration OpenScape Branch Branch Office Configuration Diagnostics & Logs Debugging

Diagnostics & logs

Select OK to temporarily store changes. Make your changes permanent by selecting Y

Settings **Debugging** **Continuous Tracing** **On Demand Trace** **St**

Log Viewer

Log data: Alarm History

Debugging Tools

Tool: ICMP

Options:

Results:

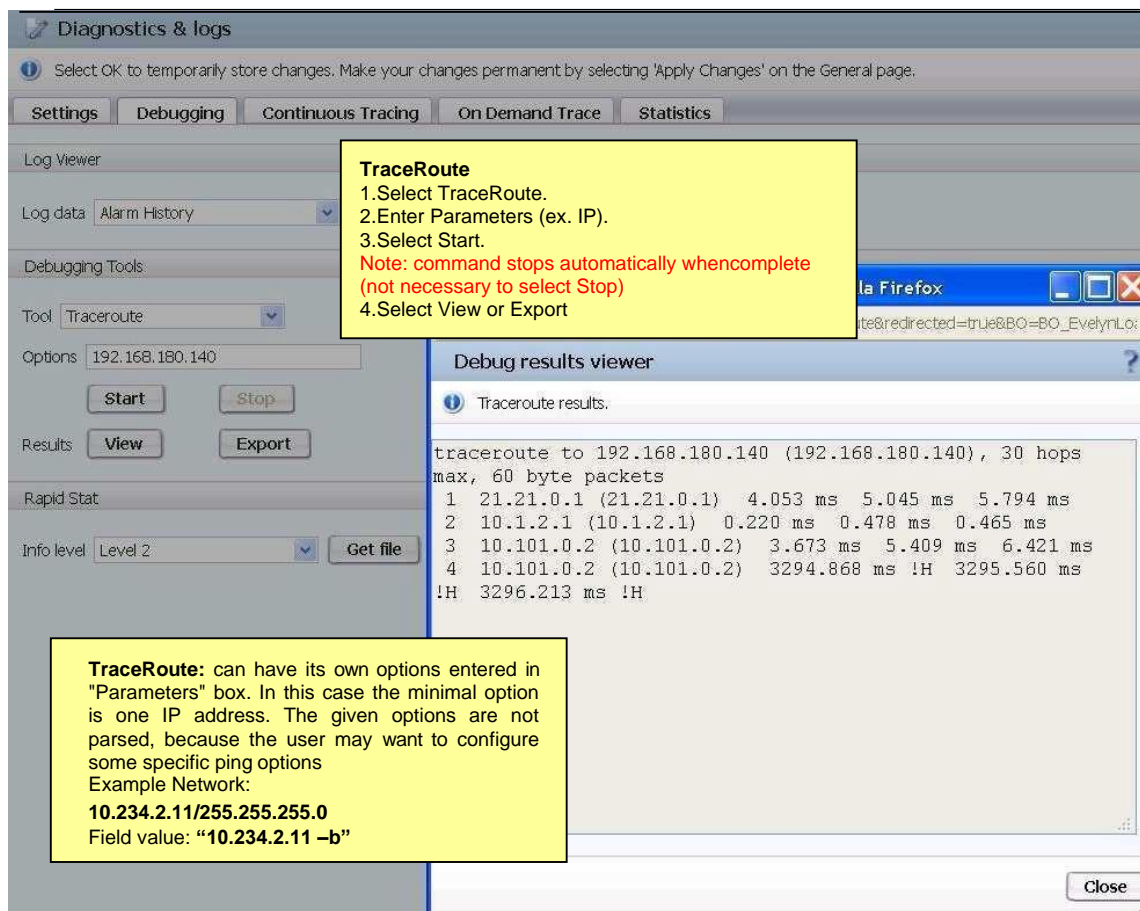
Rapid Stat

Info level: Level 2

ICMP

- 1) Select ICMP.
- 2) Enter Parameters (ex. IP).
- 3) Select Start.
- 4) Select Stop and view results in "Results Display"

ICMP: can have its own options entered in "Parameters" box. In this case the minimal option is one IP address. The given options are not parsed, because the user may want to configure some specific ping options Example Network:
10.234.2.11/255.255.255.0
 Field value: "**10.234.2.11 -b**"



Diagnostics & logs

i Select OK to temporarily store changes. Make your changes permanent by selecting 'Apply Changes' on the General page.

Settings Debugging Continuous Tracing On Demand Trace Statistics Serviceability

Log Viewer

Log Data Alarm History Show Clear Clear all logs

Debugging Tools

Tool Network Tracer

Interface All SIP/MGCP/Q931 Trace SIP/MGCP/Q931/RTP Trace

Output File Size(MB) 10

Results View Export

Rapid Stat

Info level Level 1 Get file

Network Tracer:

- 1) Select **Network Tracer**.
- 2) Select **Interface**.
- 3) Click **Start**.
- 4) Click **Stop**.
- 5) Press **Export** to get the *.cap file.

Network Tracer: The drop-down list is available for the user to select interface. When selecting **Stop**, the user is able to get the file and Open/Save it. The file is created as *.pcap. The maximum file size is also available to be selected as an input. The size should range between 1MB and 100MB.

Note: Ethereal or Wireshark is required to open the Network Tracer file.

Note: The SIP/MGCP trace option limits the amount of data captured to 1MB. SIP messages exceeding the limit of 2048 bytes are truncated.

43.5 Continuous Tracing

User can configure a trace manager server (OSVTM) so that traces/logs are captured 24x7. Log level categories are set under Settings tab (Default is Error).

Note: setting the log levels to Warning, Notice, Info, or Debug may affect system performance and/or call processing and should only be done during maintenance windows.

Please note that even in a maintenance window Basic functionality can be affected if high level of tracing is done.

Tracing should only be enabled if requested by service.

Configuration > OpenScope Branch > Branch Office > Configuration > Diagnostics & Logs > Continuous Tracing

The screenshot shows the 'Diagnostics & logs' section with the 'Continuous Tracing' tab selected. A yellow callout box explains the fields: 'System Name' is the OSV system name, 'Username/Password' is for connecting to the OSB SFTP server, and a note states that logs are sent as *.bz2 by the OSB for previous releases and as *.gz for the current release. The 'Enable' checkbox is checked. The 'Server' field contains '192.168.100.99', 'System name' is 'OSV7R0DQ', 'File size threshold (kbytes)' is '1024', 'SFTP username' is 'tracedata', and 'Time interval threshold (min)' is '60'. The 'SFTP password' field is masked with dots. Below these, 'SIP/Q931 trace' and 'MGCP trace' are both checked. Another yellow callout box explains the 'Enable' flag, IP address, file size/time interval thresholds, and notes that the polling time is about 10 seconds. It also states that SIP/Q931 and MGCP traces are enabled when their respective checkboxes are checked.

43.6 On Demand Trace

Allows selecting a log type and log level manually or for a specific time period.

Configuration > OpenScope Branch > Branch Office > Configuration > Diagnostics & Logs > On Demand Trace

The screenshot shows the 'Logging' section with the 'On Demand Trace' tab selected. A yellow callout box on the left notes that SIP Server Info and Debug level will produce the same output. The 'On Demand Trace Settings' section shows 'Log Type' set to 'Sip', 'Log Level' set to 'Info', and 'Duration' set to '5'. There are 'Start' and 'Stop' buttons. A yellow callout box on the right explains that the Log Type/Level can be started/stopped manually or configured for a time limit (e.g., 5 minutes), and notes that the default log level is Error for most services and Notice for PM level.

Note: setting the log levels to Warning, Notice, Info, or Debug may affect system performance and/or call processing and should only be done during maintenance windows.

Please note that even in a maintenance window Basic functionality can be affected if high level of tracing is done.

Tracing should only be enabled if requested by service.

43.7 Advanced (Enabling the System Collector Logs)

39.2.1 Export the current XML

39.2.2 Edit the XML

39.2.3 Search for <showAdvancedTab/>

39.2.4 Replace to <showAdvancedTab>1</ showAdvancedTab >

Eg.

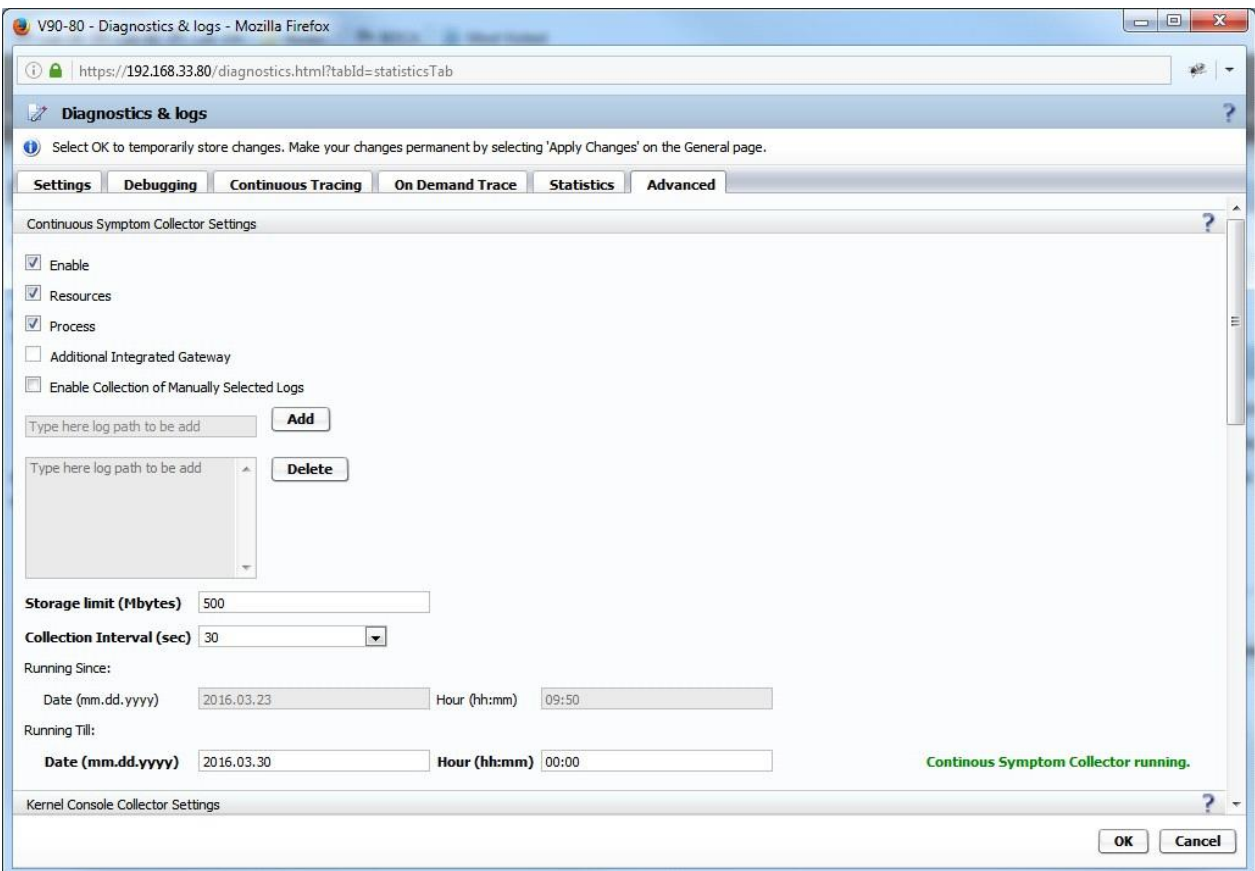
```
<continuousTracingSystemName>systemName</continuousTracingSystemName>
  <continuousTracingSFTPUsername>username</continuousTracingSFTPUsername>
<continuousTracingSFTPPassword>WGiNBgV/QfjgjZ6K/7qMUg==</continuousTracingSFTPPassword>
>

<ssmLogLevel>error</ssmLogLevel>
<redundancyLogLevel>notice</redundancyLogLevel>
<showAdvancedTab />
<cscEnable />
<cscResources />
<cscProcesses />
<cscIgw />
```

5 – **Save** the changes

6 – Import the modified XML

7 – The **Advanced** Tab is now available (Go to **Diagnostics & logs > Advanced**)



8 - Update the "**Journal Configuration**" help

Text:

Setting up a serial console:

- 1 - "Enable Forward to Console"
- 2 - "Enable "Console to Serial (COM1)"
- 3 - Set the "Console Device"

Note: If you are using the HW 50i refresh you have to set the "Console Device" to `"/dev/ttyS4"`. To the others hardware please use `"/dev/ttyS0"`

- 4 - Connect the serial cable to Linux/windows
- 5 - Open "Putty" terminal
- 6 - Set "Port" speed to 115200
- 7 - Restart the OSB

The logs will be shown at the console monitor

44 Port and Signaling Settings

Configuration > OpenScape Branch > Branch Office > Configuration > VoIP > Port and Signaling Settings

The screenshot shows the 'Port and Signaling Settings' page under the 'VOIP' section. At the top, there is a note: 'Select OK to temporarily store changes. Make your changes permanent by selecting 'Apply Changes' on the General page.' Below this are tabs for 'Sip Server Settings', 'Port and Signaling Settings' (which is active), 'Manipulation and Routing', 'Error Codes', and 'Media'. The page is divided into three main sections: 'Port Range', 'Signaling and Transport Settings', and 'Miscellaneous'. The 'Port Range' section includes fields for 'Media independent RTP ports' (Port min: 35000, Port max: 65000, Time to live (sec): 180), 'Subscribers dynamic SIP ports' (Port min: 10000, Port max: 16600), 'Gateways/trunks static SIP ports' (Port min: 9000, Port max: 9254), and 'TCP/BFCP ports' (Port min: 35000, Port max: 39999). The 'Signaling and Transport Settings' section includes 'INVITE No Answer timeout - Normal Mode (ms)' (360), 'INVITE No Answer timeout - Survival Mode (ms)' (180), a checkbox for 'Disable answer supervision for emergency calls line', 'TCP connect timeout (sec)' (4), 'TCP send timeout (sec)' (3), 'TCP connection lifetime (sec)' (350), a checkbox for 'TCP keep alive', and 'BFCP connection timer (min)' (720). The 'Miscellaneous' section has a checkbox for 'SIP SSL single context'.

Port Range

RTP Ports - These boxes specify the RTP port range (minimum and maximum) that RTP traffic uses, as well as the Time to live, which is the disconnection timer for non-RTP activity.

The range of acceptable port minimum and maximum values is 35000 to 65000. The port range should be between 2 and 48 ports in number.

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 (such as Automatic Call Distribution (ACD) Groups, Auto Attendant (AA), Multi Line Hunt Group (MLHG), Voicemail).

When negotiated media and the media profile used by the B2BUA (igw_features_lan) match, the B2BUA application may not use the port range configuration used by the RTP Proxy. In this case, the RTP Port Range is fixed at 10000 to 19999 and the "RTP ports min/max" fields are ignored.

The **Time to live** can range between 180 and 1200 seconds. Default is 180. When G729/sRTP is enabled, this field is valid for the Branch in the aforementioned modes.

Subscribers dynamic SIP ports - These boxes specify the SIP port range that is used in SIP messages. The range of acceptable port minimum and maximum values is 10000 to 65000. The port range must contain at least 500 ports. If the range is modified, the port mapping is cleared and active calls are affected. Every subscriber needs to sign up again.

Gateways/trunks static SIP ports - These boxes specify the SIP port range that is used by LAN gateways and trunks. Only the Branch SBC and SBC-Proxy modes have these boxes activated. The range of acceptable port minimum and maximum values is 9000 to 9254. The port range must be between 0 and 255.

Signaling and Transport Settings

INVITE No Answer timeout - NM (ms) - Timer in milliseconds which applies in case an INVITE is not finally answered after 100 tries in Normal mode operation. This timer is valid for outgoing calls made to both internal and external gateways.

INVITE No Answer timeout - SM (ms) - Timer in milliseconds which applies in case an INVITE is not finally answered after 100 tries in Survivable mode operation. This timer is valid for outgoing calls made to both internal and external gateways.

Disable Answer sup.: When a call is received on the OSB (Proxy, Branch SBC or SBC-Proxy) from the OSV (Normal Mode) or from the SIP Endpoint (Survivable Mode) and the DN part of the Request-URI corresponds to an Emergency Call and the **Disable Answer Supervision for Emergency Calls** flag is checked, the invite no answer monitoring timers and the invite no answer monitoring timer for outgoing calls will be canceled.

TCP connect timeout (sec) - The number in seconds until a connection attempt is abandoned.

TCP send timeout (sec) – The number of seconds in which a TCP connection will remain open before disconnected if it is unavailable.

TCP connection lifetime (sec) - TCP connection lifespan in seconds. Any TCP connection that is inactive for an extended period of time will be automatically terminated.

TCP keep alive - TCP keep alive is based on RFC 1122. The server will still respond to endpoint keep alive, even with the flag disabled. When the flag is enabled, the server will start sending TCP keep alive probes after 30 seconds of idle connection. The probes will be periodically sent every 240 seconds. In case of two consecutive failures, the TCP connection will be terminated. Only if all TCP-using endpoints are compatible with TCP keep alive should the option be enabled.

BFCP connection timer (min) – Long-term timer for a BFCP connection that is established over TCP or TLS. The value is entered in minutes and the acceptable range is between 60 and 1440 minutes. The default value is 12 hours (720 min). To prevent accidentally opening TCP ports, the TCP/BFCP connection timer needs to be activated.

Available only when using Branch SBC or SBC-proxy mode.

Miscellaneous

SIP SSL single context- It is used to share the same SSL context among the SIP Server child processes in order to save SIP Server shared memory. When the flag is disabled, there is an increase in memory usage by the SIP server compared to when it is enabled. The total system memory usage may increase up to 1%. It is recommended to disable the flag if the system has enough memory for multiple TLS processing or if multiple local addresses are used that refer to the same remote address using TLS protocol.

45 Branch SBC Mode

The OpenScapeBranch can operate as Session Border Controller (SBC) or SIP Proxy. The Session Border Controller mode is designed to isolate the Branch and its internal network components in a different sub-net. In this sense SIP headers, internal ports and internal addresses as well as RTP internal ports and internal addresses are not propagated to the external network.

SBC Configuration requires a second network interface to be used. In small model this is the 4th interface while in large model is the 2nd. For SBC mode the WAN interface should be activated. The system will reset upon saving the configuration when the mode is changed. The most common scenario is the Branch-SBC connected to the OSV via a OSS. Please refer to the Branch behind OSS chapter for more details.

Note 1: For Branch SBC mode, the WAN interface is used to access the OSV network. SIP phones should be configured with OpenScapeBranch LAN IP and OSV.

Note 2: NAT flag must not be enabled for BranchSBC.

1. Create an Endpoint for OSB SBC (All OSB Endpoints that have been configured have step 1 profile).

Configuration > OpenScape Voice > BG > Main Office > Members > Endpoints > Add

[BOCAST1] - BGLoad - Main Office - Edit Endpoint : OBSBC56

General | SIP | Attributes | Aliases | Routes | Accounting

Endpoint

Define the connection data of an endpoint, e.g. you may use this to add a gateway to a switch.

Name: OBSBC56

Remark:

Registered: ☒

Profile: OBSBC56

Branch Office:

Associated Endpoint:

SIP-Q Signaling:

For the static Endpoints the address of the SIP signaling interface can be specified in IP or FQDN format.
Note that the address of the signaling interface cannot be modified unless the entry in the security section has first been removed.

SIP Private Networking: ☐

SIP-Q Signaling: ☐

SIP Trunking: ☒

Type: Static

Address: 10.234.1.70

Port: 5060

Transport protocol: TCP

[BOCAST1] - BGLoad - Main Office - Edit Endpoint : OBSBC56

General | SIP | Attributes | Aliases | Routes | Accounting

Endpoint Template

Select a suitable Endpoint Template for this endpoint.

Endpoint Template:

Attributes

Attributes available for this SIP endpoint

UPDATE for Confirmed Dialogs Supported ☐

Send Provisional response during session updates ☐

Survivable Endpoint ☒

SIP Proxy ☒

Route via Proxy ☒

Allow Proxy Bypass ☐

Aliases

You can associate here aliases with a SIP Endpoint.

Name	Type
10.234.1.70	SIP URL

1 Item Add Delete

- Proxy flag: Update Proxy flag in OSV from RtpFalse to RtpTrue.

OpenScape Voice **Administration** **Signaling Management** **SIP**

[OSVCLUSTERV7] - [BGLoad] - [Main Office] - Edit Subscriber : 5558885230

Subscriber Description

General Displays Routing Connection Security Keyset Groups

Connection Settings

Connection Information: SIP

Type: Dynamic

Transport Protocol: UDP

IP Address: Port: 5060

Associated Endpoint: ... Clear

ANAT Support: Automatic

SBC Branch Office.

Note: In OSV V4R1 flag was removed from CMP and is enabled by default. Step only needed if older version of OSV is used

[BOCAST1] - SIP Settings

General PAC Rerouting SIP Timers Best Effort SRTP

Registration

Allow registration via proxy and enable

Enable Proxy Registration: ☒

Enable Registration Renewal: ☐

Max. Reg. Renewals(sec.): 604800

OK Cancel

Enable Proxy Registration Flag

3. Discover/Add Branch Office

Configuration > OpenScape Voice > Business Group > Branch Office List > Add

- 1) Select **Add** to discover Branch Office.
- 2) Setup **Branch Office Name**
- 3) Select SIP **endpoint** created in step 1 of OSV Configuration.
- 4) Select Appropriate **NP** and **Office Code**.
- 5) Check OpenScape Branch Flag.

[BOCAST1] - BGLoad - Edit Branch Office : SBCOB56

Here you can create a Branch Office. Representative Endpoint is mandatory

General DID Pool Access Control List

General

Branch Office Name: SBCOB56

Representative Endpoint: OBSBC56

Numbering Plan: NP_BGLoad

Office Code: 555888

Routing Area:

This is a Branch Office of type OpenScape Branch: ☒

Select OSB End Point

Note: Branch Office Flag must be checked.

4. Associate BGLs behind the SBC.

Configuration > OpenScope Voice > BG > Members > Subscribers > Select BGLs

[OSVCLUSTERV7] - [BGLoad] - [Main Office] - Edit Subscriber : 5558885230

Subscriber Description

General Displays Routing Connection Security Keyset Groups

Connection Settings

Connection Information: SIP

Type: Dynamic

Transport Protocol: UDP

IP Address: Port: 5060

Associated Endpoint: ... Clear

ANAT Support: Automatic

SBC Branch Office.

5. Select Branch Office from Office List

Configuration > OpenScope Branch > Branch Office > Select

Configuration Maintenance User Management

OpenScope Voice OpenScope Branch RGB700 Unified Communications CMP

OpenScope Branch Overview - OSVCLUSTERV6

Use the Refresh selected button to update the status of selected OpenScope Branch appliances. To update the status of all OpenScope Branch appliances use the Refresh all button.

Filter: for Branch Office Go Clear

Manage Local password... Refresh Selected Refresh All Add... Edit... Delete...

Branch Office	IP Address	Comm System	Business Group	Version	Status	Mode	Last Update
Advantech_1.56	10.234.1.56	OSVCLUSTERV6	BG_MarkP	V2R0.01.00 Build 11	Normal	Proxy	2011/07/23 09:53:37
aicharlotteosb1	10.238.16.10	OSVCLUSTERV6	EDMC	---	Unreachable	---	2011/07/23 09:53:37
boca0820_TLS	10.234.1.20	OSVCLUSTERV6	T	---	---	---	---
boca0821_BLS	10.234.1.20	OSVCLUSTERV6	T	---	---	---	---
boca0822_OS850i	20.20.1.22	OSVCLUSTERV6	B	---	---	---	---
boca0823_OS850i	20.20.4.23	OSVCLUSTERV6	B	---	---	---	---
boca08_20	10.234.1.20	OSVCLUSTERV6	BICA	V2R0.01.00 Build 11	Normal	Proxy	2011/07/23 09:53:37

Refresh status for selected Branch or Refresh all. Main Branch window allows changing of local password for user assistant/administrator (depending on release) to connect to OSB.

Help Link for subsection.

After selecting the Branch Office user has access to Statistics, Registered Subscribers, Backup link Status (if enabled), and Link Status (Advantech 50i only). License Information is covered on License Section.

OpenScope Voice
OpenScope Branch
R68700
Unified Communications
CMP

Profiles
Profiles list
Select Profile
Management
Configuration
Administration
Job Management
Licensing
OSVCLUSTERV6
Branch Office list
OSBIP170
Management
Configuration
Alarms
Logging
Media Server
Network Services
Security
Survivability
System
VoIP
ACD
Auto Attendant
Integrated gateways
Phone Software

General - OSVCLUSTERV6 - OSBIP170

Aggregated Information and data for selected Branch Office.

Apply Changes

Cancel Changes

Statistics

System Info

SIP Server

Active Dialogs: 0

Requests In: 18622

Requests Out: 5107

Responses In: 724

Responses Out: 13462

Registered subscribers:

Show...

Link status:

Show...

User Can Apply or Cancel Changes

Licensing Information

First updated: --- Last updated: ---

Logical ID: OSVCLUSTERV6:BGLoad:OSBIP170 Hw ID: N/A

Refresh

Device license update

Configure

License type	Configured	Locally Configured	Usage
OpenScope Branch Base	0	0	0
OpenScope Branch Users	0	0	0
Auto Attendant feature	0	0	0
Backup ACD feature	0	0	0
SBC sessions	0	0	0

User can apply configuration changes by using “ApplyChanges”.

Note: Depending on the changes made some processes or even the entire system will restart. GUI will alert user when restart is required.

Selecting “Cancel Changes” will revert back all changes since the last “ApplyChanges”

Go to VOIP configuration and select Mode BranchSBC.

Note: changing modes (from proxy to Branch SBC) requires a system restart.

Configuration > OpenScope Branch > Branch Office > Configuration > System > Settings

The screenshot displays the configuration interface for OpenScope Branch V10, divided into two main sections: System and VOIP.

System Configuration:

- General:** Branch Mode is set to "Branch SBC". Hostname is "PRIS250i" and Domain name is "branch.br". There is a checkbox for "Gateway only".
- Country Configuration:** Country is set to "Argentina".
- Administration:** Session expiry timer is "3 hours". There is a checkbox for "Enable SSDP".
- Watchdog Configuration:** "Enable watchdog" is checked. Watchdog expiry timer is "2 Minutes".

VOIP Configuration:

- General:** Comm System Type is "geo-separated". OPTIONS source port is "5060". IP Version Towards SIP Server is "IPv4".
- Options:** "Enable path tagging" is checked. "Branch behind SBC", "Branch behind NAT", "Synch subscriber data", "Disable notification in survivable mode", and "Enforce minimum Subscriber TransportType Security" are unchecked.
- Other trusted servers** and **Load Balance Mapping Table** buttons are present.
- Node 1:** Target type is "Binding". Primary server is "10.100.182.56" with Transport "TLS" and Port "5061". Backup server is empty with Transport "TCP" and Port "5060". SRV record is empty with Transport "TCP".
- Node 2:** Target type is "Binding". Primary server is "10.100.183.57" with Transport "TLS" and Port "5061".

Annotations:

- Annotation 1:** "1) Select **Branch SBC** mode (When configuration is changed from Proxy to SBC and vice versa, except activating WAN interface also physical cables switch is needed on the box. (eg LAN is used in Proxy mode so cable that was plugged to this eth interface has to be plugged to WAN))"
- Annotation 2:** "Branch behind SBC: Indicates whether the OpenScope Branch is behind a Centralized Session Border Controller (OSS or 3rd party). Branch behind NAT: checked for a branch whose ip address is not static but subject to dynamic change. When this is checked, then the branch shall use its "Logical Branch office ID" as "Logical- Endpoint-ID" to be encrypted in the OPTIONS sent to OSS."
- Annotation 3:** "2) Configure OSV nodes and apply settings. OSB will restart."

6. **Configure LAN interface of OpenScapeBranch and apply changes. Note: changes require a system restart.**
Configuration > OpenScape Branch > Branch Office > Configuration > Network Services > Interfaces

Network/Net. Services

Select OK to temporarily store changes. Make your changes permanent by selecting 'Apply Changes' on the General page.

Settings DNS NTP DHCP Traffic Shaping QoS

Physical Network Interface

Interface	Enabled	MTU	Speed (Mbps)	Duplex mode
eth0	<input checked="" type="checkbox"/>	1500	Auto	Auto
eth1	<input checked="" type="checkbox"/>	1500	Auto	Auto

Interface Configuration

LAN configuration

Type	Interface	IP address	Subnet mask	VLAN tag	UDP port	TCP port	TLS port	MTLS port
Main IPv4	eth0	30.30.0.45	255.255.0.0	0	5060	5060	5061	5161

Add Delete

WAN configuration

Type	Interface	IP address	Subnet mask	VLAN tag	UDP port	TCP port	TLS port	MTLS port
Main IPv4	eth1	25.25.0.45	255.255.255.0	0	5060	5060	5061	

Add Delete

LAN/WAN should be setup (LAN IP MUST BE CONFIGURED FOR PHONE REGISTRATIONS SERVER)

Note: Interface 2 is WAN for OSB50/1000/6000 systems and Interface 4 is WAN for OSB250 (Advantech)

7. Configure Phone devices to work through SBC.

Administrator Pages User Pages

Admin Login
Applications
Bluetooth
Network
System
System Identity
SIP interface
Registration
SNMP
Features
Security
File transfer
Local functions
Date and time
Speech

SIP interface

Outbound proxy ☒

Default OBP domain

SIP transport TCP

Response timer (ms) 32000

NonCall trans. (ms) 32000

Reg. backoff (seconds) 60

Connectivity check timer (seconds) 0

SIP server address 10.234.3.50

SIP registrar address 10.234.3.50

SIP gateway address 192.168.36.1

Session

Session timer enabled ☐

Session duration (seconds) 3600

Registration timer (seconds) 3600

Server type OS Voice

Realm

User ID

Password

Sip Registrar/Server should be the SIPSM1 (Even If TLS is used). OSB LAN address is used for SIP gateway address. Outbound Proxy Flag is Checked.
Note: sipism1 can be used with TLS for Proxy mode if sipism3 is added in trusted IP list on OpenScape branch configuration

When there is a Session Border Controller between the OpenScape Voice and the internet, "SIP server address" and "SIP registrar address" will point to the SBC.
If the SBC is Acme 2600 or OSS then flag # 6 has to be enabled manually (Set to 1) on the OSB XML.

Note: Phones are connected to the LAN Interface of OpenScapeBranch. Thus, in order to access phones GUI a PC that is connected to this LAN is needed. If configured so, phones can be accessed also from a PC that is attached in the WAN interface of OpenScapeBranch. In order to do this, port forwarding rules must be added on OpenScapeBranch as shown below.

Configuration > OpenScape Branch > Branch Office > Configuration > Security > Firewall > Wan

Port Forward

Port forward provisioning.

LAN/WAN should be setup
Phones can be accessed using <https://{WAN IP of OpenBranch}:{In port of phone}>

Row	In port	Out IP address	Out port	Protocol
1	5025	30.30.0.17	443	All
2	5026	30.30.0.19	443	All

Firewall Configuration

Firewall configuration provisioning for WAN.

General

☒ Enable IP masquerading

☒ Enable port forwarding

Configure

Note: The "IP masquerading" flag should be enabled for CSTA and/or any layer3 data connection from WAN to LAN.

Incoming/Outgoing network connections

DNS

Allow

SSH

Allow

SNMP

Allow

ICMP

Allow

FTP

Allow

Telnet

Allow

HTTPS

Allow

NTP

Allow

Incoming VOIP connections

SIP

Allow

TLS

Allow

RTP/sRTP

Allow

MGCP

Allow

☒ Allow all network connections

White list

Add

Delete

IP address or subnet	Port
30.30.0.17	0
30.30.0.19	0

Black list

Add

Delete

IP address or subnet	Port
----------------------	------

Note: Connection between phones located in LAN interface of SBC and DLS can be established by configuring White List (Phone IP and port empty). Please note that DLS DCMP must be configured and enabled.

External Firewall

☐ External Firewall

☐ SIP ALG

☐ Circuit Only

In order to make TDM calls using a GW that is located in the SBC branch; the Endpoint previously created for SBC in OSV has to be associated to PAC, Destination, Route, etc.

Prefix access code, destination code, destination and a new route that is going to route the GW calls to this Endpoint have to be added also.

Note: for SIPQ GWs one additional SBC OSV Endpoint is required with SIPQ checked to reflect the GW behind the OSB Proxy. Same configuration of originally created Endpoint should be used. Only exception is that alias will be empty since it is already being used on original SBC OSV Endpoint. Prefix that is used to make the call can't be sent to OpenScapeBranch because OpenScapeBranch doesn't parse SIPQ MIME. All manipulation has to be done in OSV this time (SIPQ ONLY).

Please note that since Sip GW calls are going to be routed to OpenScapeBranch, the prefix that is used to make the call, has to be sent to OpenScapeBranch. So, in Features tab sheet in OpenScape Branch in Assistant enable gateways/trunk configuration.

Configuration > OpenScape Branch > Branch Office > Features > Enable Gateways/trunk

NOTE2: On a SIPQ incoming call in Normal Mode, the trunkgroup FQDN is used in the INVITE contact's header sent to the OSV> This FQDN should be configured in the endpoint alias list for the OSV to recognize that his call has a SIPQ (SIPQv2) signaling.

If the OSV does not recognize the endpoint, it will reject the call and the OSB will fall back to SIP without mapping any SIPQ Info Elements from the trunk.

In Nomal Mode, the OSB acts as a tunnel and does not manipulate and QSIG content received from the OSB or the Trunk. Therefore, no TON configuration is applied on these QSIG calls.

In case of interconnection with old PBXs, the flag "truncated mime" should be activated in the OSV.

9 Configuration for gateways with subscribers under OSB in SBC mode

Two entries in the gateway table shall be created.

One entry shall have the routing prefix configured with the access code for external calls using the lines under the gateway.

The other entry shall match with the FXS DN prefixes in order to route the calls to the FXS under the gateway. This is necessary because the OSB in SBC mode does not store registers from static endpoints the location table.

46 Media Server (MS)

The MS provides announcements and station controlled conference for subscribers in the branch.

Note with OSV V5.1 and later: OpenScapeBranch and its internal MediaServer supports now SDESbest-effort method for tones, announcements, and conferencing in all modes automatically when they receive SDESoffers from SIP phones/clients, in Normal Mode & Survivability Mode, when setup as TLS@5061

Note: MMS Adapter runs if branch is in SBC mode, or Flag 'Branch Behind NAT' is set AND OSB is in mode 'Proxy' or 'SBC-Proxy' and MS Converter Services run in Branch SBC and SBC-Proxy modes.

Configuration > OpenScape Branch > Branch Office > Configuration > Features > Enable Media Server/Streaming

Media Server

Select OK to temporarily store changes. Make your changes permanent by selecting 'Apply'.

General

Media server listen port: 2427 ☐ Use system FQDN

Language: en_us ☐ Enable whisper mode

Advanced...

Conference

Number of conference/whisper cells: 12 Maximum conference time (sec): 18000 ☐ Unlimited

Conference prefix access code: 8000

Announcements

Number of announcement cells: 1800 ☐ Unlimited

☒ Stop announcement on DTMF

Media Server Listen Port: port the Media Server uses for communication with the Call Agent.

Language: preferred language. **Advanced:** Advanced Media Server configuration. Use System FQDN: Uses system FQDN on media transaction, instead of IP.

Number of announcement ports: max amount of ports that are opened for providing announcements (Or Unlimited). **Maximum announcement time:** max time, in seconds, an announcement session is allowed to be active (Or Unlimited). **Stop announcement on DTMF:** if enabled, announcement will stop when the Media Server receives a DTMF.

Number of Conference/whisper ports: max amount of ports opened for conferences. **Maximum Conference time:** max time, in seconds, a conference is allowed to be active. **Conference Prefix Access Code:** Prefix in SIP R- URI required to access a Media Server conference.

Note: Large Conference with MS will not show lock on phone when SRTP is used

Media Server - Advanced

Media Server provisioning:

MS Adapter

Transaction time-to-live: 30

Languages

Installed languages

en_us
es

Transaction time-to-live: used to configure the maximum duration, in seconds, of a MGCP transaction in SBC mode.

Installed languages: This area lists all Media Server languages installed. User can delete or install languages.

Note: 2 MS Languages (OSB50i/OSB250/OSB500i) or 5MS Languages (OSB1000/OSB6000) can be uploaded on OSBs but only 1 can be active.

Install Language

Language file: Seleccionar archivo... mediaserver_announcements_fr-3.3_5.7.0-677.1586.rpm **Install**

Announcements
?

Number of announcement cells 15
Maximum announcement time (sec)
☒ Unlimited

☐ Stop announcement on DTMF

Streaming Source (requires Base license V9 or greater)
?

General Settings: Streaming Source

☒ Enable Music On Hold Streaming

☒ Use HTTP proxy

HTTP proxy FQDN or IP

HTTP proxy port

Local FQDN or IP

Streaming buffer size (sec)

Streaming Source URL (first)

Status:
CONNECTED

Streaming Source URL (fallback)

Streaming Source

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

In order to ensure support to secure media exchange (SRTP) with Media Server, OpenScape Branch and phone times should be synchronized through NTP.

The language package provided during installation is English US, other packages (German Language) can be installed by using GUI.

OpenScapeBranch uses the language packs from the Open Scape Application DVD.
Those language packs are RPM files located in the folder "noarch" of the DVD.

Note: only language packs from Application V6 and above work with OSBV7.

When the Media Server is used as external media server for other branches the Protocol must be configured in OpenScape Voice as MGCP 1.0 NCS 1.0 and the treatments must be properly configured.
The log levels of MS, MS adapter and MS converter are set to the same level by setting Media Server log level.

Configuring OSB as main Media Server in OSV

It is possible to have OpenScape Branch as the Main Media Server for the OSV. These steps also assume a distributed deployment where an OpenScape Branch provides MS service at the main location.

Configuring OSB in the OSV as Branch Media Server

Steps will show how to configure an OpenScape Branch server as the Media Server for a Branch.

Configuring the main Media Server as a backup of the Branch MS

In some situations it may be desired to have the main media server as the backup of the branch mediaserver. This is entirely done in the OSV using the Media Server audit mechanism and routing. The steps to configure this are as follow:

46.1 Configuring OSB as main Media Server in OSV

NOTE: These steps are based on the "Distributed Deployment with Branches" instructions available with the OSV manual "**OpenScape Voice V7, Configuration, Administrator Documentation**" or "**OpenScape Voice V7, Installation and Upgrades, Installation Guide**". (If MOP P30310-Q2575-Q140-03-7620 is installed refer to release note for added instruction).

It is possible to have OpenScape Branch as the Main Media Server for the OSV. These steps also assume a distributed deployment where an OpenScape Branch provides MS service at the main location.
If there is another Media Server in the Main location and branch support is being added, the main Media Server configuration must be as follows to support this deployment.

Under Configuration > OpenScape Voice > Administration > Media Servers, select List and Press Add:

[NodeV5]-Media Server

Configure Media Gateway Options

General Extended Circuits

In the General Section, you can configure the main options of the media server

General Options

General options are listed below

Gateway Name: OSB527

Fully Qualified Domain Name: [10.234.5.27]

Assign Method: Automatic

Protocol Type: MGCP

Protocol Version: MGCP 1.0 NCS 1.0

Circuit Format: \$/\$

Multi Homing: Enabled

MG Signaling IP Address Allocation Method: Static

MG Signaling: 10.234.5.27

Admin Status: RsAvailable

Operational Status: RsAvailable

Location Domain:

FQDN: IP address for OSB. Please note the brackets "[]"

Circuit Format: ID for the GW/Server. \$ serves as Wildcard. Media Server will select free Endpoints as needed.

MG Signaling: IP address for OSB

Administration

- General Settings
- Media Servers
 - List
 - Intercepts
 - Audit
 - Languages
- Signaling Management

[BOCAST6] - Modify Media Server: OBIBM3250IP70

General **Extended** **Circuits**

Extended Options

Extended options are listed below

Timeout (msec):

Retry Count:

Maximum Retransmission Timer (sec):

Transmission Timer Length (sec):

History Timer Duration (sec) :

MG Receive Port:

MG Listen Port:

Keep Alive:

DTMF:

Three-way Handshake:

Overload

Overload options are listed below

Overload Support:

Allow Three-way Calls:

Allow Electronic Surveillance Calls:

Overload Levels	Gap Interval (sec)	Associated Return Code
Level 1	<input type="text" value="5"/>	<input type="text" value="400"/>
Level 2	<input type="text" value="10"/>	<input type="text" value="400"/>
Level 3	<input type="text" value="20"/>	<input type="text" value="400"/>

Overload Status:

OK **Cancel**

Depending on the traffic type the corresponding circuits must be created.

Configure Media Gateway Options

General **Extended** **Circuits**

Circuits

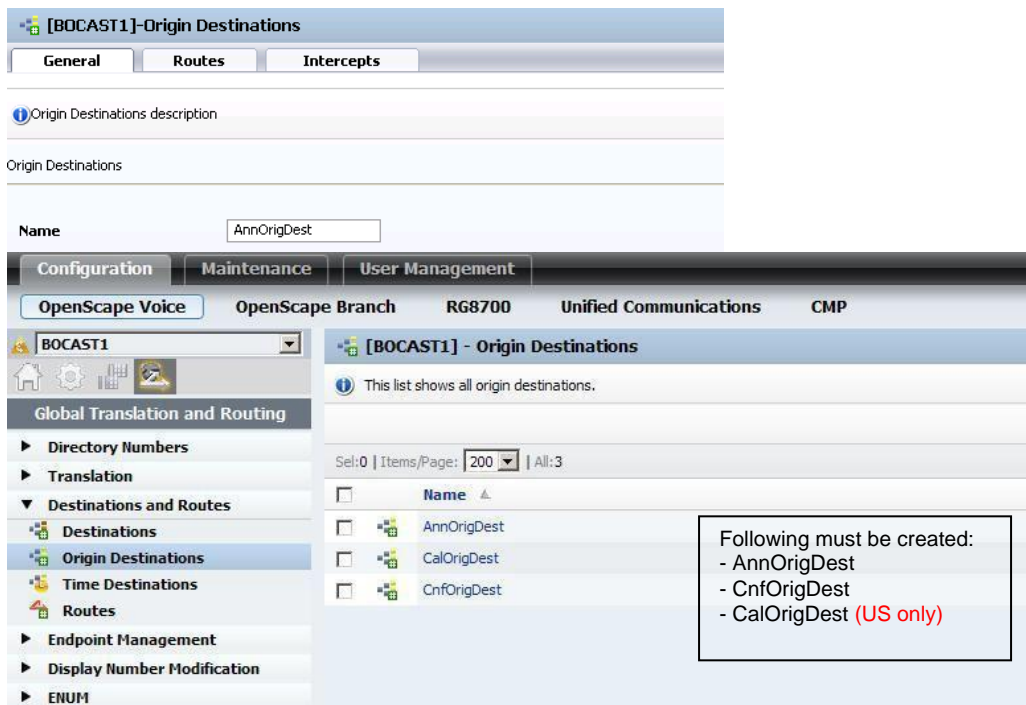
In the Circuits Section, you can configure the circuits of the media server.

Elements Per Page:

<input type="checkbox"/>	Circuit ID	Circuit End Id	Circuit Type
<input type="checkbox"/>	ann/\$	ann/\$	Announcement
<input type="checkbox"/>	cnf/\$	cnf/\$	Conference
<input type="checkbox"/>	es/\$	es/\$	Surveillance

Circuit Type: for media server. Possible circuit types Any, Announcement, Surveillance (US only), Conference, and Audit

- Create an **Origin** Destination for each traffic type: Announcements, Conference and Electronic Surveillance. OSV -> Global Translation and Routing -> Destinations and Routes -> Origin Destinations.



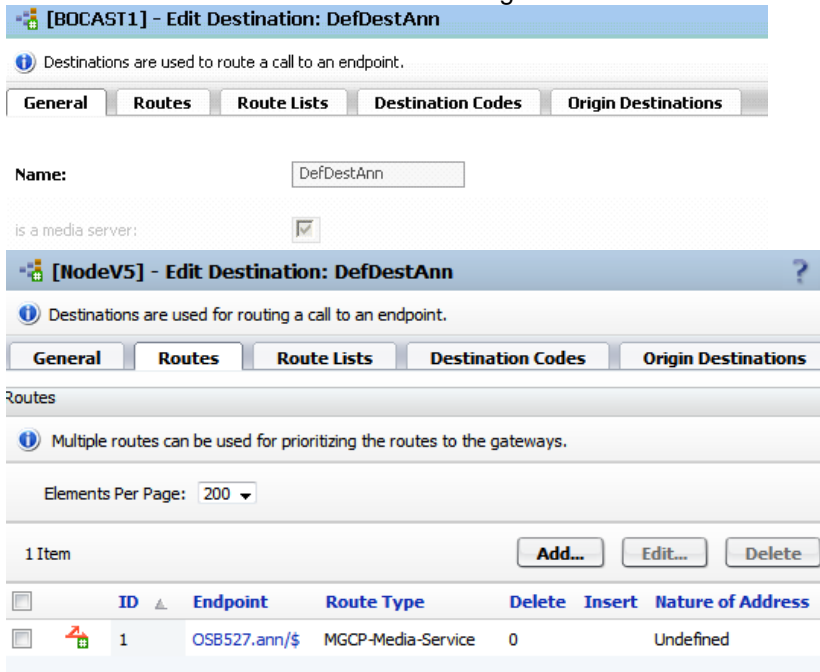
- Create **Default** Destinations for the main media server that will be used as default and for the Main Branch. The following must be created:

DefDestAnn

DefDestCnf

DefDestCal

OSV -> Global Translation and Routing -> Destinations and Routes -> Destinations



OSB configured as main media server

Or

[NodeV5] - Edit Destination: DefDestAnn

Destinations are used for routing a call to an endpoint.

General | **Routes** | **Route Lists** | **Destination Codes** | **Origin Destinations**

Routes

Multiple routes can be used for prioritizing the routes to the gateways.

Elements Per Page: 200

2 Items

Add... **Edit...** **Delete**

ID	Endpoint	Route Type	Delete	Insert	Nature of Address
1	MS1.ann/\$	MGCP-Media-Service	0		Undefined
2	OSB527.ann/\$	MGCP-Media-Service	0		Undefined

- If OSV has integrated media server, OSB can function as secondary media server for load balancing.
- If Prioritized is checked, the ID with the lowest value will always be used first until its unavailable.

General | **Routes** | **Route Lists** | **Destination Codes** | **Origin Destinations**

Route Lists

This list provides an overview of all routes with the same originating signaling type and bearer capability. Prioritization is possible.

1 Item

Originating Signaling Type	Originating Bearer Capability	Prioritized	Fallback to Local Numbering Plan	Prefix Area Code	Preface Country Code
Unassigned	Unassigned	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

- Do the same for default destination for conference and surveillance (DefDestCnf and DefDestCal).
- Add the **Default** Destination to the **Origin** Destinations as a Route
OSV -> Global Translation and Routing -> Destinations and Routes -> Origin Destinations -> Edit and go to the Routes Tab and press Add

Select the Default Destination Created. **Do not** enter a Routing Area

Note: When Routing Area is used only the matching Routing Area subscribers will have access to OSB Media Server.

[BOCAST1]-Origin Route

Routing Area:

Destination Type:

Destination Name:

[BOCAST1]-Origin Destinations

General | **Routes** | **Intercepts**

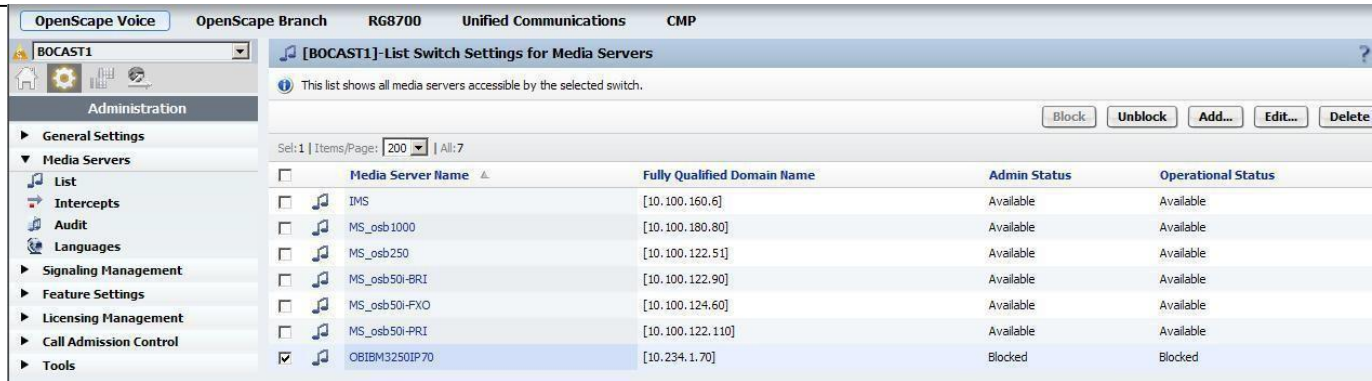
Origin Routes

Routes

Elements Per Page: 100

Routing Area	Destination Type	Destination Name
	Destination	DefDestAnn

- Unblock the Media server



Announcements for the Main Office (default) are now provided by OpenScapeBranch.

- Provision the treatments.

OSV provides media server script to add the treatments for the Media Server.

NOTE: The following instructions may change depending on the OpenScape Voice patch set level. For updated script information refer to the [OSV Media Server Configuration Instructions](#) or OSV “**OpenScape Voice V5, Configuration, Administrator Documentation**” or “**OpenScape Voice V5, Installation and Upgrades, Installation Guide**”.

The script is located at:

/unisphere/srx3000/srx/ms_scripts

Execute the script in the OSV by entering the following command (run as user “srx”):

sh msconf.sh

Select the following options:

- 11 to Assign the default treatments
- 3 to select Distributed Media Server Deployment
- Press “Enter” to assign treatments to the default Origin Destinations created or type the Origin Destination name(e.g. AnnOrigDest) and press “Enter”, for value different than Default, type the name and press “Enter”
- Press “y” to backup the current configuration of the treatments
- Press “y” to effect the selected modifications

Note: add the PAC codes in the respective numbering plan. The script provided with the system does not add PAC codes for you.

If default configuration is desired for all treatments, one can also remove all treatments and assign everything default.

46.2 Configuring OSB in the OSV as Branch Media Server

These steps are a continuation from the previous section.

Note: The Media Server for the Main Office (default) **must be created** prior to adding a branch media server following the steps described in the “Distributed Deployment with Branches” instructions available with the OSV manual “**OpenScape Voice V5, Configuration, Administrator Documentation**” or “**OpenScape Voice V5, Installation and Upgrades, Installation Guide**”..

The following steps will show how to configure an OpenScape Branch server as the Media Server for a Branch.

1. Add and Configure OpenScape Branch as a Media server following Steps from previous section.
2. Create a Routing Area for the branch.

Go to OSV -> Global Translation and Routing -> Translation

Routing Area Name

A Routing area might be the name of a location.

Name: RA527

Routing Area Codes

Codes used for routing and billing

New Codes: Add Codes

Elements Per Page: 200

0 Items Delete

Code

3. Destination for newly created Routing Area (announcement, conference and surveillance). Declare that it is a media server.

[NodeV5] - Add Destination

Destinations are used for routing a call to an endpoint.

General Routes Route Lists Destination Codes Origin Destinations

Name: Dest_OSB527cnf

is a media server: ☒

10 Items

Name	Media Server
DEST_RAGO_ANN	True
DEST_RAGO_CNF	True
DefDestAnn	True
DefDestCal	True
DefDestCnf	True
Dest_4113OB	True
Dest_OSB527ann	True
Dest_OSB527cal	True
Dest_OSB527cnf	True
Orig_Dest	True

4. Add Route to the Destination. Repeat for conference and surveillance.

[NodeV5] - Edit Destination: Dest_OS8527ann

Destinations are used for routing a call to an endpoint.

General Routes Route Lists Destination Codes Origin Destinations

Routes

Multiple routes can be used for prioritizing the routes to the gateways.

Elements Per Page: 200

1 Item

Add... Edit... Delete

ID	Endpoint	Route Type	Delete	Insert	Nature of Address
1	OS8527.ann/\$	MGCP-Media-Service	0		Undefined

5. Origin Destinations for each traffic type must have been created for the main Media Server (See previous section).

OSV -> Global Translation and Routing -> Destinations and Routes -> Origin Destinations.

Configuration Maintenance User Management

OpenScape Voice OpenScape Branch RG8700 Unified Communications CMP

BOCAST1

[BOCAST1] - Origin Destinations

This list shows all origin destinations.

Sel:0 | Items/Page: 200 | All:3

Name
AnnOrigDest
CalOrigDest
CnfOrigDest

6. Add the Routing Area to the Origin destination's routes. Repeat for conference and surveillance

[NodeV5]-Origin Destinations

General Routes Intercepts

Origin Routes

Routes

Elements Per Page: 200

5 Items

Add... Edit... Delete

Routing Area	Destination Type	Destination Name
RA527	Destination	Dest_OS8527ann
RA_MS1	Destination	Orig_Dest
RA_OBMS1205	Destination	DEST_RAG0_ANN
RA_OBMS4113	Destination	Dest_4113OB

Routing Area that was created

7. There are two ways to assign the OSB media server as a media server for a subscriber. The first is to assign the RA directly to the subscriber:

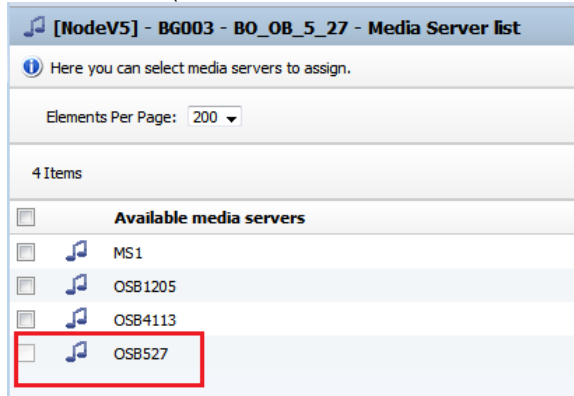
Openscape Voice -> Business group -> Members -> Subscribers -> edit Sub-> Routing Tab -> Assign Rate Area (Routing Area)

The screenshot shows the 'Edit Subscriber' form for subscriber 9546660007. The 'Routing' tab is selected. Under 'Routing Information', the 'Rate Area' field is highlighted with a red box and contains the value 'RA527'. Other fields include 'Numbering Plan' (NPBG003), 'Class of Service', and 'Calling Location Code'.

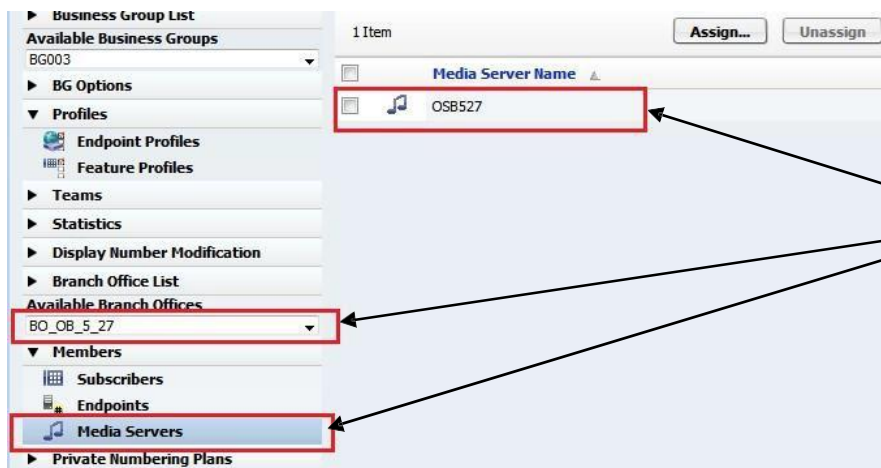
- i. The second way is to assign the Rate Area for the entire Branch: Assign the newly added Routing Area to the Endpoint Profile of the Proxy serving the Branch Office. OSV -> Business Group -> BG(x) -> Profiles -> Endpoint

The screenshot shows the 'Edit Endpoint Profile' form for profile EPP_OB527. The 'Endpoints' tab is selected. Under 'Endpoint Profile', the 'Name' field contains 'EPP_OB527'. Under 'Management Information', the 'Routing Area' field is highlighted with a red box and contains the value 'RA527'. Other fields include 'Numbering Plan' (NPBG003), 'Class of Service', 'Calling Location', 'Time Zone' (LOCAL), 'SIP Privacy Support' (Basic), and 'Failed Calls Intercept Treatment' (Disabled). The form has 'Save' and 'Cancel' buttons at the bottom.

- ii. Assign the Media Server that will serve the BranchOffice.
 - Go to OSV -> Business Group -> Members -> Media Servers and Press Assign and select the desired Media Server (Note: Branch Office of desired Media Server must be selected)



OpenScapeBranch is now configured to serve the Branch Office as Media Server.



OSB is now a default media server for all members of this branch

**Note: Can add more media servers for this branch in case the branch can't handle all the media server needs.

- iii. Edit Intercept Treatment for Conference
 Configuration ⑦ Openscape Voice -> Administration -> Media Servers -> Intercepts -> Conference -> Treatments -> Add

- iv. In cases that **another** OSB needs to be a media server, create another RA for each OSB (ex RAOSB2) and a separate destination for each (ex RAOSB2ann, RAOSB2cnf and RAOSB2cal).

v. Unblock the Media server (Branch Media Server configuration is completed)



Configuring the main Media Server as a backup of the Branch MS:

In some situations it may be desired to have the main media server as the backup of the branch media server. This is entirely done in the OSV using the Media Server audit mechanism and routing. The steps to configure this are as follow:

46.2.1 Enable Media Server Audit in the OSV

Via CMP go to Configuration OSV -> Administration -> Media Servers -> Audit

1. Enable the Media Server Audit by checking "Automatic Audit On":

[BOCAST1]-Media Server Audit

Set the audit configuration for the Media Server here.

Automatic Audit On: ☒

Heartbeat Interval (msec.):

Audit Thread Delay (sec.):

Audit Block Threshold:

Audit Unblock Threshold:

2. Create the Audit circuit in the Branch Media Server.

Go to Configuration OSV -> Administration -> Media Servers -> List and click on the desired Branch Media Server.

3. Go to the Circuits tab and add the new circuit

[BOCAST1]-Media Server Circuit

Here you can configure circuit attributes

Circuit Attributes

Circuit ID: Enter "aud/\$" as the Circuit ID

Circuit End Id:

Circuit Type: Select "Audit"

[BOCAST1]-Media Server

Configure Media Gateway Options

General **Extended** **Circuits**


Circuits

In the Circuits Section, you can configure the circuits of the media server.

Elements Per Page: 100

<input type="checkbox"/>	Circuit ID	Circuit End Id	Circuit Type
<input type="checkbox"/>	ann/\$	ann/\$	Announcement
<input type="checkbox"/>	aud/\$	aud/\$	Audit
<input type="checkbox"/>	cnf/\$	cnf/\$	Conference

4. Add Main Media Server as a second Route to the Branch Media Server

Via CMP open the Origin Destinations to get the Destination Name of the desired branch.
Go to Configuration  OSV -> Global Translation and Routing -> Destinations and Routes -> Origin Destination
the example below is for the created “AnnOrigDest”.

[BOCAST1]-Origin Destinations

General **Routes** **Intercepts**

Origin Routes

Routing Area used to route to the Branch


Corresponding Destination for the Branch

Routes

Elements Per Page: 100

<input type="checkbox"/>	Routing Area	Destination Type	Destination Name
<input type="checkbox"/>		Destination	DeDestAnn
<input type="checkbox"/>	bocaOB20_RA	Destination	DEST_RAG2_ANN
<input type="checkbox"/>	bocaOB21_RA	Destination	DEST_RAG3_ANN

5. Open the Destination from the above step.

Go to Configuration  OSV -> Global Translation and Routing -> Destinations and Routes -> Destinations

Go to the Routes Tab and press “Add” to add the main Media Server as a second Route

[BOCAST1] - Add Route

A route connects the destination with an endpoint representing a gateway.

ID

The Route ID indicates the priority level.

ID: 10

Type: MGCP Media Service

MGCP Media Service: IMS.ann/\$

Select and ID higher than the existing one used by the route to the branch MS.

Select “MGCP Media Service”.

Select the Main Media Server

The destination should have now 2 routes. One to the branch media server and the second (backup) to the main media server.

[BOCAST1] - Edit Destination: DEST_RAG3_ANN

Destinations are used to route a call to an endpoint.

General Routes **Route Lists** Destination Codes Origin Destinations

Routes

Multiple routes can be used for prioritizing the routes to the gateways.

Elements Per Page: 100

	ID	Endpoint	Route Type	Delete	Insert	Nature of Address
<input type="checkbox"/>	3	boca0821.ann/\$	MGCP-Media-Service	0		Undefined
<input type="checkbox"/>	10	IMS.ann/\$	MGCP-Media-Service	0		Undefined

Select the routes to be prioritized in the Route Lists tab

[BOCAST1] - Edit Destination: DEST_RAG3_ANN

Destinations are used to route a call to an endpoint.

General Routes Route Lists **Destination Codes** Origin Destinations

Route Lists

This list provides an overview of all routes with the same originating signaling type and bearer capability. Prioritization is possible

Originating Signaling Type	Originating Bearer Capability	Prioritized	Fallback to local Numbering Plan
Unassigned	Unassigned	<input checked="" type="checkbox"/>	<input type="checkbox"/>

Steps 4 and 5 must be done for all destinations types (announcements, conference, etc)

The Main Media Server is now the backup of the Branch Media Server. When the Branch Media server fails the audit mechanism of the OSV will set its Operational State to “Blocked” and will forward the requests to the Main Media Sever. The audit mechanism will keep trying until it gets a successful response from the Branch Media Server and it will set its Operational State back to “Available”.

46.2.2 Upload of Customized Media Server Announcements

1. Create a custom.mdp.zip file in the format as described in [INF-12-000239](#)

Note: File package.xml should be edited and version changed from 4.0.0 to 6.0.0.

2. Upload file to OSB /tmp folder using winscp

Note: if OSB Redundant system is installed then connect to physical IP address of Active/Master node.

3. Login to OSB SSH with root access and copy zip file from /tmp to /opt/siemens/mediaserver/application_host/deployment-custom

4. Verify files are synchronized to /opt/siemens/mediaserver/application_host/work/

It should not take more than 2-3 minutes.

5. The synchronization of the files on the redundancy system occurs automatically after 6 minutes

6. If the .wav file is new, configure your intercept treatment in CMP with the following address line: pa@*(an=[file:///~la/newmoh.wav](#) it=-1)

(where newmoh.wav is replaced by customer's announcement filename)

Note: The .wav files can be completely new or they can have the same name with an existing .wav file in the corresponding language. If the name of an existing announcement file is used in the customized package the corresponding announcement will be automatically replaced by Media Server.

7. For redundant systems only: restart the Active/Master OSB node and repeat steps 2 through 4

47.TLS Configuration

Configuring TLS in OpenScapeBranch as Proxy or SBC. Note: phones with TLS not supported in Proxy ACD mode.

47.1 Create TLS Certificate

Generate a Certificate Sign Request file (CSR)

1. Create the server configuration file (If not already available please refer to attachment section3)

Note: Regarding to the most common changed .cnf parameters, add default_md which can be changed from sha1 to sha256 or sha384:



2. Create the Certificate Sign Request using the osbserver.cnf configuration file from previous section. You will be prompted to enter organization information such as country, state, city and etc. The final prompt will ask for the common name. Enter the IP address or FQDN of the server here. This command will create a new key pair for osbserver and store the private key in osbserverkey.pem and enter the public key in a file called osbserver.csr.

```
openssl req -new -config osbserver.cnf -keyout osbserverkey.pem -out osbserver.csr
```

The above command will prompt for following information, enter the fields you need. If you enter '.', the field will be left blank.

Country Name (2 letter code) [US]:

State or Province Name (full name) [Florida]: Locality Name (eg, city) [Boca Raton]:

Organization Name (eg, company) [Your Company Ltd]: Organizational Unit Name (eg, section) []:

Common Name (eg, your name or your server's hostname) [OpenScape Branch's IP Address or domain name]:

Email Address [xyz@xx.com]:

If a new certificate needs to be issued, the stored certificate sign request file may simply be re-used. However, if modifications had to be made to the configuration file, then a new certificate sign request needs to be issued as follows after the modifications have been saved: from the config directory:

```
openssl req -new -config osbserver.cnf -keyout osbserverkey.pem -out osbserver.csr
```

Note: store the private key (eg: osbserverkey.pem) in a secure place as it will be required to install the certificates for OpenScapeBranch.

47.2 Submit the Certificate Sign Request file to the Certificate Authority

The signing CA may either be the CA of a customer's PKI or it may be the CA on an OpenScape Voice that functions as CA for the customer's communications solution. If a customer's PKI is used, simply transfer the file (e.g. using sFTP, e-mail) to the IT group responsible for the PKI and request a signed certificate. **Note:** User must not send the private key (osbserverkey.pem) to CA or anyone else that matters.

The same happens when the CA is on a OpenScape Voice. Following steps are needed if using the OSV Certificate Authority. Commands to be executed in the OSVSSH:

1. Obtain "root" permission in /tmp directory.
2. Copy osbserver.csr to /temp directory in OSV
3. Create rootcert.pem by using Certificate part only (Section from "-----BEGIN CERTIFICATE-----" to "-----END CERTIFICATE", not the Key)
4. from root.pem (/usr/local/ssl/certs/)
5. Sign certificate using rootcert.pem and key in root.pem of OSV
6. openssl x509 -req -in osbserver.csr -sha1 -CA rootcert.pem -CAkey
7. /usr/local/ssl/certs/root.pem -CAcreateserial -out servercert.pem -days3650
8. Copy rootcert.pem to serverCA.pem within temp directory.(osbserverkey.pem, osbservercert.pem and osbserverCA.pem

47.3 Download the Certificate from the Certificate Authority

The signing CA may either be the CA of a customer's PKI or it may be the CA on an OpenScape Voice that functions as CA for the customer's communications solution. If a customer's PKI is used, simply transfer the file (e.g. using sFTP, e-mail) from the IT group responsible for the PKI and store it in the /tmp/config directory or secure place. This file shall be the certificate signed by CA, which is named as osbservercert.pem. The same happens when the CA is on a OpenScape Voice. CA Certificate also needs to be downloaded.

Note: Please refer to attachment section 2 in case it is required to validate certificate from CA.

47.4 Upload TLS Certificates for OpenScapeBranch

Configuration:

OpenScape Branch > Branch Office > Configuration > Security > General > Certificate Management section > Configure

Certificate Creation

Create New TLS Certificates

Name CA file

Certificates Upload

CA Certificates

Upload CA certificate file Nenhum arquivo selecionado.

CA certificates

X.509 Certificates

Upload X.509 certificate file Nenhum arquivo selecionado.

X.509 certificates

Key Files

Upload key file Nenhum arquivo selecionado.

Key files

Select "CA Certificates", "Key File", or "X.509 Certificate" and Browse/OK to upload file.
Note: file upload is done one at a time.

1) From General Configuration tab/Certificate Upload section select Upload.
2) Select **Add** if new certificates are needed.

 Certificate management provisioning.

System SIP over TLS certificate profile OSV Solution

HTTPS certificate profile HTTPS System Default

Certificate Profiles

Profile name	Certificate service	Client certificate file	Server certificate file	Local CA file	Remote CA file	Local Key file
OSV Solution	SIP-TLS		servercert.pem	serverCA.pem		serverkey.pem
HTTPS System for iit	HTTPS		server.crt			server.key

Note: certificate profile called "OSV Solution" is available by default and contains a single certificate with the following files: servercert.pem, serverCA.pem and serverkey.pem. The OSB certificate file serverCA.pem matches the OSV's CA

Note: The OpenScapeBranch is installed with default Certificates generated using the default root certificate of OSV. New Certificate is required only if the root certificate of OSV changed or to add new parameters in the OpenScapeBranch certificate. NOTE: The Security Checklist recommends to never use the default certificate in the customer.

Certificate file [Download](#)

Key file [Download](#)

Certificate expiration warning period (days)	60
--	----

Certificate expiration warning interval (days) 7

Certificate expiration time of day (hh:mm) 00:00

Certificate Revocation List

Certificate expiration warning period (days): number of days before a certificate expires at which an alarm is generated to warn the administrator about the impending expiration of the certificate.

Certificate expiration warning interval (days): number of days after which to repeat the Certificate expirationwarning alarm.

Certificate expiration time of day (hh:mm): The time of day at which to run the certificate expiration check.

Add Edit Show CRL Delete

Name	CRL URL	CRL download interval	CRL short download interval	CRL time of day
------	---------	-----------------------	-----------------------------	-----------------

After editing the OSV Solution Profile we have:

Certificate Profile

i Select OK to temporarily store changes. Make your changes permanent by selecting 'Apply Changes' on the General page.

Certificate Profile configuration

Certificate profile name

OSV Solution

Certificate service

SIP-TLS

Local client certificate file

Show

Local server certificate file

servercert.pem

Show

Local CA file

serverCA.pem

Show

Remote CA file

Show

Local key file

serverkey.pem

EC param

secp256r1

Validation

Certificate Verification

None

☐ Revocation status

☐ Identity Check

Renegotiation

☐ Enforce TLS session renegotiation

TLS session renegotiation interval (minutes)

60

TLS version

Minimum TLS version

TLS V1.2

TLS V1.0

TLS V1.1

TLS V1.2

DTLS version

Minimum DTLS version

DTLS V1.0

Cipher Suites

Perfect Forward Secrecy

Preferred PFS

Encryption

Preferred AES-128

Mode of Operation

Preferred GCM

Edit and Select New
Certificates from Menus
and Press OK, then
Apply Changes.

NOTE1. Local client certificate file - this certificate shall be configured if OSB uses 2 different certificates for acting as a TLS client or TLS server.

NOTE2. Remote CA file - this certificate shall be configured if the remote endpoint uses a certificate from a different PKI than OSB.

Certificate Verification: Please refer to the FRN8423 which provides a description of the different verification levels.

48. Minimum TLS Version

Starting in V8R1, there are new definitions for Minimum TLS version and a new profile for HTTPS: Indicate the minimum version supported. Available options are TLS V1.2, TLS V1.1 and TLS V1.0.

In V10R2, after full installation, the default value for Minimum TLS version has been changed to TLS V1.2 in Certificate Profile.

It is still possible to select TLS V1.0 from menu.

Note: For security reasons SSLv23 and SSLv3 is not supported after V8R1

Minimum TLS Version Configured in OSS/ OSB	TLS Version in Remote Endpoint as Client	OSS as TLS Server	OSS as TLS Client. TLS Version offered to TLS server
TLSv1.0	TLSv1.2	Accept	TLSv1.2
	TLSv1.1	Accept	
	TLSv1.0	Accept	
	SSLv23/SSLv3	Reject	
TLSv1.1	TLSv1.2	Accept	TLSv1.2
	TLSv1.1	Accept	
	TLSv1.0	Reject	
	SSLv23/SSLv3	Reject	
TLSv1.2	TLSv1.2	Accept	TLSv1.2
	TLSv1.1	Reject	
	TLSv1.0	Reject	
	SSLv23/SSLv3	Reject	

Cipher Suites:

It's possible to define the groups of cipher suites which are supported for the endpoint associated to the certificate profile. The definition of the cipher suites is done by means of 3 parameters:

- Perfect Forward Secrecy – it defines the priority of the ephemeral Diffie-Hellman ciphers suites. This is a combo box with the following options: Preferred PFS (default) or WithoutPFS.
- Encryption – it defines the encryption cipher. Currently AES-128 is the most recommended option. This is a combo box with the following options: Preferred AES-128 (default), Required AES-256.
- Mode of Operation – it defines the encryption cipher mode of operation: CBC or GCM (TLS V1.2 only). This is a combo box with the following options: Preferred GCM (default), CBC only, GCM only.

Certificate Profile

Certificate Profile configuration.

Certificate Profile Configuration

Certificate profile name

HTTPS System Default

Certificate service

HTTPS

Local client certificate file

Show

Local server certificate file

server.crt

Show

Local CA file

Show

Remote CA file

Show

Local key file

server.key

EC param

secp256r1

Validation

Certificate Verification

None

☐

Revocation status

☐

Identity Check

Renegotiation

☐

Enforce TLS session renegotiation

TLS session renegotiation interval (minutes)

60

TLS version

Minimum TLS version

TLS V1.0

This profile defines the TLS version that will be used/accepted for HTTPS access to the branch

Chiper Suites

Perfect Forward Secrecy

Preferred PFS

Encryption

Preferred AES-128

Mode of Operation

Preferred GCM

48.1 Configuration of TLS in OpenScapeBranch/OSV

Note: Make Sure to set the OpenScapeBranch with current date/time of OSV.

1. Open the OSV Endpoint created for OpenScapeBranch and update Transport protocol/Port to MTLS/5061.

Configuration > OpenScape Voice > Business Group > BG > Members > Endpoints > SIP Tab

Note: Configure Endpoint as trusted if Digest Authentication is used in the OSV.

Route Via Proxy and **SIP Proxy** must be set. Survivable Endpoint must be set if subscriber rerouting is required for survivability.

OSB IP address must be configured for alias (Port is optional. Ex 10.234.1.70:5061). **Note:** if using OSB with Redundancy then Alias should include Redundant IP and Physical IP addresses for both OSB nodes.

Important: OSB always uses TLS port 5061 to connect OSV. Even configured as TLS, the connection is MTLS. Port 5061 must be used in order to set the endpoint OSB in the OSV configuration as well as port 5061 in the SIP server configuration in OSB.

[BOCAST1] - [BGLoad] - [Main Office] - Edit Endpoint : IBM3250-IP70

General SIP Attributes Aliases Routes Accounting

SIP-Q Signaling:

For the static Endpoints the address of the SIP signaling interface can be specified in IP or FQDN format. Note that the address of the signaling interface cannot be modified unless the entry in the security section has first been removed.

SIP Private Networking: ☐

SIP-Q Signaling: ☐

SIP Trunking: ☒

Type: Static

Signaling Binding Type: IP Address or FQDN

Signaling Binding Address: 10.234.1.70

Port: 5061

Transport protocol: MTLS

TCP:5060,UDP:5060, TLS:5061, MTLS:5061

2. Configure Keep Alive to OSV to use TLS port (5061) in the OpenScapeBranch. Configuration OpenScape Branch > Branch Office > Configuration > VoIP > General

Voice over IP

Select OK to temporarily store changes. Make your changes permanent by selecting 'Apply Changes' on the General page.

General Comm System Timers and Thresholds Codecs RTP

SIP

General

Mode: Proxy

Manipulation... Routing... Error Codes...

Call Forward...

Listening ports

TCP: 5060 UDP: 5060 TLS: 5061

Options Source Port: 5061

Update Options Destination Port to 5061

3. Configure required OSV SIPSM IPs in the OpenScapeBranch.

Configuration > OpenScape Branch > Branch Office > Configuration > VoIP > SIP Server Settings

VOIP

Select OK to temporarily store changes. Make your changes permanent by selecting 'Apply Changes' on the General page.

Sip Server Settings | Port and Signaling Settings | Manipulation and Routing | Error Codes | Media

General

Comm System Type: geo-separated

OPTIONS source port: 5060

IP Version Towards SIP Server: IPv4

☒ Enable path tagging

☐ Branch behind SBC

☐ Branch behind NAT

☐ Synch subscriber data

☐ Disable notification in survivable mode

☐ Enforce minimum Subscriber TransportType Security

Other trusted servers | Load Balance Mapping Table

Node 1

Target type: Binding

Primary server: 10.100.182.56 | Transport: TLS | Port: 5061

Backup server: | Transport: TCP | Port: 5060

SRV record: | Transport: TCP

Node 2

Target type: Binding

Primary server: 10.100.183.57 | Transport: TLS | Port: 5061

Depending on the Comm System Type (Simplex, Collocated, Geo Separated) and OSV Release, different IPs are required in the configuration. See OSB TLS/TCP/UDP configuration table below.

Important: OSB always uses TLS/MTLS on port 5061. Even configured as TLS, the connection is MTLS and port 5061 is used.

TCP/UDP Port 5060		OSV Mode	TLS/MTLS Port 5061	
OSV 3.1/4.0	OSV 4.1/5/6/7/8/9/10		OSV 3.1/4.0	OSV 4.1/5/6/7/8/9/10
Simplex				
sipsm1_vip	sipsm1_vip	Node 1 Primary Server	sipsm3_vip	sipsm3_vip
Collocated				
sipsm1_vip	sipsm1_vip	Node 1 Primary Server	sipsm3_vip	sipsm3_vip
		Node 1 Secondary Server		
sipsm2_vip	sipsm2_vip	Node 2 Primary Server	sipsm4_vip	sipsm4_vip
		Node 2 Secondary Server		
Geo-Separated				
sipsm1_vip	sipsm1_vip	Node 1 Primary Server	sipsm3_vip	sipsm3_vip
sipsm2_vip2	sipsm2_vip	Node 1 Secondary Server	sipsm4_vip2	sipsm4_vip
sipsm2_vip	sipsm2_vip	Node 2 Primary Server	sipsm4_vip	sipsm4_vip
sipsm1_vip2	sipsm1_vip	Node 2 Secondary Server	sipsm3_vip2	sipsm3_vip

-
4. Enable RTP Parameter for connectivity check (Note: only possible in certain OSV versions (Newer versions of OSV is enabled by default). Srx/Sip/ServerVersionEnable = RTPTrue

The RTP parameter can be set by verifying the Configuration -> OpenScape Voice -> Administration -> Signaling Management -> Digest Authentication -> General Tab (click: Enable TLS Keep-Alive for OpenStage phones).

48.2 Configuration of MTLS in OpenScapeBranch/OSV

Configuration in OSV V8 when configuring MTLS in OSB V9

From an OSV V8 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.

NOTE: 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/50i configured as Proxy/Gateway

- Configure EP for OSB Proxy with transport protocol MTLS

This endpoint should be configured with **Route Via Proxy** and **SIP Proxy** enabled. **Survivable Endpoint** must be set if subscriber rerouting is required for survivability.

OSB IP address must be configured for alias (Port is optional. Ex 10.234.1.70:5061). **Note:** if using OSB with Redundancy then Alias should include Redundant IP and Physical IP addresses for both OSB nodes.

Important: OSB always uses TLS/MTLS on port 5061. Even configured as TLS, the connection is MTLS and port 5061 is used.

- Configure EP for OSB 50i/500i Integrated Gateway NET5/NI2/CAS E1/CAS T1 with transport protocol UDP (alias should have <FQDN>:5096)

Note: OSB 50i/500i integrated gateway endpoint must be created behind a Proxy Endpoint. So it should have as associated endpoint EP for OSB Proxy.

- Configure EP for OSB 50i/500i Integrated Gateway Qsig / Cornet with transport protocol TCP (alias should have <FQDN>:5096)

Note : OSB 50i/500i Integrated gateway endpoint must be created behind a Proxy Endpoint.

So it should have as associated endpoint EP for OSB Proxy.

OSB50i/OSB500i Integrated Gateway End Point should be configured with Attribute Public/Offnet Traffic.

Do not Send Invite without SDP attribute must NOT be selected on OSB50i/OSB500i Integrated Gateway End Point. OSB IP address and port 5096 must be configured for alias (Ex 10.234.1.70:5096).

Note : if using OSB with Splitterbox Configuration (PRI Redundancy) then Alias should include Redundant IP and Physical IP addresses for both OSB nodes.

Example 2: OSB 500i/50i configured as GW only:

- Configure EP for OSB Proxy with transport protocol MTLS

This endpoint should be configured with Attributes “Route Via Proxy” and “SIP Proxy” must be set. Attribute “Survivable Endpoint” must be set if subscriber rerouting is required for survivability.

OSB IP address must be configured for alias (Port is optional. Ex 10.234.1.70:5061).

Important: OSB always uses TLS/MTLS on port 5061. Even configured as TLS, the connection is MTLS and port 5061 is used.

Note: if using OSB with Redundancy then Alias should include Redundant IP and Physical IP addresses for both OSB nodes.

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
- OSB 50i/500i Integrated Gateway Qsig / Cornet with transport protocol TCP or TLS (alias should have
- <FQDN>:5096)

Note: OSB 50i/500i integrated gateway endpoint must be created behind a Proxy Endpoint. So it should have as associated endpoint EP for OSB Proxy.

Note: Attribute Route via Proxy to route the calls via the associated endpoint. Attribute Public/ Offnet Traffic must be also enabled.

OSB50i/OSB500i Integrated Gateway End Point should be configured with Attribute Public/Offnet Traffic.

Do not Send Invite without SDP attribute must NOT be selected on OSB50i/OSB500i Integrated Gateway End Point.

OSB IP address and port 5096 must be configured for alias (Ex 10.234.1.70:5096).

Note: if using OSB with Splitterbox Configuration (PRI Redundancy) then Alias should include Redundant IP and Physical IP addresses for both OSB nodes.

IMPORTANT: Do not Send Invite without SDP attribute must NOT be selected on OSB50i/OSB500i Integrated Gateway EndPoint

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.

Note: If a 500i/50i GW only is connected directly to an OSV with a single EP, the possible configurations are UDP, TCP or TLS.

Note: 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.

48.3 Configuration of TLS in Phones

SIP interface
Outbound proxy ☒
Default OBP domain
SIP transport **TLS**
Response timer (ms) 32000
NonCall trans. (ms) 32000
Reg. backoff (seconds) 60
Connectivity check timer (seconds) 10
Submit **Reset**

Update Transport to TLS
(Outbound Proxy Flag is Checked)

Registration
SIP Addresses
SIP server address 10.234.3.109
SIP registrar address 10.234.3.109
SIP gateway address 10.234.1.70

TLS OSV IPs and OSB IPs configured.
Note: if phones configured with different sipsm IP address as OSB then this address must be included in OSB trusted list (ex. OSB configured with sipsm3 and phones with sipsm1. In this case sipsm1 must be configured on trusted list of OSB.)

Port configuration
SIP server 5061
SIP registrar 5061
SIP gateway 5061
SIP local 5061
Backup proxy 5060
RTP base 5010
Download server (default) 21
LDAP server 389
HTTP proxy 0
LAN port speed Automatic
PC port speed Automatic
PC port mode disabled
PC port autoMDIX ☐
Submit **Reset**

Update Port Configuration
from 5061 to **5161**.
Note: For debugging the TLS Packets between phone and OpenscapeBranch set SIP Local Port to a value other than 5161 (ex. 6061).

ConnectivityCheckInterval
should be less than 240 secs.
Note: It is better to keep the value to 10 seconds, which will cause the phone to reattempt the TLS connection in 10 seconds if no response from OSB.

Security
SIP server certificate validation ☐
Backup SIP server certificate validation ☐
Use secure calls ☒
Submit **Reset**

Secure Calls flag is checked.

Secure Calls should be checked for SRTP

Phone Transport and Port have to be updated to TLS/5161. Note: Time/Date has to match also with OSV and OSB.

48.4 Tracing with TLS

User can collect decoded traces from Logging menu by selecting the SIP/MGCP option from the Network Tracer Menu. System collects decoded TLS traces from OSB with this option.

Configuration > OpenScape Branch > Branch Office > Configuration > Diagnostics & Logs > Debugging

Note: Errors "No open TLS connections found" and "TLS Client Connection only for Trusted IP's" Will show in sipserver log when OSB is restarted.

Diagnostics & logs

Select OK to temporarily store changes. Make your changes permanent by selecting 'Apply Changes'

Settings **Debugging** **Continuous Tracing** **On Demand Trace** **Statistics**

Log Viewer

Log data: Alarm History [v] [Show] [Clear] [Clear all logs]

Debugging Tools

Tool: Network Tracer [v]

Interface: All interfaces [v]
All interfaces
SIP/MGCP/Q931 Trace
SIP/MGCP/Q931/InterworkingRTP Trace

Results: [View] [Export]

Rapid Stat

Info level: Level 2 [v] [Get file]

- 1) Select Network Tracer
- 2) Select interface (SIP/MGCP)
- 3) Click on start
- 4) Click on stop
- 5) Press Export to get *.cap file. Traces are automatically decoded using this option.

49 Certificate verification process compliant with Baseline Security Policy

This feature introduces the adaptation of specific certificate verification levels according to Baseline Security Policy document. Please check the certificate management session.

The main implementation is the addition of the certificate verification levels as shown on picture below

Configuration > OpenScope Branch > Branch Office > Configuration > Security > General > Certificate Management > Certificate Profile

The screenshot shows the 'Certificate Profile' configuration window. It has a title bar 'Certificate Profile' and a subtitle 'Certificate Profile configuration.' Below this, there are several configuration fields:

- Certificate profile name:** OSV Solution
- Certificate service:** SIP-TLS
- Local client certificate file:** (empty dropdown) with a 'Show' button.
- Local server certificate file:** servercert.pem with a 'Show' button.
- Local CA file:** serverCA.pem with a 'Show' button.
- Remote CA file:** (empty dropdown) with a 'Show' button.
- Local key file:** serverkey.pem
- EC param:** secp256r1

Below these fields is a 'Validation' section:

- Certificate Verification:** A dropdown menu with 'None' selected. The dropdown is open, showing 'None', 'Trusted', and 'Full'.
- ☐ **Revocation status**
- ☐ **Identity Check**

50 Special characters in P-Preferred Identity of SIP INVITE

This feature introduces the allowance of special characters on default Home DN and the addition of the new flag “Mandatory default Home DN – Normal Mode”

Configuration > OpenScape Branch > Branch Office > Configuration > Features > Sip Service Provider profiles

The screenshot shows the 'SIP Service Provider Provisioning' configuration window. It has a title bar with a blue icon and the text 'SIP Service Provider Provisioning.'. Below the title bar is a tabbed interface with two tabs: 'General' and 'Home DN'. The 'General' tab is active and contains the following fields and options:

- Name:** A text input field.
- Default SSP profile:** A dropdown menu.
- Options (checkboxes):**
 - ☐ Allow sending of insecure Referred-By header
 - ☐ Send authentication number in Diversion header
 - ☐ Send P-Preferred-Identity rather than P-Asserted-Identity
 - ☐ Send authentication number in P-Asserted-Identity header
 - ☐ Do not send Diversion header
 - ☐ Send authentication number in From header
 - ☐ Send URI in telephone-subscriber format
 - ☐ Include restricted numbers in From header
 - ☐ Use SIP Service Address for all identity headers
- SIP service address:** A text input field.
- Privacy support:** A dropdown menu with 'Full' selected.

The 'Home DN' tab is also visible and contains the following fields and options:

- Options (checkboxes):**
 - ☐ Mandatory default home DN
 - ☐ Mandatory default home DN - Normal Mode
- Default home DN:** A text input field.

51 OpenScape Branch SRTP Interworking and Codec Transcoding Configuration

This feature allows to use the OSS transcoding functionalities in the OSB V8.

The user can configure a different Media Profiles for Gateway on WAN side:

- **Enable LAN-WAN media interwork** under **Features** Tab.
Enables media interworking between LAN and WAN side when they are configured with different media profiles.

The **Configure** button shall be enabled only if **Enable LAN-WAN media interwork** is enabled. If so, the **Configure** button directs to the VOIP > Media.

Default: Unchecked

Features

Select OK to temporarily store changes. Make your changes permanent by selecting 'Apply Changes' on the General page.

Features Available in Normal Mode and Survivability Mode

- ☒ Enable gateways/trunks **Configure**
- Sip Service Provider profiles **Configure**
- ☒ Enable auto attendant **Configure**
- ☐ Enable Voice Mail Service **Configure**
- ☐ Enable phone software management **Configure**
- ☐ Enable Media Server / Streaming **Configure**
- ☒ **Enable LAN-WAN media interwork** **Configure**
- ☒ Enable Codec Support for transcoding **Configure**
- Emergency calling **Configure**

Features Available in Survivability Mode Only

- Multi-line Hunt Groups **Configure**
- Call Forwarding **Configure**
- ☒ Enable Call Detail Records **Configure**

VOIP

Select OK to temporarily store changes. Make your changes permanent by selecting 'Apply Changes' on the General page.

Sip Server Settings | Port and Signaling Settings | Manipulation and Routing | Error Codes | **Media**

Media Handling

- ☐ Allow multiple media lines for the same media type
- ☐ Replace the SDP Origin (o) field
- ☒ Reset SRTP context upon key change
- ☐ Use single bridge/port for audio media

LAN/WAN Media Configuration

Media profile: lgw_features_lan

Media Profiles

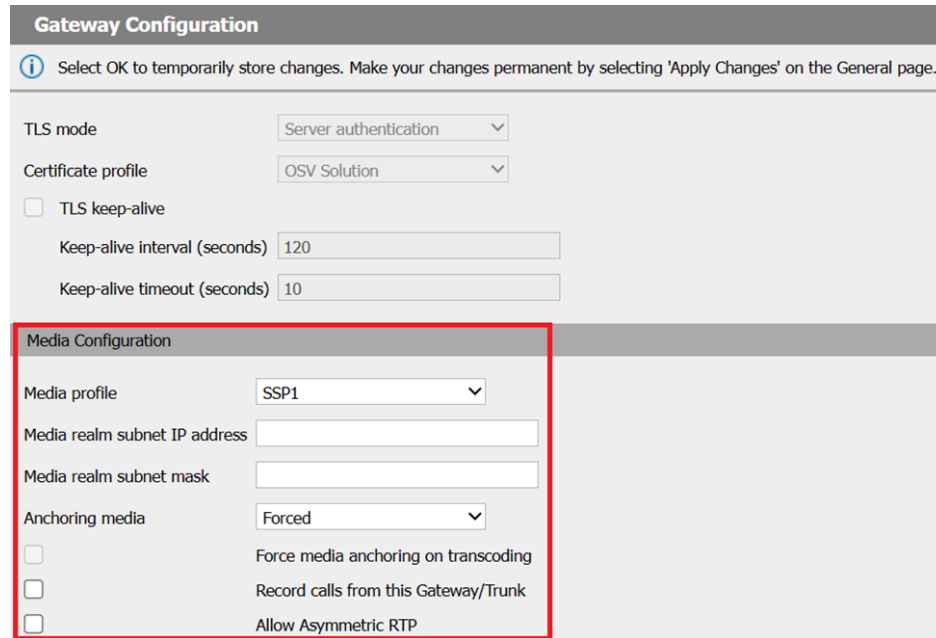
Name	Codecs	Media protocol	SRTP crypto context negotiation	Mark SRTP Call-leg
default		Strict Pass-Thru	none	
lgw_features_lan	G711A,G711U	Strict Pass-Thru	none	
SSP1	G711A,G711U	Best Effort SRTP	sdes	✓
SSP2	G711A,G711U	Best Effort SRTP	sdes	✓

After configuring the desired Media profile, with the “Enable LAN-WAN media interwork” flag enabled, it is possible to associate the Media Profile with a “Gateway/Trunk”.

1. Navigate to the **Features** tab.
2. Enable the "Enable gateways/trunks" flag.
3. Click **Configure**.
4. Select the line of the desired 'gateway' entry and click **Edit**.

A new **Gateway Configuration** window is displayed:

5. Navigate to **Media Configuration** → **Media profile**



The screenshot shows the 'Gateway Configuration' window. At the top, there is a header bar with the title 'Gateway Configuration'. Below the header, a message states: 'Select OK to temporarily store changes. Make your changes permanent by selecting 'Apply Changes' on the General page.' The main configuration area is divided into two sections. The first section contains settings for TLS mode (set to 'Server authentication'), Certificate profile (set to 'OSV Solution'), and a checkbox for 'TLS keep-alive'. Below this, there are input fields for 'Keep-alive interval (seconds)' (set to 120) and 'Keep-alive timeout (seconds)' (set to 10). The second section, titled 'Media Configuration', is highlighted with a red rectangular box. This section includes a 'Media profile' dropdown menu (set to 'SSP1'), two empty input fields for 'Media realm subnet IP address' and 'Media realm subnet mask', and an 'Anchoring media' dropdown menu (set to 'Forced'). At the bottom of the 'Media Configuration' section, there are three unchecked checkboxes with corresponding labels: 'Force media anchoring on transcoding', 'Record calls from this Gateway/Trunk', and 'Allow Asymmetric RTP'.

Gateway Configuration

Select OK to temporarily store changes. Make your changes permanent by selecting 'Apply Changes' on the General page.

TLS mode: Server authentication

Certificate profile: OSV Solution

☐ TLS keep-alive

Keep-alive interval (seconds): 120

Keep-alive timeout (seconds): 10

Media Configuration

Media profile: SSP1

Media realm subnet IP address:

Media realm subnet mask:

Anchoring media: Forced

☐ Force media anchoring on transcoding

☐ Record calls from this Gateway/Trunk

☐ Allow Asymmetric RTP

Media Profile

Media Profile

Select OK to temporarily store changes. Make your changes permanent by selecting 'Apply Changes' on the General page.

General

Name:

Media protocol:

SRTP configuration

SRTP crypto context negotiation:

☐ Mark SRTP Call-leg as Secure

☐ Single to-line SRTP

Codec configuration

☒ Allow unconfigured codecs

☐ Enforce codec priority in profile

☐ Send Telephony Event in Invite without SDP

Packratization interval:

Codec:

Priority	Codec Name
1	G711A 8 kHz - 64 kbps
2	G711U 8 kHz - 64 kbps
3	G729 8 kHz - 8 kbps

General

- **Name**
A unique profile name can be entered.
- **Media protocol**
The user chooses between unsecure and secure RTP or if the payload is passed through
Values: 'Strict Pass-Thru', 'Best Effort SRTP', 'SRTP Only', 'RTP'.
Default value: 'Strict Pass-thru'

See the SRTP crypto context negotiation in Table 1: SRTP crypto context negotiation:

Media protocol value	Possible SRTP crypto context negotiation values	default
Strict Pass-Thru	none	none (grayed out)
Best Effort SRTP	mikey , sdes , mikey+sdes	mikey
SRTP only	sdes , dtls (ansible only)	sdes
RTP	none	none (grayed out)

Table 1: SRTP crypto context negotiation

SRTP Configuration

- **Mark sRTP call-leg as secure**
Marks the FXS leg (or the iGW endpoint) as secure independent of the actual payload security
Default value: Unchecked
- **Single m-line SRTP**
Indicates if the key exchange mechanism is negotiated with a single or dual m-line SDP.
This check box shall be deactivated for this FRN. In future versions it might be configurable if single m-linekey negotiation is required.
Default value: Unchecked

The behavior of the Media Profile configuration parameters and their respective default values are summarized in Table 2: LAN WAN Media Interwork Disabled.

Parameter	Proxy (*)	Proxy-SBC	Branch SBC
VOIP→Media→LAN	Gray out / <u>igw_lan</u>	Gray out / <u>igw_lan</u> For NATed media, it is passed thru.	Gray out / <u>igw_lan</u> For NATed media, it is passed thru.
VOIP→Media→WAN	<not displayed>	<not displayed>	Gray out / wan Internally "default" (pass-thru) is used.
Gateway/Trunk (LAN)	Gray out / <u>igw_lan</u>	Gray out / <u>igw_lan</u> For NATed media, it is passed thru.	Gray out / <u>igw_lan</u> For NATed media, it is passed thru.
Gateway/Trunk (WAN)	<not possible>	Gray out / default For NATed media, it is passed thru.	Gray out / default For NATed media, it is passed thru.

Parameter	Proxy (*)	Proxy-SBC	Branch SBC
VOIP→Media→LAN	<not applicable>	Gray out / <u>igw_lan</u>	Gray out / <u>igw_lan</u>
VOIP→Media→WAN	<not applicable>	<not displayed>	Configurable / wan
Gateway/Trunk (LAN)	<not applicable>	Gray out / <u>igw_lan</u> For LAN – LAN (non IGW) call: no media interwork For LAN – IGW call: <u>igw_lan</u> is used For WAN – LAN/IGW call: <u>igw_lan</u> is used.	Gray out / <u>igw_lan</u> For LAN – LAN (non IGW) call: no media interwork For LAN – IGW call: <u>igw_lan</u> is used For WAN – LAN/IGW call: <u>igw_lan</u> is used.
Gateway/Trunk (WAN)	<not applicable>	Configurable / default	Configurable / default

Table 2: LAN WAN Media Interwork Disabled

(*) Notice that the flag “Enable LAN-WAN codec interwork” is not relevant for mode Proxy.

The media profile “default” is not configurable in order to avoid confusion for the user. For construction reason the media profile “default” has effect on integrated gateway calls in proxy mode even if the configured media profile for the integrated gateway is igw_lan. However, the media profile “default” is the default value for Gateway / Trunk on the WAN, so if different values are required for its media profile, the user shall create a new media profile.

Features tab > Gateways/Trunks tab > Gateway Configuration tab > Media Configuration

Gateway Configuration

Select OK to temporarily store changes. Make your changes permanent by selecting 'Apply Changes' on the General page.

Media Configuration

Media profile: mediaTest

Media realm subnet IP address:

Media realm subnet mask:

Anchoring media: Forced

☐ Force media anchoring on transcoding

☐ Record calls from this Gateway/Trunk

☒ Allow Asymmetric RTP

OK Cancel

Once the Enable Lan-SSP media interwork flag is set, the Media Configuration will be allowed when a SIP Trunk is added to the gateway table.

The items in that section are only configurable when the Enable LAN-SSP media interwork flag is set and the gateway is in the WAN.

- **Media profile**

Assign a media profile that has been created in the 'Media profiles' tab of the 'Voice over IP screen'.

Default: For the parameter definition and default value, see in Table 2: LAN WAN Media Interwork Disabled.

- **Media realm subnet IP address**

Enter the IP address or subnet for which media is anchored.

Default value: Empty

- **Media realm subnet mask**

Enter the subnet mask if a subnet is configured for media anchoring.

Default value: Empty

NOTE: The fields **Media Profile**, **Anchoring Media**, **Media realm subnet IP address** and **Media realm subnet mask** shall be grayed out if:

- LAN-WAN interworking is deactivated or
- LAN-WAN interworking is activated and Interface = 'LAN'

- **Anchoring media**

Choose if media anchoring for gateway / trunk calls is enforced or decided by the OSB.

Possible values: **forced**, **auto**.

Default value: **forced**

- **Force media optimization on transcoding**

Enables media optimization when media is not anchored and transcoding is active.

Default: Unchecked

Disabled: If 'Anchoring Media' is set to 'forced'

WAN GWs/SSPs entries that use the same FQDN or IP in the remote URL field, need to also be assigned the same "Media profile", "Media realm subnet IP address" (if any), "Media realm subnet IP address" (if any), "Anchoring media" value and "Force media optimization on transcoding" flag value.

- **Record calls from this Gateway/Trunk**
Enables recording using SIPREC protocol for this specific gateway.
Default is unchecked.

NOTE: This flag interacts with flag Voip > Media > Record All Calls. Please refer to the help section for the complete description.

- **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.

Asterisk non-integrated gateway features (like Auto-Attendant, MLHG, ACD or Call Park) have some special requirements regarding to RTP / SRTP:

- For calls to ACD, SRTP cannot be used because media is anchored in Asterisk for the duration of the call.
- For calls to AA, SRTP cannot be used while playing the AA announcements but it is possible after the call is transferred.
- For calls to MLHG, SRTP can be used. Media is not anchored by Asterisk.

SRTP Configuration

IMPORTANT: When the selected BCF ICE-priority is Passthrough, the SRTP configuration is disabled. All fields are disabled and all flags revert to default state.

SRTP crypto context negotiation - following the option selected between the three flags for the Media protocol selected, except for "Strict Pass-Thru"

- **MIKEY** - Multimedia Internet KEYing
- **SDES** - Security Descriptions Mark (ciphers supported: AES 128, AES 256, both)
- **DTLS** - Datagram Transport Layer Security

Mark sRTP Call-leg as Secure - Checkmark the checkbox, if calls require secure media. When active, this parameter identifies the network as secure if TLS and SRTP are not used, i.e., TCP or UDP for the signaling transport or RTP is used for the media protocol.

INFO: It is possible to see whether the SDP offer will have a single m-line SRTP, based on the media profile configuration. This information is in the media profiles table (Voip > Media > Media Profiles).

When using SRTP Only as media protocol and only one Packetization Interval for all configured codecs, the SDP offer will have one SRTP m-line.

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

INFO: 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.

INFO: When configured to generate RTCP, there is no SRTP pass-through, since the media application needs to encrypt the generated RTCP.

Media Profile

Select OK to temporarily store changes. Make your changes permanent by selecting 'Apply Changes' on the General page.

General

Name

Media protocol

☐ SDP Compatibility Mode

SRTP configuration

SRTP crypto context negotiation
 ☐ MIKEY
 ☐ SDES

☐ Mark SRTP Call-leg as Secure

RTCP configuration

RTCP Mode

RTCP generation timeout

Codec configuration

☐ Allow unconfigured codecs

☐ Enforce codec priority in profile

☐ Send Telephony Event in Invite without SDP

☐ Use payload type 101 for telephony event/8000

Codec

Priority	Codec	Packetization interval
1	G711A 8 kHz - 64 kbps	Auto
2	G711U 8 kHz - 64 kbps	Auto

52 Media Transcoding

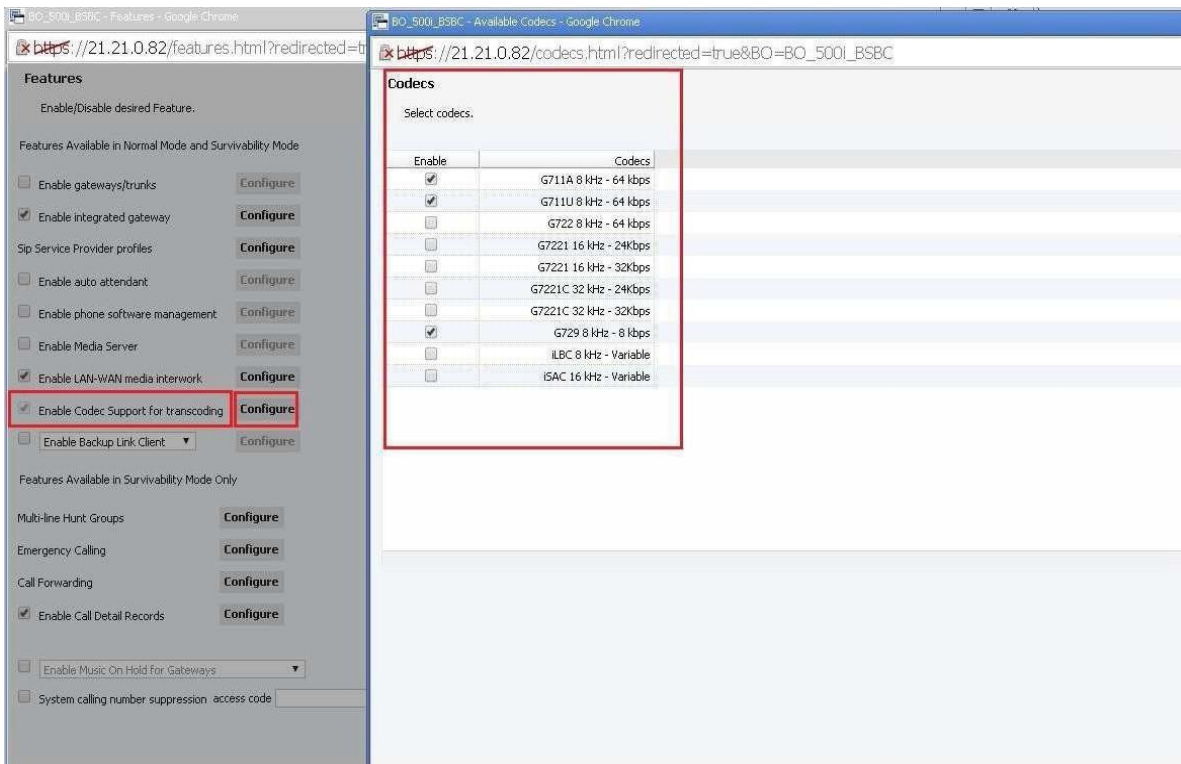
The OSB shall support media transcoding according to FRN 4358 The rules for the media profile are the same as defined in the table on page 111.

Enable Codec Support for Transcoding checkbox was created in **Features Tab**.

Description: Enables the codecs that can be selected in media profiles configuration.

The **'Configure'** button next to this check box shall be enabled only if the check box is enabled.

Default: Unchecked



In Media Profiles section configure the codecs:

5. A dropdown list 'Codec' and an 'Add' button

Description: The user can select a codec and add it to the list of codecs.

Values: Available codecs are listed below. If a codec is already in the list of codecs for this codec profile then it shall not appear in the drop-down list for adding codecs.

Support Intel IPP lib for codecs:

G.711 PCMA/PCMU

G.729 AB Functions

G722 Sub-Band ADPCM Speech Codec Functions

Support media transcoding with webrtc lib (or equivalent) for codecs:

iLBC

iSAC

List of codecs

Description: The list shows the codecs in order of priority chosen for the mediaprofile.

Buttons Move Up and Move Down

Description: Change prioritization of the listed codecs.

Button Delete

Description: Remove codec from the list

For each codec in the list there shall be also a drop down list '**packetization Interval**' next to each codec name in order to select the packetization interval with the following available options: 10ms, 20ms, 30ms, 40ms, 50ms, and 60ms and pass-through (auto) with **default value auto**.

A check box **Enforce codec priority in profile**

Description: If checked the order of the received SDP offer shall be replaced by the order of the media profile configured for the B-side

Default: False



Note: The check box shall not be checked together with the 'Allow unconfigured codecs' check box.

A check box Allow unconfigured codecs


Description: 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

Default: True

Note: The check box shall not be checked together with the 'Enforce codec priority in profile' check box.

 **Media Profile** 

Select OK to temporarily store changes. Make your changes permanent by selecting 'Apply Changes' on the General page.

General


Name

default

Media protocol

Strict Pass-Thru

☐ SDP Compatibility Mode


SRTP configuration

SRTP crypto context negotiation

☐ MIKEY ☐ SDES

SDES AES-128 only

☐ Mark SRTP Call-leg as Secure


RTCP configuration

RTCP Mode

Bypass

RTCP generation timeout

4

Codec configuration

☐ Allow unconfigured codecs

☐ Enforce codec priority in profile

☐ Send Telephony Event in Invite without SDP

☐ Use payload type 101 for telephony event/8000

Codec

G729 8 kHz - 8 kbps

Add

Move up

Move down

Delete

Priority	Codec	Packetization interval
1	G711A 8 kHz - 64 kbps	Auto
2	G711U 8 kHz - 64 kbps	Auto

53 Security enhancements

OSB supports the security enhancements (message rate limiting and quarantine):

Drop Down box '**Message Rate Limit (sec)**' was created in **Network / Net Services Tab / Settings' tab**

Interface 2 (WAN)

section Values:

5,10,25,50,75,100

Description: Select message rate limit per second for the SIP listening IP:port for the WAN interface

Default value: 100.

Drop Down box '**Trust Level**' was created in **Network / Net Services Tab / Settings' tab**

Interface

ce 2 (WAN) section

Values: 'N/A', 'Minimal', 'Medium'

Description: This pull-down 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 RateLimit":

Default value: 'N/A'

WAN configuration

Type	Interface	IP address	Subnet mask	VLAN tag	UDP port	TCP port	TLS port	Message rate limit (sec)	Trust level
Main IPv4	eth1	21.21.0.82	255.255.0.0	0	S060	S060	S061	100	N/A

Routing

Default gateway address: 21.21.0.1

Routing configuration

Row	Destination	Gateway	Netmask	Interface
-----	-------------	---------	---------	-----------

The new 'Denial of service mitigation' tab was created in Security tab.

The following parameters are configured in the "Denial of Service Mitigation" tab/section:

- "Enable gateway message rate limit" (checkbox) –
- By default the checkbox is unchecked. When checked (feature enabled) the system applies message rate limiting and quarantining according to the configuration of the OSB WAN SIP listening IP:Port address.
- An array of quarantine interval settings is provisional under a section titled "Trust Level Quarantine Intervals"
- Within this section each of the supported "Trust Levels" are displayed along with the quarantine time interval in effect. The user may change the quarantine interval value according to the supported range for each "Trust Level".
- Within this section each of the supported "Trust Levels" are displayed along with the quarantine time interval in effect. The user may change the quarantine interval value according to the supported range

for each “Trust Level”.

Trust Level	Quarantine Interval
Minimal	60 sec. (default value with range 60-3600)
Medium	10 sec. (default with range 10-3600)

Note: The default system-wide quarantine interval is variable (0-2 sec) and is not shown since it is not configurable.

'User Agent Allowed List

A new section User Agent Allowed List was added in Denial of Service Mitigation. If any User Agent is added to the list, requests will only be honored from that User Agents. SIP requests from any other User Agents will not be honored.

Security

Select OK to temporarily store changes. Make your changes permanent by selecting 'Apply Changes' on the General page.

General Firewall Message Rate Control RADIUS Tunnel Connections **Denial of Service Mitigation**

Dynamic Blacklist

☐ Block unauthorized users Unauthorized user quarantine interval (sec) 300

☐ Block unknown users Unknown user quarantine interval (sec) 300

☐ Subscriber Garbage Collector Subscriber garbage collector interval (sec) 60

☐ Enable gateway message rate limit

Trust Level Quarantine Intervals

Minimal (sec) 60

Medium (sec) 10

User Agent Allowed List

User Agent **Add**

Delete

OK Cancel

54 Support of near end NAT Firewall

The OSB shall support the external firewall address configuration according to FRN5693.

A new section **External Firewall** was created under **Security** tab > **Firewall** tab > **Edit** button
>**Firewall Configuration** pop up window

This new section contains:

- Checkbox **External Firewall** :Enables external firewall functionality in the OSB ,disabled by default
- Checkbox **SIP ALG**: Has to be checked if a firewall with SIP ALG functionality is used Default: Grayed out and unchecked – may be activated in future FRNs
- Drop down list 'Profile'
- Description: Profile list according to FRN5693 when external firewall and SIP ALG is activated.
- Default: Grayed out – may be activated in future FRNs
- Text box 'Firewall internal IP'
- Values: IP address or subnet
- Description: Enter internal IP address here
- Default: Deactivated and empty – may be activated in future FRNs
- Text box 'Firewall external IP'
- Values: IP address or subnet
- Description: The OSB will use this address to perform SIP/SDP NAT, for all IP address fields in SIP messages or SDP.
- Default: empty. Deactivate when 'External Firewall' is unchecked

The screenshot shows the 'Firewall Configuration' web interface. The URL bar indicates the page is accessed via https://21.21.0.82/firewall.html?networkId=WAN&netwInterf=WAN&redirected=true&BO=BO_500i_BSBC. The main content area is titled 'Firewall Configuration' and includes a subtitle 'Firewall configuration provisioning for WAN.'.

Key sections visible include:

- Incoming/Outgoing network connections:** A table with columns for protocol, status, and action. Protocols listed include DNS, SSH, SNMP, ICMP, FTP, Telnet, HTTPS, NTP, and others.
- Incoming VOIP connections:** A table with columns for protocol, status, and action. Protocols listed include SIP, TLS, RTP/sRTP, and MGCP.
- White list:** A table with columns for IP address or subnet / Logical-Endpoint-ID and Port.
- Black list:** A table with columns for IP address or subnet / Logical-Endpoint-ID and Port.
- External Firewall (highlighted in red):** Contains checkboxes for 'External Firewall' and 'SIP ALG', a 'Profile' dropdown menu, and text boxes for 'Firewall external IP' and 'Firewall internal IP'.

Buttons for 'Add' and 'Delete' are present for the White and Black lists. The bottom right corner features 'OK' and 'Cancel' buttons.



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.

Configurable DNS SRV Switchover Timer

Add a no-reply and a no-answer timer text field in the gateway trunkconfiguration.

The new **Signaling tab** was created in **Features tab**  'Gateways/Trunks' tab  'Gateway Configuration' tab

- New text box 'INVITE no reply timeout – Normal Mode(ms)' Default value: 3000
Minimum: 1000. Maximum: 32000
- Grayed out if Functional type is Survivable mode Egress/Ingress. Grayed out if Functional type is Emergency .
- New text box 'INVITE no reply timeout – Survivable Mode(ms)' Default value: 3000
Minimum: 1000. Maximum: 32000
- Grayed out if Functional type is Normal mode Egress/Ingress.
- New text box 'INVITE no answer timeout - Normal Mode (ms)' Default value: 360000
Minimum: 120000. Maximum: 3600000
- Grayed out if Functional type is Survivable mode Egress/Ingress. Grayed out if Functional type is Emergency.
- New text box 'INVITE no answer timeout - Survivable Mode(ms)' Default value: 180000
Minimum: 120000. Maximum: 3600000
- Grayed out if Functional type is Normal mode Egress/Ingress.

OpenScapeBranch Behind an OSS (OpenScapeSBC)

The OpenScapeBranch can be used to connect to an OSV on a WAN interface through an OSS. For the configuration details please check the V9 OpenScape SBC Configuration guide.

More information can be found on http://wiki.dev.global-intra.net/privatewiki/index.php/Chapter_18:_Branch_Offices

There are three different options in order to configure successful OSB iGW behind an SBC

1) FQDN configuration

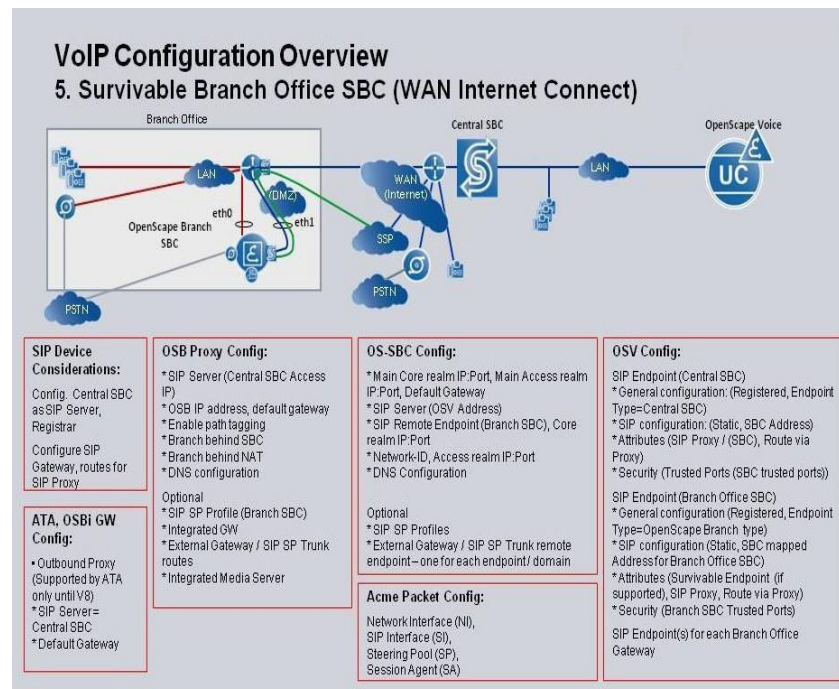
In the OSV the OSB iGW and the OSB Proxy Endpoint is configured with FQDN. This FQDN needs to be resolved both from core and access side of the SBC to the IP of the OSB. Then same FQDN as configured in the OSV endpoints needs to be defined under the Remote Endpoint Configuration--> Remote Location domain list -->Remote URL. Same configuration should take place both for Proxy and GW Remote Endpoint.

2) IP configuration: Configuring IP instead of FQDN in OSV

In the OSV the OSB iGW and the OSB Proxy Endpoint are configured with IP and in the SBC under Remote Endpoint Configuration--> Remote Location domain list -->Remote URL we include the same IP both for Proxy and GW Remote Endpoint.

3) FQDN configuration with Core FQDN

In the OSV the OSB iGW and the OSB Proxy Endpoint is configured with FQDN and in the SBC under Remote Endpoint Configuration--> Remote Location domain list -->Remote URL, both for Proxy and GW Remote Endpoint, we include the IP of the OSB that is resolved from DNS for specific FQDN. In addition under "Core FQDN" we include the FQDN entry both for in the SB iGW Remote Endpoint and proxy GW.



Gateway Configuration

Gateway configuration provisioning.

Remote URL:

Port:

Interface:

Transport:

Mapped port:

Routing prefix:

Gateway/Trunk type:

Functional type:

Trunk profile:

Output digit strip:

Output digit add:

Priority:

☐ Operational Mode in OPTIONS Response

Signaling

INVITE no answer timeout - Normal Mode (ms):

INVITE no answer timeout - Survivable Mode (ms):

INVITE no reply timeout - Normal Mode (ms):

INVITE no reply timeout - Survivable Mode (ms):

TLS

TLS mode:

Certificate profile:

☐ TLS keep-alive

Keep-alive interval (seconds):

Keep-alive timeout (seconds):

Media Configuration

Media profile:

Media realm subnet IP address:

Media realm subnet mask:

Anchoring media:

☐ Force media anchoring on transcoding

OK Cancel

55. External Firewall - Pinhole

55.1 Open External Firewall – Pinhole

When the Open Scape Branch 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.

NOTE: This feature only applies for the addresses and ports used for the media streaming. It is not applicable to the SIP or MGCP protocols.

Selecting only the **Open external firewall pinhole** has the following characteristics:

- **send single UDP packet (no RTP or RTCP)**
- **send during payload establishment (either initial call or feature)**
- **no periodic sending**
- **re-send in case the media path was put on hold and became active again**

55.2 Send RTP dummy packets

As some providers were having issues with the dummy UDP packets, a new flag **Send RTP dummy packets** has been added to send RPT packets instead.

Similar to **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.

NOTE: 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.

Selecting both **Open external firewall pinhole** and **Send RTP dummy packets** has the following characteristics:

- **send single RTP Autolearn packet**
- **send during payload establishment (either initial call or feature)**
- **no periodic sending**
- **re-send in case the media path was put on hold and became active again**

This feature can be configured/enabled under:

Gateways (Administration > Features > Gateways/Trunks > Gateway Configuration

The screenshot shows the 'Gateway Configuration' window with the following sections and settings:

- General:** A message at the top says 'Select OK to temporarily store changes. Make your changes permanent by selecting 'Apply Changes' on the General page.'
- TLS keep-alive:** An unchecked checkbox. Below it, 'Keep-alive interval (seconds)' is set to 120 and 'Keep-alive timeout (seconds)' is set to 10.
- Media Configuration:**
 - 'Media profile' is set to 'lgw_features_lan'.
 - 'Media realm subnet IP address' and 'Media realm subnet mask' are empty text boxes.
 - 'Anchoring media' is set to 'Forced'.
 - Three unchecked checkboxes: 'Force media anchoring on transcoding', 'Record calls from this Gateway/Trunk', and 'Allow Asymmetric RTP'.
- Outbound Proxy Configuration:**
 - 'Outbound Proxy' is an empty text box.
 - 'Outbound Proxy Port' is set to 0.
- Registrar Server Configuration:**
 - 'Registrar Server' is an empty text box.
 - 'Registrar Server Port' is set to 0.
- Miscellaneous:**
 - 'Open external firewall pinhole' is checked.
 - 'Send RTP dummy packets' is checked.

At the bottom right, there are 'OK' and 'Cancel' buttons.

VoIP > Port and Signalling Settings

The Open external firewall pinhole and Send RTP dummy packets configuration are only available for OSB Branch SBC and applicable for all gateways and subscribers under it.

VOIP

Select OK to temporarily store changes. Make your changes permanent by selecting 'Apply Changes' on the General page.

Sip Server Settings | **Port and Signaling Settings** | Manipulation and Routing | Error Codes | Media

Port Range

Media independent RTP ports
 Port min 35000 Port max 65000 Time to live (sec) 180

Subscribers dynamic SIP ports
 Port min 10000 Port max 16600

Gateways/trunks static SIP ports
 Port min 9000 Port max 9254

TCP/BFCP ports
 Port min 35000 Port max 39999

Signaling and Transport Settings

INVITE No Answer timeout - Normal Mode (ms) 360 INVITE No Answer timeout - Survival Mode (ms) 180

☐ Disable answer supervision for emergency calls line

TCP connect timeout (sec) 4 TCP send timeout (sec) 3

TCP connection lifetime (sec) 350 ☐ TCP keep alive

BFCP connection timer (min) 720

Miscellaneous

☒ Open external firewall pinhole

☒ Send RTP dummy packets

☐ SIP SSL single context

OK Cancel

Example of UDP packet (pinhole) that is sent when only **Open External Firewall pinhole** is enabled:

remote_subscribers_oneflag.pcap

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-F>

No.	Time	Source	src_port	Destination	dst_port	Protocol	Length	Info
225	6.691024	VMware_4a:3e:2f				ARP	44	192.168.96.40 is at 00:0c:29:4a:3e:2f
226	6.694360	127.0.0.1	5151	127.0.0.1	5181	eRTPProxy	179	REQ ucil_102_3_175 lagojb (Lookup) ba18a3b
227	6.694728	127.0.0.1	5181	127.0.0.1	5151	eRTPProxy	78	RESP ucil_102_3_175 31572 192.168.96.40
228	6.694781	192.168.96.40	31572	192.168.111.88	4502	RTP	51	Unknown RTP version 1
229	6.694810	21.21.10.40	32056	192.168.111.88	4504	RTP	51	Unknown RTP version 1
230	6.700926	VMware_dc:b8:aa				ARP	62	Who has 21.21.200.232? Tell 21.21.200.231

> Frame 228: 51 bytes on wire (408 bits), 51 bytes captured (408 bits)

> Linux cooked capture v1

> Internet Protocol Version 4, Src: 192.168.96.40, Dst: 192.168.111.88

> User Datagram Protocol, Src Port: 31572, Dst Port: 4502

> Real-Time Transport Protocol

> Data (7 bytes)

Data: 65787400000000

[Length: 7]

```

0000  00 04 00 01 00 06 00 0c 29 4a 3e 2f 61 0d 08 00  ....J>/a...
0010  45 b8 00 23 ef 35 40 00 40 11 fa 0a c0 a8 60 28  E-#-5@-@-...
0020  c0 a8 6f 58 7b 54 11 96 00 0f 50 f2 65 78 74 00  -oX{T- -P-ext-
0030  00 00 00  ...
  
```

remote_subscribers_oneflag.pcap | Packets: 1040 - Displayed: 1040 (100.0%) | Profile: Default

Example of RTP packet (pinhole) that is sent when **Send RTP dummy packets** is enabled:

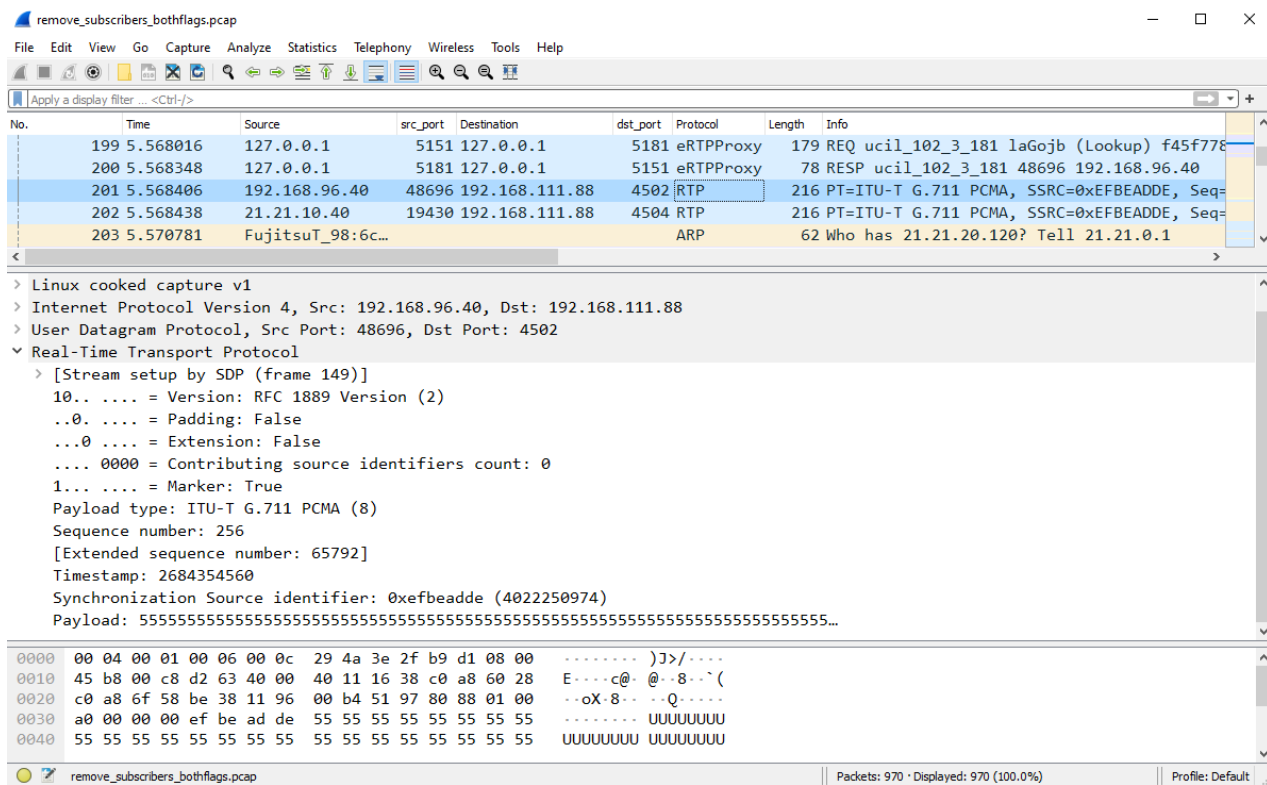


Table A: Fixed/Configurable Port Information

This table shows specific ports used by OpenScapeBranch.

Application/Mode		Port Information
Fixed Ports	DNS Server	53, 32774, 32773
	OSB Redundancy	1075
	SNMP Set/Get	161
	NTP/SNTP	123
	SSH / SFTP	22
	HTTPS to allow Phone to Download SW from OSB	4560
	HTTPS over SOAP	4709
	HTTPS over TLS/SSL	443
	B2BUA	5096
	Media Server (RTP)	20000-20499
	ISAKMP	500
	Syslog Server	514
	Ipssec NAT-Traversal	4500
	DHCP Server/Client	67/68
	B2BUA T.38	4000-4999
	B2BUA RTP (ACD/AA/MLHG/Integrated GW)	10000-19999
Configurable Ports (Default Value Under Port Information)	Media Server (MGCP)	2427
	Proxy SIP Port (TCP/UDP)	5060
	SFTP CDR	22
	Proxy SIP Port (TLS)	5061
	SBC (RTP)	35000-65000
	SBC (SIP)	10000-15000
	SNMP Traps	162
	VPN	1194
	SBC (SIP Trunk)	17000-17999

Note: Proxy/Proxy ACD RTP and SIP ports are controlled/allocated by Endpoints/GWs/OSV.

Table B: OSB Configuration Limits

The following table shows specific limits for supported OpenScape Branch Models. OSB Configuration Guide states that OSB 250 supports a maximum of 10 SBC concurrent sessions. OSB Sales documentation states that OSB 250 supports a maximum of 30 SBC sessions.

oa	Advantech 50i	Advantech 250i OSB250	Advantech 500i OSB 500i	IBM 3250 OSB1000	Fujitsu/ IBM3550 OSB6000	Remarks
Max allowed Registered Lines (Endpoints)	88	300	600	1200	6200	For Keysets, every line counts as Subscriber (Endpoint)
Max supported active Lines (Endpoints)	250	250	500	1000	6000	For Keysets, every line counts as Subscriber (Endpoint)
Concurrent sessions	30	30	120	120	400	
Calls per sec continuously	3 cps	3 cps	5 cps	5 cps	35 cps	
Registrations per sec (background)	10	10	20	50	40	
Registrations per sec (peak)	250	250	550	1000	6000	Network outage, should be tested as peak only
Media streams thru OSB in Proxy Mode	none	none	none	none	none	Media stream flows between Endpoints
Media streams thru OSB in SBC Mode	5	10	20	50	600	Media stream flows between Endpoints
Max Media Server Announcement streams (concurrent)	16	16	16	32	100	
Max Media Server Conference circuits	28	28	30	32	60	
Max No of Sessions in GUI/SOAP	5	5	5	5	5	

Table C: Hardware Types Table

OpenScapeBranch Model	Details
<p>Proxy ATA 24/48 FXS</p>   <p>Labels in rear view image: Serial, LAN Ethernet Port, WAN Ethernet Port, 24 Port Analog Adapter (25-48), Power In +12V DC, Power In +12V DC, VOA, 4x USB Ports, 24 Port Analog Adapter (1-24).</p>	<p>Advantech SYS-2USM01-6M01E Physical Dimension (W x H x D): 300 x 65 x 400 mm (11.8" x 2.6" x 15.8") OpenScape Branch 50i A024 - ADA565 / L30220-D600-A565 (24 FXS ports) OpenScape Branch 50i A048 - ADA566 / L30220-D600-A566 (48 FXS ports)</p>
<p>OpenScape Branch 50i</p> 	<p>Advantech SYS-2USM02-6M01E Physical Dimension (W x H x D): 300 x 65 x 300 mm (11.8" x 2.6" x 11.8") Power: 100~240 V AC , 50-60 Hz, 60W Part Number. ADA350 / L30220-D600-350 (FXO- FXS) Part Number. ADA351 / L30220-D600-351 (BRI- FXS) Part Number. ADA393 / L30220-D600-393/4 (PRIE1/PRIT1 and FXS) Part Number. BZF101 / L30280-Z600-F101 (Power Cord, USA Variant) Part Number. BZF102 / L30280-Z600-F102 (Power Cord, UK Variant) Part Number. BZF105 / L30280-Z600-F105 (Power Cord with Straight Appliance Connector, EURO Variant) Note: Back View for 50i is available on 50i section of Configuration Guide.</p>
<p>OpenScape Branch 250</p> 	<p>Advantech SYS-2USM12-6M01E Physical Dimension (W x H x D): 300 x 65 x 300 mm (11.8" x 2.6" x 11.8") Power: 100~240 V AC , 50-60 Hz, 60W Part Number. ADA393 / L30220-D600-395</p>

	
<p>OpenScape Branch 500i</p> 	<p>Advantech SYS-2USM03-6M01E Physical Dimension (W x H x D): 425 x 65 x 320 mm (16.8" x 2.6" x 12.9") OpenScape Branch 500i DP4 ADA571 / L30220-D600-A571 (Digital PRI – 4 E1/T1 PRI ports) OpenScape Branch 500i DP8 ADA572 / L30220-D600-A572 (Digital PRI – 8 E1/T1 PRI ports)</p>
<p>OpenScape Branch 1000</p>  <p>IBM 3250 M5</p> 	<p>IBM x3250 M2/M3/M5 server Physical Dimension (W x H x D): 435 x 43 x 576 mm (17.1" x 1.7" x 22.7") Power: 100~127/200~240 V AC, 351W</p> <p>IBM x3250 M6 server Physical Dimension (W x H x D): 435 x 43 x 576 mm (17.1" x 1.7" x 22.7") Power: 300 W, 100~127 / 200~240 V AC input Part number: x3250 M6 / 3633AC1</p>
<p>OpenScape Branch 6000</p>  <p>3550-M4</p> 	<p>IBM x3550 M3/M4 Physical Dimension (W x H x D): 429 x 43 x 734 mm (16.9" x 1.69" x 28.9") Rated Power: 100~127 / 200~240 V AC, max 351 W Part numbers: ADA569 / L30220-D600-A575</p>

Fujitsu-RX200 S6



Fujitsu Primergy RX200 S6

Physical Dimension (W x H x D): 431 x 43 x 762mm (18" x 1.69" x 30.0")

Weight: up to 17 Kg (37.5 lb) Average Power Consumption: 193W

Unify Part number: ADA603 / L30220-D600-A603

Fujitsu-RX200 S7



Fujitsu Primergy RX200 S7

Physical Dimension (W x H x D): 431 x 43 x 762 mm (16.97" x 1.69" x 30.00")

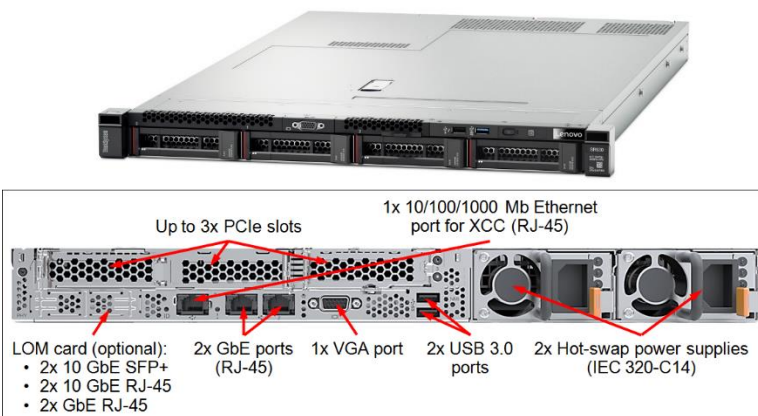
Rated Power: 100~127/200~240V AC, max 549 W

Part numbers: ADA570 / L30220-D600-A570

NOTE: RX200: LAN 1 is "LAN" and LAN 2 is "WAN" interface

NOTE: It is recommended to use a LAN/WAN cable UTP category6.

Lenovo SR530



Lenovo SR530

Physical Dimension (W x H x D): 434 x 43 x 715 mm (17.1" x 1.7" x 28.1")

Weight: Minimum configuration: 10.2 kg (22.5 lb), maximum: 16 kg (35.3 lb)

Rated Power: 100-127 / 200- 240 V AC , 50-60 Hz, 550 W

Operating Temperature: 5- 45°C (41-113°F)

Part Number: L30220-D600- A616

Lenovo-SR630 V2



3x Low Profile PCIe slots (no rear drives)



Lenovo-SR630 V2

(Replacement for Lenovo-SR530)

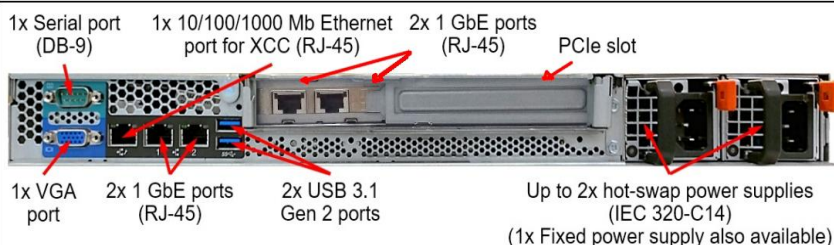
Physical Dimension (W x H x D): 440 x 43 x 773 mm
(17.3" x 1.7" x 30.4")

Weight: up to 20.8 kg (45.9 lb)

Rated Power: 100-127 / 200-240 V AC, 50-60 Hz

Part Number: S30122-X8000-X133

Lenovo-SR250



Lenovo SR250 (Replacement for IBM x3250 M3/M5/M6)

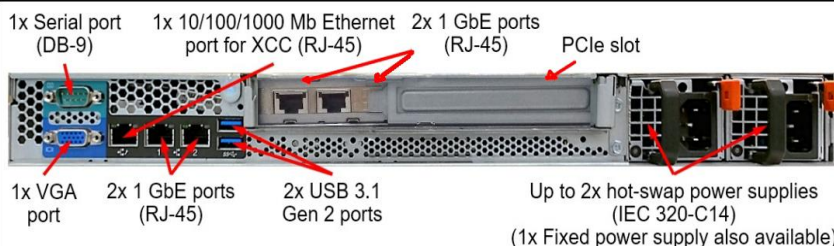
Physical Dimension (W x H x D): 434 x 43 x 498mm (17.1" x 1.7" x 19.6")

Weight: up to 12.3 kg (27.1 lb)

Rated Power: 100-127 / 200-240 V AC, 50-60 Hz

SATA: SSD 480Gb 01PE393
Part Number: S30122-X8000-X129

Lenovo-SR250 V2



Lenovo SR250 V2 (Replacement for Lenovo-SR250)

Physical Dimension (W x H x D): 435 x 43 x 545 mm
(17.1" x 1.7" x 21.5")

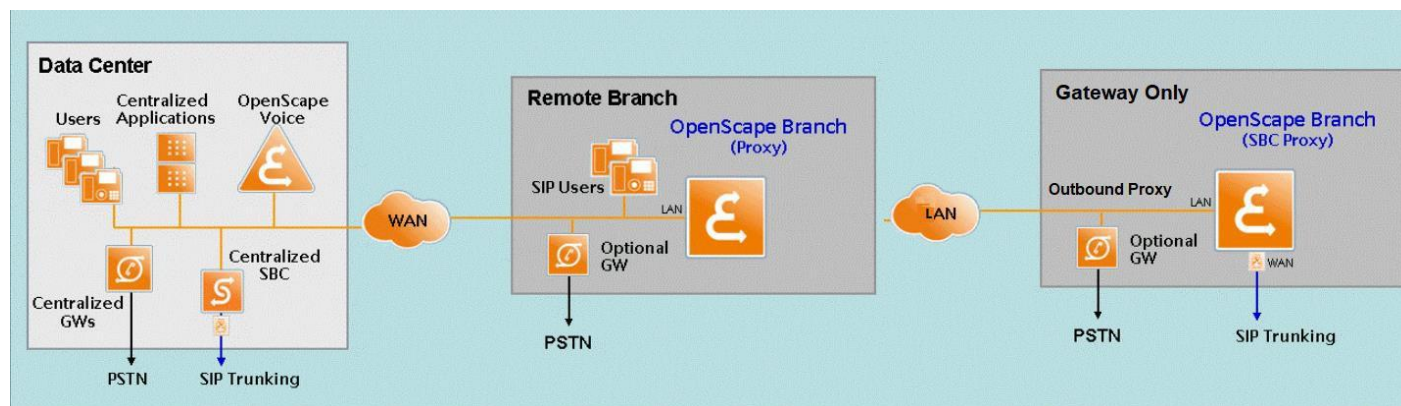
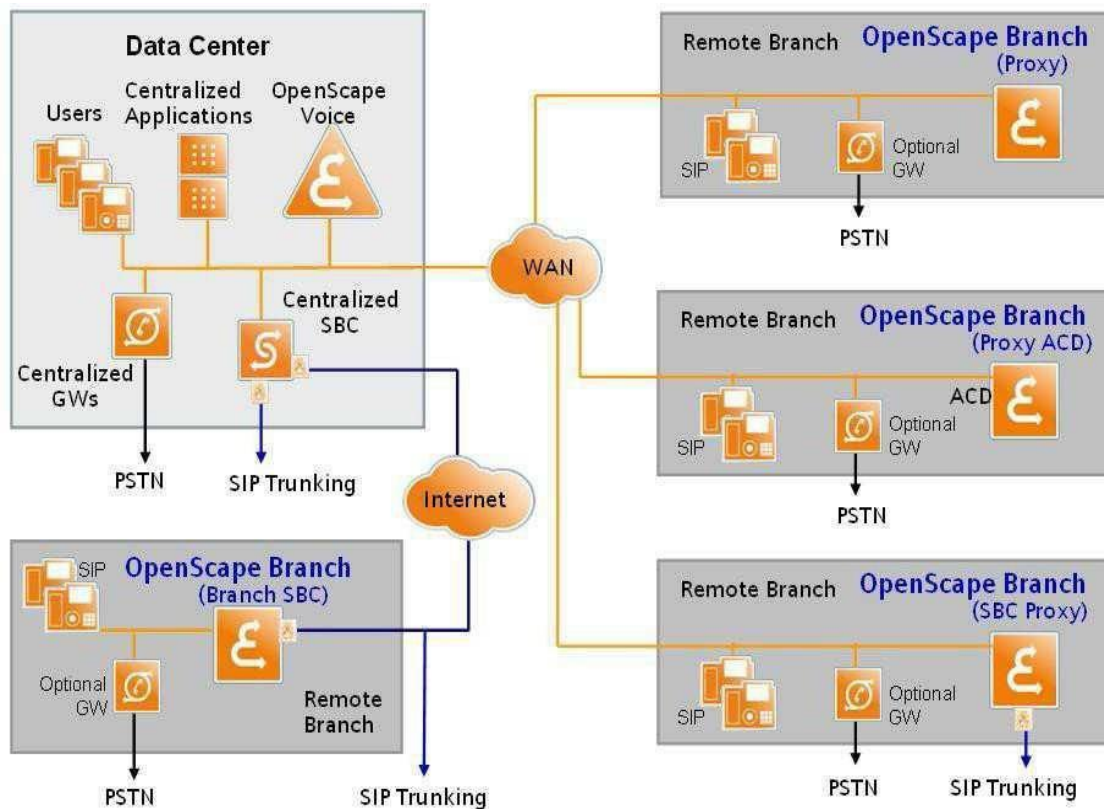
Weight: up to 12.3 kg (27.1 lb)

Rated Power: 100-127 / 200-240 V AC, 50-60 Hz

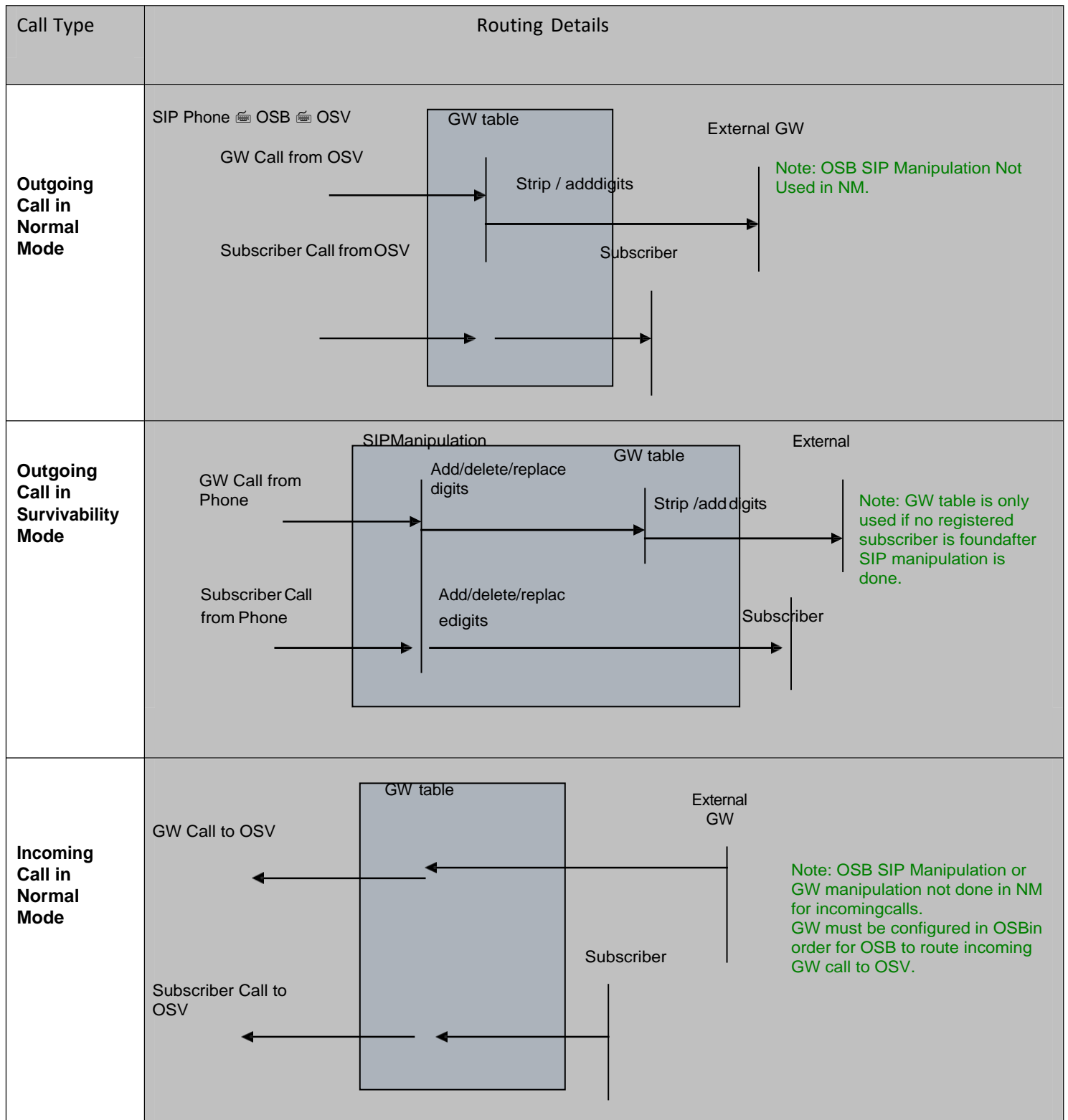
SATA: SSD 480Gb 02JG567

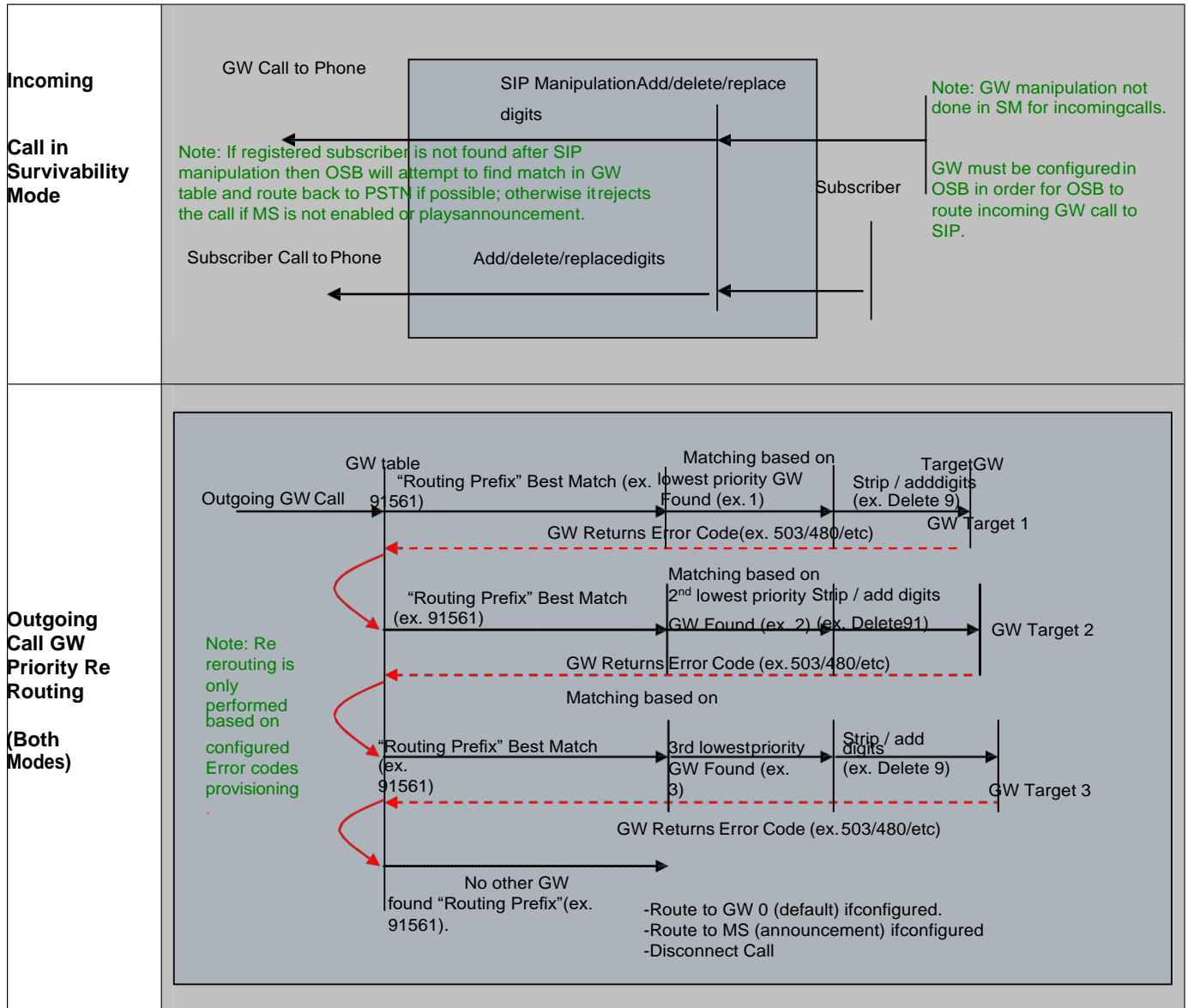
Part Number: S30122-X8000-X134

Table D: Operating Modes Diagram



57 Table E: Routing Table





56 OpenScape Branch 50i

OSB integrated gateway supports FXO/BRI/PRI as well as 4 FXS ports.

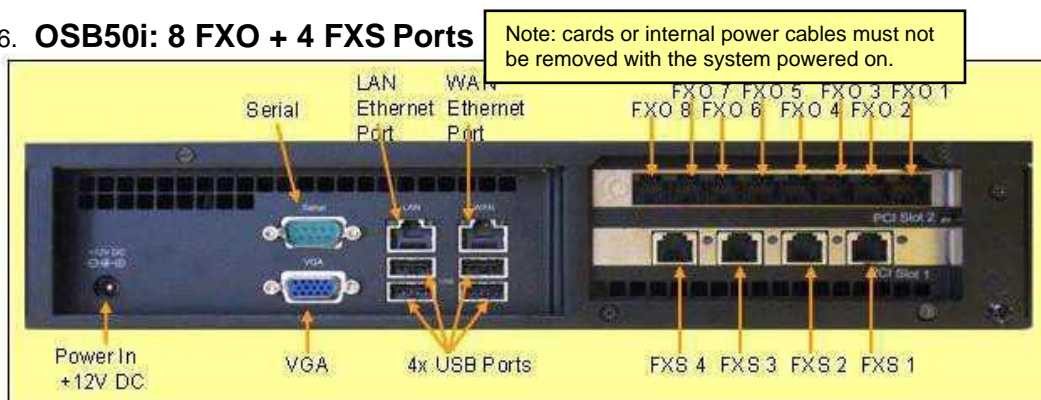
Note: "Do not Send Invite without SDP" attribute must NOT be selected on OSB50i/OSB500i Integrated Gateway End Point.

56.1 Integrated GW Configuration (Advantech 50i)

Configuration Options

Four configurations can be ordered for the OSB 50i:

6. OSB50i: 8 FXO + 4 FXS Ports



The minimum Ring Voltage for the TDM808 card (FXO):

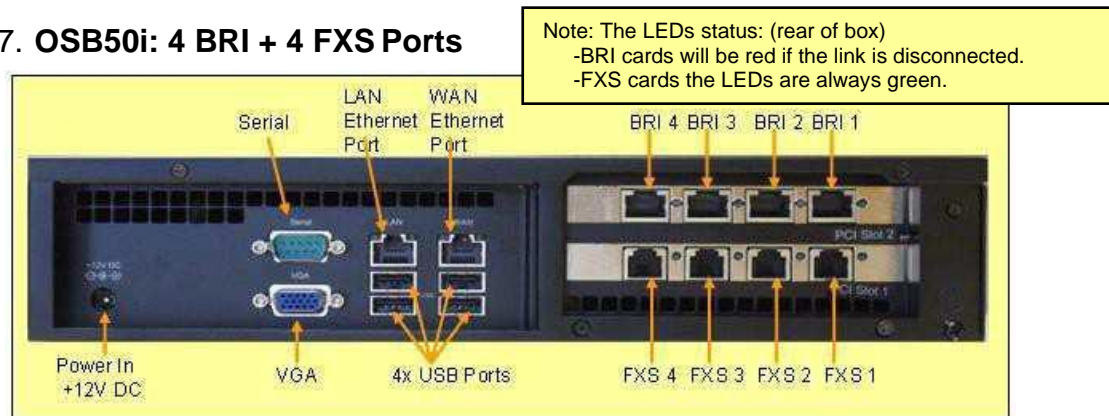
There are two modes: FCC and TBR21.

Below is the min-to-max ring voltage range of each:

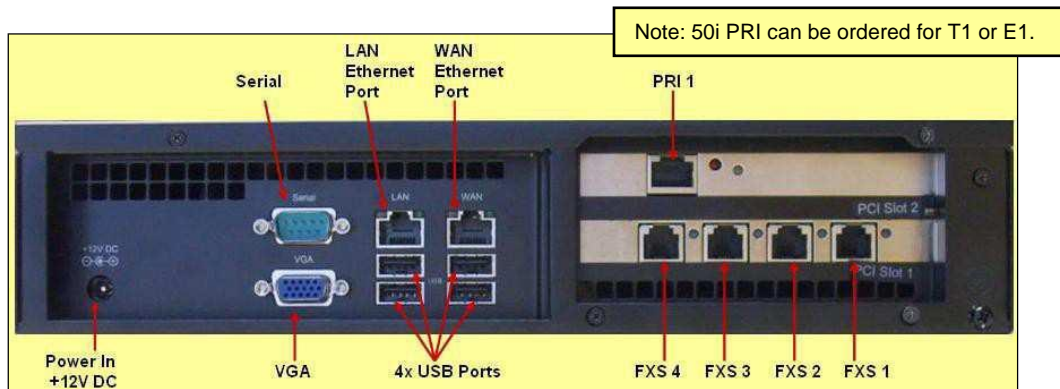
FCC is 19.35 - 23.65 Vrms.

TBR21 is 13.5 - 16.5 Vrms.

7. OSB50i: 4 BRI + 4 FXS Ports



8. -OSB50i: 1 PRI (E1 or T1) + 4 FXS Ports (DP14)



9. - OSB50i: 2 PRI (E1 or T1) + 4 FXS Ports

Note: 50i with 2 PRIs can be configured as T1 or E1.



56.2 Enable Integrated GW and Discover card configuration

Configuration -> OpenScape Branch -> Branch Office -> Configuration -> Features

Features

Enable/Disable desired Feature.

Features Available in Normal Mode and Survivability Mode

- ☐ Enable gateways/trunks Configure
- ☒ Enable integrated gateway Configure
- ☐ Enable auto attendant Configure
- ☐ Enable phone software management Configure
- ☐ Enable Media Server
- ☒ Enable Codec Support
- ☐ Enable Backup Link Cl

Emergency Calling

Message from webpage

The current Integrated Gateway configuration does not match the identified hardware, do you want to reset the configuration?
If you do not reset the configuration, the system may not work correctly.

OK Cancel

Enable Integrated GW.
Note: discovering the GW cards will require a system restart so that drivers are loaded.

Select Country Configuration for Integrated Gateway

Configuration -> OpenScape Branch -> Branch Office -> Configuration -> System -> Settings

System

Select OK to temporarily store changes. Make your changes permanent by selecting 'Apply Changes' on the General page.

Settings Licenses Branding

Country Configuration

Country Brazil Country configuration

Country Configuration

br configuration

```
#
# General
#
country = Brazil (br)
DTMF Interdigit time = 40 ms
DTMF high level = -10 dbm
DTMF low level = -12 dbm
MFR1 level = -10 dbm
MFR2 level = -8 dbm
Ring cadence = 1000,4000 ms
```


Verified Integrated Gateway Cards loaded correctly

Configuration -> OpenScape Branch -> Branch Office -> Configuration -> Features -> Enable integrated gateway -> Configure

Integrated Gateway

Integrated gateway provisioning.

Gateway Configuration

Card 1 PRI Configuration Trunk group

Card 2 FXS Configuration Trunk group

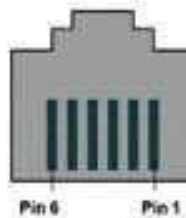
FXS/PRI cards are discovered.
If FXO/BRI configuration is used then it will show in place of PRI.

56.3 FXS and FXO Configuration

FXS Configuration

FXO/FXS port - RJ11 Telco Port Connector - pin assignment

Pin	Description
1	Not Used
2	Not Used
3	Tip
4	Ring
5	Not Used
6	Not Used



Configuration -> OpenScape Branch -> Branch Office -> Configuration -> Features -> Enable integrated gateway -> Configure -> FXS -> Configuration

Integrated Gateway

Integrated gateway provisioning.

Gateway Configuration Select Configuration for FXS parameters/settings.

Card 1 PRI Configuration Trunk group

Card 2 FXS Configuration Trunk group

FXS Configuration

FXS Card provisioning.

Port Configuration

☒ All ports (Enabling only ports with subscriber number)

☒ Echo cancellation

First SIP port

9500

Enable all ports with subscribers

Disable all ports

All ports: enabling only ports with subscriber number.

Echo cancellation: Enabling/Disabling echo cancellation for all ports.

Edit

Enable	Card	Physical port	Subscriber number	Subscriber name	Digest authentication realm	Digest authentication user ID	Digest authentication password	SIP port	Echo cancellation	Fax device
<input checked="" type="checkbox"/>	2	Port 1	551138172061	FXS_E1_2061	hipath.com	123456	*****	9500	<input checked="" type="checkbox"/>	<input type="checkbox"/>
<input checked="" type="checkbox"/>	2	Port 2	551138172062	FXS_E1_2062	hipath.com	123456	*****	9501	<input checked="" type="checkbox"/>	<input type="checkbox"/>
<input checked="" type="checkbox"/>	2	Port 3	551138172063	FXS_E1_2063	hipath.com	123456	*****	9502	<input checked="" type="checkbox"/>	<input type="checkbox"/>
<input checked="" type="checkbox"/>	2	Port 4	551138172064	FXS_E1_2064	hipath.com	123456	*****	9503	<input checked="" type="checkbox"/>	<input type="checkbox"/>

FXS port Configuration

FXS Port provisioning.

General

☒ Enable

Card

2

Physical port

Port 1

SIP port

9500

General:

Enable: Enable or disable the FXS physical port.

Physical port: Number of FXS port. It is a read only field.

Subscriber Configuration

Subscriber number

551138172061

Digest authentication realm

hipath.com

Subscriber name

FXS_E1_2061

Digest authentication user ID

123456

Registration interval (sec)

600

Digest authentication password

Endpoint service profile

FXS_Port4

Receive gain (dB)

0

Transmit gain (dB)

0

Subscriber Configuration:

Subscriber number: Subscriber directory number.

Subscriber name: This is the subscriber's name.

Registration interval timer: port DN registers every Registration Interval Timer seconds.

End Point Service Profile: allows the possibility to configure/apply dial restriction rules per FXS subscriber.

Digest authentication realm: 'realm' parameter sent in the header when challenging a request.

Digest authentication user ID: string that uniquely identifies a user within a given realm.

Digest authentication password: password to be used in the Digest Authentication.

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.

FXS Flags

☒ Echo cancellation

Echo training (ms)

none

☐ Fax device

☒ Fax T.38

☒ CNG detection

☐ FXS hoot line

FXS Flags:

Echo cancellation: enable/disable echo cancellation parameter.

Echo training (ms): This parameter is available for PRI/CAS and FXS interfaces that have echo cancellation enabled. Possible values are disabled (default) and from 400 to 1200 ms (with granularity of 100 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.

Fax device: Enables fax for this interface. It is enabled using the enable check box (CW is disabled for the port)

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 hootline: enable/disable FXS port as hoot line.

FXS Configuration

Card Configuration

Loop current (mA)

☒ Manual ring settings

Ring frequency

Ring voltage

☒ Hook flash

Hook flash duration

CLIP

☐ Enable path tagging

☐ Allow compression codecs over FAX lines

☐ Spare flag 3

Loop current: loop current for analog phones.
Manual Ring Settings: Enables configuration for Ring Frequency and Voltage.
Ring Frequency: ring frequency for analog phones. Default is 20.
Ring Voltage: ring voltage for analog phones. Default value is 75.
Hook Flash: turns on or off hook flash capabilities for all ports.
Hook Flash Duration: Long (200ms to 1250ms) or Short (80ms to 200ms) duration hook flash.
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 Configuration

FXS Cards provisioning.

Card Configuration

Loop current (mA)

☒ Manual ring settings

Ring frequency

Ring voltage

☒ Hook flash

Hook flash duration

CLIP

☐ Allow compression codecs over FAX lines

☐ Spare flag 3

CLIP:
 When Country is configured as "United States/North America" or "United States Circa 1950/North America" CLIP is always enabled and will be gray out like picture above.
 Other countries have the option to enable (Bellcore after ring) or disable (None) the CLIP.
 Default for countries different than US is disabled (None)

Flag FXS Invalid Voltage Audit

It was included a new mechanism to audit invalid voltage values in FXS ports, this condition indicates that the FXS port is unresponsive. The mechanism gracefully recovers the system and triggers an alarm while the invalid condition is read.

This new feature is enabled if the new "FXS Invalid Voltage Audit" flag is set and is valid for all FXS ports.

This new flag can be found under: Features -> Enable integrated gateway -> Configure -> FXS -> Configuration -> Card Configuration

Card Configuration

Loop current (mA)

☒ Manual ring settings

Ring frequency

Ring voltage

☒ Hook flash

Hook flash duration

CLIP

☐ Enable path tagging

☐ Allow compression codecs over FAX lines

☒ FXS Invalid Voltage Audit

FXS port Configuration

FXS Port provisioning.

Hotline/Warmline Configuration

☐ Enable

Wait time (sec)

Destination

Number of times to repeat

Repeat interval (sec)

Location Information

Building

Floor

Room

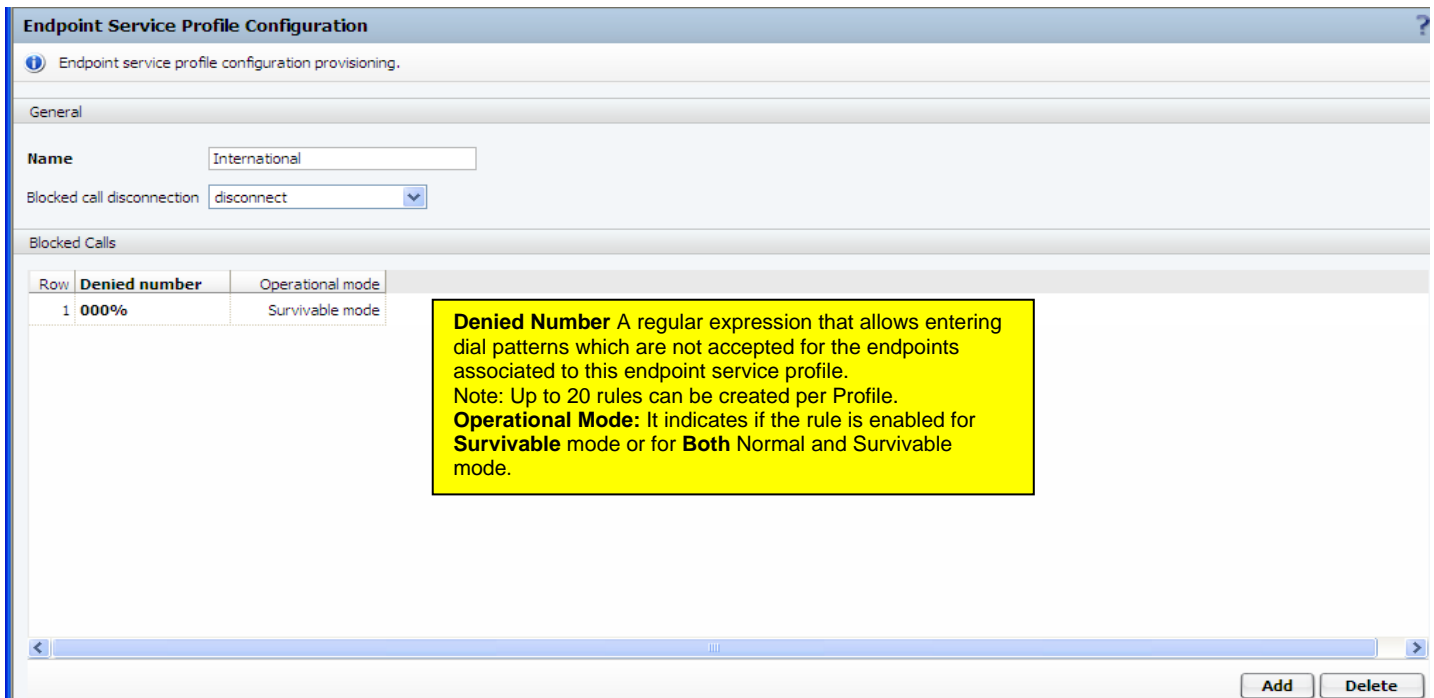
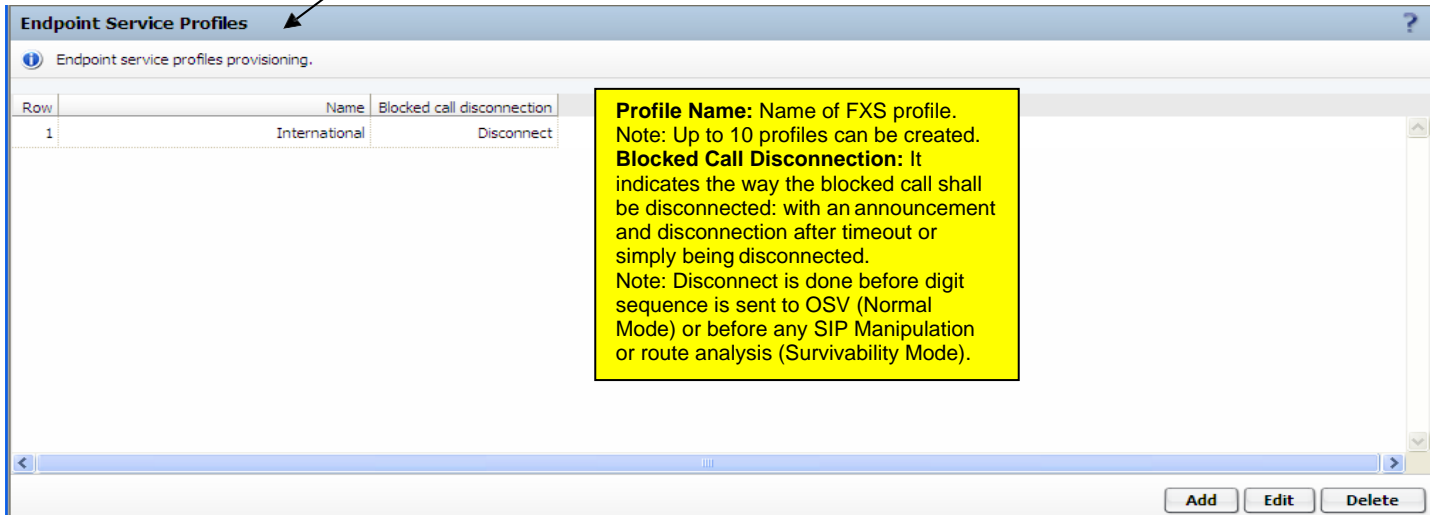
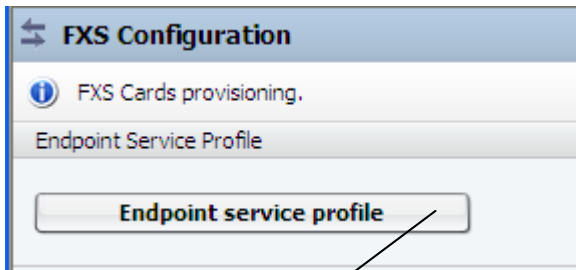
Hotline/Warmline Configuration:
Enable: This checkbox is used to enable the Hotline or Warmline feature for an FXS port. Default setting is unchecked.
Wait time (sec): This field is used to enter a delay time in whole seconds. The default value is zero. When this field is set to zero, Hotline behavior is assumed. When this field is set to a non-zero value, Warmline behavior is assumed.
Destination: This field is used to store the Hotline or Warmline destination number. This field can contain up to 24 digits, using digits 0 – 9.
Number of times to repeat: This field indicates how many times to retry an external hotline/warmline destination in the event that it is busy.
Repeat interval (sec): 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.

Note that FXS Hotline/Warmline cannot be enabled if FXS Hoot Line is enabled, and vice versa.

Location Information: Each FXS port can be set with different value for Building, Floor & Room. If any parameter is not set for a specific FXS port, general values shall be used. If a parameter is configured for a specific FXS port, this value will supersede the general value

Endpoint Service Profile For FXS Subscribers

It is possible to configure/apply dial restriction rules per FXS subscriber. Digit sequences configured in table shall be rejected.



Location Information

Location Information

Enable geo-location support ☒

Country

United States

State or region or province

FL

County or parish or district

PALM BEACH

City

BOCA RATON

Street

BROKEN SOUND

Leading street direction

NW

Street type suffix

BLVD

Address number

5500

Postal code

33487

Postal community name

BOCA RATON

Building

A

Floor

2ND

Room

2.12

Flag "Enable geo-location support" must be set in order for OSB to add the location info (PIDF-LO) based on the values from Location Information section (NG911)

Country, State or region or province, County or parish or district, City and Street are mandatory fields

Country is selected from a drop down menu, max length for State or region or province is 3 chars and for all other fields the maximum length is 150 chars

OSB will add the location information, only when all of the following conditions are met : Normal mode, INVITE was initiated from a SIP subscriber, Geo-location support is set, call (R-URI) is recognized as an emergency call and TCP or TLS is used between the OSB and the OSV/OSS. Location information data will be included only for location unaware phones.

Verify that FXS port is registered on OSB Registered Subscriber List.

Configuration -> OpenScape Branch -> Branch Office -> Configuration -> Local Dashboard -> Registered subscribers -> Show

Services status

Show

Registered subscribers

Show

Registered Subscribers

Registered Subscribers

Search for

in

Username

Search

Show All

Items/Page: 10

<<

<

1

>

>>

All: 10

CSV Export

Username	Contact	Expires (seconds)
551138172058	sip:551138172058@21.21.2.58;5061;transport=tls	2709
551138172061	sip:551138172061@21.21.0.76;9500;transport=udp	333
551138172062	sip:551138172062@21.21.0.76;9501;transport=udp	452
551138172063	sip:551138172063@21.21.0.76;9502;transport=udp	66
551138172064	sip:551138172064@21.21.0.76;9503;transport=udp	461
551138172691	sip:551138172691@21.21.1.108;transport=tcp	993

Features (FXS subscribers)

1. Three-Way Calling

Go off-hook, establish a call, hookflash, hear stutter dial tone, dial the 3rd party, hookflash, now in conference. Subsequent hookflash will drop the 3rd party. If the 3rd party goes on- hook before the conference is established, original parties are left in conversation.

2. Call Hold

Go off-hook, establish a call, hookflash, hear stutter dial tone, hookflash again to retrieve.

3. Call Transfer

Go off-hook, establish a call, hookflash, hear stutter dial tone, dial the 3rd party, go on- hook, call is now transferred.

4. Call Waiting

Make or receive a call, receive a 2nd call and hear call waiting tone, hookflash to toggle to the waiting party, hookflash again to toggle back.

5. Disable Call Waiting for Next Call: feature can be done in two ways

a) Go off-hook, dial *70 to activate, hear confirmation tone, dial the number of the person to reach (when call is established, Call Waiting will not be accepted during the call)

b) Go off-hook, establish a call, hookflash, hear stutter dial tone, dial *70 to activate, hear confirmation tone, hookflash again to retrieve (after this procedure, Call Waiting will not be accepted during the call)

6. Disable Caller ID for Next Outgoing Call

Go off-hook, dial *67 to activate, hear confirmation tone, dial the number of the person to reach.

7. Do Not Disturb

Go off-hook, hear dial tone, dial *78 to activate, or *79 to deactivate.

8. Call Forwarding Unconditional

Go off-hook, hear dial tone, dial *72 to activate, or *73 to deactivate. After dialing *72, dial the number to forward to.

9. Call Return

Go off-hook, hear dial tone, dial *69 to hear the number of the last caller. Only works if Caller ID was present.

10. End Dialing

'#' digit as the 2nd or later digit as dialing is complete

FXO Configuration

The minimum Ring Voltage for the TDM808 card (FXO):

There are two modes: FCC and TBR21.

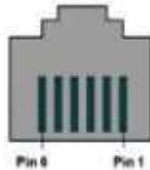
Below is the min-to-max ring voltage range of each:

FCC is 19.35 - 23.65 Vrms.

TBR21 is 13.5 - 16.5 Vrms.

FXO/FXS port - RJ11 Telco Port Connector - pin assignment

Pin	Description
1	Not Used
2	Not Used
3	Tip
4	Ring
5	Not Used
6	Not Used



Integrated Gateway

Integrated gateway provisioning.

Gateway Configuration

Card 1

Card 2

☐ Disable FXO audit

Configure FXO and Trunk Group

Configuration

Trunk group

Disable FXO audit: disable the 12 hours audit for all FXO ports.

FXO Configuration

FXO Configuration provisioning.

Fax T.38

☒ Fax T.38

☒ CNG Detection

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. The activation of the flag "CNG detection" will only take effect if T.38 flag is also enabled.
Note: T.38 fax calls always start as a voice call and then switch to the T.38 codec.

Port Configuration

Row	Enable	Physical port	Signaling mode	Answer by polarity reversal	Disconnect by polarity reversal	Polarity reversal delay hangup (ms)	Loop supervision	Echo cancellation	Receive gain (dB)	Transmit gain (dB)
1	<input checked="" type="checkbox"/>	Port 1	LoopStart	<input type="checkbox"/>	<input type="checkbox"/>	600	<input type="checkbox"/>	<input checked="" type="checkbox"/>	0	0
2	<input checked="" type="checkbox"/>	Port 2	LoopStart	<input type="checkbox"/>	<input type="checkbox"/>	600	<input type="checkbox"/>	<input checked="" type="checkbox"/>	0	0
3	<input checked="" type="checkbox"/>	Port 3	LoopStart	<input type="checkbox"/>					0	0
4	<input checked="" type="checkbox"/>	Port 4	LoopStart	<input type="checkbox"/>					0	0
5	<input type="checkbox"/>	Port 5	LoopStart	<input type="checkbox"/>					0	0
6	<input type="checkbox"/>	Port 6	LoopStart	<input type="checkbox"/>					0	0
7	<input type="checkbox"/>	Port 7	LoopStart	<input type="checkbox"/>					0	0
8	<input type="checkbox"/>	Port 8	LoopStart	<input type="checkbox"/>					0	0

Enable: Enable or disable the FXO physical port.
Physical port: port number of the FXO port (read-only field).
Signaling mode: It configures the signaling mode. Only Loopstart is available.
Answer by polarity reversal: enable/disable the detection of answer via silent reversal.
Disconnect by polarity reversal: enable/disable the detection of disconnection via silent reversal.
Polarity reversal delay hangup: 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: If enabled, the signaling mode is set to Kewlstart.
Echo cancellation: enable/disable echo cancellation for the port.
Receive gain: sets the Gain of payload for receive.
Transmit gain: sets the Gain of payload for transmit.

Ring detection timeout (sec)	Caller ID	Pre answer delay for CID (ms)	CID signaling	CID start	Busy detect disconnect	Minimum busy detect count	Default destination	FXO Hoot Line
30	<input type="checkbox"/>	500	DTMF	Ring	<input checked="" type="checkbox"/>	4	551138172043	<input type="checkbox"/>
30	<input type="checkbox"/>	500	DTMF	Ring	<input checked="" type="checkbox"/>	4	551138172025	<input type="checkbox"/>
30	<input type="checkbox"/>	500	DTMF	Ring	<input checked="" type="checkbox"/>	4	551138172045	<input type="checkbox"/>
30	<input type="checkbox"/>	500	DTMF	Ring	<input checked="" type="checkbox"/>	4	0800417070	<input type="checkbox"/>
5	<input type="checkbox"/>					4		<input type="checkbox"/>
5	<input type="checkbox"/>					4		<input type="checkbox"/>
5	<input type="checkbox"/>					4		<input type="checkbox"/>
5	<input type="checkbox"/>					4		<input type="checkbox"/>

Ring detection timeout: 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.
Pre answer delay for CID: delay in the Dial Plan before the call is answered for FXO and only used if Caller ID is enabled.
CID signaling: The protocols available are: Bell, V23 (UK), V23 (Japan) and DTMF. Only used if caller ID is enabled.
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.
Note: 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 Signaling is set to DTMF.
Busy detect disconnect: enable/disable the detection of busy lines.
Minimum busy detect count: how many busy tones to wait for before hanging up. Only used if busy detect disconnect is enabled.
Default destination: destination number for Incoming calls.
FXO Hoot Line: enable/disable FXO port as hoot line.

Note - Busy Tone detection:

This feature can lead to detect false answers when a false busy tone pattern is perceived.
The BusyTone detection is currently configured only for standard U.S. and Argentina tones.

In case of false positives, we recommend the change of busycount (from 4 to 8)

FXO - Trunk Group Configuration

Integrated Gateway

Integrated gateway provisioning.

Gateway Configuration

Card 1 FXS Configuration Trunk group

Card 2 FXO Configuration Trunk group

Trunk Groups

Trunk Groups provisioning.

Add Trunk Group.
After created, it is possible to Edit/Delete existing Trunk Groups.

Add Edit Delete

Row	Type	FQDN	Trunk group name	Trunk selection	Hunt type
1	FXO	osbnew.unow.ana.cwb	trunkautomation	TopToBottom	Circular

Trunk Group Configuration

Select OK to temporarily store changes. Make your changes permanent by selecting 'Apply Changes' on the General page.

General **Channels list** **Number Modification** **Spare Flags**

Configuration

Type FXO

FQDN osbnew.unow.ana.cwb

Trunk group name trunkautomation

Trunk selection Top To Bottom Hunt type Circular

Direction Both ☐ Mark sRTP call

Voice bearer capability Speech

Incoming Calls

Max overlap digit length

☐ Specific overlap dialing patterns

☐ Connected line identification presentation incoming

Answer Supervision Timer - Incoming Call (sec) 360

Blacklist profile BlackList01

Outgoing Calls

☐ Set Numbering Plan to ISDN

Pre dial delay for DTMF (sec) 2

☐ Send Redirect Number instead of calling number for redirected calls

☐ Calling Party Number Presentation Restricted

☐ Connected line identification presentation outgoing

Answer Supervision Timer - Outgoing Call (sec) 170

Configuration
Type: port type (read only data).
FQDN: required for Trunk Group and to be used later on in "Gateway/Trunk Configuration".
Trunk group name: name of the Trunk Group
Trunk selection: selecting from High or Low Trunk first is possible.
Hunt type: linear or circular selection
Direction: Specifies the direction of traffic flow supported on the Gateway/Trunk and Integrated Gateway to avoid racing condition simultaneous disconnection.
Mark sRTP call-leg as secure: if a secure media is negotiated for (FXO, BRI or PRI), the call will be indicated as secure (ST- Siemens Type: secure)
Incoming Calls
Answer Supervision Timer – Incoming Calls: Value between 3600. Default is 360. Note: Corresponding Answer Supervision should be configured under 'Feature'-'>'Gateway/Trunk'.
Timers should be configured with a difference of at least 10 seconds
Blacklist profile: Specifies the Blacklist profile that it will be checked for incoming calls.
Outgoing Calls:
Set numbering plan to ISDN : it is set to enable/disable. When Type is Unknown, it will set the Numbering Plan to ISDN. Otherwise to Unknown (only PRI). **NOTE:** This flag applies only to "Called Party Number Presentation Restricted".
Pre dial delay for DTMF: When an analog trunk is seized, it is until the DTMF receiver is allocated by CO. If DTMF digits are delayed until the DTMF receiver is allocated, the first digits can be lost. It shall configure a delay to start sending the DTMF digits.
Calling Party Number Presentation Restricted: Set calling party number presentation restricted to all outgoing call.
Answer Supervision Timer – Outgoing Call: Value between 170 and 3600. Default is 170. Note: Corresponding Answer Supervision should be configured under 'Feature'-'>'Gateway/Trunk'.
Timers should be configured with a difference of at least 10 seconds
Gateway/Trunk and Integrated Gateway to avoid racing condition simultaneous disconnection.

Trunk Group Configuration

Select OK to temporarily store changes. Make your changes permanent by selecting 'Apply Changes' on the General page.

General Channels list Number Modification Spare Flags

Configuration

Trunk ports

Port 1

▼

Add

Delete

Port 2

Port 3

Port 4

Port 1


Drop-down box is used to select the port that it will be added to Trunk Group.

Ports configured (in use) in Trunk Group

To remove, select a Port and press Delete button

56.4 BRI Configuration

Table A-1: RJ45 ISDN BRI S/T Port Connector

	Pin	TE	NT
	1	Unused	Unused
	2	Unused	Unused
	3	Tx+	Rx+
	4	Rx+	Tx+
	5	Rx-	Tx-
	6	Tx-	Rx-
	7	Unused	Unused
	8	Unused	Unused

Integrated Gateway

Integrated gateway provisioning.

Gateway Configuration

Configure BRI and Trunk Group

Card 1 BRI

Card 2 FXS

BRI Configuration

BRI configuration provisioning.

Card Configuration

Access type

MSN

5000
5001

☐ Flag 1
☐ Flag 2
☐ Flag 3

The interface ISDN BRI can operate in two modes: Point-to-Point (PP) or Point-to-Multi-Point (PMP). The BRI operating in PMP mode allows connecting more than one ISDN device to this same bus. Specific MSNs can be separated to be handled by each of the devices which are connected to the bus.

Notes for PMP configuration:

- Only numbers under MSN list will be accepted as calling number
- If MSN list is empty, all incoming numbers will be routed
- If PSTN does not send "send complete" flag, INVITE will be immediately send when dialed number matches with number from MSN list.
- Each MSN number is a number from 1 to 24 digits and *, # and + are also accepted
- Up to 10 MSN can be added
- In Normal Mode, the MSN must be handled by OpenScape Voice.
- In Survivable Mode, incoming calls are handled in the SIP Manipulation table. If internal numbers match with MSN, no manipulation are needed. If not, each MSN must be translated to a dialed DN as subscriber, fax, data terminal, MLHG, trunk, voice mail destination, auto attendant, etc..
- For outgoing calls it is configured a rule to convert the calling to a valid MSN number (From header).
- All other configurations should follow the same rules of Point to Point access type.

BRI Configuration

BRI configuration provisioning.

Fax T.38

- ☒ Fax T.38
- ☒ CNG Detection

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. The activation of the flag "CNG detection" will only take effect if T.38 flag is also enabled.

Note: T.38 fax calls always start as a voice call and then switch to the T.38 codec.

BRI Configuration

BRI configuration provisioning.

Port Configuration

Row	Enable	Physical port	Clock source priority	Terminal Mode	Echo cancellation	Switch type	Exclusive channel	Idle reset interval	Receive gain (dB)	Transmit gain (dB)	Default destination	T302 timer
1	<input checked="" type="checkbox"/>	Port 1	1	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	euroisdn	<input type="checkbox"/>	3600	0	0		5
2	<input checked="" type="checkbox"/>	Port 2	2	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	euroisdn	<input type="checkbox"/>	3600	0	0	551138175214	11
3	<input type="checkbox"/>	Port 3	3	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>						551138175008	10
4	<input type="checkbox"/>	Port 4	4	<input type="checkbox"/>	<input type="checkbox"/>							10

Enable: Enable or disable the BRI physical port.

Physical port: BRI port number (Read Only)

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 the source of clock timing for this card or system.

Note: In most cases clocking is a required parameter and value 0 should not be used.

Terminal Mode: indicate if a port is configured as TE. This field is not editable. If it is marked it is configured as TE, otherwise it is configured as NT.

Echo cancellation: Changed to Echo tail (ms), see new picture and info below

Switch type: Only euroisdn is supported in this phase.

Exclusive channel: enable/disable exclusive channel.

Idle reset interval: sets the time in seconds between restart of unused B-channels. If the field is empty, the functionality is disabled.

Receive gain: sets the Gain of payload for receive. A negative value decreases the gain, and a positive value increases the gain.

Transmit gain: 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: timer to wait for digits.

Configuration of the echo cancellation tail length for ISDN BRI ports via the GUI:

Possible values: none, 16, 32,64 and

128. Default value is 32

Upgrade from older versions: if flag Echo Cancellation is enabled the echo tail will be set to 32ms. If flag is disabled echo tail will be set to none.

Port Configuration

Row	Enable	Physical port	Clock source priority	Terminal Mode	Echo tail (ms)	Switch type	Exclusive channel	Idle reset interval	Rec
1	<input checked="" type="checkbox"/>	Port 1	1	<input checked="" type="checkbox"/>	32	euroisdn	<input type="checkbox"/>	3600	0
2	<input checked="" type="checkbox"/>	Port 2	2	<input checked="" type="checkbox"/>	none	euroisdn	<input type="checkbox"/>	3600	0
3	<input type="checkbox"/>	Port 3	3	<input checked="" type="checkbox"/>	16	euroisdn	<input type="checkbox"/>	3600	0
4	<input type="checkbox"/>	Port 4	4	<input checked="" type="checkbox"/>	32	euroisdn	<input type="checkbox"/>	3600	0

Far end disconnect with inband announcement	B-channel parallel restarts	Always send PI8 in ALERT	Setup progress indicator	Start early media on CALL PROCEEDING	183 Session progress without SDP	Disable far end restart	Flag 1	Flag 2	Flag 3
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	none	<input type="checkbox"/>	Alerting	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	none	<input type="checkbox"/>	Alerting	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	none	<input type="checkbox"/>	Alerting	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>							<input type="checkbox"/>

Far end disconnect with inband announcement: enable/disable disconnect with inband announcement.

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.

Always send PI8 in ALERT: if flag is enabled OSB 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.

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.

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: OpenScope Voice sends a 183 Session Progress response code without SDP. Configuration item allows to choose 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.

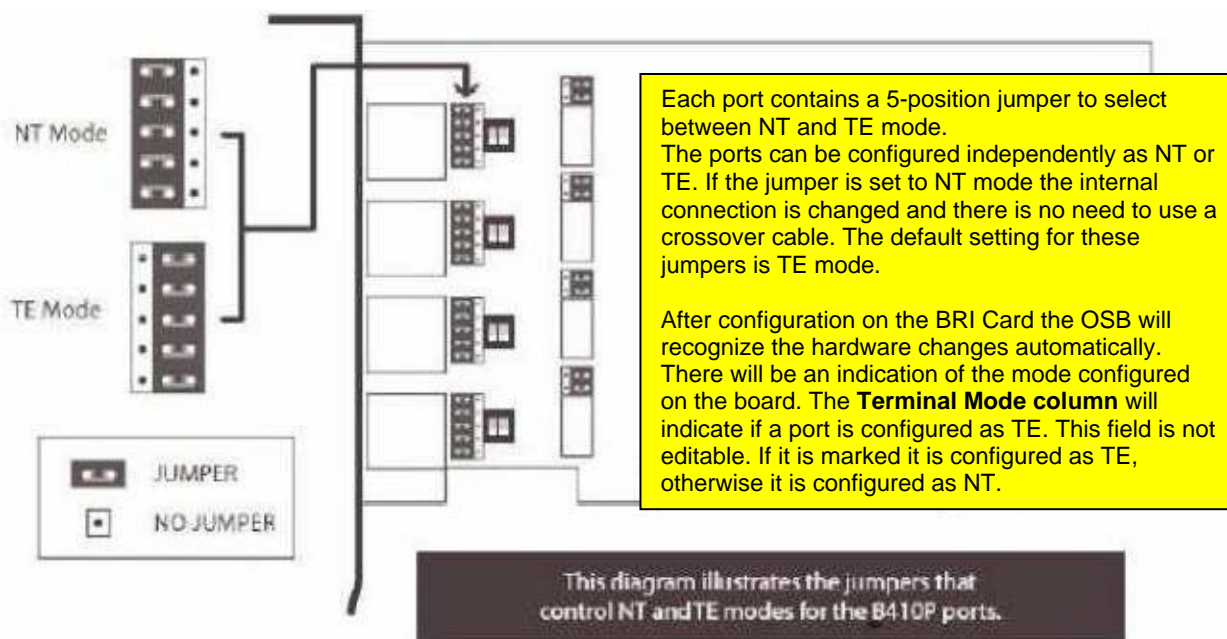
Disable far end restart: In scenarios in which 50i is connected to a CO switch that does not accept RESTART message during BRI span bring up. The flag is recommended for use in BRI PMP systems.

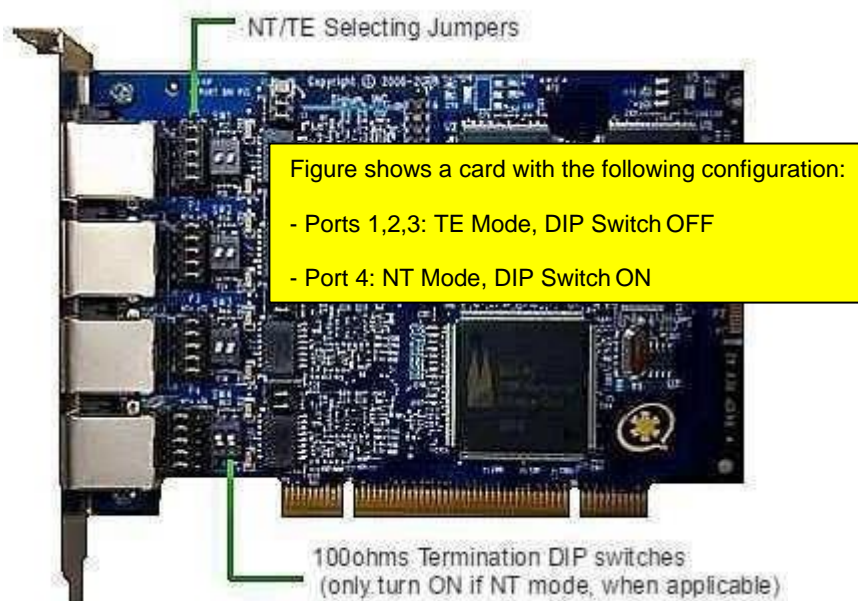
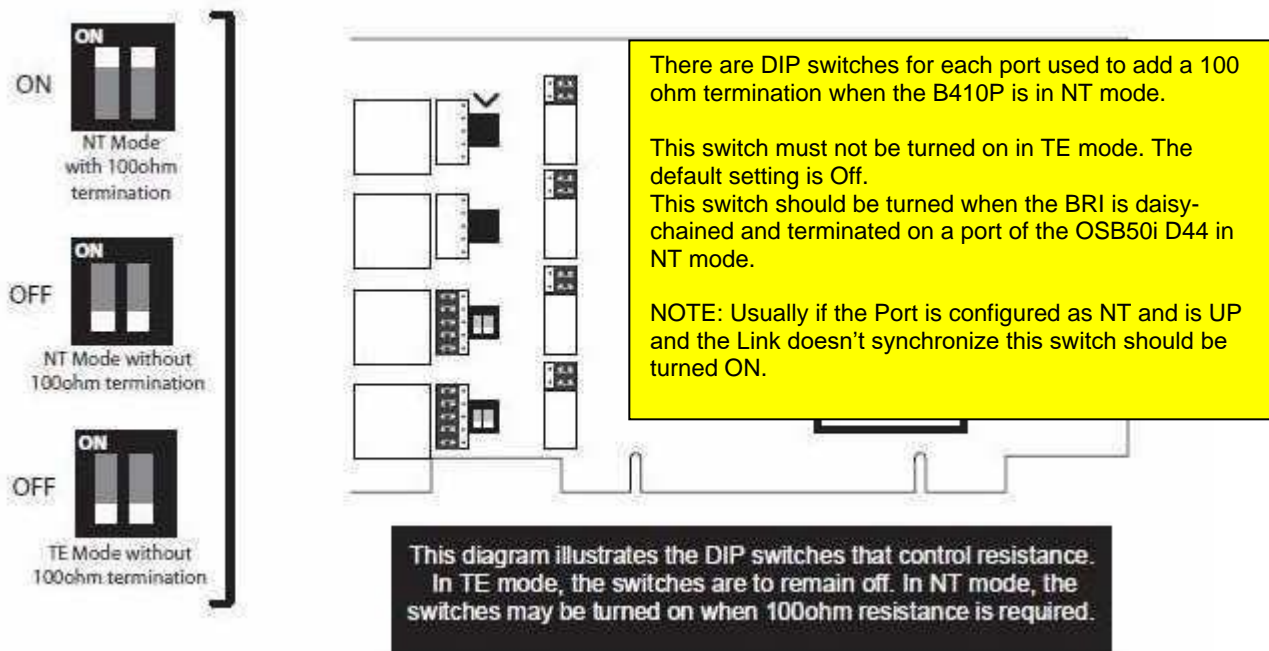
56.4.1 Configure OSB 50i D44 to be used as BRI NT (Network)

The support for OpenScope Branch BRI as NT demands some hardware configuration changes for OSB 50i D44 embedded with Digium cards model B410P. The changes apply for Point-to-Point (PP) and Point-to-Multipoint (PMP) modes.

NOTE1: Always change the card configuration with the card unplugged. Be careful when changing the jumper position.

NOTE2: No features/Services supported in the S0 bus.





DISCLAIMER: The proper GVS support should be contact in order to request for the activation for this feature.

56.4.2 BRI - Trunk Group Configuration

Integrated Gateway

Integrated gateway provisioning.

Gateway Configuration

Card 1 BRI **Configuration** **Trunk group**

Card 2 FXS **Configuration** **Trunk group**

Trunk Groups

Trunk Groups provisioning.

Add Trunk Group.
After created, it is possible to Edit/Delete existing Trunk Groups.

Add **Edit** **Delete**

Row	Type	FQDN	Trunk group name	Trunk selection	Hunt type
1	BRI	50ia.unow.s01.cwb	S0Trk	TopToBottom	Circular

Trunk Group Configuration

Select OK to temporarily store changes. Make your changes permanent by selecting 'Apply Changes' on the General page.

General **Channels list** **Number Modification** **Spare Flags**

Configuration

Type: BRI

FQDN: 50ia.unow.s01.cwb

Trunk group name: S0Trk

Trunk selection: Top To Bottom

Hunt type: Circular

Direction: Both

Voice bearer capability: Speech

☐ Mark sRTP call-leg as secure

Configuration

Type: port type (read only data).

FQDN: required for Trunk Group and to be used later on in "Gateway/Trunk Configuration"/

Trunk group name: name of the Trunk Group

Trunk selection: selecting from High or Low Trunk first is possible.

Hunt type: linear of circular selection

Direction: Specifies the direction of traffic flow supported on the trunk group.

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

Trunk Group Configuration

Select OK to temporarily store changes. Make your changes permanent by selecting 'Apply Changes' on the General page.

General Channels list Network specific facilities Number Modification Spare Flags

Voice bearer capability Speech

Incoming Calls

Max overlap digit length

☐ Specific overlap dialing patterns

☐ Connected line identification presentation incoming

☒ Called Name incoming

Answer Supervision Timer - Incoming Call (sec) 360

☐ Force FQDN in Contact Header for Incoming Calls in NM

Blacklist profile

Outgoing Calls

☐ Set Numbering Plan to ISDN

Pre dial delay for DTMF (sec) 2

☐ Send Redirect Number instead of calling number for redirected calls

☐ Calling Party Number Presentation Restricted

☐ Connected line identification presentation outgoing

☒ Called Name outgoing

Answer Supervision Timer - Outgoing Call (sec) 170

T1 CAS

These fields are only applicable when the Switch type of a port is T1 CAS.

T1 CAS signaling E&M Immediate Start T1 CAS addressing signaling DTMF

OK Cancel

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. If not configured then T302 timer would apply

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.

Connected line identification presentation incoming/outgoing: Enables treatment for connected line identification presentation. When connected number is received in connect or connect ack isdn messages.

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 Calls: Value between 120 and 3600. Default is 360. Note: Corresponding Answer Supervision Timers should be configured under 'Feature'-'>'Gateway/Trunk'.

Timers should be configured with a difference of at least 10 seconds between Gateway/Trunk and Integrated Gateway to avoid racing conditions caused by simultaneous disconnection.

Blacklist profile: Specifies the Blacklist profile that it will be checked during incoming calls.

Outgoing Calls

Send Redirect Number instead of calling number for redirected calls: If selected (enabled), a call that is redirected to the PSTN will have the last redirecting or transferring party's identity as the Calling Party Number information element. This attribute is primarily intended for use when connecting to a carrier that does not understand the Redirecting Party Number information element.

Calling Party Number Presentation Restricted: Set calling party number presentation restricted to all outgoing call.

Connected line identification presentation outgoing: Default value is unchecked. Only visible when the PRI Method is E1, or it is a BRI trunk group. 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: Value between 120 and 3600. Default is 170. Note: Corresponding Answer Supervision Timers should be configured under 'Feature'-'>'Gateway/Trunk'.

Timers should be configured with a difference of at least 10 seconds between Gateway/Trunk and Integrated Gateway to avoid racing conditions caused by simultaneous disconnection.

Trunk Group Configuration

Select OK to temporarily store changes. Make your changes permanent by selecting 'Apply Changes' on the General page.

General

Channels list

Number Modification

Spare Flags

Configuration

Trunk ports

Port 1

Add

Delete

Port 1

Port 2

Port 3

Port 4

Drop-down box is used to select the port that it will be added to Trunk Group.

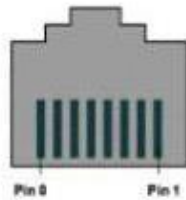
Ports configured (in use) in Trunk Group
To remove, select a Port and press Delete button

214

58.6 PRI Configuration

E1/T1 PRI port - RJ45 Telco Port Connector - pin assignment

Pin	Description
1	Rx
2	Rx
3	Not Used
4	Tx
5	Tx
6	Not Used
7	Not Used
8	Not Used



Integrated Gateway

Integrated gateway provisioning.

Gateway Configuration

Configure PRI and Trunk Group

Card 1

PRI/CAS

Configuration

Trunk group

Card 2

FXS

Configuration

Trunk group

PRI/CAS Configuration

PRI/CAS configuration provisioning.

Card Configuration

Method

E1

Channel maintenance

Method: Available for OSB 50i DP14/DP24 hardware and possible values "E1" or "T1". The default value for new systems is "T1".
Channel maintenance: redirects the user to the channel maintenance window.

Note: If the PRI Method is changed, the user will receive a warning message that says "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

 Channel maintenance































Clk Src


Channel
1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28
29
30
31

Card 1































Port 1 - NET5H4K
 up
BCAS disabled 1

☐ All Channels

State	
 IDLE	<input type="checkbox"/>
 IDLE	<input type="checkbox"/>
 IDLE	<input type="checkbox"/>
 IDLE	<input type="checkbox"/>
 IDLE	<input type="checkbox"/>
 IDLE	<input type="checkbox"/>
 IDLE	<input type="checkbox"/>
 IDLE	<input type="checkbox"/>
 IDLE	<input type="checkbox"/>
 IDLE	<input type="checkbox"/>
 IDLE	<input type="checkbox"/>
 IDLE	<input type="checkbox"/>
 IDLE	<input type="checkbox"/>
 IDLE	<input type="checkbox"/>
 IDLE	<input type="checkbox"/>
 IDLE	<input type="checkbox"/>
 IDLE	<input type="checkbox"/>
 IDLE	<input type="checkbox"/>
 IDLE	<input type="checkbox"/>
 IDLE	<input type="checkbox"/>
 IDLE	<input type="checkbox"/>
 IDLE	<input type="checkbox"/>
 IDLE	<input type="checkbox"/>
 IDLE	<input type="checkbox"/>
 IDLE	<input type="checkbox"/>
 IDLE	<input type="checkbox"/>
 IDLE	<input type="checkbox"/>
 IDLE	<input type="checkbox"/>
 IDLE	<input type="checkbox"/>
 IDLE	<input type="checkbox"/>

Port 2 - CASH4K
 up
BCAS disabled 2

☐ All Channels

State	
 IDLE	<input type="checkbox"/>
 IDLE	<input type="checkbox"/>
 IDLE	<input type="checkbox"/>
 IDLE	<input type="checkbox"/>
 IDLE	<input type="checkbox"/>
 IDLE	<input type="checkbox"/>
 IDLE	<input type="checkbox"/>
 IDLE	<input type="checkbox"/>
 IDLE	<input type="checkbox"/>
 IDLE	<input type="checkbox"/>
 IDLE	<input type="checkbox"/>
 IDLE	<input type="checkbox"/>
 IDLE	<input type="checkbox"/>
 IDLE	<input type="checkbox"/>
 IDLE	<input type="checkbox"/>
 IDLE	<input type="checkbox"/>
 IDLE	<input type="checkbox"/>
 IDLE	<input type="checkbox"/>
 IDLE	<input type="checkbox"/>
 IDLE	<input type="checkbox"/>
 IDLE	<input type="checkbox"/>
 IDLE	<input type="checkbox"/>
 IDLE	<input type="checkbox"/>
 IDLE	<input type="checkbox"/>
 IDLE	<input type="checkbox"/>
 IDLE	<input type="checkbox"/>
 IDLE	<input type="checkbox"/>
 IDLE	<input type="checkbox"/>
 IDLE	<input type="checkbox"/>
 IDLE	<input type="checkbox"/>

Restart selected channels

Block selected channels

Unblock selected channels

User can configure (restart/block/unblock channels) individual PRI links or B-channels

PRI/CAS Configuration

PRI/CAS configuration provisioning.

Fax T.38

- ☒ Fax T.38
- ☒ CNG detection

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. The activation of the flag "CNG detection" will only take effect if T.38 flag is also enabled.

Note: T.38 fax calls always start as a voice call and then switch to the T.38 codec.

PRI/CAS Configuration

PRI/CAS configuration provisioning.

Port Configuration

Row	Enable	Circuit ID	Card	Physical port	Signaling method	Clock source priority	Coding	Switch type	Line build out	Terminal mode	
1	<input checked="" type="checkbox"/>	NET5H4K	1	Port 1	ISDN	1	HDB3	EuroISDN	0	<input checked="" type="checkbox"/>	Edit
2	<input checked="" type="checkbox"/>	CASH4K	1	Port 2	CAS - MFCR2	2	HDB3	EuroISDN	0	<input type="checkbox"/>	

Enable: enable or disable the port.

Circuit ID: Circuit ID configuration

Card: Card number

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.

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

PRI/CAS Interface

Select OK to temporarily store changes. Make your changes permanent by selecting 'Apply Changes' on the General page.

General

Physical port: Card 1 - Port 1

Signaling method: ISDN

Line build out: 0

Coding: HDB3

Switch type: EuroISDN

☒ CRC

☐ BCAS

BCAS service message after restart: None

☒ Echo cancellation

Echo tail(ms): 32

Echo training (ms): none

☒ Extended Echo Cancellation

Receive gain (dB): 0

Transmit gain (dB): 0

Default destination: 2055

Clock source priority: 1

☐ Exclusive channel

NOTEa: The LBO used by the OSB T1 line is purely the attenuation of the line, by 7.5, 15 and 22.5 dB, for values 5, 6 and 7. Therefore the length should be depending also on the variation of the repeater configuration.

NOTEb: The value zero is without attenuation and with pulse shaper set to default. The pulse shaper settings are not used by OSB, but it would shape the pulse according to standard cabling and impedance to the distances.

NOTEc: The maximum cable length for the ISDN connectivity depends on the cable characteristics. The card operates in a short haul mode. Typical cable attenuation for .4 millimeter (mm) wire is 3 dB per 100 meter (m) (measured at 1024 kilohertz [KHz]). It is not recommended to use cables longer than 40m (133feet).

NOTEd: For T1 lines it's possible to use the use of Line Build-Out (waveform transmit) configuration. LBO values other than zero compensate for signal attenuation due to the length of the cable connected to an ISDN PRI card, according to the table below:

- 0: 0 db (CSU) / 0-133 feet (DSX-1)**
1: 133-266 feet (DSX-1)
2: 266-399 feet (DSX-1)
3: 399-533 feet (DSX-1)
4: 533-655 feet (DSX-1)

Physical port: PRI card/port number (Read Only)
Signaling method (E1): ISDN or CAS-MFCR2 or CAS Ring Down (only available for 50i DP24). **Framing (T1):** line formatting options ESF (Extended Super Frame) or D4 (Superframe). The ty of framing used is determined by your Telco.
Line build out: each number in the combo box corresponds the following value: 0 - 0 db (CSU) 133 feet (DSX-1), 5 - -7.5db (CSU), 6 - -15db (CSU), 7 - -22.5db (CSU).
Note: LBO is only supported for OSB Configured as T1.
Coding: Line encoding method options AMI (Alternate Mark Inversion) or B8ZS (Bipolar 8 with Z Substitution) for T1 and HDB3 (High Density Bipolar 3) for E1. The line coding used is determin by your Telco.
Switch type: sets protocol by a combo box. E1-> EuroISDN, QSIG and CorNet-NQ. **QSIG/CorNet-NQ only for 50i DP24.**
T1-> NI2, 4ESS, 5ESS Custom, T1CAS, QSIG and CorNet-NQ.
4ESS/5ESS/T1CAS/QSIG/CorNet-NQ only for 50i DP24
CRC: enable/disable CRC4 checking (only E1).
BCAS: enable B-channel Availability Signaling Procedures. Only available for 4ESS and 5ESS this parameter is enabled the user will be able to Block/Unblock an individual B-channel in Chan Maintenance screen. Only when BCAS is enabled Branch will answer isdn SERVICE messages. **BCAS service message after restart:** selects behavior upon receiving isdn RESTART/RESTA ACKNOWLEDGE messages when BCAS is enabled.
Receive gain: sets the Gain of payload for receive. A negative value decreases the gain, an positive value increases the gain (mandatory).
Transmit gain: sets the Gain of payload for transmit. A negative value decreases the gain, an positive value increases the gain (mandatory).
Default destination: destination number if no called party number received for ISDN incoming ca The default destination is also used if just one digit is received and there is not a rule to handle i the Specific Overlap Dialing Patterns table.
Clock source priority: 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 accepted, otherwise channel is preferred (only PRI). This field is editable only if port is configured terminal mode (user side), otherwise it will be always enabled.
Echo cancellation: enables the echo cancellation parameter.
Echo tail: echo tail for Hardware Echo Cancellation. The values available are: 32, 64 and 128. **Echo training (ms):** This parameter is available for PRI/CAS and FXS interfaces that have ec cancellation enabled. Possible values are disabled (default) and from 400 to 1200 ms (w granularity of 100 ms). Enabling echo training will cause the OSB to briefly mute the channel bef opening the audio channel, send an impulse with the configured duration in milliseconds, and the impulse response to pre-train the echo canceller.
Extended Echo Cancellation: This flag applies only for DP14 configured with RAM 2GB (p refresher hardware) and E1 Port, the default value is enabled. Since the OSB50i DP14 p refresher uses SW-DSP OSLEC process, the echo cancelation on 30 simultaneous E1 chann requires high dynamic processing that may affect the system performance. This effect compensated by the **"Extended Echo Cancellation"** functionality but with a possible perception the audio quality level, depending on the phone (e.g. lower on OpenStages or higher on phones). This function can now be disabled to improve voice quality.

PRI/CAS Interface	
PRI/CAS interface provisioning.	
Timers	
T302 timer	15
T305 timer	30
T308 timer	4
T309 timer	90
T313 timer	4

T302: timer to wait for digits for overlap dialing.
T305: timer to wait for DISCONNECT ACK once DISCONNECT is sent out, if this timer expires RELEASE is sent and T308 is started.
T308: 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.
T309: maintain active calls on layer 2 disconnection, calls are cleared if connection is not established before T309 timer expires.
T313: 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).

If you are experiencing audio / noises issues, configure each step at time and perform call tests to check the call quality if the noise persists.

Step by step

10. Disable **Extended Echo Cancellation** and perform new tests. (Only for DP14). Check if it that brings better quality to your calls.

11. Uncheck the flag **Extended Echo Cancellation** (Only for DP14).
 - 2.1 Set the **Echo Training System** to **400ms**. Perform new tests and check the result.

- 2.2 Set the **Echo Training System** to **800ms**. Perform new tests and check the result.

- 12.If none of the previous alternatives takes effect, consider disabling the **Echo Cancellation Feature** as indicated below:

PRI/CAS Interface

PRI/CAS interface provisioning.

Advanced

<input checked="" type="checkbox"/> Sending complete	<input type="checkbox"/> Far end disconnect with inband announcement
<input type="checkbox"/> Calling name delay	<input type="checkbox"/> Second screening indicator
<input type="checkbox"/> Send calling party name	<input type="checkbox"/> Data calls allowed
Calling party name: Facility IE	Setup progress indicator: none
<input type="checkbox"/> Send redirecting number	183 Session progress without SDP: Alerting
Redirecting number: Facility IE	<input checked="" type="checkbox"/> Always send PI8 in ALERT
Channel mapping: Physical	<input type="checkbox"/> QSIG ringback
<input checked="" type="checkbox"/> Restart link at start-up	<input type="checkbox"/> Start early media on CALL PROCEEDING
L3 trunk restart type: Restart Interface	<input type="checkbox"/> Disable far end restart
<input type="checkbox"/> B-channel parallel restarts	Idle reset interval:
<input type="checkbox"/> Group restarted b-channels in channel identification IE	<input type="checkbox"/> Busy Detect Disconnect
<input checked="" type="checkbox"/> Ignore Dial Tone On Setup Without CPN	<input type="checkbox"/> Do not send ISDN Status Message

Sending complete: add Sending Complete information element in SETUP messages (T1 Only)

Calling name delay: Calling Name will be provided in a separate ISDN message. In this case, the SIP INVITE message will postponed until the Facility with Calling Name is received or after a fixed 2 seconds timer expires.

Send calling party name: enable/Disable the sending of the Calling Name information in outgoing calls

Calling party name: Indicates in which Information Element the Calling Party Name information should be delivery: Facility IE or Display IE.

Send redirect number: Enable/Disable the sending of the Redirecting Number in outgoing calls

Redirecting number: Indicates in which Information Element the Redirecting Number information should be delivery in outgoing calls: Facility IE or Redirecting number IE.

Channel mapping: possible values: Logical/Physical
Physical: channels from 1-15 17-31, channel 16 is not used.
Logical: channels from 1-30, channel 16 is used as "pseudo" b-channel. This is default for Qsig/Cornet switch types.

Restart link at start-up: if enabled send PRI restart message after link start-up.

L3 trunk restart type: Restart Channel (a RESTART message is sent for each channel) or Interface can be configured.

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

Group restarted b-channels in channel identification IE: ability to daisy-chain channels within the Channel Identification Information Element (CIIE). The multi-channel CIIE will be used in the RESTART and RESTART ACKNOWLEDGE messages.

Ignore Dial Tone On Setup Without CPN: incoming SETUP is received without Called Party Number and without Sending Complete the OSB will play dial tone on the line if this flag is clear. If this flag is set the OSB won't play dial tone in this scenario.

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).

Second screening indicator: second screening indicator will be used in incoming setup message (E1 Only).

Data calls allowed: Incoming call with digital information bearer capability is allowed or not.

Setup progress indicator: Configures the Progress Indicator in SETUP message (New Zealand). The following options are supported: Call is not end-to-end, Destination address is non ISDN, Origination address is non ISDN and None

183 Session progress without SDP: OSV 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, Alerting, Progress and Alerting and None.

Always send PI8 in ALERT: if flag is enabled, OSB 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.

QSIG ringback: Do not play ringback for QSIG/CORNET if flag is disabled.

Start early media on CALL PROCEEDING: command will cause the OSB to raise a SIP 183 Session Progress message with an SDP Answer as soon as it receives the ISDN CALL PROCEEDING message.

Disable far end restart: 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.

Idle reset interval:

Busy Detect Disconnect: If enabled the call is disconnected upon busy tone detection.

Do not send ISDN Status Message: If this flag is set OSB will never send ISDN Status Message out.

PRI/CAS Interface

PRI/CAS interface provisioning.

Channels

☒ All channels

Enable	Number	CAS Initial State
<input checked="" type="checkbox"/>	1	idle
<input checked="" type="checkbox"/>	2	idle
<input checked="" type="checkbox"/>	3	idle
<input checked="" type="checkbox"/>	4	idle
<input checked="" type="checkbox"/>	5	idle
<input checked="" type="checkbox"/>	6	idle
<input checked="" type="checkbox"/>	7	idle
<input checked="" type="checkbox"/>	8	idle
<input checked="" type="checkbox"/>	9	idle

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.

Channels

☒ All channels

Enable	Number	Trunk group	CAS profiles	Own number	Ring-down destination	Comments
<input checked="" type="checkbox"/>	1	OGPort2	ARD - ARD E1 Default Profile	15619232555	23451222	
<input checked="" type="checkbox"/>	2	OGPort2	MRD - MRD	15619232556	23451223	
<input checked="" type="checkbox"/>	3	OGPort2	Hoot n Holler - HootHoller	15619232557	23451224	

PRI/CAS Interface -> Channels

List is showed when PRI Interface is configured with Signaling method as CAS Ring Down.

PRI/CAS Configuration

PRI/CAS configuration provisioning.

CAS Advanced Settings

These fields are only applicable when the signaling method of a PRI/CAS port is CAS.

☒ Enable E1 CAS MFC-R2 advanced settings

E1 CAS MFC-R2 advanced settings

E1 CAS MFC-R2 profile

E1 CAS Ring Down profile

Ring down channels

☐ Enable Session Refresh Timeout

Ring-down audit interval (sec)

0

☐ Enable Ring-Down Call Refresh to Integrated Gateway

☐ Enable Notify on Switchover to MLC

CAS E1 Advanced Settings

Enable E1 CAS MFC-R2 advanced settings: Enabling/Disabling CAS Table Configuration Timers. To configure the timer values click the "CAS Advanced Settings" button. Only recommended for advanced users

Enable Session Refresh Timeout: When this flag is set, the call will be disconnected if the session's time expires

Ring-down audit interval (sec): Interval in seconds in which audit mechanism will be executed, checking transmitting and receiving RBS bits and unexpected states. It can assume values from 10s to 3600s, or 0 to disable it. The default is 0.

Enable Ring-Down Call Refresh to Integrated Gateway: If flag is enabled, when an ARD, MRD or Hoot-n-Holler channel is involved in a call and it receives an INVITE with the X-Siemens-Application-Data and with a new call id from the same originator DN as from the current ongoing call, it shall disconnect the old call and establish a new call from the received INVITE. This action shall be taken both in normal and in survivable mode.

Enable Notify on Switchover to MLC: enable / disable sending the NOTIFY message with the header Event: server-switchover to each MLC.

CAS Advanced Settings

These fields are only applicable when the signaling method of a PRI/CAS port is CAS.

☐ Enable E1 CAS advanced settings

☐ Enable Session Refresh Timeout

Ring-down audit interval (sec)

☐ Enable Ring-Down Call Refresh to Integrated Gateway

☐ Enable Notify on Switchover to Integrated Gateway

Advanced SIP to ISDN Cause Code Mapping

500/503 (38) Network Out of Order
(38) Network Out of Order
(41) Temporary Failure

OK Cancel

Advanced SIP to ISDN Cause Code 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**

E1 CAS Advanced Settings

E1 CAS Advanced Settings provisioning.

Timeout for backward request to resume cycle	150
Call forward safety	30000
Wait for seize acknowledge	8000
Wait for answer	65000
Double answer	400
Answer delay	150
Persistence check	500
DTMF start dialing	500
MF threshold time	0
spare timer1	
spare timer2	
spare timer3	
spare timer4	
spare timer5	

E1 CAS MFC-R2 advanced settings

NOTE: 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.

Call forward safety: Forward Safety Timer.

Wait for seize acknowledge: How much time it is waited for a response to our SEIZE signal.

Wait for answer: How much time it is waited when the call has been accepted.

Double answer: When double answer is in effect, it is the interval between the ANSWER, CLEARBACK and ANSWER again.

Answer delay: Short delay before answering to give the other end an additional time to detect the tone off condition

Persistence check: How much time it is waited for CAS signaling before handling the new signal.

DTMF start dialing: DTMF Start Dialing Timer

MF threshold time: Time that an MF tone should last before being handled.

E1 CAS Profiles

E1 CAS Profiles provisioning.

Default E1 CAS Profiles

Default E1 CAS profiles Argentina Telefonica

Add profile

E1 CAS MFC-R2 profile

There are several pre-defined CAS profiles that can be used on a Branch. 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.

E1 CAS Profiles

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.

Row	Name	ANI before DNIS	Maximum amount of ANI	Maximum amount of DNIS	Maximum waiting time of MF back tone	Metering pulse timeout	Skip category	Immediate accept	Charge calls	Enable forced release
1	Automation	<input type="checkbox"/>	12	12			<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
2	Argentina Telecom	<input type="checkbox"/>							<input type="checkbox"/>	<input type="checkbox"/>
3	Brazil Embratel 2	<input type="checkbox"/>							<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
4	Mexico 1	<input type="checkbox"/>							<input checked="" type="checkbox"/>	<input type="checkbox"/>
5	Korea	<input type="checkbox"/>							<input checked="" type="checkbox"/>	<input type="checkbox"/>

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.

E1 CAS Profiles

E1 CAS Profiles provisioning.

E1 CAS Ring Down profile

Table with a summary of E1 CAS Ring Down profiles. It is possible to Add/Edit/Delete a profile.

Add

Edit

Delete

Row	Name	Profile type
1	ARD E1 Default Profile	ARD - Automatic Ring Down
2	MRD	MRD - Manual Ring Down
3	ARD N to 1	ARD N to 1 - Automatic Ring Down
4	HootHoller	Hoot-n-Holler

ARD E1 Default Profile is a reserved profile that can not be deleted. The only editable fields are Idle/Onhook bits and Seized/Offhook bits. This profile will be automatically assigned to all channels in a trunk group which E1 CAS signaling is Ring Down and the field E1 CAS profile is empty.

E1 CAS Profile

E1 CAS Profile provisioning.

Profile

Profile name: Name of the profile.

Profile type: Type of the profile E1 CAS signaling

Profile name

MRD

Profile type

MRD - Manual Ring Down

Timer

Start time (ms)

300

After start time (ms)

500

Wink time (ms)

1500

Receiver wink time (ms)

1000

Advanced

Idle/Onhook bits

1001

Seized/Offhook bits

0001

Ring-down refresh

info

Timer

Start time: this timer is used to delay dial in Immediate Start and to delay the seizure in ARD
After start time: this timer determines a guard time after seizure in ARD.

Wink time: timer determines for how long the wink will be applied in an incoming call in E&M Wink and determines for how long the wink will be applied in an outgoing call in MRD

Receiver wink time: this timer determines the longest time the GW will wait for the wink to be removed by PSTN.

Advanced

Idle/Onhook bits: Sets the RBS bits which will be defined to an idle state.

Seized/Offhook bits: Sets the RBS bits which will be defined to a seizure state.

Ring-down refresh: Defines the method of manual ring down receiving or sending a call refresh on the VoIP connection after a call is established. It can be "dtmf", which sends an RTP event 'A', or "info", which sends an INFO SIP message. (MRD only).

Ring Down Channels

Ring Down Channels management.

Ring down channels

Table with the summary of E1 CAS channels configured as Ring Down.

Search for in

Row	Enable	Channel	Trunk group	CAS signaling	CAS profile	Own number	Ring-down destination	Comments
1	<input checked="" type="checkbox"/>	Card 1 - Port 2 - Channel 1	OGPort2	ARD - Automatic Ring Down	ARD E1 Default Profile	15619232555	23451222	
2	<input checked="" type="checkbox"/>	Card 1 - Port 2 - Channel 2	OGPort2	MRD - Manual Ring Down	MRD	15619232556	23451223	
3	<input checked="" type="checkbox"/>	Card 1 - Port 2 - Channel 3	OGPort2	Hoot-n-Holler	HootHoller	15619232557	23451224	
4	<input checked="" type="checkbox"/>	Card 1 - Port 2 - Channel 4	OGPort2	ARD - Aut				
5	<input checked="" type="checkbox"/>	Card 1 - Port 2 - Channel 5	OGPort2	ARD - Aut				

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 signaling: The signaling 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)

PRI/CAS Configuration

CAS Advanced Settings

These fields are only applicable when the signaling method of a PRI/CAS port is CAS.

T1 CAS profile

☐ Enable Session Refresh Timeout

Ring-down audit interval (sec)

0

☐ Enable Ring-Down Call Refresh to Integrated Gateway

☐ Enable Notify on Switchover to MLC

Ring down channels

CAS T1 (and E1) Advanced Settings

Enable Session Refresh Timeout: When this flag is set, the call will be disconnected if the session's time expires

Ring-down audit interval (sec): Interval in seconds in which audit mechanism will be executed, checking transmitting and receiving RBS bits and unexpected states. It can assume values from 10s to 3600s, or 0 to disable it. The default is 0.

Enable Ring-Down Call Refresh to Integrated Gateway: If flag is enabled, when an ARD, MRD or Hoot-n-Holler channel is involved in a call and it receives an INVITE with the X-Siemens-Application-Data and with a new call id from the same originator DN as from the current ongoing call, it shall disconnect the old call and establish a new call from the received INVITE. This action shall be taken both in normal and in survivable mode.

Enable Notify on Switchover to MLC: enable / disable sending the NOTIFY message with the header Event: server-switchover to each MLC.

T1 CAS Profiles

T1 CAS Profiles provisioning.

T1 CAS Profiles

Table with the summary of T1 CAS profiles configuration. It is possible to Add/Edit/Delete a profile.

Add Edit Delete

Row	Name	Profile type
1	ARD Default Profile	ARD - Automatic Ring Down
2	MRD T1	MRD - Manual Ring Down
3	ARD N to 1 T1	ARD N to 1 - Automatic Ring Down
4	HootHoller T1	Hoot-n-Holler
5	EM Imm T1	E&M Immediate Start
6	EM Wink	E&M Wink Start

ARD Default Profile is a reserved profile that can not be deleted. The only editable fields are Idle/Onhook bits and Seized/Offhook bits. This profile will be automatically assigned to all channels in a trunk group which T1 CAS signaling is Ring Down and the field T1 CAS profile is empty.

T1 CAS Profile

T1 CAS Profile provisioning.

Profile

Profile name: Name of the profile.
Profile type: Type of the profile T1 CAS signaling.

Profile name Profile type

Timer

Pre-wink time (ms) Delayed dial/Start time (ms)
Wink time (ms) **Receiver wink time (ms)**
 Digit guard time (ms) Ring detection time (sec)
 Debounce time (ms) Interdigit time (sec)
 Wait disconnect time (sec) After start time (ms)

Advanced

Idle/Onhook bits Seized/Offhook bits
 Ring-down refresh

Advanced

Idle/Onhook bits: Sets the RBS bits which will be defined to an idle state.
Seized/Offhook bits: Sets the RBS bits which will be defined to a seizure state.
Ring-down refresh: Defines the method of manual ring down receiving or sending a call refresh on the VoIP connection after a call is established. It can be "dtmf", which sends an RTP event 'A', or "info", which sends an INFO SIP message. (MRD only).

Timer

Pre-wink time: after the offhook is detected from PSTN, the GW shall wait this time before sending the wink signal.
Delayed dial/Start time: this timer is used to delay dial in Immediate Start and to delay the seizure in ARD.
Wink time: timer determines for how long the wink will be applied in an incoming call in E&M Wink and determines for how long the wink will be applied in an outgoing call in MRD.
Receiver wink time: this timer determines the longest time the GW will wait for the wink to be removed by PSTN.
Digit guard time: this timer determines a delay on starting sending digits after the wink.
Ring detection time: this time will determine how long an incoming call will ring before being disconnected.
Debounce time: this time will prevent an offhook (as answer) to be changed to an onhook before being debounced by the peer party.
Interdigit time: this timer determines the timeout for dialing.
Wait disconnect time: this time will determine how long the iGW will wait for the peer side to disconnect after it has gone onhook.
After start time: this timer determines a guard time after seizure in ARD.

56.4.3 PRI - Trunk Group Configuration

Integrated Gateway

Integrated gateway provisioning.

Gateway Configuration

Card 1 PRI/CAS Configuration Trunk group

Card 2 FXS Configuration Trunk group

OSB-GW-Only-2PRI - Trunk Groups - Windows Internet Explorer

http://21.21.29.10/trunkGroups.html?board=0&country=br&mode=proxy

Trunk Groups

Trunk Groups provisioning.

Add Trunk Group.
After created, it is possible to Edit/Delete existing Trunk Groups.

Add Edit Delete

Row	Type	FQDN	Trunk group name	Trunk selection	Hunt type
1	PRI/CAS	og.unow.net5.cwb	OGPort1	TopToBottom	Circular
2	PRI/CAS	og.unow.cas.cwb	OGPort2	TopToBottom	Circular

Trunk Group Configuration

Select OK to temporarily store changes. Make your changes permanent by selecting 'Apply Changes' on the General page.

General Channels list Number Modification Spare Flags

Configuration

Type PRI/CAS

FQDN og.unow.cas.cwb

Trunk group name OGPort2 Restart trunk group channels

Trunk selection Top To Bottom

Hunt type Circular

Direction Both

Voice bearer capability Speech

☐ Mark sRTP call-leg as secure

Configuration

Type: port type (read only data).

FQDN: required for Trunk Group and to be used later on in "Gateway/Trunk Configuration"/

Trunk group name: name of the Trunk Group

Restart trunk group channels: Restart the enabled channels from selected list.

Trunk selection: selecting from High or Low Trunk first is possible.

Hunt type: linear or circular selection

Direction: Specifies the direction of traffic flow supported on the trunk group.

Mark sRTP call-leg as secure: if a secure media isnegotiated 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

Trunk Group Configuration

Select OK to temporarily store changes. Make your changes permanent by selecting 'Apply Changes' on the General page.

General Channels list Number Modification Spare Flags

Incoming Calls

Max overlap digit length

☒ Specific overlap dialing patterns

Add

Delete

Row	Dialing pattern	Maximum digit length
1	0800%	10

☐ Connected line identification presentation incoming

Answer Supervision Timer - Incoming Call (sec) 360

Blacklist profile

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. If not configured then T302 timer would apply

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.

Connected line identification presentation incoming:

Answer Supervision Timer – Incoming Calls: Value between 120 and 3600. Default is 360. Note: Corresponding Answer Supervision Timers should be configured under 'Feature'-'>'Gateway/Trunk'.

Timers should be configured with a difference of at least 10 seconds between Gateway/Trunk and Integrated Gateway to avoid racing conditions caused by simultaneous disconnection.

Blacklist profile: Specifies the Blacklist profile that it will be checked during incoming calls.

Trunk Group Configuration

Select OK to temporarily store changes. Make your changes permanent by sel

General Channels list Number Modification Spare Flags

Outgoing Calls

☐ Set Numbering Plan to ISDN

Pre dial delay for DTMF (sec)

2

☐ Send Redirect Number instead of calling number for redirected calls

☐ Calling Party Number Presentation Restricted

☐ Connected line identification presentation outgoing

Answer Supervision Timer - Outgoing Call (sec) 170

Outgoing Calls

Set numbering plan to ISDN: it is set to enable/disable. When the Number Type is Unknown, it will set the Numbering Plan to ISDN. Otherwise, it will set to Unknown (only PRI)

NOTE: This flag applies only to Called Party Number

Send Redirect Number instead of calling number for redirected

calls: If selected (enabled), a call that is redirected to the PSTN will have the last redirecting or transferring party's identity as the Calling Party Number information element. This attribute is primarily intended for use when connecting to a carrier that does not understand the Redirecting Party Number information element.

Calling Party Number Presentation Restricted: Set calling party number presentation restricted to all outgoing call.

Connected line identification presentation incoming:

Answer Supervision Timer – Outgoing Call: Value between 120 and 3600. Default is 170. Note: Corresponding Answer Supervision Timers should be configured under 'Feature'-'>'Gateway/Trunk'.

Trunk Group Configuration

Select OK to temporarily store changes. Make your changes permanent by selecting

General

Channels list

Number Modification

Spare Flags

Collect Calls

These fields are only applicable when the country is Brazil.

Collect call control

☒ Permission for receiving collect calls by category

☒ Permission for receiving collect calls by double answer

Unify Inc.

Pag

Collect Calls

Collect call control: who will check the permission for collect calls:

Server -> will add X-Siemens-header:collect-call in NM for calls with the indication of collect call. In SM, these calls will be rejected if permission is denied.

Gateway -> Branch will check the permission in SM and NM, and reject calls with the indication of collect call, if permission is denied.

Permission for receiving collect calls by category: In case of CAS, it 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 if Collect Call Control is Gateway (NM/SM) or Server (SM). In case of ISDN, if this flag is not checked, incoming calls with Reverse Charge Indication will be rejected, if Collect Call Control is Gateway (NM/SM) or Server (SM).

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. Only works for CAS and Brazil.

Trunk Group Configuration

Select OK to temporarily store changes. Make your changes permanent by selecting 'Apply Changes' on the General page.

General Channels list Number Modification Spare Flags

E1 CAS - Ring Down

E1 CAS signaling Ring Down

E1 CAS profile ARD - Default Profile

Number	Cas Profile	Own number	Ring-down destination	Comments
Card 1 - Port 2 - Channel 1	ARD - ARD E1 Default Profile	15619232555	23451222	
Card 1 - Port 2 - Channel 2	MRD - MRD	15619232556	23451223	
Card 1 - Port 2 - Channel 3	Hoot - HootHoller	15619232557	23451224	
Card 1 - Port 2 - Channel 4	ARD - ARD E1 Default Profile			
Card 1 - Port 2 - Channel 5	ARD - ARD E1 Default Profile			

E1 CAS – Ring Down

Number: Shows Card, Port, and Channel Number

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)

Trunk Group Configuration

Select OK to temporarily store changes. Make your changes permanent by selecting 'Apply Changes' on the General page.

General Channels list Number Modification Spare Flags

E1 CAS - MFC R2

These fields are only applicable when the framing of a port is E1 CAS.

E1 CAS profile Automation

☐ Do Not Accept Call on Offer

☒ CAS Answer for Early Media

☐ Send End of ANI with Presentation Allowed

☐ CAS Send Early Media

E1 CAS – MFC R2

E1 CAS profile: Select any of the created CAS profiles in CAS profiles table. CAS profile association is **mandatory** for CAS E1 trunk groups.

Do Not Accept Call on Offer: If set, the gateway waits for subscriber state (free, busy, unallocated) before sending backward tone from Group B. If not set, the gateway always sends free subscriber backward tone immediately after receiving a CAS call. The default is disabled.

CAS Answer for Early Media: If set allows answer in CAS calls to play announcements. Otherwise, send the appropriate backward tone.

Send End of ANI with Presentation Allowed: If set sends end of identification with presentation allowed. Otherwise, sends end of identification with presentation restricted. (Only Argentina)

CAS Send Early Media: If set sends 183 Session Progress to the SIP side when making outgoing calls in E1 CAS. Otherwise, sends 180 Ringing.

Trunk Group Configuration

Select OK to temporarily store changes. Make your changes permanent by selecting 'Apply Changes' on the General page.

General Channels list Number Modification Spare Flags

T1 CAS

These fields are only applicable when the Switch type of a port is T1 CAS.

T1 CAS signaling E&M Immediate Start T1 CAS addressing signaling DTMF

T1 CAS profile EM Imm T1 - E&M Immediat

T1 CAS

T1 CAS signaling: The signaling of the selected channels. It defines the protocol the Gateway is configured with the CO.

T1 CAS addressing signaling: The addressing type of digits to be sent in the signaling. It can be DTMF or MF.

T1 CAS profile: Select a profile from the available profile list. The profiles must be created before in PRI Configuration. If T1 CAS signaling is Ring Down, ARD Default Profile will be automatically assigned to those channels that have never had the T1 CAS profile assigned before, this value can be changed afterwards.

Trunk Group Configuration

Select OK to temporarily store changes. Make your changes permanent by selecting 'Apply Changes' on the General page.

General Channels list Number Modification Spare Flags

T1 CAS

These fields are only applicable when the Switch type of a port is T1 CAS.

T1 CAS signaling Ring Down T1 CAS addressing signaling None

T1 CAS profile ARD Default Profile - ARD -

T1 CAS – Ring Down

Number	Cas Profile	Own number	Ring-down destination	Comments
Card 1 - Port 1 - Channel 1	ARD - ARD Default Profile	551138172001	12341001	
Card 1 - Port 1 - Channel 2	MRD - MRD T1	551138172002	12341002	
Card 1 - Port 1 - Channel 3	Hoot - HootHoller T1	551138172003	12341003	
Card 1 - Port 1 - Channel 4	ARD - ARD Default Profile			
Card 1 - Port 1 - Channel 5	ARD - ARD Default Profile			

Trunk Group Configuration

Select OK to temporarily store changes. Make your changes permanent by selecting 'Apply Changes' on the General page.

General Channels list Number Modification Spare Flags

Configuration

When adding a trunk group with E1/T1 CAS channels, specific configuration will be shown only after the first E1/T1 CAS channel is added to the trunk group.

Channels list

Filter

Card 1 - Port 1
Card 1 - Port 2

>>

<<

Selected Channel

Card 1 - Port 1 - channel 1
Card 1 - Port 1 - channel 2
Card 1 - Port 1 - channel 3
Card 1 - Port 1 - channel 4
Card 1 - Port 1 - channel 5
Card 1 - Port 1 - channel 6
Card 1 - Port 1 - channel 7
Card 1 - Port 1 - channel 8
Card 1 - Port 1 - channel 9
Card 1 - Port 1 - channel 10
Card 1 - Port 1 - channel 11
Card 1 - Port 1 - channel 12
Card 1 - Port 1 - channel 13
Card 1 - Port 1 - channel 14

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.

The left-hand list shows the list of PRI 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.

Trunk Group Configuration

Select OK to temporarily store changes. Make your changes permanent by selecting 'Apply Changes' on the General page.

General Channels list Network specific facilities Number Modification Spare Flags

Configuration

☒ Send NSF

Network ID

Facility coding value

Service parameters

☐ Ignore incoming NSF

NSF is only available for T1.

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

Send NSF: enabling/disabling sending the NSF.

Network ID: Four-digit code that indicates the carrier network which the service/feature will be requested. If empty, it indicates the local service provider.

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.

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

56.5 Integrated Gateway – General Settings

56.5.1 Gateway/Trunk Configuration

Gateways/Trunks												
Gateways/Trunks provisioning.												
Row	Signaling address type	Remote URL	Port	Interface	Transport	Routing prefix	Gateway/Trunk type	Functional type	Trunk profile	Output digit strip	Output digit add	Priority
1	IP address or FQDN	og.unow.net5.cwb	5096	LAN	UDP	0290%	Integrated Gateway	All Modes Egress/Ingress	Gateway	4		1
2	IP address or FQDN	og.unow.cas.cwb	5096	LAN	UDP	0291%	Integrated Gateway	All Modes Egress/Ingress	Gateway	4		1

Remote URL: should contain FQDN configured for trunk group.

Port: 5096 must be used for Integrated GW.

Transport: UDP must be used.

GW Type: Integrated Gateway must be selected.

Trunk profile: Gateway must be used.

56.5.2 SIPQ V2

50i DP24 supports QSIG and Cornet-NQ.

In normal mode QSIG and Cornet-NQ messages are tunneled to OSV through SIPQ V2. In survivable mode QSIG and Cornet-NQ will be translated to regular SIP with a limitation on feature support.

The support of QSIG by OSB is required to allow subscribers on an OSV to interwork with subscribers on networked HiPath3000/4000 and 3rd party PBXs. SIPQ V2 is required in order to support SRTP over connections established via SIPQ. SIPQv1 will not be supported by OSB.

In case of interconnection with old PBXs, the flag "truncated mime" should be activated in the OSV.

56.5.3 Blacklist

Trunk Groups	
Trunk Groups provisioning.	
Blacklist Profile	
Blacklist Profile	

Possible to blacklist incoming calls based on Calling Party Number.
Feature applies only for integrated gateway trunks on both NM and SM.
Disconnection cause code will be Normal Call Clearing.
No CDR will be created.

Blacklist Profiles

Blacklist profiles provisioning.

Row	Name
1	List01
2	List02

Max of 20 profiles can be created

Add Edit Delete

Trunk Groups

Trunk Groups provisioning.

Row	Type	FQDN
1	PRI/CAS	siemens.com

Endpoint Service Profile

Blacklist profile

Blacklist profiles

Endpoint service profiles provisioning.

Row	Name
1	Blacklist profile 1

Add Edit Delete

Blacklist profile configuration

Endpoint service profile configuration provisioning.

General

Name Blacklist profile 1

Blocked Calls

Row	Denied number
1	0800%

Add Delete

Max of 20 entries in each profile.
Max of 24 digits in each entry.

Denied numbers can be defined with special character %: i.e, %5000 (suffix) or 4989% (prefix)

Patterns can be defined with special character %, i.e, %9232473 (suffix) or 561923% (prefix) using the same match pattern as in the trunkgroup match.

Trunk Group Configuration

Select OK to temporarily store changes. Make your changes permanent by selecting OK and Save.

General Channels list Number Modification Spare Flags

Configuration

Type

FQDN

Trunk group name

Trunk selection Hunt type

Direction ☐ Mark sRTP call-ID

Voice bearer capability

Incoming Calls

Max overlap digit length

☐ Specific overlap dialing patterns

☐ Connected line identification presentation incoming

Blacklist profile

Outgoing Calls

Each trunk group can have a profile associated

New call restriction context will be created in B2B extension files;

Blacklist feature shall apply only for integrated gateway trunks (S0,S2,FXO), on both NM and SM;

FXO: Only possible if the CLIP is supported.

B2B will disconnect/hangup and no INVITE will be sent to Kamailio;

Trunk Group Configuration

Select OK to temporarily store changes. Make your changes permanent by selecting 'Apply Changes' on the General page.

General Channels list Network specific facilities Number Modification Spare Flags


Configuration


Type: PRI/CAS
 FQDN: tkg1.unify
 Trunk group name: tkg1 **Restart trunk group channels**
 Trunk selection: Top To Bottom Hunt type: Linear
 Direction: Both ☐ Mark sRTP call-leg as secure
 Voice bearer capability: Speech

Incoming Calls

Max overlap digit length:
☐ Specific overlap dialing patterns
☐ Connected line identification presentation incoming
 Answer Supervision Timer - Incoming Call (sec): 360
☐ Force FQDN in Contact Header for Incoming Calls in NM
 Blacklist profile:
☐ Enable IPC Redundancy Call delay in ms: 0

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 0 msec.

 **Integrated Gateway**

 Integrated gateway provisioning.

Gateway Configuration

Card 1	<input type="text" value="PRI/CAS"/>	<input type="button" value="Configuration"/>	<input type="button" value="Trunk group"/>
Card 2	<input type="text" value="FXS"/>	<input type="button" value="Configuration"/>	<input type="button" value="Trunk group"/>

QoS Monitoring

☒ Enable 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.

QoS Monitoring

QoS monitoring provisioning.

Configuration

☒ Send traps

Reporting mechanism: Threshold crossing

QCU IP address: 10.234.1.10

QCU port: 12010

Maximum jitter threshold: 20

Average round trip delay threshold: 100

Lost packets threshold compressing: 10

Lost packets threshold not compressing: 10

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.

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.

56.5.4 Codec Configuration

VOIP

Select OK to temporarily store changes. Make your changes permanent by selecting 'Apply Changes' on the General page.

Sip Server Settings | Port and Signaling Settings | Manipulation and Routing | Error Codes | **Media**

Media Profiles

Select Profile "igw_lan" and press Edit

Add Edit Delete

Profile name	Codecs	Media protocol	Key exchange method	Mark sRTP Call-leg as Secure	Single m-line SRTP
default		Strict Pass-Thru	none		
igw_lan	G711A,G711U,G729	Best Effort SRTP	mikey	✓	
b2bua_profile	G711A,G711U	RTP only	none		

Media Profile

Select OK to temporarily store changes. Make your changes permanent by selecting 'Apply Changes' on the General page.

General

Name: igw_jan

Media protocol: Best Effort SRTP

SRTP configuration

SRTP crypto context negotiation: mikey

☒ Mark SRTP Call-leg as Secure

☐ Single m-line SRTP

Codec configuration

☒ Allow unconfigured codecs

☐ Enforce codec priority in profile

☐ Send Telephony Event in Invite without SDP

Packetization interval: auto

Codec: G722 8 kHz - 64 kbps **Add**

Move up **Move down** **Delete**

Priority	Codec Name
1	G711A 8 kHz - 64 kbps
2	G711U 8 kHz - 64 kbps
3	G729 8 kHz - 8 kbps

Media Protocol: Media security supported for calls to and from the Integrated GW.

Key Exchange Method: if Best Effort SRTP is selected then is possible to configure mikey (Multimedia Internet KEYing) or sdes (Security Descriptions).

Mark SRTP call-leg as Secure: if checked then the call will be marked as secure with the SIP X-Siemens Call-Type: ST-Secure header for all FXS ports when TLS/SRTP is used. Otherwise, the SIP X-Siemens-Call-Type: ST-Insecure header will be sent.

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.
Note: Codecs can be selected/enable under Features->Enable Codec Support for transcoding->Configure->Select codecs.

Priority: 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.

NOTE: For OSB, Multiple packetization interval is not allowed, the same value for all rows **MUST** be used.

56.5.5 CID Suppression

Features

Enable/Disable desired Feature.

Features Available in Survivability Mode Only

Multi-line Hunt Groups **Configure**

Call Forwarding **Configure**

☒ Enable Call Detail Records **Configure**

☒ Enable Music On Hold for Gateways & Subscribers

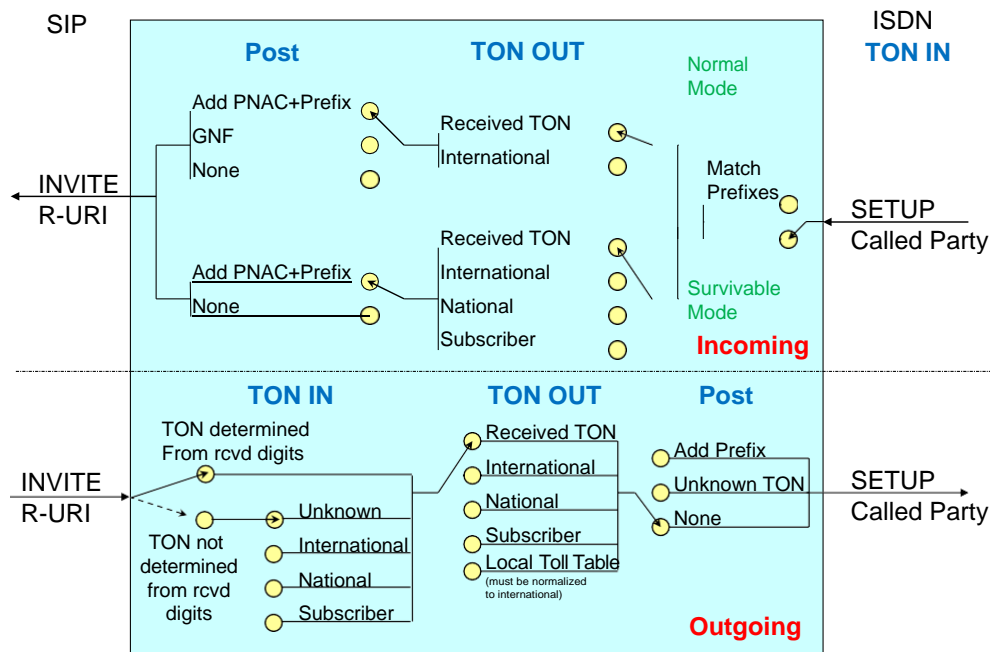
☐ Use PAI/PPI as ISDN Calling Party Number

☒ System calling number suppression access code: *51

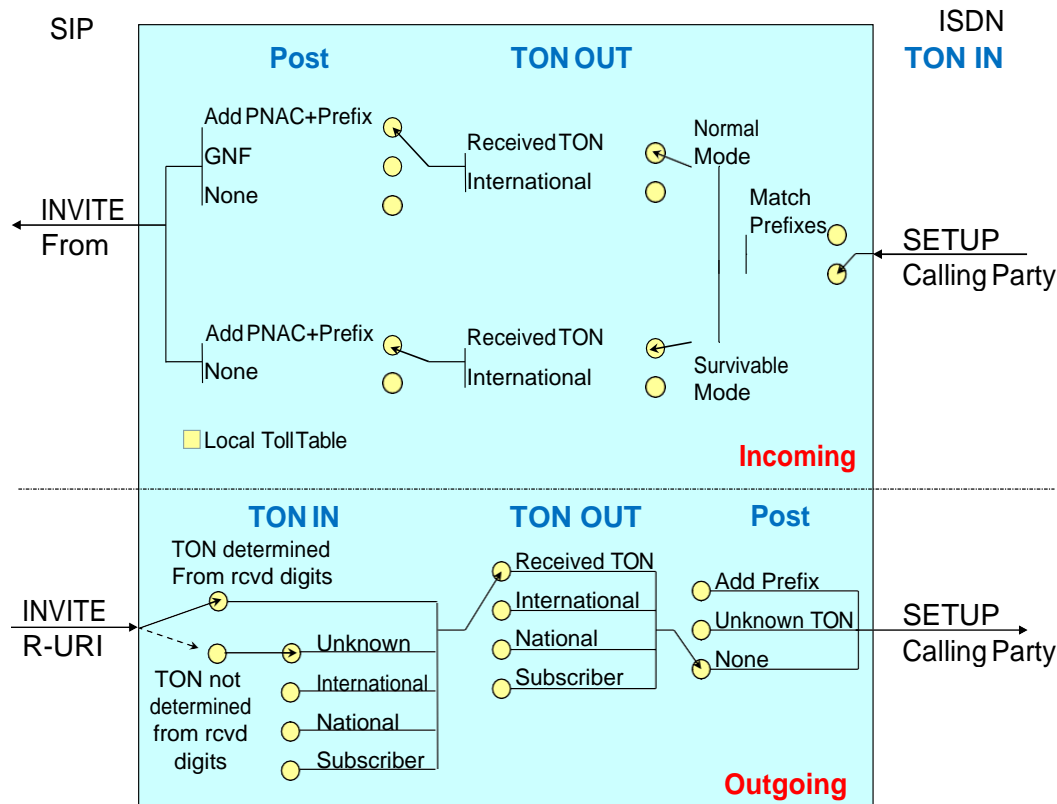
System calling number suppression – access code: allows the Branch subscriber to use the Calling Line Identification Restriction (CLIR) feature in a per call basis. To avoid the presentation of the caller party number to the called party, the caller shall enter de configured access code in the beginning of dial, before the gateway routing prefix and the destination number.
Note: Only applies in Survivable Mode.

56.5.6 Number Modification

The new Called Party Number/Request URI handling will be as shown below:



The new Calling Party Number handling will be as shown below:



Trunk Group Configuration

Select OK to temporarily store changes. Make your changes permanent by selecting 'Apply Changes' on the General page.

General **Channels list** **Number Modification** **Spare Flags**

Definitions

Country code Area code

National number length Subscriber number length

Prefixes

International PNAC International prefix

National PNAC National prefix

Subscriber PNAC Subscriber prefix

Definitions

Country code: configuration of the country code

Area code: configuration of the Local Area Code

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: configuration of the international Public Network Access Code (PNAC)

International prefix: configuration of the international prefix.

National PNAC: configuration of the national PNAC.

National prefix: configuration of the national prefix.

Subscriber PNAC: configuration of the subscriber PNAC.

Subscriber prefix: configuration of the subscriber prefix

Gateway Number Modification Default Settings

With the default settings:

- Incoming calling and called party numbers are sent as received to the proxy's Number Manipulation function, prefixed with PNACs and prefixes.
- Outgoing calling party numbers are sent to the PSTN as received from the proxy's Number Manipulation function without post-manipulation.
- Outgoing called party numbers are sent to the PSTN as received from the proxy's Gateway Routing function without post-manipulation.

Note that not having post-manipulation enabled means that if the OSB 50i/500i receives prefixed numbers from the OSB proxy, these numbers are mostly sent without the prefixes to the PSTN. In order to still send the prefixes, the post-manipulation must be set to 'Send Prefixes'.

The integrated gateway will perform best when it receives numbers with PNACs and prefixes. That way the number modification can be easily controlled.

58.7.8.1 Incoming Calls

Trunk Group Configuration

Select OK to temporarily store changes. Make your changes permanent by selecting 'Apply Changes' on the General page.

General **Channels list** **Number Modification** **Spare Flags**

Incoming Calls

TON-IN	TON-OUT	Post Manipulation
Calling party number		
<input type="checkbox"/> Match prefixes for Unknown numbers	Normal Mode	
<input type="checkbox"/> TON via length check	Preferred TON to SIP: Same as TON-IN	Add PNAC and Prefix
	Survivable Mode	
	Preferred TON to SIP: Same as TON-IN	Add PNAC and Prefix
	<input type="checkbox"/> Use Local Toll Table	
Called party number		
<input type="checkbox"/> Match prefixes for Unknown numbers	Normal Mode	
<input type="checkbox"/> TON via length check	Preferred TON to SIP: Same as TON-IN	Add PNAC and Prefix
	Survivable Mode	
	Preferred TON to SIP: Same as TON-IN	Add PNAC and Prefix
Connected number		
<input type="checkbox"/> Copy configuration from OUTGOING calling party number		
<input checked="" type="checkbox"/> Match PNACs and/or prefixes	Preferred TON to PSTN: Same as TON-IN	None
<input type="checkbox"/> TON via length check		
Default TON from SIP: Unknown		

Note: "Use Local Toll Table" 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'.

When determining TON-IN, "TON via length check" is disabled unless "Match prefixes for Unknown numbers" is checked. Both flags can be checked at the same time.

Match Prefixes for Unknown Numbers (calling and called): 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 (calling and called): 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.

The following are the possible options on the drop-down list boxes:

Incoming calls from the PSTN during Normal Mode			
Calling Party Number		Called Party Number	
Preferred TON to SIP	Post Manipulation	Preferred TON to SIP	Post Manipulation
Same as TON-IN	None	Same as TON-IN	None
International	Add PNAC and Prefix	International	Add PNAC and Prefix
	GNF		GNF

Incoming calls from the PSTN during Survivable Mode			
Calling Party Number		Called Party Number	
Preferred TON to SIP	Post Manipulation	Preferred TON to SIP	Post Manipulation

Same as TON-IN International	None Add PNAC and Prefix	Same as TON-IN International National Subscriber	None Add PNAC and Prefix
---------------------------------	-----------------------------	---	-----------------------------

Preferred TON to SIP in Normal Mode:

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 in Survivable Mode:

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 in when in Normal mode:

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

Post-Manipulation Settings in when in Survivability mode:

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.

58.7.8.2 Outgoing Calls

Trunk Group Configuration

Select OK to temporarily store changes. Make your changes permanent by selecting 'Apply Changes' on the General page.

General **Channels list** **Number Modification** **Spare Flags**

Outgoing Calls

TON-IN	TON-OUT	Post Manipulation
Calling party number		
<input checked="" type="checkbox"/> Match PNACs and/or prefixes	Preferred TON to PSTN: Same as TON-IN	None
<input type="checkbox"/> TON via length check		
Default TON from SIP: Unknown		
Called party number		
<input checked="" type="checkbox"/> Match PNACs and/or prefixes	Preferred TON to PSTN: Same as TON-IN	None
<input type="checkbox"/> TON via length check	<input type="checkbox"/> Set TON-OUT to Unknown for E911 calls	
Default TON from SIP: Unknown		
Connected number		
<input checked="" type="checkbox"/> Copy configuration from INCOMING calling party number		
<input type="checkbox"/> Match prefixes for Unknown numbers	Normal Mode	
<input type="checkbox"/> TON via length check	Preferred TON to SIP: Same as TON-IN	Add PNAC and Prefix
	Survivable Mode	
	Preferred TON to SIP: Same as TON-IN	Add PNAC and Prefix

Match PNACs and Prefixes (calling and called): If set, the leading digits of the incoming calling or called party number are matched against (in this order) the International PNAC and Prefix, National PNAC and Prefix and Subscriber PNAC and Prefix. The combination of PNAC and prefix field must have a non-empty value to match.

TON via Length Check (calling and called): If the TON after the previous checks is still Unknown and if this check is 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.

The following are the possible options on the drop-down list boxes:

Outgoing Calls to the PSTN					
Calling Party Number			Called Party Number		
Default TON from SIP	Preferred TON to PSTN	Post Manipulation	Default TON from SIP	Preferred TON to PSTN	Post Manipulation
International	Same as TON-IN	None	International	Same as TON-IN	None
National	International	Unknown TON	National	International	Unknown TON
Subscriber	National	Add Prefix + Unknown TON	Subscriber	National	Add Prefix + Unknown TON
Unknown	Subscriber		Unknown	Subscriber	Add Prefix + Unknown TON
				Local Toll Table	

Preferred TON to PSTN:

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 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 code, then the area code is

stripped as well.

Local Toll Table: the output TON will be determined from the LTT lookup.

Post-Manipulation Settings:

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.

For outgoing numbers:

- IF “Match PNACs and Prefixes” is set THEN
 - Set “Default TON from SIP” to “Unknown” and disable it.
 - Enable “TON via length check” and reset the checkbox.
- ELSE
 - Set “Default TON from SIP” to “Unknown” and enable it.
 - Disable “TON via length check” and reset the checkbox.

58.7.8.3 OSB 50i/500i Gateway Number Modification Implementation

Below is the logic that is implemented for each of these settings:

Step 1a (Outgoing Calls): Determine the **TON-IN** of the From/PAI/P-Preferred-Identity/Diversion/Request-URI number received in the SIP INVITE message as follows:

- IF number starts with '+', TON-IN is **INT** (strip the '+').
- ELSE IF *Match PNACs and Prefixes* is not checked, set TON-IN according to GUI field "Default TON from SIP"
- ELSE IF *Match PNACs and Prefixes* is checked:
 - IF number starts with *International PNAC and Prefix*, TON-IN is **INT** (strip the PNAC and Prefix).
 - ELSE IF number starts with *National PNAC and Prefix*, TON-IN is **NAT** (strip the PNAC and Prefix).
 - ELSE IF number starts with *Subscriber PNAC and Prefix*, TON-IN is **SUBS** (strip the PNAC and Prefix).
 - IF *Country Code* is 1 and *National Number Length* is 10, TON-IN is **SUBSwAC**
 - ELSE TON-IN is **Unknown**
 - IF TON-IN is **Unknown** and *TON via Length Check* is checked and *National Number Length* and/or *Subscriber Number Length* are not empty:
 - IF *Number Length* matches the *National Number Length*, TON-IN is **NAT**
 - ELSE IF *Number Length* matches the *Subscriber Number Length*, TON-IN is **SUBS**
 - ELSE TON-IN remains **Unknown**

Step 1b (Incoming Calls): Determine the **TON-IN** of the Calling/Redirecting/Called Party number received in the ISDN SETUP message as follows:

- IF NPI is ISDN and ISDN TON is International, TON-IN is **INT**
- ELSE IF NPI is ISDN and ISDN TON is National, TON-IN is **NAT**
- ELSE IF NPI is ISDN and ISDN TON is Subscriber, TON-IN is **SUBS**
- ELSE IF *Match Prefixes for Unknown Numbers* is checked and the *International/National/Subscriber Prefixes* fields are not empty:
 - IF Number starts with *International Prefix*, TON-IN is **INT** (strip international prefix)
 - ELSE IF Number starts with *National Prefix*, TON-IN is **NAT** (strip national prefix)
 - ELSE IF Number starts with *Subscriber Prefix*, TON-IN is **SUBS** (strip subscriber prefix)
 - ELSE TON-IN is **SUBS** (do not strip anything)
 - IF *Country Code* is 1 and *Number Length* is 10, TON-IN is **SUBSwAC**
- ELSE IF *TON via Length Check* is checked and *National Number Length* and/or *Subscriber Number Length* are not empty:
 - IF *Number Length* matches the *National Number Length*, TON-IN is **NAT**
 - ELSE IF *Number Length* matches the *Subscriber Number Length*, TON-IN is **SUBS**
- ELSE TON-IN is **Unknown**

Step 2a: Determine the **TON-OUT** for the **Calling Party** based on the **Preferred TON** setting:

- IF the OSB is in Survivable Mode AND the "Local Toll Table" checkbox (see **Error! Reference source not found.**) is checked:
 - Look up the Called Party/Calling Party relationship in the Local Toll Tables (see section **Error! Reference source not found.**) and use the resulting output to create an X-Oscar header to insert into the INVITE message. Proceed with the next bullet in the sequence.
- IF Preferred TON is International:
 - IF TON-IN is INT, TON-OUT is INT (leave number unchanged)

- ELSE IF TON-IN is NAT, TON-OUT is INT (add country code)
- ELSE IF TON-IN is SUBSwAC, TON-OUT is INT (add country code)
- ELSE IF TON-IN is SUBS, TON-OUT is INT (add country code and area code)
- ELSE, TON-OUT is UNKNOWN
- ELSE IF Preferred TON is National (applies to outgoing calls only):
 - IF TON-IN is INT and number starts with country code, TON-OUT is NAT (remove country code)
 - ELSE IF TON-IN is INT and number does not start with country code, TON-OUT is INT (leave number unchanged)
 - ELSE IF TON-IN is NAT, TON-OUT is NAT (leave number unchanged)
 - ELSE IF TON-IN is SUBSwAC, TON-OUT is NAT (leave number unchanged)
 - ELSE IF TON-IN is SUBS, TON-OUT is NAT (add area code)
 - ELSE, TON-OUT is UNKNOWN
- ELSE IF Preferred TON is Subscriber (applies to outgoing calls only):
 - IF TON-IN is INT and number starts with country code and area code, TON-OUT is SUBS (remove country code and area code)
 - ELSE IF TON-IN is INT and number starts with country code, TON-OUT is NAT (remove country code)
 - ELSE IF TON-IN is INT and number does not start with country code, TON-OUT is INT (leave number unchanged)
 - ELSE IF TON-IN is NAT and number starts with area code, TON-OUT is SUBS (remove area code)
 - ELSE IF TON-IN is NAT and number does not start with area code, TON-OUT is NAT (leave number unchanged)
 - ELSE TON-OUT is TON-IN (leave number unchanged)
- ELSE IF Preferred TON is Same as TON-IN
 - TON-OUT is TON-IN (leave number unchanged)

Step 2b: Determine the **TON-OUT** for the **Called Party** based on the **Preferred TON** setting:

- IF Outgoing call and Preferred TON is Local Toll Table:
 - Look up the Called Party/Calling Party relationship in the Local Toll Tables (see section **Error! Reference source not found.**) and use the resulting output to set TON-OUT.
 - IF TON-OUT from LTT is National:
 - IF TON-IN is INT and number starts with country code, TON-OUT is NAT (remove country code)
 - ELSE IF TON-IN is INT and number does not start with country code, TON-OUT is INT (leave number unchanged)
 - ELSE IF TON-IN is NAT, TON-OUT is NAT (leave number unchanged)
 - ELSE IF TON-IN is SUBSwAC, TON-OUT is NAT (leave number unchanged)
 - ELSE IF TON-IN is SUBS, TON-OUT is NAT (add area code)
 - ELSE, TON-OUT is UNKNOWN
 - ELSE IF TON-OUT from LTT is Subscriber:
 - IF TON-IN is INT and number starts with country code and area code, TON-OUT is SUBS (remove country code and area code)
 - ELSE IF TON-IN is INT and number starts with country code, TON-OUT is NAT (remove country code)
 - ELSE IF TON-IN is INT and number does not start with country code, TON-OUT is INT (leave number unchanged)
 - ELSE IF TON-IN is NAT and number starts with area code, TON-OUT is SUBS (remove area code)

- ELSE IF TON-IN is NAT and number does not start with area code, TON-OUT is NAT (leave number unchanged)
 - ELSE TON-OUT is TON-IN (leave number unchanged)
- ELSE IF TON-OUT from LTT is SUBSwAC:
 - IF TON-IN is INT and number starts with country code, TON-OUT is SUBSwAC (remove country code)
 - ELSE IF TON-IN is INT and number does not start with country code, TON-OUT is INT (leave number unchanged)
 - ELSE IF TON-IN is NAT, TON-OUT is SUBSwAC (leave number unchanged)
 - ELSE IF TON-IN is SUBS, TON-OUT is SUBSwAC (add area code)
 - ELSE TON-OUT is TON-IN (leave number unchanged)
- ELSE IF TON-OUT from LTT is Unknown
 - TON-OUT is TON-IN (leave number unchanged)
- ELSE IF Preferred TON is International:
 - IF TON-IN is INT, TON-OUT is INT (leave number unchanged)
 - ELSE IF TON-IN is NAT, TON-OUT is INT (add country code)
 - ELSE IF TON-IN is SUBSwAC, TON-OUT is INT (add country code)
 - ELSE IF TON-IN is SUBS, TON-OUT is INT (add country code and area code)
 - ELSE, TON-OUT is UNKNOWN
- ELSE IF Preferred TON is National (does not apply to incoming Normal Mode calls):
 - IF TON-IN is INT and number starts with country code, TON-OUT is NAT (remove country code)
 - ELSE IF TON-IN is INT and number does not start with country code, TON-OUT is INT (leave number unchanged)
 - ELSE IF TON-IN is NAT, TON-OUT is NAT (leave number unchanged)
 - ELSE IF TON-IN is SUBSwAC, TON-OUT is NAT (leave number unchanged)
 - ELSE IF TON-IN is SUBS, TON-OUT is NAT (add area code)
 - ELSE, TON-OUT is UNKNOWN
- ELSE IF Preferred TON is Subscriber (does not apply to incoming Normal Mode calls):
 - IF TON-IN is INT and number starts with country code and area code, TON-OUT is SUBS (remove country code and area code)
 - ELSE IF TON-IN is INT and number starts with country code, TON-OUT is NAT (remove country code)
 - ELSE IF TON-IN is INT and number does not start with country code, TON-OUT is INT (leave number unchanged)
 - ELSE IF TON-IN is NAT and number starts with area code, TON-OUT is SUBS (remove area code)
 - ELSE IF TON-IN is NAT and number does not start with area code, TON-OUT is NAT (leave number unchanged)
 - ELSE TON-OUT is TON-IN (leave number unchanged)
- ELSE IF Preferred TON is Same as TON-IN
 - TON-OUT is TON-IN (leave number unchanged)

Step 3: Determine the **Post Manipulation** based on the TON-OUT from 2a or 2b:

- IF there is an LTT Header and Post Manipulation is set to **Add PNAC and Prefix**
 - IF LTT lookup result is INT, add International PNAC and Prefix to the X-Oscar-LTT-Calling-DN Header
 - ELSE IF LTT lookup result is NAT, add National PNAC and Prefix to the X-Oscar-LTT-Calling-DN Header
 - ELSE IF LTT lookup result is SUBSwAC, add Subscriber PNAC and Prefix to the X-Oscar-LTT-Calling-DN Header
 - ELSE IF LTT lookup result is SUBS, add Subscriber PNAC and Prefix to the X-Oscar-LTT-Calling-DN Header

- ELSE nothing to be done
- IF Post Manipulation is set to **None**
 - IF TON-OUT is SUBSwAC, TON-OUT is NAT (leave number unchanged)
 - ELSE nothing to be done (leave number unchanged)
- ELSE IF Post Manipulation is set to **GNF** (does not apply to Survivable Mode)
 - IF TON-OUT is INT, TON-OUT is Unknown (add '+')
 - ELSE IF TON-OUT is SUBSwAC, TON-OUT is NAT (leave number unchanged)
 - ELSE nothing to be done anymore (leave number unchanged)
- ELSE IF Post Manipulation is set to **Add Prefix + Unknown TON**
 - IF TON-OUT is INT, TON-OUT is Unknown (add International Prefix)
 - ELSE IF TON-OUT is NAT, TON-OUT is Unknown (add National Prefix)
 - ELSE IF TON-OUT is SUBSwAC, TON-OUT is Unknown (add Subscriber Prefix)
 - ELSE IF TON-OUT is SUBS, TON-OUT is Unknown (add Subscriber Prefix)
 - ELSE (leave number unchanged)
- ELSE IF Post Manipulation is set to **Add PNAC and Prefix**
 - IF TON-OUT is INT, TON-OUT is Unknown (add International PNAC and Prefix)
 - ELSE IF TON-OUT is NAT, TON-OUT is Unknown (add National PNAC and Prefix)
 - ELSE IF TON-OUT is SUBSwAC, TON-OUT is Unknown (add Subscriber PNAC and Prefix)
 - ELSE IF TON-OUT is SUBS, TON-OUT is Unknown (add Subscriber PNAC and Prefix)
 - ELSE nothing to be done anymore
- ELSE IF Post Manipulation is set to **Unknown TON**
 - TON-OUT is Unknown (leave number unchanged)

56.5.7 Local Toll Table

The screenshot shows the 'Integrated Gateway' configuration page. It has sections for 'Gateway Configuration' (with Card 1 PRI and Card 2 FXS), 'QoS Monitoring' (with an 'Enable QoS monitoring' checkbox), and 'Local Toll Tables'. A note states: 'These fields are only applicable when the country is United States / North America or United States Circa 1950 / North America.' A 'Local Toll Tables' button is highlighted with a yellow box and an arrow pointing to the 'Local Toll Table Configuration' page below.

Local Toll Table Configuration

Local Toll Table Configuration

Local Toll Tables Imported to OSB

	Local Toll Table Name	Number	Modified
1	Boca-Toll-3	1 561 923	2012-06-18 11:34:55
2	Boca-Toll-32	1 561 923	2012-06-18 11:34:55

Upload a new Local Toll Table

Upload Local Toll Table from OSV

Local Toll Tables (LTT) will be used by the OSB to determine how to display an incoming PSTN calling party number, and, if the customer so selects, how to set the Type Of Number (TON) for an outgoing calling party number.

Local Toll Tables are created on the OSV and then imported into an OSB using mechanisms described further below. The OSB will have no mechanisms for creating or updating local Toll Tables.

Local Toll Tables will apply to the OSB 50i and OSB 500i integrated gateways only. They will not apply to SSPs or other types of external gateways.

Any number that is presented for LTT handling must be normalized to international format.

Local Toll Tables apply to the North American Numbering Plan (NANP) only.

Note that LTT manipulation applies to the **called party** of outgoing calls in both Normal Mode and Survivability Mode.

For incoming calls, the LTT will be used for the **calling party number**.

58.7.9.1 Creation of LTT

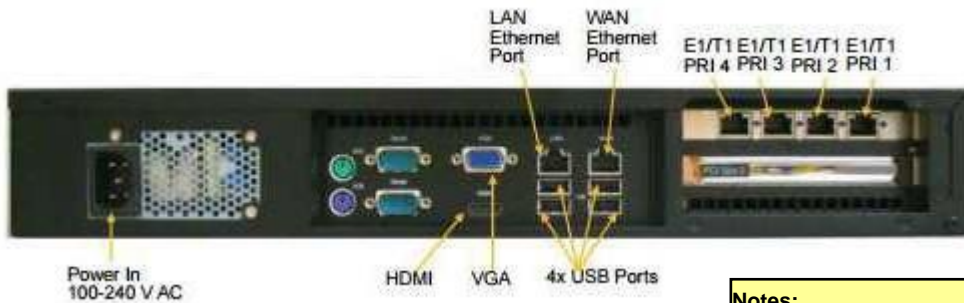
- The LTT that is populated on the OSV will be downloaded by the customer to a local server and then uploaded to the OSB. The creation of the OSV LTT file will be handled manually by the user.
- To create the file, the user must start the RTP CLI on the OSV and enter the following command:
- soapExport "-f=<output file name and path> -NumMod"
- The '*output file name and path*' will typically point to a location on the user's computer, or a network share location

57 OpenScape Branch 500i

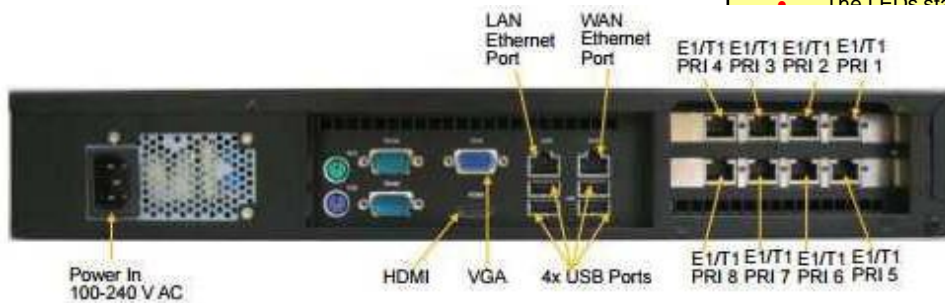
Note: "Do not Send Invite without SDP" attribute must NOT be selected on OSB500i/OSB500i Integrated Gateway End Point.

Configuration Options

1. OSB500i DP4



2. OSB500i DP8

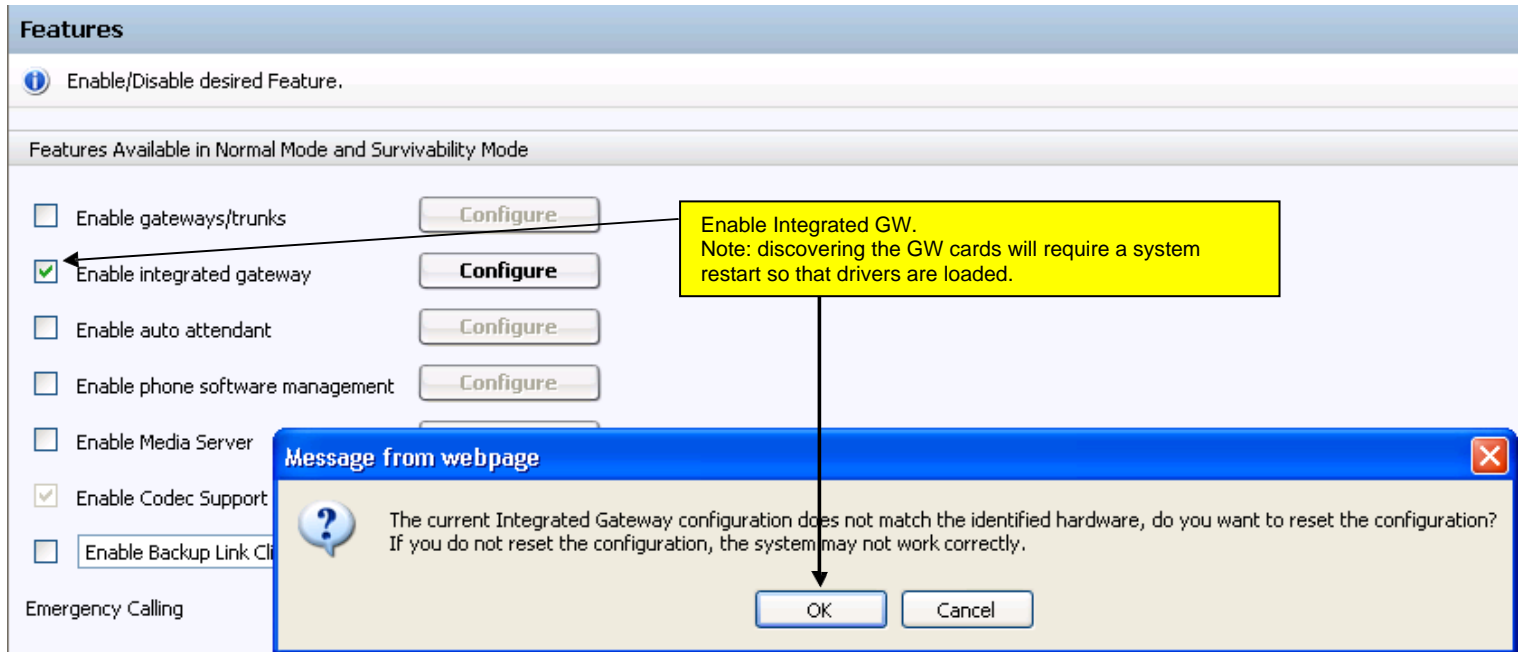


Notes:

- 500i can be configured as T1 or E1
- Cards or internal power cables must not be removed with the system powered on
- The LEDs status: (rear of box) - PRI cards will be red if the card is not detected.

57.2 Enable Integrated GW and Discover card configuration

Configuration -> OpenScape Branch -> Branch Office -> Configuration -> Features



Select Country Configuration for Integrated Gateway

Configuration -> OpenScape Branch -> Branch Office -> Configuration -> System -> Settings

System

Select OK to temporarily store changes. Make your changes permanent by selecting 'Apply Changes' on the General page.

Settings | **Licenses** | **Branding**

Country Configuration

Country: Brazil

Country configuration

Country Configuration

br configuration

```
#
# General
#
country                = Brazil (br)
DTMF Interdigit time   = 40 ms
DTMF high level         = -10 dbm
DTMF low level          = -12 dbm
MFR1 level              = -10 dbm
MFR2 level              = -8 dbm
Ring cadence            = 1000,4000 ms
```

Verified Integrated Gateway Cards loaded correctly

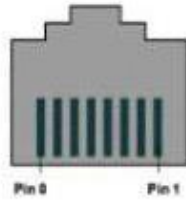
Configuration -> OpenScape Branch -> Branch Office -> Configuration -> Features -> Enable integrated gateway -> Configure

The screenshot displays the 'Integrated Gateway' configuration window. At the top, a blue header bar contains the title 'Integrated Gateway'. Below this, a status bar with an information icon and the text 'Integrated gateway provisioning.' is visible. The main section is titled 'Gateway Configuration'. A yellow callout box with the text 'PRI cards are discovered.' has two arrows pointing to the 'Card 1' and 'Card 2' dropdown menus, both of which are currently set to 'PRI/CAS'. To the left of these dropdowns is a checkbox labeled 'Per card clock source', which is currently unchecked. To the right of the dropdowns are two buttons: 'Configure...' and 'Trunk group...'.

57.3 PRI Configuration

E1/T1 PRI port - RJ45 Telco Port Connector - pin assignment

Pin	Description
1	Rx
2	Rx
3	Not Used
4	Tx
5	Tx
6	Not Used
7	Not Used
8	Not Used



Integrated Gateway

Integrated gateway provisioning.

Gateway Configuration

Card 1 PRI/CAS

☐ Per card clock source

Card 2 PRI/CAS

Configure PRI and Trunk Group

Configure...

Trunk group...

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.

PRI/CAS Configuration

PRI/CAS configuration provisioning.

Card Configuration

Method E1

Channel maintenance

Method: possible values "E1" or "T1".

Channel maintenance: redirects the user to the channel maintenance window.

Channel Maintenance

Channel maintenance

User can configure (restart/block/unblock channels) individual PRI links or B-channels

Combined Clock Source

Channel	Card 1				Card 2			
	Port 1 - NI2HKK BCAS disabled 1	Port 2 - CAST1HKK up 2	Port 3 - SESSMasterLoopBack BCAS disabled 3	Port 4 - disabled 4	Port 1 - QSIGHKK BCAS disabled 5	Port 2 - CorNetHKK BCAS disabled 6	Port 3 - SESSSlaveLoopBack BCAS disabled 7	Port 4 - 4ESSHKK BCAS disabled 8
	<input type="checkbox"/> All Channels	<input type="checkbox"/> All Channels	<input type="checkbox"/> All Channels	<input type="checkbox"/> All Channels	<input type="checkbox"/> All Channels	<input type="checkbox"/> All Channels	<input type="checkbox"/> All Channels	
	State	State	State	State	State	State	State	
	TX/RX Bits	TX/RX Bits	TX/RX Bits	TX/RX Bits	TX/RX Bits	TX/RX Bits	TX/RX Bits	
1	IDLE	IDLE	IDLE	OOS/NE	IDLE	IDLE	IDLE	
2	IDLE	IDLE	IDLE	OOS/NE	IDLE	IDLE	IDLE	
3	IDLE	IDLE	IDLE	OOS/NE	IDLE	IDLE	IDLE	
4	IDLE	IDLE	IDLE	OOS/NE	IDLE	IDLE	IDLE	
5	IDLE	IDLE	IDLE	OOS/NE	IDLE	IDLE	IDLE	
6	IDLE	IDLE	IDLE	OOS/NE	IDLE	IDLE	IDLE	
7	IDLE	IDLE	IDLE	OOS/NE	IDLE	IDLE	IDLE	
8	IDLE	IDLE	IDLE	OOS/NE	IDLE	IDLE	IDLE	
9	IDLE	IDLE	IDLE	OOS/NE	IDLE	IDLE	IDLE	
10	IDLE	IDLE	IDLE	OOS/NE	IDLE	IDLE	IDLE	
11	IDLE	IDLE	IDLE	OOS/NE	IDLE	IDLE	IDLE	
12	IDLE	IDLE	IDLE	OOS/NE	IDLE	IDLE	IDLE	
13	IDLE	IDLE	IDLE	OOS/NE	IDLE	IDLE	IDLE	
14	IDLE	IDLE	IDLE	OOS/NE	IDLE	IDLE	IDLE	
15	IDLE	IDLE	IDLE	OOS/NE	IDLE	IDLE	IDLE	
16	IDLE	IDLE	IDLE	OOS/NE	IDLE	IDLE	IDLE	
17	IDLE	IDLE	IDLE	OOS/NE	IDLE	IDLE	IDLE	
18	IDLE	IDLE	IDLE	OOS/NE	IDLE	IDLE	IDLE	
19	IDLE	IDLE	IDLE	OOS/NE	IDLE	IDLE	IDLE	
20	IDLE	IDLE	IDLE	OOS/NE	IDLE	IDLE	IDLE	
21	IDLE	IDLE	IDLE	OOS/NE	IDLE	IDLE	IDLE	
22	IDLE	IDLE	IDLE	OOS/NE	IDLE	IDLE	IDLE	
23	IDLE	IDLE	IDLE	OOS/NE	IDLE	IDLE	IDLE	
24	IN-SERVICE	IDLE	IN-SERVICE	OOS/NE	IN-SERVICE	IN-SERVICE	IN-SERVICE	

Restart selected channels Block selected channels Unblock selected channels

PRI/CAS Configuration

PRI/CAS configuration provisioning.

Fax T.38

- ☒ Fax T.38
- ☒ CNG detection

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. The activation of the flag "CNG detection" will only take effect if T.38 flag is also enabled.

Note: T.38 fax calls always start as a voice call and then switch to the T.38 codec.

PRI/CAS Configuration

PRI/CAS configuration provisioning.

Port Configuration

Combined Clock Source

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.

Row	Enable	Circuit ID	Card	Physical port	Framing	Clock source priority	Coding	Switch type	Line build out	Terminal mode	
1	<input checked="" type="checkbox"/>	NI2H4K	1	Port 1	ESF	1	B8ZS	NI 2	0	<input checked="" type="checkbox"/>	
2	<input checked="" type="checkbox"/>	CAST1H4K	1	Port 2	D4	2	AMI	T1 CAS	0	<input checked="" type="checkbox"/>	
3	<input checked="" type="checkbox"/>	5ESSMasterLoopBack	1	Port 3	ESF	3	B8ZS	5ESS Custom	0	<input checked="" type="checkbox"/>	
4	<input type="checkbox"/>		1	Port 4	ESF	4	AMI	T1 CAS	0	<input type="checkbox"/>	
5	<input checked="" type="checkbox"/>	QSIGH4K	2	Port 1	ESF	5	B8ZS	QSIG	0	<input checked="" type="checkbox"/>	
6	<input checked="" type="checkbox"/>	CorNetH4K	2	Port 2	ESF	6	B8ZS	CorNet-NQ	0	<input checked="" type="checkbox"/>	
7	<input checked="" type="checkbox"/>	5ESSSlaveLoopBack	2	Port 3	ESF	7	B8ZS	5ESS Custom	0	<input type="checkbox"/>	
8	<input checked="" type="checkbox"/>	4ESSH4K	2	Port 4	ESF	8	B8ZS	4ESS	0	<input checked="" type="checkbox"/>	

Edit

Enable: enable or disable the port.
Circuit ID: Circuit ID configuration
Card: Card number
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.
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

PRI/CAS Interface

PRI/CAS interface provisioning.

General

Physical port: Card 1 - Port 1

Signaling method: ISDN

Line build out: 0

Coding: HDB3

Switch type: EuroISDN

☒ CRC

☐ BCAS

BCAS service message after restart: None

Receive gain (dB): 0

Transmit gain (dB): 0

Default destination:

Clock source priority: 1

☐ Exclusive channel

☒ Echo cancellation

Echo tail(ms): 128

Physical port: PRI card/port number (Read Only)

Signaling method (E1): ISDN or CAS-MFCR2 or CAS Ring Down (only available for 50i DP24).

Framing (T1): line formatting options ESF (Extended Super Frame) or D4 (Superframe). The type of framing used is determined by your Telco.

Line build out: 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).

Note: LBO is only supported for OSB Configured as T1.

Coding: Line encoding method options AMI (Alternate Mark Inversion) or B8ZS (Bipolar 8 with Zero Substitution) for T1 and HDB3 (High Density Bipolar 3) for E1. The line coding used is determined by your Telco.

Switch type: sets protocol by a combo box.

E1-> EuroISDN, QSIG and CorNet-NQ.

QSIG/CorNet-NQ only for 50i DP24.

T1-> NI2, 4ESS, 5ESS Custom, T1CAS, QSIG and CorNet-NQ.

4ESS/5ESS/T1CAS/QSIG/CorNet-NQ only for 50i DP24

CRC: enable/disable CRC4 checking (only E1).

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.

BCAS service message after restart: selects behavior upon receiving isdn RESTART/RESTART ACKNOWLEDGE messages when BCAS is enabled

Receive gain: sets the Gain of payload for receive. A negative value decreases the gain, and a positive value increases the gain (mandatory).

Transmit gain: sets the Gain of payload for transmit. A negative value decreases the gain, and a positive value increases the gain (mandatory).

Default destination: 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: 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.

Echo cancellation: enables the echo cancellation parameter. **Note:** Echo cancellation may affect DTMF detection.

Echo tail: echo tail for Hardware Echo Cancellation. The values available are: 16, 32, 64 and 128 (msec).

PRI/CAS Interface

PRI/CAS interface provisioning.

Timers

T302 timer: 15

T305 timer: 30

T308 timer: 4

T309 timer: 90

T313 timer: 4

T302: timer to wait for digits for overlap dialing.

T305: timer to wait for DISCONNECT ACK once DISCONNECT is sent out, if this timer expires RELEASE is sent and T308 is started.

T308: timer to wait for RELEASE COMPLETE once RELEASE is sent out, if this timer expires RELEASE is retransmitted and T308 is restarted. If this timer expires twice the B-channel is placed in maintenance condition and call reference is released.

T309: maintain active calls on layer 2 disconnection, calls are cleared if connection is not established before T309 timer expires.

T313: 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).

PRI/CAS Interface

PRI/CAS interface provisioning.

Advanced

<input checked="" type="checkbox"/> Sending complete	<input type="checkbox"/> Far end disconnect with inband announcement
<input type="checkbox"/> Calling name delay	<input type="checkbox"/> Second screening indicator
<input type="checkbox"/> Send calling party name	<input type="checkbox"/> Data calls allowed
Calling party name: Facility IE	Setup progress indicator: none
<input type="checkbox"/> Send redirecting number	183 Session progress without SDP: Alerting
Redirecting number: Facility IE	<input checked="" type="checkbox"/> Always send PI8 in ALERT
Channel mapping: Physical	<input type="checkbox"/> QSIG ringback
<input checked="" type="checkbox"/> Restart link at start-up	<input type="checkbox"/> Start early media on CALL PROCEEDING
L3 trunk restart type: Restart Interface	<input type="checkbox"/> Disable far end restart
<input type="checkbox"/> B-channel parallel restarts	Idle reset interval:
<input type="checkbox"/> Group restarted b-channels in channel identification IE	<input type="checkbox"/> Busy Detect Disconnect
<input checked="" type="checkbox"/> Ignore Dial Tone On Setup Without CPN	<input type="checkbox"/> Do not send ISDN Status Message

Sending complete: add Sending Complete information element in SETUP messages (T1 Only)

Calling name delay: Calling Name will be provided in a separate ISDN message. In this case, the SIP INVITE message will postponed until the Facility with Calling Name is received or after a fixed 2 seconds timer expires.

Send calling party name: enable/Disable the sending of the Calling Name information in outgoing calls

Calling party name: Indicates in which Information Element the Calling Party Name information should be delivery: Facility IE or Display IE.

Send redirect number: Enable/Disable the sending of the Redirecting Number in outgoing calls

Redirecting number: Indicates in which Information Element the Redirecting Number information should be delivery in outgoing calls: Facility IE or Redirecting number IE.

Channel mapping: possible values: Logical/Physical

Physical: channels from 1-15 17-31, channel 16 is not used.

Logical: channels from 1-30, channel 16 is used as "pseudo" b-channel. This is default for Qsig/Cornet switch types.

Restart link at start-up: if enabled send PRI restart message after link start-up.

L3 trunk restart type: Restart Channel (a RESTART message is sent for each channel) or Interface can be configured.

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

Group restarted b-channels in channel identification IE: ability to daisy-chain channels within the Channel Identification Information Element (CIIE). The multi-channel CIIE will be used in the RESTART and RESTART ACKNOWLEDGE messages.

Ignore Dial Tone On Setup Without CPN: incoming SETUP is received without Called Party Number and without Sending Complete the OSB will play dial tone on the line if this flag is clear. If this flag is set the OSB won't play dial tone in this scenario.

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).

Second screening indicator: second screening indicator will be used in incoming setup message (E1 Only).

Data calls allowed: Incoming call with digital information bearer capability is allowed or not.

Setup progress indicator: Configures the Progress Indicator in SETUP message (New Zealand). The following options are supported: Call is not end-to-end, Destination address is non ISDN, Origination address is non ISDN and None

183 Session progress without SDP: OSV 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, Alerting, Progress and Alerting and None.

Always send PI8 in ALERT: if flag is enabled, OSB 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.

QSIG ringback: Do not play ringback for QSIG/CORNET if flag is disabled.

Start early media on CALL PROCEEDING: command will cause the OSB to raise a SIP 183 Session Progress message with an SDP Answer as soon as it receives the ISDN CALL PROCEEDING message.

Disable far end restart: 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.

Idle reset interval:

Busy Detect Disconnect: If enabled the call is disconnected upon busy tone detection.

Do not send ISDN Status Message: If this flag is set OSB will never send ISDN Status Message out.

PRI/CAS Interface

PRI/CAS interface provisioning.

Channels

☒ All channels

Enable	Number	CAS Initial State
<input checked="" type="checkbox"/>	1	idle
<input checked="" type="checkbox"/>	2	idle
<input checked="" type="checkbox"/>	3	idle
<input checked="" type="checkbox"/>	4	idle
<input checked="" type="checkbox"/>	5	idle
<input checked="" type="checkbox"/>	6	idle
<input checked="" type="checkbox"/>	7	idle
<input checked="" type="checkbox"/>	8	idle
<input checked="" type="checkbox"/>	9	idle

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.

Channels

☒ All channels

Enable	Number	Trunk group	CAS profiles	Own number	Ring-down destination	Comments
<input checked="" type="checkbox"/>	1	OGPort2	ARD - ARD E1 Default Profile	15619232555	23451222	
<input checked="" type="checkbox"/>	2	OGPort2	MRD - MRD	15619232556	23451223	
<input checked="" type="checkbox"/>	3	OGPort2	Hoot n Holler - HootHoller	15619232557	23451224	

PRI/CAS Interface -> Channels

List is showed when PRI Interface is configured with Signaling method as CAS Ring Down.

PRI/CAS Configuration

PRI/CAS configuration provisioning.

CAS Advanced Settings

These fields are only applicable when the signaling method of a PRI/CAS port is CAS.

☒ Enable E1 CAS MFC-R2 advanced settings

E1 CAS MFC-R2 advanced settings

E1 CAS MFC-R2 profile

E1 CAS Ring Down profile

Ring down channels

☐ Enable Session Refresh Timeout

Ring-down audit interval (sec)

0

☐ Enable Ring-Down Call Refresh to Integrated Gateway

☐ Enable Notify on Switchover to MLC

CAS E1 Advanced Settings

Enable E1 CAS MFC-R2 advanced settings: Enabling/Disabling CAS Table Configuration Timers. To configure the timer values click the "CAS Advanced Settings" button. Only recommended for advanced users

Enable Session Refresh Timeout: When this flag is set, the call will be disconnected if the session's time expires

Ring-down audit interval (sec): Interval in seconds in which audit mechanism will be executed, checking transmitting and receiving RBS bits and unexpected states. It can assume values from 10s to 3600s, or 0 to disable it. The default is 0.

Enable Ring-Down Call Refresh to Integrated Gateway: If flag is enabled, when an ARD, MRD or Hoot-n-Holler channel is involved in a call and it receives an INVITE with the X-Siemens-Application-Data and with a new call id from the same originator DN as from the current ongoing call, it shall disconnect the old call and establish a new call from the received INVITE. This action shall be taken both in normal and in survivable mode.

Enable Notify on Switchover to MLC: enable / disable sending the NOTIFY message with the header Event: server-switchover to each MLC.

E1 CAS Advanced Settings

E1 CAS Advanced Settings provisioning.

Timeout for backward request to resume cycle	150
Call forward safety	30000
Wait for seize acknowledge	8000
Wait for answer	65000
Double answer	400
Answer delay	150
Persistence check	500
DTMF start dialing	500
MF threshold time	0
spare timer1	
spare timer2	
spare timer3	
spare timer4	
spare timer5	

E1 CAS MFC-R2 advanced settings

NOTE: 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.

Call forward safety: Forward Safety Timer.

Wait for seize acknowledge: How much time it is waited for a response to our SEIZE signal.

Wait for answer: How much time it is waited when the call has been accepted.

Double answer: When double answer is in effect, it is the interval between the ANSWER, CLEARBACK and ANSWER again.

Answer delay: Short delay before answering to give the other end an additional time to detect the tone off condition

Persistence check: How much time it is waited for CAS signaling before handling the new signal.

DTMF start dialing: DTMF Start Dialing Timer

MF threshold time: Time that an MF tone should last before being handled.

E1 CAS Profiles

E1 CAS Profiles provisioning.

Default E1 CAS Profiles

Default E1 CAS profiles Argentina Telefonica

Add profile

E1 CAS MFC-R2 profile

There are several pre-defined CAS profiles that can be used on a Branch. 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.

E1 CAS Profiles

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.

Row	Name	ANI before DNIS	Maximum amount of ANI	Maximum amount of DNIS	Maximum waiting time of MF back tone	Metering pulse timeout	Skip category	Immediate accept	Charge calls	Enable forced release
1	Automation	<input type="checkbox"/>	12	12			<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
2	Argentina Telecom	<input type="checkbox"/>							<input type="checkbox"/>	<input type="checkbox"/>
3	Brazil Embratel 2	<input type="checkbox"/>							<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
4	Mexico 1	<input type="checkbox"/>							<input checked="" type="checkbox"/>	<input type="checkbox"/>
5	Korea	<input type="checkbox"/>							<input checked="" type="checkbox"/>	<input type="checkbox"/>

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.

E1 CAS Profiles

E1 CAS Profiles provisioning.

E1 CAS Ring Down profile
 Table with a summary of E1 CAS Ring Down profiles. It is possible to Add/Edit/Delete a profile.

Add Edit Delete

Row	Name	Profile type
1	ARD E1 Default Profile	ARD - Automatic Ring Down
2	MRD	MRD - Manual Ring Down
3	ARD N to 1	ARD N to 1 - Automatic Ring Down
4	HootHoller	Hoot-n-Holler

ARD E1 Default Profile is a reserved profile that can not be deleted. The only editable fields are Idle/Onhook bits and Seized/Offhook bits. This profile will be automatically assigned to all channels in a trunk group which E1 CAS signaling is Ring Down and the field E1 CAS profile is empty.

E1 CAS Profile

E1 CAS Profile provisioning.

Profile
Profile name: Name of the profile.
Profile type: Type of the profile E1 CAS signaling

Profile name Profile type MRD - Manual Ring Down

Timer

Start time (ms) After start time (ms)

Wink time (ms) **Receiver wink time (ms)**

Advanced

Idle/Onhook bits 1001 Seized/Offhook bits 0001

Ring-down refresh info

Advanced
Idle/Onhook bits: Sets the RBS bits which will be defined to an idle state.
Seized/Offhook bits: Sets the RBS bits which will be defined to a seizure state.
Ring-down refresh: Defines the method of manual ring down receiving or sending a call refresh on the VoIP connection after a call is established. It can be "dtmf", which sends an RTP event 'A', or "info", which sends an INFO SIP message. (MRD only).

Timer
Start time: this timer is used to delay dial in Immediate Start and to delay the seizure in ARD
After start time: this timer determines a guard time after seizure in ARD.
Wink time: timer determines for how long the wink will be applied in an incoming call in E&M Wink and determines for how long the wink will be applied in an outgoing call in MRD
Receiver wink time: this timer determines the longest time the GW will wait for the wink to be removed by PSTN.

Ring Down Channels

Ring Down Channels management.

Ring down channels

Table with the summary of E1 CAS channels configured as Ring Down.

Search for in

Row	Enable	Channel	Trunk group	CAS signaling	CAS profile	Own number	Ring-down destination	Comments
1	<input checked="" type="checkbox"/>	Card 1 - Port 2 - Channel 1	OGPort2	ARD - Automatic Ring Down	ARD E1 Default Profile	15619232555	23451222	
2	<input checked="" type="checkbox"/>	Card 1 - Port 2 - Channel 2	OGPort2	MRD - Manual Ring Down	MRD	15619232556	23451223	
3	<input checked="" type="checkbox"/>	Card 1 - Port 2 - Channel 3	OGPort2	Hoot-n-Holler	HootHoller	15619232557	23451224	
4	<input checked="" type="checkbox"/>	Card 1 - Port 2 - Channel 4	OGPort2	ARD - Aut				
5	<input checked="" type="checkbox"/>	Card 1 - Port 2 - Channel 5	OGPort2	ARD - Aut				

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 signaling: The signaling 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)

PRI/CAS Configuration

CAS Advanced Settings

These fields are only applicable when the signaling method of a PRI/CAS port is CAS.

T1 CAS profile

☐ Enable Session Refresh Timeout

Ring-down audit interval (sec)

0

☐ Enable Ring-Down Call Refresh to Integrated Gateway

☐ Enable Notify on Switchover to MLC

Ring down channels

CAS T1/E1 Advanced Settings

Enable Session Refresh Timeout: When this flag is set, the call will be disconnected if the session's time expires

Ring-down audit interval (sec): Interval in seconds in which audit mechanism will be executed, checking transmitting and receiving RBS bits and unexpected states. It can assume values from 10s to 3600s, or 0 to disable it. The default is 0.

Enable Ring-Down Call Refresh to Integrated Gateway: If flag is enabled, when an ARD, MRD or Hoot-n-Holler channel is involved in a call and it receives an INVITE with the X-Siemens-Application-Data and with a new call id from the same originator DN as from the current ongoing call, it shall disconnect the old call and establish a new call from the received INVITE. This action shall be taken both in normal and in survivable mode.

Enable Notify on Switchover to MLC: enable / disable sending the NOTIFY message with the header Event: server-switchover to each MLC.

T1 CAS Profiles

T1 CAS Profiles provisioning.

T1 CAS Profiles

Table with the summary of T1 CAS profiles configuration. It is possible to Add/Edit/Delete a profile.

Add Edit Delete

Row	Name	Profile type
1	ARD Default Profile	ARD - Automatic Ring Down
2	MRD T1	MRD - Manual Ring Down
3	ARD N to 1 T1	ARD N to 1 - Automatic Ring Down
4	HootHoller T1	Hoot-n-Holler
5	EM Imm T1	E&M Immediate Start
6	EM Wink	E&M Wink Start

ARD Default Profile is a reserved profile that can not be deleted. The only editable fields are Idle/Onhook bits and Seized/Offhook bits. This profile will be automatically assigned to all channels in a trunk group which T1 CAS signaling is Ring Down and the field T1 CAS profile is empty.

T1 CAS Profile

T1 CAS Profile provisioning.

Profile

Profile name: Name of the profile.
Profile type: Type of the profile T1 CAS signaling.

Profile name Profile type

Timer

Pre-wink time (ms) Delayed dial/Start time (ms)
Wink time (ms) **Receiver wink time (ms)**
 Digit guard time (ms) Ring detection time (sec)
 Debounce time (ms) Interdigit time (sec)
 Wait disconnect time (sec) After start time (ms)

Advanced

Idle/Onhook bits Seized/Offhook bits
 Ring-down refresh

Advanced

Idle/Onhook bits: Sets the RBS bits which will be defined to an idle state.
Seized/Offhook bits: Sets the RBS bits which will be defined to a seizure state.
Ring-down refresh: Defines the method of manual ring down receiving or sending a call refresh on the VoIP connection after a call is established. It can be "dtmf", which sends an RTP event 'A', or "info", which sends an INFO SIP message. (MRD only).

Timer

Pre-wink time: after the offhook is detected from PSTN, the GW shall wait this time before sending the wink signal.
Delayed dial/Start time: this timer is used to delay dial in Immediate Start and to delay the seizure in ARD.
Wink time: timer determines for how long the wink will be applied in an incoming call in E&M Wink and determines for how long the wink will be applied in an outgoing call in MRD.
Receiver wink time: this timer determines the longest time the GW will wait for the wink to be removed by PSTN.
Digit guard time: this timer determines a delay on starting sending digits after the wink.
Ring detection time: this time will determine how long an incoming call will ring before being disconnected.
Debounce time: this time will prevent an offhook (as answer) to be changed to an onhook before being debounced by the peer party.
Interdigit time: this timer determines the timeout for dialing.
Wait disconnect time: this time will determine how long the iGW will wait for the peer side to disconnect after it has gone onhook.
After start time: this timer determines a guard time after seizure in ARD.

57.3.1 PRI - Trunk Group Configuration

Integrated Gateway

Integrated gateway provisioning.

Gateway Configuration

Card 1 PRI/CAS

☐ Per card clock source

Configure... Trunk group...

Card 2 PRI/CAS

500iDQ01 - Trunk Groups - Windows Internet Explorer

https://21.21.0.81/trunkGroups.html?trunkId=0&country=us&node=proxy

Trunk Groups

Trunk Groups provisioning.

Add Trunk Group.
After created, it is possible to Edit/Delete existing Trunk Groups.

Add Edit Delete

Row	Type	FQDN	Trunk group name	Trunk selection	Hunt type
1	PRI/CAS	500i01a.unow.ni2.cwb	Card1Port1	TopToBottom	Circular
2	PRI/CAS	500i01h.unow.ni2.cwb	Card2Port4	TopToBottom	Circular
3	PRI/CAS	500i01b.unow.ni2.cwb	Card1Port2	TopToBottom	Circular
4	PRI/CAS	500i01c.unow.ni2.cwb	Card1Port3	TopToBottom	Circular
5	PRI/CAS	500i01d.unow.ni2.cwb	Card1Port4	TopToBottom	Circular
6	PRI/CAS	500i01e.unow.ni2.cwb	Card2Port1	TopToBottom	Circular
7	PRI/CAS	500i01f.unow.ni2.cwb	Card2Port2	TopToBottom	Circular
8	PRI/CAS	500i01g.unow.ni2.cwb	Card2Port3	TopToBottom	Circular

Trunk Group Configuration

Select OK to temporarily store changes. Make your changes permanent by selecting 'Apply Changes' on the General page.

General Channels list Number Modification Spare Flags

Configuration

Type PRI/CAS

FQDN og.unow.cas.cwb

Trunk group name OGPort2

Trunk selection Top To Bottom

Direction Both

Voice bearer capability Speech

Hunt type Circular

Restart

Mark sRTP call

Configuration

Type: port type (read only data).

FQDN: required for Trunk Group and to be used later on in "Gateway/Trunk Configuration"/

Trunk group name: name of the Trunk Group

Restart trunk group channels: Restart the enabled channels from selected list.

Trunk selection: selecting from High or Low Trunk first is possible.

Hunt type: linear of circular selection

Direction: Specifies the direction of traffic flow supported on the trunk group.

Mark sRTP call-leg as secure: if a secure media isnegotiated 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

Trunk Group Configuration

Select OK to temporarily store changes. Make your changes permanent by selecting 'Apply Changes' on the General page.

General Channels list Number Modification Spare Flags

Incoming Calls

Max overlap digit length

☒ Specific overlap dialing patterns

Add

Delete

Row	Dialing pattern	Maximum digit length
1	0800%	10

☐ Connected line identification presentation incoming

Answer Supervision Timer - Incoming Call (sec) 360

Blacklist profile

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. If not configured then T302 timer would apply

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.

Connected line identification presentation incoming:

Answer Supervision Timer – Incoming Calls: Value between 120 and 3600. Default is 360. Note: Corresponding Answer Supervision Timers should be configured under 'Feature'-'>'Gateway/Trunk'.

Timers should be configured with a difference of at least 10 seconds between Gateway/Trunk and Integrated Gateway to avoid racing conditions caused by simultaneous disconnection.

Blacklist profile: Specifies the Blacklist profile that it will be checked during incoming calls.

Trunk Group Configuration

Select OK to temporarily store changes. Make your changes permanent by selecting 'Apply Changes' on the General page.

General Channels list Number Modification Spare Flags

Outgoing Calls

☐ Set Numbering Plan to ISDN

Pre dial delay for DTMF (sec)

2

☐ Send Redirect Number instead of calling number for redirected calls

☐ Calling Party Number Presentation Restricted

☐ Connected line identification presentation outgoing

Answer Supervision Timer - Outgoing Call (sec) 170

Outgoing Calls

Set numbering plan to ISDN: it is set to enable/disable. When the Number Type is Unknown, it will set the Numbering Plan to ISDN. Otherwise, it will set to Unknown (only PRI)

Send Redirect Number instead of calling number for redirected calls: If selected (enabled), a call that is redirected to the PSTN will have the last redirecting or transferring party's identity as the Calling Party Number information element. This attribute is primarily intended for use when connecting to a carrier that does not understand the Redirecting Party Number information element.

Calling Party Number Presentation Restricted: Set calling party number presentation restricted to all outgoing call.

Connected line identification presentation incoming:

Answer Supervision Timer – Outgoing Call: Value between 120 and 3600. Default is 170. Note: Corresponding Answer Supervision Timers should be configured under 'Feature'-'>'Gateway/Trunk'.

Trunk Group Configuration

Select OK to temporarily store changes. Make your changes permanent by selecting 'Apply Changes' on the General page.

General Channels list Number Modification

Collect Calls

These fields are only applicable when the country is Brazil.

Collect call control

server

☒ Permission for receiving collect calls by category

☒ Permission for receiving collect calls by double answer

Collect Calls

Collect call control: who will check the permission for collect calls:

Server -> will add X-Siemens-header:collect-call in NM for calls with the indication of collect call. In SM, these calls will be rejected if permission is denied.

Gateway -> Branch will check the permission in SM and NM, and reject calls with the indication of collect call, if permission is denied.

Permission for receiving collect calls by category: In case of CAS, it 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 if Collect Call Control is Gateway (NM/SM) or Server (SM). In case of ISDN, if this flag is not checked, incoming calls with Reverse Charge Indication will be rejected, if Collect Call Control is Gateway (NM/SM) or Server (SM).

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. Only works for CAS and Brazil.

Trunk Group Configuration

Select OK to temporarily store changes. Make your changes permanent by selecting 'Apply Changes' on the General page.

General Channels list Number Modification Spare Flags

E1 CAS - Ring Down

E1 CAS signaling Ring Down

E1 CAS profile ARD - Default Profile

Number	Cas Profile	Own number	Ring-down destination	Comments
Card 1 - Port 2 - Channel 1	ARD - ARD E1 Default Profile	15619232555	23451222	
Card 1 - Port 2 - Channel 2	MRD - MRD	15619232556	23451223	
Card 1 - Port 2 - Channel 3	Hoot - HootHoller	15619232557	23451224	
Card 1 - Port 2 - Channel 4	ARD - ARD E1 Default Profile			
Card 1 - Port 2 - Channel 5	ARD - ARD E1 Default Profile			

E1 CAS – Ring Down

Number: Shows Card, Port, and Channel Number

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)

Trunk Group Configuration

Select OK to temporarily store changes. Make your changes permanent by selecting 'Apply Changes' on the General page.

General Channels list Number Modification Spare Flags

E1 CAS - MFC R2

These fields are only applicable when the framing of a port is E1 CAS.

E1 CAS profile Automation

☐ Do Not Accept Call on Offer

☒ CAS Answer for Early Media

☐ Send End of ANI with Presentation Allowed

☐ CAS Send Early Media

E1 CAS – MFC R2

E1 CAS profile: Select any of the created CAS profiles in CAS profiles table. CAS profile association is **mandatory** for CAS E1 trunk groups.

Do Not Accept Call on Offer: If set, the gateway waits for subscriber state (free, busy, unallocated) before sending backward tone from Group B. If not set, the gateway always sends free subscriber backward tone immediately after receiving a CAS call. The default is disabled.

CAS Answer for Early Media: If set allows answer in CAS calls to play announcements. Otherwise, send the appropriate backward tone.

Send End of ANI with Presentation Allowed: If set sends end of identification with presentation allowed. Otherwise, sends end of identification with presentation restricted. (Only Argentina)

CAS Send Early Media: If set sends 183 Session Progress to the SIP side when making outgoing calls in E1 CAS. Otherwise, sends 180 Ringing.

Trunk Group Configuration

Select OK to temporarily store changes. Make your changes permanent by selecting 'Apply Changes' on the General page.

General Channels list Number Modification Spare Flags

T1 CAS

These fields are only applicable when the Switch type of a port is T1 CAS.

T1 CAS signaling E&M Immediate Start T1 CAS addressing signaling DTMF

T1 CAS profile EM Imm T1 - E&M Immediat

T1 CAS

T1 CAS signaling: The signaling of the selected channels. It defines the protocol the Gateway is configured with the CO.

T1 CAS addressing signaling: The addressing type of digits to be sent in the signaling. It can be DTMF or MF.

T1 CAS profile: Select a profile from the available profile list. The profiles must be created before in PRI Configuration. If T1 CAS signaling is Ring Down, ARD Default Profile will be automatically assigned to those channels that have never had the T1 CAS profile assigned before, this value can be changed afterwards.

Trunk Group Configuration

Select OK to temporarily store changes. Make your changes permanent by selecting 'Apply Changes' on the General page.

General Channels list Number Modification Spare Flags

T1 CAS

These fields are only applicable when the Switch type of a port is T1 CAS.

T1 CAS signaling Ring Down T1 CAS addressing signaling None

T1 CAS profile ARD Default Profile - ARD -

T1 CAS – Ring Down

Number	Cas Profile	Own number	Ring-down destination	Comments
Card 1 - Port 1 - Channel 1	ARD - ARD Default Profile	551138172001	12341001	
Card 1 - Port 1 - Channel 2	MRD - MRD T1	551138172002	12341002	
Card 1 - Port 1 - Channel 3	Hoot - HootHoller T1	551138172003	12341003	
Card 1 - Port 1 - Channel 4	ARD - ARD Default Profile			
Card 1 - Port 1 - Channel 5	ARD - ARD Default			

Trunk Group Configuration

Select OK to temporarily store changes. Make your changes permanent by selecting 'Apply Changes' on the General page.

General **Channels list** **Network specific facilities**

Configuration

Channels list

Filter

Card Card 1 - Port 1
Card Card 1 - Port 2
Card Card 1 - Port 3
Card Card 1 - Port 4
Card Card 2 - Port 1
Card Card 2 - Port 2
Card Card 2 - Port 3
Card Card 2 - Port 4
Card 1 - Port 4 - channel 9
Card 1 - Port 4 - channel 10
Card 1 - Port 4 - channel 11
Card 1 - Port 4 - channel 12
Card 1 - Port 4 - channel 13
Card 1 - Port 4 - channel 14

>>
<<

Selected Channel

Card 1 - Port 1 - channel 6
Card 1 - Port 1 - channel 7
Card 1 - Port 1 - channel 8
Card 1 - Port 1 - channel 9
Card 1 - Port 1 - channel 10
Card 1 - Port 1 - channel 11
Card 1 - Port 1 - channel 12
Card 1 - Port 1 - channel 13
Card 1 - Port 1 - channel 14

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.

The left-hand list shows the list of PRI 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.

Trunk Group Configuration

Select OK to temporarily store changes. Make your changes permanent by selecting 'Apply Changes' on the General page.

General **Channels list** **Network specific facilities** **Number Modification** **Spare Flags**

Configuration

☒ Send NSF

Network ID

Facility coding value

Service parameters

☐ Ignore incoming NSF

NSF is only available for T1.
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

Send NSF: enabling/disabling sending the NSF.
Network ID: Four-digit code that indicates the carrier network which the service/feature will be requested. If empty, it indicates the local service provider.
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.
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

57.4 500i - General Settings

57.4.1 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.

Enabling/Disabling Redundancy

It is recommended to change the default redundancy password on each node separately before enabling the Redundancy; otherwise the system will fail to replicate the configuration to the other node. Both nodes must use the same redundancy password. Data synchronization will also fail if different software versions run in the system. After configuring the redundant system, the passwords are included in the data synchronization. When changing the redundancy password in the master node, the previous password is used in the backup node until data synchronization. After the synchronization, the redundancy password is updated.

To enable Redundancy, it is necessary to configure the IP address of Nodes 1 and 2 and configure the redundant virtual IP address. This operation requires a system restart. After the restart, 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.

Time synchronization: with redundancy enabled, it is mandatory that both nodes (master and slave) should have a time/date synchronized (both boxes must have the same time).

Network/Net Services
Select OK to temporarily store changes. Make your changes permanent by selecting 'Apply Changes' on the General page.

Settings | DNS | NTP | DHCP | Traffic Shaping | QoS

Redundancy

☒ Enable redundancy ☒ Enable PRI/CAS redundancy Failed links threshold ☒ Switchover without Link Check

☒ Test Default Gateway instead of subscribers during failover

Interface	IP address	Backup IP address	Virtual IP Address
LAN	21.21.25.10	21.21.25.11	21.21.25.15

Backup IP address: LAN IP address of the other Branch box, which is sharing the virtual IP.
Virtual IP Address: virtual IP address shared by the Branch boxes.

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 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: 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.
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.

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.

System Status – Redundancy State

When Redundancy is enabled, this state shows the status of the redundant system.

System Status			
Branch mode:	Proxy ACD	Auto refresh timer	30 sec
Operational state:	normal	Redundancy state:	Master

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

System Status			
Branch mode:	Proxy ACD	Auto refresh timer	30 sec
Operational state:	--	Redundancy state:	Backup

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.

System Status			
Branch mode:	Proxy ACD	Auto refresh timer	30 sec
Operational state:	normal	Master IP Address	21.21.25.10

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.



IMPORTANT: It is not possible to use both, the new 500i Refresh (SYS-2USM13-6M01E) together with old one 500i (SYS-2USM03-6M01E), in the 500i redundancy systems.

57.4.2 Gateway/Trunk Configuration

Remote URL: should contain FQDN configured for trunk group.
Port: 5096 must be used for Integrated GW.
Transport: UDP must be used.
GW Type: Integrated Gateway must be selected.
Trunk profile: Gateway must be used.

Gateways/Trunks												
Gateways/Trunks provisioning.												
Row	Signaling address type	Remote URL	Port	Interface	Transport	Routing prefix	Gateway/Trunk type	Functional type	Trunk profile	Output digit strip	Output digit add	Priority
1	IP address or FQDN	og.unow.net5.cwb	5096	LAN	UDP	0290%	Integrated Gateway	All Modes Egress/Ingress	Gateway	4		1
2	IP address or FQDN	og.unow.cas.cwb	5096	LAN	UDP	0291%	Integrated Gateway	All Modes Egress/Ingress	Gateway	4		1

SIPQ V2

500 supports QSIG and Cornet-NQ.

In normal mode QSIG and Cornet-NQ messages are tunneled to OSV through SIPQ V2.

In survivable mode QSIG and Cornet-NQ will be translated to regular SIP with a limitation on feature support.

The support of QSIG by OSB is required to allow subscribers on an OSV to interwork with subscribers on networked HiPath3000/4000 and 3rd party PBXs.

SIPQ V2 is required in order to support SRTP over connections established via SIPQ. SIPQv1 will not be supported by OSB.

Blacklist

Trunk Groups	
Trunk Groups provisioning.	
Blacklist Profile	
<div>Blacklist Profile</div>	

Possible to blacklist incoming calls based on Calling Party Number.
 Feature applies only for integrated gateway trunks on both NM and SM.
 Disconnection cause code will be Normal Call Clearing.
 No CDR will be created.

Blacklist Profiles ?

Blacklist profiles provisioning.

Row	Name
1	List01
2	List02

Max of 20 profiles can be created

Add Edit Delete

Blacklist Profile Configuration ?

General ?

Name List01

Blocked Calls ?

Row	Denied number
1	4989%
2	4567890
3	%5000

Max of 20 entries in each profile.
Max of 24 digits in each entry.
Denied numbers can be defined with special character %:
i.e, %5000 (suffix) ou 4989% (prefix)

Add Delete

Trunk Group Configuration

Select OK to temporarily store changes. Make your changes permanent by selecting 'Apply Changes' on the General page.

General

Channels list

Number Modification

Spare Flags

Incoming Calls

Max overlap digit length

☒ Specific overlap dialing patterns

Add

Delete

Row	Dialing pattern	Maximum digit length
1	0800%	10

☒ Connected line identification presentation incoming

Answer Supervision Timer - Incoming Call (sec)

Blacklist profile



Each trunk group can have one profile associated.

Integrated Gateway

Integrated gateway provisioning.

Gateway Configuration

Card 1	<input type="text" value="PRI/CAS"/>	<input type="button" value="Configuration"/>	<input type="button" value="Trunk group"/>
Card 2	<input type="text" value="FXS"/>	<input type="button" value="Configuration"/>	<input type="button" value="Trunk group"/>

QoS Monitoring

☒ Enable 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.

QoS Monitoring

QoS monitoring provisioning.

Configuration

☒ Send traps

Reporting mechanism	<input type="text" value="Threshold crossing"/>
QCU IP address	<input type="text" value="10.234.1.10"/>
QCU port	<input type="text" value="12010"/>
Maximum jitter threshold	<input type="text" value="20"/>
Average round trip delay threshold	<input type="text" value="100"/>
Lost packets threshold compressing	<input type="text" value="10"/>
Lost packets threshold not compressing	<input type="text" value="10"/>

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.

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.

VOIP

Select OK to temporarily store changes. Make your changes permanent by selecting 'Apply Changes' on the General page.

Sip Server Settings **Port and Signaling Settings** **Manipulation and Routing** **Error Codes** **Media**

Media Profiles

Select Profile "igw_lan" and press Edit

Add Edit Delete

Profile name	Codecs	Media protocol	Key exchange method	Mark sRTP Call-leg as Secure	Single m-line SRTP
default		Strict Pass-Thru	none		
igw_lan	G711A,G711U,G729	Best Effort SRTP	mikey	✓	
b2bua_profile	G711A,G711U	RTP only	none		

Media Profile

Select OK to temporarily store changes. Make your changes permanent by selecting 'Apply Changes' on the General page.

General

Name: igw_lan

Media protocol: Best Effort SRTP

SRTP configuration

SRTP crypto context negotiation: mikey

☒ Mark SRTP Call-leg as Secure

☐ Single m-line SRTP

Codec configuration

☒ Allow unconfigured codecs

☐ Enforce codec priority in profile

☐ Send Telephony Event in Invite without SDP

Packetization interval: auto

Codec: G722 8 kHz - 64 kbps Add

Media Protocol: Media security supported for calls to and from the Integrated GW.
Key Exchange Method: if Best Effort SRTP is selected then is possible to configure mikey (Multimedia Internet KEYing) or sdes (Security Descriptions).
Mark SRTP call-leg as Secure: if checked then the call will be marked as secure with the SIP X-Siemens Call-Type: ST-Secure header for all FXS ports when TLS/SRTP is used. Otherwise, the SIP X-Siemens-Call-Type: ST-Insecure header will be sent.

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.
 Note: Codecs can be selected/enable under Features->Enable Codec Support for transcoding->Configure->Select codecs.

Priority: 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.

Move up Move down Delete

Priority	Codec Name
1	G711A 8 kHz - 64 kbps
2	G711U 8 kHz - 64 kbps
3	G729 8 kHz - 8 kbps

57.5 CID Suppression

Features

Enable/Disable desired Feature.

Features Available in Survivability Mode Only

Multi-line Hunt Groups

Configure

Call Forwarding

Configure

☒ Enable Call Detail Records

Configure

☒ Enable Music On Hold for Gateways & Subscribers

☐ Use PAI/PPI as ISDN Calling Party Number

☒ System calling number suppression

access code *51

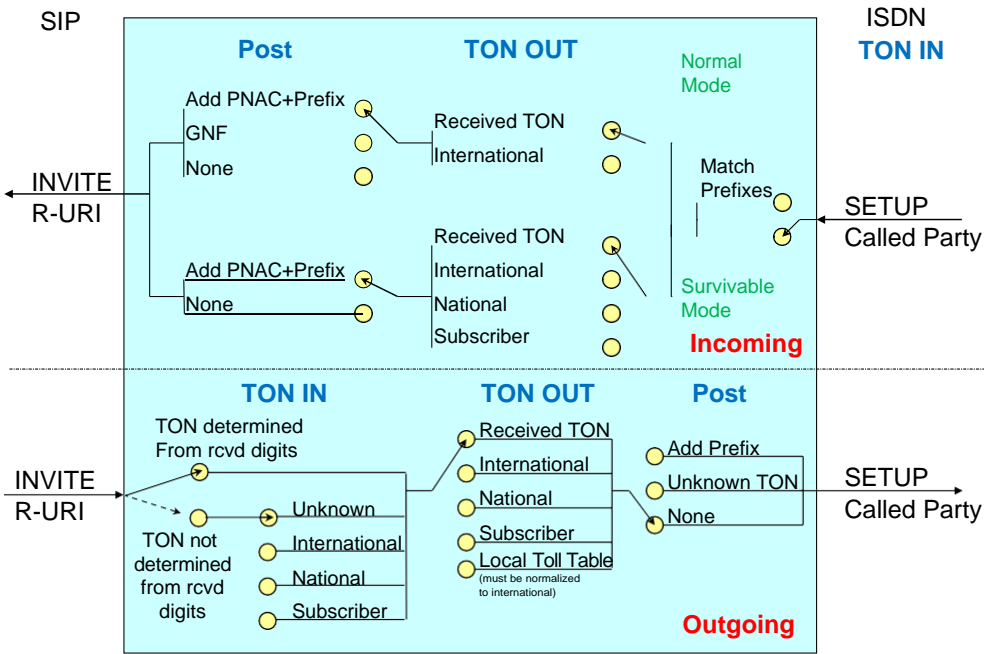
System calling number suppression – access code:

allows the Branch subscriber to use the Calling Line Identification Restriction (CLIR) feature in a per call basis. To avoid the presentation of the caller party number to the called party, the caller shall enter de configured access code in the beginning of dial, before the gateway routing prefix and the destination number.

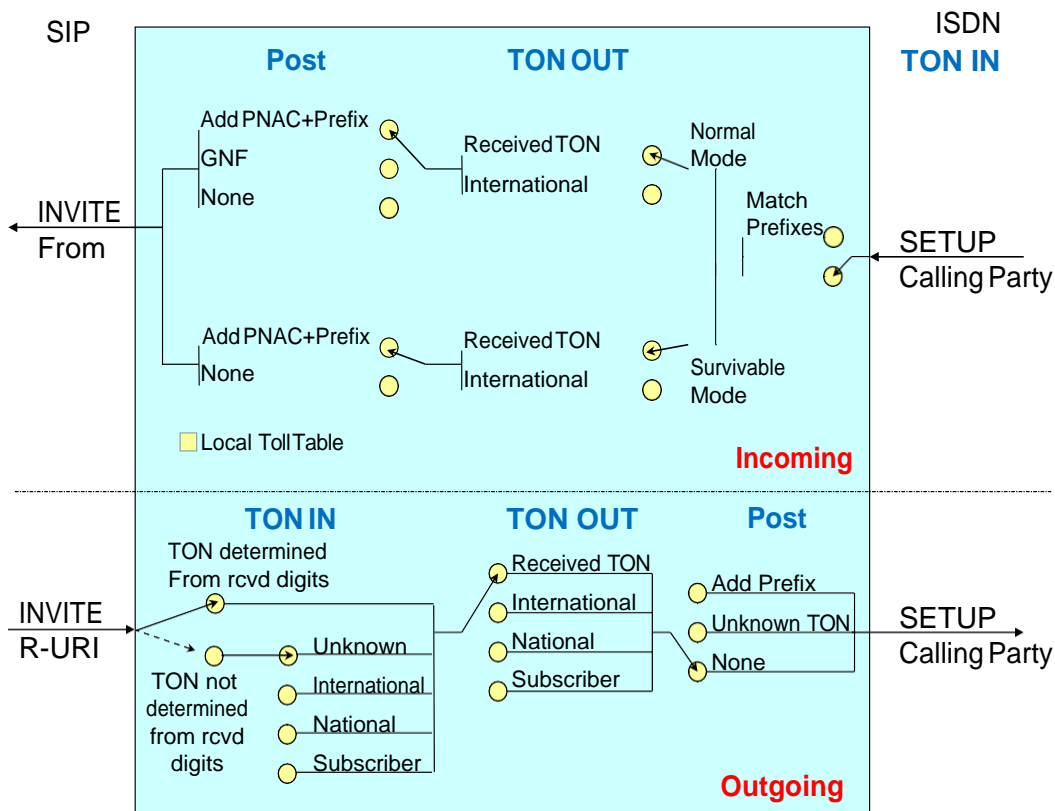
Note: Only applies in Survivable Mode.

57.6 Number Modification

The new Called Party Number/Request URI handling will be as shown below:



The new Calling Party Number handling will be as shown below:



Trunk Group Configuration

Select OK to temporarily store changes. Make your changes permanent by selecting 'Apply Changes' on the General page.

General **Channels list** **Number Modification** **Spare Flags**

Definitions

Country code Area code

National number length Subscriber number length

Prefixes

International PNAC International prefix

National PNAC National prefix

Subscriber PNAC Subscriber prefix

Definitions

Country code: configuration of the country code

Area code: configuration of the Local Area Code

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: configuration of the international Public Network Access Code (PNAC)

International prefix: configuration of the international prefix.

National PNAC: configuration of the national PNAC.

National prefix: configuration of the national prefix.

Subscriber PNAC: configuration of the subscriber PNAC.

Subscriber prefix: configuration of the subscriber prefix

Gateway Number Modification Default Settings

With the default settings:

- Incoming calling and called party numbers are sent as received to the proxy's Number Manipulation function, prefixed with PNACs and prefixes.
- Outgoing calling party numbers are sent to the PSTN as received from the proxy's Number Manipulation function without post-manipulation.
- Outgoing called party numbers are sent to the PSTN as received from the proxy's Gateway Routing function without post-manipulation.

Note that not having post-manipulation enabled means that if the OSB 50i/500i receives prefixed numbers from the OSB proxy, these numbers are mostly sent without the prefixes to the PSTN. In order to still send the prefixes, the post-manipulation must be set to 'Send Prefixes'.

The integrated gateway will perform best when it receives numbers with PNACs and prefixes. That way the number modification can be easily controlled.

57.6.1 Incoming Calls

Trunk Group Configuration

Select OK to temporarily store changes. Make your changes permanent by selecting 'Apply Changes' on the General page.

General **Channels list** **Number Modification** **Spare Flags**

Incoming Calls

TON-IN	TON-OUT	Post Manipulation
Calling party number		
<input type="checkbox"/> Match prefixes for Unknown numbers	Normal Mode	
<input type="checkbox"/> TON via length check	Preferred TON to SIP: Same as TON-IN	Add PNAC and Prefix
	Survivable Mode	
	Preferred TON to SIP: Same as TON-IN	Add PNAC and Prefix
	<input type="checkbox"/> Use Local Toll Table	
Called party number		
<input type="checkbox"/> Match prefixes for Unknown numbers	Normal Mode	
<input type="checkbox"/> TON via length check	Preferred TON to SIP: Same as TON-IN	Add PNAC and Prefix
	Survivable Mode	
	Preferred TON to SIP: Same as TON-IN	Add PNAC and Prefix
Connected number		
<input type="checkbox"/> Copy configuration from OUTGOING calling party number		
<input checked="" type="checkbox"/> Match PNACs and/or prefixes	Preferred TON to PSTN: Same as TON-IN	None
<input type="checkbox"/> TON via length check		
Default TON from SIP: Unknown		

Note: "Use Local Toll Table" 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'.

When determining TON-IN, "TON via length check" is disabled unless "Match prefixes for Unknown numbers" is checked. Both flags can be checked at the same time.

Match Prefixes for Unknown Numbers (calling and called): 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 (calling and called): 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.

The following are the possible options on the drop-down list boxes:

Incoming calls from the PSTN during Normal Mode			
Calling Party Number		Called Party Number	
Preferred TON to SIP	Post Manipulation	Preferred TON to SIP	Post Manipulation
Same as TON-IN	None	Same as TON-IN	None
International	Add PNAC and Prefix	International	Add PNAC and Prefix
	GNF		GNF

Incoming calls from the PSTN during Survivable Mode			
Calling Party Number		Called Party Number	
Preferred TON to SIP	Post Manipulation	Preferred TON to SIP	Post Manipulation

Same as TON-IN International	None Add PNAC and Prefix	Same as TON-IN International National Subscriber	None Add PNAC and Prefix
---------------------------------	-----------------------------	---	-----------------------------

Preferred TON to SIP in Normal Mode:

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 in Survivable Mode:

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 in when in Normal mode:

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

Post-Manipulation Settings in when in Survivability mode:

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.

57.6.2 Outgoing Calls

Trunk Group Configuration

Select OK to temporarily store changes. Make your changes permanent by selecting 'Apply Changes' on the General page.

General

Channels list

Number Modification

Spare Flags

Outgoing Calls

TON-IN	TON-OUT	Post Manipulation
Calling party number		
<input checked="" type="checkbox"/> Match PNACs and/or prefixes	Preferred TON to PSTN Same as TON-IN	None
<input type="checkbox"/> TON via length check		
Default TON from SIP Unknown		
Called party number		
<input checked="" type="checkbox"/> Match PNACs and/or prefixes	Preferred TON to PSTN Same as TON-IN	None
<input type="checkbox"/> TON via length check	<input type="checkbox"/> Set TON-OUT to Unknown for E911 calls	
Default TON from SIP Unknown		
Connected number		
<input checked="" type="checkbox"/> Copy configuration from INCOMING calling party number		
<input type="checkbox"/> Match prefixes for Unknown numbers	Normal Mode	
<input type="checkbox"/> TON via length check	Preferred TON to SIP Same as TON-IN	Add PNAC and Prefix
	Survivable Mode	
	Preferred TON to SIP Same as TON-IN	Add PNAC and Prefix

Match PNACs and Prefixes (calling and called): If set, the leading digits of the incoming calling or called party number are matched against (in this order) the International PNAC and Prefix, National PNAC and Prefix and Subscriber PNAC and Prefix. The combination of PNAC and prefix field must have a non-empty value to match.

TON via Length Check (calling and called): If the TON after the previous checks is still Unknown and if this check is 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.

The following are the possible options on the drop-down list boxes:

Outgoing Calls to the PSTN					
Calling Party Number			Called Party Number		
Default TON from SIP	Preferred TON to PSTN	Post Manipulation	Default TON from SIP	Preferred TON to PSTN	Post Manipulation
International	Same as TON-IN	None	International	Same as TON-IN	None
National	International	Unknown TON	National	International	Unknown TON
Subscriber	National	Add Prefix + Unknown TON	Subscriber	National	Add Prefix + Unknown TON
Unknown	Subscriber		Unknown	Subscriber	
				Local Toll Table	

Preferred TON to PSTN:

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 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 code, then the area code is stripped as well.

Local Toll Table: the output TON will be determined from the LTT lookup.

Post-Manipulation Settings:

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.

For outgoing numbers:

- IF "Match PNACs and Prefixes" is set THEN
 - Set "Default TON from SIP" to "Unknown" and disable it.
 - Enable "TON via length check" and reset the checkbox.
- ELSE
 - Set "Default TON from SIP" to "Unknown" and enable it.
 - Disable "TON via length check" and reset the checkbox.

57.6.3 OSB 50i/500i Gateway Number Modification Implementation

Below is the logic that is implemented for each of these settings:

Step 1a (Outgoing Calls): Determine the [TON-IN](#) of the From/PAI/P-Preferred-Identity/Diversion/Request-URI number received in the SIP INVITE message as follows:

- IF number starts with '+', TON-IN is **INT** (strip the '+').
- ELSE IF *Match PNACs and Prefixes* is not checked, set TON-IN according to GUI field "Default TON from SIP"
- ELSE IF *Match PNACs and Prefixes* is checked:
 - IF number starts with *International PNAC and Prefix*, TON-IN is **INT** (strip the PNAC and Prefix).
 - ELSE IF number starts with *National PNAC and Prefix*, TON-IN is **NAT** (strip the PNAC and Prefix).
 - ELSE IF number starts with *Subscriber PNAC and Prefix*, TON-IN is **SUBS** (strip the PNAC and Prefix).
 - IF *Country Code* is 1 and *National Number Length* is 10, TON-IN is **SUBSwAC**
 - ELSE TON-IN is **Unknown**
 - IF TON-IN is **Unknown** and *TON via Length Check* is checked and *National Number Length* and/or *Subscriber Number Length* are not empty:
 - IF *Number Length* matches the *National Number Length*, TON-IN is **NAT**
 - ELSE IF *Number Length* matches the *Subscriber Number Length*, TON-IN is **SUBS**
 - ELSE TON-IN remains **Unknown**

Step 1b (Incoming Calls): Determine the [TON-IN](#) of the Calling/Redirecting/Called Party number received in the ISDN SETUP message as follows:

- IF NPI is ISDN and ISDN TON is International, TON-IN is **INT**
- ELSE IF NPI is ISDN and ISDN TON is National, TON-IN is **NAT**
- ELSE IF NPI is ISDN and ISDN TON is Subscriber, TON-IN is **SUBS**
- ELSE IF *Match Prefixes for Unknown Numbers* is checked and the *International/National/Subscriber Prefixes* fields are not empty:
 - IF Number starts with *International Prefix*, TON-IN is **INT** (strip international prefix)
 - ELSE IF Number starts with *National Prefix*, TON-IN is **NAT** (strip national prefix)
 - ELSE IF Number starts with *Subscriber Prefix*, TON-IN is **SUBS** (strip subscriber prefix)
 - ELSE TON-IN is **SUBS** (do not strip anything)
 - IF *Country Code* is 1 and *Number Length* is 10, TON-IN is **SUBSwAC**
- ELSE IF *TON via Length Check* is checked and *National Number Length* and/or *Subscriber Number Length* are not empty:
 - IF *Number Length* matches the *National Number Length*, TON-IN is **NAT**
 - ELSE IF *Number Length* matches the *Subscriber Number Length*, TON-IN is **SUBS**
- ELSE TON-IN is **Unknown**

Step 2a: Determine the [TON-OUT](#) for the **Calling Party** based on the **Preferred TON** setting:

- IF the OSB is in Survivable Mode AND the "Local Toll Table" checkbox (see **Error! Reference source not found.**) is checked:
 - Look up the Called Party/Calling Party relationship in the Local Toll Tables (see section **Error! Reference source not found.**) and use the resulting output to create an X-Oscar header to insert into the INVITE message. Proceed with the next bullet in the sequence.
- IF Preferred TON is International:

- IF TON-IN is INT, TON-OUT is INT (leave number unchanged)

- ELSE IF TON-IN is NAT, TON-OUT is INT (add country code)
- ELSE IF TON-IN is SUBSwAC, TON-OUT is INT (add country code)
- ELSE IF TON-IN is SUBS, TON-OUT is INT (add country code and area code)
- ELSE, TON-OUT is UNKNOWN
- ELSE IF Preferred TON is National (applies to outgoing calls only):
 - IF TON-IN is INT and number starts with country code, TON-OUT is NAT (remove country code)
 - ELSE IF TON-IN is INT and number does not start with country code, TON-OUT is INT (leave number unchanged)
 - ELSE IF TON-IN is NAT, TON-OUT is NAT (leave number unchanged)
 - ELSE IF TON-IN is SUBSwAC, TON-OUT is NAT (leave number unchanged)
 - ELSE IF TON-IN is SUBS, TON-OUT is NAT (add area code)
 - ELSE, TON-OUT is UNKNOWN
- ELSE IF Preferred TON is Subscriber (applies to outgoing calls only):
 - IF TON-IN is INT and number starts with country code and area code, TON-OUT is SUBS (remove country code and area code)
 - ELSE IF TON-IN is INT and number starts with country code, TON-OUT is NAT (remove country code)
 - ELSE IF TON-IN is INT and number does not start with country code, TON-OUT is INT (leave number unchanged)
 - ELSE IF TON-IN is NAT and number starts with area code, TON-OUT is SUBS (remove area code)
 - ELSE IF TON-IN is NAT and number does not start with area code, TON-OUT is NAT (leave number unchanged)
 - ELSE TON-OUT is TON-IN (leave number unchanged)
- ELSE IF Preferred TON is Same as TON-IN
 - TON-OUT is TON-IN (leave number unchanged)

Step 2b: Determine the **TON-OUT** for the **Called Party** based on the **Preferred TON** setting:

- IF Outgoing call and Preferred TON is Local Toll Table:
 - Look up the Called Party/Calling Party relationship in the Local Toll Tables (see section **Error! Reference source not found.**) and use the resulting output to set TON-OUT.
 - IF TON-OUT from LTT is National:
 - IF TON-IN is INT and number starts with country code, TON-OUT is NAT (remove country code)
 - ELSE IF TON-IN is INT and number does not start with country code, TON-OUT is INT (leave number unchanged)
 - ELSE IF TON-IN is NAT, TON-OUT is NAT (leave number unchanged)
 - ELSE IF TON-IN is SUBSwAC, TON-OUT is NAT (leave number unchanged)
 - ELSE IF TON-IN is SUBS, TON-OUT is NAT (add area code)
 - ELSE, TON-OUT is UNKNOWN
 - ELSE IF TON-OUT from LTT is Subscriber:
 - IF TON-IN is INT and number starts with country code and area code, TON-OUT is SUBS (remove country code and area code)
 - ELSE IF TON-IN is INT and number starts with country code, TON-OUT is NAT (remove country code)
 - ELSE IF TON-IN is INT and number does not start with country code, TON-OUT is INT (leave number unchanged)
 - ELSE IF TON-IN is NAT and number starts with area code, TON-OUT is SUBS (remove area code)
 - ELSE IF TON-IN is NAT and number does not start with area code, TON-OUT is NAT (leave number unchanged)

- ELSE TON-OUT is TON-IN (leave number unchanged)
- ELSE IF TON-OUT from LTT is SUBSwAC:
 - IF TON-IN is INT and number starts with country code, TON-OUT is SUBSwAC (remove country code)
 - ELSE IF TON-IN is INT and number does not start with country code, TON-OUT is INT (leave number unchanged)
 - ELSE IF TON-IN is NAT, TON-OUT is SUBSwAC (leave number unchanged)
 - ELSE IF TON-IN is SUBS, TON-OUT is SUBSwAC (add area code)
 - ELSE TON-OUT is TON-IN (leave number unchanged)
- ELSE IF TON-OUT from LTT is Unknown
 - TON-OUT is TON-IN (leave number unchanged)
- ELSE IF Preferred TON is International:
 - IF TON-IN is INT, TON-OUT is INT (leave number unchanged)
 - ELSE IF TON-IN is NAT, TON-OUT is INT (add country code)
 - ELSE IF TON-IN is SUBSwAC, TON-OUT is INT (add country code)
 - ELSE IF TON-IN is SUBS, TON-OUT is INT (add country code and area code)
 - ELSE, TON-OUT is UNKNOWN
- ELSE IF Preferred TON is National (does not apply to incoming Normal Mode calls):
 - IF TON-IN is INT and number starts with country code, TON-OUT is NAT (remove country code)
 - ELSE IF TON-IN is INT and number does not start with country code, TON-OUT is INT (leave number unchanged)
 - ELSE IF TON-IN is NAT, TON-OUT is NAT (leave number unchanged)
 - ELSE IF TON-IN is SUBSwAC, TON-OUT is NAT (leave number unchanged)
 - ELSE IF TON-IN is SUBS, TON-OUT is NAT (add area code)
 - ELSE, TON-OUT is UNKNOWN
- ELSE IF Preferred TON is Subscriber (does not apply to incoming Normal Mode calls):
 - IF TON-IN is INT and number starts with country code and area code, TON-OUT is SUBS (remove country code and area code)
 - ELSE IF TON-IN is INT and number starts with country code, TON-OUT is NAT (remove country code)
 - ELSE IF TON-IN is INT and number does not start with country code, TON-OUT is INT (leave number unchanged)
 - ELSE IF TON-IN is NAT and number starts with area code, TON-OUT is SUBS (remove area code)
 - ELSE IF TON-IN is NAT and number does not start with area code, TON-OUT is NAT (leave number unchanged)
 - ELSE TON-OUT is TON-IN (leave number unchanged)
- ELSE IF Preferred TON is Same as TON-IN
 - TON-OUT is TON-IN (leave number unchanged)

Step 3: Determine the **Post Manipulation** based on the TON-OUT from 2a or 2b:

- IF there is an LTT Header and Post Manipulation is set to **Add PNAC and Prefix**
 - IF LTT lookup result is INT, add International PNAC and Prefix to the X-Oscar-LTT-Calling-DN Header
 - ELSE IF LTT lookup result is NAT, add National PNAC and Prefix to the X-Oscar-LTT-Calling-DN Header
 - ELSE IF LTT lookup result is SUBSwAC, add Subscriber PNAC and Prefix to the X-Oscar-LTT-Calling-DN Header
 - ELSE IF LTT lookup result is SUBS, add Subscriber PNAC and Prefix to the X-Oscar-LTT-Calling-DN Header
 - ELSE nothing to be done

- IF Post Manipulation is set to **None**
 - IF TON-OUT is SUBSwAC, TON-OUT is NAT (leave number unchanged)
 - ELSE nothing to be done (leave number unchanged)
- ELSE IF Post Manipulation is set to **GNF** (does not apply to Survivable Mode)
 - IF TON-OUT is INT, TON-OUT is Unknown (add '+')
 - ELSE IF TON-OUT is SUBSwAC, TON-OUT is NAT (leave number unchanged)
 - ELSE nothing to be done anymore (leave number unchanged)
- ELSE IF Post Manipulation is set to **Add Prefix + Unknown TON**
 - IF TON-OUT is INT, TON-OUT is Unknown (add International Prefix)
 - ELSE IF TON-OUT is NAT, TON-OUT is Unknown (add National Prefix)
 - ELSE IF TON-OUT is SUBSwAC, TON-OUT is Unknown (add Subscriber Prefix)
 - ELSE IF TON-OUT is SUBS, TON-OUT is Unknown (add Subscriber Prefix)
 - ELSE (leave number unchanged)
- ELSE IF Post Manipulation is set to **Add PNAC and Prefix**
 - IF TON-OUT is INT, TON-OUT is Unknown (add International PNAC and Prefix)
 - ELSE IF TON-OUT is NAT, TON-OUT is Unknown (add National PNAC and Prefix)
 - ELSE IF TON-OUT is SUBSwAC, TON-OUT is Unknown (add Subscriber PNAC and Prefix)
 - ELSE IF TON-OUT is SUBS, TON-OUT is Unknown (add Subscriber PNAC and Prefix)
 - ELSE nothing to be done anymore
- ELSE IF Post Manipulation is set to **Unknown TON**
 - TON-OUT is Unknown (leave number unchanged)

57.7 Local Toll Table

The screenshot shows the 'Integrated Gateway' configuration page. It includes sections for 'Gateway Configuration' (with Card 1 FRI and Card 2 FXS), 'QoS Monitoring' (with an 'Enable QoS monitoring' checkbox), and 'Local Toll Tables'. An arrow points from the 'Local Toll Tables' button in the top section to the 'Local Toll Table Configuration' section below. This section includes a table of 'Local Toll Tables Imported to OSB' and an 'Upload Local Toll Table from OSV' button.

	Local Toll Table Name	Number	Modified
1	Boca-Toll-3	1 561 923	2012-06-18 11:34:55
2	Boca-Toll-32	1 561 923	2012-06-18 11:34:55

Local Toll Tables (LTT) will be used by the OSB to determine how to display an incoming PSTN calling party number, and, if the customer so selects, how to set the Type of Number (TON) for an outgoing calling party number.

Local Toll Tables are created on the OSV and then imported into an OSB using mechanisms described further below. The OSB will have no mechanisms for creating or updating local Toll Tables.

Local Toll Tables will apply to the OSB 50i and OSB 500i integrated gateways only. They will not apply to SSPs or other types of external gateways.

Any number that is presented for LTT handling must be normalized to international format.

Local Toll Tables apply to the North American Numbering Plan (NANP) only.

Note that LTT manipulation applies to the **called party** of outgoing calls in both Normal Mode and Survivability Mode.

For incoming calls, the LTT will be used for the **calling party number**.

57.7.1 Creation of LTT

- The LTT that is populated on the OSV will be downloaded by the customer to a local server and then uploaded to the OSB. The creation of the OSV LTT file will be handled manually by the user.
- To create the file, the user must start the RTP CLI on the OSV and enter the following command:
- `soapExport "-f=<output file name and path> -NumMod"`
- The '*output file name and path*' will typically point to a location on the user's computer, or a network share location

58 OpenScape Branch 50i/500i as GW Only

58.1 OpenScape Voice

In the OpenScape Voice the following endpoints shall be configured:

One endpoint for the OSB Main as the main destination of all calls to the gateway.

GeneralSIPAttributesAliasesRoutesAccounting

Endpoint Type

SIP Private Networking:☐

SIP Trunking:☒

SIP-Q Signaling:☐

SIP Signaling

For the static Endpoints the address of the SIP signaling interface can be specified in IP or FQDN format.
Note that the address of the signaling interface cannot be modified unless the entry in the security section has first been removed.

Type:

Static

Signaling Address Type:

IP Address or FQDN

Endpoint Address:

21.21.31.10

Port:

5061

Transport protocol:

TLS

Security

Set the Realm, Username and Password for digest authentication or configure the signaling address as a trusted one.

Add...

Edit...

Delete...

Sel:0 | Items/Page: 200 | All:1

☐

Trusted

☐

☒

General SIP **Attributes** Aliases Routes Accounting

Attributes

Attributes available for this SIP endpoint

Supports SIP UPDATE Method for Display Updates	<input type="checkbox"/>
UPDATE for Confirmed Dialogs Supported	<input type="checkbox"/>
Survivable Endpoint	<input checked="" type="checkbox"/>
SIP Proxy	<input checked="" type="checkbox"/>
Central SBC	<input type="checkbox"/>
Route via Proxy	<input checked="" type="checkbox"/>
Allow Proxy Bypass	<input checked="" type="checkbox"/>


Endpoint Attributes:
 - Survivable Endpoint
 - SIP Proxy
 - Route via Proxy
 - Allow Proxy Bypass

General SIP **Attributes** **Aliases** Routes Accounting

Aliases

You can associate here aliases with a SIP Endpoint.

Sel:0 | Items/Page: 200 | All:1

<input type="checkbox"/>	Name
<input type="checkbox"/>	 21.21.31.10

Public/Offnet Traffic must also be enabled.

Note: Do not Send Invite without SDP must NOT be selected on OSB50i/OSB500i Integrated Gateway EndPoint.

OSB IP address must be configured for alias. When using OSB with Splitterbox Configuration (PRI Redundancy), Alias should include Redundant IP and Physical IP addresses for both OSB nodes.

Two additional endpoints shall be configured for each gateway in order to provide an alternative if the OSB Main is not accessible:

1. SIP Endpoint on OSV for OpenScape Branch

The screenshot shows the configuration interface for a SIP endpoint. The 'SIP' tab is active. Under 'Endpoint Type', 'SIP Trunking' is selected. Under 'SIP Signaling', the 'Type' is set to 'Static'. The 'Signaling Address Type' is 'IP Address or FQDN'. The 'Endpoint Address' is '21.21.29.10'. The 'Port' is '5061'. The 'Transport protocol' is 'TLS'. A yellow note box with an arrow pointing to the port field contains the following text:

If port is set to a different port (e.g. **5062**), then it is necessary to add this port as an alias (21.21.31.10:5062)''

General SIP **Attributes** Aliases Routes Accounting

Attributes

Attributes available for this SIP endpoint

Supports SIP UPDATE Method for Display Updates	<input type="checkbox"/>
UPDATE for Confirmed Dialogs Supported	<input type="checkbox"/>
Survivable Endpoint	<input type="checkbox"/>
SIP Proxy	<input checked="" type="checkbox"/>
Central SBC	<input type="checkbox"/>
Route via Proxy	<input checked="" type="checkbox"/>

Attributes **Route Via Proxy** and **SIP Proxy** must be set. Attribute **Survivable Endpoint** must be set if subscriber rerouting is required for survivability.

General SIP Attributes **Aliases** Routes Accounting

Aliases

You can associate here aliases with a SIP Endpoint.

Set:0 | Items/Page: 200 | All:1

<input type="checkbox"/>	Name
<input type="checkbox"/>	 21.21.31.10

If OPTIONS port is set to a different port (e.g. 5062), then it is necessary to add this port as an alias (21.21.31.10:5062)

OSB IP address must be configured for alias (Port is optional. Ex 10.234.1.70:5060).

Note: if using OSB with Redundancy then Alias should include Redundant IP and Physical IP addresses for both OSB nodes.

2. SIP Endpoint on OSV for gateway

General

SIP

Attributes

Aliases

Routes

Accounting

Endpoint Type

SIP Private Networking:

☐

SIP Trunking:

☒

SIP-Q Signaling:

☐

SIP Signaling

For the static Endpoints the address of the SIP signaling interface can be specified in IP or FQDN format.
Note that the address of the signaling interface cannot be modified unless the entry in the security section has first been removed.

Type:

Static

Signaling Address Type:

IP Address or FQDN

Endpoint Address:

21.21.29.10

Port:

5061

Transport protocol:

TLS

General SIP Attributes Aliases Routes Accounting

Endpoint

Define the connection data of an endpoint, e.g. you may use this to add a gateway to a switch.

Name: osb_autom_og

Remark:

Registered: ☒

Profile: epp_Proxy_Autom ...

Branch Office: Proxy_BRI_FXS ...

Associated Endpoint: 50iBRI_Aproxy

Endpoint associated to OSB Main endpoint

General SIP Attributes Aliases Routes Accounting

Attributes

Attributes available for this SIP endpoint

Supports SIP UPDATE Method for Display Updates ☐

UPDATE for Confirmed Dialogs Supported ☐

Survivable Endpoint ☐

SIP Proxy ☐

Central SBC ☐

Route via Proxy ☒

Allow Proxy Bypass ☐

Public/Offnet Traffic ☒

Attribute Route via Proxy to route the calls via the associated endpoint.
Attribute Public/Offnet Traffic must be also enabled
Note: "Do not Send Invite without SDP" attribute must NOT be selected on OSB50i/OSB500i Integrated Gateway End Point.

General SIP Attributes Aliases Routes Accounting

Aliases

You can associate here aliases with a SIP Endpoint.

Sel:0 | Items/Page: 200 | All:2

<input type="checkbox"/>	Name
<input type="checkbox"/>	21.21.29.10:5096

IP Address and port of Asterisk (5096)

RTP Parameter:
Srx/Sip/CentralSbcSupport must be
RtpTrue (this will make OSV look for ports
in aliases)

When using OSB with Splitterbox Configuration (PRI Redundancy), Alias should include Redundant IP and Physical IP addresses for both OSB nodes.

All SIP Requests shall be sent to the OSB Main and if the OSB Main is not accessible, the SIPRequests will be directly sent to the 50i/500i gateway.

58.2 OpenScope Branch Main

The OSB Main shall be configured as a regular SIP Proxy/ Branch SBC. Operation modes SBC- Proxy and Proxy ACD are also possible.

If OSB Main is not able to communicate to both OSV Node 1 and OSV Node 2 it shall switch to survivable mode. The OSB Main will be responsible for providing the survivable features to the branch

The OSB Main shall not perform any PNAC handling in outgoing calls to the external gateways. The PNAC shall be performed by TON handling in the gatewayitself.

58.2.1 VoIP

TCP/Port 5060	OSV Mode	TLS/Port 5061
	Simplex	
sipsm1_vip	Node 1 Primary Server	sipsm3_vip
	Collocated	
sipsm1_vip	Node 1 Primary Server	sipsm3_vip
	Node 1 Secondary Server	
sipsm2_vip	Node 2 Primary Server	sipsm4_vip
	Node 2 Secondary Server	
	Geo-Separated	
sipsm1_vip	Node 1 Primary Server	sipsm3_vip
sipsm2_vip	Node 1 Secondary Server	sipsm4_vip
sipsm2_vip	Node 2 Primary Server	sipsm4_vip

sipsm1_vip	Node 2 Secondary Server	sipsm3_vip
------------	----------------------------	------------

Select OK to temporarily store changes. Make your changes permanent by selecting 'Apply Changes' on the General page.

Sip Server Settings

Port and Signaling Settings

Manipulation and Routing

Error Codes

Media

General

Comm System Type geo-separated

OPTIONS source port 5062

IP Version Towards SIP Server IPv4

- ☐ Enable path tagging
- ☐ Branch behind SBC
- ☐ Branch behind NAT
- ☐ Synch subscriber data
- ☐ Disable notification in survivable mode
- ☐ Enforce minimum Subscriber TransportType Security

If the OSV is addressed by means of a DNS SRV, the DNS SRV record shall be configured in the field SRV Record.

If there is a central SBC (e.g. OpenScape SBC) in front of the OSV in the Data Center, the central SBC shall be configured as the SIP Server.

If the Gateway Only is an OSB 50i with FXS ports, the flag Enable Path Tagging shall be enabled

Other trusted servers

Load Balance Mapping Table

Node 1

Target type Binding

Primary server 10.100.182.56 Transport TLS Port 5061

Backup server 10.100.183.57 Transport TLS Port 5061

SRV record Transport TCP

Node 2

Target type Binding

Primary server 10.100.183.57 Transport TLS Port 5061

Backup server 10.100.182.56 Transport TLS Port 5061

58.2.2 Gateway

Gateways/Trunks										
Gateways/Trunks provisioning.										
Row	Signaling address type	Remote URL	Port	Interface	Transport	Routing prefix	Gateway/Trunk type	Functional type	Trunk profile	Output digit strip
1	IP address or FQDN	50ia.unow.s01.cwb	5096	LAN	UDP	8%	Integrated Gateway	All Modes Egress/Ingress	Gateway	9
2	IP address or FQDN	50ia.unow.s01.cwb	5096	LAN	UDP	0280%	Integrated Gateway	All Modes Egress/Ingress	Gateway	4
3	IP address or FQDN	og.unow.net5.cwb	5061	LAN	TLS	0290%	OSB 50i/500i	All Modes Egress/Ingress	Gateway	0
4	IP address or FQDN	og.unow.cas.cwb	5061	LAN	TLS	0291%	OSB 50i/500i	All Modes Egress/Ingress	Gateway	0

Gateway Configuration

Gateway configuration provisioning.

General

Signaling address type

IP address or FQDN

Remote URL

og.unow.net5.cwb

Port

5061

Interface

LAN

Transport

TLS

Routing prefix

0290%

Gateway/Trunk type

OSB 50i/500i

Functional type

All Modes Egress/Ingress

Trunk profile

Gateway

Output digit strip

0

Output digit add

Priority

1

The OSB50i/500i shall be configured as external gateway with Gateway / Trunk type set to the new option OSB 50i/500i

58.2.3 Media Server

The integrated media server in the OSB Main shall serve the SIP Subscribers and gateways.

58.2.4 Auto Attendant

The auto-attendant in the OSB Main shall serve the SIP Subscribers and gateways.

58.2.5 Survivable Mode features

Survivable mode features like MLHG, Backup ACD, System Call Forward, SIP Manipulation and CDR shall only be provided by OSB Main.

58.2.6 Redundancy

It shall be possible to configure a redundant SIP Proxy. The SIP Proxy shall be addressed by means of a Virtual IP.

58.2.7 Backup Link

Backup link shall be managed by the OSB Main and it shall be established through the external gateways which can be the OSB 50i/500i.

58.2.8 DNS

The OSB Main shall be configured as DNS Server as slave or forward to a DNS Master in the Data Center.

58.2.9 NTP

The OSB Main shall be configured to synchronize with an NTP server and it can also be configured to operate as NTP server for the external gateways

58.2.10 Digest Authentication

Digest Authentication in SM shall be performed by the OSB Main.

Synchronization of Subscriber Data and Digest Authentication Credentials shall be performed by the OSB Main.

58.2.11 Licensing

The OSB Main shall control the licenses which are applicable to the branch, that means:

. Base license.

User licenses.

Auto-Attendant license.

Backup ACD license.

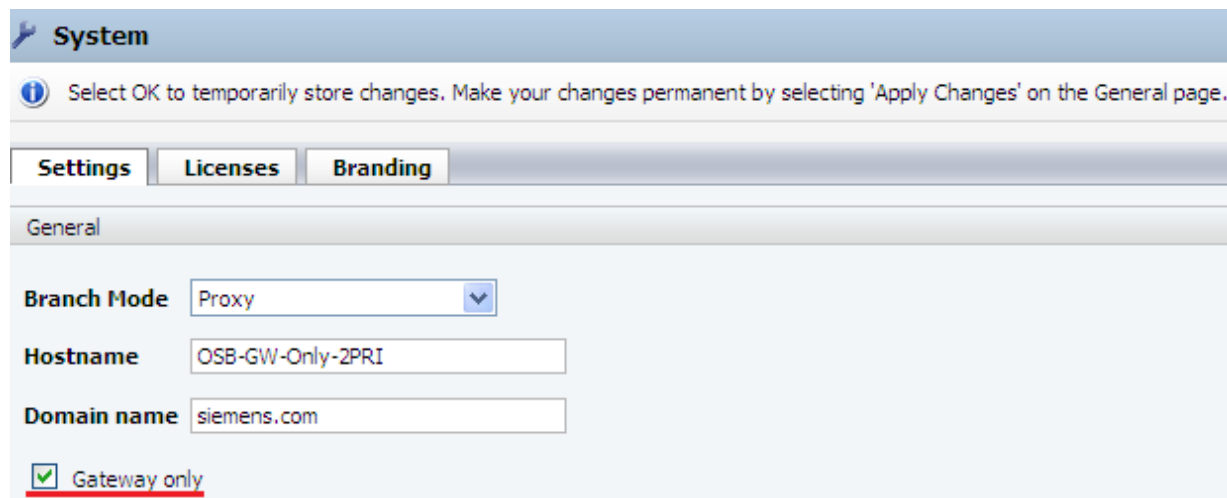
SBC session licenses

58.2.12 Caller Number Suppression

In a call to be routed through the Gateway Only, the access code of Caller Number Suppression shall be handled by the Gateway Only if the OSB Main is in survivable mode

58.3 OpenScape 50i/500i Gateway

58.3.1 Gateway Only Configuration



The screenshot displays the 'System' configuration page for an OpenScape 50i/500i Gateway. At the top, a blue header bar contains a wrench icon and the word 'System'. Below this, a message box with an information icon states: 'Select OK to temporarily store changes. Make your changes permanent by selecting 'Apply Changes' on the General page.' A tabbed interface follows, with 'Settings', 'Licenses', and 'Branding' tabs; 'Settings' is currently selected. Under the 'Settings' tab, the 'General' sub-tab is active. The configuration fields include: 'Branch Mode' set to 'Proxy' (via a dropdown menu), 'Hostname' set to 'OSB-GW-Only-2PRI', and 'Domain name' set to 'siemens.com'. At the bottom, the 'Gateway only' checkbox is checked and underlined in red.

System

Select OK to temporarily store changes. Make your changes permanent by selecting 'Apply Changes' on the General page.

Settings Licenses Branding

General

Branch Mode Proxy

Hostname OSB-GW-Only-2PRI

Domain name siemens.com

☒ Gateway only

VOIP

Select OK to temporarily store changes. Make your changes permanent by selecting 'Apply Changes' on the General page.

Sip Server Settings
Port and Signaling Settings
Manip

Comm System Type

OPTIONS source port

IP Version Towards SIP Server

☐ Enable path tagging
☐ Branch behind SBC
☐ Branch behind NAT
☐ Synch subscriber data
☐ Disable notification in survivable mode
☐ Enforce minimum Subscriber TransportType Security

Other trusted servers

Load Balance Ma

Outbound Proxy

☒ Enable outbound proxy

Target type

Outbound proxy Transport **Outbound proxy port**

SRV record Transport

Node 1

Target type

Primary server Transport **Port**

Backup server Transport **Port**

SRV record Transport

Node 2

Target type

Primary server Transport **Port**

Backup server Transport **Port**

The OSB Main shall be configured as the Outbound Proxy.

The OpenScape Voice Node 1 shall be configured as the Primary SIP Server of Node 1. In case of Geo-Separated, the OSV Node 2 shall be configured as Backup SIP Server of Node 1. For Collocated and Geo-Separated the OpenScape Voice Node 2 shall be configured as the Primary SIP Server of Node 2. In case of Geo-Separated, the OSV Node 1 shall be configured as the Backup Server of Node 2

Following the concept of "loose routing", the Outbound Proxy shall indicate to which IP address the message shall be sent to. The Node 1 configuration shall indicate the final destination of the SIP message, that means, the IP address or FQDN which will be used in the R-URI.

If the OSB 50i/500i as Gateway only is connected to an OSB Main which is configured as Branch SBC, the configuration of the SIP Server in the OSB 50i/500i remains the same.

If the OSB 50i/500i as Gateway only is connected to an OSB Main which is connected to a Central SBC (e.g. OpenScape SBC), the SIP Server shall be configured in the OSB 50i/500i to point to the Central SBC.

If the OSB50i/500i as Gateway only is directly connected to an OpenScape SBC, no Outbound Proxy shall be configured and the OS SBC shall be configured as the SIP Server.

Gateway Configuration

Gateway configuration provisioning.

General

Signaling address type: IP address or FQDN

Remote URL: og.unow.net5.cwb

Port: 5096

Interface: LAN

Transport: UDP

Routing prefix: 0290%

Gateway/Trunk type: Integrated Gateway

Functional type: All Modes Egress/Ingress

Trunk profile: Gateway

Output digit strip: 4

Output digit add:

Priority: 1

☐ Operational Mode in OPTIONS Response

The gateway shall be configured as **Integrated Gateway**, which shall be the only option for the Gateway Type.

The trunks can be FXO, BRI or PRI.
Analog phones (FXS) in the OSB50i can be used.

The analog phones shall be registered through the OSB Main.

60.3.4 DNS

Network/Net Services

Select OK to temporarily store changes. Make your changes permanent by selecting 'Apply Changes' on the General page.

Settings DNS NTP DHCP Traffic Shaping QoS

Client

Refresh DNS

DNS server IP address: 21.21.31.10
192.168.100.4

Add

Alias:

Server

☐ Enable DNS server

DNS configuration

The OSB50i/500i shall be configured as DNS client with the OSB Main as the primary DNS server and the Master DNS server in the data center as the secondary DNS server

If the OSB 50i/500i is set as Gateway only, the flag Enable DNS Server shall be grayed out

Network/Net Services

Select OK to temporarily store changes. Make your changes permanent by selecting 'Apply Changes' on the General page.

Settings DNS **NTP** DHCP Traffic Shaping QoS

NTP Settings

Timezone (GMT -3:00) Brasilia, Buenos Aires, Georgetown

☐ Enable local NTP server

☐ Manual configuration

Date (mm.dd.yyyy) 06.22.2015 Time (hh:mm) 15:49

☒ Synchronize with NTP server

NTP server Add Synchronize now

21.21.31.10

If the OSB 50i/500i is set as Gateway only, the flag Enable local NTP Server shall be grayed out

The OSB Main shall be configured as the NTP server for the OSB 50i/500i.

58.3.2 Licensing

If the OSB 50i/500i is set as Gateway only, a Base License shall be required. For the FXS, no licenses shall be required on the Gateway Only box because they will be controlled by the OSB Main or by OSV.

General - BO-BG01-50iA

Branch aggregated information and data.

Alarms

Alarm summary: Critical: 0 ■ Major: 0 ■ Minor: 0 ■
Show alarm details

System Status

System Info

Branch mode: Proxy Auto refresh timer: 30 sec ▼

Operational state: normal

The OSB Main will present the System Status screen as shown

Com Node 1

Primary server: 10.100.182.56 Penalty box state: ■ Active
 Backup server: 10.100.183.57 Penalty box state: ■ Active

Com Node 2

Primary server: 10.100.183.57 Penalty box state: ■ Active
 Backup server: 10.100.182.56 Penalty box state: ■ Active

Services status Show

Registered subscribers Show

Link status Show

Dynamic port mapping Show

Backup link status Show

Subscriber data Show

Denial of Service Mitigation Show

CPU ■ 8.67 %
 Memory ■ 52.56 % - 2 Gb
 Disk ■ 27.89 % - 8 Gb
 System uptime: 14 days 1:56
 Hardware type: Advantech 50i (BRI - FXS)
 Hostname: BO-BG01-50iA

Software Info

Software version: V8 R1.01.00
 Software Partition information: Active Backup

General - OSB-GW-Only-2PRI

Branch aggregated information and data.

Alarms

Alarm summary: Critical: 0 Major: 0 Minor: 0 [Show alarm details](#)

System Status

Branch mode: Proxy - Gateway Only
Operational state: Normal - Outbound Proxy Normal

Auto refresh timer: 30 sec

Com Outbound Proxy

Outbound proxy: 21.21.31.10

Penalty box state: Active

Com Node 1

Primary server: 10.100.182.56

Penalty box state: Reachable

Backup server: 10.100.183.57

Penalty box state: Reachable

Com Node 2

Primary server: 10.100.183.57

Penalty box state: Reachable

Backup server: 10.100.182.56

Penalty box state: Reachable

Services status

[Show](#)

Registered subscribers

[Show](#)

Link status

[Show](#)

Dynamic port mapping

[Show](#)

Backup link status

[Show](#)

Subscriber data

[Show](#)

Denial of Service Mitigation

[Show](#)

System Info

CPU: 4.88 %
Memory: 36.72 % - 2 Gb
Disk: 27.18 % - 8 Gb
System uptime: 14 days 1:51
Hardware type: Advantech 50i (2 PRIs/CAS E1 - FXS)
Hostname: OSB-GW-Only-2PRI

Software Info

Software version: V8 R1.01.00

Software Partition information:

[Active](#)

[Backup](#)

The OSB 50i/500i Gateway will present the System Status screen as shown

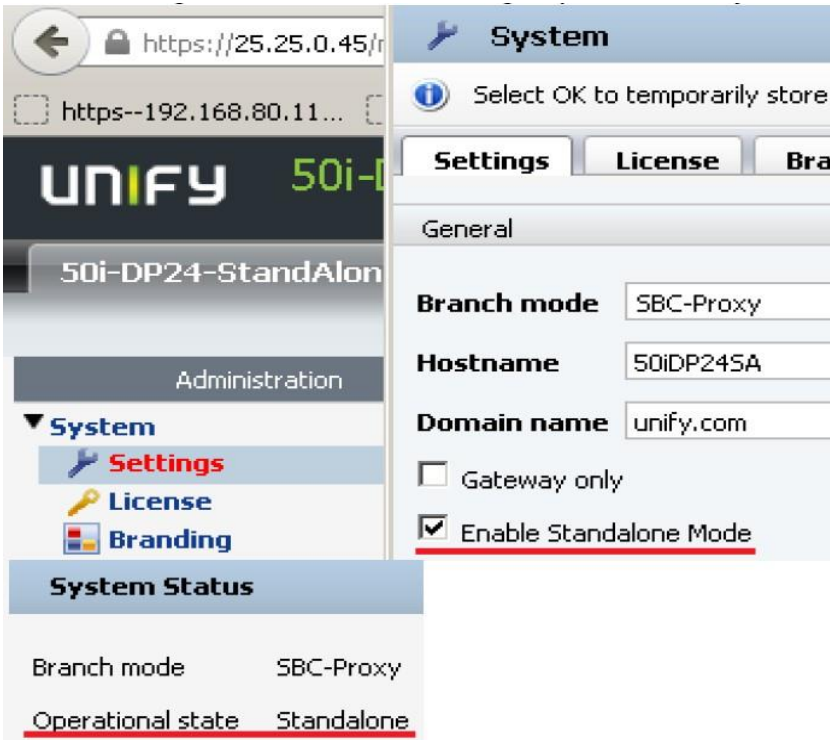
59

OSB 50i DP24 and OSB 500i DP4/8 as standalone PRI Adapters to SIP Trunking

With this functionality the OSB can be used as standalone unit for legacy TDM PBX systems to be connected to new SIP Trunking providers. The OSB supports NT PRI links to interconnect deployed PBX systems and be able to support same capacity of SIP Trunking channels to SIP Service providers.
This configuration introduction requires a new 'Standalone' operating mode.
Supported Models:

- OSB500i DP4/8
- OSB50i DP24
- OSB50i DP14E/T
- OSB50i D44

Standalone Mode can be enabled via flag under **Administration >System >Settings >General**
The enabling of the Standalone flag is possible only if the OSB Branch mode is SBC-Proxy.



When OSB is running in Standalone Mode ,PRI ports license is required.

License type	License configured
OSB Base	1
SBC sessions	60
PRI Ports	2

PSTN interfaces will not be available if the proper license is applied.

OSB 50i D44: a single "PRI Ports" license would activate all 4 BRIs.

NOTE: Currently only the Sipconnect1.1 is supported

60 Proxy ATA

Proxy ATA HW supports 24/48 FXS ports.

The Proxy ATA registers with only one Proxy/OSV and only supports FXS subscribers. PSTN connectivity/routing during Survivability mode is handled by the Proxy. Connection to OSV can be done directly or via Proxy while in Normal Mode operation.

Note: only FXS-FXS calls are possible using Proxy ATA if Proxy and OSV are not available.

60.1 Configuration Options

Proxy ATA can be deployed with direct connectivity to OSV (without survivability) or to another OSB at a branch to provide survivability with the remaining users of the branch.

Note: Maximum distance to analog device is 300feet.

60.1.1 Proxy ATA behind OSB Proxy (ex. OSB500i) connected to OSV

OSV/CMP

- Create ProxyATA Endpoint Profile
- Create ProxyATA Endpoint within the branch office of the OSB Proxy. This will associate the ProxyATA to the OSB Proxy.

--> Attributes "Route Via Proxy" and "SIP Proxy" must be set

--> Attribute "Survivable Endpoint" must be set if subscriber rerouting is required for survivability,

--> Alias is configured with IP address of ProxyATA.

--> No ports need to be set to trusted if using OSV V6 PS23 or OSV V7 PS08. If the OSV is running an older patch set then the OPTIONS port needs to be set to Trusted.

- Add Branch Office using the ProxyATA Endpoint as representative endpoint.
- Configure FXS Subscribers of Proxy ATA in the branch office of the OSB Proxy unless subscriber rerouting is required. In the latter case, the FXS subscribers need to be configured in the branch office of the ProxyATA.

OSB Proxy

- Enable Path Tagging

Configuration ➤ OpenScape Branch ➤ Branch Office ➤ Configuration ➤ VoIP ➤ Sip Server Settings

VOIP

Select OK to temporarily store changes. Make your changes permanent by selecting 'Apply Changes' on the General page.

Sip Server Settings | **Port and Signaling Settings** | **Manipulation and Routing** | **Error Codes** | **Media**

General

Comm System Type: Simplex

OPTIONS source port: 5062

IP Version Towards SIP Server: IPv4

☒ Enable path tagging

Enable Path Tagging: allows an OpenScape Branch in Proxy-ATA mode to send the header "Path" in SIP messages and an OpenScape Branch which has a connected ATA to handle the messages with this header. Flag adds the path header Path: <sip:21.21.0.72;transport=tcp;lr> where 21.21.0.72 is the ProxyATA IP.

- Add GW Entry in Gateways/Trunk Provisioning with IP Address/Port/Transport of ProxyATA.

Configuration > OpenScape Branch > Branch Office > Configuration > Features > Enable gateways/trunks > Configure > Gateways/Trunks

Gateways/Trunks

Gateways/Trunks provisioning.

DNS dynamic refresh interval (min): 60

☐ Route to R-URI domain

Note: Routing Prefix/FQDN value is required to create entry.

Add **Edit** **Delete**

Row	Signaling address type	Remote URL	Port	Interface	Transport	Routing prefix	Gateway/Trunk type	Functional type	Trunk profile	Output digit strip	Output digit add	Priority
1	IP address or FQDN	21.21.0.72	5060	LAN	TCP	24%	Proxy ATA	All Modes Egress/Ingress	Gateway	0		1

Proxy ATA

- Configure "Outbound proxy"/"Outbound proxy port" to IP address/Port of OSB Proxy, Enable Path Tagging, Comm System Type, Primary, and Backup OSV.

Configuration > OpenScape Branch > Branch Office > Configuration > VoIP > Sip Server Settings
Note: Licenses are not required to be installed on ProxyATA (Only on OSV/OSB Proxy)

VOIP

Select OK to temporarily store changes. Make your changes permanent by selecting 'Apply Changes' on the General page.

Sip Server Settings | **Port and Signaling Settings** | **Manipulation and Routing** | **Error Codes** | **Media**

Comm System Type:

OPTIONS source port:

IP Version Towards SIP Server:

☒ Enable path tagging

☐ Branch behind SBC

☐ Branch behind NAT

☐ Synch subscriber data

☐ Enforce minimum Subscriber TransportType Security

Other trusted servers | **Load Balance Mapping Table**

Outbound Proxy

☒ Enable outbound proxy

Target type:

Outbound proxy: Transport: **Outbound proxy port**:

SRV record: Transport:

Node 1

Target type:

Primary server:

Backup server: Transport: Port:

SRV record: Transport:

Node 2

Target type:

Primary server: Transport: Port:

Enable Path Tagging: allows an OpenScape Branch in Proxy-ATA mode to send the header "Path" in SIP messages and an OpenScape Branch which has a connected ATA to handle the messages with this header. Flag adds the path header Path: <sip:21.21.0.72;transport=tcp;lr> where 21.21.0.72 is the ProxyATA IP.

Outbound proxy/Port: The Outbound Proxy IP Address/FQDN/Port where the OpenScape Branch in Proxy-ATA mode will try to connect in case the "enable outbound proxy" flag is enabled. Note: ProxyATA does not support DHCP/DNS server. This is done by OSB Proxy or external DNS/ DHCP.

Primary, Backup, OSV node configuration

60.1.2 Proxy ATA connected directly to OSV

OSV/CMP

- **Create ProxyATA Endpoint Profile**
- **If subscriber rerouting (regular or enhanced) is NOT required, then configure FXS subscribers of the Proxy ATA under the OSV's "Main Office".**
 - Attributes "Route Via Proxy" and "SIP Proxy" must be set
 - Alias is configured with IP address of ProxyATA.
 - No ports need to be set to trusted if using OSV V6 PS23 or OSV V7 PS08. If the OSV is running an older patch set then the OPTIONS port needs to be set to Trusted.
- **If subscriber rerouting (regular or enhanced) IS required, then you must create a branch office for the Proxy ATA, using the Proxy ATA Endpoint as the representative endpoint. You must also create the Proxy ATA FXS subscribers behind that ProxyATA branch.**
 - Attributes "Route Via Proxy", "Survivable Endpoint" and "SIP Proxy" must be set
 - Alias is configured with IP address of ProxyATA.
 - > No ports need to be set to trusted if using OSV V6 PS23 or OSV V7 PS08. If the OSV is running an older patch set then the OPTIONS port needs to be set to Trusted.

Proxy ATA

- **Configure Comm System Type, Primary, and Backup OSV.**

Configuration > OpenScape Branch > Branch Office > Configuration > VolP > Sip Server Settings

Configuration ➤ OpenScape Branch ➤ Branch Office ➤ Configuration ➤ VolP ➤ Sip Server Settings

Note: Licenses are not required to be installed on ProxyATA (Only on OSV).

VOIP

Select OK to temporarily store changes. Make your changes permanent by selecting 'Apply Changes' on the General page.

Sip Server Settings
Port and Signaling Settings
Manipulation and Routing
Error Codes
Media

Comm System Type collocated

OPTIONS source port 5060

IP Version Towards SIP Server IPv4

☐ Enable path tagging
☐ Branch behind SBC
☐ Branch behind NAT
☐ Synch subscriber data
☐ Enforce minimum Subscriber TransportType Security

Other trusted servers
Load Balance Mapping Table

Outbound Proxy

☐ Enable outbound proxy

Target type Binding
 Outbound proxy Transport TCP Outbound proxy port 5060
 SRV record Transport TCP

Node 1

Target type Binding
Primary server 10.100.182.54 Transport TCP **Port** 5060
 Backup server Port
 SRV record

Primary, Backup, OSV node configuration

Node 2

Target type Binding
Primary server 10.100.183.55 Transport TCP **Port** 5060

60.1.3 General Proxy ATA Configuration

Enable Integrated GW

Configuration ➤ OpenScape Branch ➤ Branch Office ➤ Configuration ➤ Features

Features

Enable/Disable desired Feature.

Features Available in Normal Mode and Survivability

☒ Enable integrated gateway **Configure**

Enable Integrated GW.
Note: discovering the GW cards will require a system restart so that drivers are loaded.

Select Country Configuration for Integrated Gateway

Configuration ➤ OpenScape Branch ➤ Branch Office ➤ Configuration ➤ System ➤ Settings

System

Select OK to temporarily store changes. Make your changes permanent by selecting 'Apply Changes' on the right.

Settings Licenses Branding

Country Configuration

Country: United States / North America **Country configuration**

Select Country to get correct defaults for the hookflash timers, ring cadence, and tone frequency.

Country Configuration

us configuration

```
#
# 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.
#
```

Configure FXS ports

Configuration ➤ OpenScape Branch ➤ Branch Office ➤ Configuration ➤ Features ➤ Enable integrated gateway
➤ Gateway Configuration ➤ Configure

Integrated Gateway

Integrated gateway provisioning.

Gateway Configuration

Card 1 FXS

Card 2 FXS

Configure...

FXS card/cards is/are discovered.
Note: Drivers for each FXS port are loaded on a port by port basis during boot process

Select Configuration for FXSparameters/settings.

FXS Configuration

FXS Cards provisioning.

Port Configuration

☒ All ports (Enabling only ports with subscriber number)

☒ Echo cancellation

First SIP port 9500

Enable all ports with subscribers Disable all ports

Edit

Enable	Card	Physical port	Subscriber number	Subscriber name	Digest authentication realm	Digest authentication user ID	Digest authentication password	SIP port	Echo cancellation	Fax device
<input checked="" type="checkbox"/>	1	Port 1	551138172441		hipath.com	123456	*****	9500	<input checked="" type="checkbox"/>	
<input checked="" type="checkbox"/>	1	Port 2	551138172442		hipath.com	123456	*****	9501	<input checked="" type="checkbox"/>	
<input checked="" type="checkbox"/>	1	Port 3	551138172443		hipath.com	123456	*****	9502	<input checked="" type="checkbox"/>	
<input checked="" type="checkbox"/>	1	Port 4	551138172444		hipath.com	123456	*****	9503	<input checked="" type="checkbox"/>	
<input checked="" type="checkbox"/>	1	Port 5	551138172445		hipath.com	123456	*****	9504	<input checked="" type="checkbox"/>	

All ports: enabling only ports with subscriber number.

Echo cancellation: Enabling/Disabling echo cancellation for all ports.

FXS Configuration

FXS Cards provisioning.

Card Configuration

Loop current (mA)

☒ Manual ring settings

Ring frequency

Ring voltage

☒ Hook flash

Hook flash duration

CLIP

☐ Allow compression codecs over FAX lines

☐ Spare flag 3

Loop current: loop current for analog phones.

Manual Ring Settings: Enables configuration for Ring Frequency and Voltage.

Ring Frequency: ring frequency for analog phones. Default is 20.

Ring Voltage: ring voltage for analog phones. Default value is 75.

Hook Flash: turns on or off hook flash capabilities for all ports.

Hook Flash Duration: Long (200ms to 1250ms) or Short (80ms to 200ms) duration hook flash.

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 Configuration

FXS Cards provisioning.

Card Configuration

Loop current (mA)

☒ Manual ring settings

Ring frequency

Ring voltage

☒ Hook flash

Hook flash duration

CLIP

☐ Allow compression codecs over FAX lines

CLIP:
When Country is configured as "United States/North America" or "United States Circa 1950/North America" CLIP is always enabled and will be gray out like picture above.

Other countries have the option to enable (Bellcore after ring) or disable (None) the CLIP.

Default for countries different than US is disabled (None)

FXS port Configuration

FXS Port provisioning.

General

☒ Enable

Card Physical port

SIP port

General:

Enable: Enable or disable the FXS physical port.
Physical port: Number of FXS port. It is a read only field.

Subscriber Configuration

Subscriber number **Digest authentication realm**
Subscriber name **Digest authentication user ID**
Registration interval (sec) **Digest authentication password**
Endpoint service profile **Receive gain (dB)**
Transmit gain (dB)

FXS Flags

☒ Echo cancellation
☐ FAX device
☒ FAX T.38
☒ CNG detection
☐ FXS hoot line

FXS Flags:

Echo cancellation: enable/disable echo cancellation parameter.
Fax device: Enables fax for this interface. It is enabled using the enable check box (CW is disabled for the port)
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/disable FXS port as hoot line.

Subscriber Configuration:

Subscriber number: Subscriber directory number.
Subscriber name: This is the subscriber's name.
Registration interval timer: port DN registers every Registration Interval Timer seconds.
End Point Service Profile: allows the possibility to configure/apply dial restriction rules per FXS subscriber.
Digest authentication realm: 'realm' parameter sent in the header when challenging a request.
Digest authentication user ID: string that uniquely identifies a user within a given realm.
Digest authentication password: password to be used in the Digest Authentication.
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.

FXS port Configuration

FXS Port provisioning.

Hotline/Warmline Configuration

☐ Enable

Wait time (sec)

0

Destination

Number of times to repeat

0

Repeat interval (sec)

5

Location Information

Building

Floor

Room

Hotline/Warmline Configuration:

Enable: This checkbox is used to enable the Hotline or Warmline feature for an FXS port. Default setting is unchecked.

Wait time (sec): This field is used to enter a delay time in whole seconds. The default value is zero. When this field is set to zero, Hotline behavior is assumed. When this field is set to a non-zero value, Warmline behavior is assumed.

Destination: This field is used to store the Hotline or Warmline destination number. This field can contain up to 24 digits, using digits 0 – 9.

Number of times to repeat: This field indicates how many times to retry an external hotline/warmline destination in the event that it is busy.

Repeat interval (sec): 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.

Note that FXS Hotline/Warmline cannot be enabled if FXS Hoot Line is enabled, and vice versa.

Location Information: Each FXS port can be set with different value for Building, Floor & Room.

If any parameter is not set for a specific FXS port, general values shall be used. If a parameter is configured for a specific FXS port, this value will supersede the general value

62.2.3.1 End Point Service Profile For FXS Subscribers

It is possible to configure/apply dial restriction rules per FXS subscriber. Digit sequences configured in table shall be rejected.

The screenshot displays the 'FXS Configuration' window. Under the 'FXS Cards provisioning' section, the 'Endpoint Service Profile' tab is selected. A button labeled 'Endpoint service profile' is visible. An arrow points from this button to the 'Endpoint Service Profiles' window below.

The 'Endpoint Service Profiles' window shows a table with the following data:

Row	Name	Blocked call disconnection
1	International	Disconnect

A yellow callout box provides additional information:

- Profile Name:** Name of FXS profile.
- Note:** Up to 10 profiles can be created.
- Blocked Call Disconnection:** It indicates the way the blocked call shall be disconnected: with an announcement and disconnection after timeout or simply being disconnected.
- Note:** Disconnect is done before digit sequence is sent to OSV (Normal Mode) or before any SIP Manipulation or route analysis (Survivability Mode).

At the bottom of the window, there are three buttons: 'Add', 'Edit', and 'Delete'.

Endpoint Service Profile Configuration

Endpoint service profile configuration provisioning.

General

Name

Blocked call disconnection

Blocked Calls

Row	Denied number	Operational mode
1	000%	Survivable mode

Denied Number A regular expression that allows entering dial patterns which are not accepted for the endpoints associated to this endpoint service profile.

Note: Up to 20 rules can be created per Profile.

Operational Mode: It indicates if the rule is enabled for **Survivable** mode or for **Both** Normal and Survivable mode.

Add Delete

62.3 Emergency Numbers

FXS Configuration

FXS Cards provisioning.

Emergency Calling Numbers

Emergency numbers

Add

911

Delete

When a subscriber dials any number that is configured in this list, the OSB will identify an Emergency Call (e.g. in the USA the number is 911)

62.3.1 Location Information

Location Information	
Enable geo-location support	<input checked="" type="checkbox"/>
Country	United States
State or region or province	FL
County or parish or district	PALM BEACH
City	BOCA RATON
Street	BROKEN SOUND
Leading street direction	NW
Street type suffix	BLVD
Address number	5500
Postal code	33487
Postal community name	BOCA RATON
Building	A
Floor	2ND
Room	2.12

Flag "Enable geo-location support" must be set in order for OSB to add the location info (PIDF-LO) based on the values from Location Information section (NG911)

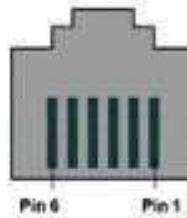
Country, State or region or province, County or parish or district, City and Street are mandatory fields

Country is selected from a drop down menu, max length for State or region or province is 3 chars and for all other fields the maximum length is 150 chars

OSB will add the location information, only when all of the following conditions are met : Normal mode, INVITE was initiated from a SIP subscriber, Geo-location support is set, call (R-URI) is recognized as an emergency call and TCP or TLS is used between the OSB and the OSV/OSS. Location information data will be included only for location unaware phones.

FXO/FXS port - RJ11 Telco Port Connector - pin assignment

Pin	Description
1	NotUsed
2	NotUsed
3	Tip
4	Ring
5	NotUsed
6	NotUsed



60.2 System Status

Connectivity and System state in relation to the SIP server (Checking if OSB is in SM or NM)

Configuration → OpenScope Branch → Branch Office → Configuration → Local Dashboard

Unify OpenScope Branch Management Portal

ATA71-Test-VLAN - V10R2.0.1

User name: administrator

Administration

- System
- Network/Net Services
- VoIP
- Features
- Security
- Diagnostics & logs
- Alarms
- Maintenance

General - ATA71-Test-VLAN

Branch aggregated information and data.

Alarms

Alarm summary: Critical: 0 Major: 0 Minor: 0 Show alarm details

System Status

Branch mode: Proxy ATA Auto refresh timer: 1 min

Operational state: Normal - Outbound Proxy Normal

Com Outbound Proxy

Outbound proxy: 21.21.0.81 Outbound proxy: Active

Com Node 1

Primary server: 80.253.239.150 Penalty box state: Reachable

Backup server: Penalty box state

Com Node 2

Primary server: Penalty box state

Backup server: Penalty box state

System Info

CPU: 4.81 %

Memory: 36.76 % - 2 Gb

Disk: 39.84 % - 8 Gb

System uptime: 17 days 44 min

Hardware type: Advantech 50i (ATA - 24)

Hostname: ATA71-Test-VLAN

Software Info

Software version: V10 R2.00.01

Software Partition information: Active Backup

- Green = ATA in NM and Outbound proxy in NM
- Orange = ATA in NM and Outbound proxy in SM
- Red = ATA in SM

Analog FXS Features Support Table

Analog FXS Features Supported						
Feature	OSB 50i NM	OSB 50i SM	OB 50i Comments	OSB Feature	OSV Feature	OSB PAC
Basic call	X	X				
Consultation & Transfer	X	X	OSB50i: As part of TWC, the user can hookflash then dial the C party, then talk to them (consultation), then go on-hook and transfer the call.	Y		
Call Transfer	X	X	OSB50i: In addition to consultation and transfer, the user can also go on-hook while the C-Party is ringing and that will also transfer the call.	Y		
Conference (limited to 3 parties = TWC)	X	X	OSB50i: Three Party Conference is provided by Asterisk	Y		
Toggle/Alternate			OSB50i: not supported due to 3-party conference feature			
Call Hold	X	X	OSB50i: While on a call, the user can hookflash and place the B-Party on hold. When ready to continue, the user presses hookflash again and is reconnected. No MOH is available.	Y		
Call Forward	X	X	OSB50i: Call Forwarding Unconditional only	Y		*72, *73
Call park	Partial		OSV: V4R1 and beyond OSB50i: Cannot park to server. Can retrieve parked calls.		Y	
Callback no reply	X		OSB50i: PAC necessary		Y	
Callback on busy	X		OSB50i: PAC necessary		Y	
Last Inc Num Redial	X		OSB50i: In SM, only if the device supports the capability		Y	
Last Out Num Redial	X		OSB50i: In SM, only if the device supports the capability		Y	
Call Pickup (group)	Partial		OSB50i: FXS can pickup the call by dialing CPG access code but does not get CPG indication (no NOTIFY) since it cannot subscribe.		Y	
Speed dial list	X		OSB50i: In SM, only if the device supports the capability		Y	
DND	X	X		Y		*78, *79
Call Return	X	X	OSB50i: Audible playback of last incoming number	Y		*69
Call Waiting	X	X		Y		
Disable Call Waiting for next call	X	X		Y		*70
Disable Caller ID for next call	X	X	OSB50i: This feature is provided by Asterisk	Y		*67
Caller ID	X	X		Y		
Caller ID with Call Waiting	X	X	OSB50i: Hookflash will toggle between existing call and CW call	Y **		
Note: One branch-wide flag turns on all hookflash-based features for all analog FXS subscribers in						
Note: The PACs that Asterisk uses are hard-coded, and may conflict with OSV-defined PACs. In						
** Note that this feature is causing some trouble and may need to be turned off.						

Note1: Music on Hold will be played when an FXS subscriber places a call on hold by hookflashing. The music that is played is not configurable, and the capability cannot be turned off. This capability applies to FXS ports on the ATA only. The FXS ports on the OSB 50i do not have this capability."

Note2: if power to the card is lost, an alarm will be generated. During the power loss, FXS ports will not be able to make or receive calls, but callers to the FXS ports will hear audible ringback tone since the ports are still registered.

Three-Way Calling: Go off-hook, establish a call, hookflash, hear stutter dial tone, dial the 3rd party, hookflash, now in conference. Subsequent hookflash will drop the 3rd party. If the 3rd party goes on-hook before the conference is established, original parties are left in conversation.

Call Hold: Go off-hook, establish a call, hookflash, hear stutter dial tone, hookflash again to retrieve.

Call Transfer: Go off-hook, establish a call, hookflash, hear stutter dial tone, dial the 3rd party, go on-hook, call is now transferred.

Call Waiting: Make or receive a call, receive a 2nd call and hear call waiting tone, hookflash to toggle to the waiting party, hookflash again to toggle back.

Disable Call Waiting for Next Call: *feature can be done in twoways.*

Go off-hook, dial *70 to activate, hear confirmation tone, dial the number of the person to reach (when call is established, Call Waiting will not be accepted during the call)

Go off-hook, establish a call, hookflash, hear stutter dial tone, dial *70 to activate, hear confirmation tone, hookflash again to retrieve (after this procedure, Call Waiting will not be accepted during the call)

Disable Caller ID for Next Outgoing Call: Go off-hook, dial *67 to activate, hear confirmation tone, dial the number of the person to reach.

Do Not Disturb: Go off-hook, hear dial tone, dial *78 to activate, or *79 to deactivate.

Call Forwarding Unconditional: Go off-hook, hear dial tone, dial *72 to activate, or *73 to deactivate. After dialing *72, dial the number to forward to.

Call Return: Go off-hook, hear dial tone, dial *69 to hear the number of the last caller. Only works if Caller ID was present.

End Dialing: '#' digit as the 2nd or later digit as dialing is complete

61 Multiple OSBs in a Branch

Goal is to provide the ability to share gateway resources and to increase the capacity of subscribers as members of the same branch.
Provides support for up to four (4) OSBs within a cluster.
Different OSB models can be grouped within the cluster.
Can interoperate with OSBs with External or Integrated Gateways.

61.1 Configuration in the OSV:

A strategic subscriber numbering plan should be devised for subscribers which will be registered for each OSB within the cluster for ease of provisioning as well as efficient routing (Prefix Codes, Destination Codes, etc).

Example:

Subscriber DNs for OSB1 > 561-555-1xxx

Subscriber DNs for OSB2 > 561-555-2xxx

Subscriber DNs for OSB3 > 561-555-3xxx

Each OSB to be configured in the cluster is created in the OSV via the “Add” button in “Branch Offices” as in all branch creation.

Each OSB to be part of a cluster is created in the OSV with its Representative Endpoint and shared Office Code.

The concept of the cluster from the OSB point of view is the “Peer OSB”; the concept of the cluster from the OSV point of view is that the OSBs are geographically collocated and share an Office Code as well as LAN connectivity.

For accessing trunks within the cluster, Destinations are created which contained a prioritized Route List pointing to the Endpoint destined for each corresponding OSB (OSV limits the reroute to 4 routes).

Calls are then distributed between the gateway trunks in the OSBs based on the configured routes for each OSB Destination.

If a route is unavailable, the prioritized list is used to select the next route to ensure the outbound call can find an available trunk via one of the OSBs in the cluster.

61.2 Configuration in the OSB:

All OSBs which compose the cluster are configured independently from each other via the Local GUI or via the Assistant.

Each OSB monitors the heartbeat to the OSV independently via SIP Options.

Calls between branches in different operation modes (Normal vs. Survivability mode) are not possible.

The OSBs must be geographically collocated in order to avoid long time of different operation modes; the OSBs within the cluster must also be configured with the same operational mode (Proxy, SBC- Proxy, Branch-SBC).

A maximum of 4 OSBs can be grouped in a cluster allowing the configuring of a maximum of 3 priority GW rules to Peer OSBs for the same Routing Prefix.

To access trunks associated with the same OSB, a Priority 1 route is created in the Gateways/Trunks table with Gateway/Trunk Type set to “RG”, “Integrated Gateway”, etc. for its own associated gateway.

To access trunks associated with different Peer OSBs, additional priority routes (2,3,4) are created in the Gateways/Trunks table pointing to the other Peer OSBs for the same Routing Prefix (max 3).

Routes to subscribers registered in other OSB boxes are configured via a route pointing to each OSB box in the Gateways/Trunks table as Peer OSB with the configured Routing Prefix required to access those subscribers.

Peer OSB links are handled in the LAN side.

The OSV handles all call routing decisions while the OSBs are in Normal Mode. Routing to OSB registered subscribers or to OSB gateway trunks within the cluster while the OSBs are in Normal Mode is based upon the Prefix Codes, Destination Codes, Destinations, and configured Routes which determine how trunks are accessed.

The graphic on the next slide shows how the Gateways/Trunks Table is configured for a typical OSB within a cluster.

The first focus will be on how the Gateways/Trunks Table in the OSBs are provisioned to allow all subscribers within the clustered OSBs to communicate with each other.

Row	IP Address or FQDN	Port	Interface	Transport	Routing prefix/FQDN	Gateway/Trunk type	Functional type	Trunk Profile	Output digit strip	Output digit add	Priority
1	pri1.jgosh208.siemens.com	5096	LAN	UDP	911999	Integrated Gateway	Emergency	Gateway	0		
2	10.234.1.209	5060	LAN	TCP	32%	Peer OSB	Survivability Mode Egress/Ingress	Gateway	0		1
3	10.234.1.210	5060	LAN	TCP	4249231%	Peer OSB	Survivability Mode Egress/Ingress	Gateway	0		1
4	10.234.1.209	5060	LAN	TCP	4249232%	Peer OSB	Survivability Mode Egress/Ingress	Gateway	0		1
5	10.234.1.209	5060	LAN	TCP	9305%	Peer OSB	Survivability Mode Egress/Ingress	Gateway	1	8	3
6	10.234.1.210	5060	LAN	TCP	9305%	Peer OSB	Survivability Mode Egress/Ingress	Gateway	1	7	2
7	pri1.jgosh208.siemens.com	5096	LAN	UDP	9305%	Integrated Gateway	All Modes Egress/Ingress	Gateway	1		1

Example:

- OSB1 DN Range for Subscribers: 424-923-0XXX
- OSB2 DN Range for Subscribers: 424-923-1XXX
- OSB3 DN Range for Subscribers: 424-923-2XXX

The above is a screenshot of OSB1's Gateway/Trunks Table.

Row	IP Address or FQDN	Port	Interface	Transport	Routing prefix/FQDN	Gateway/Trunk type	Functional type	Trunk Profile	Output digit strip	Output digit add	Priority
1	pri1.jgosh208.siemens.com	5096	LAN	UDP	911999	Integrated Gateway	Emergency	Gateway	0		
2	10.234.1.209	5060	LAN	TCP	32%	Peer OSB	Survivability Mode Egress/Ingress	Gateway	0		1
3	10.234.1.210	5060	LAN	TCP	4249231%	Peer OSB	Survivability Mode Egress/Ingress	Gateway	0		1
4	10.234.1.209	5060	LAN	TCP	4249232%	Peer OSB	Survivability Mode Egress/Ingress	Gateway	0		1
5	10.234.1.209	5060	LAN	TCP	9305%	Peer OSB	Survivability Mode Egress/Ingress	Gateway	1	8	3
6	10.234.1.210	5060	LAN	TCP	9305%	Peer OSB	Survivability Mode Egress/Ingress	Gateway	1	7	2
7	pri1.jgosh208.siemens.com	5096	LAN	UDP	9305%	Integrated Gateway	All Modes Egress/Ingress	Gateway	1		1

On this OSB1, while in Survivability Mode, any calls initiated from its own registered subs (424-923-0XXX) destined for subscribers registered to OSB2 will use the Routing Prefix of 4249231% and send the calls via its Peer OSB route to OSB2 at 10.234.1.210.

Any calls initiated from its own registered subscribers (424-923-0XXX) destined for subscribers registered to OSB3 will use the Routing Prefix of 4249232% and send the calls via its Peer OSB route to OSB3 at 10.234.1.209.

All OSB subscribers can communicate amongst the clustered OSBs while in Survivability Mode via the Peer OSB concept by establishing Routing Prefixes pointing to the destined Peer OSBs.

Row	IP Address or FQDN	Port	Interface	Transport	Routing prefix/FQDN	Gateway/Trunk type	Functional type	Trunk Profile	Output digit strip	Output digit add	Priority
1	pri1.jgosh208.siemens.com	5096	LAN	UDP	911999	Integrated Gateway	Emergency	Gateway	0		
2	10.234.1.209	5060	LAN	TCP	32%	Peer OSB	Survivability Mode Egress/Ingress	Gateway	0		1
3	10.234.1.210	5060	LAN	TCP	4249231%	Peer OSB	Survivability Mode Egress/Ingress	Gateway	0		1
4	10.234.1.209	5060	LAN	TCP	4249232%	Peer OSB	Survivability Mode Egress/Ingress	Gateway	0		1
5	10.234.1.209	5060	LAN	TCP	9305%	Peer OSB	Survivability Mode Egress/Ingress	Gateway	1	8	3
6	10.234.1.210	5060	LAN	TCP	9305%	Peer OSB	Survivability Mode Egress/Ingress	Gateway	1	7	2
7	pri1.jgosh208.siemens.com	5096	LAN	UDP	9305%	Integrated Gateway	All Modes Egress/Ingress	Gateway	1		1

This slide represents how the Gateways/Trunks Table in the OSBs are provisioned for trunk access within the clustered OSBs.

The graphic above provides an example where a subscriber for this OSB must dial the prefix 9 to access and outside trunk and send the call to a destined gateway (Routing Prefix is 9305%).

As stated previously, the OSV handles all call routing decisions involving trunk access while the OSBs are in Normal Mode. Peer OSB's will have the Functional Type set to "Survivability Mode Egress / Ingress" for OSB routing to the peers during Survivability Mode.

OpenScape Branch Management: Portal												Gateways/Trunks												OpenScape Branch Management: Portal												Gateways/Trunks												Emergency calling subnets											
Gateways/Trunks																																																											
Gateways/Trunks provisioning.																																																											
Row		IP Address or FQDN		Port	Interface	Transport	Routing prefix/FQDN		Gateway/Trunk type		Functional type		Trunk Profile		Output digit strip		Output digit add		Priority																																								
1		pri1.jgosh208.siemens.com		5096	LAN	UDP	911999		Integrated Gateway		Emergency		Gateway		0																																												
2		10.234.1.209		5060	LAN	TCP	32%		Peer OSB		Survivability Mode Egress/Ingress		Gateway		0				1																																								
3		10.234.1.210		5060	LAN	TCP	4249231%		Peer OSB		Survivability Mode Egress/Ingress		Gateway		0				1																																								
4		10.234.1.209		5060	LAN	TCP	4249232%		Peer OSB		Survivability Mode Egress/Ingress		Gateway		0				1																																								
5		10.234.1.209		5060	LAN	TCP	9305%		Peer OSB		Survivability Mode Egress/Ingress		Gateway		1		8		3																																								
6		10.234.1.210		5060	LAN	TCP	9305%		Peer OSB		Survivability Mode Egress/Ingress		Gateway		1		7		2																																								
7		pri1.jgosh208.siemens.com		5096	LAN	UDP	9305%		Integrated Gateway		All Modes Egress/Ingress		Gateway		1				1																																								

The focus now is on Survivability Mode. Priority 1 is assigned to its own Integrated Gateway for the Routing Prefix 9305%. Calls made outbound to the PSTN where the dialed string is 9305. send the call out via its Integrated Gateway, but first strip off the 9 sending

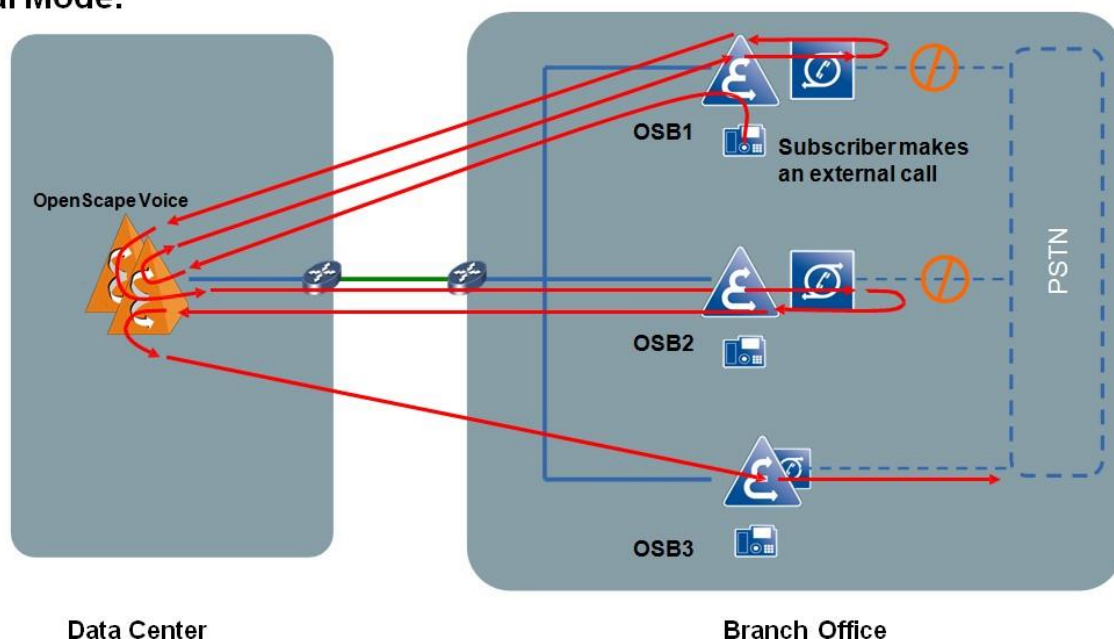
10 digits. This could also have been provisioned to send the 9 as 11 digits and then let the gateway handle the routing based on receiving all 11 digits.

If OSB1's Integrated Gateway has no available trunks (returns an error code, etc), OSB1 then sends this call over to its assigned Priority 2 Peer OSB2 via IP 10.234.1.210. OSB2 then completes routing the call to its assigned gateway via one of its available trunks. If the Peer OSB2 also has no available trunks, it will return an error code back to OSB1 to allow the originating OSB1 to then send this call over to its assigned Priority 3 Peer OSB3 via IP 10.234.1.209. This OSB3 then completes routing the call to its assigned gateway via one of its available trunks.

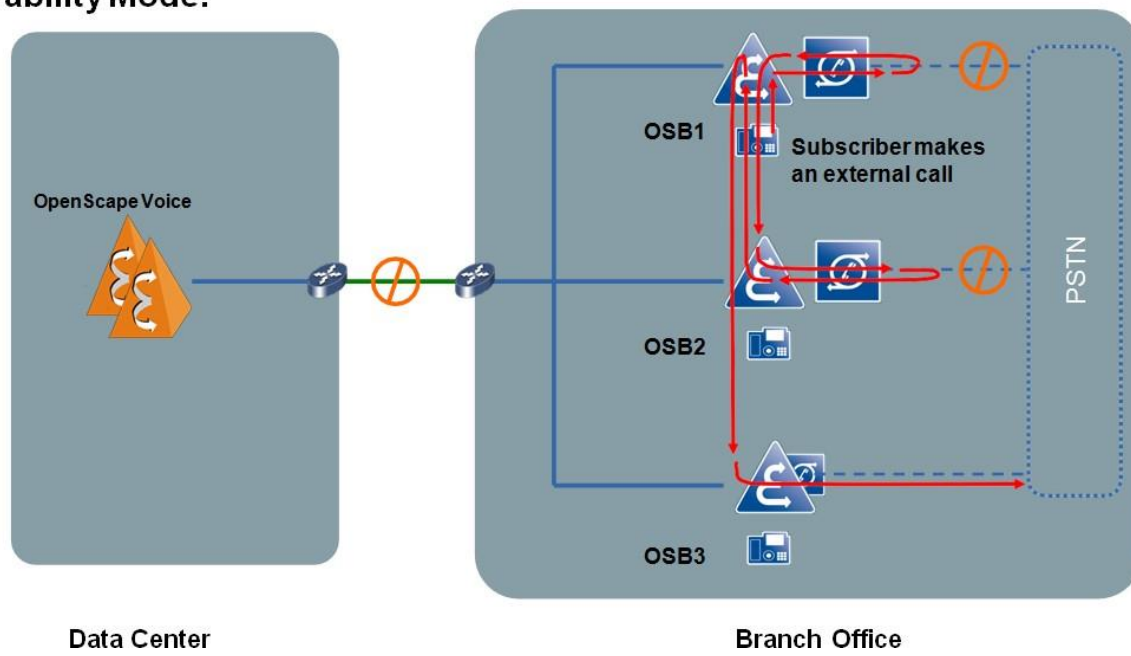
It is also necessary to Enable Routing for all desired Error Codes in the Error Codes Table for Survivable Mode. This is required in order to traverse the Peer OSB Priority Rankings when trunks are unavailable and the Peer OSBs return error responses for such events.

In Survivability Mode, the concept is that the originating OSB makes all the routing decisions for trunk access based on its Priority rankings, and use of the Peer OSBs simply complete the calls if they have available trunks. If the Peer OSBs have no available trunks, then they return error codes back to the originating OSB who then uses its own configured Priorities to control trunk access

Normal Mode:



Survivability Mode:



Additional Notes:

Only one Area Code/Office Code is supported per cluster.

MLHGs members can be registered on different OSBs. MLHGs must be configured on each peer OSB.

All phones which have instances of a keyset subscriber must be registered on the same OSB.

Media Server - in Normal Mode it is possible to share the integrated media servers located in different OSB boxes (Branch Media Server concept); in Survivability Mode each call is attended by the Media Server located in the OSB which originated the call.

62 Simplified Installation

There are two types of installation procedures: “Simplified Installation” and “Basic Installation” (See “Full Installation” section of this document). Simplified Installation provides four options: Option 1 (LAN MAC Address), Option 2 (Local Logical ID), Option 3 (Local CMP URL), and Option 4 (Local xml Config File).

62.1 Common Management Portal and OSB Assistant configuration:

To install an OpenScape Branch device using the “Simplified Installation” procedure, it is required that the administrator pre- configures the OSB Assistant prior to starting the installation.

1. Load the OpenScape Branch Software into CMP:

The OpenScape Branch software must be loaded into the Repository area of CMP.

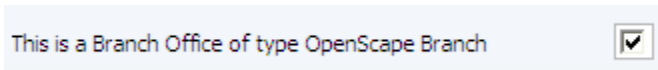
- a) In CMP under Maintenance go to Inventory
- b) Go to Repository and press Add
- c) Select and add the OpenScape Branch SPA and image files Press Save after the files are transferred

The OpenScape Branch software is now available in the CMP Repository

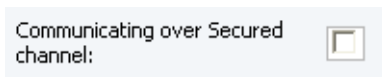
2. Configure the OpenScape Branch Office for Installation

Under the OpenScape Voice configuration create the Endpoint and create the Branch office:

- a) For this newly created Branch Office set the flag:



- b) Under the OpenScape Branch configuration select the Branch Office just created and click “Edit”. Make sure the “Communicating over Secured channel” flag is unchecked:



NOTE: This flag must always be unchecked to perform a Simplified Installation of the OSB. During the installation process a security process takes place between OSB and CMP and the “Security Status” is automatically changed to “Secured”

- c) In the General Tab click on “Configure Installation”.

d) Enter the following information:

Installation info

Enter OpenScape Branch Appliance installation information and select the software version to install.

General

Software load: V2R0.01.12

Hardware type: Advantech

MAC address: 00:0A:0B:25:3E:2F

Select Software version to install from the pull down menu

Advantech:	OSB 250
Advantech 501:	OSB with integrated Gateway
Advantech 250:	OSB without integrated gateway card
KAZ00:	OSB with integrated gateway card
KAZ00:	OSB without integrated gateway card
KAZ00:	Fujitsu KAZ00
KAZ00:	Fujitsu KAZ00
D945:	Acrosser - OSB 50

MAC Address of the LAN interface. For Branch SBC configuration the LAN HW ID must be configured as well.
 ** MANDATORY: For Zero Touch Installation
 ** LEAVE BLANK: For all other options

Make sure the "Installation" flag is set (checked):

Installation: ☒

- e) Proceed to the next section to upload the desired files during installation.
- f) After all the desired files have been uploaded press Ok.

Configuration is complete and automated installation could be started.

NOTE: The Logical ID folder used for the next steps will be automatically created in the CMP server after the steps described in the above procedure. The Logical ID is created as:

<OSV Name>:<BG Name>:<Branch Office Name>

Installation progress could be followed in OSB Assistant

Branch Office	IP Address	Comm System	Business Group	Version	Status	Mode	Last Update	Security status
bocaOB_20_FujRX330	10.234.1.20	Node105VV6	BGCA	---	Unreachable	---	2011/11/03 03:33:35	Unsecured Mode

Load the OpenScape Branch Files into CMP

During automated installation certain files are transferred and installed automatically in the OpenScape Branch device. Some of these files are mandatory and must be loaded into the CMP.

Required files

The configuration (XML) file is required. It must contain the IP address and the correct hardware type of the OSB device. The file must be transferred via GUI:

Goto Configuration ➤ OpenScape Branch ➤ Select Branch Office ➤

Click on Configure Installation and goto the "Data Configuration File"

tab.

Locate the configuration file and press the Add button The file will be uploaded to CMP into the following directory:

Offboard CMP: /opt/siemens/openbranch/ob_config/<Logical_ID>/Configuration_data/

Integrated CMP: /enterprise/openbranch/ob_config/<Logical_ID>/Configuration_data/

Optional files

The following files are optional and if desired when available they will automatically be installed in the OpenScape Branch device

Media server

Files must be transferred via GUI

The files must be uploaded to CMP into the following directory: (e.g. WinSCP)

Offboard CMP: /opt/siemens/openbranch/ob_config/ms_languages/ or

Integrated CMP: /enterprise/openbranch/ob_config/ms_languages/

Then a language must be selected via GUI Configuration --> OpenScape Branch --> Select Branch Office -->

Edit --> Configure Installation --> Media Server

Language Files --> Add

NOTE: OSB1000 and OSB6000 support up to 5 languages. All other OSB platforms support up to 2 languages. For an off-board CMP a maximum of 10 languages can be uploaded. For integrated CMP a maximum of 3. Total allowable size for media server languages is 150MB

64.1.1.1 ACD announcement

These are divided into two types: ACD announcement files and ACD music on Hold files. The files must be transferred via GUI

Configuration ➤ OpenScape Branch ➤ Select Branch Office ➤ Edit ➤ Configure Installation ➤ ACD Announcements ➤ ACD Music on Hold Files ➤ Add

The files will be uploaded to CMP into the following directory:

Offboard CMP: /opt/siemens/openbranch/ob_config/<Logical_ID>/ACD_Announcements/

Integrated CMP: /enterprise/openbranch/ob_config/<Logical_ID>/ACD_Announcements/

NOTE: The total size of ACD announcements and ACD music on hold combined cannot exceed 100MB.

64.1.1.2 Auto Attendant:

Files must be transferred via GUI

Configuration ➤ OpenScape Branch ➤ Select Branch Office ➤ Edit ➤ Configure Installation ➤ Auto Attendant Announcement Files ➤ Add

The files will be uploaded to CMP into the following directory:

Offboard CMP:

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

Integrated CMP:

/enterprise/openbranch/ob_config/<Logical_ID>/AutoAttendant_Announcements/

NOTE: The total allowable size for AA Announcements is 100MB.

NOTE: For Integrated systems a packet filter to allow communication to port 444 should be created. This is the port used to transfer the files during simplified installation.

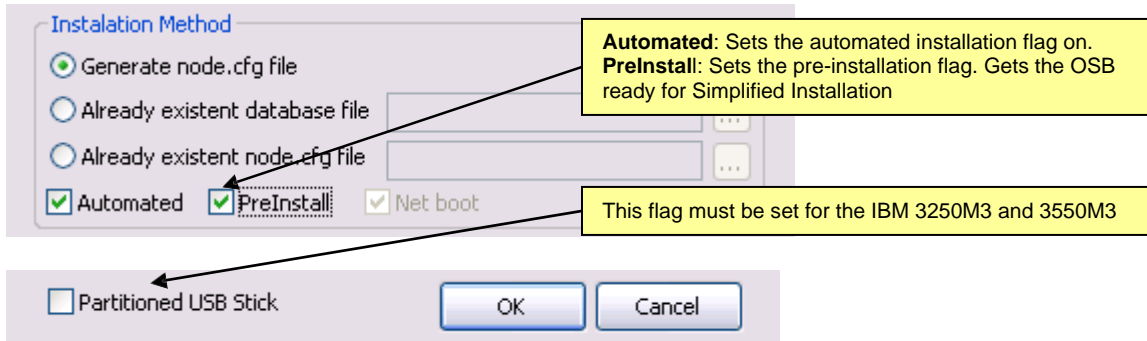
62.2 Option 1 - Zero Touch Installation

For this installation procedure it is a pre-requirement that the OpenScape Branch device is pre-loaded with the pre-staging software.

Pre-staging (for Staging Center)

The following procedure is for the pre-installation step to be done in the OSB boxes by manufacturing or the staging center prior to sending the box to the customer site for installation.

Using a Windows based PC create the USB stick with the following options enabled:



Once the USB stick is created plug it into a USB stick port in the OpenScape Branch. Please refer to the Software Installation section for BIOS settings if required. First boot up option must be the USB port.

Power up the OpenScape Branch and the image from the USB stick will automatically be installed in the device. When the installation is complete, the device will alert the user by providing one audible beep for 10 cycles.

Power off the OpenScape Branch and remove the USB stick. Device is ready for delivery

DHCP Configuration

It is a pre-requirement that the DHCP server is configured to provide the CMP IP with Option 43.

The OpenScape device will broadcast a DHCP Discover message with: Option 60: Vendor class identifier = "OpenScapeBranch"

The DHCP server must be configured to provide:

A temporary IP address

Network information (i.e. default route, DNS, domain..etc)

When receiving the specified Options 60 it should provide Option 43 vendor specific information

Type = 01 only

IP address or FQDN of the Software Supply Server (CMP)

If multiple IP addresses are used they must be separated by a comma ",". (Only two IP addresses for CMP are supported)

For more information about configuring the DHCP for the OSB's phones, please refer to the DHCP Configuration section in the OpenScape Branch Configuration Guide or in the OpenScape Branch V2 Administrator and Installation documents.

64.2.1 Zero Touch Installation Steps


NOTE: CMP and OSB Assistant must be configured to proceed with installation. Also all the necessary files must also exists in CMP.

64.2.1.1 Connect the OpenScape Branch device LAN interface to the network.

Note: For Branch-SBC scenarios where the link to CMP is via the WAN interface, this interface (WAN) must be connected to the network. The LAN MAC ID is still needed in the installation configuration in CMP for validation purposes.


64.2.1.2 Power the OpenScape Branch device up

The OpenScape Branch device will receive via DHCP a temporary IP address as well as the CMP information and it will automatically download and install the software image, configuration file and announcement files if necessary.

Branch Office	IP Address	Comm System	Business Group	Version	Status	Mode	Last Update	Security status
 bocaOB_20_FujRX330	10.234.1.20	Node1OSVW6	BGCA	---	Installation started	---	2011/11/03 03:56:32	Secured Mode

Status indicates installation progress and mode is set to Secured

When the installation is finished the device will alert providing 10 audible beeps (single beep followed by a pause and the cycle is repeated 10 times)

Branch Office	IP Address	Comm System	Business Group	Version	Status	Mode	Last Update	Security status
 bocaOB_20_FujRX330	10.234.1.20	Node1OSVW6	BGCA	V2R0.06.00 Build 1	Normal	Proxy	2011/11/03 03:16:52	Secured Mode

Status indicates installation progress and mode is set to Secured

Note: The simplified installation does not cover any pre configuration like, but not limited to, certificates, logos, DNS Zones files or Customer MOH.

These services shall be configured after the installation procedure.

64.3 Option 2 – Simplified Installation Using Logical ID and DHCP Option 43

This installation procedure requires a DHCP server configured to provide CMP information via Option 43

64.3.1 USB Stick preparation

The USB Stick must be created with the following options:

Media Select

E:\ (1.86 GB) Refresh

WARNING: all partitions of Removable Medias will be deleted and a single FAT32 partition will be created. Therefore, all data of the removable media will be erased.

Installation Method

☒ Generate node.cfg file

☐ Already existent database file

☐ Already existent node.cfg file

☒ Automated ☐ PreInstall ☒ Net boot ☒ DHCP

Logical ID: Node105VV6:BGCA:nodeOB50i_21_PRI

☐ Partitioned USB Stick

OK Cancel

Automated: Sets the automated installation flag on

DHCP: Flag must be set

Enter correct Logical ID (must be exact)

This flag must be set for the IBM 3250M3 and 3550M3

When the USB is created, remove it and plug it into a USB port in the OSB Server.

64.3.2 DHCP Configuration

It is a pre-requirement that the DHCP server is configured to provide the CMP IP with Option 43.

The OpenScape device will broadcast a DHCP Discover message with: Option 60: Vendor class identifier = "OpenScapeBranch"

The DHCP server must be configured to provide:

A temporary IP address

Network information (i.e. default route, DNS, domain..etc)

When receiving the specified Options 60 it should provide Option 43 vendor specific information

Type = 01 only

IP address or FQDN of the Software Supply Server (CMP)

If multiple IP addresses are used they must be separated by a comma ",". (Only two IP addresses for CMP are supported)

For more information about configuring the DHCP Server please refer to the DHCP Configuration section in the OpenScape Branch Configuration Guide or in the OpenScape Branch V2 Administrator and Installation documents.

64.3.3 Option 2 Installation Steps

NOTE: CMP and OSB Assistant must be configured to proceed with installation. Also all the necessary files must also exists in CMP.

Connect the USB stick previously created to a USB port in the OpenScape Branch server.

Connect the OpenScape Branch device LAN interface to the network.

Note: For Branch-SBC scenarios where the link to CMP is via the WAN interface, this interface (WAN) must be connected to the network. The LAN MAC ID is still needed in the installation configuration in CMP for validation purposes.

Power the OpenScape Branch device up

The OpenScape Branch device will boot up off of the USB stick and receive via DHCP a temporary IP address as well as the CMP information and it will automatically download and install the software image, configuration file and announcement files if necessary.

OSB Assistant will show the installation progress in the Status column.

Branch Office	IP Address	Comm System	Business Group	Version	Status	Mode	Last Update	Security status
 bocaOB_20_FujRX330	10.234.1.20	Node1OSVV6	BGCA	---	Installation started	---	2011/11/03 03:56:32	Secured Mode

Status indicates installation progress and mode is set to Secured

When the installation is finished the device will alert providing 10 audible beeps (single beep followed by a pause and the cycle is repeated 10 times).

Branch Office	IP Address	Comm System	Business Group	Version	Status	Mode	Last Update	Security status
 bocaOB_20_FujRX330	10.234.1.20	Node1OSVV6	BGCA	---	Reboot is required	---	2011/11/03 03:25:27	Secured Mode

Status indicates installation finish and a restart is required

When the installation finishes remove the USB Stick. This will automatically restart the server. After the restart the server will be online and the status in OSB Assistant will be updated.

Branch Office	IP Address	Comm System	Business Group	Version	Status	Mode	Last Update	Security status
 bocaOB_20_FujRX330	10.234.1.20	Node1OSVV6	BGCA	V2R0.06.00 Build 1	Normal	Proxy	2011/11/03 03:16:52	Secured Mode

Status is updated to show OSB Operational Mode

64.4 Option 3 – Simplified Installation Using Logical ID with DHCP not providing Option 43

This installation procedure requires a DHCP server configured to provide only an IP address and no Option 43

64.4.1 USB Stick preparation

The USB Stick must be created with the following options:

The screenshot shows the 'Installation Method' and 'OpenScape Branch Network Configuration' sections of a dialog box. The 'Installation Method' section has three radio buttons: 'Generate node.cfg file' (selected), 'Already existent database file', and 'Already existent node.cfg file'. Below these are checkboxes for 'Automated' (checked), 'PreInstall', and 'Net boot'. The 'OpenScape Branch Network Configuration' section has a checkbox for 'DHCP' (checked). Below this are fields for 'Logical ID', 'CMP URL 1', 'CMP URL 2', 'DNS 1', and 'DNS 2'. At the bottom is a checkbox for 'Partitioned USB Stick' and 'OK'/'Cancel' buttons. Annotations point to specific fields with yellow boxes containing text:

- 'Automated': Sets the automated installation flag on (points to the 'Automated' checkbox)
- 'DHCP: Flag must be set' (points to the 'DHCP' checkbox)
- 'Enter correct Logical ID (must be exact)' (points to the 'Logical ID' field)
- 'Enter the CMP IP addresses where the OpenScape Branch is going to retrieve the installation files from. Enter DNS information if not provided by DHCP' (points to the 'CMP URL 1' and 'CMP URL 2' fields)
- 'This flag must be set for the IBM 3250M3 and 3550M3' (points to the 'Partitioned USB Stick' checkbox)

When the USB is created, remove it and plug it into a USB port in the OSB Server

64.4.2 DHCP Configuration

It is a pre-requirement that the DHCP server is configured to provide only basic networking information:

- Temporary IP address, Subnet Mask, Default Gateway, DNS IP. No

Option 43 is configured in this scenario.

64.4.3 Option 3 Installation Steps

NOTE: CMP and OSB Assistant must be configured to proceed with installation. Also all the necessary files must also exist in CMP.

Connect the USB stick previously created to a USB port in the OpenScape Branch server.

Connect the OpenScape Branch device LAN interface to the network.

Note: For Branch-SBC scenarios where the link to CMP is via the WAN interface, this interface (WAN) must be connected to the network. The LAN MAC ID is still needed in the installation configuration in CMP for validation

purposes.

Power the OpenScape Branch device up

The OpenScape Branch device will boot up off of the USB stick and receive via DHCP a temporary IP address. It will get the CMP information from the USB Stick and it will automatically download and install the software image, configuration file and announcement files if necessary.

OSB Assistant will show the installation progress in the Status column.

Branch Office	IP Address	Comm System	Business Group	Version	Status	Mode	Last Update	Security status
 bocaOB_20_FujRX330	10.234.1.20	Node1OSVV6	BGCA	---	Installation started	---	2011/11/03 03:56:32	Secured Mode

Status indicates installation progress and mode is set to Secured

When the installation is finished the device will alert providing 10 audible beeps (single beep followed by a pause and the cycle is repeated 10 times).

Branch Office	IP Address	Comm System	Business Group	Version	Status	Mode	Last Update	Security status
 bocaOB_20_FujRX330	10.234.1.20	Node1OSVV6	BGCA	---	Reboot is required	---	2011/11/03 03:25:27	Secured Mode

Status indicates installation finish and a restart is required

When the installation finishes remove the USB Stick. This will automatically restart the server. After the restart the server will be online and the status in OSB Assistant will be updated.

Branch Office	IP Address	Comm System	Business Group	Version	Status	Mode	Last Update	Security status
 bocaOB_20_FujRX330	10.234.1.20	Node1OSVV6	BGCA	V2R0.06.00 Build 1	Normal	Proxy	2011/11/03 03:16:52	Secured Mode

Status is updated to show OSB Operational Mode

64.5 Option 4 – Simplified Installation Using Existing Configuration File

This installation procedure requires the USB Stick to be created with an existing database

64.5.1 USB Stick preparation

Create the USB Stick following these steps:

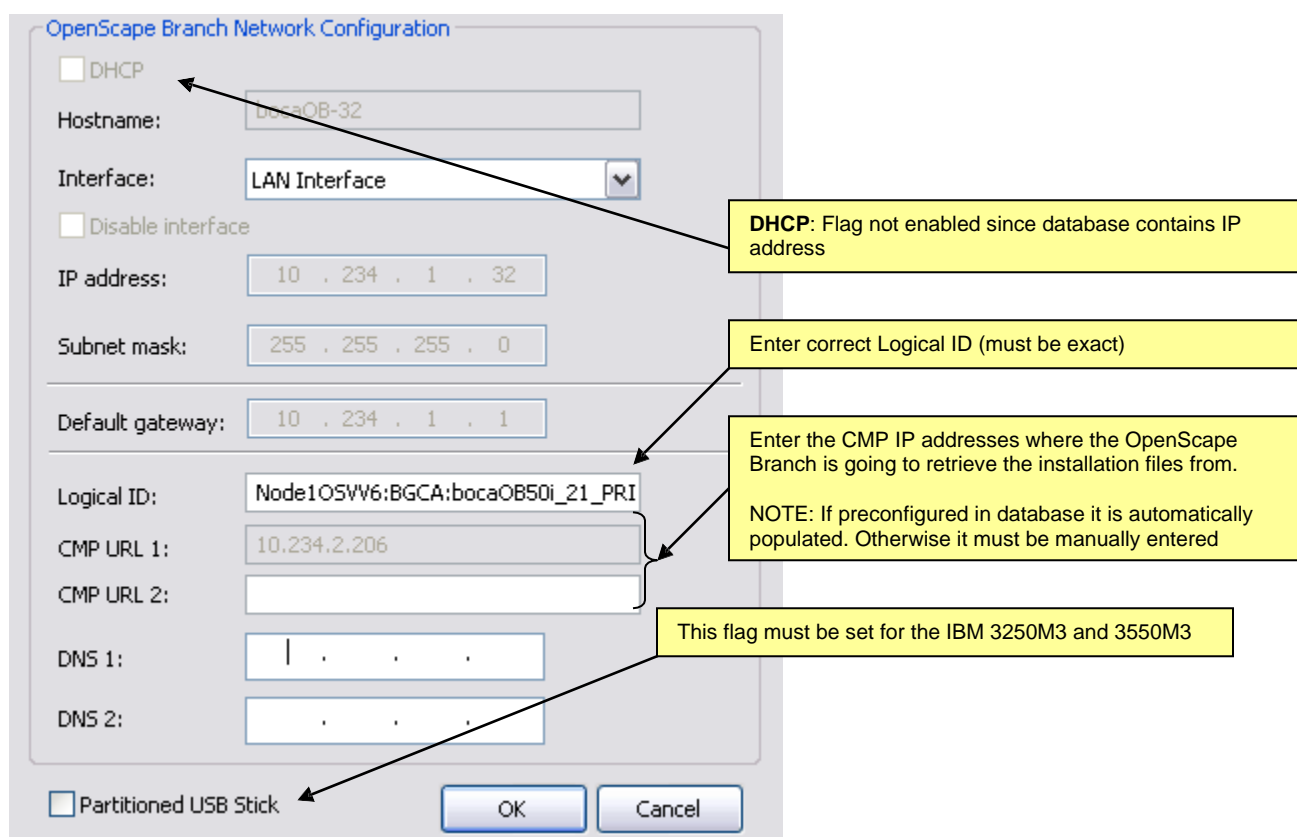
a) **Select the database by clicking on “Already existent database file”:**



b) **Enable the “Automated” and “Net boot” flags:**



c) **Enter the required configuration as shown below:**



The screenshot shows the 'OpenScape Branch Network Configuration' dialog box. The 'DHCP' checkbox is unchecked. The 'Hostname' field contains 'bocaOB-32'. The 'Interface' dropdown is set to 'LAN Interface'. The 'Disable interface' checkbox is unchecked. The 'IP address' field contains '10 . 234 . 1 . 32'. The 'Subnet mask' field contains '255 . 255 . 255 . 0'. The 'Default gateway' field contains '10 . 234 . 1 . 1'. The 'Logical ID' field contains 'Node105VV6:BGCA:bocaOB50i_21_PRI'. The 'CMP URL 1' field contains '10.234.2.206'. The 'CMP URL 2' field is empty. The 'DNS 1' and 'DNS 2' fields are empty. The 'Partitioned USB Stick' checkbox is unchecked. The 'OK' and 'Cancel' buttons are at the bottom right.

Annotations:

- DHCP:** Flag not enabled since database contains IP address
- Enter correct Logical ID (must be exact)
- Enter the CMP IP addresses where the OpenScape Branch is going to retrieve the installation files from.
NOTE: If preconfigured in database it is automatically populated. Otherwise it must be manually entered
- This flag must be set for the IBM 3250M3 and 3550M3

64.5.2 DHCP Configuration

DHCP is not required to perform a Simplified installation using this procedure

64.5.3 Option 4 Installation Steps

NOTE: CMP and OSB Assistant must be configured to proceed with installation. Also all the necessary files must also exists in CMP.

Connect the USB stick previously created to a USB port in the OpenScape Branch server.


Connect the OpenScape Branch device LAN interface to the network.

Note: For Branch-SBC scenarios where the link to CMP is via the WAN interface, this interface (WAN) must be connected to the network. The LAN MAC ID is still needed in the installation configuration in CMP for validation purposes.

Power the OpenScape Branch device up

The OpenScape Branch device will boot up off of the USB stick with the defined IP address. It will get the CMP information from the USB Stick and it will automatically download and install the software image, configuration file and announcement files if necessary.

OSB Assistant will show the installation progress in the Status column.

Branch Office	IP Address	Comm System	Business Group	Version	Status	Mode	Last Update	Security status
 bocaOB_20_FujRX330	10.234.1.20	Node10SVV6	BGCA	---	Installation started	---	2011/11/03 03:56:32	Secured Mode

Status indicates installation progress and mode is set to Secured

When the installation is finished the device will alert providing 10 audible beeps (single beep followed by a pause and the cycle is repeated 10 times).

Branch Office	IP Address	Comm System	Business Group	Version	Status	Mode	Last Update	Security status
 bocaOB_20_FujRX330	10.234.1.20	Node10SVV6	BGCA	---	Reboot is required	---	2011/11/03 03:25:27	Secured Mode

Status indicates installation finish and a restart is required

When the installation finishes remove the USB Stick. This will automatically restart the server. After the restart the server will be online and the status in OSB Assistant will be updated.

Branch Office	IP Address	Comm System	Business Group	Version	Status	Mode	Last Update	Security status
 bocaOB_20_FujRX330	10.234.1.20	Node10SVV6	BGCA	V2R0.06.00 Build 1	Normal	Proxy	2011/11/03 03:16:52	Secured Mode

Status is updated to show OSB Operational Mode

64.6 Option 5 – Secured Simplified Installation Using VPN

This installation follows the same procedure the used on the Option 3, although Option 4 is also possible.

Option 5 is required when Simplified Installation must proceeds through a secured path, for a hosted OpenScape Branch using a secured management network.

NOTE: This installation option makes a configuration with OSB in Branch SBC Mode only. So, interface WAN must be connected to the network. After first boot, CMP could send xml files with any other operational mode.

64.6.1 USB Stick preparation

The USB Stick must be created with the following options:

USB Stick Setup

Media Select

F:\ (3.73 GB) Refresh

WARNING: all partitions of Removable Medias will be deleted and a single FAT32 partition will be created. Therefore, all data of the removable media will be erased.

Installation Method

☒ Generate node.cfg file
☐ Already existent database file
☐ Already existent node.cfg file

☒ Automated ☐ PreInstall ☒ Net boot ☒ DHCP VPN

Automated: Sets the automated installation flag on

DHCP: Flag could be set if there is a DHCP on the WAN side

VPN: Sets the VPN (IPSec) configuration

Logical ID: Node105VV7:BGCA:bocaOB50i_21_PR

CMP URL 1: 10.234.2.206

CMP URL 2: 10.234.3.35

DNS 1: . . .

DNS 2: . . .

☐ Partitioned USB Stick

OK Cancel

Enter correct Logical ID (must be exact)

Enter the CMP IP addresses where the OpenScape Branch is going to retrieve the installation files from. Enter DNS information if not provided by DHCP

This flag must be set for the IBM 3250M3 and 3550M3

The Boot VPN Settings must be configured too. These VPN options will be used only for the boot. After boot, CMP will provide the complete configuration.

Click on VPN button and check the configuration as below:

Boot VPN Settings

IPsec

Disable

Enable

Files

Browse...

CA

C:\custom_CA.pem

X.509

C:\custom_cert.pem

Key

C:\custom_key.pem

Network Settings

Partner IP

10.10.10.1

Partner Network

192.168.80.0

Partner Network Mask Bits

24

OK

Cancel

Enable IPsec

Select Browse to upload customized certificates.

Customized certificates can be selected here.

Partner IP: Enter the IP address of VPN Concentrator on the WAN. Note: This address must be routed to the Partner Network by the routers on the internal network.

Partner Network: Enter Boot VPN network, i.e. network of CMP.

Partner Network Masks Bits: Enter the number of bits of network mask (e.g. 24 for 255.255.255.0).

NOTE: All customer certificates could be imported here. For example, it is possible to have one certificate for the Boot VPN and other for the hosted OSB secured management. All imported certificates are kept after installation.

NOTE: To establish VPN IPsec tunnel, only authentication RSA with customized certificates is possible. The authentication type PSK (pre-shared key) is not available.

When the USB is created, remove it and plug it into a USB port in the OSB Server

64.6.2 DHCP Configuration

It is possible to use the DHCP server configured to provide only basic networking information:
- Temporary IP address, Subnet Mask, Default Gateway, DNS IP. No

Option 43 is configured in this scenario.

NOTE: It is required that DHCP Server is installed on the WAN side. No other DHCP Server should be available on the LAN side. But DHCP Server is just an option. If there is no server available, manual settings are required via NetBoot or existing xml file could be selected (like Option 4) for temporary IP address of LAN and WAN, Subnet Mask, Default Gateway and DNS IP.

339

OpenScape Branch V10 Configuration Guide

64.6.3 Option 5 Installation Steps

NOTE: CMP and OSB Assistant must be configured to proceed with installation. Also all the necessary files must also exists in CMP.

NOTE: Data Center must have a VPN concentrator previously configured to establish the VPN connection with OSB for Simplified Installation. This VPN concentrator must consider that the VPN connection should be done with the OpenScape Branch's WAN address as partner.

Connect the USB stick previously created to a USB port in the OpenScape Branch server.

Connect the OpenScape Branch device LAN interface to the network. This option will need that WAN interface is also connected to the network for IPsec establishment. The LAN MAC ID is still needed in the installation configuration in CMP for validation.

Power the OpenScape Branch device up

The OpenScape Branch device will boot up off of the USB stick and receive via DHCP a temporary IP address (if used, because if not, then takes the defined IP address).

In this point, the VPN tunnel is created and CMP is contacted. If IPsec tunnel is not OK, installation will not continue.

If everything is OK, the OpenScape Branch will get the CMP information from the USB Stick and it will automatically download and install the software image, configuration file, announcement files (optional) and additional certificates if necessary.

OSB Assistant will show the installation progress in the Status column.

Branch Office	IP Address	Comm System	Business Group	Version	Status	Mode	Last Update	Security status
 bocaOB_20_FujRX330	10.234.1.20	Node105VV6	BGCA	---	Installation started	---	2011/11/03 03:56:32	Secured Mode

Status indicates installation progress and mode is set to Secured

When the installation is finished the device will alert providing 10 audible beeps (single beep followed by a pause and the cycle is repeated 10 times).

Branch Office	IP Address	Comm System	Business Group	Version	Status	Mode	Last Update	Security status
 bocaOB_20_FujRX330	10.234.1.20	Node105VV6	BGCA	---	Reboot is required	---	2011/11/03 03:25:27	Secured Mode

Status indicates installation finish and a restart is required

When the installation finishes remove the USB Stick. This will automatically restart the server. After the restart the server will be online and the status in OSB Assistant will be updated.

Branch Office	IP Address	Comm System	Business Group	Version	Status	Mode	Last Update	Security status
 bocaOB_20_FujRX330	10.234.1.20	Node105VV6	BGCA	V2R0.06.00 Build 1	Normal	Proxy	2011/11/03 03:16:52	Secured Mode

Status is updated to show OSB Operational Mode

64.6.4 Error Conditions

When the simplified installation fails the following log files must be provided:

From Common Management Portal (CMP): symphonia.log

This file is located under the following directories

Offboard: /var/siemens/common/log/

Onboard: /log/

From OpenScape Branch: autoinstall.log

This file is located under the following directories:

For Zero Touch installation (Option 1): /opt/siemens/openbranch/var/log/openbranch/

For all other options (Option 2 – 4): /mnt/usbstick/

After a failed installation the OpenScape Branch will fall back to a default IP address: 192.168.0.1. The service personnel can access the OSB server via this IP to gather the required log file.

65 Back Up Data Link

This capability allows the activation of multiple alternate back-up links to the OpenScape Voice through the PSTN network for the event of an interconnectivity failure of the existing data network. This functionality requires an OpenScape Branch unit collocated with the OpenScape Voice. The OpenScape Branch may set up a backup link between a branch office and data center in case of a WAN outage.

65.1 Network and Connectivity Requirements

65.1.1 Media Server

When working with the Backup Link feature with OpenScape Branch, the media server functionality for each branch must be provided by the OpenScape Branch. Please refer to the Branch Media Server section in the OpenScape Branch configuration Guide.

65.1.2 Network Services

When communicating with the OpenScape Voice via the backup link channel only MGCP, SIP and SNMP messages are allowed. It is recommended that network services like DNS, SNTP and DHCP are provided by OpenScape Branch.

65.1.3 Gateways

PSTN gateways are required in the Data Center as well as the Branch. These gateways must support clearmode. This is also referred to as clear-channel data or 64 Kbit/s unrestricted .

65.1.4 Data Center Router

It is mandatory that the router serving the data center is configured to re-route packets to the Backup Link Server when the WAN connectivity is down.

65.1.5 IPSec VPN

It is recommended to provide IPSec VPNs on the WAN tunnels to guarantee that any outage in the WAN is detected by the data center router. In case of OSB in Branch SBC Mode, it is recommended that IPSec tunnel is established directly from the Data Center router to the OpenScape Branch WAN interface.

65.1.6 PPP Network

Connections between BLC and BLS use PPP network. The chosen subnet must be enough to fit the number of multiple links needed. In practice, the number of available IPs (hosts) must be greater than or equal 2 times the number of maximum number of backup links used. This network should also be chosen in a non-routable address, i.e. a network not used in the branch and data center routers.

65.2 Known Restrictions

65.2.1 General

OpenScape Voice tunnel status validation is not supported for Simplex or Collocated configurations.
Backup link is not a supported functionality when OpenScape Branch is behind Centralized SBC environment
Backup Link Client (BLC) is not supported on Proxy ACD Mode
Backup Link Server (BLS) is not supported on Proxy ACD Mode and Branch SBC Mode
Additional media servers on the branch are not supported when backup link is configured
Some OSV features are limited during Normal Backup Mode due to CAC restrictions
Traffic bursts can cause transition to survivable mode if TLS is chosen
Up to 30 data channels are released per BLS/BLC
Auto-attendant calls should be forwarded to phones within the branch in backup mode

65.2.2 OSB V1R4

Backup link call through the peer OSB is not supported

65.2.3 OSB V1R3

Only single link is supported
Supports continuous traffic and registration load up to 1 calls per second per BLS/BLC

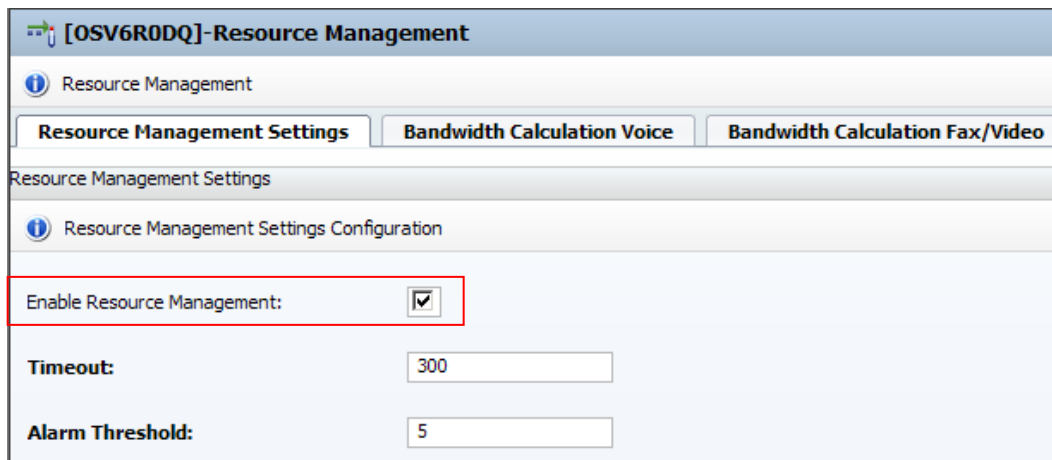
65.3 Configuration for OpenScape Branch with OpenScape Voice Integrated Simplex or Collocated

65.3.1 Configuring the OpenScape Voice for Backup Data Link Support

65.3.1.1 CAC Configuration

Go to OpenScape Voice -> Administration -> Call Admission Control -> Resource Management

1. Check if *Enable Resource Management flag is marked:*



The screenshot shows the 'Resource Management Settings Configuration' page in the OpenScape Voice administration interface. The page has a title bar '[OSV6R0DQ]-Resource Management' and a sidebar with 'Resource Management' selected. The main content area has three tabs: 'Resource Management Settings' (active), 'Bandwidth Calculation Voice', and 'Bandwidth Calculation Fax/Video'. Under the 'Resource Management Settings' tab, there is a section 'Resource Management Settings Configuration'. This section contains three settings: 'Enable Resource Management' with a checked checkbox (highlighted by a red rectangle), 'Timeout' with a text input field containing '300', and 'Alarm Threshold' with a text input field containing '5'.

Go to OpenScape Voice -> Administration -> Call Admission Control -> Groups

- Create a CAC Group for each branch and add the members based on the branch's subnets and enter all the subnets for the branch:

2. Add the CAC policy and limit based on 'Bandwidth'. Enter '0' for the Backup Max Bandwidth value.

Policy configuration

In this section the specified policy can be activated and configured.

Limit Type: Bandwidth

Max number of calls:

Backup Max number of calls:

Max Bandwidth (kbps):

Backup Max Bandwidth (kbps):

Max Bandwidth is defined for the WAN interface, which can be configured with the max value (1000000) supported by OSV.

Backup Max Bandwidth must be set to zero '0'.

Ensure the Srx/Lsm/CheckRouter flag is set to RtpFalse

Configure the BLS IP Address in Data Center Router SNMP Configuration entry in the OpenScope Voice. This is only possible via StartCli. Select the following options:

Application-level Management. 6

Network Traffic Management. 9

Call Admission Control Management. 1

CAC Access Link Status Monitoring. 6

Modify Data Center Router SNMP Configuration.. 3

Enter the IP address of the BLS as the Data Center Router and select default values for all other parameters.

Data Center Router IPv4 Address < (max length: 46)> (default: 0.0 0.0): 10.234.3.21

Snmpv2c Community string < (max length: 2048)> (default: public): public o Snmp version used to access router < 2 = Snmpv2c, 3 = Snmpv3 >: 2

The Data Center Router SNMP configuration should look like this once completed:

Data Center Router 1 SNMP Configuration:

```
Username:           None
Authentication Key:  None
Authentication Protocol: None
SnmpV2c Community String: public
IPv4 Address:       10.234.3.21
Sends Snmpv2 Traps/Informs: true
```

OpenBranch BLS IP Address.

- All the branches must have a CAC Group configured.

[BOCAST1]- CAC Groups

In this section the specified policy can be activated and configured.

Search for: in No Criteria Search Show All Advanced... Elements Per Page: 10

<input type="checkbox"/>	CAC group name	Member Type	Parent Cac Group	Monitored Link Type	Monitored Link Status
<input type="checkbox"/>	bocaOB22_O5B50i	Subnets		Primary access link	Link down
<input type="checkbox"/>	bocaOB23_O5B50i	Subnets		Primary access link	Link down

65.3.2 Subscriber Rerouting Configuration

65.3.2.1 Activate Rerouting and configure Prefix Access Code

Go to OpenScope Voice -> Administration -> Signaling Management -> SIP Under Rerouting Tab:

Set the Subscriber Rerouting Prefix Access Code

Enable Rerouting for SIP Subscribers

SIP Settings

General Rerouting SIP Timers Best Effort SRTP FQDN

Rerouting

Although using Subscriber Rerouting through the PSTN is useful during WAN failures, CAC bandwidth restrictions, it can also lead to additional charges for the PSTN calls.

Enable Rerouting for SIP Subscribers: ☒

Subscriber Rerouting Prefix Access Code: 8

International:

National:

Local:

Enter a desired prefix.

65.3.2.2 Configure Branch Office for Remote Branch

- **Add a Routing Area and DID Pool to each Branch Office, including BLS.**

Go to OpenScope Voice -> Business Group -> Branch Office Lists and select the branch office

Assign a Routing Area and a DID Pool

General DID Pool Access Control List

General

Branch Office Name: BO_osb50i-PRI

Representative Endpoint: osb50i-PRI

Numbering Plan: NP_BG_DQ_OSB

Office Code:

Routing Area: ra_osb50i-PRI

This is a Branch Office of type OpenScope Branch: ☒

Branch must have a Routing Area.

DID Pool

Select the DID Pool of the Branch Office

Add Range... Add... Delete

Sel: 0 | Items/Page: 200 | All: 2

Directory Number
551146687499
551146687498

Select subscribers. These cannot be used for anything else.

NOTE1 : The subscribers selected in this pool cannot be used for anything else. One DID number is required per 180 subscribers in the branch office, but it's recommended to have at least 2 DID numbers assigned to each one.

NOTE 2: All subscribers in the remote branch must be added to their respective branch office.

- **Ensure the DID Home DN's selected for the DID Pool are set to “Service” type “DID Pool Number”.**

This is done automatically by Assistant when the Home DN is selected for the DID Pool. To verify the service is set check the DN in the Home DN Table (Global Translation and Routing -> Home Directory Numbers)

[OSV6R0DQ]-Home Directory Numbers

Directory Numbers are system resources that can be assigned to a Business Group.

Filter By: Start range: End range:

Sel:0 | Items/Page: 200 | All:2

<input type="checkbox"/>	Directory Number	Destination Type	Destination Name	Business Group
<input type="checkbox"/>	55 (11) 4668-7498	Service	DID Pool Number	
<input type="checkbox"/>	55 (11) 4668-7499	Service	DID Pool Number	

65.3.2.3 Configure Branch Office for Data Center

First, create a virtual endpoint and use it as a representative Endpoint for the Data Center's Branch Office. This is required to provide survivability functionality to subscribers in the Data Center via the backup link when the CAC policy is into effect. i.e. calls from branch to data center subscribers

General | SIP | Attributes | Aliases | Routes | Accounting

Endpoint

Define the connection data of an endpoint, e.g. you may use this to add a gateway to a switch.

Name:

Remark:

Registered: ☒

Profile:

Branch Office:

Associated Endpoint:

Default Home DN:

Location Domain:

SIP Signaling

For the static Endpoints the address of the SIP signaling interface can be specified in IP or FQDN format. Note that the address of the signaling interface cannot be modified unless the entry in the security section has first been removed.

Type:

Signaling Address Type:

Endpoint Address:

Port:

Transport protocol:

Best Effort SRTP support:

ANAT Support:

Use Proxy/SBC Best-Effort SRTP settings for calls to subscribers: ☐

NOTE: Add all Data Center subscribers to this branch office. For all those subscribers kept in the 'Main Office' calls will only work in the direction from data center to branch office.

Create a virtual endpoint with an inexistent IP address and set the Survivable Endpoint attribute. Ensure that “Do not audit endpoint” attribute is also set. No other attribute is needed.

General	SIP	Attributes	Aliases	Routes	Accounting
Attributes					
Attributes available for this SIP endpoint					
Supports SIP UPDATE Method for Display Updates					<input type="checkbox"/>
UPDATE for Confirmed Dialogs Supported					<input type="checkbox"/>
Send Provisional response during session updates					<input type="checkbox"/>
Survivable Endpoint					<input checked="" type="checkbox"/>
SIP Proxy					<input type="checkbox"/>
Route via Proxy					<input type="checkbox"/>
Allow Proxy Bypass					<input type="checkbox"/>
Do Not Audit Endpoint					<input checked="" type="checkbox"/>
Use Proxy/SBC ANAT settings for calls to subscribers					<input type="checkbox"/>
Support for Callback Path Reservation					<input type="checkbox"/>
Send Progress to Stop Call Proceeding Supervision Timer					<input type="checkbox"/>

Allow Proxy Bypass: Proxy Bypass is a system-wide OpenScape Voice feature that is turned on per default.

It is only used when deploying Type 2 or 5 branch offices. If selected (enabled), Proxy Bypass allows OpenScape Voice to bypass the recorded proxy in a contact if an INVITE request to the contact's recorded proxy does not receive a response within a specified time.

IMPORTANT: This attribute is not applicable for SIP Private Networking

NOTE: For previous OSV versions, the configuration of “Do Not Audit Endpoint” flag can only be done via StartCli. In this case, select the following options:

Application-level Management. 6

Zone Management. 5

Modify Endpoint. 2

- Set the “Do not audit Endpoint” to “true”

Change SIP endpoint attributes as bitmap sums? (default: true): false

Do not audit Endpoint <0=false|1=true|-1=unchanged> (default: -1): 1

- **Create the Branch Office using the virtual endpoint just created.**

Go to OpenScope Voice -> Business Group -> Branch Offices List and select the branch office Do not assign a Routing Area and assign a DID Pool.

NOTE: The subscribers selected in this pool cannot be used for anything else.

- **Ensure the DID Home DNs selected for the DID Pool are set to “Service” type “DID Pool Number”**

This is done automatically by Assistant when the Home DN is selected for the DID Pool. To verify the service is set check the DN in the Home DN Table (Global Translation and Routing -> Home Directory Numbers)

65.3.2.4 Configure Destinations to Gateways serving all branches and data Center

- **Add a Destination to the Gateway in the Data Center**

If not existent, add a destination to go to the endpoint for the gateway at the Data Center

Note 1: For Geo-Separated systems each node location will need a gateway, thus two destinations are needed. One for each gateway. See next session for Geo-Separated configuration.

Note 2: All gateways must support clearmode. This is also referred to as clear-channel data or 64 Kbit/s unrestricted.

ID	Endpoint	Route Type	Delete	Insert	Nature of Address
1	RG8700_DC_BLS	SIP-Endpoint	0		Undefined

NOTE: Use symmetric routing (GW behind proxy) and make destination point to the proxy (OSB).
 If using asymmetric routing (OSV talks directly to GW in branch) calls in backup mode can fail, because OSV may audit and set gateway as inaccessible during an outage.

GeneralRoutesRoute ListsDestination Codes

Name:OB2250i_BLC_DES

is a media server:

GeneralRoutesRoute ListsDestination Codes

Routes

Multiple routes can be used for prioritizing the routes to the gateways.

Elements Per Page: 100

	ID	Endpoint	Route Type	Delete	Insert	Nature of Address
	1	bocaOB22-OSB50i	SIP-Endpoint	0		Undefined

65.3.2.5 Configure a Code Index

- Add a Code Index for Rerouting**

Code Index

GeneralPatterns

Identification

Text for the Code Index Identification info box. Note: No more than 15 charac

Code Index Name:CI_Local_Gwy

Remark:

Nature Of Address:Code Index

Originator Attributes

i Optionally, an additional match is required if the originator of the call below

Class Of Service: ...

Traffic Type: ▼

Routing Area: ...

Destination

i Specify additional parameters to determine how the call will be routed.

Destination Type: ▼

Destination Name: ...

Office Code: ...

Enter the Branch's Routing Area.

- **Add a second pattern to point to the branch endpoint (for calls from branch to data center)**

NOTE: The branch needs to have a Routing Area.

The gateway in the branch must be configured for symmetric signaling (GW is behind proxy)

Originator Attributes

i Optionally, an additional match is required if the originator of the call belongs to

Class Of Service: ...

Traffic Type: ▼

Routing Area: ...

Destination

i Specify additional parameters to determine how the call will be routed.

Destination Type: ▼

Destination Name: ...

Office Code: ...

The Code Index will then have multiple patterns. For each branch with a Routing Area and with no Routing Area for the DataCenter.




General

Patterns

A pattern associates a rate area and a class of service with a destination.

Patterns


Elements Per Page: 100

<input type="checkbox"/>	Routing Area	Class Of Service	Destination
<input type="checkbox"/>	 OB22_OSB50i_RA		OB2250i_BLC_DES
<input type="checkbox"/>			RG8700_DC_DES
<input type="checkbox"/>	 OB23_OSB50i_RA		OB2350i_BLC_DES


65.3.2.6 Configure Routing to the Code Index

- **Add Prefix Access Code for the Subscriber Rerouting PAC**

Go to OpenScope Voice -> Business Group -> Default Numbering Plan
Under Translation add the Prefix Access Code

 **[BOCAST1] - [BGCA] - [NP_BGCA] - Edit Prefix Access Code: 8**

Identification

 If the dialed digits match this code, the specified modification to these dialed digits is executed.

Prefix Access Code:

Remark:


Minimum Length:

Maximum Length:

Digit Position:

Digits to insert:

Settings


 Specify additional parameters to determine how the call will be routed.

Prefix Type:

Nature of Address:

Destination Type:

Destination Name:



- **Add a Destination Code**

Add it to point to the Code Index created for re-routing (Note: Nature of Address must be International for number normalization if using Mobile UC Clients on the Branches)

[BOCAST1] - [BGCA] - [NP_BGCA] - Edit Destination Code: 8

General	Extensions
This destination code will be used for a call if the dialed or modified (in PAC) digits and the Nature Of Address are as follows:	
Destination Code:	<input type="text" value="8"/>
Remark:	<input type="text"/>
Country Code:	<input type="text"/>
Nature Of Address:	<input type="text" value="Unknown"/>
Traffic Type:	<input type="text" value="None"/>
Originator Attributes	
Optionally, an additional match is required if the originator of the call belongs to the specified Class Of Service:	
Class Of Service:	<input type="text"/>
Routing Area:	<input type="text"/>
NPA:	<input type="text"/>
Destination	
Specify additional parameters to determine how the call will be routed.	
Destination Type:	<input type="text" value="Code Index Destination"/>
Code Index Name:	<input type="text" value="CI_Local_Gwy"/>
DN Office Code:	<input type="text"/>

65.3.2.7 Configuration of Routing to BLS DID number

- **Add a Destination to the OSB-BLS EndPoint:**

Go to OpenScope Voice -> Business Group -> Destination and Routes -> Destinations

Sel:0 Items/Page: 200 All:1			Add...	Edit...	Delete
<input type="checkbox"/>	Name ▲	Media Server	Number of Routes		
<input type="checkbox"/>	OSB_BLS	False	1		

- **Create a Prefix Access Code to reach BLS's DID number**

Go to OpenScope Voice -> Business Group -> Translation -> Prefix Access Code (Note: Nature of Address must be International for number normalization if using Mobile UC Clients on the Branches)

Identification

If the dialed digits match this code, the specified modification to these dialed digits is executed.

Prefix Access Code:

5541334167

Remark:

Minimum Length:

12

Maximum Length:

12

Digit Position:

0

Digits to insert:

Settings

Specify additional parameters to determine how the call will be routed.

Prefix Type:

Off-net Access

Nature of Address:

Unknown

Destination Type:

None

Destination Name:

...

355

OpenScope Branch V10 Configuration Guide

- **Create a Destination Code to BLS's DID number:**

Go to OpenScape Voice -> Business Group -> Translation -> Destination (Note: Nature of Address must be International for number normalization if using Mobile UC Clients on the Branches)

The screenshot shows a configuration window with a 'General' tab. It contains several input fields and dropdown menus for configuring a destination code. The 'Destination Code' field is populated with '5541334167'. The 'Nature Of Address' dropdown is set to 'Unknown'. The 'Destination Type' dropdown is set to 'Destination'. The 'Destination Name' field is populated with 'OSB_BLS'. There are also sections for 'Originator Attributes' and 'Destination' with additional configuration options.

General	
Destination Code:	5541334167
Remark:	
Country Code:	
Nature Of Address:	Unknown
Traffic Type:	
Originator Attributes	
Optionally, an additional match is required if the originator of the call belongs to the specified Class of Service and Routing Area.	
Class Of Service:	
Routing Area:	
NPA:	
Destination	
Specify additional parameters to determine how the call will be routed.	
Destination Type:	Destination
Destination Name:	OSB_BLS

65.3.3 Configuration of Voice Mail Rerouting (optional)

Calls to subscriber can be forwarded to Voice Mail Server located in Data Center (for example OpenScape Xpressions Voice Mail Service). In the case of WAN outage with Backup Link support, calls forwarded from subscribers to Voice Mail Service should be rerouted through PSTN.

To allow rerouting to Voice Mail Server, go to OpenScape Voice -> Business Group -> Members -> Endpoint and select your Voice Mail endpoint (e.g. Xpressions). Check if the following attributes are enabled.

The screenshot displays the configuration page for an endpoint named 'Xpressions'. The 'Attributes' tab is selected, showing a list of configuration options. A red rectangular box highlights three specific attributes, each with a checked checkbox: 'Rerouting Direct Incoming Calls', 'Rerouting Forwarded Calls', and 'Enhanced Subscriber Rerouting'. A yellow callout box with a black border contains the text: 'Enable "Rerouting Forwarded Calls", "Rerouting Direct Incoming Calls" and "Enhanced Subscriber Rerouting"'. An arrow points from this callout box to the three highlighted attributes.

Attribute	Enabled
Send URI In Telephone Subscriber Format	<input type="checkbox"/>
Rerouting Direct Incoming Calls	<input checked="" type="checkbox"/>
Rerouting Forwarded Calls	<input checked="" type="checkbox"/>
Enhanced Subscriber Rerouting	<input checked="" type="checkbox"/>
Automatic Collect Call Blocking supported	<input type="checkbox"/>
Send Authentication Number in P-Asserted-Identity header	<input type="checkbox"/>
Set NPT/TON to Unknown	<input type="checkbox"/>

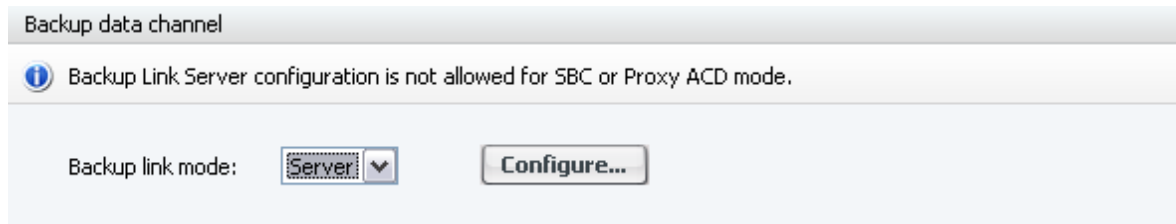
NOTE: If gateways are used for networking with PSTN, do not enable "Rerouting Direct Incoming Calls" because it may lead to loops with PSTN.

65.4 Configuring the OpenScape Branch for Backup Data Link Support

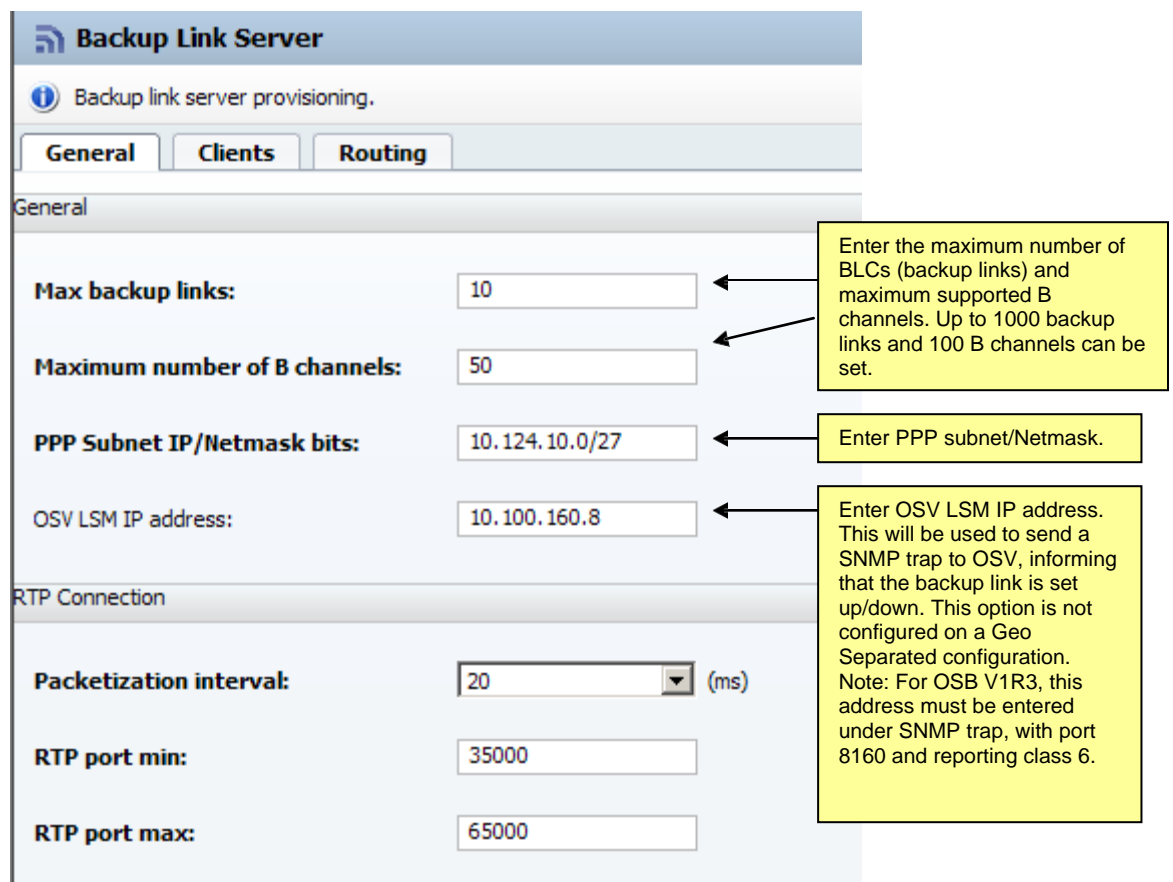
65.4.1 Backup Link Server (BLS) Configuration

The following are the configuration steps for the OpenBranch located in the Data Center (Proxy, SBC-Proxy only)

- **After login to the OSB Assistant go to the OpenScape Branch -> Configuration -> VoIP option and under General select “Server” for Backup link mode and click on “Configure...”:**



- **Enter desired values for the General area:**

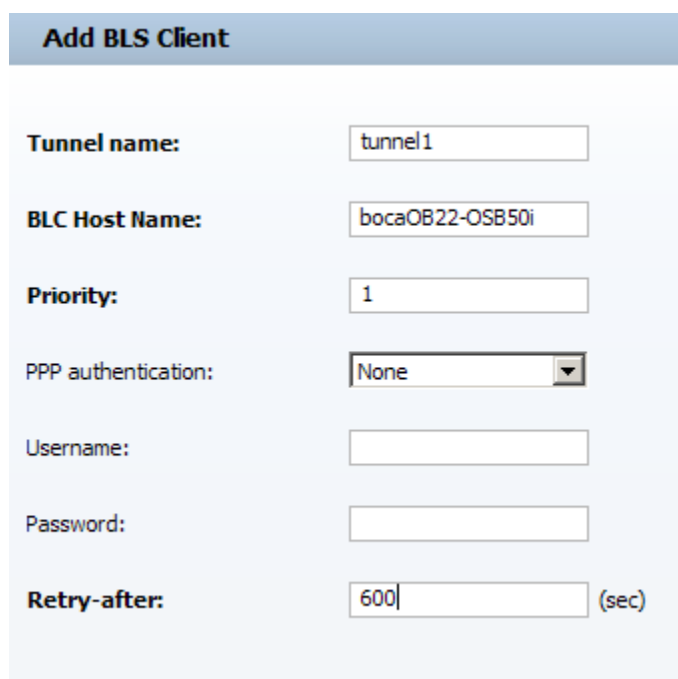


NOTE 1: The configuration of “PPP Subnet IP/Netmask bits” should be enough to fit the amount of BLC devices on the network. To have this, the number of hosts must be at least 2 times the number configured for “Max backup links” (this is because each backup link has one PPP address for BLS and other for BLC).

For example, in the subnet 10.124.10.0/27 we have 32 PPP addresses (10.124.10.0 to 10.124.10.31) that must be greater or equal to 2 times the number configured in “Max backup link” (in this case up to 16 BLCs are possible with this subnet).

NOTE 2: The PPP subnet IP addresses shall not conflict with any IP/subnets in the branch or data center

-
- **Under the Clients tab area, click on “Add” and create the tunnel for each BLC.**



The screenshot shows a web form titled "Add BLS Client". It contains the following fields:

- Tunnel name:** A text input field containing "tunnel1".
- BLC Host Name:** A text input field containing "bocaOB22-OSB50i".
- Priority:** A text input field containing "1".
- PPP authentication:** A dropdown menu with "None" selected.
- Username:** An empty text input field.
- Password:** An empty text input field.
- Retry-after:** A text input field containing "600" followed by "(sec)".

Tunnel Name: Any desired name for this tunnel. It must match the name assigned to the tunnel in OSV CAC group policy (See CAC configuration section)

BLC Hostname: The configured hostname of the OSB client (BLC) that will be using this tunnel. This name must match the hostname of each BLC.

Priority: This is the priority used by BLS for accept or reject each BLCs tunnel request. If the maximum number of backup links or B channel is achieved, the BLS will decide which BLC request must be prioritized. Lower the number, higher the priority of BLC's tunnel.

NOTE: Each BLS Client (BLC) must have a different Priority

PPP authentication, Username, Password: Configure the PPP authentication method as None, PAP or MS-CHAP. If PAP or MS-CHAP is chosen, Username and Password must be used.

NOTE: PPP authentication, username and password must be the same on BLS and BLC sides.

Retry After: BLS send this timer to BLC to indicate how long BLC must wait until retrylink establishment in case of rejection due to priority evaluation.

- **Under VOIP -> General -> Gateways click on “Configure...”. Enter the following line in the Gateway Table:**


Gateways

Sel:0 | Items/Page: 200 | All:1

Add...

Edit...

Delete

<input type="checkbox"/>	Signaling	IP	Port	Interface	Transport	Routing	Type	Functional type	Trunk	Output	Output	Priority
	Address Type	Address/FQDN				Prefix/FQDN			Profile	digit strip	digit add	
<input type="checkbox"/>	 IP Address or FQDN	10.100.124.10	5086	LAN	UDP	5541334167%	Backup Link Server	All Modes Egress/Ingress	Gateway	0		

IP Address/FQDN: Note this is its own IP. The IP address of the same BLS

Port: Port 5086 is the only acceptable option. This is the port the BLS uses for backup link

Routing prefix/FQDN: This is the DID number that is dialed through the GW to establish the link

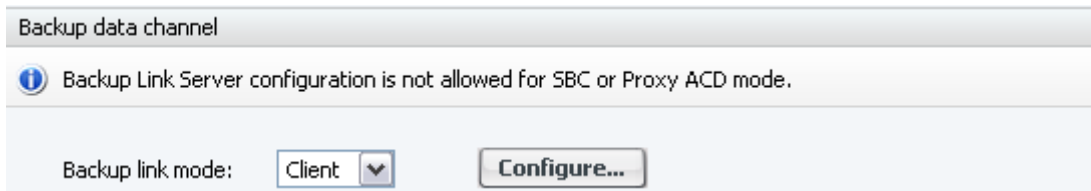
Transport: UDP is the only acceptable protocol for backup link connection.

Type: Backup Link Server is the only option allowed for a backup link call.

65.4.2 Backup Link Client (BLC) Configuration

The following are the configuration steps for the OpenBranch located in the Branch (BLC). (Supported OpenScope Branch modes are Proxy, SBC and SBC-Proxy only)

- **After login to the OSB Assistant go to the VOIP option and under General select “Client” for Backup link mode and click on “Configure...”:**

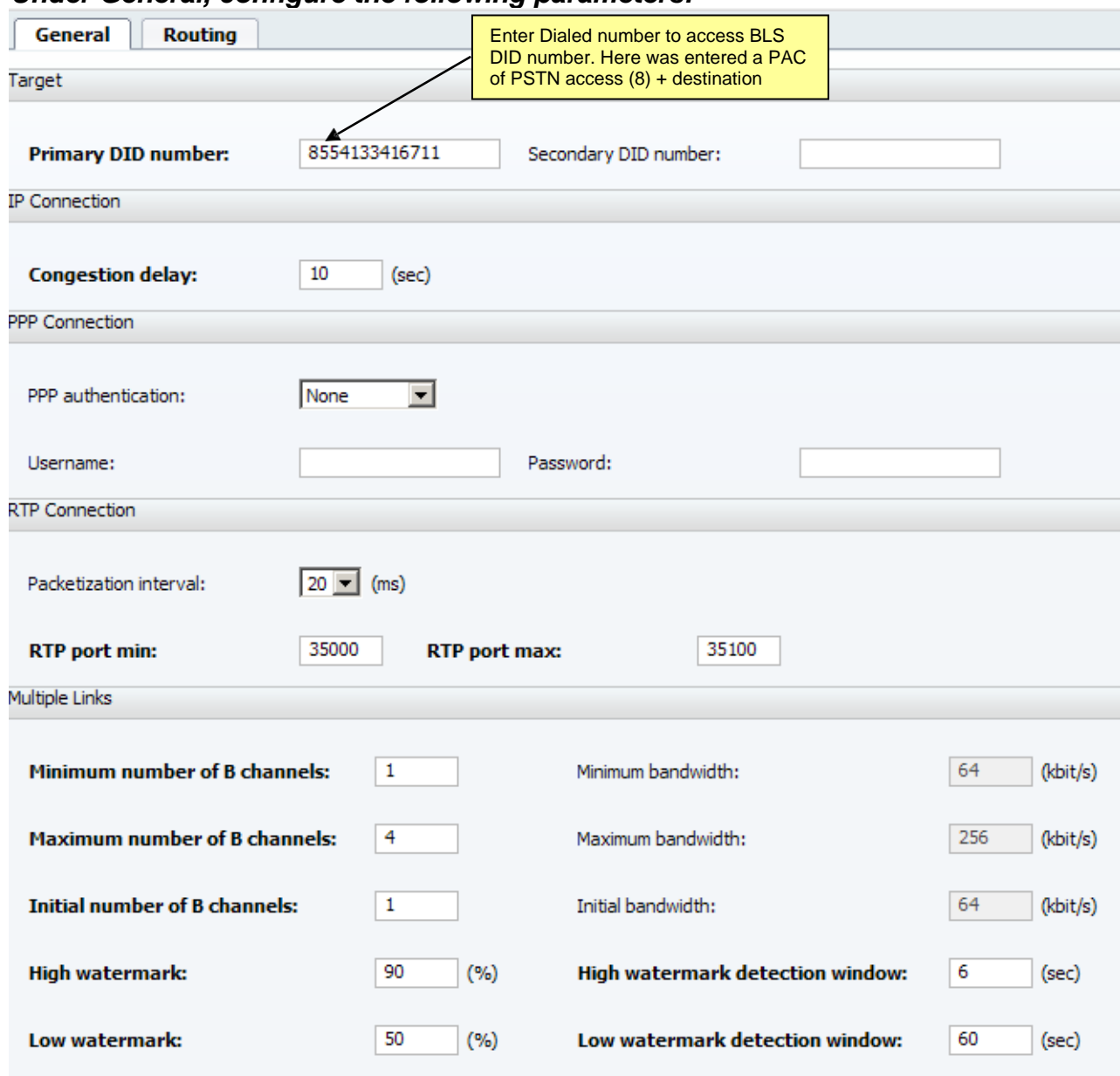


Backup data channel

Backup Link Server configuration is not allowed for SBC or Proxy ACD mode.

Backup link mode: Client

- **Under General, configure the following parameters:**



General Routing

Target

Primary DID number: 8554133416711 Secondary DID number:

IP Connection

Congestion delay: 10 (sec)

PPP Connection

PPP authentication: None

Username: Password:

RTP Connection

Packetization interval: 20 (ms)

RTP port min: 35000 RTP port max: 35100

Multiple Links

Minimum number of B channels:	1	Minimum bandwidth:	64 (kbit/s)
Maximum number of B channels:	4	Maximum bandwidth:	256 (kbit/s)
Initial number of B channels:	1	Initial bandwidth:	64 (kbit/s)
High watermark:	90 (%)	High watermark detection window:	6 (sec)
Low watermark:	50 (%)	Low watermark detection window:	60 (sec)

Primary DID number: This is the number to be dialed to access BLS through PSTN and establish the PPP link.

Secondary DID number: In a geo-separated scenario, each BLS receives its own IP address and DID number. It is not used for a Simplex/ Collocated configuration.

PPP authentication, Username and Password are configured based on what was also configured in the BLS Multiple Links values are used to configure multilink feature. The multilink bandwidth is calculated by the number of B channels multiplied by 64 kbit/s

Minimum number of B channel: This number will define the minimum bandwidth configured.

Maximum number of B channels: This number will define the maximum bandwidth configured. It is also used to initial bandwidth when there is a transition from survivable to backup mode.

Initial number of B channels: This number will define the initial bandwidth of backup link, i.e. how many channels will start the PPP link when transition from normal to backup mode

High Watermark: Indicate the percentage of usage of the last channel that will trigger BLC to add a new channel to the multilink bundle.

High Watermark detection window: after achieving High watermark, this is the time that BLC will stay over the high watermark before adding a new channel to the bundle.

Low Watermark: Indicate the percentage of the seizure of the last channel that will trigger BLC to delete a channel from the multilink bundle.

Low Watermark detection window: after achieving Low Watermark, this is the time that BLC will stay below the low watermark before delete a channel from the bundle.

NOTE 1: If multilink achieves 100 % of bandwidth usage, BLS will detect a state of congestion and will send an order to BLC immediately add a new channel, if possible, irrespectively of the High Watermark configuration. During congestion, new calls will be rejected with a retry-after timer response.

NOTE 2: If BLC is using TCP or UDP as SIP transport protocol, PPP tunnel is compressed and channels are optimized. For TLS, the channels are uncompressed. In case of TLS, OSB should send signaling to OSV sipm3 address.

NOTE 3: The default values for Initial, Maximum and Minimum number of B-Channels are according to the table below (this table can be used as reference for TCP and UDP):

Device Model	Minimum and Initial Number of Backup Links	Maximum Number of Backup Links
OSB 50 / 50i	1	1
OSB 250	1	3
OSB 1000	2	6
OSB 6000	4	10

NOTE 4: For TLS, the following table shows the recommended configuration values.

Device Model	Minimum and Initial Number of Backup Links	Maximum Number of Backup Links	Maximum Continuous Traffic (calls per second)	Maximum Registration Load
OSB 50 / 50i	1	3	1	40
OSB 250	2	7	3	40
OSB 1000	4	11	5	40
OSB 6000	7	30	17	40

Under Routing, configure trusted addresses for backup mode. Enter all IP Addresses that will be in the routing table when backup mode is achieved. For example, enter here the IP address of ccm05 address of OpenScope Voice to have Media Server working on Backup Mode.

Backup link client provisioning.

General **Routing**

Sel:0 | Items/Page: 200 | All:1

<input type="checkbox"/>	IP Address	Description
<input type="checkbox"/>	10.100.150.58	ccm05 01

Enter the IP addresses of trusted servers. OSV ccm05 must be entered here (MGCP traffic).

Note: OSV's SIPSM node address and SNMP trap destination are already trusted and must not be entered here. A maximum of 6 addresses are allowed.

- In OpenScope Branch under the Gateway Table configure the BLC to route the call to the gateway when receiving the configured subscriber rerouting access code:

Under VOIP -> General -> Gateways click on "Configure..."

Verify routing to the DID is configured in the gateway configuration:

Gateways

Sel:0 | Items/Page: 200 | All:1

<input type="checkbox"/>	IP Address/FQDN	Port	Interface	Transport	Routing Prefix/FQDN	Type	Functional type	Trunk Profile	Output digit strip	Output digit add	Priority
<input type="checkbox"/>	rg8700-177.blc.backuplink	5060	LAN	TCP	8%	RG	All Modes Egress/Ingress	Gateway	1		1

Enter the subscriber rerouting code and a wildcard for routing to the branch gateway.

Note 1: In this case, only one routing rule was created because prefix access code to dial DID in Survivable Mode is the same as the code for rerouting in Normal Mode. If not, 2 different routing rules must be entered.

Note 2: Gateways must support clearmode. This is also referred to as clear-channel data or 64 Kbit/s unrestricted . If OSB 50i PRI is used, check if "data calls allowed" flag is enable (go to CMP on OpenScope Branch -> Integrated Gateway -> General -> Configuration, Edit the PRI link and check for flag)

- Add a SNMP trap to CMP server. This is used to inform CMP that OpenScope Branch started or stopped backup mode.

- **Go to Alarms -> Trap Destinations**

Add trap destination SNMP

IP Address: 10.100.160.6

Port: 162

Reporting class set: 7

Blocked: ☐

This is the IP address of CMP management

65.4.3 Survivability Mode Avoidance

The Backup Link Client must avoid where possible that an OpenScape Branch moves to the Survivable Mode state after a transition. To have a better approach for survivability mode avoidance, it is highly suggested that some configurations are made on survivability providers parameters.

For transition from Normal Mode to Backup Mode, the maximum transition time is considered 60 seconds for a Simplex / Collocated Mode and 120 seconds for Geo Separated configuration.

For an optimized configuration, Timers and Thresholds values of Survivability Provider should be configured as follows:

- Under OpenScape Branch -> VoIP -> Timers and Thresholds:

General **Comm System** **Timers and Thresholds** **Codecs** **RTP**

Timers and Thresholds

Failure threshold: 3 (pings)

Success threshold: 1 (pings)

Transition Mode threshold: 3 (pings)

OPTIONS interval: 20 (sec)

OPTIONS request timeout: 10 (sec)

Notification Rate: 10

To have a fast transition, OPTIONS interval should be the lowest possible. The minimum value is 11 seconds. Please see Note1 below*.

To avoid unnecessary transitions, use these values. The minimum OPTIONS value is 10 seconds. Please see Note2 below**.

Increase the transition mode threshold to 3, to have a lower OPTIONS interval. Please see Note1 below*.

***NOTE 1:** OPTIONS interval value should be long enough to avoid survivable mode on the transition from Normal to Backup Mode and at the same time the lowest possible value to have a fast transition to Normal Backup Mode. So, the timers and thresholds must be configured according to the following formula:

$$Mtt \leq Tt * Oi + (Tt - 1) * Ot$$

Where:

Mtt = Maximum time in transition mode (60 seconds if only Primary link is configured – Simplex or Collocated
- or 120 seconds if also Secondary link is configured – Geo Separation)

Tt = Transition Mode threshold

Oi = OPTIONS interval (min. 11 sec.)

Ot = OPTIONS timeout (min. 10 sec.)

If the criteria are not fulfilled, system will show an error message.

****NOTE 2:** If BLC is in Normal Backup Mode, unnecessary system transitions due to network issues, like packet losses, TCP retransmissions and others should be avoided. So, to optimize the link transition, we must consider that Failure threshold (pings) multiplied by OPTIONS timeout (sec) must be at least 30 seconds.

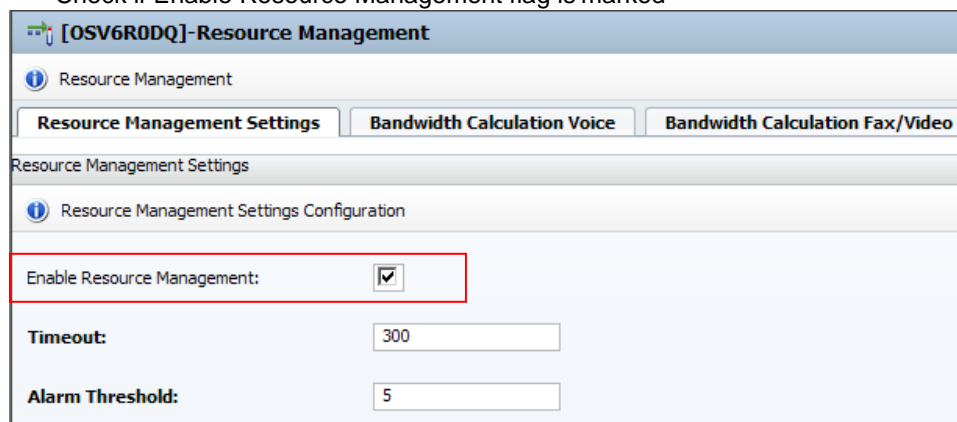
65.5 Configuration for OpenScape Branch with OpenScape Voice Geo Separated

65.5.1 Configuring the OpenScape Voice for Backup Data Link Support

65.5.1.1 CAC Configuration

- **Go to OpenScape Voice -> Call Admission Control -> Resource Management**

- Check if Enable Resource Management flag is marked



The screenshot shows the 'Resource Management' configuration page for '[OSV6R0DQ]'. It features three tabs: 'Resource Management Settings' (selected), 'Bandwidth Calculation Voice', and 'Bandwidth Calculation Fax/Video'. Under the 'Resource Management Settings' tab, there is a section titled 'Resource Management Settings Configuration'. This section contains three settings: 'Enable Resource Management' with a checked checkbox, 'Timeout' with a value of 300, and 'Alarm Threshold' with a value of 5. The 'Enable Resource Management' checkbox is highlighted with a red rectangle.

- **Go to OpenScape Voice -> Administration -> Call Admission Control -> Groups**

- Create a CAC Group for each branch and add the members based on the branch's subnets and enter all the subnets for the branch:

GeneralMembersPoliciesGroup To Group Policies

CAC group configuration

Please enter a CAC Group name without any special characters or blanks.

CAC group name: CAC_NET180_OSB1000

Parent CAC Group Name:

Backup Selection Parameters

The fields below allow enabling a backup access link for this CAC group.

Enable Backup Access Link: ☒

Access Link type: Data Center

Node 1 Data Center router IP address: 10.10.1.1

Node 1 Tunnel name: tunnel1

Node 1 Tunnel Link Status:

Node 2 Data Center router IP address: 10.20.1.1

Node 2 Tunnel name: tunnel1

Node 2 Tunnel Link Status:

GeneralMembersPoliciesGroup To Group Policies

CAC group configuration

Group Type: Subnets

CAC group Member(s) List

Use the buttons to add or remove Members from the Group. The Group can only contain Members of the type you have selected above.

Elements Per Page: 200

2 Items

<input type="checkbox"/>	CAC Group Members
<input type="checkbox"/>	10.100.180.0/24
<input type="checkbox"/>	27.27.0.0/16

- **Add the CAC policy and limit based on 'Bandwidth'. Enter '0' for the Backup Max Bandwidth value.**

Policy configuration

In this section the specified policy can be activated and configured.

Limit Type: Bandwidth

Max number of calls:

Backup Max number of calls:

Max Bandwidth (kbps): 1000000

Backup Max Bandwidth (kbps): 0

Max Bandwidth is defined for the WAN interface, which can be configured with the max value (1000000) supported by OSV.

Backup Max Bandwidth must be set to zero '0'.

The Srx/Lsm/CheckRouter flag can be set to RtpFalse or RtpTrue, depending on Data Center Router configuration. Check Appendix A for more details of router configuration. If true, the Data Center Router is queried for the current tunnel status when the synchronization timer expires. If false, the Tunnel status timestamp is simply reset.

- **Configure the BLS1 and BLS2 IP Address in Data Center Router SNMP Configuration entry in the OpenScape Voice.**

This is only possible via StartCli.
Select the following options:

Application-level Management. 6
Network Traffic Management. 9
Call Admission Control Management. 1
CAC Access Link Status Monitoring. 6
Modify Data Center Router SNMP Configuration. 3

Enter the IP address of the BLS1 as the Data Center Router 1, the IP address of the BLS2 as the Data Center Router 2 and default values for all other parameters.

```
Modify settings for DCR 1 <(y/n)> ? (default:y): y
Data Center Router IPv4 Address <(max length: 46)> (default: 0.0.0.0): 10.10.1.1
oSnmpv2c Community string <(max length: 2048)> (default: public): public
Snmp version used to access router < 2 = Snmpv2c, 3 = Snmpv3 >: 2
```

```
Modify settings for DCR 2 <(y/n)> ? (default:y): y
Data Center Router IPv4 Address <(max length: 46)> (default: 0.0.0.0): 10.20.1.1
oSnmpv2c Community string <(max length: 2048)> (default: public): public
Snmp version used to access router < 2 = Snmpv2c, 3 = Snmpv3 >: 2
```

```
Modify settings for DCR 3 <(y/n)> ? (default:y): n Modify
settings for DCR 4 <(y/n)> ? (default:y): n
```

The Data Center Router SNMP configuration should look like this once completed:

Data Center Router 1 SNMP Configuration:

```
Username: None
Authentication Key: None
Authentication Protocol: None SnmpV2c
Community String: public IPv4
Address: 10.10.1.1
Sends Snmpv2 Traps/Informs: true
```

Data Center Router 1 tunnel IP

Data Center Router 1 SNMP Configuration:

```
Username: None
Authentication Key: None
Authentication Protocol: None SnmpV2c
Community String: public IPv4
Address: 10.20.1.1
Sends Snmpv2 Traps/Informs: true
```

Data Center Router 2 tunnel IP

Note: In this documentation, OpenScape Voice is using SNMPv2c to traps/informs. However, SNMPv3 is also allowed. For configuration of SNMP parameters for SNMPv3, check for documentation “Link Status Manager (LSM)” that can be found at Wiki-LIP Development Published Website.

- All the branches must have a CAC Group configured.

[OSV4R1DQ6EO]- CAC Groups

This list shows all existing Routing Call Admission Control Groups.

Search for: in Elements Per Page:

2 Items

<input type="checkbox"/>	CAC group name	Member Type	Parent Cac Group	Monitored Link Type	Monitored Link Status
<input type="checkbox"/>	CAC_NET180_OSB1000	Subnets		Data center tunnel	Node1 link up, Node2 link up
<input type="checkbox"/>	CAC_NET22_OSB50i	Subnets		Data center tunnel	Node1 link up, Node2 link up

Subscriber Rerouting Configuration

65.5.1.2 Activate Rerouting and configure Prefix Access Code

- **Go to OpenScope Voice -> Administration -> Signaling Management -> SIP Under**

Rerouting Tab:

Set the Subscriber Rerouting Prefix Access Code

Enable Rerouting for SIP Subscribers

SIP Settings

General **Rerouting** **SIP Timers** **Best Effort SRTP** **FQDN**

Rerouting

Although using Subscriber Rerouting through the PSTN is useful during WAN failures & CAC bandwidth restrictions, it can also lead to additional charges for the PSTN calls. For more information, see the OpenScope Voice documentation.

Enable Rerouting for SIP Subscribers: ☒

Subscriber Rerouting Prefix Access Code: Enter a desired prefix.

International:

National:

Local:

65.5.1.3 Configure Branch Office for Remote Branch

Follow the same steps used for the configuration for Simplex/Collocated (item 3.1.2.2).

NOTE: All subscribers in the remote branch must be added to their respective branch office.

65.5.1.4 Configure Branch Office for Data Center 1

- **First, create a virtual endpoint and use it as a representative Endpoint for the Data Center's Branch Office of Primary Node.**

NOTE: Add all Data Center 1 subscribers to this branch office. For all those subscribers kept in the 'Main Office' calls will only work in the direction from data center to branch office.

- **Following the same configuration for Simplex/Collocated, enable the Survivable Endpoint and “Do not audit endpoint” attributes.**

The screenshot shows the 'Attributes' tab in the OpenScope configuration interface. The 'Survivable Endpoint' checkbox is checked and highlighted with a red box. The 'Do Not Audit Endpoint' checkbox is also checked and highlighted with a red box. Other attributes like 'Supports SIP UPDATE Method for Display Updates', 'UPDATE for Confirmed Dialogs Supported', 'Send Provisional response during session updates', 'SIP Proxy', 'Route via Proxy', 'Allow Proxy Bypass', 'Use Proxy/SBC ANAT settings for calls to subscribers', 'Support for Callback Path Reservation', and 'Send Progress to Stop Call Proceeding Supervision Timer' are listed but not checked.

NOTE: For previous OSV versions, the configuration of “Do Not Audit Endpoint” flag can only be done via StartCli. In this case, select the following options:

Application-level Management. 6

Zone Management. 5

Modify Endpoint. 2

- Set the “Do not audit Endpoint” to “true”

Change SIP endpoint attributes as bitmap sums? (default: true): false

Do not audit Endpoint <0=false/1=true/-1=unchanged> (default: -1): 1

- **Create the Branch Office using the virtual endpoint just created.**

Go to OpenScope Voice -> Business Group -> Branch Offices List and select the branch office Assign a Routing Area and a DID Pool.

NOTE: The subscribers selected in this pool cannot be used for anything else.

The screenshot shows the 'General' tab for a Branch Office configuration. The 'Branch Office Name' is 'BO_Data_Center1', 'Representative Endpoint' is 'Virtual_EP_DC1', 'Numbering Plan' is 'NP_BG_DQ_OSB', 'Office Code' is empty, 'Routing Area' is 'ra_DataCenter1', and 'This is a Branch Office of type OpenScope Branch' is checked. A yellow callout box points to the 'Routing Area' field with the text 'Assign a Routing Area to Data Center Router.' The 'DID Pool' tab is also visible, showing a list of subscribers with a yellow callout box stating 'Select subscribers. These cannot be used for anything else.'

- **Ensure the DID Home DNs selected for the DID Pool are set to “Service” type “DID Pool Number”.**

This is done automatically by Assistant when the Home DN is selected for the DID Pool. To verify the service is set check the DN in the Home DN Table (Global Translation and Routing -> Home Directory Numbers)

65.5.1.5 Configure Branch Office for Data Center 2

Create a Branch Office virtual Endpoint for Data Center 2 following the same procedure of Data Center 1.

The screenshot shows the 'General' tab for a virtual endpoint configuration. The 'Name' is 'Virtual_EP_DC2', 'Remark' is 'Virtual Endpoint for Data Center subscribers. Used for Enhanced Subscriber Rerouting (branch to DC)', 'Registered' is checked, 'Profile' is 'EPP_Data_Center2', 'Branch Office' is empty, 'Associated Endpoint' is empty, 'Default Home DN' is empty, and 'Location Domain' is empty. A yellow callout box points to the 'Endpoint Address' field in the 'SIP Signaling' tab with the text 'Enter an inexistent IP address'. The 'SIP Signaling' tab shows 'Type' as 'Static', 'Signaling Address Type' as 'IP Address or FQDN', 'Endpoint Address' as '1.1.1.2', 'Port' as '5060', 'Transport protocol' as 'TCP', 'Best Effort SRTP support' as 'MIKEY,SDS', 'ANAT Support' as 'Enabled', and 'Use Proxy/SBC Best-Effort SRTP settings for calls to subscribers' is checked.

NOTE: Add all Data Center 2 subscribers to this branch office. For all those subscribers kept in the 'Main Office' calls will only work in the direction from data center to branch office.

- ***As before, enable the Survivable Endpoint and “Do not audit endpoint” attributes.***

General	SIP	Attributes	Aliases	Routes	Accounting
Attributes					
Attributes available for this SIP endpoint					
Supports SIP UPDATE Method for Display Updates			<input type="checkbox"/>		
UPDATE for Confirmed Dialogs Supported			<input type="checkbox"/>		
Send Provisional response during session updates			<input type="checkbox"/>		
Survivable Endpoint			<input checked="" type="checkbox"/>		
SIP Proxy			<input type="checkbox"/>		
Route via Proxy			<input type="checkbox"/>		
Allow Proxy Bypass			<input type="checkbox"/>		

Do Not Audit Endpoint	<input checked="" type="checkbox"/>
Use Proxy/SBC ANAT settings for calls to subscribers	<input type="checkbox"/>
Support for Callback Path Reservation	<input type="checkbox"/>
Send Progress to Stop Call Proceeding Supervision Timer	<input type="checkbox"/>

- **Create the Branch Office for Data Center 2 using the virtual endpoint just created as like as for Data Center 1.**

NOTE: The subscribers selected in this pool cannot be used for anything else.

General | **DID Pool** | **Access Control List**

General

Branch Office Name: BO_Data_Center2

Representative Endpoint: Virtual_EP_DC2

Numbering Plan: NP_BG_DQ_OSB

Office Code:

Routing Area: ra_DataCenter2

This is a Branch Office of type OpenScope Branch

Assign a Routing Area to Data Center Router.

DID Pool

Select the DID Pool of the Branch Office

Elements Per Page: 200

3 Items

Add Range... Add... Delete

Directory Number
554133411997
554133411998
554133411999

Select subscribers. These cannot be used for anything else.

65.5.1.6 Configure Destinations to Gateways serving all branches and Data Center

- **Add a Destination to the Gateway in the Data Center 1**

If not existent, add a destination to go to the endpoint for the gateway at the Data Center 1

General | **Routes** | **Route Lists** | **Destination Codes**

Name: RG8700_DC1_Dest

is a media server: ☐

General | **Routes** | **Route Lists** | **Destination Codes**

Routes

Multiple routes can be used for prioritizing the routes to the gateways.

Add... Edit...

Sel:0 | Items/Page: 200 | All:1

ID	Endpoint	Route Type	Delete	Insert	Nature of Address
1	RG8700_PSTN_DC1	SIP-Endpoint	0		Undefined

- **Add a Destination to the Gateway in the Data Center 2**

If not existent, add a destination to go to the endpoint for the gateway at the Data Center 2

General
Routes
Route Lists
Destination Codes

Name: RG8700_DC2_Dest

is a media server: ☐

General
Routes
Route Lists
Destination Codes

Routes

Multiple routes can be used for prioritizing the routes to the gateways.

Add...
Edit...
Delete

Sel: 0 | Items/Page: 200 | All: 1

	ID	Endpoint	Route Type	Delete	Insert	Nature of Address
<input type="checkbox"/>	1	RG8700_PSTN_DC2	SIP-Endpoint	0		Undefined

- **Add a Destination for each Gateway serving a Branch**

NOTE: Use symmetric routing (GW behind proxy) and make destination point to the proxy (OSB).

If using asymmetric routing (OSV talks directly to GW in branch) calls in backup mode can fail, because OSV may audit and set gateway as inaccessible during an outage.

General
Routes
Route Lists
Destination Codes

Name: OB2250i_BLC_DES

is a media server: ☐

General
Routes
Route Lists
Destination Codes

Routes

Multiple routes can be used for prioritizing the routes to the gateways.

Elements Per Page: 100

	ID	Endpoint	Route Type	Delete	Insert	Nature of Address
<input type="checkbox"/>	1	bocaOB22-OSB50i	SIP-Endpoint	0		Undefined

65.5.1.7 Configure a Code Index

- **Add a Code Index for Rerouting**

Code Index

General

Patterns

Identification

Text for the Code Index Identification info box. Note: No more than 15 charac

Code Index Name:

CI_Local_Gwy

Remark:

Nature Of Address:

Code Index

Following the same configuration steps for Simplex/Collocated configuration (see 3.1.2), add a pattern to point to both Data Center Gateway (for calls from data center to branch) and for all branches.

NOTE: One Data Center must have “empty” Routing Area.
The gateway in the branch must be configured for symmetric signaling (GW is behind proxy)

The Code Index will then have multiple patterns.
For each branch with a Routing Area and with no Routing Area for one of the Data Centers.

General

Patterns

A pattern associates a rate area and a class of service with a destination.

Patterns

Add...

Edit...

Delete...

Sel:0 | Items/Page: 200 | All:4

	Routing Area	Class Of Service	Destination
<input type="checkbox"/>		← Data Center 1 has “empty” Routing	RG8700_DC1_Dest
<input type="checkbox"/>	ra_DataCenter2		RG8700_DC2_Dest
<input type="checkbox"/>	ra_osb50i-PRI		osb50i_PRI_dest
<input type="checkbox"/>	ra_osb1k-BLC ← Enter the Branch's Routing Area.		osb1k_BLC_dest

65.5.1.8 Configure Routing to the Code Index

- **Add Prefix Access Code for the Subscriber Rerouting PAC**

Go to OpenScape Voice -> Business Group -> Default Numbering Plan
Under Translation add the Prefix Access Code

The screenshot shows the 'Edit Prefix Access Code' configuration window. The title bar reads '[BOCAST1] - [BGCA] - [NP_BGCA] - Edit Prefix Access Code: 8'. The window is divided into two main sections: 'Identification' and 'Settings'.


Identification Section:

- A blue information icon is followed by the text: 'If the dialed digits match this code, the specified modification to these dialed digits is executed.'
- Prefix Access Code:** A text input field containing the value '8'.
- Remark:** A large, empty text area.
- Minimum Length:** A text input field containing the value '8'.
- Maximum Length:** A text input field containing the value '15'.
- Digit Position:** A text input field containing the value '0'.
- Digits to insert:** An empty text input field.


Settings Section:


- A blue information icon is followed by the text: 'Specify additional parameters to determine how the call will be routed.'
- Prefix Type:** A dropdown menu with 'Off-net Access' selected.
- Nature of Address:** A dropdown menu with 'Unknown' selected.
- Destination Type:** A dropdown menu with 'None' selected.
- Destination Name:** An empty text input field followed by a button with three dots '...'.

- **Add a Destination Code to point to the Code Index created for re-routing**
(Note: Nature of Address must be International for number normalization if using Mobile UC Clients on the Branches)

 [BOCAST1] - [BGCA] - [NP_BGCA] - Edit Destination Code: 8

General
Extensions


 This destination code will be used for a call if the dialed or modified (in PAC) digits and the Nature of Address are specified.

Destination Code: 


Remark:


Country Code:


Nature Of Address:

Traffic Type: 

Originator Attributes


 Optionally, an additional match is required if the originator of the call belongs to the specified Class of Service.


Class Of Service: 


Routing Area: 


NPA:

Destination

 Specify additional parameters to determine how the call will be routed.

Destination Type: 



Code Index Name: 

DN Office Code: 

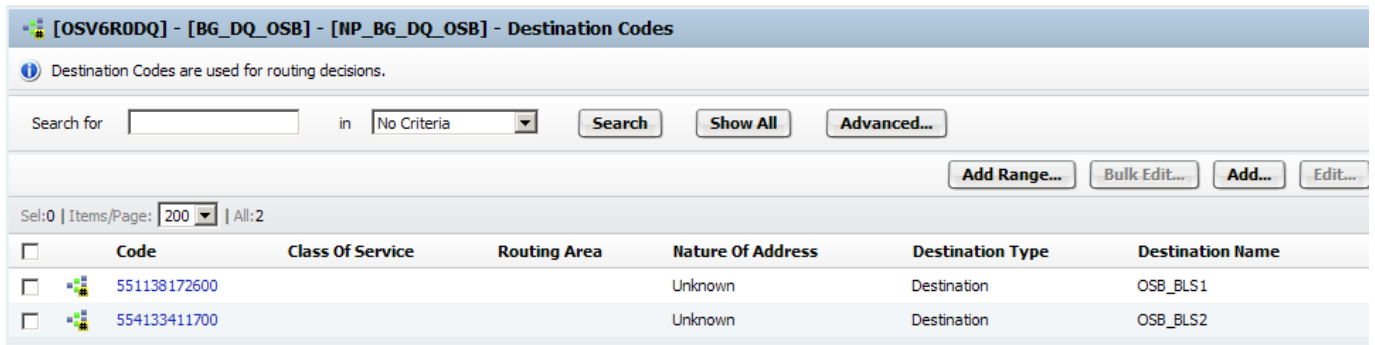
65.5.1.9 Configuration of Routing to BLS DID number

- **Add a Destination OSB-BLS1 from Data Center 1 and another Destination OSB-BLS2 from Data Center 2:**

Go to OpenScope Voice -> Business Group -> Destination and Routes -> Destinations

<input type="checkbox"/>	Name ▲	Media Server	Number of Routes
<input type="checkbox"/>	 OSB_BLS1	False	1
<input type="checkbox"/>	 OSB_BLS2	False	1

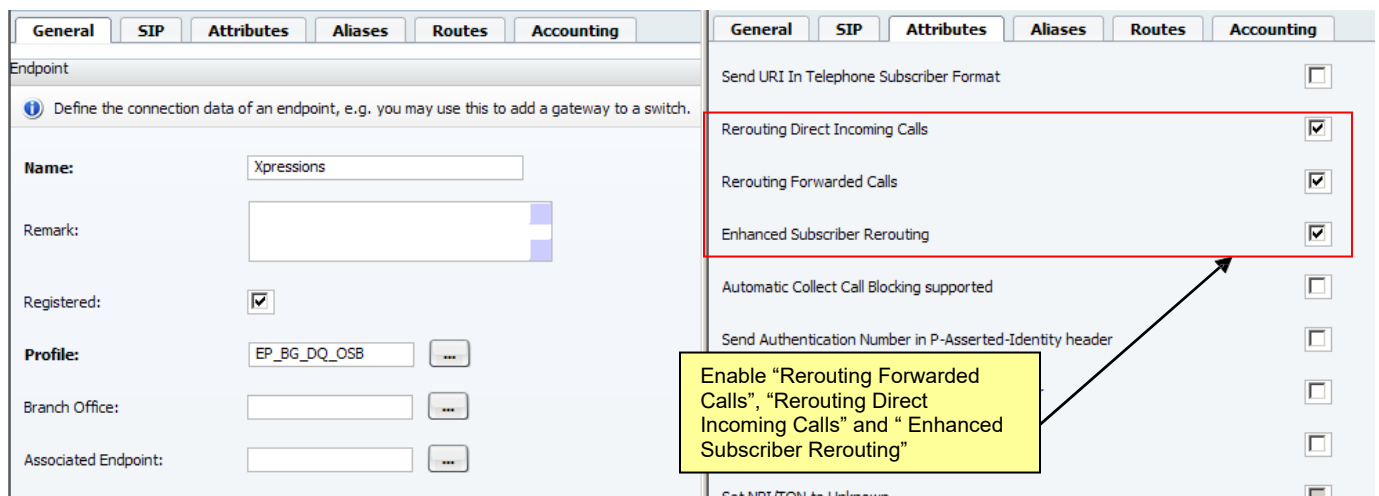
- **Following the procedure for a Simplex / Collocated (see 3.1.3), create a PAC and Destination Code for OSB-BLS1 and OSB-BLS2.**



Code	Class Of Service	Routing Area	Nature Of Address	Destination Type	Destination Name
551138172600			Unknown	Destination	OSB_BLS1
554133411700			Unknown	Destination	OSB_BLS2

65.5.2 Configuration of Voice Mail Rerouting (optional)

Follow the same procedure used for a Simplex / Collocated configuration (see 3.1.4)



Endpoint

Define the connection data of an endpoint, e.g. you may use this to add a gateway to a switch.

Name: Xpressions

Remark:

Registered: ☒

Profile: EP_BG_DQ_OSB

Branch Office:

Associated Endpoint:

Send URI In Telephone Subscriber Format ☐

Rerouting Direct Incoming Calls ☒

Rerouting Forwarded Calls ☒

Enhanced Subscriber Rerouting ☒

Automatic Collect Call Blocking supported ☐

Send Authentication Number in P-Asserted-Identity header ☐

Set NPT/TON to Unknown ☐

Enable "Rerouting Forwarded Calls", "Rerouting Direct Incoming Calls" and "Enhanced Subscriber Rerouting"

NOTE 1: If gateways are used for networking with PSTN, do not enable "Rerouting Direct Incoming Calls" because it may lead to loops with PSTN.

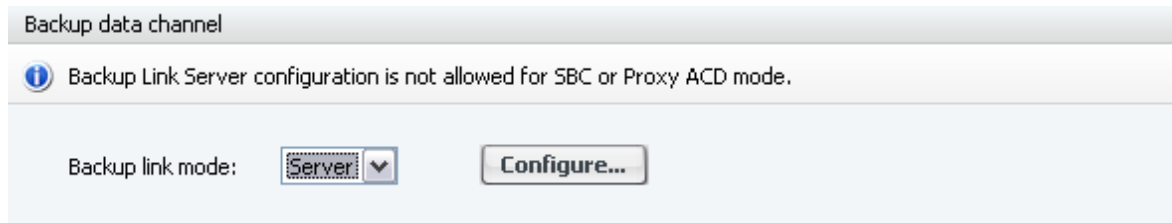
NOTE 2: Only one Voice Mail can be used for both Data Centers. However, if Voice Mail Server is located on Data Center 1 then an alternate route to a redundant Voice Mail EndPoint on Data Center 2 is desired.

65.5.3 Configuring the OpenScape Branch for Backup Data Link Support

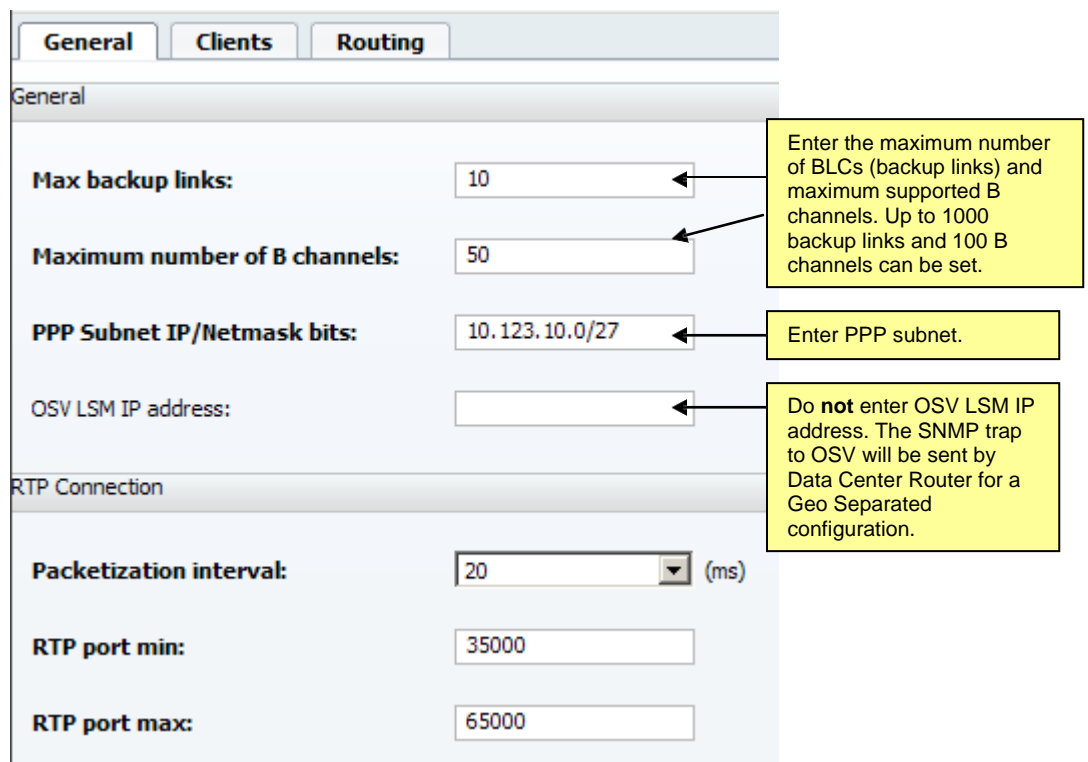
65.5.3.1 Backup Link Server 1 (BLS1) Configuration:

Follow the same procedure used to create BLS for Simplex/Collocated.

- **After login to the OSB Assistant go to the OpenScape Branch -> Configuration -> VoIP option and under General select “Server” for Backup link mode and click on “Configure...”:**



- **Enter desired values for the General area:**



NOTE 1: The configuration of “PPP Subnet IP/Netmask bits” should be enough to fit the amount of BLC devices on the network. To have this, the number of hosts must be at least 2 times the number configured for “Max backup links” (this is because each backup link has one PPP address for BLS and other for BLC).

For example, in the subnet 10.123.10.0/27 we have 32 PPP addresses (10.124.10.0 to 10.124.10.31) that must be greater or equal to 2 times the number configured in “Max backup link” (in this case up to 16 BLCs are possible with this subnet).

NOTE 2: The PPP subnet IP addresses shall not conflict with any IP/subnets in the branch or data center

- Under **Clients** tab area, click on “Add” and create the tunnel for each BLC.

The screenshot shows the 'Clients' tab in a configuration interface. It has tabs for 'General', 'Clients', and 'Routing'. Below the tabs are buttons for 'Add...', 'Edit...', and 'Delete'. A status bar shows 'Sel:0 | Items/Page: 200 | All:2'. Below this is a table with the following data:

	Tunnel name	BLC Host Name	Priority	Retry-after
<input type="checkbox"/>	tunnel1	BO-OSB50i-PRI-01	1	120
<input type="checkbox"/>	tunnel2	BO-OSB1000-BLC	2	600

- Under **VoIP** -> **General** -> **Gateways** click on “Configure...”. Enter the following line in the Gateway Table:

The screenshot shows the 'Gateways' tab in a configuration interface. It has buttons for 'Add...', 'Edit...', and 'Delete'. A status bar shows 'Sel:0 | Items/Page: 200 | All:1'. Below this is a table with the following data:

	Signaling Address Type	IP Address/FQDN	Port	Interface	Transport	Routing Prefix/FQDN	Type	Functional type	Trunk Profile	Output digit strip	Output digit add	Priority
<input type="checkbox"/>	IP Address or FQDN	10.100.123.20	5086	LAN	UDP	551138172600	Backup Link Server	All Modes Egress/Ingress	Gateway	0		

- Under **VoIP** -> **Comm System** -> **Configure BLS1** at the OSV Node in the same Data Center Router 1:

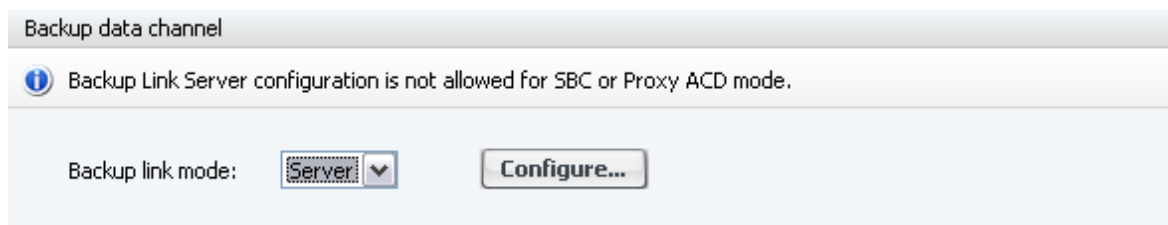
The screenshot shows the 'Comm System' configuration page. It has tabs for 'General', 'Comm System', 'Timers and Thresholds', and 'Codecs'. The 'General' tab is selected. There are two main sections: 'General' and 'Node 1'.
 In the 'General' section, the 'Comm System Type' is set to 'Simplex'. A yellow box with an arrow points to this dropdown with the text: 'Enter System Type as Simplex'.
 In the 'Node 1' section, the 'Primary server' is set to 'node1.dc1.osv'. A yellow box with an arrow points to this text field with the text: 'Set the IP address or FQDN of Node located on the same Data Center than OSB-BLS. For TCP and UDP, set OSV sipasm1. For TLS, OSV sipasm3 should be used.'.
 Other fields include 'Outbound SIP server' (Node 1), 'Outbound proxy port' (5060), and 'Target type' (Binding).

Note: Even though we have a Geo Separated environment, we should configure OSV System Type as Simplex, pointing to the Node collocated on the same Data Center. This is because in a case of Node failure, BLS should be in Survivable Mode.

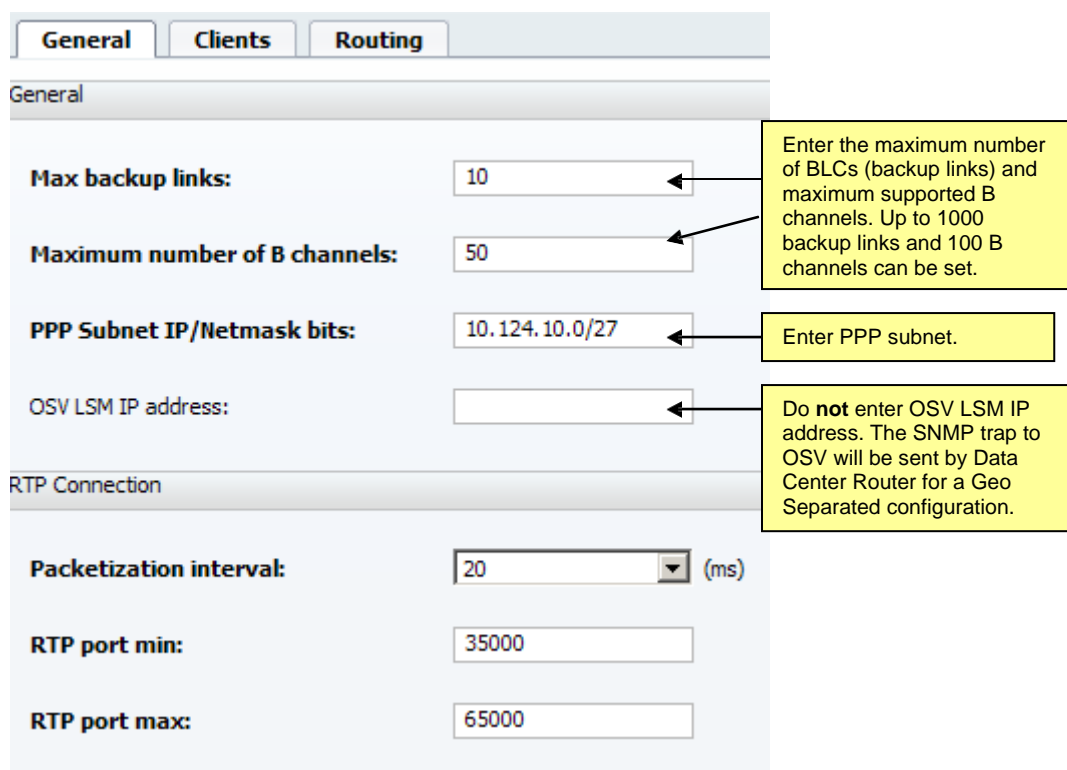
65.5.3.2 Backup Link Server 2 (BLS2) Configuration:

Repeat the procedure for BLS2.

- **After login to the OSB Assistant go to the OpenScape Branch -> Configuration -> VoIP option and under General select “Server” for Backup link mode and click on “Configure...”:**



- **Enter desired values for the General area:**



- Under **Clients** tab area, click on “Add” and create the tunnel for each BLC (same than BLS1)

The screenshot shows the 'Clients' configuration tab. At the top, there are tabs for 'General', 'Clients', and 'Routing'. Below the tabs, there are buttons for 'Add...', 'Edit...', and 'Delete'. A status bar shows 'Sel:0 | Items/Page: 200 | All:2'. Below this is a table with the following columns: Tunnel name, BLC Host Name, Priority, and Retry-after.

	Tunnel name	BLC Host Name	Priority	Retry-after
<input type="checkbox"/>	tunnel1	BO-OSB50i-PRI-01	1	120
<input type="checkbox"/>	tunnel2	BO-OSB1000-BLC	2	600

Note: The configuration must be the same than BLC1 for values under Clients tab.

- Under **VOIP -> General -> Gateways** click on “Configure...”. Enter the following line in the Gateway Table

The screenshot shows the 'Gateways' configuration table. At the top, there are buttons for 'Add...', 'Edit...', and 'Delete'. A status bar shows 'Sel:0 | Items/Page: 200 | All:1'. Below this is a table with the following columns: Signaling Address Type, IP Address/FQDN, Port, Interface, Transport, Routing Prefix/FQDN, Type, Functional type, Trunk Profile, Output digit strip, Output digit add, and Priority.

	Signaling Address Type	IP Address/FQDN	Port	Interface	Transport	Routing Prefix/FQDN	Type	Functional type	Trunk Profile	Output digit strip	Output digit add	Priority
<input type="checkbox"/>	IP Address or FQDN	10.100.124.50	5086	LAN	UDP	55413411700	Backup Link Server	All Modes Egress/Ingress	Gateway	0		

- Under VoIP -> Comm System -> Configure BLS2 at the OSV Node in the same Data Center Router2:

The screenshot shows the 'Comm System' configuration page. At the top, there are tabs for 'General', 'Comm System', 'Timers and Thresholds', and 'Codecs'. The 'General' tab is selected. Below the tabs, there are fields for 'Comm System Type' (set to 'Simplex'), 'Outbound SIP server' (set to 'Node 1'), 'Enable outbound proxy' (unchecked), 'Outbound proxy port' (set to '5060'), and 'Enable path tagging' (unchecked). There is a 'Configure...' button next to the 'Comm System Type' field. Below this, there is a section for 'Node 1' with fields for 'Target type' (set to 'Binding'), 'Primary server' (set to 'node2.dc2.osvi'), 'Secondary server' (empty), and 'SRV record' (empty). There are also fields for 'Transport' (set to 'TCP') and 'Port' (set to '5060').

Enter System Type as Simplex

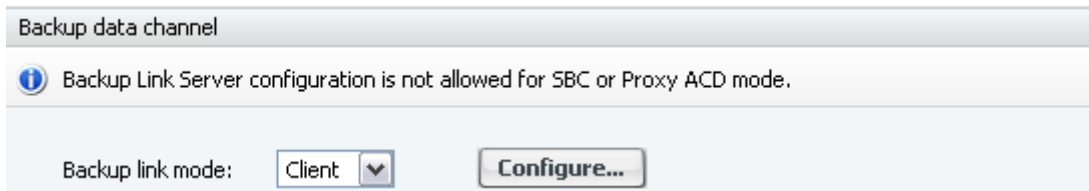
Set the IP address or FQDN of Node located on the same Data Center than OSB-BLS. For TCP and UDP, set OSV sipism2. For TLS, OSV sipism4 should be used.

Note: Even though we have a Geo Separated environment, we should configure OSV's System Type as Simplex, pointing to the Node collocated on the same Data Center. This is because in a case of Node failure, BLS should go to Survivable Mode.

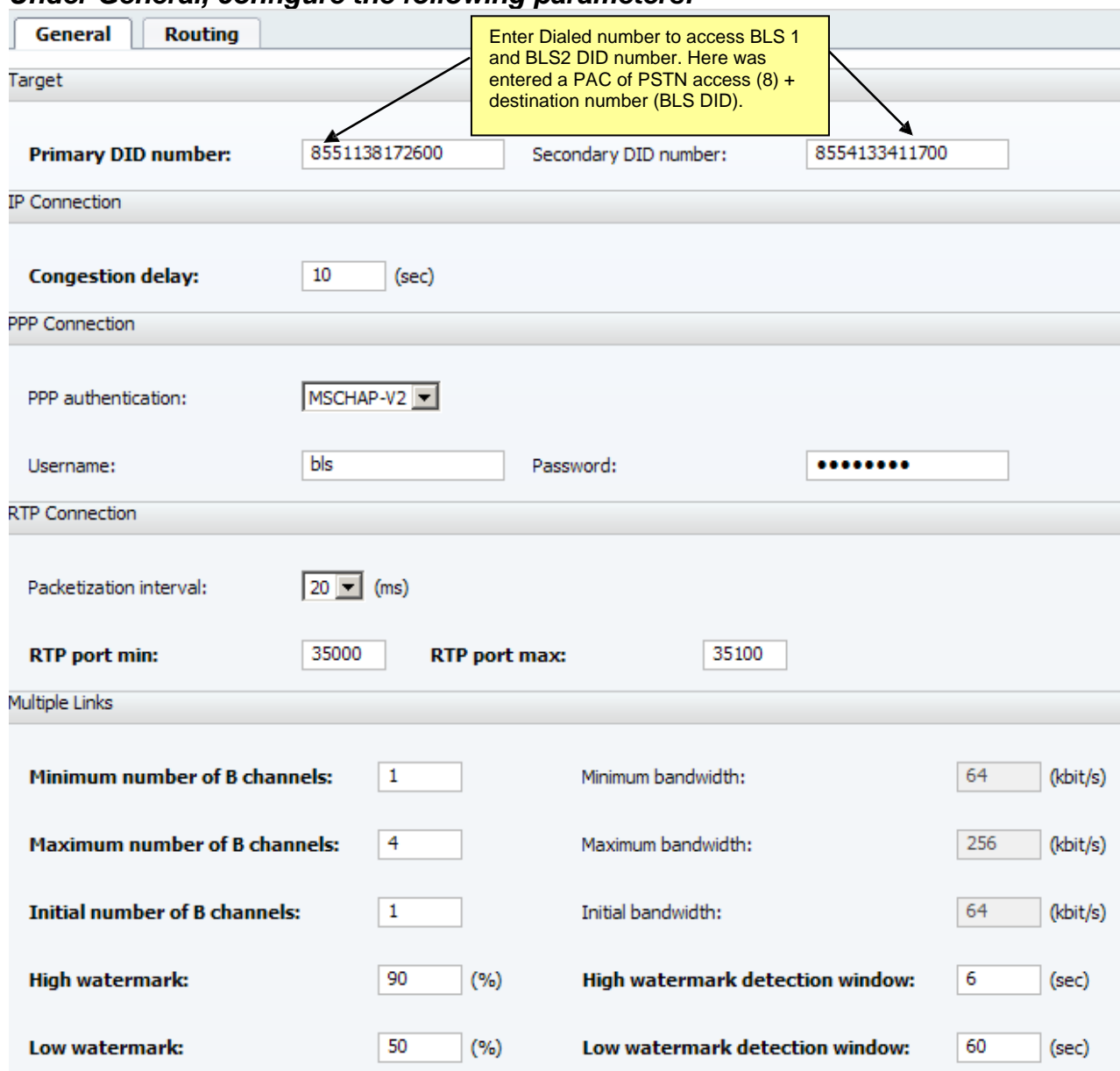
65.5.3.3 Backup Link Client (BLC) Configuration:

The following are the configuration steps for the OpenBranch located in the Branch (BLC). (Supported OpenScope Branch modes are Proxy, SBC and SBC-Proxy only)

- **After login to the OSB Assistant go to the VOIP option and under General select “Client” for Backup link mode and click on “Configure...”:**



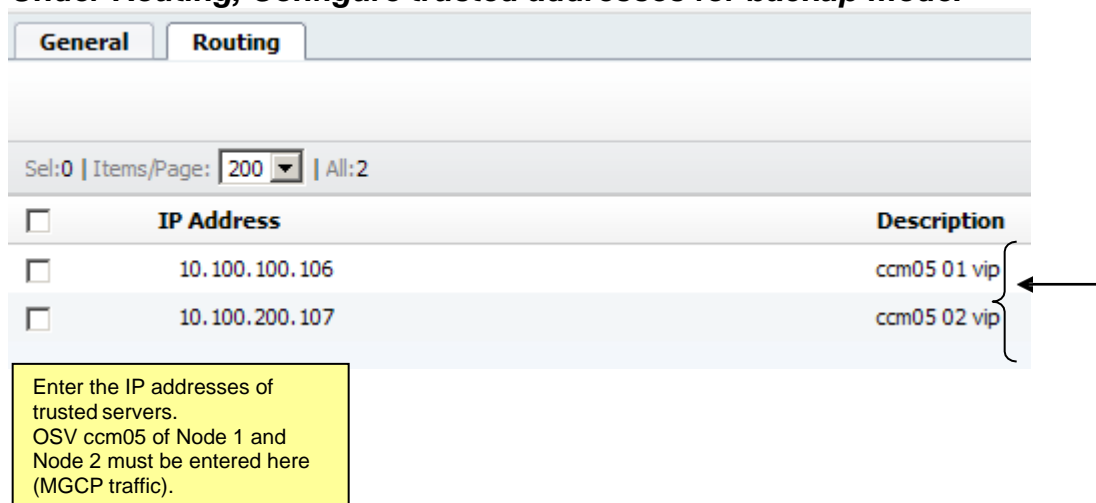
- **Under General, configure the following parameters:**



General		Routing	
Target			
Primary DID number:	8551138172600	Secondary DID number:	8554133411700
IP Connection			
Congestion delay:	10	(sec)	
PPP Connection			
PPP authentication:	MSCHAP-V2		
Username:	bls	Password:	••••••••
RTP Connection			
Packetization interval:	20	(ms)	
RTP port min:	35000	RTP port max:	35100
Multiple Links			
Minimum number of B channels:	1	Minimum bandwidth:	64 (kbit/s)
Maximum number of B channels:	4	Maximum bandwidth:	256 (kbit/s)
Initial number of B channels:	1	Initial bandwidth:	64 (kbit/s)
High watermark:	90 (%)	High watermark detection window:	6 (sec)
Low watermark:	50 (%)	Low watermark detection window:	60 (sec)

- NOTE 1:** If multilink achieves 100 % of bandwidth usage, BLS will detect a state of congestion and will send an order to BLC immediately add a new channel, if possible, irrespectively of the High Watermark configuration. During congestion, new calls will be rejected with a retry-after timer response.
- NOTE 2:** If BLC is using TCP or UDP as SIP transport protocol, PPP tunnel is compressed. For TLS, the channels are uncompressed.
- NOTE 3:** If BLC is connected to OSV Node 1 as Primary, so the preferable Primary DID number should be the number to access BLS1 located on the same Data Center than OSV Node 1. If BLC is connected to the OSV Node 2 as Primary, then the preferable Primary DID number should be the number to access BLS2 located on the same Data Center than OSV Node 2.
- NOTE 4:** While in Backup Mode, BLC will create only one route to BLS1 or BLS2. For example, if BLS1 on Data Center 1 is connected, Data Center 2 is considered as out of service.

- **Under Routing, Configure trusted addresses for backup mode.**



IP Address	Description
10.100.100.106	ccm05 01 vip
10.100.200.107	ccm05 02 vip

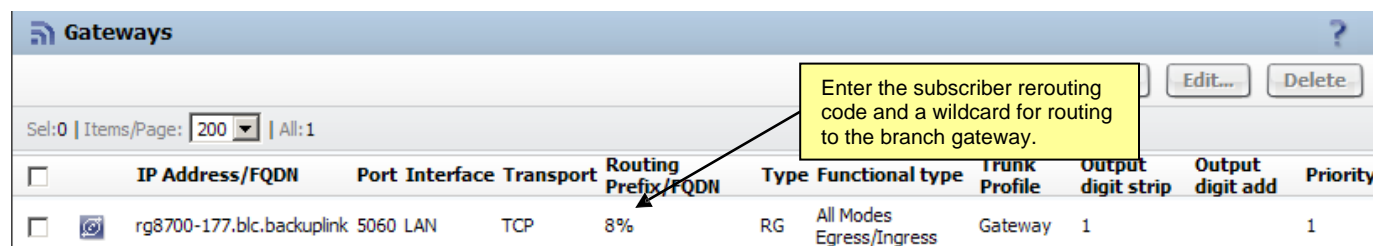
Enter the IP addresses of trusted servers.
OSV ccm05 of Node 1 and Node 2 must be entered here (MGCP traffic).

Note: OSV's SIPSM node address and SNMP trap destination are already trusted and must not be entered here. A maximum of 6 addresses are allowed.

In OpenScope Branch under the Gateway Table configure the BLC to route the call to the gateway when receiving the configured subscriber rerouting access code:

- **Under VOIP -> General -> Gateways click on "Configure..."**

Verify routing to the DID is configured in the gateway configuration:



IP Address/FQDN	Port	Interface	Transport	Routing Prefix/FQDN	Type	Functional type	Trunk Profile	Output digit strip	Output digit add	Priority
rg8700-177.blc.backuplink	5060	LAN	TCP	8%	RG	All Modes Egress/Ingress	Gateway	1		1

Enter the subscriber rerouting code and a wildcard for routing to the branch gateway.

Note 1: In this case, only one routing rule was created because the prefix access code to dial DID in Survivable Mode is the same as the code for rerouting in Normal Mode. If not, more routing rules should be entered.

Note 2: Gateways must support clearmode. This is also referred to as clear-channel data or 64 Kbit/s unrestricted". If OSB 50i PRI is used, check if "data calls allowed" flag is enable (go to CMP on OpenScope Branch -> Integrated Gateway -> General -> Configuration, Edit the PRI link and check for flag)

- **Add a SNMP trap to CMP server. This is used to inform CMP that OpenScape Branch started or stopped backup mode.**

Go to Alarms -> Trap Destinations

Add trap destination SNMP

IP Address: 192.168.80.117

Port: 162

Reporting class set: 7

Blocked: ☐

This is the IP address of CMP management

- **Under VoIP -> Comm System -> Configure BLC to access a Geo Separated OpenScape Voice**

General | **Comm System** | Timers and Thresholds | Codecs | RTP

General

Comm System Type: Geo-Separated

Outbound SIP server : Node 1

Node 1

Target type: SRV record

Primary server:

Secondary server:

SRV record : dc1.osv6r0.br

Transport: TCP

Port: 0

Node 2

Target type: SRV record

Primary server:

Secondary server:

SRV record : dc2.osv6r0.br

Transport: TCP

Port: 0

Set Geo-Separated

Always choose Node1

SRV record is preferred for Geo Separated configurations

Note 1: If BLC is using TCP or UDP as SIP transport protocol, PPP tunnel is compressed. For TLS, the channels are uncompressed.

Note 2: For TCP, BLC should point traffic to sipsm1/sipsm2. In case of TLS, sipsm3/sipsm4 are preferred.

65.5.4 Survivability Mode Avoidance

As like configured for Simplex/Collocated configuration, it is suggested that some configurations are made on timers and thresholds.

For transition from Normal Mode to Backup Mode on Geo-Separated configurations, it must be considered that 120 seconds are necessary for BLC goes to Normal Backup Mode. This is the double of the time configured for Simplex/Collocated systems, because in the worst case, OSB-BLC will look for a valid connection on two BLS (looks for Secondary BLS only if Primary fails).

So, for an optimized configuration, Timers and Thresholds values of Survivability Provider should be configured as follows:

- **Under OpenScape Branch -> VoIP -> Timers and Thresholds:**

General Comm System **Timers and Thresholds** Codecs RTP

Timers and Thresholds

Failure threshold: 3 (pings) OPTIONS interval: 40 (sec)

Success threshold: 1 (pings) OPTIONS request timeout: 10 (sec)

Transition Mode threshold: 3 (pings) Notification Rate: 10

To have a fast transition, OPTIONS interval should be the lowest possible. The minimum value is 11 seconds. Please see Note1 below*.

To avoid unnecessary transitions, use these values. The minimum OPTIONS value is 10 seconds. Please see Note2 below**.

Increase the transition mode threshold to 3, to have a lower OPTIONS interval. Please see Note1 below*.

***NOTE 1:** OPTIONS interval value should be long enough to avoid survivable mode on the transition from Normal to Backup Mode and at the same time the lowest possible value to have a fast transition to Normal Backup Mode. So, the timers and thresholds must be configured according to the following formula:

$$Mtt \leq Tt * Oi + (Tt - 1) * Ot$$

Where:

Mtt = Maximum time in transition mode (60 seconds if only Primary link is configured – Simplex or Collocated

- or 120 seconds if also Secondary link is configured – Geo Separation)

Tt = Transition Mode threshold

Oi = OPTIONS interval (min. 11 sec.)

Ot = OPTIONS timeout (min. 10 sec.)

If the criteria are not fulfilled, system will show an error message.

****NOTE 2:** If BLC is in Normal Backup Mode, unnecessary system transitions due to network issues, like packet losses, TCP retransmissions and others should be avoided. So, to optimize the link transition, we must consider that Failure threshold (pings) multiplied by OPTIONS timeout (sec) must be at least 30 seconds.

66 Data Center Router Settings for Geo Separated Configuration

In the configuration of Data Center Router, the following requisites must be attended:

SNMP Configuration

WAN Monitoring

Alternate routing to Backup Link Server

Note: In this configuration a Cisco Router is used, following the recommendations from BO2707 - Back-up Link for Survivable Branch for Free Media Choice.

66.1 SNMP Configuration

This configuration is used to Data Center Router to send a trap to OpenScape Voice and OSV pools information from DCR status. This trap and inform can use SNMPv2c or SNMPv3. In this document, it is shown the configuration for SNMPv2c.

Configuration on DC Router 1 at OpenScape Voice Node 1 (LSM IP Address is 10.100.100.8):

```
snmp-server community public ro
snmp-server enable traps snmp linkdown linkup
snmp-server user public V2C-Group v2c
snmp-server group V2C-Group v2c
snmp-server host 10.100.100.8 informs version 2 public udp-port 8160 snmp
snmp-server host 10.100.100.8 version 2c public udp-port 8160 snmp
```

Configuration on DC Router 2 at OpenScape Voice Node 2 (LSM IP Address is 10.100.200.9):

```
snmp-server enable traps snmp linkdown linkup
snmp-server user public V2C-Group v2c
snmp-server group V2C-Group v2c
snmp-server host 10.100.200.9 informs version 2 public udp-port 8160 snmp
snmp-server host 10.100.200.9 version 2c public udp-port 8160 snmp
```

Note: SNMP link status information depends on the OSV Srx/Lsm/CheckRouter flag set to RtpTrue.

66.2 WAN Monitoring

Data Center Router will monitor the WAN connection. In case of failure in any part in the WAN tunnel, Data Center Router will detect that the link is down.

For the supervision of the WAN link to the branch office is created an IPsec Virtual Tunnel Interface, which shall detect a WAN outage that will be used to report the linkdown/up.

66.2.1 Configuration on Data Center Router 1

```
crypto isakmp policy 1
  encr aes 256
  authentication pre-share
  group 5
  lifetime 3600
crypto isakmp key UNIFY address 0.0.0.0 0.0.0.0
crypto isakmp keepalive 10 periodic
!
crypto ipsec transform-set ESP-AES-SHA esp-aes 256 esp-sha-hmac
!
crypto ipsec profile Branch
  set security-association lifetime seconds 1200
  set transform-set ESP-AES-SHA
!
```

```
interface tunnell
ip address 10.10.50.1 255.255.255.252
tunnel source Ethernet1/0
tunnel destination 10.1.1.2
tunnel mode ipsec ipv4
tunnel protection ipsec profile Branch
```

```
interface GigabitEthernet0/1
description DCR1 to WAN
ip address 10.10.1.1 255.255.255.252
duplex auto
speed auto
```

Note: The name of the IPSec interface (in this case “tunnel1”) must be the configured on the CAC Group of OpenScape Voice (see 4.1.1)

66.2.2 Configuration on Data Center Router 2

```
crypto isakmp policy 1
encr aes 256
authentication pre-share
group 5
lifetime 3600
crypto isakmp key UNIFY address 0.0.0.0 0.0.0.0
crypto isakmp keepalive 10 periodic
!
crypto ipsec transform-set ESP-AES-SHA esp-aes 256 esp-sha-hmac
!
crypto ipsec profile Branch
set security-association lifetime seconds 1200
set transform-set ESP-AES-SHA
!
interface tunnell
ip address 10.20.50.1 255.255.255.252
tunnel source Ethernet1/0
tunnel destination 10.1.2.2
tunnel mode ipsec ipv4
tunnel protection ipsec profile Branch

interface GigabitEthernet0/1
description DCR2 to WAN
ip address 10.20.1.1 255.255.255.252
duplex auto
speed auto
```

Note: The destination is a branch router, but if the BLC is using Branch SBC mode, it is recommended to configure an IPSec tunnel directly to the BLC’s interface.

66.3 Configuration on Branch Router

```
crypto isakmp
  policy 1 encr aes
  256
  authentication
  pre-share group 5
  lifetime 3600
crypto isakmp key UNIFY address 0.0.0.0
0.0.0.0 crypto isakmp keepalive 10
periodic
!
crypto ipsec transform-set ESP-AES-SHA esp-aes 256 esp-sha-hmac
!
crypto ipsec profile Branch
  set security-association lifetime
  seconds 1200 set transform-set ESP-AES-
  SHA
!
interface Tunnel10
  ip address 10.10.50.2 255.255.255.252
  tunnel source
  Serial0/1/0.123 tunnel
  destination 10.10.1.1
  tunnel mode ipsec ipv4
  tunnel protection ipsec profile Branch
!
interface Tunnel11
  ip address 10.20.50.2 255.255.255.252
  tunnel source
  Serial0/1/0.124 tunnel
  destination 10.20.1.1
  tunnel mode ipsec ipv4
  tunnel protection ipsec profile Branch
!
interface
  Serial0/1/0
  bandwidth
  2000
  no ip address
  encapsulation
  frame-relay
!
interface Serial0/1/0.123 point-
to-point description branch to
WAN
bandwidth 2000
ip address 10.1.1.2 255.255.255.252
snmp trap link-status
frame-relay interface-dlci 123
!
interface Serial0/1/0.124 point-
to-point description branch to
WAN
bandwidth 2000
ip address 10.1.2.2 255.255.255.252
snmp trap link-status
frame-relay interface-dlci 124
```

66.4 Alternate routing to Backup Link Server

In a WAN outage, Data Center Router must create an alternate network route to send the WAN traffic through BLS address.

66.4.1 Configuration on Data Center Router 1

OSB-BLC subnet =

10.100.122.0 / 24 BLS1

address = 10.100.123.20

router rip version 2

network 10.0.0.0

ip route 10.100.122.0

255.255.255.0 10.100.123.20

160

Note: This command shows that alternate route uses priority = 160. This mean that the route to BLS will be valid only on the case that directly connected interfaces (priority =1) or dynamic router (e.g. RIPv2 with priority = 120) are down.

66.5 Configuration on Data Center Router 2

OSB-BLC subnet =

10.100.122.0 / 24 BLS2

address = 10.100.124.50

router rip version 2

network 10.0.0.0

ip route 10.100.122.0

255.255.255.0 10.100.124.50

67 SIP Service Provider Provisioning

This capability allows the direct interconnection to a SIP Service Provider (SSP) from the remote branch. It provides the functionality of SIP Header Manipulation for topology hiding.

The following steps need to be taken in OSB for configuring SIP Service Provider:

1. **Enable the WAN interface**
2. **Create SIP Service Provider Profile 3- Create SIP Trunk**
3. **Create Routing Map**
4. **Point to Service Provider DNS Server (If Applicable)**

67.1 Enable the WAN interface

When the OSB is in “SBC” or “SBC-Proxy” mode, OSB WAN interface has to be enabled. Configuration ➤ OpenScope Branch ➤ Branch Office ➤ Configuration ➤ Network Services ➤ Interfaces
Edit/enable the last interface.

The screenshot displays the 'Edit Interface' dialog box with the 'WAN' tab selected. A yellow callout box points to the 'Enabled' checkbox and the 'IP Address Node 1' field, with the text 'Enter IP address, subnetmask and Enable WAN interface'. The 'Enabled' checkbox is checked, and 'IP Address Node 1' is set to 65.207.168.136. The 'Netmask' is set to 255.255.255.0. Below this, there are empty fields for 'IP Address Node 2' and 'Virtual IP Address'.

Below the dialog is the 'Network Services' window, which has tabs for 'Interfaces', 'Routing', 'Redundancy', 'Traffic Shaping', 'NTP', 'DNS', and 'DHCP'. The 'Interfaces' tab is active, showing a table with 2 items. The table has columns for 'IP Address', 'Enabled', 'Interface', and 'Type'.

IP Address	Enabled	Interface	Type
10.234.1.169	✓	Interface1	LAN
65.207.168.136	✓	Interface2	WAN

67.2 Create SIP Service Provider Profile

Configuration → OpenScape Branch → Branch Office → Configuration →
Features → SIP Service Provider Profiles

Features

Enable/Disable desired Feature.

Features Available in Normal Mode and Survivability Mode

- ☒ Enable gateways/trunks **Configure**
- ☐ Enable integrated gateway **Configure**
- Sip Service Provider profiles **Configure**

Select **Configure** and then select **Add**

SIP Service Providers Profiles

SIP service providers profiles provisioning.

Add **Edit** **Delete**

Row	Name	Default home DN	Registration required	Registration interval
1	verizon	5619626159	<input type="checkbox"/>	60
2	testonly		<input type="checkbox"/>	3600

SIP Service Provider Profile

Select OK to temporarily store changes. Make your changes permanent by selecting 'Apply Changes' on the General tab.

General

Name **Default SSP profile**

<input type="checkbox"/> Allow sending of Insecure Referred-By header	<input type="checkbox"/> Send authentication number in Diversion header
<input type="checkbox"/> Send P-Preferred-Identity rather than P-Asserted-Identity	<input type="checkbox"/> Send authentication number in P-Asserted-Identity header
<input type="checkbox"/> Do not send Diversion header	<input type="checkbox"/> Send authentication number in From header
<input type="checkbox"/> Send URI in telephone-subscriber format	<input type="checkbox"/> Include restricted numbers in From header

SIP Service Address

☐ Use SIP Service Address for identity headers

SIP service address **Privacy support**

<input type="checkbox"/> Use SIP Service Address in Request-URI header	<input type="checkbox"/> Use SIP Service Address in From header
<input type="checkbox"/> Use SIP Service Address in To header	<input type="checkbox"/> Use SIP Service Address in P-Asserted-Identity header
<input type="checkbox"/> Use SIP Service Address in Diversion header	<input type="checkbox"/> Use SIP Service Address in Contact header
<input type="checkbox"/> Use SIP Service Address in Via header	<input type="checkbox"/> Use SIP Service Address in P-Preferred-Identity header

Home DN

☐ Mandatory default home DN ☐ Mandatory default home DN - Normal Mode

Default home DN

Name: SIP Service Provider name.

Note: Name must not exceed 14 characters. (Skype only. Others up to 20 characters).

Default SSP Profile: list of default SSP profiles available. If one is selected certain options/flags are enabled/checked/made required automatically. Field is optional.

Privacy Support: define OSB behavior in respect to receiving/sending /ignoring PAI (or PPI) header.

Note: For Skype SSP, even with Privacy Support set to Full, the OSB only sends a PAI if the Send authentication number in PAI flag is set and the Default Home DN field is populated (and the Mandatory Default Home DN box is checked). Same behavior for the PPI flag as well. For other SSPs, the OSB sends the PPI/PAI when Privacy Support is set to Full.

Mandatory Default Home DN: If selected (enabled), the default home DN will always be used as the authentication number.

Note: For Skype SSP, this field must be populated for the OSB to send a PAI (the PAI is populated with what is contained in the Default Home DN field).

Default Home DN: number required by SSP.

Mandatory default home DN Normal Mode: If selected (enabled), the default home DN will always be used as the authentication number. As a result, if this field checked, then the home DN shall be used for all identity headers.

SIP User Agent

SIP User Agent towards SSP: Passthru SIP User Agent

Passthru
Add if non received
Add or Replace

Registration

☐ Registration required

Registration interval (sec)

Business Identity

☐ Business identity required

Business identity DN

Manipulation

☐ Insert anonymous caller ID for blocked Caller-ID

Manipulation

SIP User Agent towards SSP

- Default value is "Passthru" for all SSP profiles.
 Available options:

- Passthru - the SIP User Agent configuration box is grayed out. If no SIP User Agent is received from the LAN side, nothing will be added.
- Add if non received - the received User Agent from the LAN side is passed on unchanged.
- Add or Replace - the received User Agent from the LAN side will be replaced with the configured User Agent.

IMPORTANT: If no User Agent is received from the LAN side, the configured User Agent will be added

• **SIP User Agent** - Configurable SIP User Agent able to recognize a SIP soft switch and apply dynamically a profile to this SIP soft switch and monitor it.
 Up to 32 alphanumeric characters allowed,
 e.g "OSB-test-24"

Registration

Registration required - This flag enables sending of SIP REGISTER to the SSP. This flag must be enabled for the new configuration item "Registration Mode" take effect.

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. It shall be configured accordingly to the phone number blocks provided by the provider to the SIP-PBX.

Registration interval (sec) - Registration interval in seconds.

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. If active, it enables by default the SIP Service Address in Request-URI, From, To, P-Asserted-Identity and Diversion headers.

Use SIP Service Address in Request-URI header - Modifies Request-URI header to include the SIP Service Address network domain.

Use SIP Service Address in From header - Modifies From header to include the SIP Service Address network domain.

Use SIP Service Address in To header - Modifies To header to include the SIP Service Address network domain.

Use SIP Service Address in P-Asserted-Identity header - Modifies P-Asserted-Identity header to include the SIP Service Address network domain.

Use SIP Service Address in Diversion header - Modifies Diversion header to include the SIP Service Address network domain.

Use SIP Service Address in Contact header - Modifies Contact header to include the SIP Service Address network domain.

Use SIP Service Address in Via header - Modifies Via header to include the SIP Service Address network domain.

Use SIP Service Address in P-Preferred-Identity header - Modifies P-Preferred-Identity header to include the SIP Service Address network domain.

SIP Service Address: FQDN or IP address identifying the network domain for the SIP Service Provider. Registration Required: If selected (enabled), the OpenScape Branch will send registrations to SSP (60-7200 seconds).

Note: For Skype SSP, Registration info (TO, FROM, Contact headers sent to Skype SSP) contains what is populated in the Business Identity DN field.

Interval: Registration interval in seconds.

Note: Alarm of loss of communication with SIP Service Provider will show after 4 registration failures

Business Identity Required: if enabled, requires the caller identified in the From header field contain the Business Identity DN. **Business identity DN:** Contains the Business DN. Parameter takes precedence over Default Home DN if both are configured for the From Header.

Note: For Skype SSP, this field is mandatory and must contain the Skype User ID assigned by Skype for populating the From and Diversion headers (in addition to Registration info).

SIP Service Provider Profile

Select OK to temporarily store changes. Make your changes permanent by selecting **Business Identity Required**.

Business identity DN

Outgoing SIP manipulation

☐

Insert anonymous caller ID for blocked Caller-ID

☐

Use single via header

Manipulation

Incoming SIP manipulation

Calling Party Number

From header user and display name

Flags

☐

FQDN in TO header to SSP

☐

REFER supported by SSP

☐

FQDN in Request-URI to SSP

☐

Use To DN to populate the RURI

☐

Send Default Home DN in Contact for Call messages

☐

Request-URI user in TO header to SSP

☐

Allow SDP changes from SSP without session version update

☐

Do not send INVITE with sendonly media attribute

☐

Do not send INVITE with inactive media attribute

☐

Do not send INVITE with video media line

☐

Do not send Invite without SDP

☐

Renew core side crypto keys

☐

Do not send Re-Invite when no media type change

☐

Do not send Re-Invite

☐

Remove Silence Suppression parameter from SDP

☐

Enable local MOH in Survivable Mode

☐

Force direction attribute to sendrcv

TLS

TLS Signaling

Pass-Thru

Sip Connect

☐

Use tel URI

☐

Send user=phone in SIP URI

☐

Registration mode

FQDN in TO header to SSP: f 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.

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.

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.

Use To DN to populate the R-URI: Enable if the SIP Service Provider is sending the Account information in the Request URI and the destination information in the To header.

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.

Request-URI user in TO header to SSP: If enabled, To header user matches the Request-URI user in a new call 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.

Do not send INVITE with sendonly media attribute: Do not send INVITE with send only media attribute to SSP. In this case, SSM removes the attribute from the SDP towards the 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.

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.

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 (sendrcv, inactive, sendonly, or rcvonly) 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.

INFO: 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

INFO: To use the flags, LAN-WAN or LAN-SSP interworking must be enabled.

INFO: Starting from V10R3.03.00.

SIP Service Provider Profile

 Select OK to temporarily store changes. Make your changes p

Flags

- ☐ FQDN in TO header to SSP
- ☐ REFER supported by SSP
- ☐ FQDN in Request-URI to SSP
- ☐ Use To DN to populate the RURI
- ☐ Send Default Home DN in Contact for Call messages
- ☐ Request-URI user in TO header to SSP
- ☐ Allow SDP changes from SSP without session version update
- ☐ Do not send INVITE with sendonly media attribute
- ☐ Do not send INVITE with inactive media attribute
- ☐ Do not send INVITE with video media line
- ☐ Do not send Invite without SDP
- ☐ Renew core side crypto keys
- ☐ Do not send Re-Invite when no media type change
- ☐ Do not send Re-Invite
- ☐ Remove Silence Suppression parameter from SDP
- ☐ Enable local MOH in Survivable Mode
- ☐ Force direction attribute to sendrcv
- ☐ Keep Digest Authentication Header

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.

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.

INFO: 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.

INFO: To use the flags, LAN-WAN or LAN-SSP interworking must be enabled.

Remove Silence Suppression Parameter on SDP: If enabled, removes the silence suppression parameter from SDP towards SSP.

Enable local MOH in Survivable Mode: When checked, the OSB provides local MOH, i.e., no re-INVITE is sent to destination endpoint for media negotiation. Use this flag when MOH is enabled and the target SSP does not re-INVITEs or re-INVITEs without SDP.

Force direction attribute to sendrcv: The flag is used to indicate whether 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.

SIP Service Provider Profile – Incoming SIP Manipulation

Most of SSPs send the calling party number only in the user part of From or P-Asserted-Identity headers. However, some provides send the user and display name parts of those headers as described in RFC2161. This configuration item allows to configuration which information shall be used.

The possible options are:

SIP Service Provider Profile

Select OK to temporarily store changes. Make your changes permanent by selecting 'Apply Changes' on the General page.

Incoming SIP manipulation

Calling Party Number: From header user and disp ▼

Flags:

- ☐ FQDN in TO head
- ☐ REFER supported by SSP

From header user and display name part: Preserves the user and display name parts of From header. **Default value.**

From header user part: Uses the From user part as the Calling Party Number. If present, the display name is removed from this header.

From header display name part: Uses the display name part of the From header as the Calling Party Number. If present, the display name replaces the user part in From header. Otherwise, no manipulation is done.

P-Asserted-Identity user part: Uses the P-Asserted-Identity user part as the Calling Party Number. If present, the display name is removed from this header.

P-Asserted-Identity display name part: Uses the display name part of the P-Asserted-Identity header as the Calling Party Number. If present, the display name replaces the user part in P-Asserted-Identity header. Otherwise, no manipulation is done.

NOTE: This configuration applies to both Normal and Survivability modes of OSB. When in Survivability mode, the SIP Manipulation configured in the OSB may apply to From and P-Asserted-Identity headers. However, the SIP Manipulation is applied only after the SSP Calling Party Number manipulation.

SIP Service Provider Profile

Select OK to temporarily store changes. Make your changes permanent by selecting 'Apply Changes' on the General page.

☐ Business identity required

Business identity DN

Outgoing SIP manipulation

☐ Insert anonymous caller ID for blocked Caller-ID

Manipulation

Flags

☐ FQDN in TO header to SSP

☐ REFER supported by SSP

☐ FQDN in Request-URI to SSP

☐ Use To DN to populate the RURI

☐ Request-URI user in TO header to SSP

☐ Allow SDP changes from SSP without session version update

☐ Do not send INVITE with sendonly media attribute

☐ Do not send INVITE with video media line

☐ Do not send Invite without SDP

☐ Do not send Re-Invite when no media type change

☐ Do not send Re-Invite

☐ Remove Silence Suppression parameter from SDP

☐ Enable local MOH in Survivable Mode

Digest Authentication

☐ Digest authentication supported

Digest authentication realm

Digest authentication user ID

Digest authentication password

TLS

TLS Signaling

SIP Connect

☐ Use tel URI

☐ Send user=phone in SIP URI

☐ Registration mode

Digest Authentication

Digest Authentication Supported: Enables Digest Authentication support.
Digest Authentication realm: Configures Digest Authentication realm. A realm is specified with an IP address, a FQDN or in format user@domain. A realm can be 128 characters

Digest Authentication user ID: Configures Digest Authentication user.
Digest Authentication password: Configures Digest Authentication password.

TLS Signaling - This box is used to configure how TLS as a transport type is signaled in the SIP messages of remote endpoint calls. Possible values are:

- *transport=tls* - Uses parameter *transport=tls* in SIP messages and accepts SIPS URI.
- *SIPS Scheme* - Uses the TLS connection to identify the transport registration, uses SIPS URI in Record-Route header of remote requests.
- *Endpoint Config* - Uses the remote endpoint configuration to determine transport and does not use *transport=tls* nor SIPS URI in the SIP Message.
- *Pass-Thru* - Accept or Send *transport=tls* or SIPS in SIP Message.

SIP Connect

Use Tel URI - When the SSP requires the use of tel URIs the user must check this check box, in which case the SBC shall convert all SIP URIs to Tel URIs towards the SSP and vice versa.

Send user=phone in SIP URI - When checked, the OSB adds "user=phone" in SIP URIs towards SSP.

Registration Mode - This flag represents the registration mode support. By default it is set in a new SSP Default Profile called **DTAG/NGN Registration Mode** as in the OS-SBC. This new profile should also have the following configuration items set by default:

- **Do not send Diversion header**
- **Send URI in telephone-subscriber format**
- **Send authentication number in P-Asserted-Identity header**
- **Send authentication number in From header**
- **Use SIP Service Address for all identity header**

The Registration Mode flag is the one that enables the special handling in the register process: adding of option tag 'gin', 'path' and 'vp-rtcpxr' and contact with 'bnc'.

INFO: Once the Use SIP service address is set, the SIP Service address configuration becomes mandatory.

BasicOptionsFlagsSIP manipulation

SIP manipulation

Insert Anonymous Caller-ID for blocked Caller-ID:

Move up

Move down

Add...

Edit...

Delete

Sel:0

Items/Page: 100

All:0

	Match digits	Match position	Header	Delete/insert position	Number of digits to delete	Insert digits	Add prefix	Replace all with	Call Type
<input type="checkbox"/>									

Insert anonymous caller ID for blocked Caller-ID - If enabled, blocked Caller-ID's will be updated by adding Anonymous to message headers.
Note: SIP Manipulation allows creation/modification/deletion of specific SIP manipulation rules for SSP. For more details please see SIP Manipulation section of OpenScope Branch Configuration Guide.

Note: Outgoing SIP Manipulation (SSP) can be used for outgoing calls in both Normal and Survivability Mode.

67.3 Create SIP Trunk

Configuration → OpenScope Branch → Branch Office → Configuration → Features → Enable gateways/trunks (Configure)

Features

Enable/Disable desired Feature.

Features Available in Normal Mode and Survivability Mode

☒ Enable gateways/trunks

Configure

☐ Enable integrated gateway

Configure

Sip Service Provider profiles

Configure

check **Enable gateways/trunks**, then click **Configure**

click **Add** to create or click **Edit** to edit

Gateways/Trunks

Gateways/Trunks provisioning.

DNS dynamic refresh interval (min)

60

☐ Route to R-URI domain

Add

Edit

Delete

Row	Signaling address type	Remote URL	Port	Interface	Transport	Mapped port	Routing prefix	Gateway/Trunk type	Functional type	Trunk profile	Output digit strip	Output digit add	Priority
1	IP address or FQDN	siemenscomm.g	5060	WAN	UDP	21000,21001,21	561923%	SIP Trunk	All Modes Egress/Ingress	verizon	2		2
2	IP address or FQDN	10.233.20.125	5060	LAN	UDP	9000	125%	Peer OSB	Survivability Mode Egress/Ingress	Gateway	3		1
3	IP address or FQDN	siemenscomm.g	5060	WAN	UDP	21000,21001,21	98%	SIP Trunk	All Modes Egress/Ingress	verizon	2		1

Gateway Configuration

Gateway configuration provisioning.

General

Signaling address type	IP address or FQDN ▼
Remote URL	<input type="text"/>
Port	5060
Interface	LAN ▼
Transport	TCP ▼
Mapped port	9001
Routing prefix	<input type="text"/>
Gateway/Trunk type	SIP Trunk ▼
Functional type	All Modes Egress/Ingress ▼
Trunk profile	verizon ▼
Output digit strip	0
Output digit add	<input type="text"/>
Priority	1 ▼

☐ Operational Mode in OPTIONS Response

Signaling

INVITE no answer timeout - Normal Mode (sec)

Signaling address type: List box provides two choices: IP address or FQDN or DNS SRV

Remote URL: This is the configuration of the IP address, Fully Qualified Domain Name, or DNS SRV of the SIP Service Provider.

Port: This box is used to configure the SIP port of the SIP Service Provider (Not applicable if using DNS SRV).

Interface: WAN interface is valid only for SBC and SBC-Proxy modes.

Transport: SIP transport protocol to be used in communication with the Service Provider. TLS is not supported at the present time.

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.

NOTE: 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, to assign one mapped port to each IP resolved.

NOTE: 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.

Routing Prefix: This box defines a valid Dial Number to be used in search for the Service Provider.

Gateway/Trunk type: This field should be set as "SIP Trunk".

Functional type: For SIP Trunk this field must be set as All Modes Egress/Ingress.

Trunk profile: Selecting a SIP Service Provider Profile.

NOTE: If the flag **Registration required** is **enabled** in the SIP Service Provider profile, different Trunk profiles must be used for different Gateways/Trunks.

Output digit strip: The number of digits to be deleted of the destination URI. The digits are deleted from the beginning.

Output digits 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.

TLS	
TLS mode	Server authentication ▼
Certificate profile	OSV Solution ▼
<input type="checkbox"/> TLS keep-alive	
Keep-alive interval (seconds)	120
Keep-alive timeout (seconds)	10
Media Configuration	
Media profile	igw_lan ▼
Media realm subnet IP address	
Media realm subnet mask	
Anchoring media	Forced ▼
<input type="checkbox"/> Force media anchoring on transcoding	

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

Media realm subnet IP address -

Media realm subnet mask -

Anchoring media:

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.

SIP Service Providers are allowed in WAN only.

It is not allowed to configure the same IP or FQDN for different Gateway/Trunk types.

Gateways must be of type "Others", "Integrated Gateway" or "Peer OSB" when in Proxy ACD mode.

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.

Force media anchoring on transcoding : If 'Force media anchoring on transcoding' check box is checked, always anchor the media if codec transcoding is required. If this check box is not checked, optimize media if possible, even if codec transcoding is required.

67.4 Create Routing Map

Configuration ➤ OpenScope Branch ➤ Branch Office ➤ Configuration ➤ Network Services ➤ Routing

Once the routes are entered or deleted the save button will save the configuration and the window will close. To apply this configuration the user must click on Apply Changes button.

Network Services

Select OK to temporarily store changes.
Make your changes permanent by selecting 'Apply Changes' on the General page.

Interfaces Routing Redundancy Traffic Shaping NTP DNS DHCP

Gateway

Default Gateway Address : 10.234.1.1

Configure the destination IP address, Gateway IP address, Network mask and choose which interface will be used to route the IP packets to the Service Provider.

Routes

Add... Edit... Delete

Sel:0 | Items/Page: 100 | All:6

	Destination	Netmask	Gateway	Interface
<input type="checkbox"/>	68.68.120.47	255.255.255.0	65.207.168.130	Interface2
<input type="checkbox"/>	204.0.0.0	255.0.0.0	65.207.168.130	Interface2
<input type="checkbox"/>	8.8.8.8	255.255.255.255	65.207.168.130	Interface2
<input type="checkbox"/>	65.0.0.0	255.0.0.0	65.207.168.130	Interface2
<input type="checkbox"/>	63.0.0.0	255.0.0.0	65.207.168.130	Interface2
<input type="checkbox"/>	10.234.0.0	255.255.0.0	10.234.1.1	Interface1

67.5 Do not send invite without SDP and MOH in Survivability Mode

To provide the MOH for Gateways in survivability mode OSB needs to send a reINVITE without SDP. It happens even if the flag "Do not send invite without SDP" is enabled in the SIP Service Provider Profile.

To be able to provide MOH to the SIP Service Providers that do not accept INVITEs without SDP, the flag **Enable local MOH in Survivable Mode** shall be enabled.

67.5.1 No MOH to SSP in Survivability Mode

Under **Features** tab:

The feature **Enable Music on Hold for Gateways** shall be disabled

Under **Features > Sip Service Provider Profiles > Sip Service Provider Profile:**

The flag **Do not send invite without SDP** shall be enabled.

In this configuration, placing the SSP on hold OSB will send a reINVITE with SDP inactive.

67.5.2 Providing MOH to the SSP in Survivability Mode

Under **Features** tab:

- **Enable Media Server / Streaming** shall be enabled
- **Enable Music on Hold for Gateways** shall be enabled

Under **Features > Sip Service Provider Profiles > Sip Service Provider Profile**:

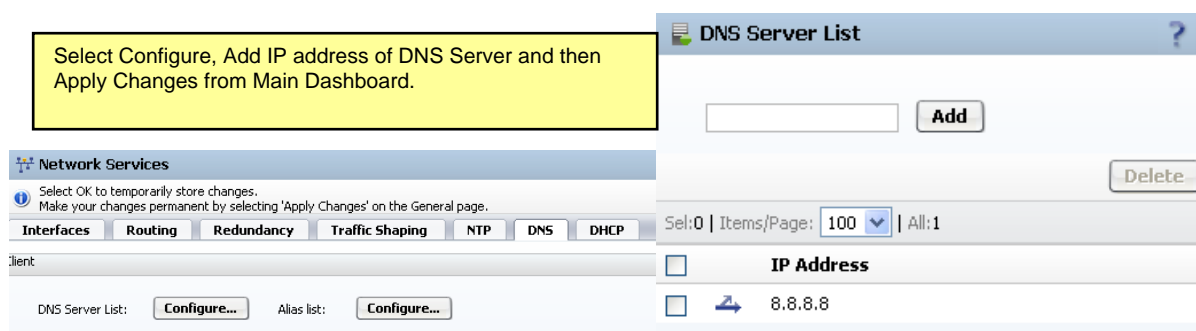
- The flag **Do not send invite without SDP** shall be enabled
- The flag **Enable local MOH in Survivable Mode** shall be enabled

In this configuration, placing the SSP on hold OSB switches the source of media stream to the Media Server (MOH) internally. +No INVITE is sent to the SSP+

67.6 Point to Service Provider or Publix DNS (If Applicable)

If using FQDN for SSP then it is required to configure OpenScope Branch to point to Service Provider or Publix DNS for Resolution.

Configuration ➤ OpenScope Branch ➤ Branch Office ➤ Configuration ➤ Network Services ➤ DNS



67.7 Cseq updates for Digest Authentication

NOTE: Disabling CSeq updates for Digest Authentication

By default, OSB will increase the CSeq when responding to a challenge from the SIP Service Provider. This mechanism can be disabled by setting the flag "**trackCseqUpdatesEnable**" to 0 in the configuration XML. The flag "**trackCseqUpdatesEnable**" is not available in the GUI.

To disable CSeq Updates, follow the instructions below:

1. Export the current xml file.
2. Edit the xml.
3. Search for `<trackCseqUpdatesEnable>1</trackCseqUpdatesEnable>`
4. Change the value of the flag to 0 -> `<trackCseqUpdatesEnable>0</trackCseqUpdatesEnable>`
5. **Save** the changes
6. Import the modified xml.
7. **Apply Changes**

68 Licensing

Feature implements License enforcement to the OpenScape Branch. The OpenScape Branch license file can be installed/maintained via CMP or Stand Alone.

Feature implements License enforcement to the OpenScape Branch. The OpenScape Branch license file can be installed and maintained via CMP or Stand Alone. License types include:

- **OSB Base License (per OpenScape Branch):** provides full usage of the basic switch software. **Note: OSB Configured as "Gateway only" requires only Base license.**
- **OSB Register Lines License (per User):** controls the number of lines that can register with an OpenScape Branch. Note: each device registering to the OpenScape Branch will deduct from license total (Ex. Device with Main Line and 2 Line Appearances will require 3licenses).
- **OSB Auto Attendant License (per OpenScape Branch):** allows access to Auto Attendant feature.
- **OSB Backup ACD License (per OpenScape Branch):** allows access to ACDfeature/mode.
- **OpenScape SBC Session License (per Session):** controls the maximum number of system wide SBC Sessions.
- **OSB Single Load Line License:** allows the decrease in sustaining costs and maintenance and then evolves to the release of new features faster and with a better ROI. During the "Grace Period" (30 Days), no License applied, or no Licence Version available, the OSB/OS-SBC allows only the Implementation/Feature set based on V8R1 version.



CMP will provide the OSB / OS-SBC Base License Version.

The Base License Version and the SID will be stored in the XML file.

Currently the CMP applied License message doesn't contain the License Version as well as the SIEL ID info.

- **SIEL ID** : the unique identifier for every system

68.1 Supported License Types

Regular License Files (RLF): licenses purchased by customer (no expiration date).

- OpenScape Branch Base Licenses (maximum allowed 3,000).
- OpenScape Branch User Licenses (maximum allowed 100,000).
- Auto Attendant Licenses (maximum allowed 3,000).
- Backup ACD Licenses (maximum allowed 3,000).
- OpenScape SBC Session Licenses (Maximum allowed 160K for Branches) SBC/SBC- Proxy modes only.

Evaluation License: Regular License File with an expiration time of 180 days.

- 1 OpenScape Branch Base License.
- 1 Auto Attendant Feature License.
- 1 Backup ACD Feature License.
- 50 OpenScape Branch User licenses.
- 100 OpenScape SBC Session Licenses. SBC/SBC-Proxy modes only.

Demo License: Regular License File with no expiration.

- 1 OpenScape Branch Base License.
- 1 Auto Attendant License.
- 1 Backup ACD License.
- 50 OpenScape Branch User licenses.
- 100 OpenScape SBC Session Licenses. SBC/SBC-Proxy modes only.

Attempts to exceed license amounts results in blocked registrations and a critical alarm is generated.

The alarm must be manually cleared.

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

Common License FAQ

Consider the branch is configured and the licenses required are assigned.

- **How often does the branch check the CMP server for the licenses?**

Once a day.

- **If the branch fails to connect with the CMP server because of a network issue, then how often will the branch try to reach the CMP license server and at what interval?**

Once a day (if the initial request fails the branch will try again after 30 minutes. Then again in 15 minutes and again in 5 minutes. In other words, four trials over the course of an hour, followed by four further trials 24 hours later).

- **If OSB fails to get connected for a specified time interval then how long does the branch go into the grace period?**

30 days.

- **Does OSB continuously try to connect to the license server during the grace period and how often?**

Yes, Once a day.

- **If the OSB gets connected to the CMP license server during the grace period, does the branch return to normal? Does the grace period value reset to 0?**

OSB goes back to normal and the grace period is reset to 0.

- **Is the branch blocked if the grace period expires? Does the branch check for the license server if the grace period expires?**

When the grace time ends, licensed features cease to function. OSB continues to check for license server, and if license server is found, the OSB returns to regular operation.

- **What is the expected behavior in a branch if more users attempt registration than are permitted?**

Some additional registrations are allowed. The number of additional registrations allowed depends on the OSB type.

68.2 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 Portal. The transfer of the license file to Common Management Portal occurs automatically via the internet.

OpenScape Branch Base licenses are configured via the Common Management Portal (Using MAC Address of CMP in CLS) or Stand Alone (Using MAC Address of OSB eth0/LAN in CLS).

68.3 Common Management Portal License Configuration

The licenses can be activated with Common Management Portal. The Common Management Portal transfers the License Authorization Code (LAC) to the CLS and receives the associated license file. The licenses and their related information are displayed in Common Management Portal.

Note: Applying licenses require SIP server to restart in OSB so this should be done during a maintenance window. Note: after installing the OSB a 30 day grace period is allowed until licenses are applied. During this grace period, the product may be restricted or fully functional. If licenses are not installed after the grace period, the product becomes severely restricted or stops working entirely.

Upload License File using the Common Management Portal Maintenance > Licenses > Information > Offline Activation

Configuration Maintenance User Management Fault Management Performance Management Accounting

Inventory Monitoring Recovery Licenses

Management

Information

Locking IDs

Software Subscription

License Information

Filter: for System Go Clear

Offline Activation...

License Activation

Choose and activate a new license file.

License File: Browse...

Select License File and

Activate Cancel

License Information

Filter: OpenScape Branch/SBC for Product Name Go Clear

Items/Page: 200 All: 5

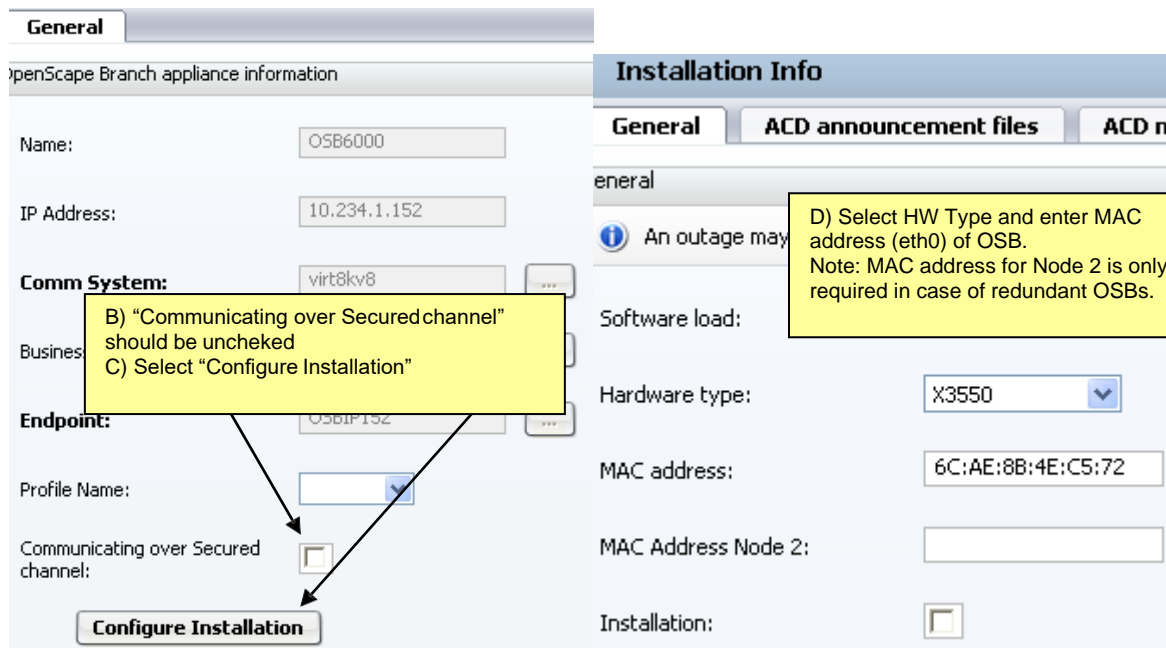
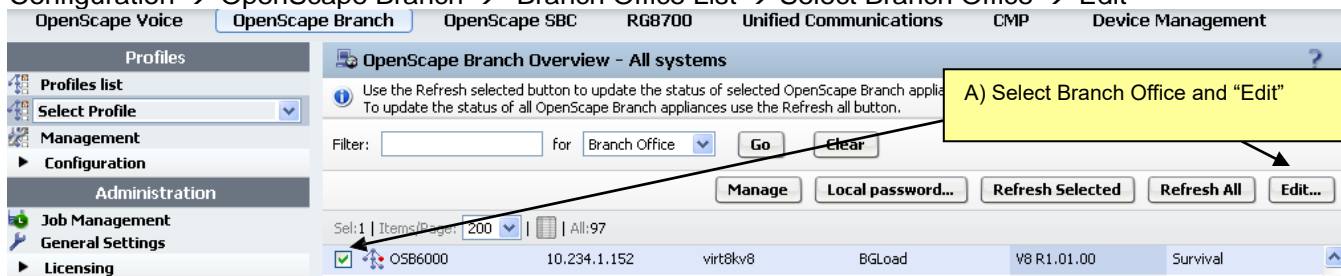
License information for OSB shows

Offline Activation... Online Activation...

System	Product Name	Feature Name	Number of used licenses	Validity
offboard	OpenScape Branch/SBC V8	OpenScape Branch Backup ACD (per OSB)	18 of 500	unlimited
offboard	OpenScape Branch/SBC V8	OpenScape Branch Auto Attendant (per OSB)	21 of 500	unlimited
offboard	OpenScape Branch/SBC V8	OpenScape SBC Session (per Session)	4250 of 30000	unlimited
offboard	OpenScape Branch/SBC V8	OpenScape Branch Base	21 of 500	unlimited
offboard	OpenScape Branch/SBC V8	OpenScape Branch Registered Lines	17720 of 100000	unlimited

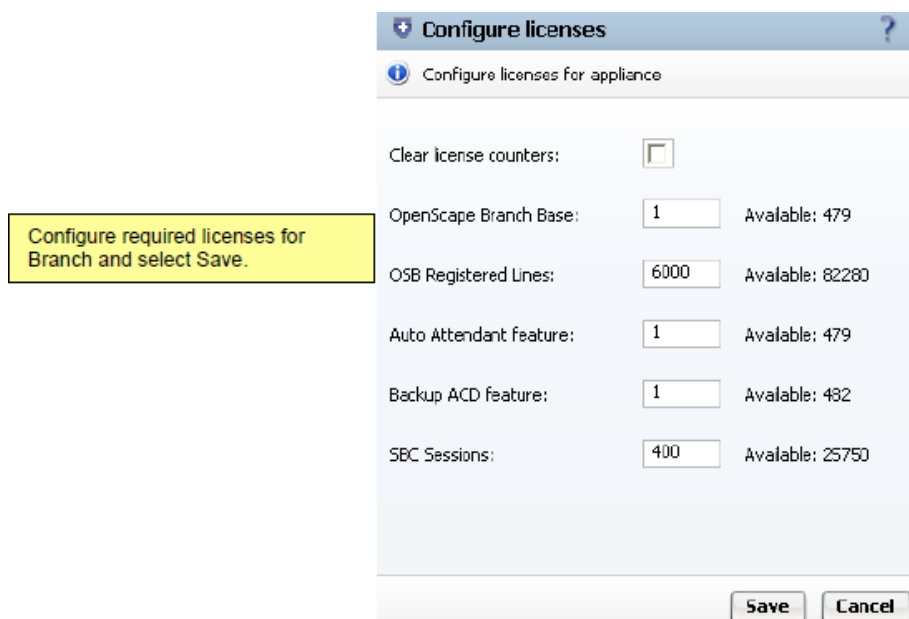
Edit MAC Address in OpenScape Branch Assistant

Configuration → OpenScape Branch → Branch Office List → Select Branch Office → Edit



Configure and Apply Licenses

Configuration → OpenScape Branch → Branch Office List → Select Branch Office → Manage → Licensing Information → e



OpenScape Voice
OpenScape Branch
OpenScape SBC
RG8700
Unified Communications
CMP

Profiles
Profiles list
Select Profile
Management
Configuration
Administration
Job Management
General Settings
Licensing
All systems
Branch Office list
OSB6000
Management
Configuration
Local Dashboard
System
Network/Net Services
VoIP

General - virt8kv8 - OSB6000

Aggregated information and data for selected Branch Office.

After Selecting "Device License Update" licenses are applied.
Note: Applying licenses require SIP server to restart in OSB so this should be done during a maintenance window.

Licensing Information

First updated: 12/21/14 11:18 AM Last updated: 6/8/15 3:06 PM

Logical ID: virt8kv8:BGLoad:OSB6000 Hw ID: 6C:AE:8B:4E:C5:72 Hw ID2: N/A

Refresh
Device license update
Configure

License type	Configured	Reported locally	Usage(Peak)
OpenScape Branch Base	1	1	1
OSB Registered Lines	6000	6000	0
Auto Attendant Feature	1	1	0
Backup ACD Feature	1	1	0
SBC Sessions	400	400	0

68.4 Stand Alone License Configuration

Stand alone Mode is defined as when an OpenScape Branch is deployed at a customer who does not have a Common Management Portal (CMP). Customers can use the OpenScape Branch local GUI to manage the licenses created with CLS. Note: after installing the OSB a 30 day grace period is allowed until licenses are applied. During this grace period, the product may be restricted or fully functional. If licenses are not installed after the grace period, the product becomes severely restricted or stops working entirely.

Login to Local GUI and upload license file

System ➤ Licenses ➤ License Information ➤ Browse ➤ Upload

System

Select OK to temporarily store changes. Make your changes permanent by selecting 'Apply Changes' on the General page.

Settings
Licenses
Branding

General

License server
Port 4709

Hardware ID
Browse/Upload LIC file created with CLS.

Logical ID

Advanced Locking ID
Not available. Refresh it
Refresh

License Information

License type
None
Grace period
28 days

Stand alone license file:
Browse...
Upload

Licenses are applied after about one minute.
System → Licenses → License Information

System

Select OK to temporarily store changes. Make your changes permanent by selecting 'Apply Changes' on the General page.

Settings Licenses Branding

General

License server Port

Hardware ID Master

Hardware ID Backup

Logical ID

Advanced Locking ID

License Information

License type Days till license expires

Stand alone license file:

License type	Licenses configured	Licenses usage (peak)
Base	1	1
OpenScape Branch Registered Lines	550	118
Auto Attendant	1	0
Backup ACD	1	0
SBC sessions	550	0

StandAlone mode License - is a special license that defines the number of PSTN ports that can be used:

In this case, an OSB DP24 are using a PSTN license for two PRI Ports.

If a license for a single PSTN PRI Port had been applied, this system would have being restricted to use only its first PRI Port.

50DP245A - System - Google Chrome

https://25.25.0.45/systemConfiguration.html?tabId=licensesTab

System

Select OK to temporarily store changes. Make your changes permanent by selecting 'Apply Changes' on the General page.

Settings License Branding

General

License server

License server port

4709

Hardware ID

00:0B:AB:2D:8C:9A

Logical ID

Advanced Locking ID

Not available. Refresh it

Refresh

License Information

License type

Stand Alone

Days till license expires

15 days

Stand alone license file:

Choose File

No file chosen

Upload

Refresh from License Server

License type	License configured	Licenses usage (peak)
OSB Base	1	1
SBC sessions	60	60
PSTN Ports	2	2

PSTN Ports - This license type defines how many ports can be used on the stand alone mode.

Open Source Software Licenses

Component

Mesa-libEGL1

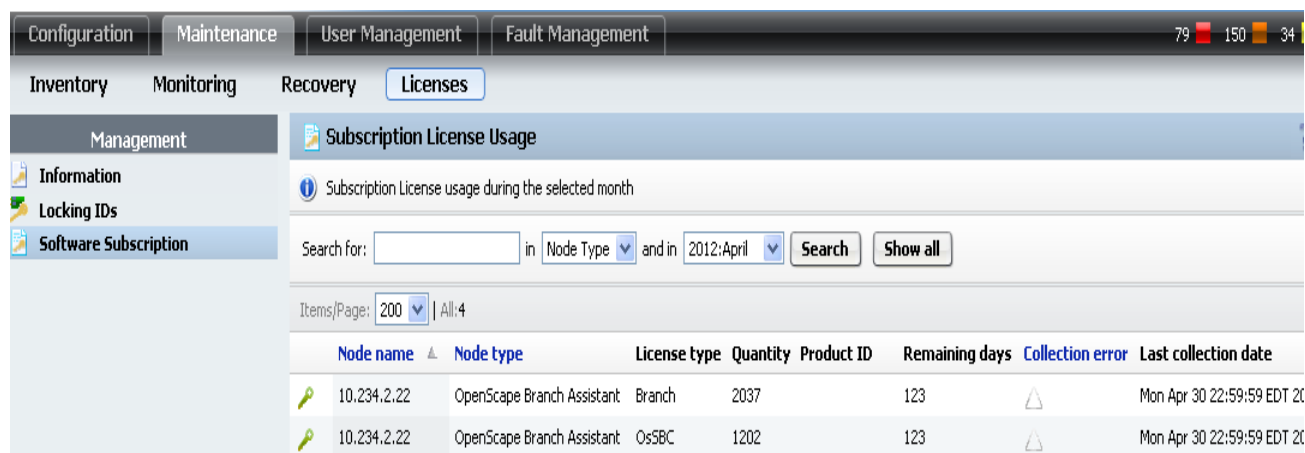
Show

OK Cancel

68.5 Subscription License

License usage is reported on a daily/monthly basis under software subscription license screen.

Maintenance → Licenses → Software Subscription



Configuration Maintenance User Management Fault Management 79 150 34

Inventory Monitoring Recovery Licenses

Management

Information

Locking IDs

Software Subscription

Subscription License Usage

Subscription License usage during the selected month

Search for: in and in

Items/Page: | All: 4

	Node name	Node type	License type	Quantity	Product ID	Remaining days	Collection error	Last collection date
	10.234.2.22	OpenScope Branch Assistant	Branch	2037		123		Mon Apr 30 22:59:59 EDT 2012
	10.234.2.22	OpenScope Branch Assistant	OsSBC	1202		123		Mon Apr 30 22:59:59 EDT 2012

License Type Branch: reports usage calculated based on the configured license usage (Branch Users)

License Type OsSBC: reports usage based on the high watermark of the number consumed SBC session licenses in the month (SBC Sessions).

69 Automatic Call Distribution (ACD)

OSB can be configured in Proxy ACD mode to support Automatic Call Distribution.

Under ACD menu user can configure Automatic Call Distribution parameters. New window is opened when selecting ACD.

Note: ACD user has access to ACD configuration only (Local GUI)

Important: ACD currently uses the rmemory hunt mechanism (round robin with memory, remember where we left off last ring pass)

69.1 General Configuration

User can configure Agent Log on/off access codes as well as agent ring no answer timeout. Toggle Keyset Feature is also available for login/logoff functionality instead of using the Login/Logoff access code.

Configuration ➤ OpenScape Branch ➤ Select Branch Office ➤ Configuration ➤ ACD ➤ General

The screenshot shows the 'ACD' configuration window with the 'General' tab selected. The window has a title bar with 'ACD' and a help icon. Below the title bar, there is a message: 'Select OK to temporarily store changes. Make your changes permanent by selecting 'Apply Changes' on the General page.' The main area contains four tabs: 'General', 'Queue', 'Profiles', and 'Agents'. The 'Agents' tab is active, showing 'Agents' Settings. The settings include: 'Log On Service Access Code' (21), 'Log Off Service Access Code' (22), 'Timeout' (30), 'Support Keyset Toggle Key' (checkbox), and 'Keyset Toggle Service access code' (empty field). A yellow callout box on the right explains the fields: 'Log On Access Code: log on access code for all agents. Valid digits are 0-9 and "*".'; 'Log Off Access Code: log off access code for all agents. Valid digits are 0-9 and "*".'; 'Timeout: defines how long agent will ring before agent is considered unavailable and is automatically logged off from the queue. It will not have effect if the advance timeout is greater than the Queue Advance timeout.'; and 'Toggle Key Support/Code: 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.'

69.2 ACD Queues

User can configure up to 100 queues for ACD. The "Add" button is disabled when this limit is reached.

Configuration ➤ OpenScape Branch ➤ Select Branch Office ➤ Configuration ➤ ACD ➤ Queues

ACD

Select OK to temporarily store changes.
Make your changes permanent by selecting 'Apply Changes' on the General page.

General

Queue

Profiles

Agents

Filter: for

Name

Go



Clear

1 Item

Add...

Edit...

Delete

<input type="checkbox"/>		Id	Name	DID List	Destination	Assigned Agent IDs	Overflow to Voice Mail Server
<input type="checkbox"/>		1	CustomerService	15619231314	15619231313	Show	

Name: Queue name.

Destination (Overflow, Voice Mail): destination of queued calls when limit of calls in queue is reached or timeout for a call in queue elapses. This could also be the Voice Mail number when applied.

Overflow to Voice Mail Server: immediate diversion of a call to Voice Mail Server when there are no agents available in the queue (no logged agents or no free agents)

Note: it is necessary to check flag Generate Diversion Header when Overflow to Voice Mail Server is checked.

Queue Advance Time Out: time to advance call to the next available agent if current ringing agent does not pick up.

Wrap Up Time: time to keep agent unavailable after handling a call. Allows time for post call processing.

Play Ring tone and Music on Hold: play ring back tone to caller or MOH when waiting in queue. MOH files can be uploaded (See Audio Files)

ACD - Add Queue

General

DID

Announcements

ID:	<input type="text" value="0"/>	Queue advance time out:	<input type="text" value="35"/> (sec)
Name:	<input type="text" value="Sales"/>	Agent wrap-up time:	<input type="text" value="5"/> (sec)
Destination (Overflow, Voice Mail):	<input type="text" value="15619231315"/>	Play ring tone instead of music on hold:	<input type="checkbox"/>
Overflow to Voice Mail Server :	<input checked="" type="checkbox"/>	Music on hold:	<input type="text" value="fpm-calm-river.wav"/>
Generate diversion header:	<input checked="" type="checkbox"/>		

Caller Parameters

Maximum waiting time: (sec)

Unlimited: ☒

Maximum Callers:

Maximum waiting time: max time that a caller will be in queue before being sent to overflow destination (If not overflow the call will clear).

Max Callers: max number of callers in the queue or unlimited (if number is reached then calls go to overflow)

Note: If the Agent timeout is lower 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. If the Agent timeout is equal or 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.

ACD - Add Queue

General

DID

Announcements

<input type="text"/>	<input type="button" value="Add"/>
1 Item	<input type="button" value="Delete"/>
<input type="checkbox"/>	Directory Numbers
<input type="checkbox"/>	15619231316

DID List: DIDs used to reach queue (DIDs must be unique and can not be the same as login/logoff/toggle key codes). There is no limit on the amount of DIDs that can be configured.

ACD - Add Queue

General

DID

Announcements

Queue join:

priv-introsaved.wav

Play

Announce position to caller:

☐

Queue waiting:

queue-periodic-announce.wav

Play

Announce estimated hold time to caller:

☐

Agent:

queue-thankyou.wav

Play

Announce hold time to agent:

☐

Position/hold time announcement frequency:

120

(sec)

Interval between queue join and queue waiting:

60

(sec)

Queue join: played when a call is entered in the queue. (File can be uploaded in Audio Files).

Queue waiting: periodically played to the caller while in queue. (File can be uploaded in Audio Files).

Agent: played to the agent before the call is connected. (File can be uploaded in Audio Files).

Position/hold time announcement frequency: defines (in seconds) how often the announcements of position and estimated hold time are played to the caller.

Announce position to caller: position in queue is periodically played to the caller.

Announce estimated hold time to caller: estimated hold time is periodically played to the caller.
 Note: sometimes OB will not play the time and only present "The Estimated hold time is, thank you for your Patience. If estimated time reaches 0 before call is answered, then OB will recalculate the time and present this time to callers.

Announce hold time to agent: time the caller has been waiting in the queue is played to the agent before the call is connected. (Note: ex will play as 5 minutes 300 seconds)

Interval between queue join and queue waiting: defines (in seconds) how often the queue waiting announcement is played to the caller after the queue join announcement.
 Note: queue timeout starts counting only after the join announcement ending.

69.3 ACD Profiles

Profiles are assigned to ACD queues. User can configure up to 100 profiles for ACD. The Add button is disabled when this limit is reached.

Configuration ➤ OpenScape Branch ➤ Select Branch Office ➤ Configuration ➤ ACD ➤ Profiles

ACD

Select OK to temporarily store changes.

Make your changes permanent by selecting 'Apply Changes' on the General page.

General

Queue

Profiles

Agents

Filter:

For Name

Go

Clear

2 Items

Add...

Edit...

Delete

	Name	Assigned Queue IDs
<input type="checkbox"/>	Profile1	1
<input type="checkbox"/>	Profile2	2

ACD - Add Profile

Name:

Profile1and2

Assigned Queue IDs:

1,2

69.4 ACD Agents

User can configure/update agents as well as show status of agents (login/logoff).

Configuration ➤ OpenScape Branch ➤ Select Branch Office ➤ Configuration ➤ ACD ➤ Agents

ACD

Select OK to temporarily store changes.
Make your changes permanent by selecting 'Apply Changes' on the General page.

General Queue Profiles Agents

Filter: for Name

3 Items

<input type="checkbox"/>	Id	Name	Assigned Profile
<input type="checkbox"/>	100	MartinBrooks	Profile1
<input type="checkbox"/>	101	PeterSmith	Profile1and2
<input type="checkbox"/>	102	MarkRoberts	Profile1

ACD - Add Agent

ID:

Name:

Password:

Confirm password:

Profile:

Agent ID: number used in logon/logoff (must be unique).
Note: if using Keyset toggle, it is mandatory for the Agent ID to match the subscriber number.

Agent Name: name to identify agent.

Password: agents password used in logon/logoff (must be numeric).

Assigned Profile: queue Profile assigned to agent.
Note: circular round robin is done to offer calls to agents.


Configuration ➤ OpenScape Branch ➤ Select Branch Office ➤ Configuration ➤ ACD ➤ General ➤ Status (Show)

There is a maximum number of ACD agents allowed to be configured (For large HW types)

(only when V9 Base License is applied):

- 500 for OSB1000 and OSB6000.
- 250 for OSB 500i

The Add button is disabled when this Main Agent status window shows all agents for all queues along with status (logged off/logged in) and Phone number when Agent is logged in.

 **Show agent status**

Filter: for Name ▾ Go Clear

4 Items

Id	Name	Status	Phone Number	Assigned Profile
100	MartinBrooks	logged in	5558885246	Profile1
101	PeterSmith	logged off		Profile1and2
102	MarkRoberts	logged in	5558885288	Profile1
103	JenaMartins	logged off		Profile1

69.5 ACD Audio Files

User can upload files to be used for configuring queue Announcement or MOH. Sound files can be used in one or more queues. If a short file is used then OB will automatically continue to play the file (Loop).

Note: Only WAV audio files (.wav) with: Bit Rate: 128kbps, Audio Sample size: 16 bit, Channels: Mono, Sampling Rate: 8 kHz, Audio Format: PCM are allowed for announcements.

Configuration ➤ OpenScape Branch ➤ Select Branch Office ➤ Configuration ➤ ACD ➤



➤ Audio Files

ACD

Select OK to temporarily store changes.
Make your changes permanent by selecting 'Apply Changes' on the General page.

General **Queue** **Profiles** **Agents**

Agents' Settings

Log On Service Access Code: 21

Log Off Service Access Code: 22

Timeout: 30 (sec)

Support Keyset Toggle Key: ☐

Keyset Toggle Service access code:

Status: **Show...**

Audio Files

Music on hold: **Configure...**

Announcement: **Configure...**

Go

Music on hold

2 Items

<input type="checkbox"/>	File name
<input type="checkbox"/>	OpenBranchFormatFile.wav
<input type="checkbox"/>	fpm-calm-river.wav

Announcement

3 Items

<input type="checkbox"/>	File name
<input type="checkbox"/>	priv-introsaved.wav
<input type="checkbox"/>	queue-periodic-announce.wav
<input type="checkbox"/>	queue-thankyou.wav

Logs: user can download a tar file containing the log files for all queues. 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 occurred in the last 24 hours.

Note: using Assistant it is possible to schedule announcements to be applied. This is used to substitute the announcements without needing to edit the queues and to apply same announcements to several OSBs at the same time. Functionality is under Configuration ➤ OpenScape Branch ➤ Job Management ➤ Add ➤ Action (Transfer WAV Files).

69.6 Configuration for Toggle Key

Administrator Pages

User Pages

Logout

Admin Login

Applications

Bluetooth

Network

System

System Identity

SIP interface

Registration

SNMP

Features

Configuration

DSS settings

Program keys

Fixed Keys

Keyset operation

Addressing

Program keys

To assign a new function to a key, select from the drop down list box. To view or modify the parameters associated with the key, use the Edit button.

Normal	Key	Shifted
Feature toggle Label: Agent	1	Clear (no feature assigned)
Group pickup Label: Group pickup	2	Clear (no feature assigned)
Conference Label: Conference	3	Clear (no feature assigned)

Create Toggle Key on Phone using configured "Keyset Toggle Service access code" for Feature Code field (ex. *23)

Feature toggle

Key label 1 Agent

Feature code *23

Description Agent

Submit

Reset

Label: Group pickup

Conference

3

Clear (no feature assigned)

ACD

Select OK to temporarily store changes.
Make your changes permanent by selecting 'Apply Changes' on the General page.

General

Queue

Profiles

Agents

Agents' Settings

Log On Service Access Code: 21

Log Off Service Access Code: 22

Timeout: 30 (sec)

Support Keyset Toggle Key: ☒

Keyset Toggle Service access code: *23

Status: Show...

ACD - Add Agent

ID: 5558885249

Name: Name 5249

Password:

Confirm password:

Profile: Profile1

Agent ID must match with Phone Number.

70 Virtualized OpenScape Branch Solution

The Virtualized OpenScape Branch solution provides the same functionality as the existing OpenScape Branch deployment on native HW.

Note: The Virtualized OpenScape Branch only applies to branches without Analog/TDM interface cards.

OSB virtualization offers three deployments based on capacity: Virtual OSB 250, Virtual OSB 1000, or Virtual OSB 6000.

In order to set up a Virtual OSB, user must create an iso image file with the OSB software, mount it on to the virtual machine and start the installation procedure. Once the installation is completed, user must install VMware tools.

70.1 OSB iso image

User can either set up a fresh installation on a virtual OSB or can migrate a native OSB to virtual environment (**integrated gateway boxes are not supported in the virtual environment**).

70.2 ISO Image for fresh installation

For the OSB VM deployment, an iso image needs to be created with the usbsticksetup.exe. In the media select drop down menu user must select “Virtual Machine ISO image” and then select the appropriate hardware type.

Note: user must have at least 500Mb free space for ISO image.

Rest of the fields should be completed in the same way that is done for native installations.

Up to V10R1:

USB Stick Setup

Media Select
Virtual Machine ISO image Refresh

WARNING: all partitions of Removable Medias will be deleted and a single FAT32 partition will be created. Therefore, all data of the removable media will be erased.

Installation Method
☒ Generate node.cfg file
☐ Already existent database file
☐ Already existent node.cfg file
☐ Automated ☐ PreInstall ☐ Net boot ☐ DHCP ☐ VPN

Branch Network Configuration
Hardware type: Virtual OSB 250
Hostname: Virtual OSB 1000
Interface: Virtual OSB 6000
☐ Disable interface ☐ Enable IPv6
IPv4 address: . . .
IPv4 netmask: . . .
IPv6 address:
IPv6 netmask:
IPv4 gateway: . . .
IPv6 gateway:
Logical ID:
CMP URL 1:
CMP URL 2:
DNS 1: . . .
DNS 2: . . .
Change Branding Names and Logo
☐ Partitioned USB Stick OK Cancel

Starting from V10R2:

USB Stick Setup

Media Select

Virtual Machine ISO image Refresh

WARNING: all data of the removable media will be erased.

Configuration database

☒ Generate node.cfg file

☐ Already existent database file

☐ Already existent node.cfg file

Branch Network Configuration

Hardware type: Virtual OSB 250 Virtual OSB 1000 Virtual OSB 6000 interface

VPN

Hostname: Virtual OSB 250

Interface: Virtual OSB 1000

IPv4 address: . . .

IPv4 netmask: . . .

IPv4 gateway: . . .

☐ Enable IPv6

IPv6 address: . . .

IPv6 netmask: . . .

IPv6 gateway: . . .

Installation Method

☐ Automated

☐ PreInstall

☐ Net boot

☐ DHCP

☒ UEFI Bootloader

General

DNS 1: . . .

DNS 2: . . .

Logical ID: . . .

CMP URL 1: . . .

CMP URL 2: . . .

Change Branding Names and Logo

☐ Partitioned USB Stick

OK Cancel

After completing the necessary configuration or use the already existent database file the user selects OK and will be prompted where to save the ISO file (this ISO file will be used for the installation and should be accessible from the VM). Once this is completed, a success message is displayed.

Up to V10R1:

USB Stick Setup

Media Select
Virtual Machine ISO image Refresh
WARNING: all partitions of Removable Medias will be deleted and a single FAT32 partition will be created. Therefore, all data of the removable media will be erased.

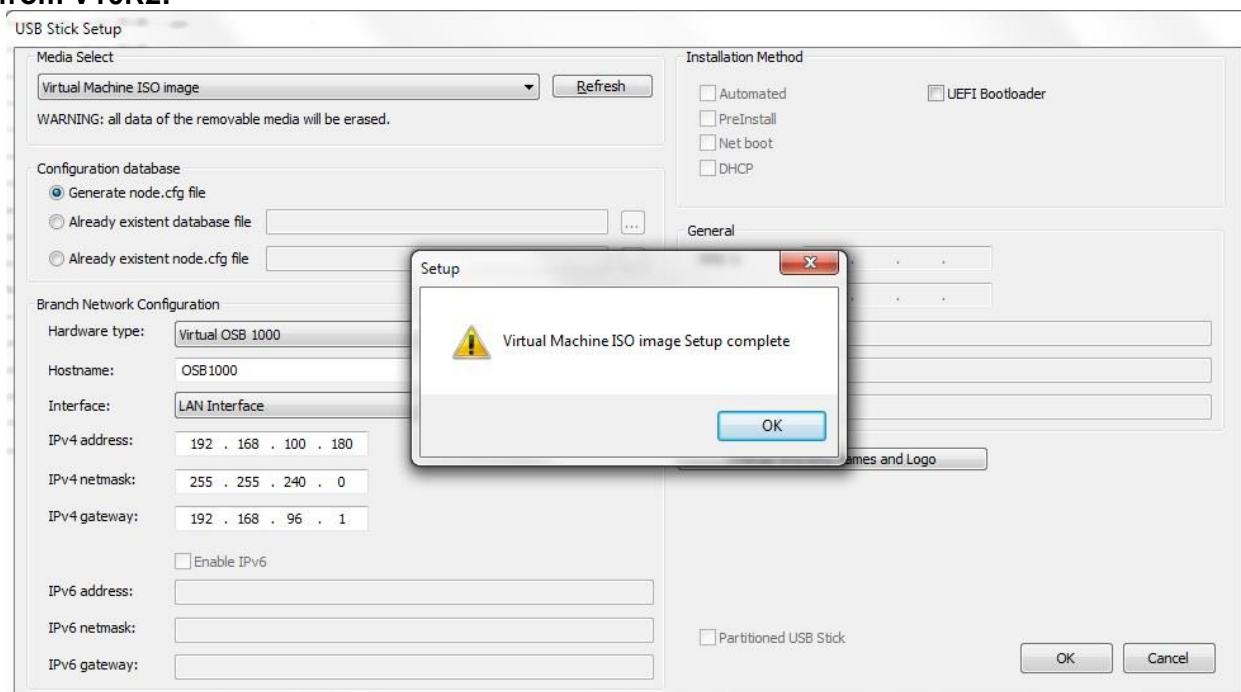
Installation Method
☒ Generate node.cfg file
☐ Already existent database file ...
☐ Already existent node.cfg file ...
☐ Automated ☐ PreInstall ☐ Net boot ☐ DHCP ☐ VPN

Branch Network Configuration
Hardware type: Virtual OSB 6000
Hostname: OSB6000LoadBox

Inter Setup
☐ IPv4
☐ IPv4
☐ IPv6
☐ IPv6
IPv4 gateway: 192 . 168 . 6 . 1
IPv6 gateway:
Logical ID:
CMP URL 1:
CMP URL 2:
DNS 1: . . .
DNS 2: . . .
Change Branding Names and Logo
☐ Partitioned USB Stick OK Cancel

Virtual Machine ISO image Setup complete
OK

Starting from V10R2:



70.3 ISO Image for migration of native hardware

For migration scenarios, the xml config file of the native box that is up and running will be used to create the iso image. Each native box corresponds to a virtual box. See table below. No manual modification is required.

Hardware	VM Implementation
Advantech	OSB250
x3250	OSB 1000
x3550	OSB 6000
RX330	OSB 6000
D945	OSB250
Advantech50i	Not Supported
RX200	OSB 6000
Advantech250	OSB250
Advantech500i	Not Supported
SR250/SR250 V2	OSB 1000
SR530	OSB 6000
SR630 V2	OSB 6000

In the media select drop down menu user must select “Virtual Machine ISO image” and then select “Already existent database file” and import the xml from the native box

The screenshot shows the 'USB Stick Setup' window. In the 'Media Select' section, 'Virtual Machine ISO image' is selected in the dropdown menu. Below it, a warning states: 'WARNING: all data of the removable media will be erased.' In the 'Configuration database' section, the 'Already existent database file' radio button is selected, and the file path 'C:\psb-10.02.00.00-2\OSB1000V10-osb-config_1_201' is entered. This section is highlighted with a red rectangle. In the 'Branch Network Configuration' section, the 'Hardware type' dropdown menu is set to 'Virtual OSB 1000', also highlighted with a red rectangle. Other fields include 'Hostname' (OSB1000V10), 'Interface' (LAN Interface), and various IP address fields. The 'Installation Method' section on the right has 'UEFI Bootloader' checked. At the bottom right are 'OK' and 'Cancel' buttons.

Based on the table above, “Hardware type” will be modified accordingly.
Note: using a 50i/500i XML for “Already existent database file” is not supported.

70.4 Virtual Machine (VM)

ESXi 6.5 or higher can be managed by any web browser using the VMware Host Client, which is based on HTML5 technology.

In order to create the Virtual Machine (VM), user can either select to deploy a vApps that is delivered with the OSB software or create manually the VM itself. After creating the virtual machine, some specific settings must be configured on the VM.

70.5 Creating the VM

VM can be created by deploying an OSB vApps file or by creating the VM manually.

70.6 Deploying OSB vApp

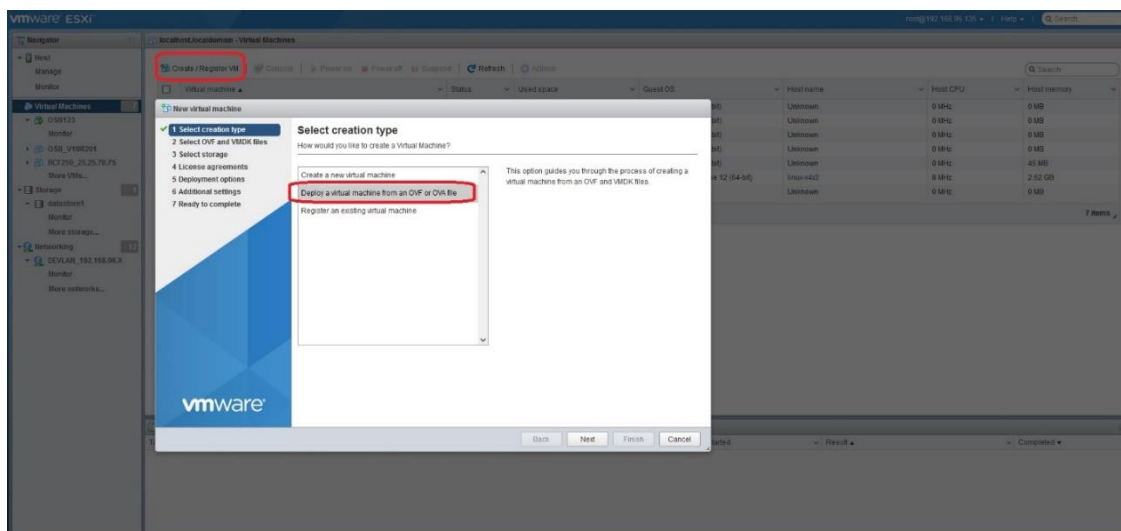
Before initiating the procedure, user must navigate to the directory where the OSB software resides and unzip the vApps_osb-*.zip.

Name	Type	Size
usbsticksetup_osb-10.02.00.00-2	File folder	
vApps	File folder	
image_osb-10.02.00.00-2.spa	SPA File	1 KB
image_osb-10.02.00.00-2.tar	TAR File	730,990 KB
misc_osb-10.02.00.00-2.tar.gz	GZ File	157 KB
sw-metadata-osb-10.02.00.00-2.json	JSON File	1 KB
usbsticksetup_osb-10.02.00.00-2.zip	Compressed (zipp...	21,972 KB
vApps_osb-10.02.00.00-2.zip	Compressed (zipp...	8 KB

vApps directory contains 3 subdirectories, each one corresponding to the appropriate hardware type

osb-10.02.00.00-2	Name	Type	Size
usbsticksetup_osb-10.02.00.00-2	OSB-250	File folder	
vApps	OSB-1000	File folder	
usbsticksetup_osb-10.02.00.00-2.zip	OSB-6000	File folder	
vApps_osb-10.02.00.00-2.zip			

Login to vSphere Host Client and select to **Create/Register VM**. Select the option **Deploy a virtual machine from an OVF or OVA file**. Press **Next**. The **Select OVF and VMDK files** windows appears.

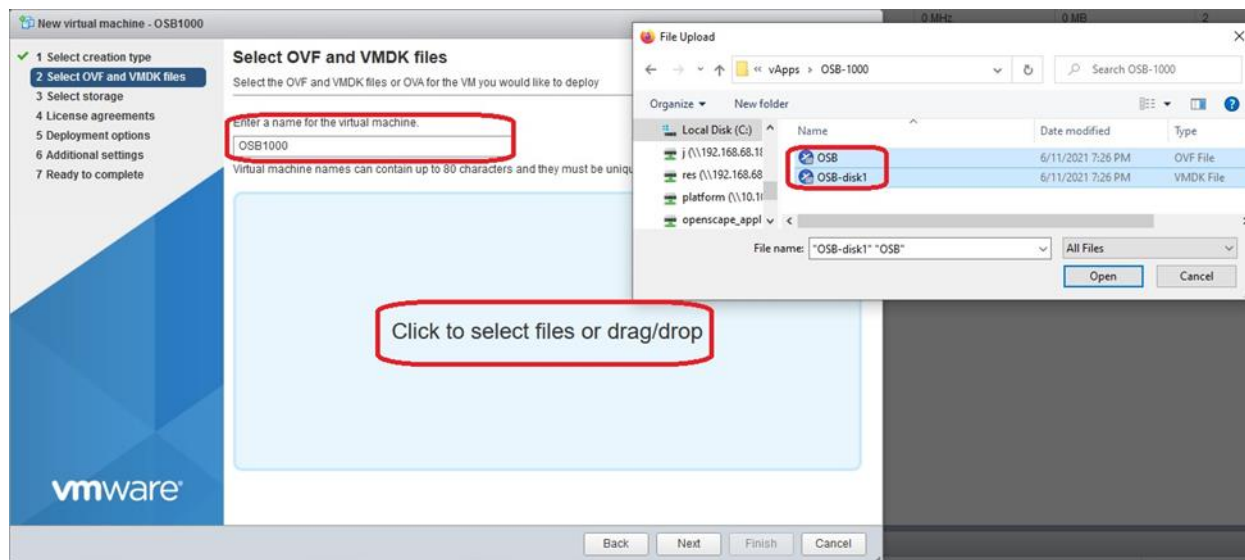


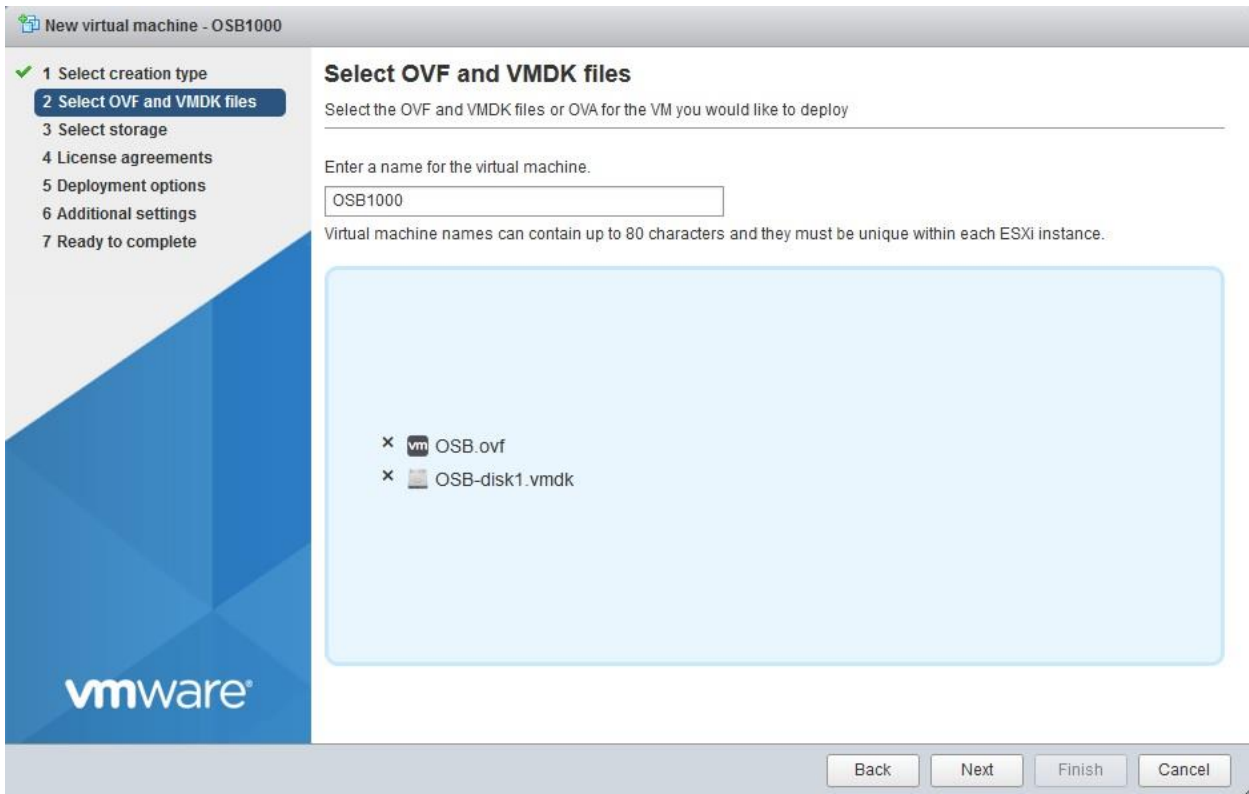
Enter the virtual machine **Name**. The name must be unique for each virtual machine and can contain up to 80 characters.

Select the files from the following profiles in vApps:

- a) **OSB-250**
- b) **OSB-1000**
- c) **OSB-6000**

Click to select files or drag/drop and choose the **OSB.ovf** and **OSB-disk1.vmdk** files.

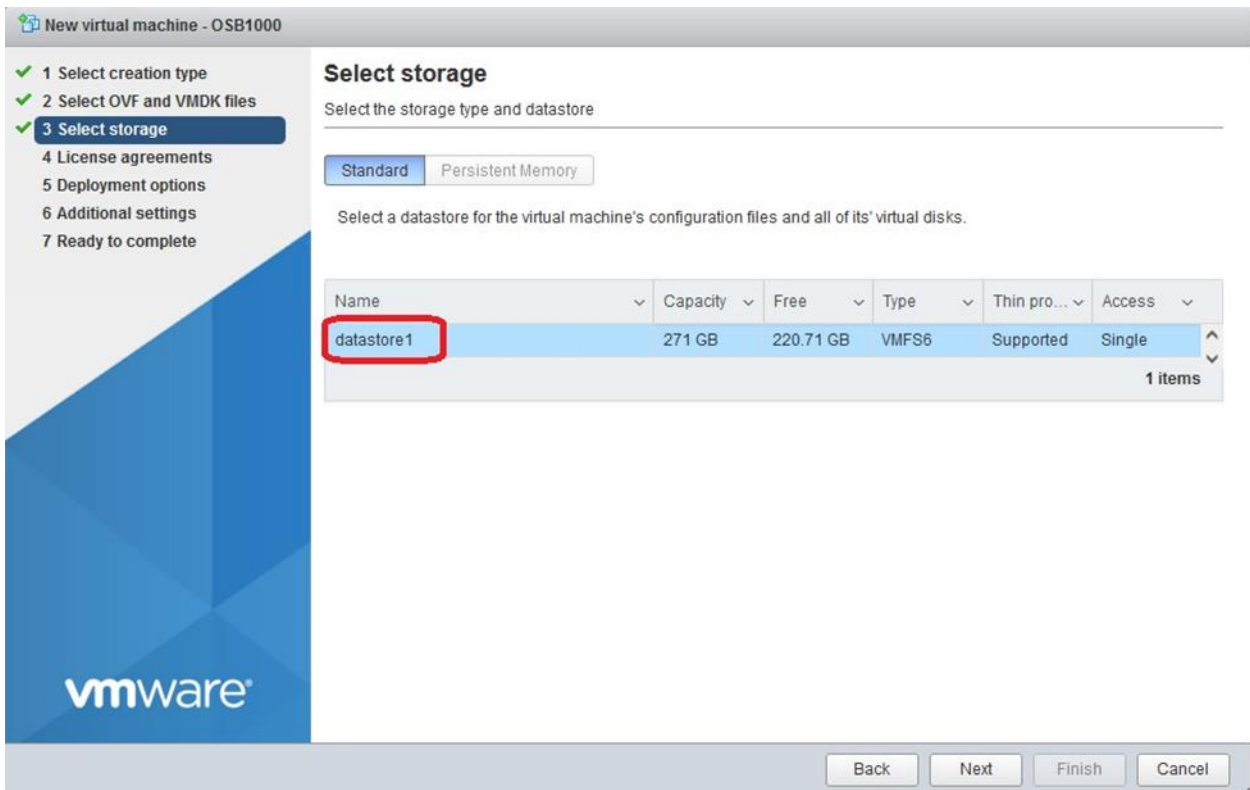




Select **Next**.

The **Select storage** windows appears.

Select the destination storage from the datastore list.



Select **Next**.

The **Deployment options** window appears.

Set the appropriate **LAN** and **WAN** interfaces in **Network mappings** in accordance with desired OSB configuration type.

Select one of the available Disk Provisioning options:

- a) **Thin**: This method helps you eliminate storage underutilization problems by allocating storage space in a flexible on-demand manner.
- b) **Thick**: Traditional method of storage provisioning. With thick provisioning, large amount of storage space is provided in anticipation of future storage needs. The space might remain unused causing underutilization of storage capacity.

Enabling the **Power on automatically** option, the virtual machine is started automatically after finishing the installation process.

The screenshot shows the 'New virtual machine - OSB1000' wizard in VMware Workstation. On the left, a progress bar indicates five steps: 1. Select creation type, 2. Select OVF and VMDK files, 3. Select storage, 4. Deployment options (highlighted), and 5. Ready to complete. The main area is titled 'Deployment options' and contains a table with the following settings:

Select deployment options	
Network mappings	
LAN	NET37_REDE21
WAN	NET173
Disk provisioning	<input checked="" type="radio"/> Thin <input type="radio"/> Thick
Power on automatically	<input checked="" type="checkbox"/>

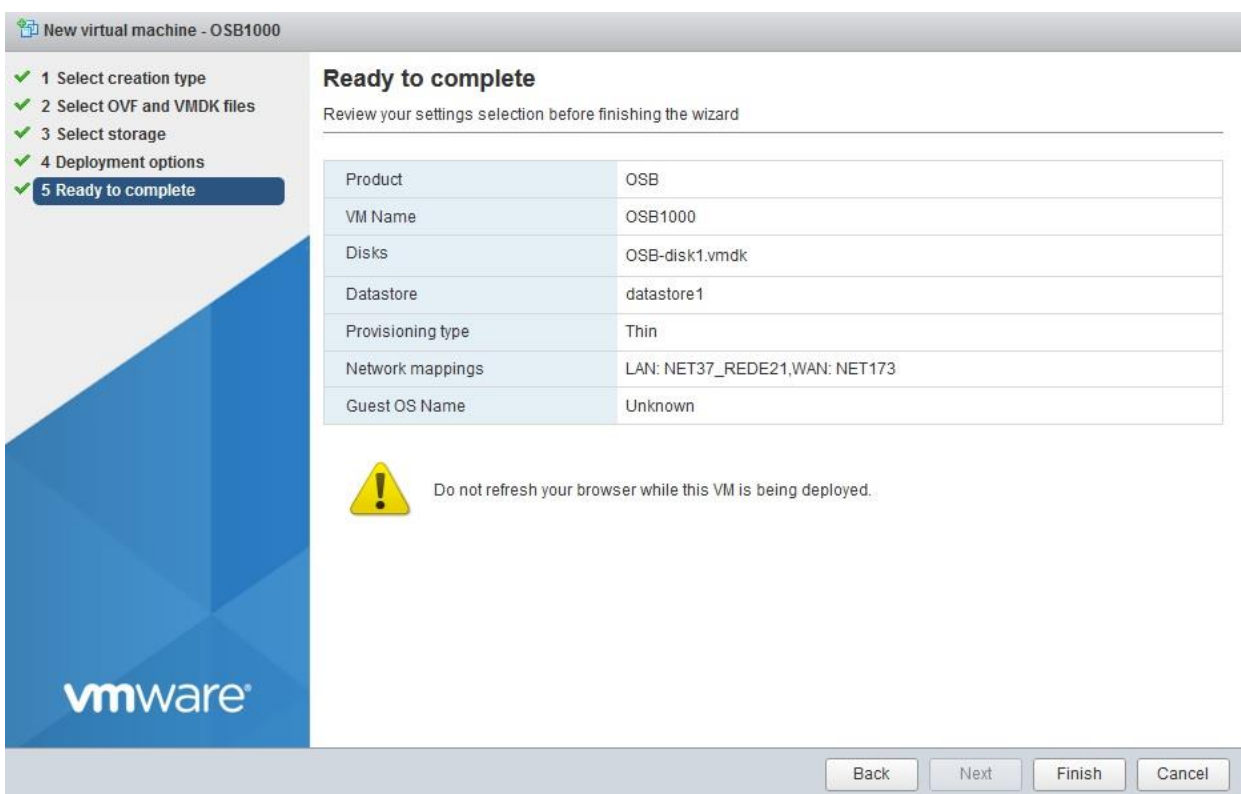
At the bottom right, there are four buttons: 'Back', 'Next', 'Finish', and 'Cancel'. The VMware logo is visible in the bottom left corner of the window.

Click **Next**.

The **Ready to complete** window appears.

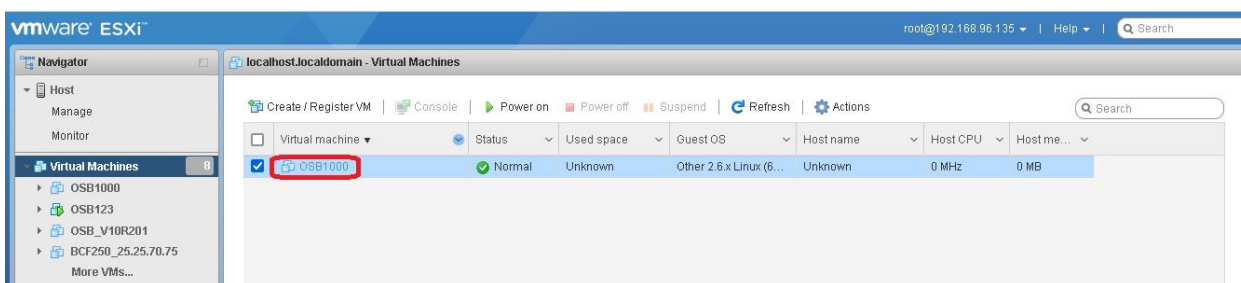
Verify the deployment settings displayed in the work area on the **Ready to Complete** screen and if necessary, use the option **Back** to return to previous configuration windows.

To complete the installation, click **Finish**.



The deployment will start and run to completion. When the process is completed, the virtual OpenScale Branch appliance will be ready to power on.

VM for Virtual OSB 1000 has been created.



Note:

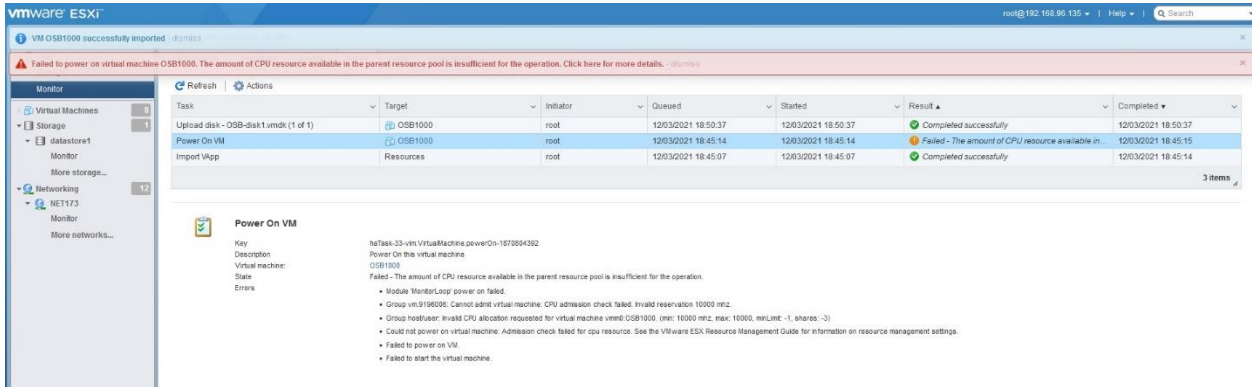
When deploying vApps these values are set automatically (based on the 2.5 GHz core processor).

In OVF file in vApps, the CPU reservation is configured for Virtual OSS 250 (5000 MHz), Virtual OSS 6000 (10000 MHz) and Virtual OSS 20000 (20000 MHz).

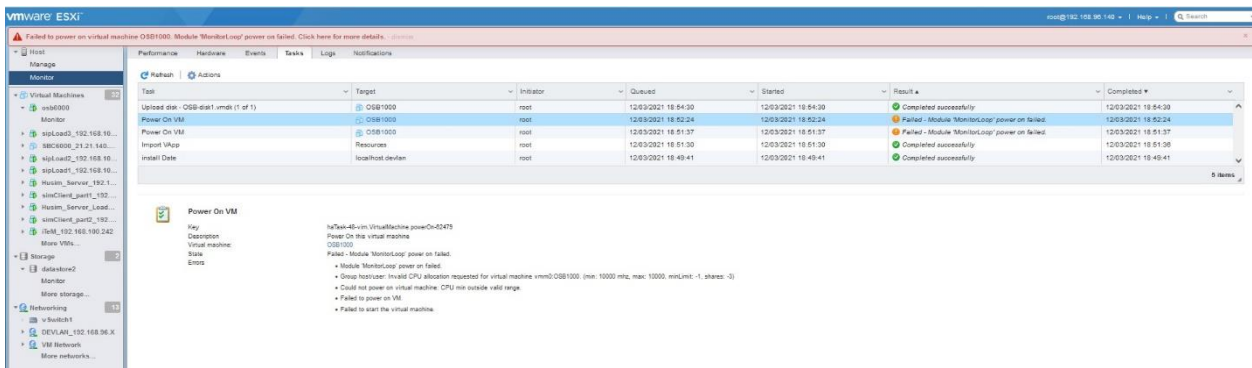
Regardless if VM has been created manually or with vApps, these values need to be adjusted to fit the host processor capabilities. Other critical applications running at same host need to be taken into consideration as well.

The recommended settings for the reservation is the number of cores used by OSB/SBC multiplied by the core frequency of host processor.

If the resources are not available in used VMWare Host server or due to the processor type, the following messages can be received in virtual machine power on:



- **“Failed - The amount of CPU resource available in the parent resource pool is insufficient for the operation.”**



- **“Failed - Module 'MonitorLoop' power on failed.”**

In this case, it is necessary to set the parameter Reservation to a value that fits the host processor capabilities (considering also other applications) and parameter Limit=Unlimited.

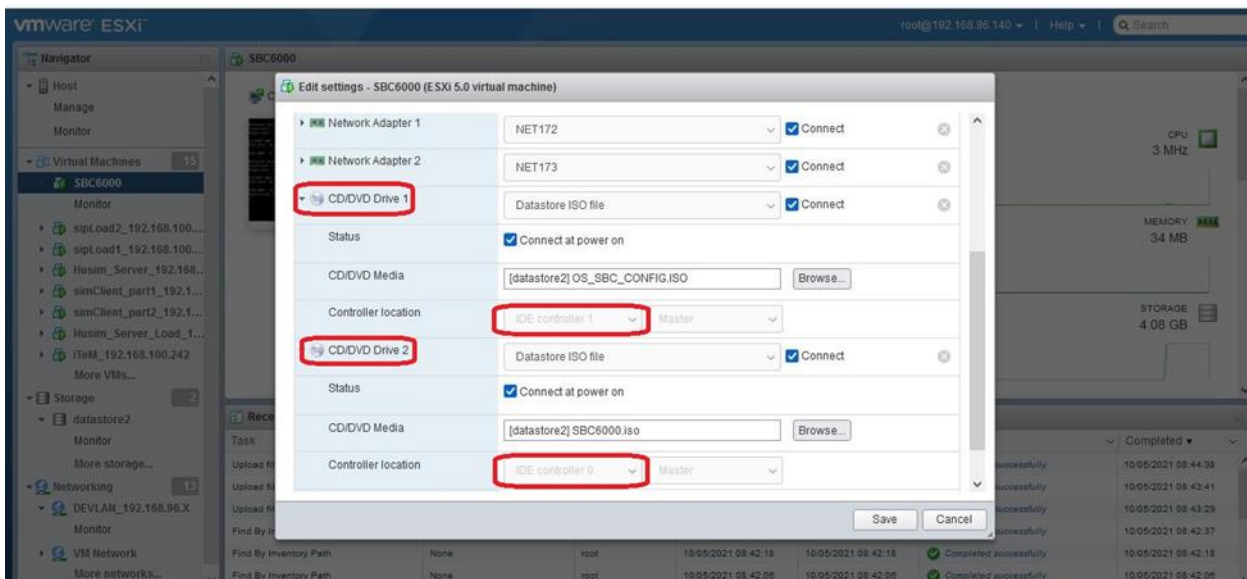
To avoid this risk, close monitoring of the SBC CPU usage is recommended. An alarm is raised when there is high CPU usage.

Note:

Using vApps, **two CD/DVD Drive** are created in virtual machine.

Verify the **CD/DVD Drive 1** and **CD/DVD Drive 2**. The OSB system software ISO file is connected in **CD/DVD Drive** that is associated with **IDE Controller 0(IDE 0)**.

The other **CD/DVD Drive** is associated to **IDE Controller 1(IDE 1)**, that is used to connect the OSB Configuration ISO file related to xml database. **If it is not used, this CD/DVD Drive associated to IDE Controller 1 can be removed.**

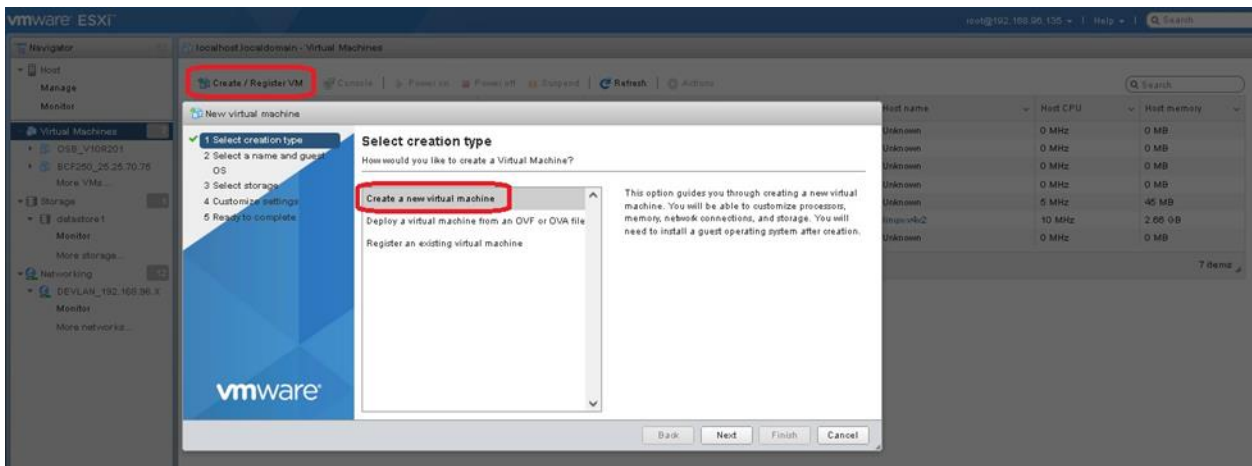


70.7 Creating VM manually

ESXi 6.5 or higher can be managed by any web browser using the VMware Host Client, which is based on HTML5 technology.

In order to create the Virtual Machine (VM), user select the option to create the VM manually.

Login to vSphere Host Client and select **Create/Register VM** and choose **Create a new virtual machine** option.



Click **Next** button.

The **Select a name and guest OS** window is displayed.

Enter the name of the OpenScape Branch virtual machine in the **Name** field. The name must be unique for each virtual machine and can contain up to 80 characters.

Choose the option to **Compatibility (ESXi 6.5 virtual machine or higher)**, **Guest OS family (Linux)** and **Guest OS version (Other 2.6x Linux (64 bit))**.

New virtual machine - OSB1000 (ESXi 6.5 virtual machine)

1 Select creation type

2 Select a name and guest OS

3 Select storage

4 Customize settings

5 Ready to complete

Select a name and guest OS

Specify a unique name and OS

Name

OSB1000

Virtual machine names can contain up to 80 characters and they must be unique within each ESXi instance.

Identifying the guest operating system here allows the wizard to provide the appropriate defaults for the operating system installation.

Compatibility

ESXi 6.5 virtual machine

Guest OS family

Linux

Guest OS version

Other 2.6.x Linux (64-bit)

Back

Next

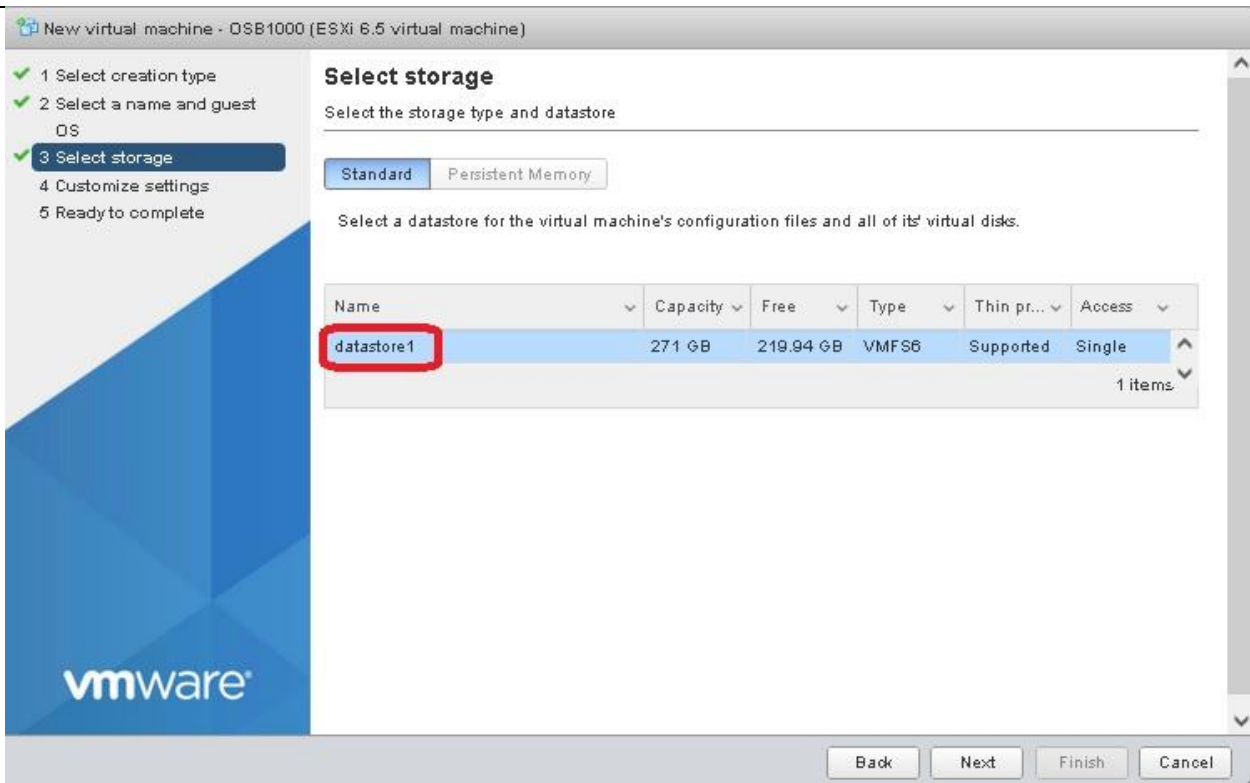
Finish

Cancel

Click the **Next** button.

The **Select storage** window is displayed.

Select the **datastore** (Name) from the datastore list display in which to store the OpenScape Branch virtual machine file.



Click the **Next** button.

The **Customize settings** screen is displayed.

Select the CPU, Memory and Hard Disk capacities in accordance with the desired Hardware Type:

Deployment	Virtual OSB-250	Virtual OSB-1000	Virtual OSB-6000
CPU	2	4	8
Memory(GB)	4	4	6
HD size(GB)	40	40	60

The number of processors in use depends on the number of licensed CPUs on the host and the number of processors supported by the guest OS.

By default, the parameter CPU Reservation is configured as None and CPU limit is configured as Unlimited if the virtual machine has been installed manually.

If the virtual machine has been installed using vApps, the specified values are reserved in accordance with the values in the table.

The same procedure applies to the amount of **Memory**.

When deploying vApps these values are set automatically (based on the 2.5 GHz core processor).

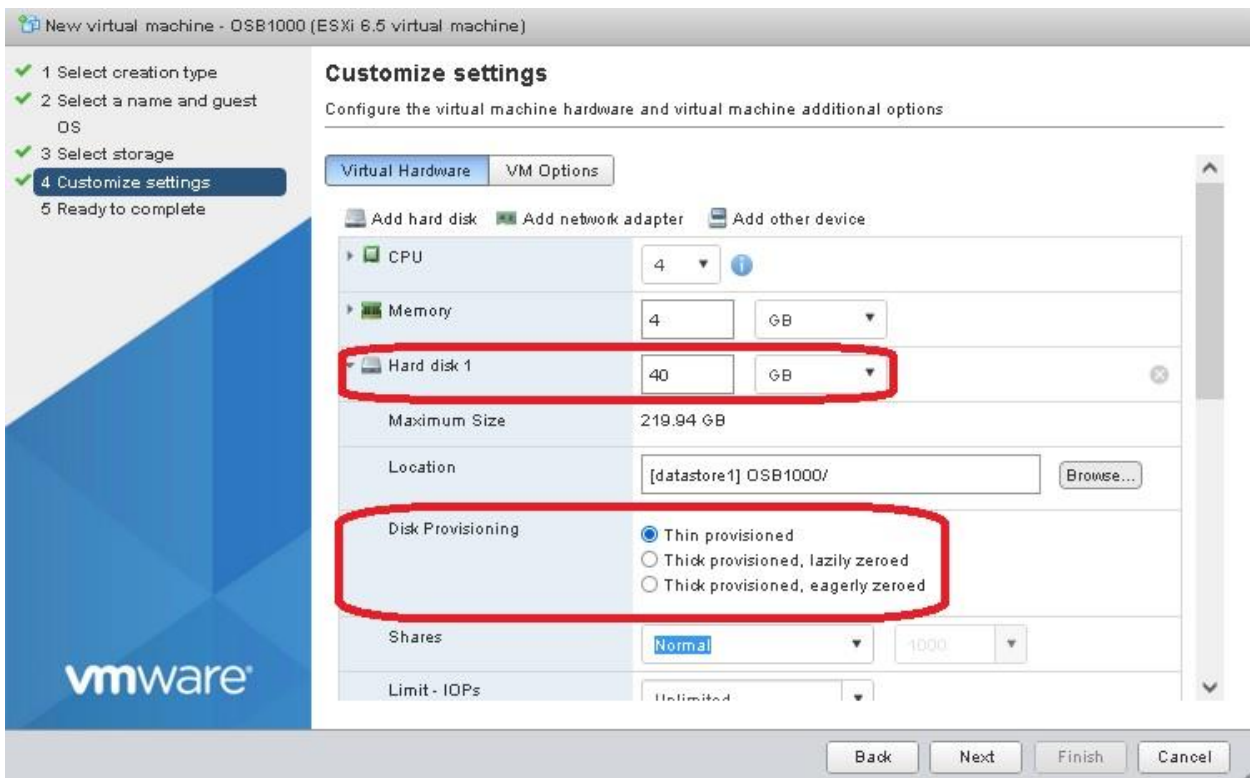
In OVF file in vApps, the CPU reservation is configured for Virtual OSS 250 (5000 MHz), Virtual OSS 6000 (10000 MHz) and Virtual OSS 20000 (20000 MHz).

Regardless if VM has been created manually or with vApps these values need to be adjusted to fit the host processor capabilities. Other critical applications running at same host need to be considered as well.

The recommended settings for the reservation is the number of cores used by OSB/SBC multiplied by the core frequency of host processor.

Select the **Hard Disk** size for the virtual machine. The value should be set to e.g., **Hard Disk = 40 GB**. Choose Thin or Thick provisioned option.

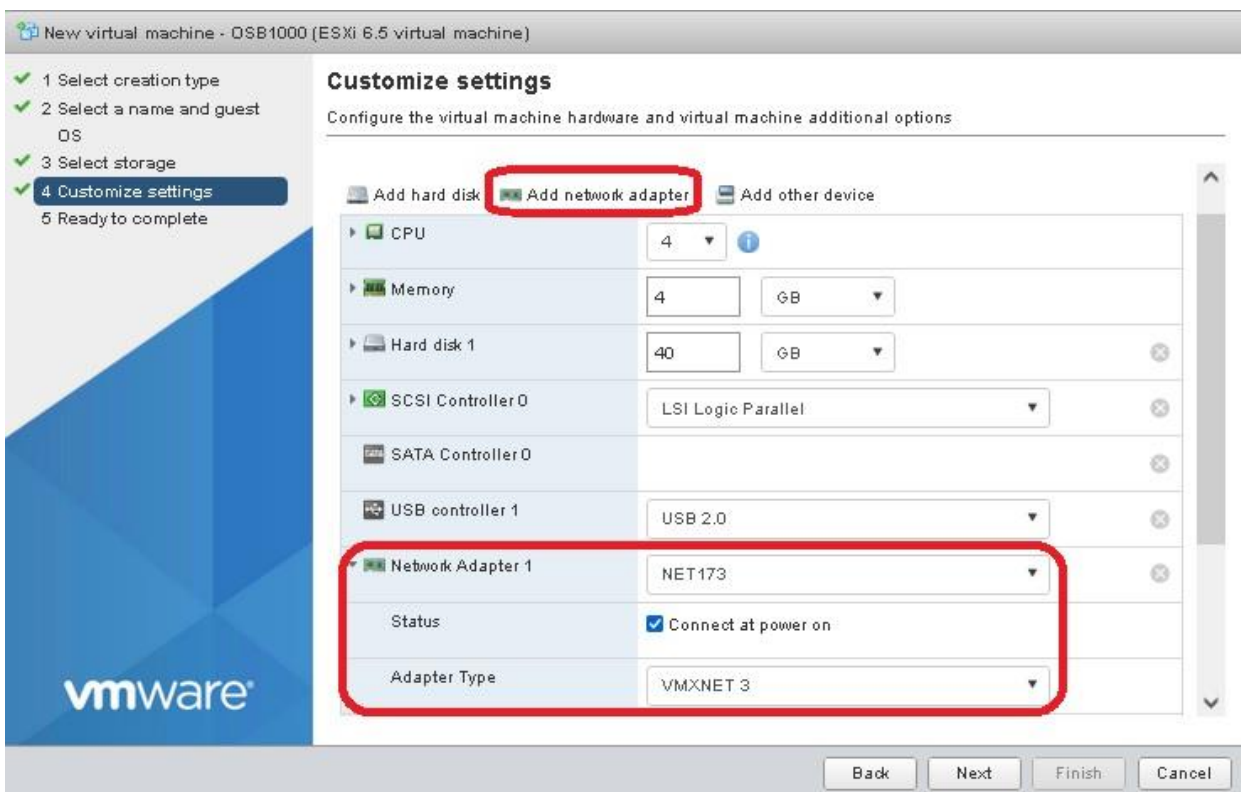
- **Thin:** This method helps you eliminate storage underutilization problems by allocating storage space in a flexible on-demand manner.
- **b) Thick:** Traditional method of storage provisioning. With thick provisioning, large amount of storage space is provided in anticipation of future storage needs. The space might remain unused causing underutilization of storage capacity.



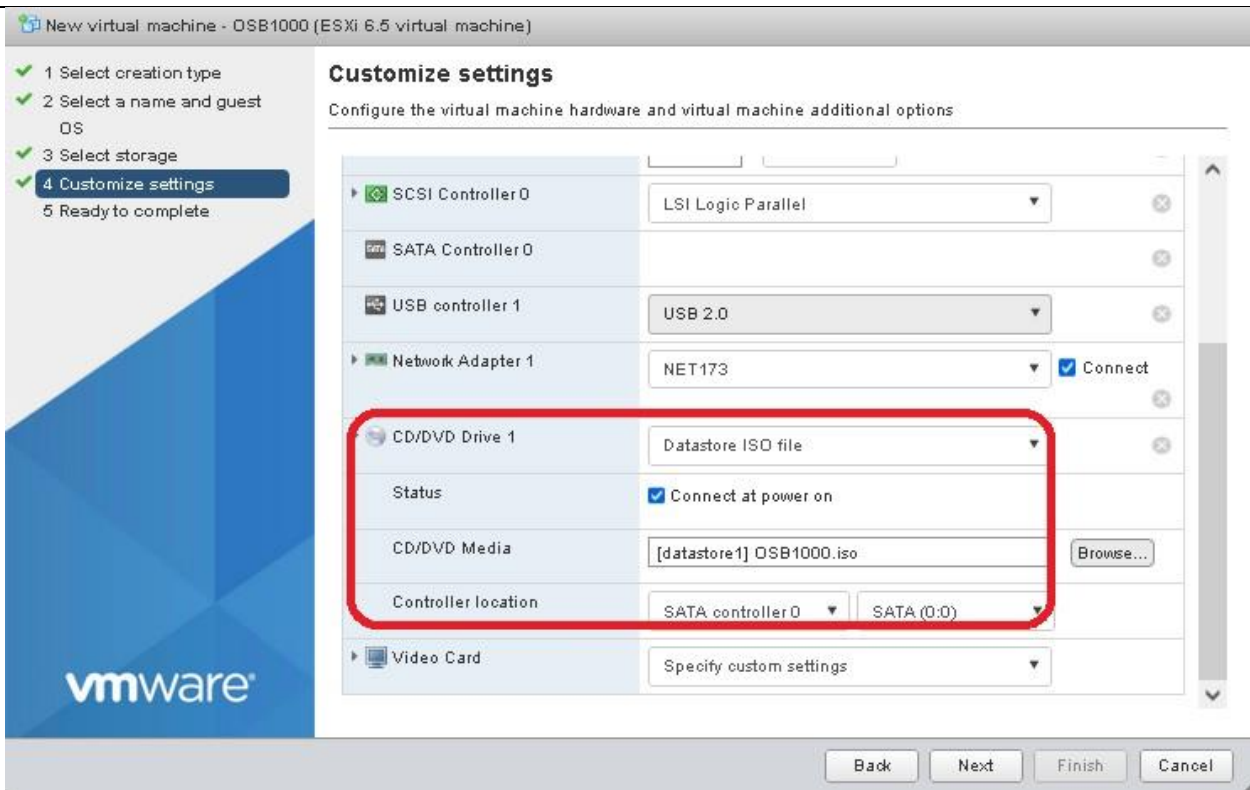
Set the number of network interfaces based on the Hardware Type. Use the option **Add network adapter** to increase the number of NICs in virtual machine. In Network adapter uses **VMXNET3** option in **Adapter Type** field.

Connect at Power On checkboxes is activated for the NICs.

For **SCSI Controller** select the **LSI Logic Parallel** option.



Normally the virtual machine is created only with one **CD/DVD Drive 1**. Verify if the **controller location type** is using **SATA Controller 0 - SATA (0:0)**. The ISO file related to system software is added in this device.

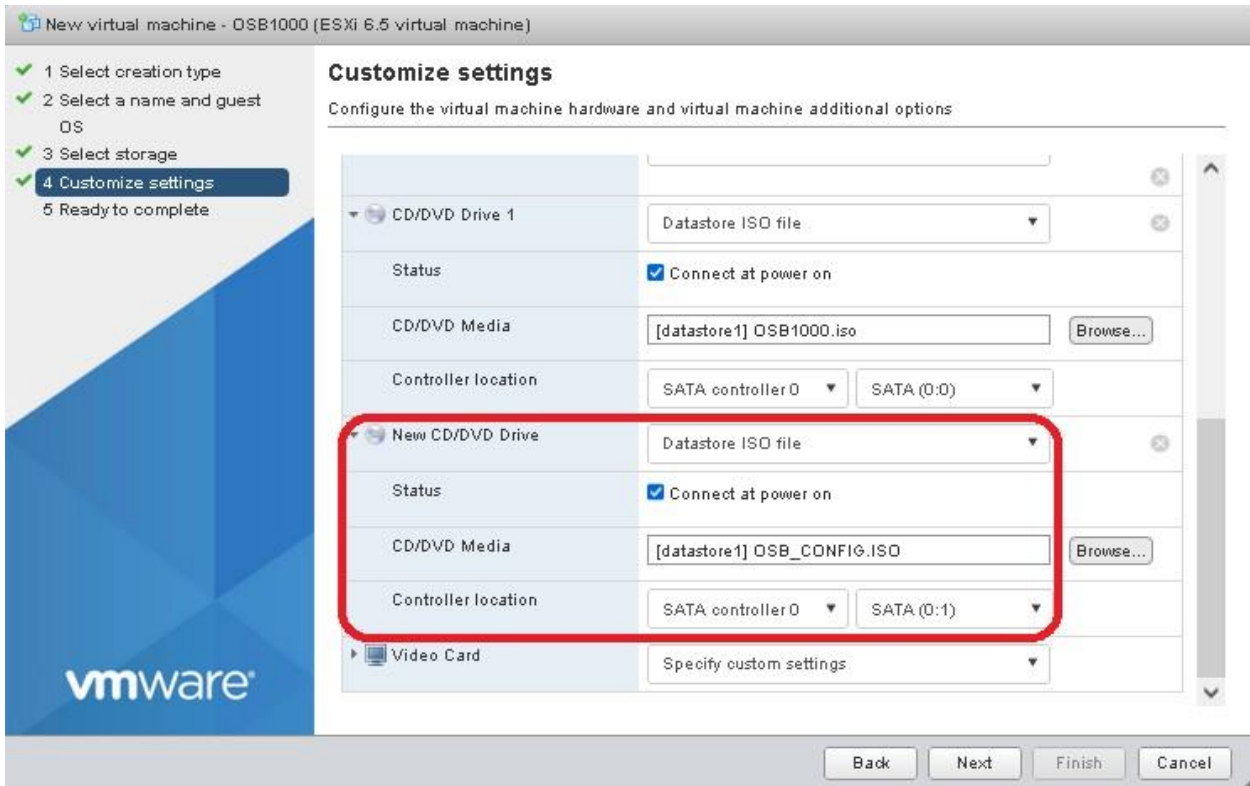


Note:

If the system is not detecting the CD/DVD, please change the **controller location type** from **SATA** to **IDE (IDE controller 0)** type.

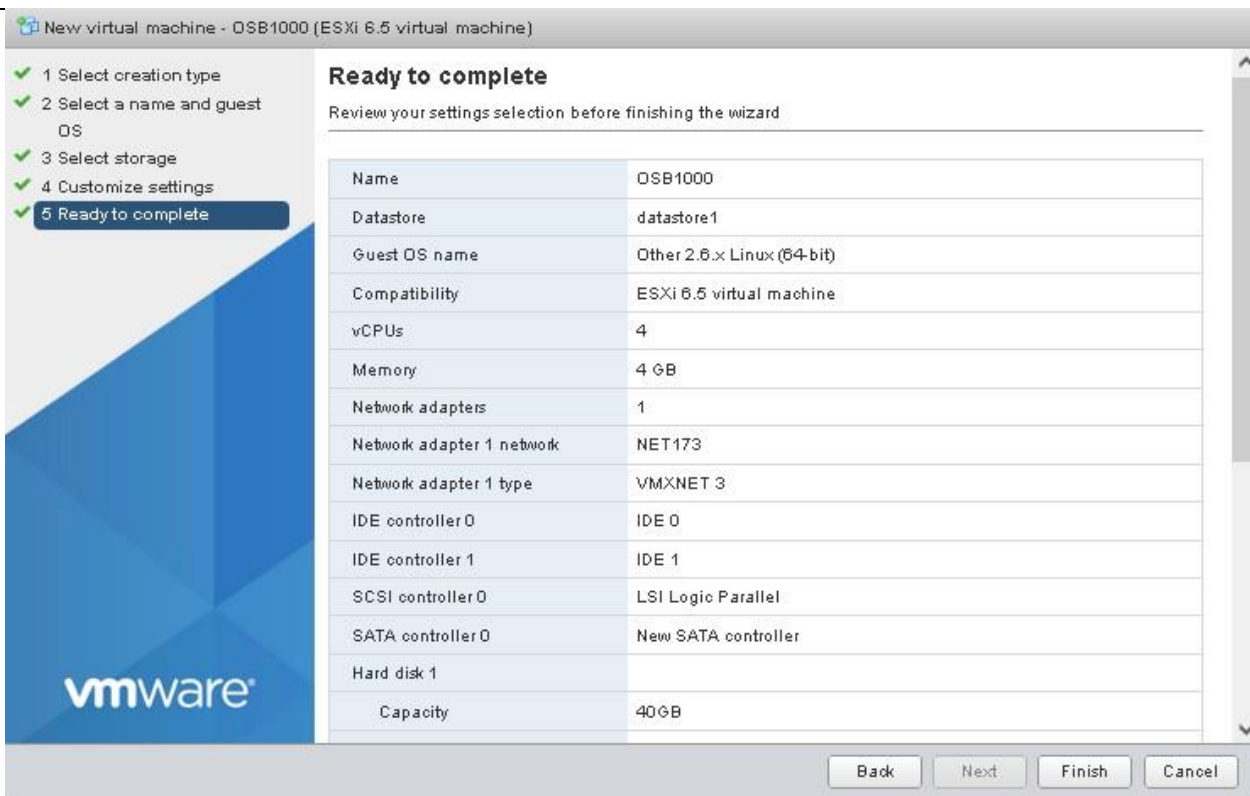
If ISO file related to database is used, add another CD/DVD device. Add using **Add other device, CD/DVD drive** option. **New CD/DVD Drive or CD/DVD Drive 2** is using **SATA Controller 0 - SATA (0:1)**. Configure the OSB Configuration ISO file repeating the procedure used to CD/DVD Drive 1.

Connect at Power On checkboxes is activated for CD/DVD Drives.



Click the **Next** button.

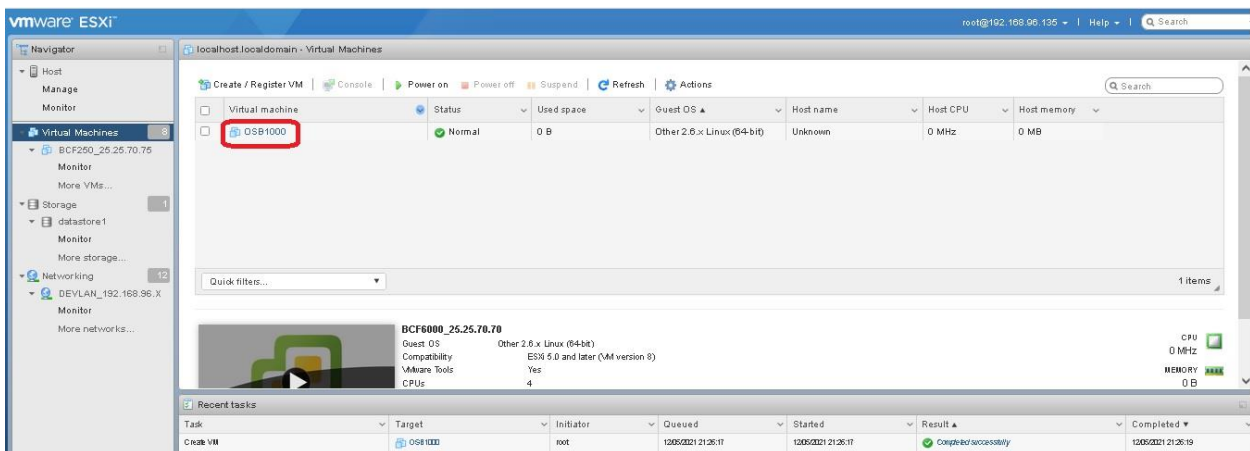
The **Ready to complete** screen is displayed.



Prior to starting the task that will create the OpenScope Branch virtual machine, check the **virtual machine properties**. If it is necessary to correct some parameter, use the **Back** option to return to previous settings and change it.

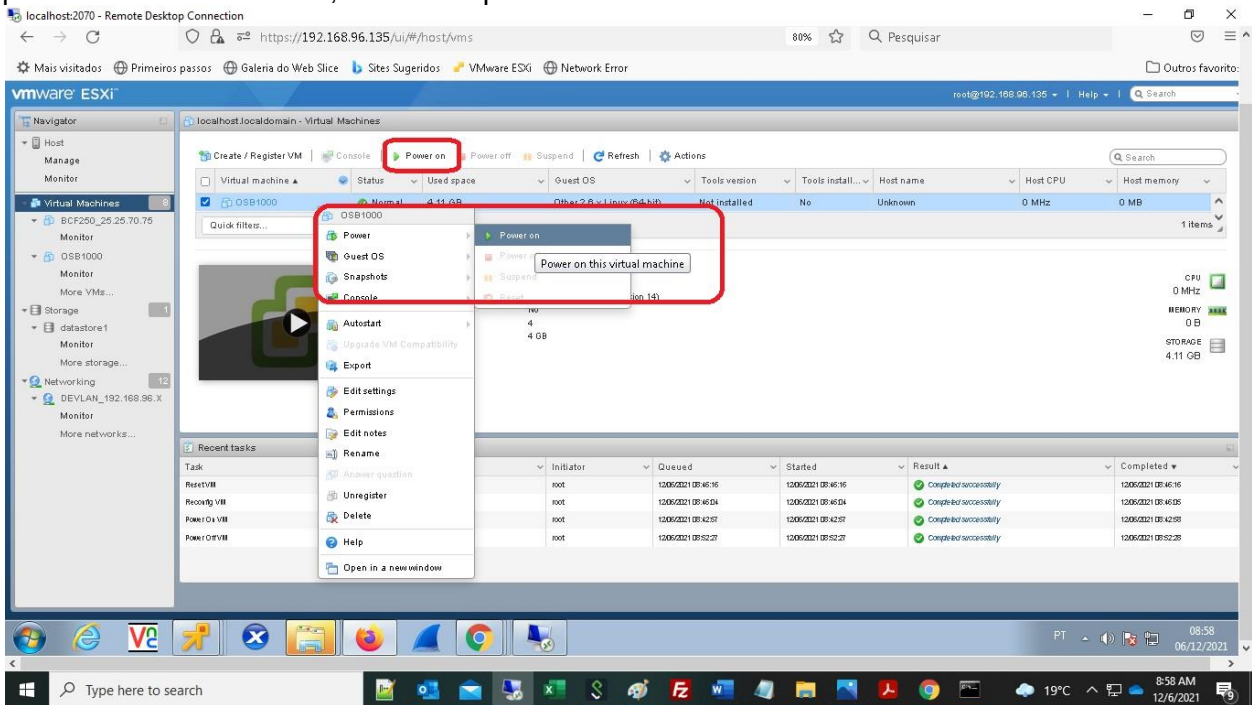
Press **Finish** to complete the virtual machine creation.

The OpenScope Branch virtual machine is created.

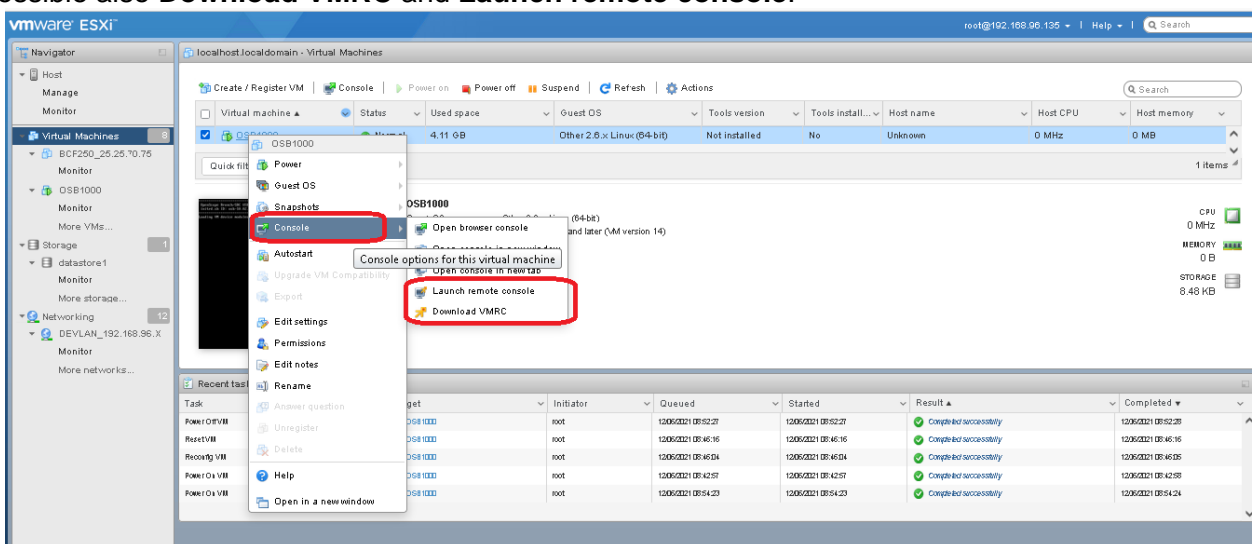


70.8 Virtual OSB Installation

Having completed the VM installation, user must power on the VM in order to start the virtual OSB installation procedure.



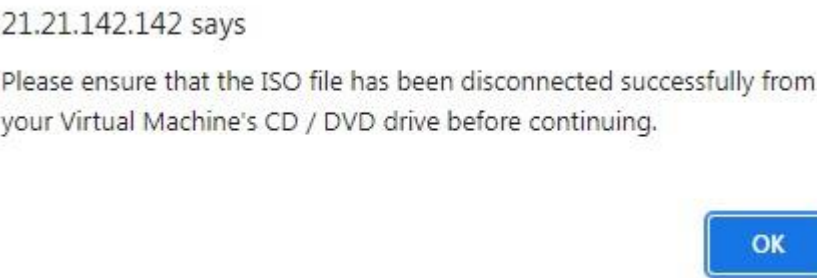
VMware offers console to monitor the boot up sequence of the VM. It is possible also **Download VMRC** and **Launch remote console**.



Once the VM has booted up, user can login to the Local GUI page in order to complete the installation procedure, in the same way as it is executed for native hardware.

Before the first reboot user is prompted by the OSB to detach the ISO file from the VM's CD/DVD drive.

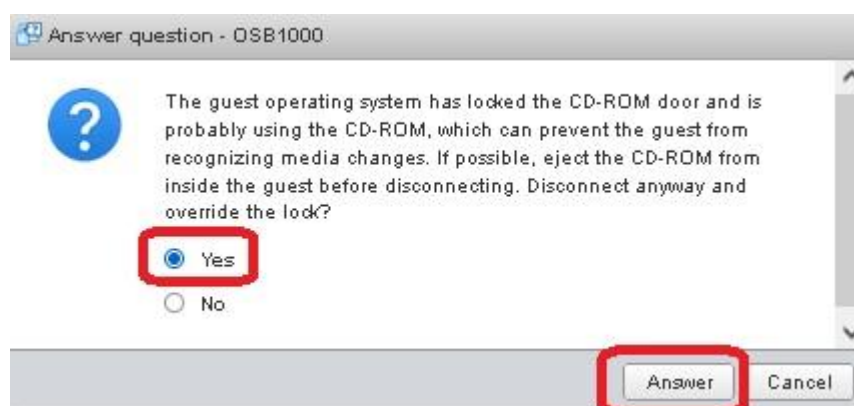
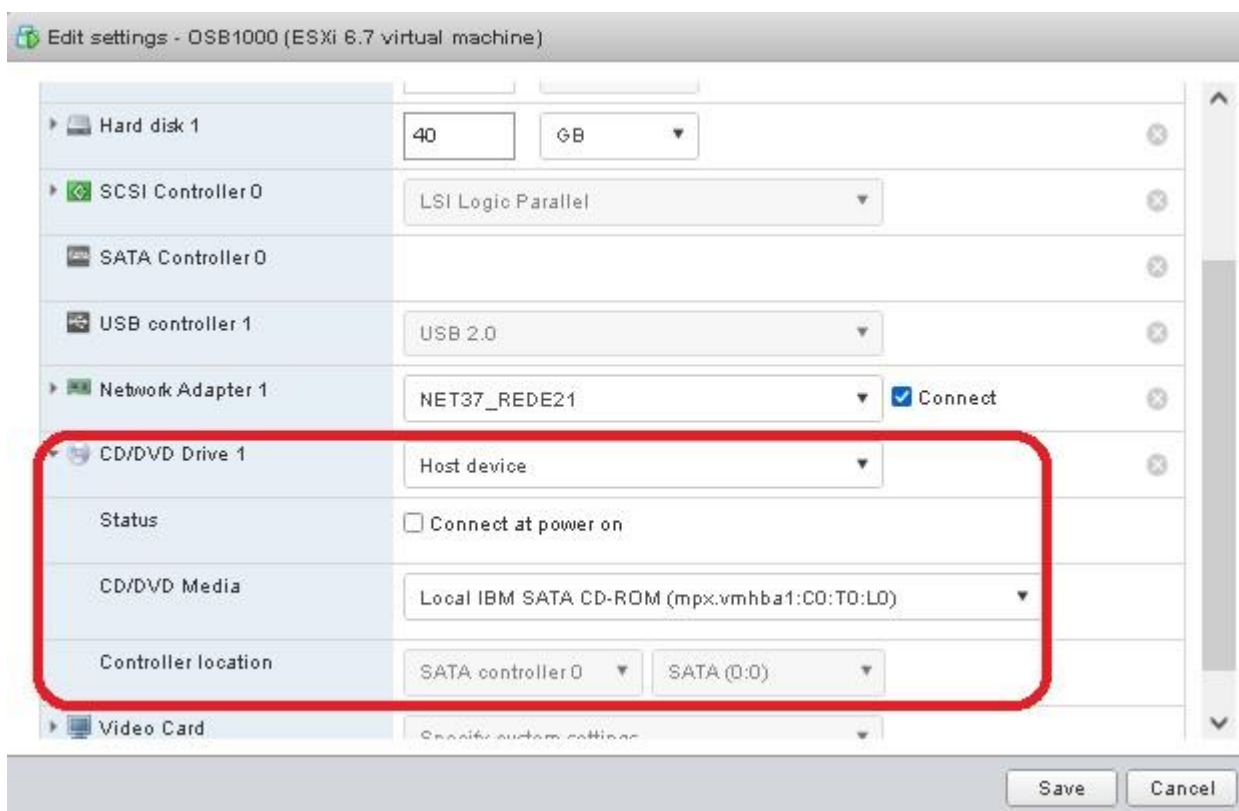
Select **"OK"** on the OSB local GUI in order to reboot and complete the installation procedure.



Installation has been completed but keep in mind that the iso file in the CD/DVD virtual drive is set to connect at power on. This means that if the VM is powered off and then powered on again, installation procedure will be initiated again.

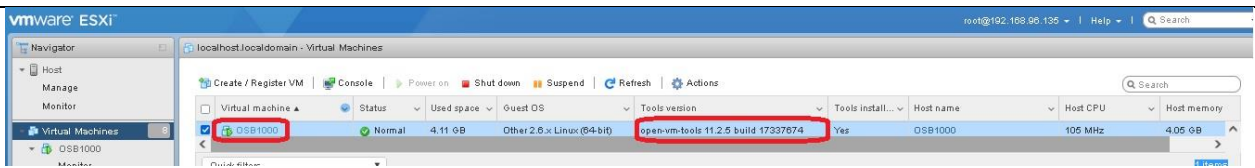
It is strongly recommended to edit the VM settings and set the **CD/DVD drive to "Host Device"** option and **remove the "Connect at power on" flag**.

Select **Yes** and **Answer** question to complete this procedure.



Note:

From V10, the open-vm-tools is installed in full install and the flag **Enable Open VM Tools** should be checked in **System / Settings**. If checked, this field enables the **Open Virtual Machine Tools (open-vm-tools)**.

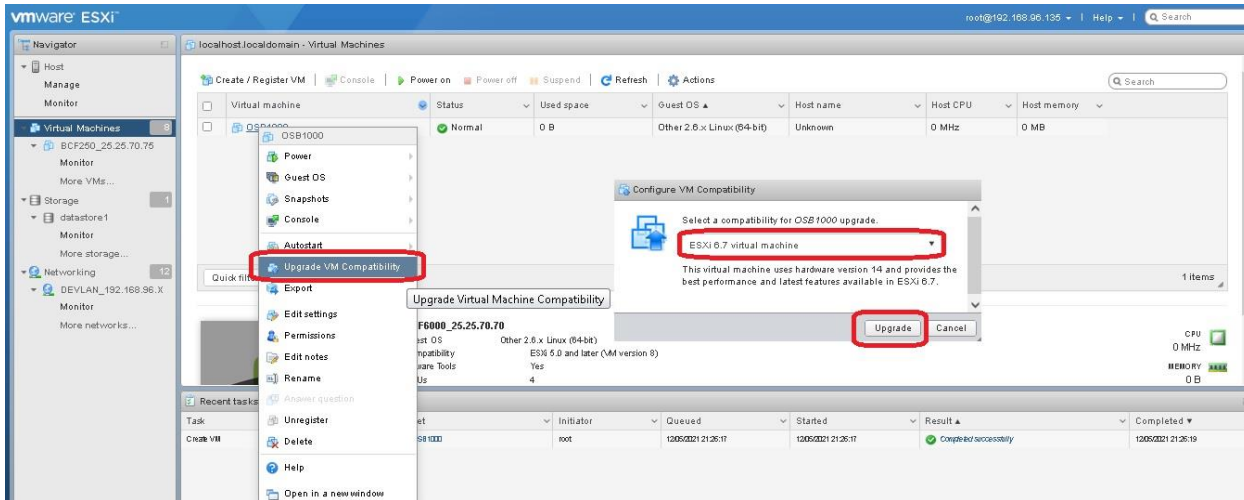


70.9 VM version

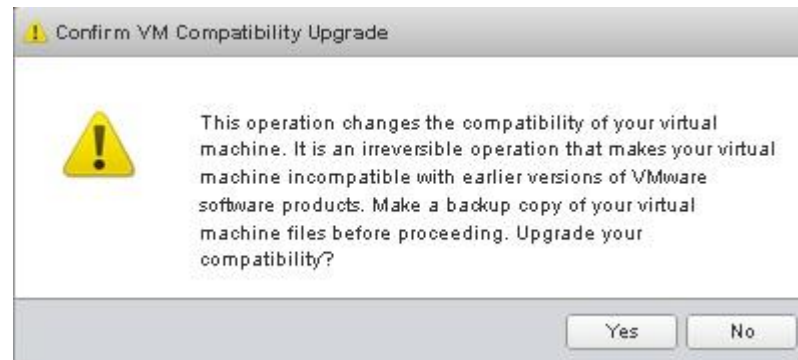
VMware offers the option to upgrade the virtual hardware version. VM must be powered off in order to upgrade the virtual hardware.

Upgrading a Virtual Machine to the latest hardware version is the physical equivalent of swapping the drive out of one system and placing it into a new one. VMware does not recommend upgrading virtual hardware version if you do not need the new features exposed by the new version.

Set the option **Upgrade VM Compatibility**, select the available options and press **Upgrade**.



The message **Confirm VM Compatibility Upgrade** is shown. Press **Yes** to confirm the upgrade.



VM version 10 @ ESXi 5.5 and later
VM version 11 @ ESXi 6.0 and later
VM version 13 @ ESXi 6.5 and later
VM version 14 @ ESXi 6.7 and later
VM version 15 @ ESXi 6.7U2 and
VM version 17 @ ESXi 7.0 and later
VM version 18 @ ESXi 7.0U1 and
VM version 19 @ ESXi 7.0U2/U3 and later

70.10 OpenScape Branch and SBC distribution via OVA

The OpenScape Branch is now distributed in an Open Virtual Appliance (OVA) package to simplify the deployment on a VMware installation.

This OVA contains a pre-installed, ready-to-use, software of the OpenScape Branch, with the following configuration:

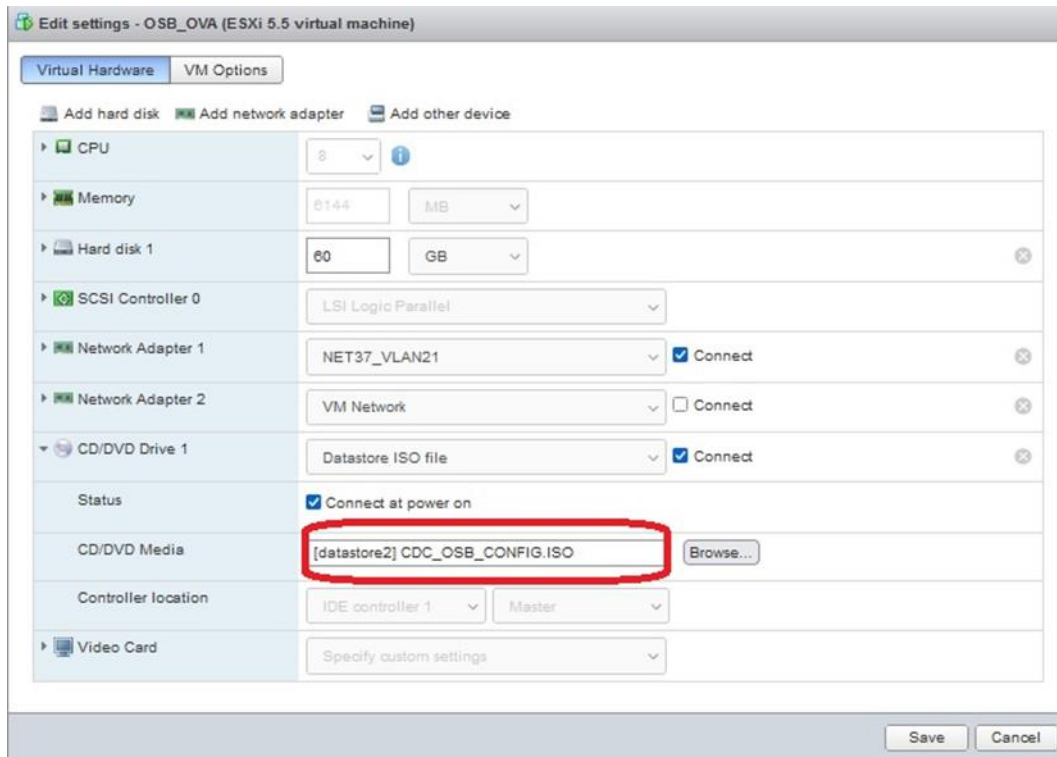
	HW Type	Num of CPUs	Ram memory	Disk space	Lan IP	Wan IP
OS Branch	Virtual OSB 6000	8	6Gb	60Gb	10.20.30.51/24	none

Only in the first boot, the system tries to find a CD/DVD on the VM and looks for an XML configuration file. If this file is present, the system automatically applies it.

This XML file must be one OpenScape Branch database file compatible with the version and with also desired configuration. For example: with another LAN IP and WAN IP configuration when it is configured.

In case it is used together with OVA installation, the XML file must also be one ISO file. The OpenScape Branch XML file must be renamed to: **CDC_OSB_CONFIG.ISO**

NOTE: Please do not set the parameter **Power on** after deployment in OVA installation if you choose the option to connect the CD/DVD with ISO file in first boot.



In V10R2 OVA, the system has 5 partitions.

70.11 VLAN configuration for OSB VM

L2 switch ----- ESXi Host ----- OSB VM

Port on L2 switch configured as untagged

ESXi Host VLAN configured: None (0) ---- OSB: No VLAN ID config

ESXi Host VLAN configured: All (4095) ---- OSB: No VLAN ID config

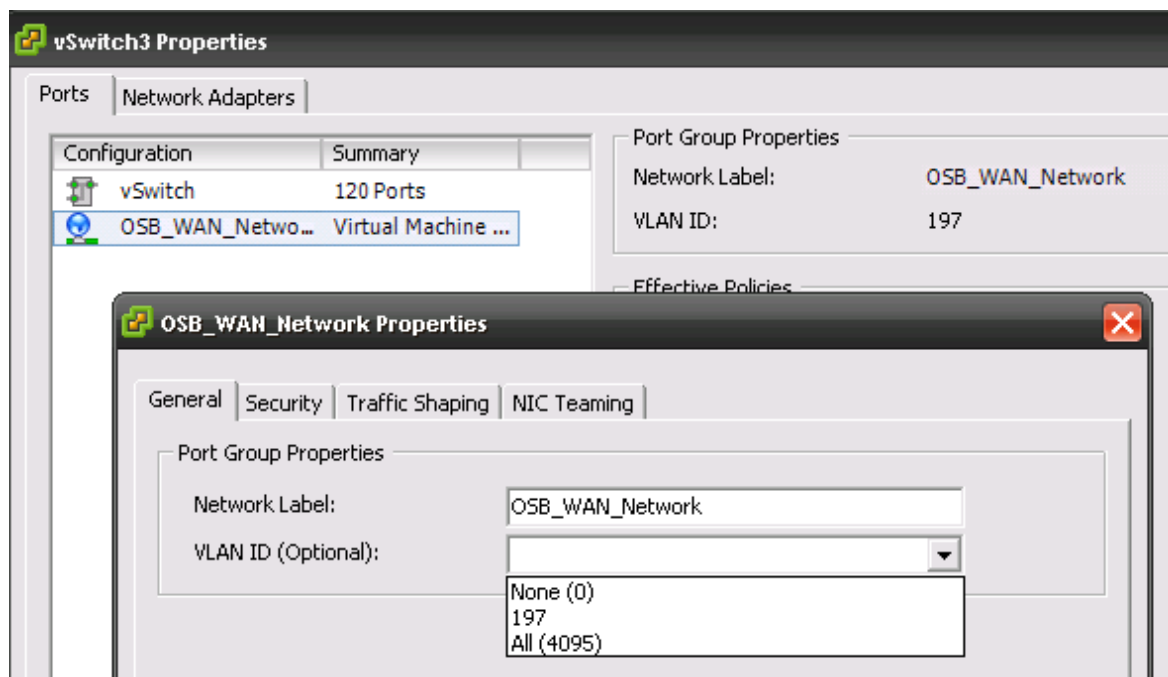
Port on L2 switch configured as tagged

(e.g. vlan 197)

ESXi Host VLAN configured: 197 ---- OSB: No VLAN ID configured

ESXi Host VLAN configured: All (4095) ---- OSB: VLAN ID 197 configured

ESXi Host Interface VLAN configuration



71 Hosted OpenScape Branch with Secured Management Network

This feature is used for customers that need a separation between management and SIP/VoIP network, using a hosted solution through IPSec tunnel.

This is also a solution for customer which needs to manage OpenScape Branch located under a public network and connected to OpenScape SBC Server.

71.1 Network Requirements

71.1.1 VPN Concentrator Options

The VPN Concentrator shall be configured to establish an IPSec tunnel to each Hosted OpenScape Branch. When creating the VPN Concentrator IPSec tunnel, it must be taken into account that the following configuration is accepted by OpenScape Branch:

VPN type: IPSec Strong Swan

IPSec Protocol: ESP

IPSec Mode: Tunnel

Authentication algorithms: RSA Signature or PSK

Hash Algorithm: md5, sha1 or sha:256

Encryption Algorithms: 3DES, AES-128 or AES-256

DH Group: 2, 5 or 14

IKE version 1

VPN's Supported Features: NAT Traversal, Dead Peer Detection, Perfect Forward Secrecy(PFS), compression

Note:

Open SSL (openVPN) is not released for this feature.

For Geo-Separated configuration, it is possible to have one secured management network for each Data Center (e.g. in the case of more than one CMP on different networks). In this case, use one VPN Concentrator for each site.

It is suggested to use Fortinet FortiGate 1240B VPN Concentrator, although other VPN concentrator products configured in the above configuration are also possible.

The VPN Concentrator's Redundancy feature is not supported at the moment.

71.1.2 Firewall

It is possible to use a Firewall Server between CMP and hosted secured network (firewall could be possibly included within the VPN Concentrator equipment). If enabled, firewall shall be configured with the following rules to access some of the applications:

HTTPS : port 443 allowed – for management communication

FTP : port 21 and **SFTP :** port 22 allowed – for general file transferring, trace file transfer (OSV-TM), CDR push (Billing Server) or software load.

HTTPS : ports 4709 and 444 – for communication with OpenScape Branch Assistant and Fault Management

HTTPS : ports 18443 and 18080 – for DLS and DCMP Server communication

Other services, if required: DHCP (ports 67 and 68), DNS (port 53), SNTP (port 123), etc.

71.1.3 Network Configuration

For the WAN connection, it is required that VPN Concentrator and OpenScape Branch have a public IP following the external public IP routing requirements. These addresses should be routed separated from the public addresses used for VoIP, even if the sub network has some overlaps.

The management address (Admin IP) used for the secured access to the OpenScape Branches is a private IP and should be routed internally only. This address must be routed from the CMP (or from any other management Server within secured management network) to the VPN concentrator of respective Data Center.

71.2 Configuration for OpenScape Branch

71.2.1 Configuring the VPN using IPSec

Create a VPN tunnel between OpenScape Branch and VPN Concentrator.

Go to **OpenScape Branch Assistant > Configuration > Security** and select **IPSec** tab. Click on the **Add** button to create a VPN connection.

The screenshot shows the 'Edit IPsec' configuration window. The fields and their values are as follows:

- Name:** AdminIP
- Partner:** 20.1.1.1
- Partner network :** 192.168.0.0
- Partner netmask:** 255.255.0.0
- Authentication type:** secret
- Certificate profile :** VPN default
- ☐ Enable compression
- Local network:** 10.102.0.80
- Local netmask:** 255.255.255.255
- Secret key file:** hipath
- ☐ Enable PFS

Yellow callout boxes provide additional information:

- Enter IPsec tunnel name:** Points to the 'Name' field.
- Enter the public IP address of VPN Concentrator here.** Points to the 'Partner' field.
- Under Local Network, enter the Admin IP with Local netmask 255.255.255.255.** Points to the 'Local network' and 'Local netmask' fields.
- Partner network defines the network of secured management on the cloud side. The CMP address shall be within this network.** Points to the 'Partner network' and 'Partner netmask' fields.
- Enable PFS and compression are optional, depending on the VPN concentrator configuration.** Points to the 'Enable compression' and 'Enable PFS' checkboxes.
- Choose the Authentication type:**
 - Secret** -> This is the Pre-shared Key method (PSK). It is necessary to define the secret under "Secret key file".
 - X.509** -> This is for RSA signature method (X.509 certificates). It is necessary to define a certificate profile. See configuration below.

Note 1: For the first configuration, CMP must use the WAN address of OpenScope Branch for management. If WAN is not possible, so a local management using the LAN address is required.

Note 2: The configuration of IPsec is possible over WAN interface only. Due to this, this feature is only allowed to OpenScope Branches configured as Branch SBC or SBC-Proxy mode.

71.3 Certificate Profile

Create a certification Profile (optional), as follows:

For Authentication type X.509 selected, it is necessary to create a VPN profile. Before the configuration of IPSec, create a new profile under OpenScape Branch Assistant > Configuration > Security and select **Certificate Management Configuration button** under **General tab**.

To upload customized certificates, go to **General Configuration tab** and **Certificate upload**.

The screenshot shows the 'Certificate Management' window with the 'General Configuration' tab selected. The 'Certificate upload' section is highlighted, showing an 'Upload...' button. A yellow box with the text 'Select Upload add certificate files' points to this button. Another yellow box with the text 'Click to add new certificates.' points to the 'Add...' button in the 'TLS Certificates' panel. A third yellow box with the text 'It is necessary to upload the customized CA Certificate, X.509 and Key files. These certificates shall be also applied to the VPN Concentrator.' points to the 'Certificate' panel at the bottom, which shows a 'Choose File' button and a file path 'serverCA-co...t-sha1.pem'.

Certificate Management

Certificate Management

General Configuration | Certificate Profiles | Certificate expiration checking

System TLS Certificate : VPN default

Certificate creation

Select Upload add certificate files

Name: CA file: CAcert_cust_md5.pem Create

Certificate upload

Upload...

Certificate download

Certificate File: CAcert_cust_md5.pem Download

Key File: certkey_cust_md5.pem Download

TLS Certificates

move certificates

Add... Delete

Self:0 | Items/Page: 200 | All 9

Certificate	Type
CAcert_cust_md5.pem	CA Certificate
serverCA-osb-sha1.pem	CA Certificate
serverCA.pem	CA Certificate
servercert-osb-sha1.pem	X.509 Certificate
servercert_cust_md5.pem	X.509 Certificate
servercert.pem	X.509 Certificate
certkey_cust_md5.pem	Key File
serverkey-osb-sha1.pem	Key File
serverkey.pem	Key File

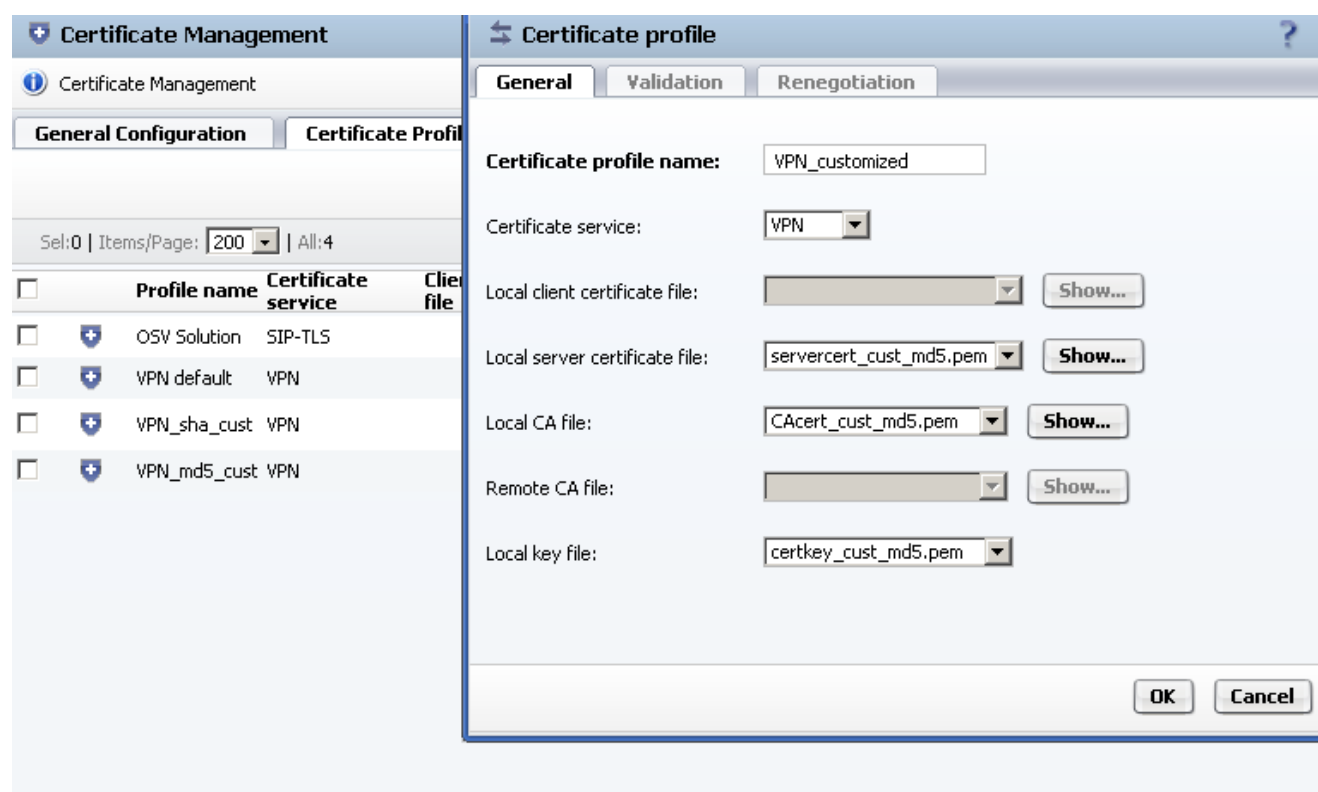
Certificate

CA Certificate Path: Choose File serverCA-co...t-sha1.pem

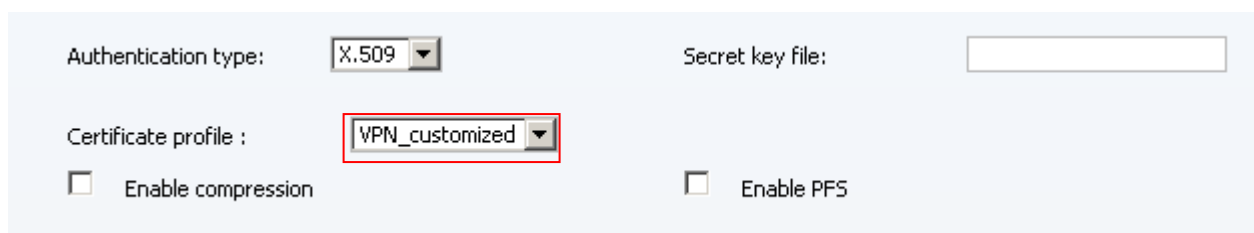
Click to add new certificates.

It is necessary to upload the customized CA Certificate, X.509 and Key files. These certificates shall be also applied to the VPN Concentrator.

To create a new profile, go to **Certificate Profiles** tab and add a new profile, choosing the customized certificates for Certificate service “VPN”.



Select Certificate profile under IPSec configuration page:



To verify the tunnel status, go to Log Files Viewer and check for System Log
Go to Management > Nodes, select Branch Office, and under Dashboard, go to Actions > Log Files.

Select log: System

```
2012-07-16T12:16:09-03:00 [warning] "AdminIP" #1: initiating Main Mode
2012-07-16T12:16:09-03:00 [warning] "AdminIP" #1: received Vendor ID payload [RFC 3947]
2012-07-16T12:16:09-03:00 [warning] "AdminIP" #1: received Vendor ID payload [Dead Peer Detection]
2012-07-16T12:16:09-03:00 [warning] "AdminIP" #1: enabling possible NAT-traversal with method 3
2012-07-16T12:16:09-03:00 [warning] "AdminIP" #1: NAT-Traversal: Result using RFC 3947: no NAT detected
2012-07-16T12:16:09-03:00 [warning] "AdminIP" #1: Peer ID is ID_IPV4_ADDR: '20.1.1.1'
2012-07-16T12:16:09-03:00 [warning] "AdminIP" #1: ISAKMP SA established
2012-07-16T12:16:09-03:00 [warning] "AdminIP" #2: initiating Quick Mode PSK+ENCRYPT+TUNNEL+UP {using
isakmp#1}
2012-07-16T12:16:09-03:00 [warning] "AdminIP" #2: Dead Peer Detection (RFC 3706) enabled
2012-07-16T12:16:09-03:00 [warning] "AdminIP" #2: sent QI2, IPsec SA established {ESP=>0x06f3a5da
<0xc4531dc6}
```

Tunnel name

Add Admin IP to the WAN interface

Go to **OpenScape Branch Assistant > Configuration > Network Service**. Select Interface WAN (Interface2) and Edit. Configure the IP address for management under Admin IP Address:

Edit Interface2

General | **VLAN**

☒ Enabled

IP Address Node 1: 10.100.180.80

Subnet Mask: 255.255.255.0

IP Address Node 2:

Virtual IP Address:

Admin IP Address: 10.102.0.80

Speed: Auto

The Admin IP Address is the same than the configured under Local Network of IPSec.
Note: This configuration is not allowed for OSB Redundant.

Note: Configuration causes system restart.

71.4 Configuration for OpenScape Voice

71.5.1 Configuring Management IP for the Endpoint

To configure the management address, go to **OpenScape Voice > Business Group > EndPoints** and under **SIP** tab, enter the Admin IP on Management Address field and save.

General | **SIP** | **Attributes** | **Aliases** | **Routes** | **Accounting**

Transport protocol: TCP

Best Effort SRTP support: MIKEY,SDES

ANAT Support: Enabled

Use Proxy/SBC Best-Effort SRTP settings for calls to subscribers: ☐

Management Address: 10.102.0.80

This field accepts IP or FQDN.

Verify under **OpenScape Branch > Branch Office** if Admin IP is being used for management.

72 Replacing OSB Voice Prompts (Features)

OSB provides three features that use sound files:

Automatic Call Distribution Groups (ACD)

Auto Attendant (AA)

Voice Mail (VM)

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. If desired to change the language used for those features, it shall be done manually.

72.1 Language File

ACD, AA and 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.

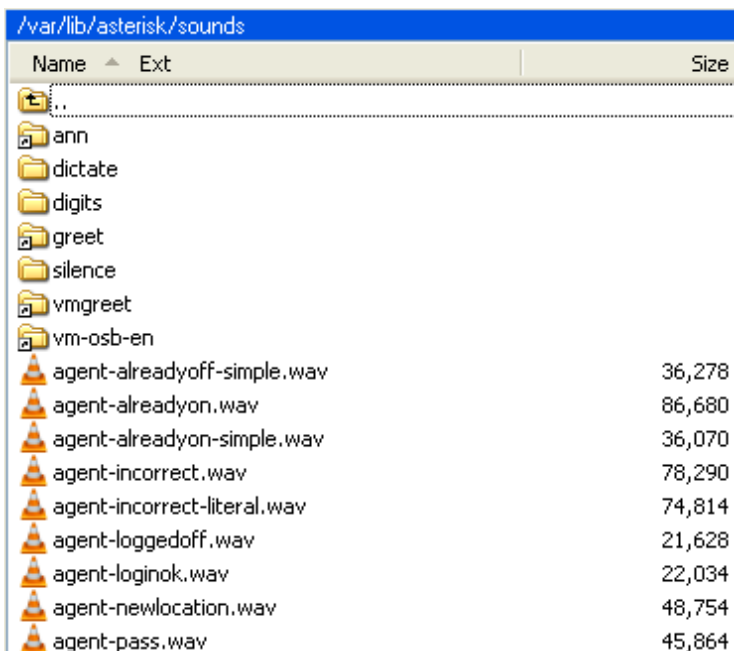
Usually the voice prompts have the same name in all languages so they can be easily replaced.

IMPORTANT: 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.

72.2 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/var/mngmt/announcements)
/var/lib/asterisk/sounds/greet (link to /opt/siemens/openbranch/var/mngmt/greetings)
/var/lib/asterisk/sounds/vm-osb-en (link to /opt/siemens/openbranch/var/mngmt/vm-osb-en)
/var/lib/asterisk/sounds/vmgreet (link to /opt/siemens/openbranch/var/mngmt/vmgreetings)
```



Name	Ext	Size
ann		
dictate		
digits		
greet		
silence		
vmgreet		
vm-osb-en		
agent-alreadyoff-simple.wav		36,278
agent-alreadyon.wav		86,680
agent-alreadyon-simple.wav		36,070
agent-incorrect.wav		78,290
agent-incorrect-literal.wav		74,814
agent-loggedoff.wav		21,628
agent-loginok.wav		22,034
agent-newlocation.wav		48,754
agent-pass.wav		45,864

72.3 General Purpose Voice Prompts

The files under the sounds directory and in the subdirectories dictate, digits and silence are general purpose voice prompts and cannot 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.

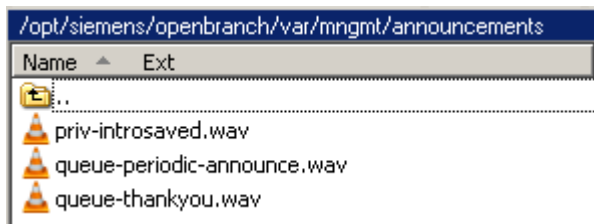
For other languages, these files can be also created based on other voice prompts in a specific language or recorded according to the customer decision. The file names shall be preserved to replace them in the OSB.

72.4 ACD Announcements

Customized ACD announcements are stored under:

```
/opt/siemens/openbranch/var/mngmt/announcements
```

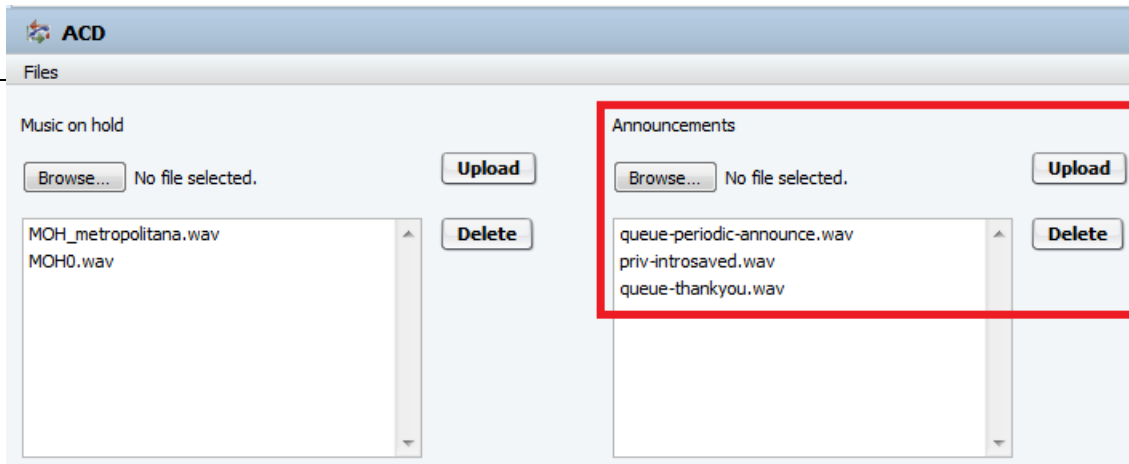
This directory stores the voice prompts for "**queue join**", "**queue wait**" or "**agent announcement**" selection.



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
```

New voice prompts can be copied directly to this directory or uploaded via local GUI.



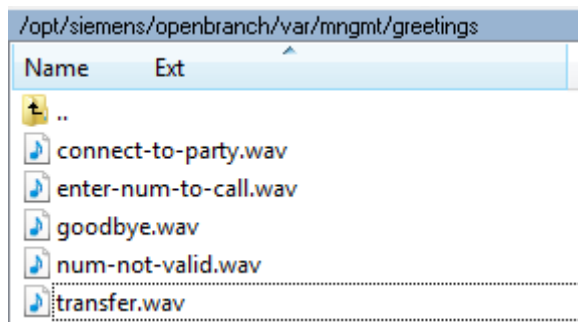
If desired to have the default voice prompts in other language, they can be also created based on other voice prompts in a specific language or recorded according to the customer decision. The file names shall be preserved to replace them in the OSB.

72.5 Auto Attendant Announcements

Customized AA announcements are stored under:

```
/opt/siemens/openbranch/var/mngmt/greetings
```

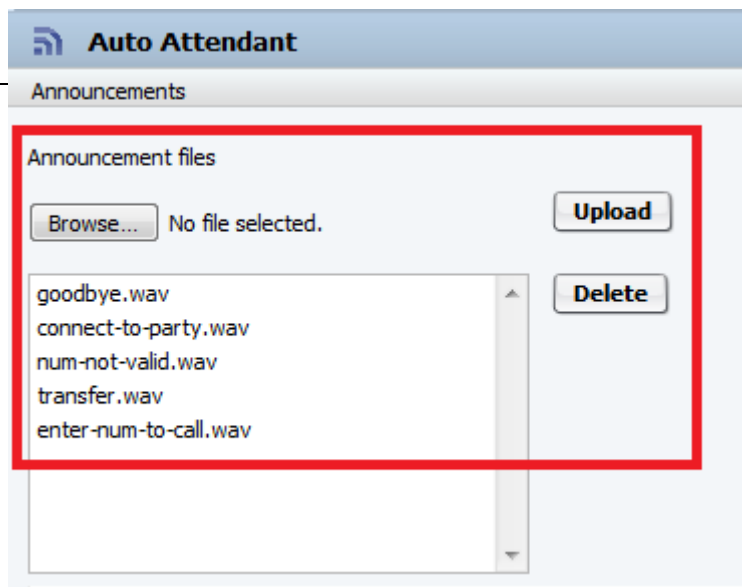
This directory stores the voice prompts for AA "**Destination selection greeting**", "**Failure prompt**", "**Final prompt**", "**Default destination prompt**" or "**Transfer prompt**" selection.



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
```

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.

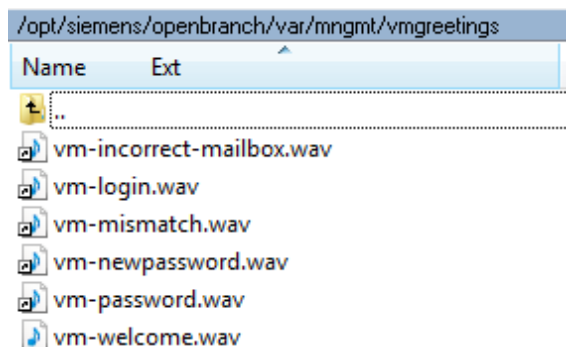
72.6 Voice Mail Announcements

Customized VM announcements are stored under:

`/opt/siemens/openbranch/var/mngmt/vmgreetings`

This directory stores the voice prompts for selection of:

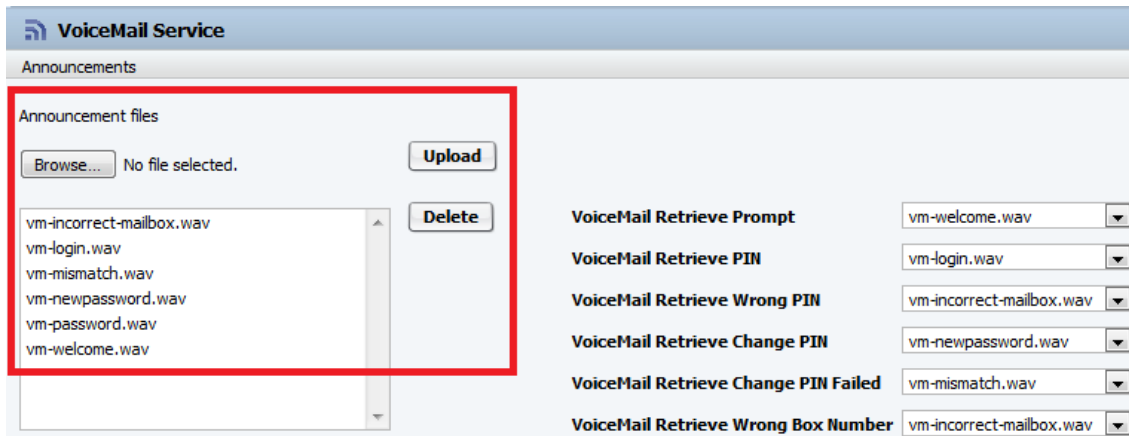
- VoiceMail Greeting
- VoiceMail Retrieve Prompt (From Own Extension)
- VoiceMail Retrieve Prompt (From Other Extension)
- Voicemail Retrieve Wrong PIN
- Voicemail Retrieve Change PIN
- VoiceMail Retrieve Change PIN failed
- VoiceMail Retrieve Wrong Box Number



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
```

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.

72.7 Replacing files

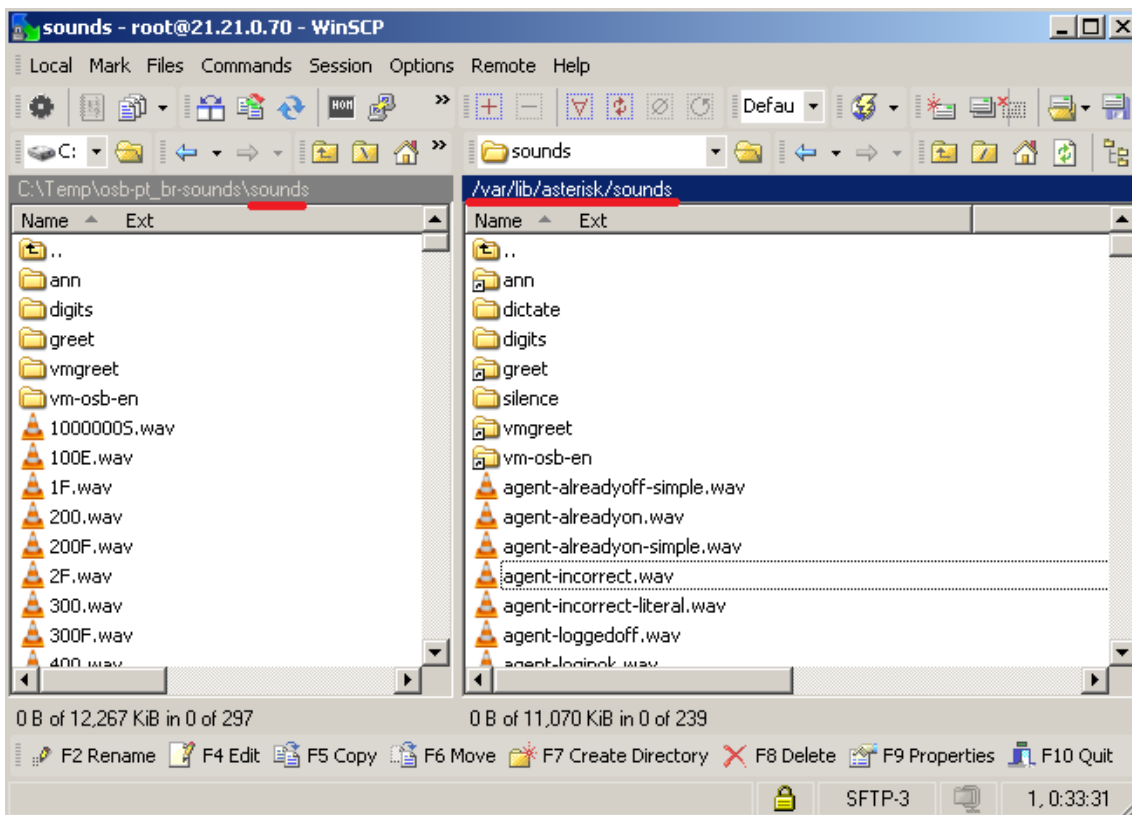
The [osb-pt_br-sounds.zip](http://download.sourceforge.net/disc-os/Disc-OS-Sounds-1.0-pt_BR.tar.gz?use_mirror=osdn) file were created based on voice prompts provided by the Disc-OS project. (http://download.sourceforge.net/disc-os/Disc-OS-Sounds-1.0-pt_BR.tar.gz?use_mirror=osdn)

The files in there are organized following the OSB directory structure to make the installation easier:

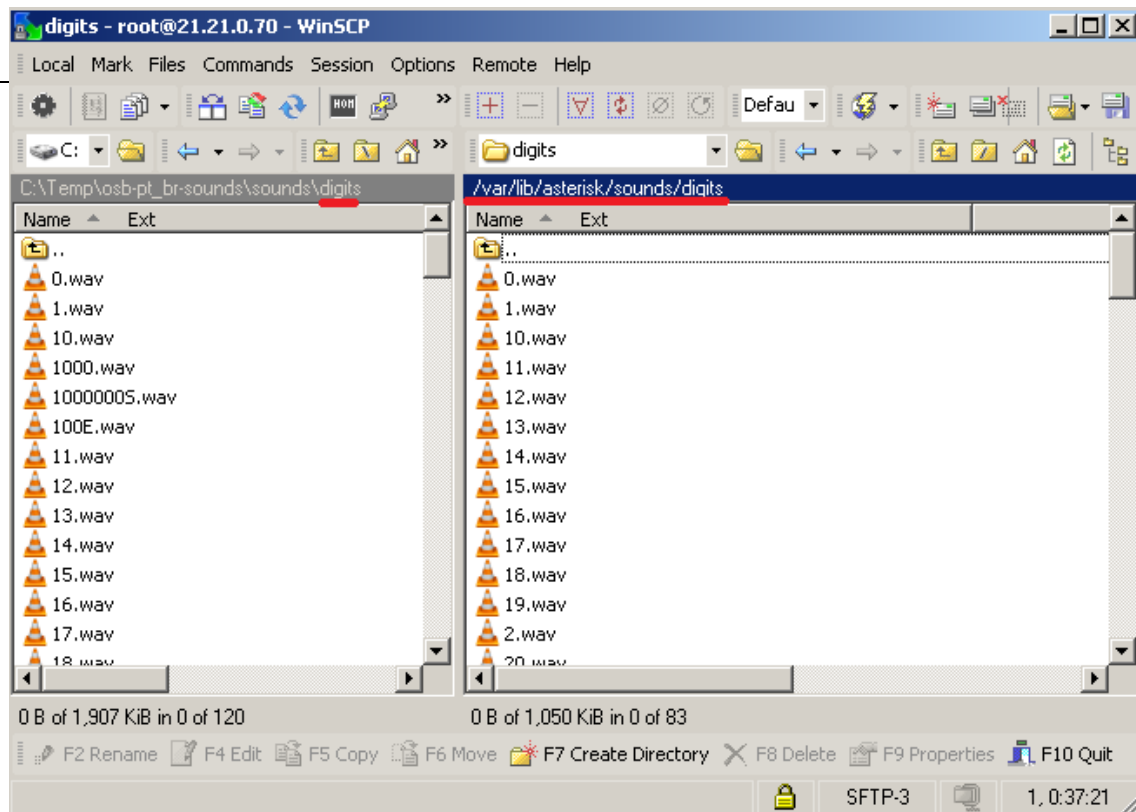
```
/sounds
/sounds/digits
/sounds/ann
/sounds/greet
/sounds/vmgreet
/sounds/vm-osb-en
```

72.8 Steps to Install

- a) SSH to OSB using WinSCP or another tool. **Ensure you have the root access to the OSB**
- b) Under `/var/lib/asterisk/sounds/` replace the voice prompts by the ones in the **sounds** directory of the zip file.



- c) Under `/var/lib/asterisk/sounds/digits` replace the voice prompts by the ones in the **sounds/digits** directory of the zip file.



- d) 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

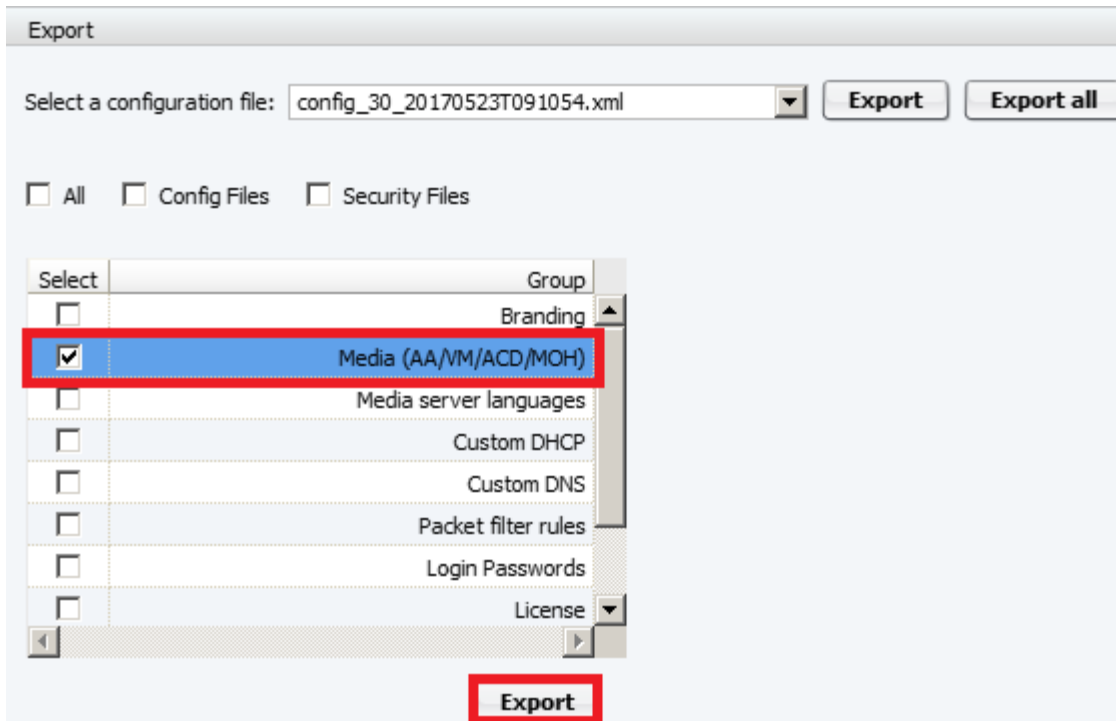
```

72.9 V9 Backup/Restore Custom Files

This procedure needs to be done only once after OSB V9 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:

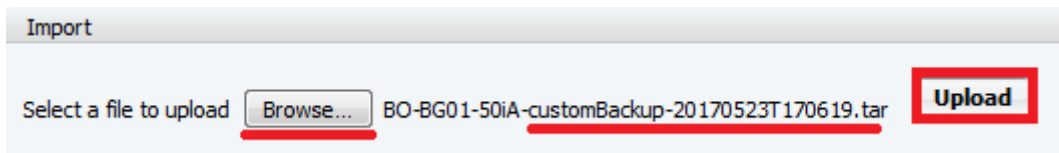
- a) Go to **Maintenance>Import/Export**
- b) Under **Export** section, select group **Media (AA/VM/ACD/MOH)**



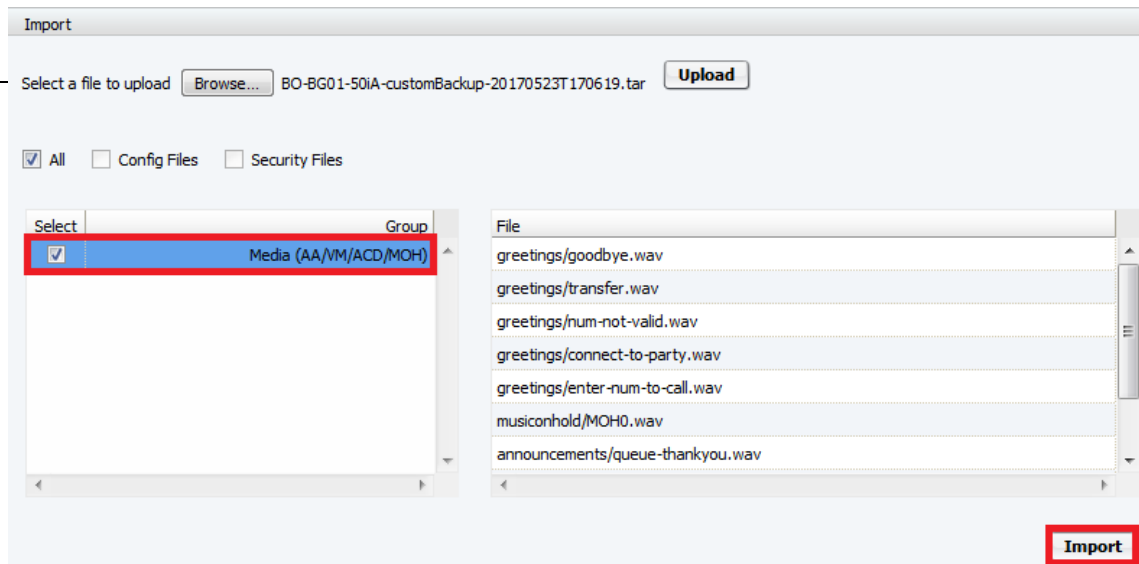
- c) Click on **Export**
- d) A tar file will be generated with voice prompts used for the features

To **import** the voice prompts:

- a) Go to **Maintenance>Import/Export**
- b) Under **Import** section, select the tar file to be uploaded and press **Upload**



- c) select group **Media (AA/VM/ACD/MOH)** and click on **Import**



d) Wait for window message informing that import was done

