



A MITEL
PRODUCT
GUIDE

Unify OpenScape Session Border Controller

OpenScape SBC 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

1	General information.....	4
2	Software Installation.....	5
2.1	Boot sequence setup.....	5
2.1.1	Configure BIOS for IBM/Lenovo 3250M3/M5/M6 and 3550M4	5
2.1.2	Change boot device for one time use: for IBM 3250M3/M5/M6 and 3550M3/M4/M5, Lenovo SR250/SR250 V2 and SR530	5
2.1.2.1	IBM x3250M3/M5/M6, x3550M3/M4/M5 platforms	5
2.1.2.2	Lenovo SR530 and Lenovo SR250 / SR250 V2 platforms	6
2.1.2.3	Fujitsu RX200 platforms	6
2.1.3	System Boot Mode – Legacy Mode or UEFI Mode	7
2.1.3.1	Lenovo x3250M6 and x3550 M5 platforms	7
2.1.3.2	7
2.1.4	RAID (Redundant array of independent disks) information for IBM3550, RX200 and SR530	8
2.1.5	Configuration of Virtual OS-SBC (VM-OS-SBC).....	8
2.1.6	OpenScape Branch and SBC distribution via OVA	9
2.2	USB Stick Setup tool (classic method)	10
2.2.1	USB setup for single node system	12
2.2.1.1	<i>Branding Information on the USB Stick Setup</i>	14
2.2.2	Full Installation for single node system.....	15
2.2.3	Full Installation for a Collocated redundant system with an existing configuration database 18	
2.2.4	Full Installation for a Collocated redundant system without an existing configuration database 19	
2.3	Deployment of a virtual OS-SBC as a vApp	20
2.3.1	Advanced Locking Id (ALI) information	20
2.3.2	Detailed steps to deploy with a vApp	21
2.3.2.1	<i>How to create the OS-SBC ISO image with the Software Load</i>	23
2.3.3	NIC Teaming on VMHost	25
2.3.4	Detailed steps to deploy with a vApp (cont)	26
3	Configuration.....	33
3.1	General steps to add a OS-SBC	33
3.2	OpenScape Voice (OSV) Configuration	35
3.2.1	RTP parameters	35
3.2.2	/etc/hosts in OSV	35
3.2.3	OS-SBC SIP Endpoint Configuration: create Sip Endpoint.....	36
3.2.3.1	OSV Endpoint/OSS Configuration with MTLS.....	36
3.2.4	Add an appliance to OpenScape SBC list	41
3.3	Centralized Licensing On CMP	43
3.3.1	Software Subscription License Usage on CMP.....	45
3.3.2	SBC sessions peak usage on OS-SBC.....	46
3.3.3	Standalone licenses for OS-SBC	46

3.4	OS-SBC Configuration / Displays	47
3.4.1	Dashboard.....	47
3.4.1.1	<i>System Status and info</i>	47
3.4.1.2	<i>Service status and alarms</i>	49
3.4.1.3	<i>Registered subscribers and Dynamic port mapping</i>	51
3.4.1.4	<i>SSP Connectivity Status</i>	52
3.4.1.5	<i>Dynamic IP Remote Endpoints</i>	53
3.4.1.6	<i>Denial of Service Mitigation display</i>	53
3.4.2	System Settings	53
3.4.2.1	Enable Open VM Tools	54
3.4.2.2	Licenses.....	55
3.4.2.3	Branding	56
3.4.3	Network / Net Services	57
3.4.3.1	<i>Physical Network Interfaces</i>	57
3.4.3.2	<i>Ethernet Bonding on LAN and/or WAN interfaces</i>	57
3.4.3.3	<i>Core realm configuration</i>	58
3.4.3.4	<i>Configuring separate management interface in an isolated subnet</i>	58
3.4.3.5	<i>Access and Admin realm configuration</i>	61
3.4.3.6	<i>SIP listening ports for LAN and WAN Main IPAddresses</i>	68
3.4.3.7	<i>Realm Profile</i>	70
3.4.3.8	<i>Routing</i>	71
3.4.3.9	<i>OS-SBC Redundancy</i>	73
3.4.3.10	<i>DNS</i>	79
3.4.3.11	<i>NTP</i>	80
3.4.3.12	<i>Traffic Shaping</i>	81
3.4.3.13	<i>QOS Settings</i>	82
3.4.4	VOIP / SIP Server Settings.....	83
3.4.4.1	<i>SIP Server Settings none clustered</i>	83
3.4.4.2	<i>VOIP / SIP server Settings Clustered</i>	85
3.4.4.3	<i>Timers and thresholds</i>	87
3.4.4.4	<i>Port and Signaling Settings</i>	88
3.4.4.5	<i>Media</i>	90
3.4.4.6	<i>Core Side Media Configuration</i>	95
3.4.4.7	<i>Media Realm Groups</i>	96
3.4.4.8	<i>Media Optimization</i>	100

3.4.4.9	Support of Media optimization across multiple SBCs	105
3.4.4.10	QoS Monitoring	108
3.4.5	Features.....	109
3.4.5.1	Remote Subscribers	109
3.4.5.2	Remote Endpoints	114
3.4.5.3	Media Server profiles.....	120
3.4.5.4	SIP Service Provider (SSP) Profiles	121
3.4.5.5	Remote Endpoint Configuration	131
3.4.5.6	Transcoding	139
3.4.5.7	Enable THIG	140
3.4.5.8	Enable Standalone	141
3.4.5.9	Enable Turn Server.....	144
3.4.5.10	Enable Circuit Telephony Connector	145
3.4.5.11	Enable SIP Load Balancer	146
3.4.5.12	Sip Enable Push Notification Service	153
3.4.5.13	Enable Ganglia Monitoring Daemon	153
3.4.5.14	Enable Circuit Zookeeper Client.....	153
3.4.6	Security	154
3.4.6.1	Certificate Management	154
3.4.6.2	Users/Password Recovery/Change.....	165
3.4.6.3	Administration Accounts	166
3.4.6.4	SIP/SDP Information Filtering.....	167
3.4.6.5	Advanced	168
3.4.6.6	Firewalls.....	169
3.4.6.7	Message Rate Control	173
3.4.6.8	RADIUS	174
3.4.6.9	Denial of Service Mitigation	175
3.4.6.10	PKI Configuration for SSH	177
3.4.7	Diagnostics & Logs	178
3.4.7.1	Settings.....	178
3.4.7.2	Debugging	181
3.4.7.3	Continuous tracing	183
3.4.7.4	On Demand Trace	184
3.4.7.5	Statistics	184

3.4.7.6	Serviceability	185
3.4.8	Alarms	186
3.4.8.1	Alarm Settings	186
3.4.8.2	SNMP v3 GET Configuration	187
3.4.8.3	Trap Destinations	188
3.4.8.4	Alarm for Malformed SIP Message Received	190
3.4.9	Maintenance.....	192
3.4.9.1	How to import / export a file	192
3.4.9.2	How to install / upgrade a file	193
3.4.9.3	How to configure Bulk Configuration (Delta XML)	202
3.4.9.4	How to Restart.....	207
3.4.9.5	How to configure Scheduled Maintenance	209
3.4.10	Open External Firewall-Pinhole	211
3.4.10.1	Send RTP dummy packets	211
3.5	Example configurations	216
3.5.9	OpenScape SBC remote endpoint configuration.....	225
3.5.10	OpenScape Voice endpoint configuration.....	226
3.5.10.1	OpenScape Branch (OSB) configuration in OpenScape Voice.....	226
3.5.10.2	Gateway in OSB branch office configuration in OpenScape Voice	227
3.5.10.3	Standalone Gateway directly in OS SBC configuration in OpenScape Voice	227
3.5.10.4	Auto Attendant configuration in OpenScape Voice	227
3.5.11	OpenScape Branch configuration.....	229
3.5.11.1	OSB SBC-Proxy mode configuration	229
3.5.11.2	OSB Branch SBC mode configuration	229
3.5.12	NAT configuration	229
3.5.12.1	OSB SBC configuration using static NAT.....	229
3.5.12.2	OSB SBC configuration using dynamic NAT.....	230
3.5.13	Media server configuration.....	231
3.5.13.1	Configuring OSB as main Media Server in OSV	231
3.5.13.2	Configuring OSB in the OSV as Branch Media Server:.....	238
3.5.13.3	Configuring the main Media Server as a backup of the Branch MS:	242
3.6	SBC using OpenScape 4000 as SIP Server.....	249
3.6.9	Installation	249
3.6.10	Configuration change at OpenScape 4000/HG3500 w/ OpenScape SBC	250
3.6.11	Configuration on OpenScape SBC	252
3.6.11.1	SIP Server Settings	252
3.6.11.2	Remote Endpoints Configuration	256
3.6.11.3	Remote Endpoint configuration for OpenScape 4000	260

3.6.12	Restrictions	260
3.7	Support secure calls to Microsoft Lync Mediation Server.....	260
3.8	Phone Configuration as Remote user.....	269
3.9	OpenScape Mobile Configuration	271
3.10	Generating an effective OS-SBC Ticket	271
3.10.9	Describe the setup and problem.....	271
3.10.10	Gather information (some information may not apply)	271
3.10.11	Gather traces, logfiles and Configuration files	271
4	Trouble shooting hints---what if?	272
4.4	The OS-SBC is in survivable mode.	272
4.5	A node server is “in penalty box” state.....	272
4.6	A redundant node is in “FAULT” state	272
4.7	Call processing is “slow” even for single calls	272
4.8	Remote subscribers can not register	272
4.9	Remote endpoints are in survivable mode	272
4.10	Calls of some protocols do not pass through the OS-SBC	273
4.11	Lines receive a code 606 when attempting a call.....	273
4.12	Line receives code 401 Unauthorized when attempting to register.....	273
4.13	Line receives code 403 Forbidden when attempting to register.....	273
4.14	Line receives code 404 Not Found when attempting to register	273
4.15	Lines receive a code 406 when attempting a call.....	273
4.16	Line receives code 503 service unavailable when attempting to register.....	273
4.17	Errors report Not possible to get authentication statement during simplified installation	273
4.18	Devices can not communicate with the OS-SBC	273
4.19	Trouble doing an "Import" of a XML configuration file.....	275
4.20	You see the alarm "License using temporary grace period" on SBC, when centralized licensing is in use.....	275
4.21	Can not upload a local file for upgrade	275
4.22	Calls which did work, are blocked at times.....	275
4.23	Receive a message indicating invalid HW type during XML validation	275
4.24	Receive a message indicating a file problem when booting a VM.....	275
4.25	Branch behind a “dynamic IP address NAT stays in penalty box.	276
4.26	A redundant system must have redundancy disabled.....	276
4.27	Can not login to OS-SBC	276
4.28	Cannot upgrade due to old license version.....	276
5	Table A: Fixed/Configurable Port Information:	277
6	OS-SBC Performance Configuration Limits:	277
6.4	SIP Requests Limits.....	277
6.4.9	Message rate limit.....	278
6.4.10	CPU load limit.....	278
6.4.11	Network limit.....	278
6.4.12	Limits per HW type	278
7	Table B: Hardware Types Table	280
8	Appendix C: OS-SBC External Interfaces	286
9	Create Certificate	287
9.4	Create Server Configuration file	287
9.5	Create Certificate Sign Request (CSR) and Install Certificates.....	294
9.5.9	Generate a Certificate Sign Request file (CSR)	294
9.5.9.1	Create the server configuration file, Refer to the section above.....	294

9.5.10	Submit the Certificate Sign Request file to the Certificate Authority	295
9.5.11	Download the Certificate from the Certificate Authority	295
9.5.12	Validate the Certificate	295
9.6	Change Certificate Parameters for OSS default certificate	298
9.7	Formatting Certificates	299
9.7.9	Viewing a Certificate or Certificate Sign Request	299
9.7.10	Converting certificate format	299
9.7.11	Validate Certificates	300
9.8	Terminology	300
9.9	Server Configuration File Template	300
10	OS SBC Support of IPV6	301
11	Generating SBC Configuration XML file via CDC Tool	313
12	Security considerations for the OS-SBC	325
12.4	Configuration of “allowed user agent” for OS-SBC	326
13	Appendix FortiNet Firewall model 310B Version 4 non TLS	326
14	Appendix FortiNet Firewall model 310B Version 5 TLS	330
14.4	Overview	330
14.5	Requirements	331
14.6	Restrictions	331
14.7	Constraints	331
14.8	VoIP Configuration	332
14.8.9	Operation modes	332
14.8.9.1	Network operation mode	332
14.8.9.2	Virtualization (VDOM)	332
14.8.9.3	SIP ALG / session-helper	332
14.8.9.4	Service objects and session expiration (TTL)	332
14.8.9.5	Firewall rule set	333
14.8.10	Parameters UTM Voice Profile	334
14.8.10.1	General profile for UDP, TCP and TLS/MTLS	334
14.8.10.2	Profile extension for TLS	338
14.8.10.3	Profile extension for MTLS	339
14.8.10.4	Parameters UTM IPS Sensor	340
14.8.10.5	Certificates for SIP-TLS	340
14.8.10.6	Client – Server connection (TLS)	341
14.8.10.7	Server – Server connection (MTLS)	342
14.8.10.8	Using High-Availability (HA) with VoIP	343
14.8.10.9	DiffServ Configuration	344
14.8.10.10	Alternate/Additional service port for SIP	344
14.8.11	Configuration blocks	345
14.8.11.1	Deactivate legacy session-helper on FortiGate (CLI)	345
14.8.11.2	Service objects and service session timer (CLI)	346

14.8.11.3	Certificates for SIP-TLS	347
14.8.11.4	Voice profile (CLI)	348
14.8.11.5	IPS sensor (CLI)	352
14.8.11.6	Activate the SIP ALG with firewall rule set (CLI)	353
14.8.11.7	Certificate Revocation Checking for SIP-TLS	354
14.8.11.8	High-Availability settings.....	355
14.8.11.9	Optional DiffServ Configuration (CLI).....	355
14.8.11.10	Alternate/Additional service port for SIP	355
14.8.12	Recommended settings for OpenScape Voice.....	357
14.8.12.1	Maximum time for call in provisional state “AlertTimer”	357
14.8.12.2	Session timers	357
14.8.12.3	Maximum time for an established call	357
14.8.13	OpenScape UC Firewall (VPN only mode).....	359
14.8.14	Abbreviations	360
15	Simplified Installation	361
16	DNSSRV for TLS phones	379
17	Configuration of location for emergency calls	384
18	Single-Armed-OS SBC.....	393
19	SIP Connect 1.1	395
19.4	Registration Mode	395
19.5	Static Mode	395
20	UCaaS Functionality	398
20.4	Support Cascaded SBC configuration.....	398
20.4.9	Standalone mode.....	398
20.4.9.1	OSCloud Trunk SBC configuration	398
20.4.10	Standalone SBC Configuration.....	399
20.4.11	Cascaded SBC mode.....	404
20.4.12	OSCloud Trunk SBC configuration.....	404
20.4.13	Cascaded SBC configuration	405
20.5	Support SBC on Premise configuration	411
20.5.9	Standalone mode.....	411
20.5.9.1	OSCloud Trunk SBC configuration	411
20.5.9.2	Standalone SBC Configuration	412
20.5.10	On premise SBC mode.....	417
20.5.10.1	OSCloud Trunk SBC configuration	417
20.5.10.2	On premise SBC configuration	419
21	Glossary and Abbreviations	424

1 General information

Refer to the software release notes for the latest information on restrictions, known issues and workarounds.

This is a living document with new information being added as functions / features are added and tested for each software release.



In this document this symbol represents what is considered important information.

Issue	Date	History of Changes
8.1.00	12/11/15	Based on 8.0.03 document and new features
9.1.00	01/12/16	V9R0 Initiation based on V8
9.2.00	10/03/17	FRN 10553 - Support of Media optimization across multiple SBCs)
9.3.00	03/04/17	FRN 10685 - Support of SNMP V3 GET Configuration
9.4.00	25/07/17	FRN10676 - Bulk OpenScape SBC Change Management (Delta XML)
9.6.00	27/10/2017	SBC support to UCaaS N+1 availability
9.7.00	26/01/2018	<ul style="list-style-type: none">▪ Remote Endpoint configuration for OpenScape 4000▪ OpenScape Branch and SBC distribution via OVA
9.8.00	16/03/2018	<ul style="list-style-type: none">▪ FRN 10620 - IOS push feature
9.9.00	11/05/2018	<ul style="list-style-type: none">▪ Open External Firewall – Pinhole feature
9.10.00	24/05/2018	<ul style="list-style-type: none">▪ IOS push feature enhancements
9.11.00	17/08/2018	<ul style="list-style-type: none">▪ Incoming SIP Manipulation▪ Advanced Locking Id (ALI)
9.12.00	28/09/2018	<ul style="list-style-type: none">▪ BCF Event Handling
9.13.00	11/12/2018	<ul style="list-style-type: none">▪ Minor enhancements & modifications
9.14.00	12/02/2019	<ul style="list-style-type: none">▪ UCaaS functionality<ul style="list-style-type: none">a) On premise configurationo b) Cascaded configuration
9.15.00	01/03/2019	<ul style="list-style-type: none">▪ Redesign of Time Zone configuration
9.16.00	29/03/2019	<ul style="list-style-type: none">▪ Rest API
9.17.00	12/04/2019	<ul style="list-style-type: none">▪ Minor enhancements & modifications
9.18.00	05/07/2019	<ul style="list-style-type: none">▪ Minor enhancements & modifications
9.19.00	15/11/2021	<ul style="list-style-type: none">▪ Documentation enhancements and updates
9.20.00	13/12/2022	<ul style="list-style-type: none">▪ Added note under Chapter 3.4.4.5 Media
9.21.00	11/1/2023	<ul style="list-style-type: none">▪ Minor updates
9.22.00	20/4/2023	<ul style="list-style-type: none">▪ Updated Section 3.4.5.1.1 Remote Subscriber Settings
9.23.00	26/06/2023	<ul style="list-style-type: none">▪ Minor updates
9.24.00	01/08/23	<ul style="list-style-type: none">▪ Updates and enhancements
9.25.00	22/07/24	<ul style="list-style-type: none">▪ Rebranded to Mitel Layout

2 Software Installation

2.1 Boot sequence setup

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

- IBM3550/3250/Fujitsu: Boot sequence. First device should be set to USB and second to Hard Disk.

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

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

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 Manager" 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 Change boot device for one time use: for IBM 3250M3/M5/M6 and 3550M3/M4/M5, Lenovo SR250/SR250 V2, 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 **USB Storage** option.
5. Press **Esc** to exit.

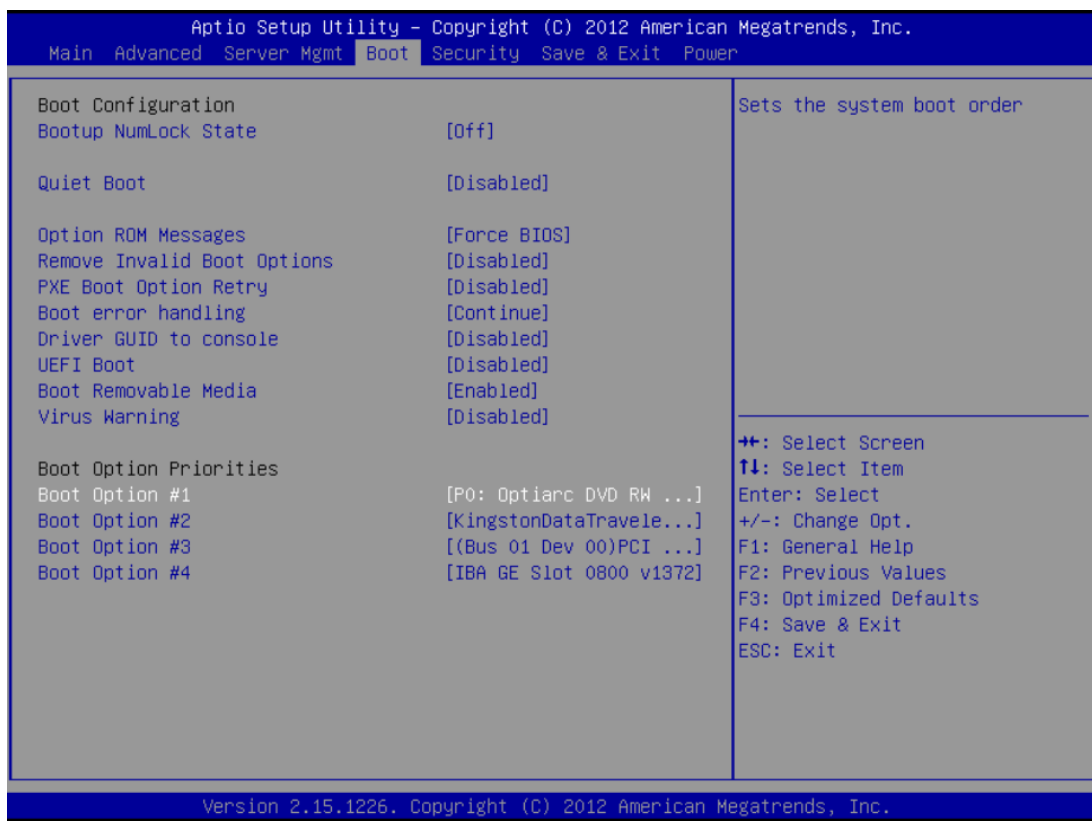
2.1.2.2 Lenovo SR530, SR630 V2 and Lenovo SR250 / SR250 V2 platforms

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 and Lenovo SR630 V2 are 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:

1. Select **F1** to enter in System Setup.
2. Choose the **Boot Manager** option.
3. Configure the **Boot Modes** as **Legacy Mode**.

UEFI MODE:

1. Select **F1** to enter in System Setup.
2. Choose the **Boot Manager** option. The Boot Mode must be changed to UEFI mode.
3. Disable the **Legacy Support** in **System Settings**.

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. Change the **Boot Manager/Boot Mode** to **UEFI mode**.
4. Disable the **Legacy BIOS** in **System Settings**.

IMPORTANT:

The following servers do not support UEFI Boot Mode:

- Fujitsu Rx 200 S6
- Fujitsu Rx 200 S7

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 to the following document for instructions: [OpenScape Voice V10, Service Manual: Installation and Upgrades, Installation Guide](#)



Note: Only RAID level 1 is supported.

2.1.5 Configuration of Virtual OS-SBC (VM-OS-SBC)

As of V9, Virtual OS-SBCs run on a host or hosts using VMware vSphere V6.0, V6.5, V6.7 and V7.0. It is assumed that the user is familiar with VMware vSphere V6.0, V6.5, V6.7 and V7.0.

No other virtualization software is supported.

When creating a VM-OS-SBC the following parameter values are supported:

VM-OS-SBC size	OS-SBC-250	OS-SBC-6000	OS-SBC-20000
Number of CPUs	2	4	8
Memory size	2 Gig	2 Gig	4 Gig
Hard disk size	40 Gig	40 Gig	60 Gig
Network adapter type	VMXNET3	VMXNET3	VMXNET3
Number of network adaptors	2	2	2

From V10R1 the memory size has increased according to the following table:

VM-OS-SBC size	OS-SBC-250	OS-SBC-6000	OS-SBC-20000
Number of CPUs	2	4	8
Memory size	4 Gig	4 Gig	6 Gig
Hard disk size	40 Gig	40 Gig	60 Gig
Network adapter type	VMXNET3	VMXNET3	VMXNET3
Number of network adaptors	2	2	2

Note: Each OS-SBC VM is associated and tuned with a equivalent HW server. increasing the Memory size does not increase its components memory size automatically (e.g. sipserver).

Refer to **Deployment of a virtual OS-SBC** on the [OpenScape Solution Set V10, OpenScape Virtual Machine Resourcing and Configuration Guide, Service Documentation](#).

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).

2.1.6 OpenScape Branch and SBC distribution via OVA

The OpenScape SBC 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 SBC, with the following configuration:

	Hardware Type	Num of CPUs	Ram memory	Disk space	Lan IP	Wan IP
OS SBC	Virtual OSS 20000	8	6Gb	60Gb	10.82.53.225/26	10.20.30.41/24

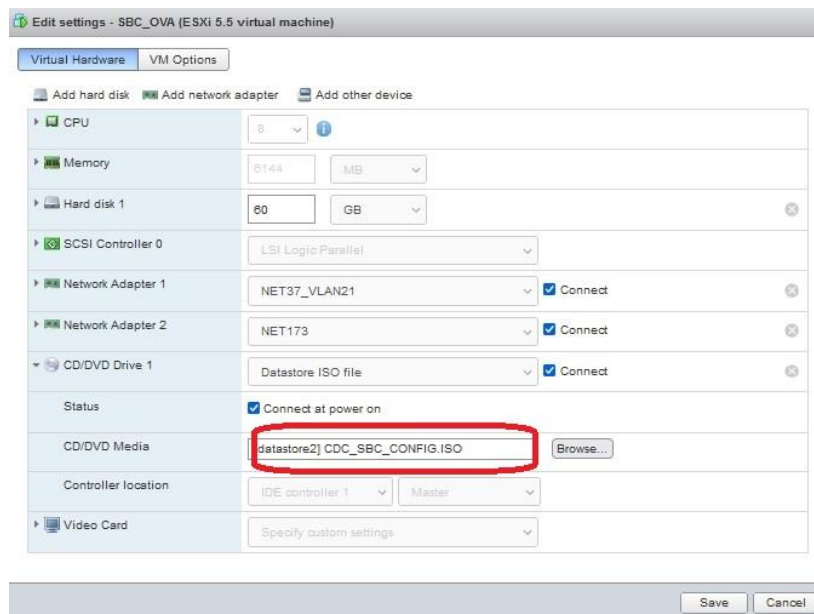
NOTE: In previous release, the OVA was used with OSEE/THIG(4 CPUs).

Only in the first boot, the system will try to find a CD/DVD on the VM, and will look for an XML configuration file. If this file is present, the system will automatically apply it.

This XML file must be one OpenScape SBC database file compatible with the version and with also desired configuration. For example:with another LAN IP and WAN IP configuration.

And if it will be used together with OVA installation, the XML file must be also one ISO file. The OpenScape SBC XML file must be renamed to: CDC_SBC_CONFIG.ISO

NOTE: Please do not set the parameter Power on after deployment in OVA installation if choose the option to connect the CD/DVD with iso file in first boot.










In V10R2 OVA, the system has 5 partitions. The HD size was increased from 40Gb to 60Gb.

2.2 USB Stick Setup tool (classic method)




This application is distributed with the following files from SWS

- **oss-10.02.*.*.zip**, that contains:
 - **image_oss-10.02.*.*.tar** – Software image file for upgrade or install.
 - **image_oss-10.02.*.*.spa** – File contains the compatibility information from the old release to new release for use by the CMP.
 - **usbsticksetup_oss-10.02.*.*.zip** - Contains the USB Stick Wizard.
- **misc_oss-10.02.*.*.tar.gz** - has the default XML configuration files and the MIBS
- **vApps_oss-10.02.*.*.zip** - Contains the OVF templates to create and deploy a virtual machine for the various models of Virtual SBC.
- **oss-10.02.*.*.bz2** – Software image file for 4K Hosted.
- **sw-metadata-oss-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 OS-SBC Installation.

Name	Type	Size
 image_oss-10.02.00.00-2.spa	SPA File	1 KB
 image_oss-10.02.00.00-2.tar	TAR File	405,990 KB
 misc_oss-10.02.00.00-2.tar.gz	GZ File	90 KB
 oss-10.02.00.00-2.bz2	BZ2 File	253,135 KB
 sw-metadata-oss-10.02.00.00-2.json	JSON File	1 KB
 usbsticksetup_oss-10.02.00.00-2	Compressed (zipped) Folder	21,971 KB
 vApps_oss-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	2,206 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_oss-10.02.00.00-2.tar	TAR File	405,990 KB
 initrd.gz	GZ File	12,092 KB
 vmlinuz	File	8,838 KB

3. The “syslinux” folder will look like:

 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 by running usbsticksetup.exe application.
5. After filling in the required information, press **OK** to create the USB Stick.
6. After the process is completed, the USB Stick can be removed and it will be ready for installation.

2.2.1 USB setup for single node system

- Up to V10R1

USB Stick Setup

Media Select: I:\ (7.77 GB) Min 2GB USB Stick Required

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

Installation Method:

- ☒ Generate node.cfg file Option to create new Config File. Network interfaces configuration is required with this option.
- ☐ Already existent database file USB Stick will be created with existing DB file (*.xml). If option is used Server Name, and Interfaces are grayed out. See Appendix on CDC tool.
- ☐ Already existent node.cfg file USB Stick will be created with existing Config file (*.cfg). If option is used Server Name, and Interfaces are grayed out.

☐ Automated ☐ PreInstall ☐ Net boot ☐ DHCP ☐ Circuit SBC ☐ Single Armed SBC

SBC Network Configuration:

Hardware type: [Dropdown]

Hostname: ConfigGuideDemo Circuit SBC Refer to appendix "Single-Armed-SBC"

Interface: LAN Interface Refer to appendix on **Simplified Installation** for information on these options

☐ Disable interface

IPv4 address: 10 . 232 . 63 . 94 System Name

IPv4 netmask: 255 . 255 . 255 . 0

IPv4 gateway: 10 . 232 . 63 . 1 Configure LAN and WAN
As each is selected in the dropdown the information may be viewed or entered. These fields are grayed out if existing database or node.cfg are selected. Note that each interface must be on separate subnets.

IPv6 address: [Field]

IPv6 netmask: [Field]

IPv6 gateway: [Field] This is always the gateway which belongs to the LAN network, after installation the user should change the default gateway to the WAN and add static routes for the LAN network,

Logical ID: [Field]

CMP URL 1: [Field]

CMP URL 2: [Field]

DNS 1: [Field]

DNS 2: [Field]

Change Branding Names and Logo

☒ Partitioned Note: Partitioned USB Stick **must be checked** for IBM3550M3/M4 or 3250M3/M4/M5/M6

OK Cancel

Interface: Available options: LAN Interface, ADMIN Interface.

- **From V10R2**

The screenshot shows the 'USB Stick Setup' window with the following sections and callouts:

- Media Select:** A dropdown menu showing 'F:\ (14,3 GB)' and a 'Refresh' button. A callout box states: 'Min 2GB USB Stick Required'.
- Configuration database:** Three radio buttons: 'Generate node.cfg file' (selected), 'Already existent database file', and 'Already existent node.cfg file'. A callout box points to the 'Generate node.cfg file' option, stating: 'Option to create new Config File. Network interfaces configuration is required with this option.'
- SBC Network Configuration:** Fields for 'Hardware type', 'Hostname' (set to 'ConfigGuideDemo'), 'Interface' (set to 'LAN Interface'), 'IPv4 address' (10 . 232 . 63 . 94), 'IPv4 netmask' (255 . 255 . 255 . 0), 'IPv4 gateway' (10 . 232 . 63 . 1), 'IPv6 address', 'IPv6 netmask', and 'IPv6 gateway'. A callout box points to the 'Interface' dropdown, stating: 'USB Stick will be created with existing Config file (*.cfg). If option is used Server Name, and Interfaces are graved out.'
- Installation Method:** Checkboxes for 'Automated', 'PreInstall', 'Net boot', 'DHCP', 'UEFI Bootloader', 'Circuit SBC', 'Single Armed', and 'Invert'. A callout box points to the 'Circuit SBC' checkbox, stating: 'Circuit SBC'. Another callout box points to the 'Single Armed' checkbox, stating: 'Refer to appendix "Single-Armed-SBC"'. A third callout box points to the 'UEFI Bootloader' checkbox, stating: 'From V10R2, the new flag was added to set the System Boot as UEFI Mode'.
- General:** Fields for 'DNS 1', 'DNS 2', 'Logical ID', 'CMP URL 1', and 'CMP URL 2'. A callout box points to these fields, stating: 'Refer to appendix on Simplified Installation for information on these options.'
- Buttons:** 'Change Branding Names and Logo', 'OK', and 'Cancel'.
- Partitioned USB Stick:** A checkbox labeled 'Partitioned USB Stick' which is checked. A callout box points to it, stating: 'Note: Partitioned USB Stick must be checked for HW servers.'

Additional callout boxes at the bottom of the image provide further context:

- Bottom left: 'USB Stick will be created with existing DB file (*.xml). If option is used Server Name, and Interfaces are grayed out.'
- Bottom right: 'Note: Partitioned USB Stick must be checked for HW servers.'

SBC Network Configuration

The SBC Network Configuration window contains the following fields and annotations:

- System Name:** A yellow box points to the title bar of the window.
- Hardware type:** A dropdown menu.
- Hostname:** A text field containing "ConfigGuideDemo".
- Interface:** A dropdown menu showing "LAN Interface". A yellow box points to it with the text: "Interface: Available options: LAN Interface, ADMIN Interface."
- Disable interface:** An unchecked checkbox.
- IPv4 address:** A text field containing "10 . 232 . 63 . 94".
- IPv4 netmask:** A text field containing "255 . 255 . 255 . 0".
- IPv4 gateway:** A text field containing "10 . 232 . 63 . 1". A yellow box points to it with the text: "This is always the gateway which belongs to the LAN network, after installation the user should change the default gateway to the WAN and add static routes for the LAN network."
- IPv6 address:** A text field.
- IPv6 netmask:** A text field.
- IPv6 gateway:** A text field.

Configure LAN and WAN
As each is selected in the dropdown the information may be viewed or entered. These fields are grayed out if existing database or node,cfg are selected.

Note: Each interface must be on separate subnets.

2.2.1.1 Branding Information on the USB Stick Setup

The Branding window contains the following fields and annotations:

- Company Name:** A text field containing "Unify Software and Solutions". A yellow box points to it with the text: "The **Change Branding Names and Logo** button will open the Branding Window, where branding information can be entered. The same entry rules that are valid in GUI apply to USB Stick Setup as well."
- Product Name:** A text field containing "OpenScape SBC".
- TLA:** A text field containing "Copyright (c) Unify Software and Solutions GmbH & Co. KG 2021. All r".
- Logo Picture File:** A text field with a "Browse" button next to it.
- Buttons:** "OK" and "Cancel" buttons at the bottom.

2.2.2 Full Installation for single node system

Installation erases both backup and active partitions and overwrites them with existent SW on the USB. The configuration 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 USB stick.

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

1. Restart OS-SBC with the 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
 - User Name: "administrator".
 - Password: "Asd123!."

After the login OS-SBC will alert the user that OS-SBC is running with the 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 Session Border Control platform is available in the following languages: English, German and French(starting from V10R2.2.0). You may choose the language of your preference (English, German or French) before login.

- Up to V10R1

- From V10R2

Default login
 UserName: "administrator"
 Password: "Asd123!."

Unify OpenScape Session Border Controller

UO Hybrid SBC Management Portal

This session has expired. Please log back in.

User name	<input style="width: 150px;" type="text" value="administrator"/>
Password	<input style="width: 150px;" type="password"/>
Language	<div style="border: 1px solid #ccc; padding: 2px;">English ▼</div>

IMPORTANT: The **OpenScape Branch** platform is also available in German. You may choose the language of preference (English or German) before login.

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

- Go to **Maintenance** → **Install/Upgrade** tab. The full **Installation** option appears (**Note** this option is only available when booting from USB stick).

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

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.

2.2.3 Full Installation for a Collocated redundant system with an existing configuration database

If you are performing a full installation on a collocated redundant system, it is suggested that you follow these steps:

1. Export the current configuration (Local GUI→ Maintenance → Import/Export → Export), from the **master node**, to a safe location. It is assumed that the configuration already contains the information for a redundant system.
2. Create **two** USB sticks, each with its own information for the LAN and WAN interfaces and default gateway. This is so each node will come up with its own configuration for IP addresses. One USB may contain the information related to redundancy.
3. Boot each node with its USB stick. See 2.2.2 Full Installation for single node system.
4. Restore the database in the master node. This will make the master node aware of its backup again if it was not supplied in step 2. See 2.2.2 Full Installation for single node system.

The database will be copied to the backup node.

2.2.4 Full Installation for a Collocated redundant system without an existing configuration database

1. Create two USB sticks, each with its own information for the LAN and WAN interfaces and default gateway. This is so each node will come up with its own configuration for IP addresses. Do not use any exported xml file which may have any information relating to redundancy.
2. Boot each node with its USB stick. See 2.2.2 Full Installation for single node system.
3. Go to node 1, considered to be the master. Go to Local GUI → Network/Network Services → Settings → Redundancy. Check the box for “Enable redundancy” and fill in the columns for “backup IP address” and “virtual IP address” for the LAN and WAN.
4. Apply the changes.
5. This operation requires a system restart. After restart, the configuration of the Node 1 will be automatically replicated to the Node 2 (redundancy will be automatically enabled on the Node 2). Once the Redundancy is activated, the configuration is allowed only in the Master node.

2.3 Deployment of a virtual OS-SBC as a vApp

Using this method the virtual OS-SBC is built using the software load in an ISO image file, loaded into the customer's vCenter.

The vCenter's deployment wizard is then used to deploy the OpenScape Virtual Appliance. Once the VM is up and running the configuration proceeds as normal.

2.3.1 Advanced Locking Id (ALI) information

Prior to requesting a standalone license file with an Advanced Locking Id (ALI) for a Virtual SBC, configure the OS-SBC according to the OS-SBC Configuration Guide. Be sure to configure the OS-SBC to use the **default gateway** and be sure to have at least one DNS server in the DNS Server list (or check/enable the DNS Server box and provide the eth0 interface IP address as the DNS server address for purposes of calculating an ALI. An ALI cannot be requested if no DNS Server is configured.

If Standalone licensing is to be used on a VM-OS-SBC, then the license file should be requested by providing the following information from the VM-OS-SBC to generate an Advanced Locking ID (ALI). There is a folder Calculate Locking ID in [CLS](#). For a redundant SBC cluster, this information should be taken from the master node:

Hostname of the OS-SBC: from Local GUI of OS-SBC, from the the main page, navigate to System Info section → Hostname field.

Primary DNS Server: from Local GUI of OS-SBC, navigate to Network/NetServices page → DNS → Client section → DNS server IP Address list box and select the Primary DNS.

Default Gateway Address: from Local GUI of OS-SBC, navigate to Network/Net Services page → Settings → Routing section → "Default Gateway Address field.

Host IP Address: from Local GUI of OS-SBC, navigate to Network/Net Services page → Interface Configuration section → Access Realm Configuration box IP Address field of the "Main Core IPv4" row.

Timezone: from Local GUI of OS-SBC, navigate to Network/Net Services page → NTP → Timezone configuration

This data is used to generate an Advanced Locking ID (ALI) and the license file will be generated with that ALI. Then apply this license file from the OS-SBC Local GUI → System → Licenses → License Information section → Standalone license file Browse button → select file → click Upload → click OK → click Save to exit page. For a redundant SBC cluster, apply the license file on the master node only by logging into LOCAL GUI via the VRRP address of the SBC cluster. **Applying a license file/or allocating licenses to SBC from the OSB Assistant will result in a SIPServer restart on the SBC and potential loss of existing calls.**

Note: If any of these parameters changes, a new licence file will be required.

- This method of standalone licensing of Virtual OS-SBC is not the preferred method, but may still be used.
- The **Advanced Locking ID** is also available in System → License folder.
- Press **Refresh** in **Advanced Locking ID** option.

Note: Configure the DNS server and NTP server before and activate the flag **Enable DNS server**.

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: 192.168.96.64 License server port: 4709

Hardware ID Node1: 00:0C:29:A7:22:87

Hardware ID Node2: 00:0C:29:92:05:F4

Logical ID: senhora:BG_RD_OSB_OSSBC:ossvmred

Advanced Locking ID: L3DJDH9FXU9PDWUD#2*XT* Refresh

License Information

License Version: V10 SIEL ID: SID:152135222399

License type: Floating Days till license expires: unlimited

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
Circuit SBC Sessions	0	0
SBC sessions	100	0
SBC BCF	0	0
SBC M5 Direct Routing	0	0

2.3.2 Detailed steps to deploy with a vApp

After unzipping the **usbsticksetup** and **vApps** archives your file folder should look like this:

Name	Type	Size
usbsticksetup_oss-10.02.00.00-2	File folder	
vApps	File folder	
image_oss-10.02.00.00-2.spa	SPA File	1 KB
image_oss-10.02.00.00-2.tar	TAR File	405,990 KB
misc_oss-10.02.00.00-2.tar.gz	GZ File	90 KB
oss-10.02.00.00-2.bz2	BZ2 File	253,135 KB
sw-metadata-oss-10.02.00.00-2.json	JSON File	1 KB
usbsticksetup_oss-10.02.00.00-2.zip	Compressed (zipped) Folder	21,971 KB
vApps_oss-10.02.00.00-2.zip	Compressed (zipped) Folder	8 KB

In the **vApps** folder, you can see the three types of Virtual SBCs:

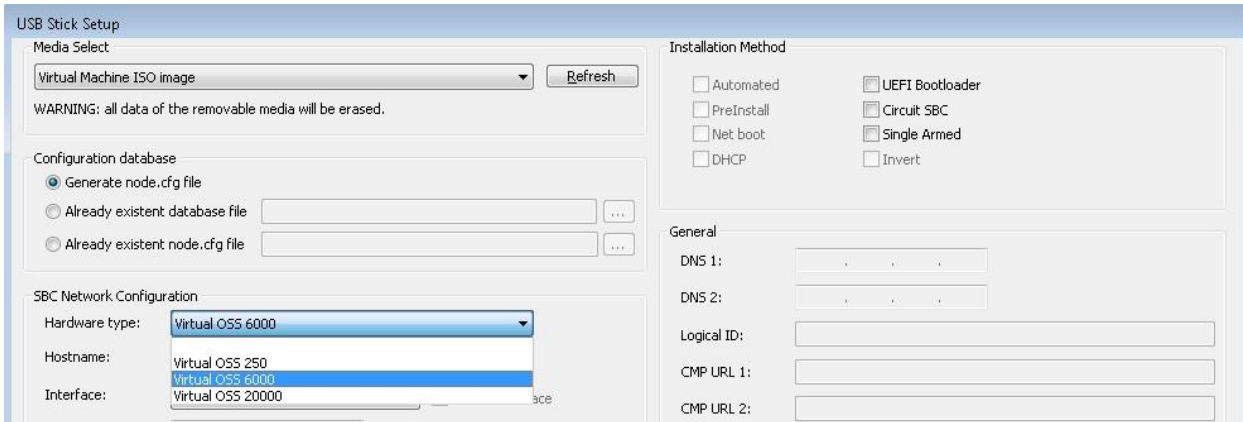
oss-10.02.00.00-2	Name	Type	Size
usbsticksetup_oss-10.02.00.00-2	OSS-250	File folder	
vApps	OSS-6000	File folder	
usbsticksetup_oss-10.02.00.00-2.zip	OSS-20000	File folder	
vApps_oss-10.02.00.00-2.zip			

The **OSS.ovf** and **OSS-disk1.vmdk** files are used to deploy the vApps template for creating a OS-SBC VM in sizes 250, 6000 or 20000.

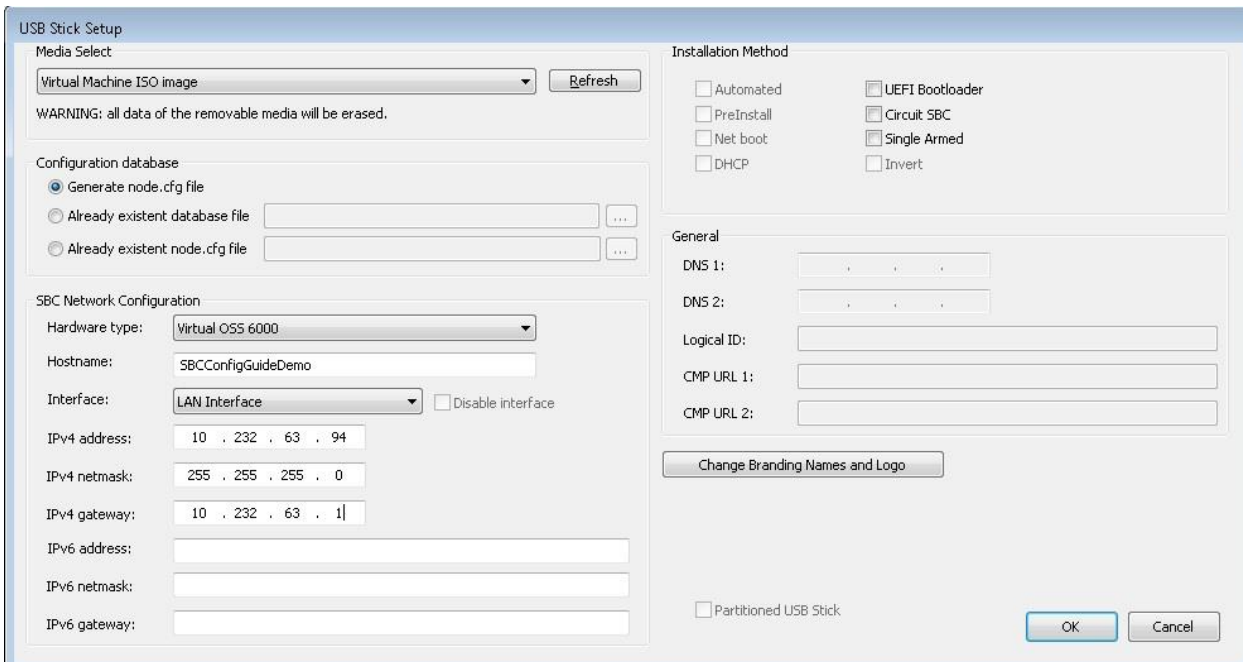
This PC > j (\\data.global-ad.net) (J:) > AUTOCLEAN > WEEKLY > oss-10.02.00.00-2 > vApps > OSS-6000			
oss-10.02.00.00-2	Name	Type	Size
usbsticksetup_oss-10.02.00.00-2	OSS.ovf	OVF File	7 KB
vApps	OSS-disk1.vmdk	VMDK File	71 KB
OSS-250			
OSS-6000			
OSS-20000			
usbsticksetup_oss-10.02.00.00-2.zip			
vApps_oss-10.02.00.00-2.zip			

2.3.2.1 How to create the OS-SBC ISO image with the Software Load

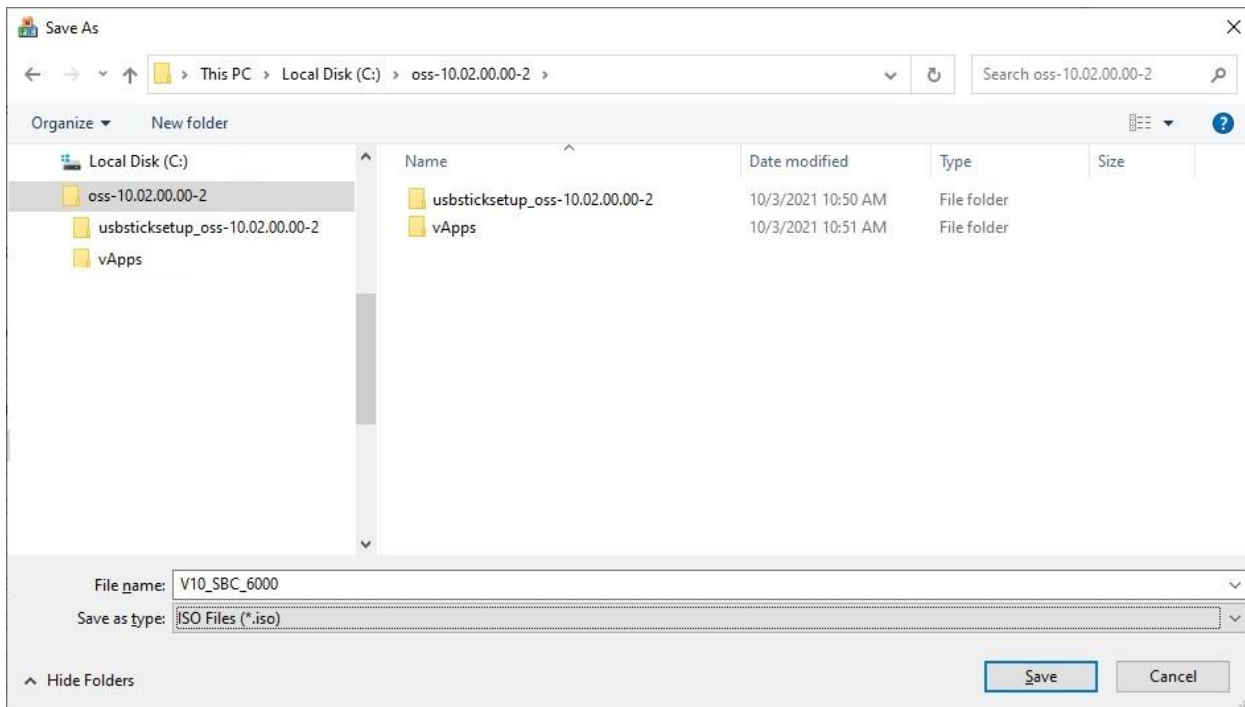
1. Move the **image_oss-10.02.*.*.tar** file to the **ob** folder.
2. Run the **usbsticksetup.exe** program that was downloaded with the OS-SBC load from SWS:



3. In the **Media Select** field, select **Virtual Machine ISO image**.
4. In the **Installation Method** field, select **Generate new node.cfg**, or **Already existent database file** if one is available.
5. In the **SBC Network Configuration** field:
 - a. Select the hardware type you want to create (**Virtual OSS 250** is **OS-SBC-250**, **Virtual OSS 6000** is **OS-SBC 6000** and **Virtual OSS 20000** is **OS-SBC-20000**).
 - b. Provide the hostname and the IP addresses for WAN and LAN side and click **OK**.

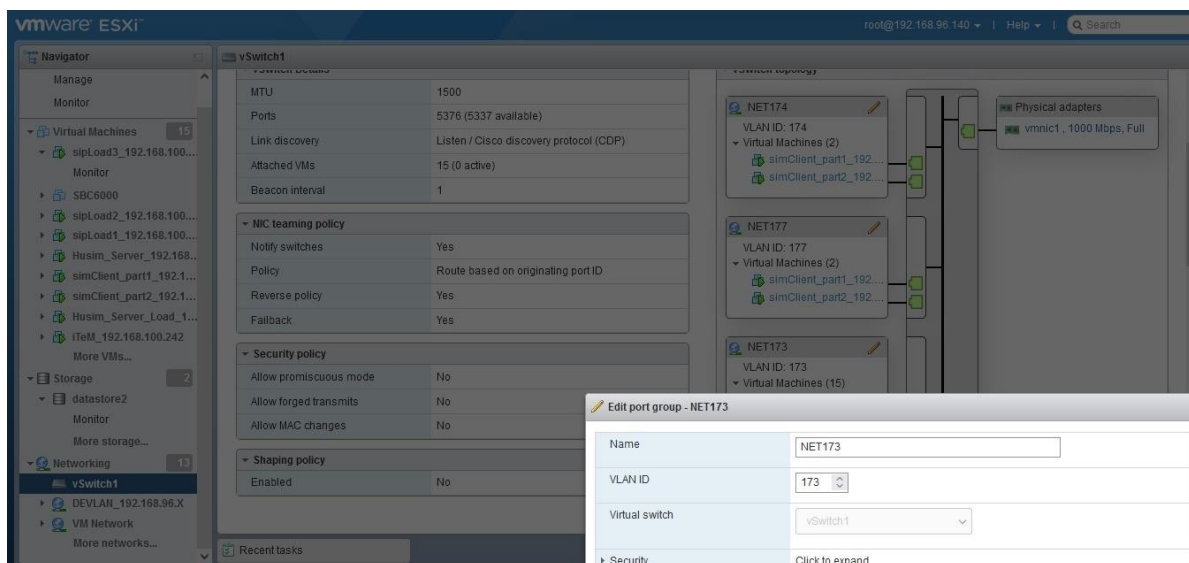
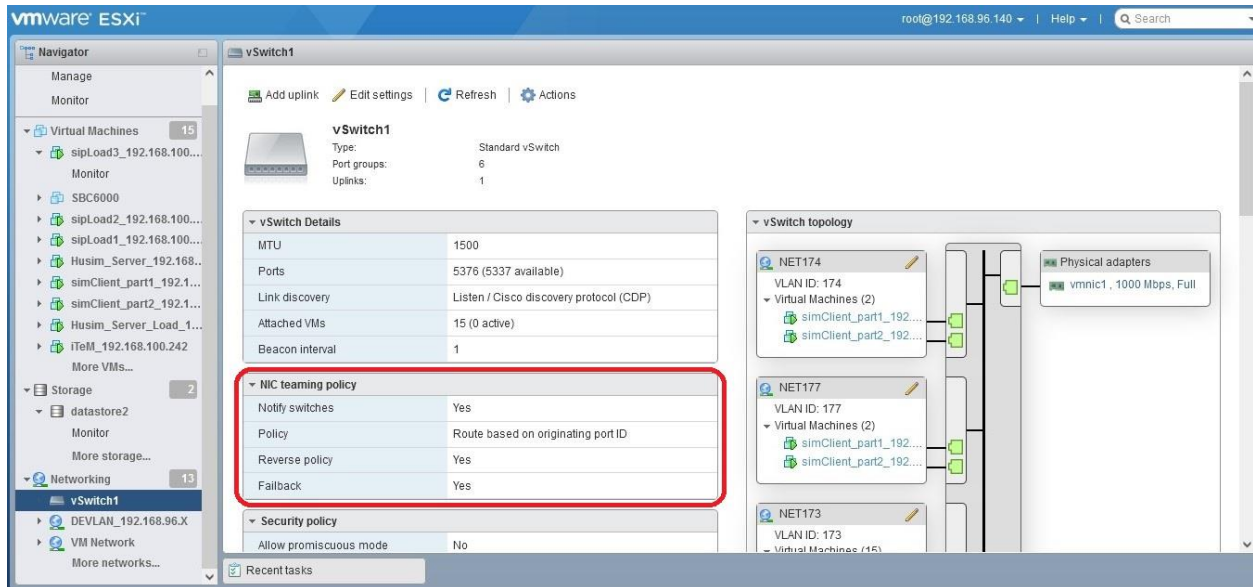


After clicking **OK**, you will be asked to configure where to save the resulting ISO file.



2.3.3 NIC Teaming on VMHost

1. Identify the physical NICs on the VM Host to be teamed (i.e. **vmnic5** for the Access side).
2. Connect cables from these NICs to the Access Network from the VM Host. Configure in accordance with VMWare documentation.
3. Enable the four checkboxes for: Load Balancing, Network Failover Detection, Notify Switches, Fallback. Keep the default settings for each.

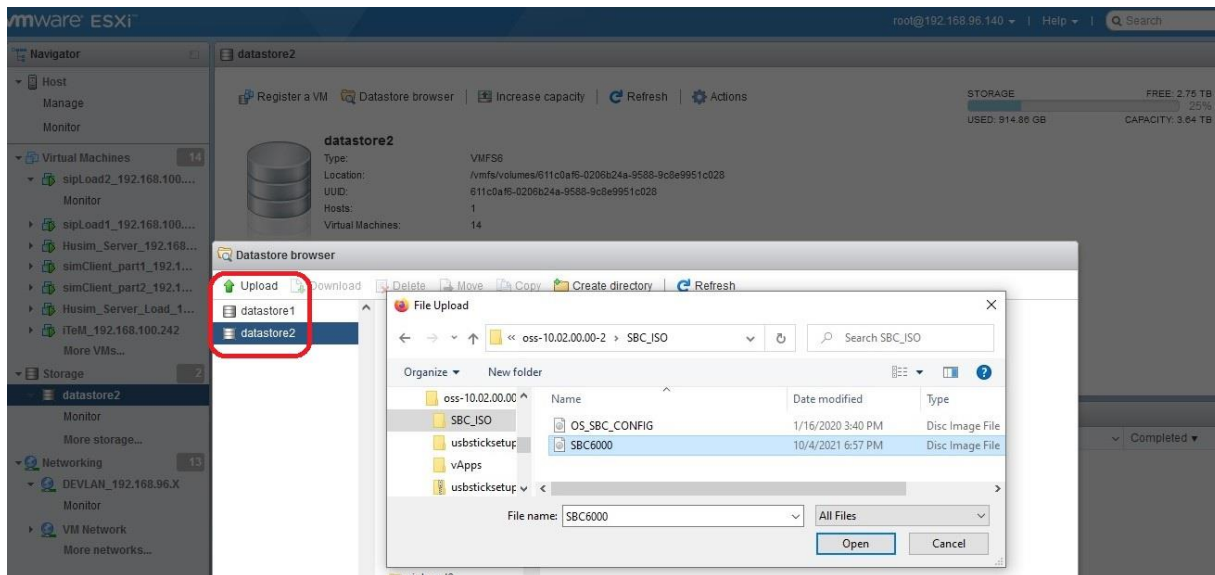


4. When creating the OS-SBC VM, assign this Network label to the appropriate interface of the OS-SBC (i.e. LAN or WAN). There is no need to modify the Hostname of the OS-SBC to append any suffix.

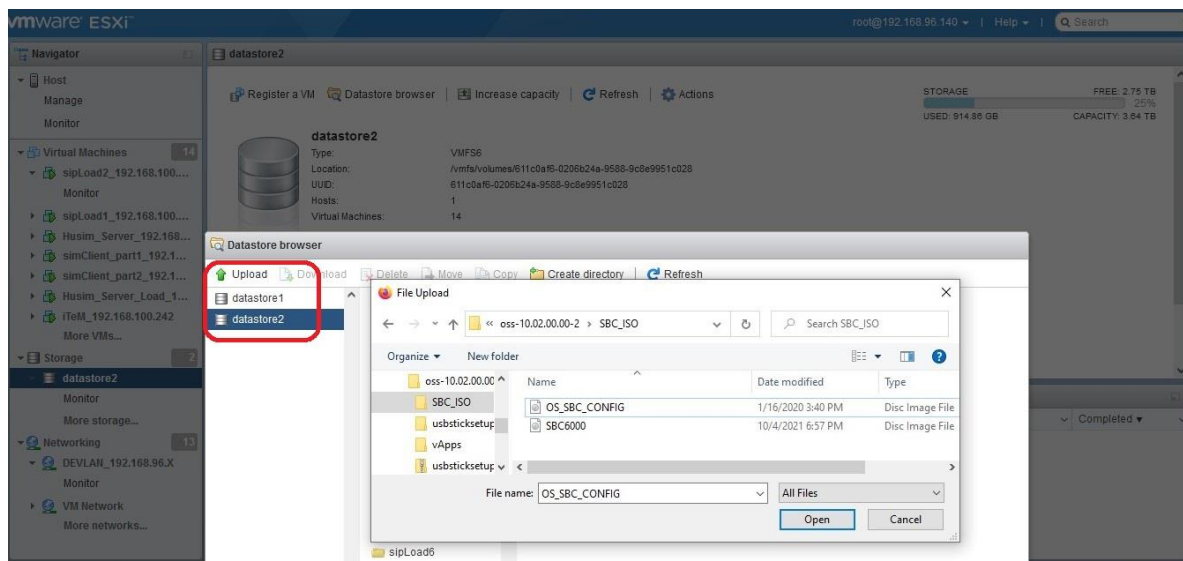
2.3.4 Detailed steps to deploy with a vApp (cont)

ESXi 6.5 or higher can be managed by any web browser using the VMware Host Client, which is based on HTML5 technology.

1. Upload the OS-SBC ISO image to VM Host Datastore. The ISO image generation is mentioned in **2.3.2.1 How to create the OS-SBC ISO image with the Software Load**.
2. Select the **Storage** option.
3. Right click on **datastore** and select **Datastore browse**.
4. Select the folder where you want to store the file and click the **Upload** File Icon.
5. Click **Open** and then point to the file to be uploaded.



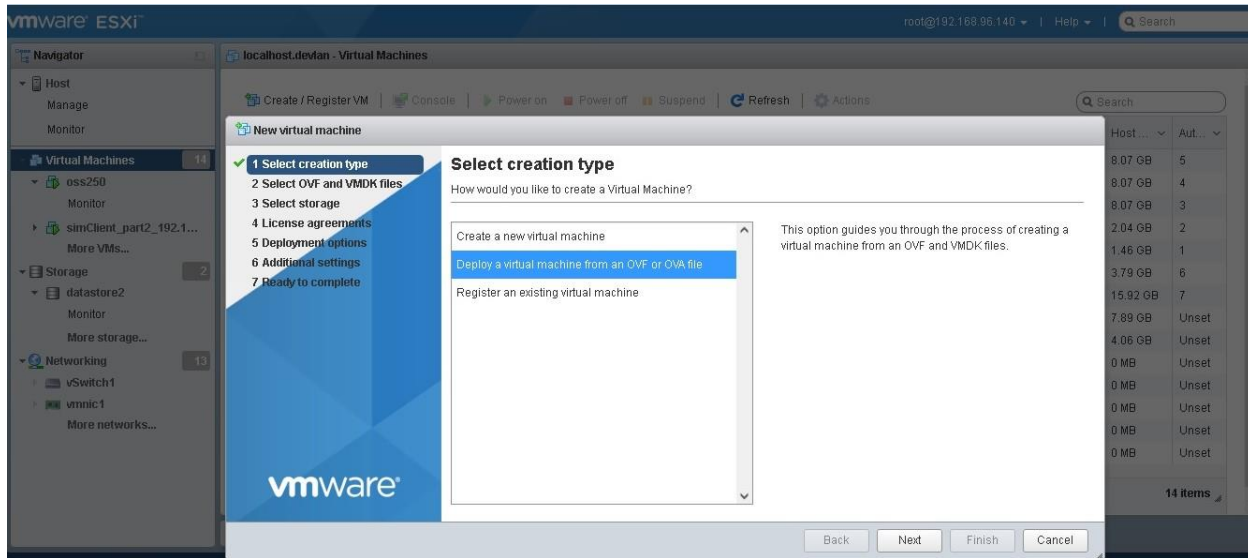
Repeat this procedure to upload the OS-SBC Configuration ISO image if it is available.



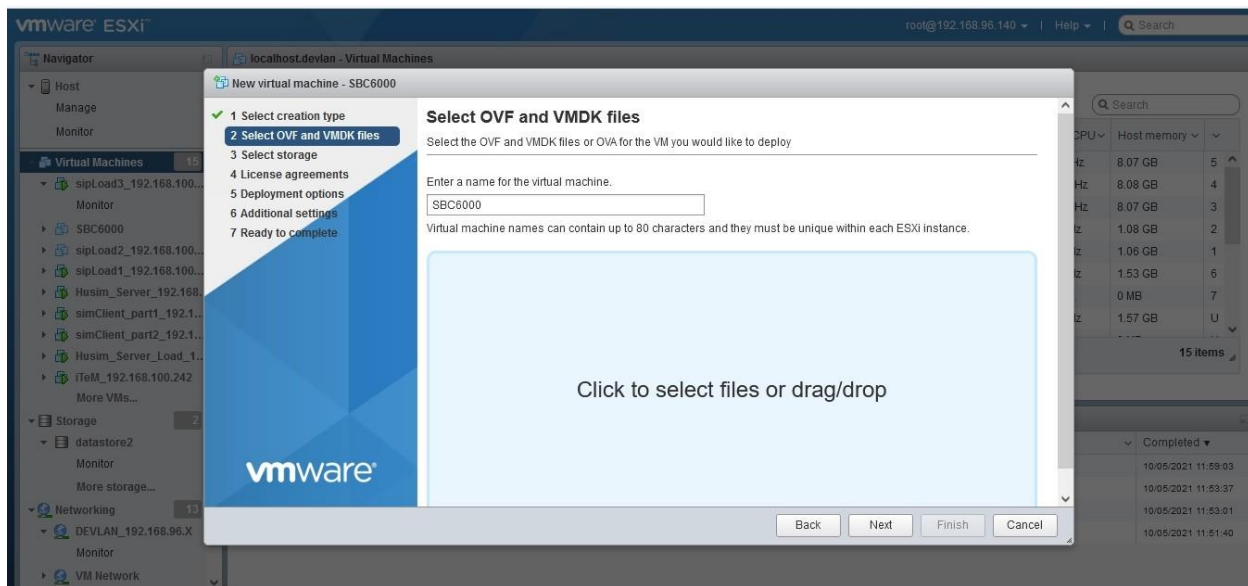
Now, you are ready to deploy the OVF template and create the OS-SBC VM:

6. From the VMWare Host Client, select the option **Create / Register**.

7. In the **Select creation type** field select **Deploy a virtual machine from an OVF or OVA file** and click **Next**.



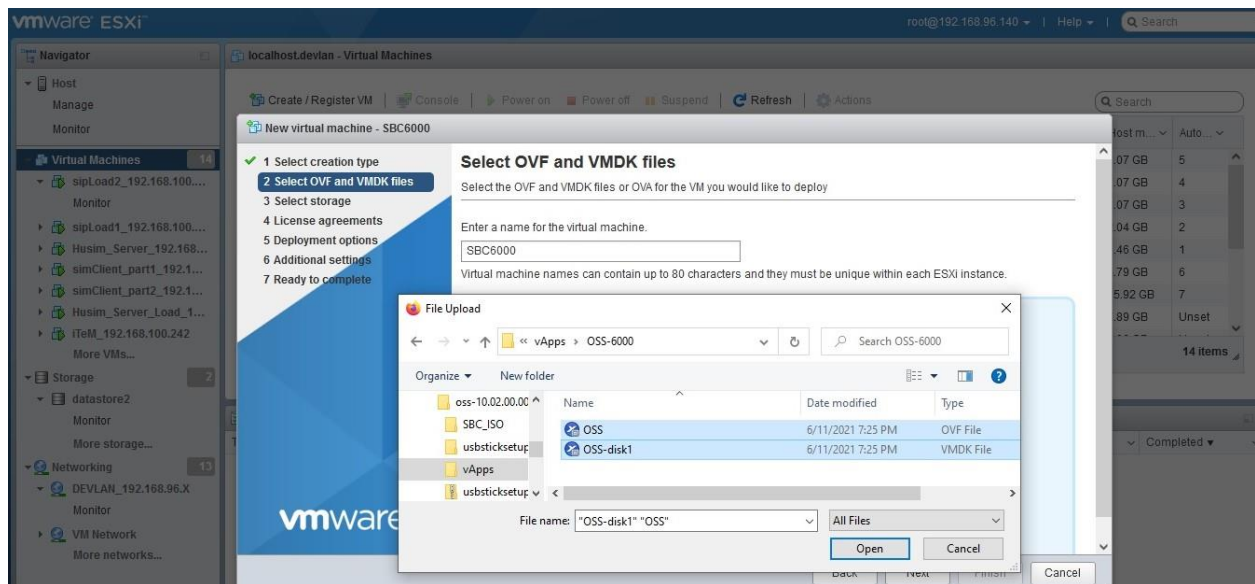
8. Enter a name for the virtual machine and click to select files.



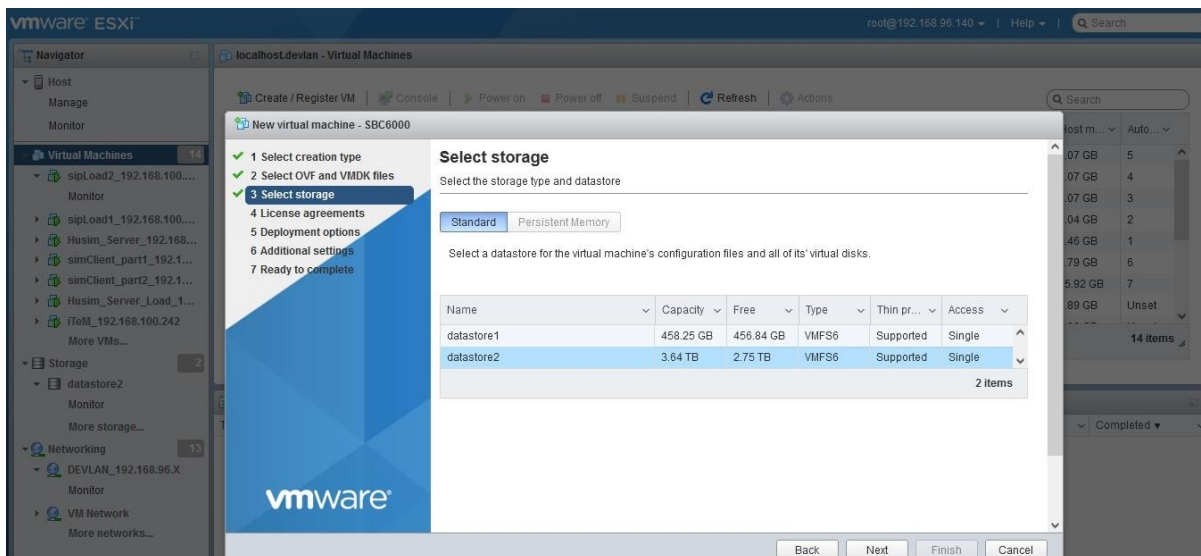
9. Select the **vApps** folder for the right OS-SBC type (OSS 250, OSS 6000 or OSS 20000).

10. Select the **OSS.ovf** and **OSS-disk1.vmdk** files and click **Next**.

Note: You need to select both files to complete this step successfully.



11. Click **Select storage** to select where to install the virtual machine and then click **Next**.



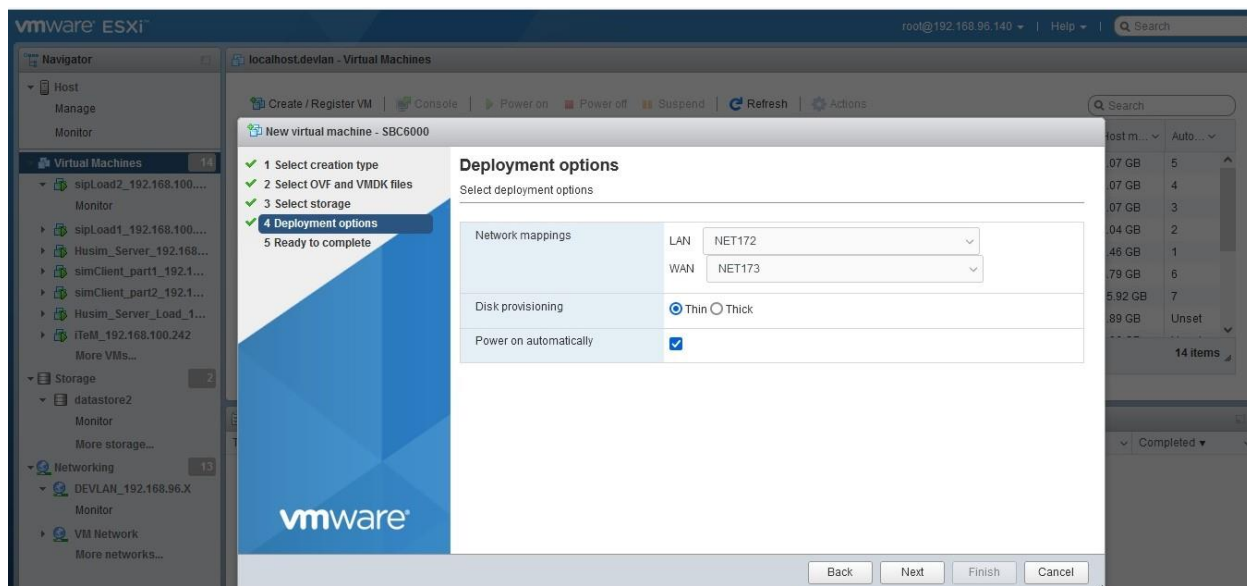
Map Network cards to ports and configure LAN and WAN options:

12. Select the option to Disk provisioning. Two options are available:

- **Thick:** A traditional model of storage provisioning. With thick provisioning, large amount of storage space is provided in advance in anticipation of future storage needs. However, the space might remain unused causing underutilization of storage capacity.
- **Thin:** This method helps you eliminate storage underutilization problems by allocating storage space in a flexible on-demand manner. When you use thin provisioning, monitor actual storage usage to avoid running out of physical storage space.

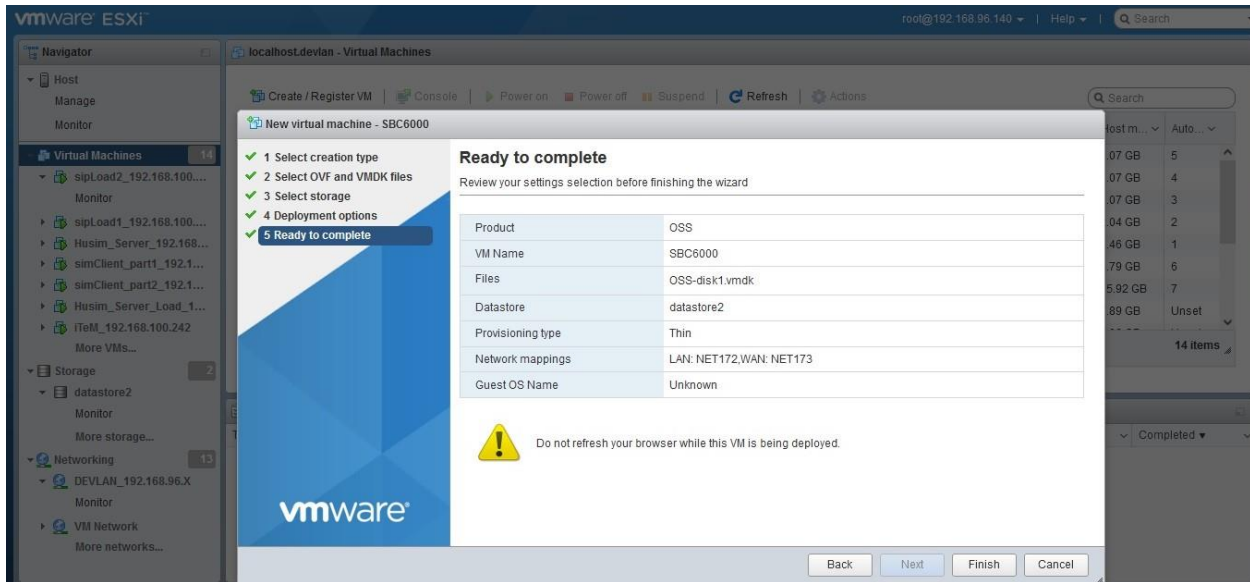
Note: Using thick eager-zeroed virtual disk reduces delays the first time that a block is written to the disk and ensures that all space is allocated and initialized at creation time.

13. Select **Power on automatically** and click **Next**.

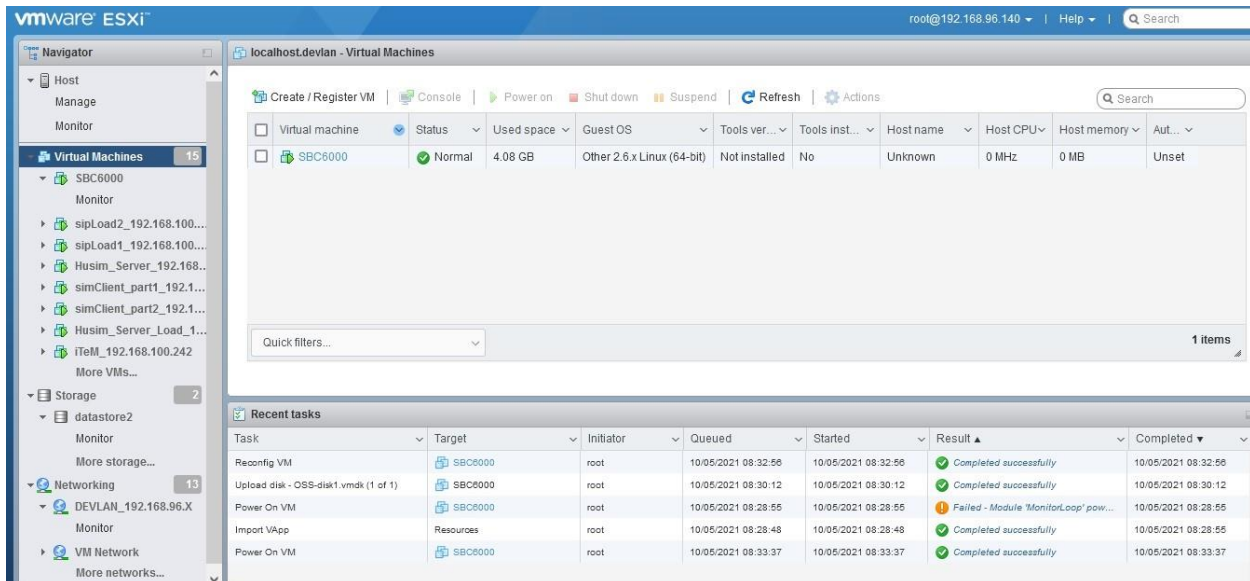


The virtual machine is ready to complete.

14. Click **Finish**.



The virtual machine has been created.



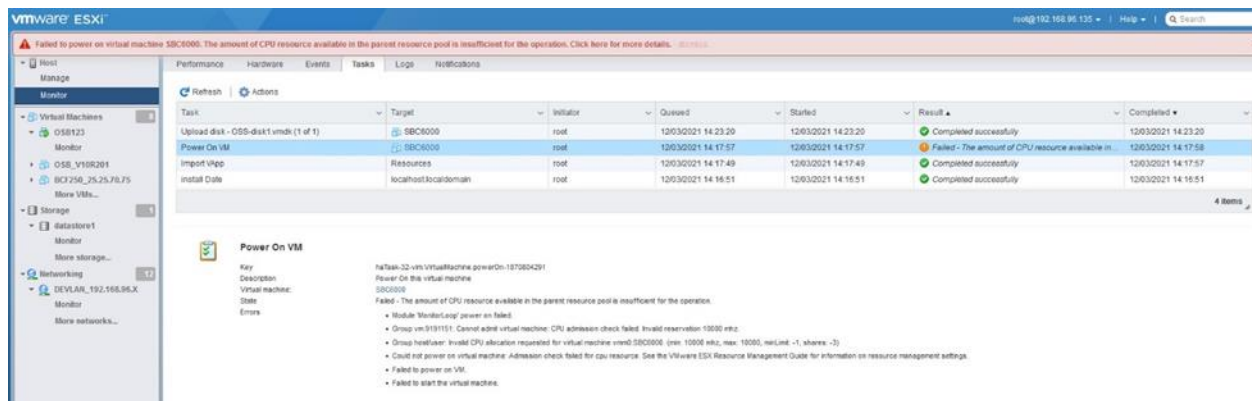
Note: When deploying vApps these values are set automatically (based on the 2.5 GHz core processor). In OVF file in vApps, the CPU reservation is configured for Virtual OSS 250 (5000 MHz), Virtual OSS 6000 (10000 MHz) and Virtual OSS 20000 (20000 MHz). Regardless if VM has been created manually or with vApps these values need to be adjusted to fit the host processor capabilities. Other critical applications running at same host need to be 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.

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.”

Errors

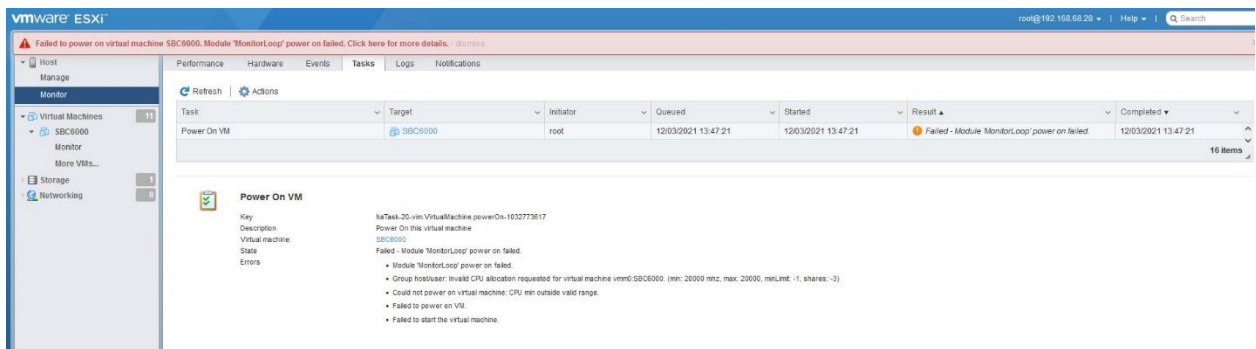
- Module 'MonitorLoop' power on failed.
- Group vm.8998268: Cannot admit virtual machine: CPU admission check failed. Invalid reservation 20000 mhz.
- Group host/user: Invalid CPU allocation requested for virtual machine vmm0:SBCCConfigDemo. (min: 20000 mhz, max: 20000, minLimit: -1, shares: -3)
- Could not power on virtual machine: Admission check failed for cpu resource. See the VMware ESX Resource Management Guide for information on resource management settings.
- Failed to power on VM.
- Failed to start the virtual machine.



“Failed - Module 'MonitorLoop' power on failed.”

Errors

- Module 'MonitorLoop' power on failed.
- Group host/user: Invalid CPU allocation requested for virtual machine vmm0:SBCCConfigDemo. (min: 20000 mhz, max: 20000, minLimit: -1, shares: -3)
- Could not power on virtual machine: CPU min outside valid range.
- Failed to power on VM.
- Failed to start the virtual machine.



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 in case of high CPU usage.

15. Click **Edit Settings** on your VM to attach the ISO image to the CD/DVD Drive.

Verify the **CD/DVD Drive 1** and **CD/DVD Drive 2**.

Please select the **CD/DVD Drive** that is associated with **IDE Controller 0(IDE 0)** to map to the **OS-SBC ISO image**:

- Select the option **Datastore ISO file** and browse the **OS-SBC ISO image**.
- Set the flag **Connect at power on**.

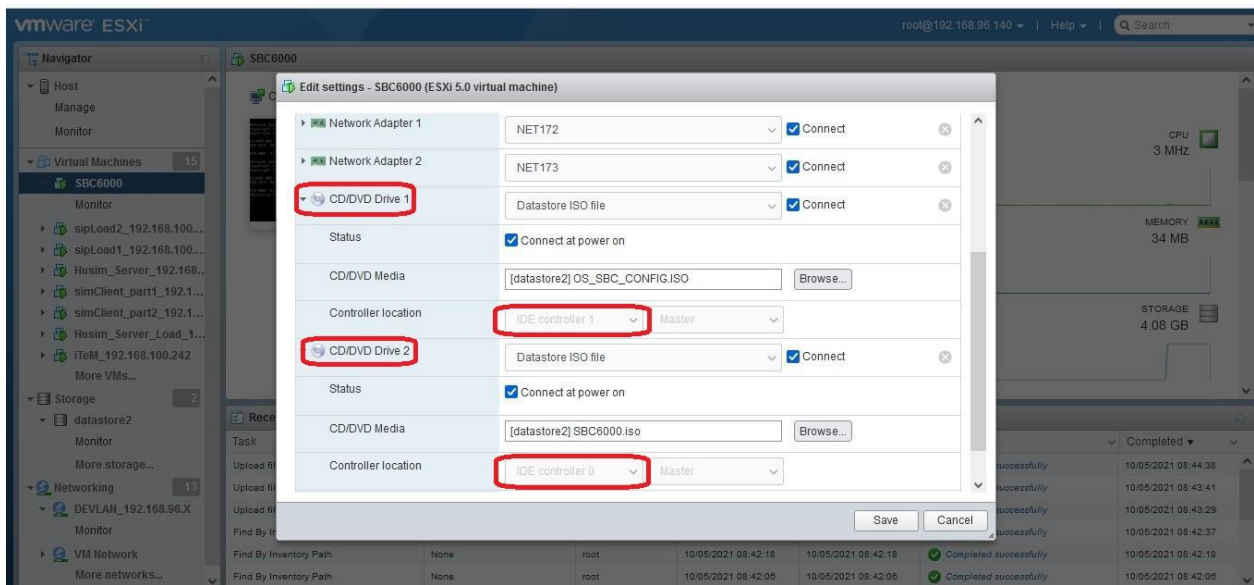
The other **CD/DVD Drive** is associated to **IDE Controller 1(IDE 1)**, that is used to connect the ISO related to **OS-SBC Configuration ISO image**.

- Select the option **Datastore ISO file** and browse the **OS-SBC Configuration ISO image**.
- Set the flag **Connect at power on**.

Note: If the OS-SBC Configuration ISO file is not available, the CD/DVD Drive associated to IDE Controller 1 can be removed.

In the example, the CD/DVD Drive 2 is associated to the IDE Controller 0 and the CD/DVD Drive 1 is associated to the IDE Controller 1.

The OS-SBC ISO image is selected to CD/DVD Drive 2 and the OS-SBC Configuration ISO image is selected to CD/DVD Drive 1.



3 Configuration

3.1 General steps to add a OS-SBC

1. Add the endpoint to the OpenScapeVoice
2. Add the OS-SBC to the OpenScape SBC Assistant
3. Load the OS-SBC
4. On the OS-SBC under the “Network / Net Services” tab verify / update
 - a. LAN and WAN information including ports for TCP,UDP and MGCP
 - If multiple LAN core addresses are used they are configured here
 - If multiple WAN addresses are used they are configured here
 - b. Default gateway information. The default gateway starts out as the LAN for bring-up of an OS- SBC, then is should be changed the make the gateway for the WAN thedefault.
 - c. Redundancy (if required)
 - d. NTP information (This is especially important if the protocol used is SRTP- Mikey)
 - e. DNS information
5. On the OS-SBC under the “security” tab
 - a. Enable Message Rate Control
 - b. The user must configure a Message rate threshold value for VoIP operation following one of the procedures below:
 - The Message rate threshold of 20000 must be used during system upgrades if the

network server interface IP address used for performing the file uploading during system upgrade cannot be identified. Once the system upgrade is complete, the Message rate threshold of 20000 must be lowered to the VoIP PPS threshold (recommended value of 300).

- The Message rate threshold is configured to the VoIP PPS threshold (recommended value of 300) and all network interface(s) used for the system upgrade file upload are configured in the white-list. By placing these network interface address(es) into the white-list, they are not subject to any packet filtering with the Message rate threshold.
 - If the user finds that calls are still being blocked by Message rate threshold (check the Firewall &Msg Rate control log – Diagnostics & Logs → Debugging → Log Viewer → select the log → show), the user will need to either increase the limit for blocking or add the IOP address which is being blocked to the white list.
- c. Default firewall settings are created for the “main” access interface by default. If additional firewalls are required, for VLANs, click “add”. Here you can select the VLAN, control network connections, edit the white and black lists and control administrative access. To control administrative access click add, enter the IP address or IP address and mask in the form address/mask (eg.10.191.9.253/24), then hit the “tab” key and select the protocols (a check means to allow).

Important: In case ALL available eth interfaces are bonded the respective **Realm Network IDs** cannot be added under Firewall Settings.

- d. If required, set up the external firewall parameters. Refer to section Firewalls
- e. Under General → Passwords, change /reset Password.
- Change the password for all functions. The default password **should not be kept**.
6. On the Network / Net Services Tab:
- a. Enable the desired interfaces
 - b. Configure the core realms
 - c. Configure the Access realms
 - d. Configure the realm profiles
 - e. s

7. On the OS-SBC under the "VOIP"→Sip server Settings tab verify / update
 - a. Configuration for the OSV node(s)
8. On the OS-SBC under the "Features" verify / update
 - a. Configuration information for remote subscribers (if required)
 - This includes changing the "Port Mapping TTL timer" to a value just greater than the longest time it takes a valid user to re-register.
 - b. Configuration information for remote endpoints"(if required), for branches, gateways and SSPs.
9. On the OS-SBC under the "SYSTEM" tab verify / update
 - a. Local GUI→ System→OpenScape OS-SBC licenses. Verify the licenses which allow the OS- SBC to operate.
10. On the OS-SBC dashboard, verify that OSVs are NOT in the penaltybox.
11. This is the minimum to allow the addition of subscribers, gateways and branches.

3.2 OpenScape Voice (OSV) Configuration

Following configuration is required in the OSV.

3.2.1 RTP parameters

startCli →OSV parameter Srx/Sip/AuthTraverseViaHdrs should be set to "RtpFalse"



This flag is to enable authorization credentials to be looked up by traversing requests via headers.
 When set to false the Via header will not be checked and every request will be challenged.
 If set to true and the IP from the via header is set as trusted host then every request coming from this IP would not be challenged.

Srx/Sip/CentralSbcSupport should be set to "RtpTrue"

This flag enables code in the OSV which supports the use of OS-SBCs.

3.2.2 /etc/hosts in OSV

When using FQDN for phones to address the OS-SBC, the OSV must also be set to resolve the FQDN to SIPSM of the OSV.

In the example shown below the name sbc11.csbc.unify.com, which is the FQDN programmed into the phones, is set to resolve to the SIPSM of the OSV 10.232.65.102.

```
# tail /etc/hosts
10.232.2.15      v5_ms_2_15.unify.com
10.232.2.15      Assistant2-15
10.232.63.94     rgtls.unify.com
10.232.65.102    unify-osv1
10.232.65.102C-SBC-3550-B2.csbc.unify.com
10.232.65.102sbc11.csbc.unify.com
10.232.65.102  osv.obsbc.com
```

3.2.3 OS-SBC SIP Endpoint Configuration: create Sip Endpoint.

This will create the endpoint for the OS-SBC using port 5060 or 5061. The endpoints of any branch or gateway “behind” this SBC will be created latter using a unique port number.

Configuration → OpenScape Voice → select the OSV → BG → Members → Endpoints → Add

It is necessary that the “Endpoint Template” of “Central SBC” be selected. This will cause the “Endpoint Type” to be set to “Central SBC”.

Data is required on the “General”, “SIP”, “Attributes” (select SIP Proxy, Route via Proxy) and Aliases (for example the IP address of the OS-SBC like 10.232.63.94:5060) tabs.

3.2.3.1 OSV Endpoint/OSS Configuration with MTLS

Configuration in OpenScape Voice

The OS SBC endpoint configuration in OpenScape Voice:

Create the OS SBC endpoint in OpenScape Voice. Configure the **Endpoint Address**.

In the following example port **5161** was used with Transport Protocol MTLS.

The IP port has to match the configured core IP and "SIP-TLS" core port shown under "Configuration in OS SBC" point "a)".

Configure the Aliases with the ip address and port.

Save the configuration.

The screenshot displays the configuration interface for an endpoint named 'ossvmred' in the 'Main Office' context. The interface is divided into two main panels. The left panel, titled 'SIP', contains settings for 'Endpoint Type' (set to 'Central SBC'), 'SIP Private Networking' (disabled), 'SIP Trunking' (enabled), and 'SIP-Q Signaling' (disabled). Below these is the 'SIP Signaling' section, which includes a note about static endpoints and a 'Type' dropdown set to 'Static'. The 'Signaling Address Type' is set to 'IP Address or FQDN'. The 'Endpoint Address' is '21.21.100.50', the 'Port' is '5161', and the 'Transport protocol' is 'MTLS'. There are checkboxes for 'Endpoint does not accept incoming TLS connections' (unchecked), 'Best Effort SRTP support' (set to 'MIKEY, SDP'), and 'ANAT Support' (set to 'Enabled'). The right panel, titled 'Aliases', shows a list of aliases with one entry: '21.21.100.50:5161'. Both panels have 'Save' and 'Cancel' buttons at the bottom.

OpenScope Voice MTLS port configuration

The MTLS port in OpenScope Voice SIP is configured with port **5161**.

UNIFY Common M

Configuration Maintenance

OpenScope Voice OpenScope

senhora

Administration

- General Settings
- Media Servers
- Certificate Management
- ▼ Signaling Management
 - SIP
 - SIP-Q
 - Authentication
 - TLS Settings
 - CSTA
- Feature Settings
- Licensing Management
- Call Admission Control
- Tools

https://10.100.123.82/management/portal/Applications/Operation/OSV/Administration/SignalingManagement

[senhora]- SIP Settings

SIP Settings

Best Effort SRTP ICE Interworking AEI Support FQDN ANAT Interworking Responsible Domains

General Rerouting Audit SIP Timers DTLS Interworking

Signaling Protocol

ⓘ If MTLS IP is different from TLS IP traffic to the OSV MTLS IP may use port "MTLS port" and "TLS port".

Node 1 Listening IP Address 1 for UDP, TCP and TLS: 10.80.24.54

Node 1 Listening IP Address 2 for Mutual TLS (MTLS): 10.80.24.56

Node 2 Listening IP Address 1 for UDP, TCP and TLS: 10.81.24.55

Node 2 Listening IP Address 2 for Mutual TLS (MTLS): 10.81.24.57

Node TCP/UDP Port: 5060

TLS Port: 5061

MTLS Port: 5161

Protocol Version: 2.0

Mime Version: 1.0

Registration

ⓘ Set maximum Registration Renewal.

Max. Reg. Renewals(s): 604800

Dummy Answer RTP Parameters

ⓘ Read-only Display of the RTP Parameters Used for Handling the Possible Dummy SDP Answers

Dummy Connection IPv4 Address 1: 10.80.24.54

Dummy Connection IPv4 Address 2: 10.81.24.55

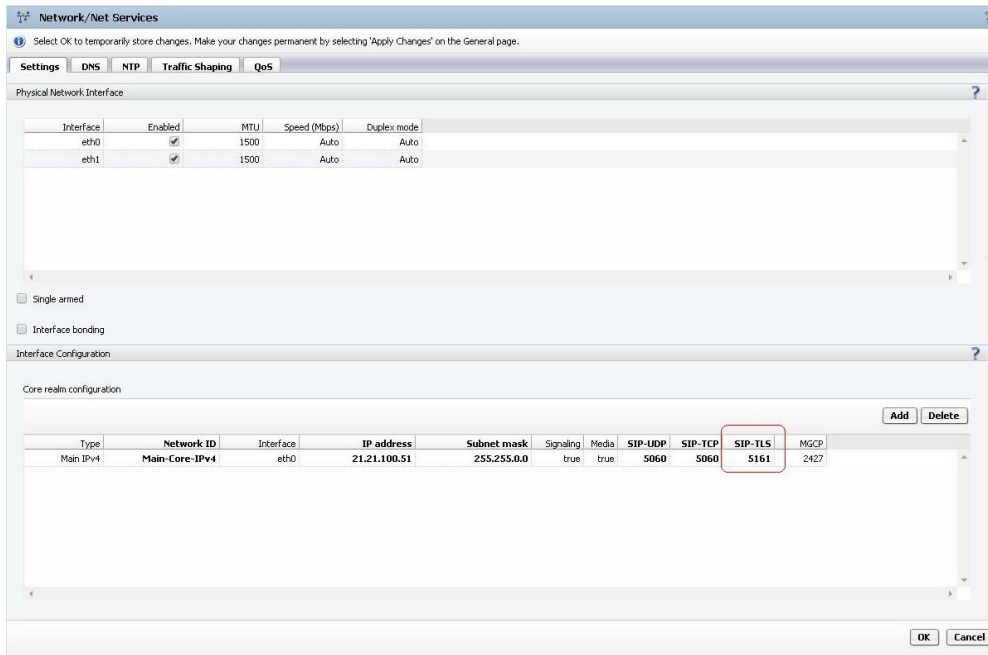
Dummy Connection IPv4 Port: 5004

Dummy Connection IPv6 Address 1: fdc1:80:243::9

Save Cancel

Configuration in OS SBC

- a) Configure the SIP TLS port as 5161 in Network/Net Services/Interfaces Configuration/Core realm configuration in OS SBC:



- b) Under folder **VOIP/ SIP Port Settings** configure the OSV's MTLS addresses for OSV Node1 and Node2. Use the information described in the item 3.4.4.1.

The OSV's MTLS addresses can be found in the **node.cfg** (parameters **sipsm3_vip** for Node1 and **sipms4_vip** for Node2) or via the CMP (see below screenshot).

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** | **Media** | **QoS Monitoring**

General

Conn System Type: Active-Standby

☐ Allow Register from SERVER

Other trusted servers

Node 1

Target type: Binding

Primary server: 10.80.24.56 Transport: TLS Port: 5161

Backup server: Transport: TCP Port:

SRV record: Transport: TCP

Node 2

Target type: Binding

Primary server: 10.81.24.57 Transport: TLS Port: 5161

Backup server: Transport: TCP Port:

SRV record: Transport: TCP

Timers and Thresholds

Failure threshold (pings): 2 OPTIONS interval (sec): 60

Success threshold (pings): 1 OPTIONS timeout (sec): 4

Transition mode threshold (pings): 1 Notification rate (per sec): 100

OK Cancel

c) Configure the other trusted servers in OS SBC:

In this case it was configured **sipsm1_vip** and **sipsm2_vip** for OSV Node1 and Node2.

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** | **Media** | **QoS Monitoring**

General

Conn System Type: Active-Standby

☐ Allow Register from SERVER

Other trusted servers

Node 1

Target type: Binding

Primary server: 10.80.24.56

Backup server:

SRV record:

Node 2

Target type: Binding

Primary server: 10.81.24.57

Backup server:

SRV record:

Timers and Thresholds

Failure threshold (pings): 2

Success threshold (pings): 1

Transition mode threshold (pings): 1

Other trusted servers

Row	IP address or FQDN	Port	Transport
1	10.80.24.54	5061	TLS
2	10.81.24.55	5061	TLS

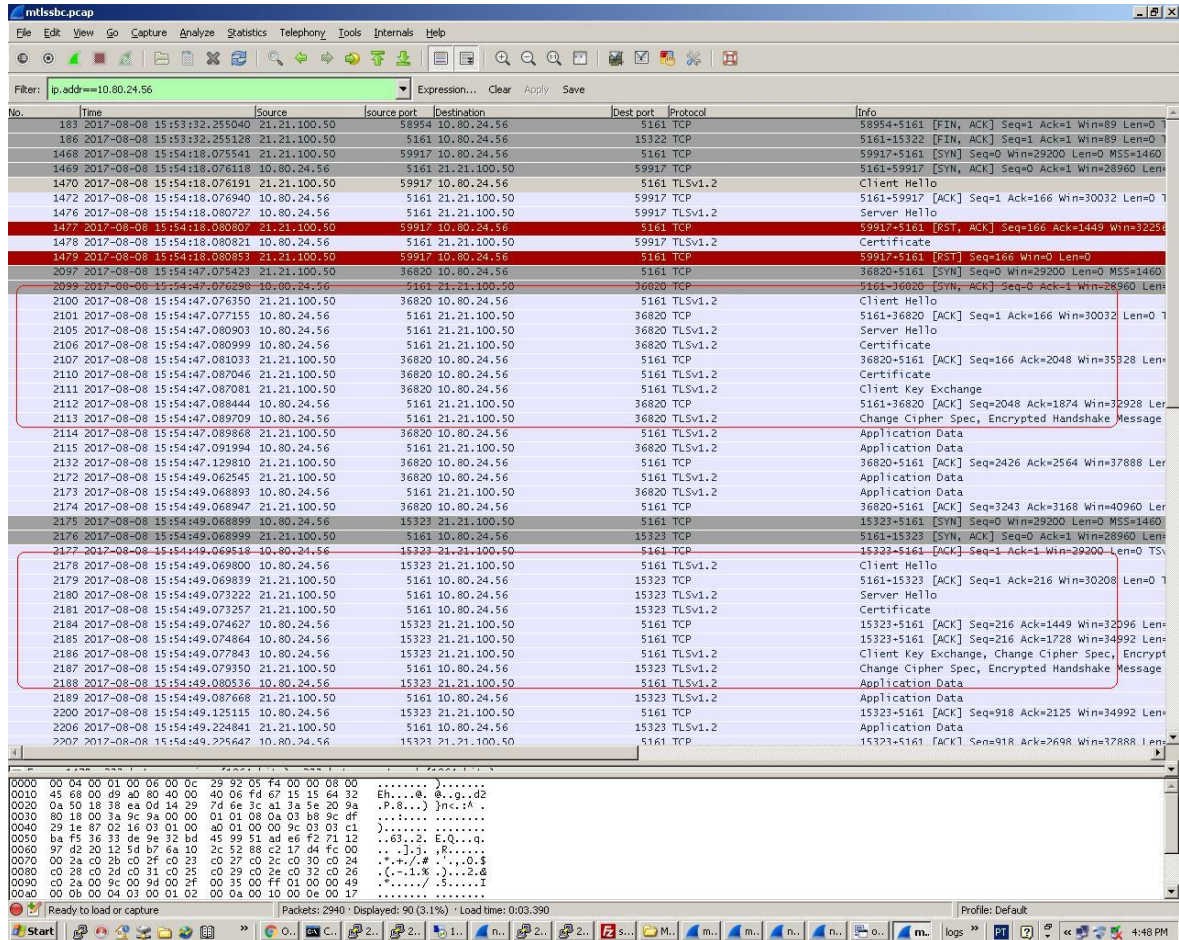
Add Delete

OK Cancel

Wireshark example

See the messages Client and Server Hello.

In this case it is important to use the correct certificate to see the messages.



3.2.4 Add an appliance to OpenScape SBC list

CMP→Configuration → OpenScape SBC→ OpenScape SBC list →Add

These will be filled in automatically when the other fields are selected

Add OpenScape SBC

Enter OpenScape SBC appliance information and select its users.

General

OpenScape SBC Name:

IP Address or FQDN:

Comm System Type:

Comm System: ...

Business Group: ...

Endpoint: ...

Communicating over Secured channel: ☐

Endpoint

Items/Page: 200 | All: 18

	EndpointName	IP Address
<input checked="" type="radio"/>	OB_CSBC	10.232.65.226
<input type="radio"/>	C-SBC-65-240	10.232.65.240
<input type="radio"/>	cSBC-Skype-Main	10.232.63.95
<input type="radio"/>	cSBC-Skype	10.232.63.95
<input type="radio"/>	C-SBC-RG8/UU	10.232.65.228
<input type="radio"/>	C-SBC-Branch	10.232.65.228
<input type="radio"/>	C-SBC-SSPt0130	10.232.65.228

Comm Systems

Please select a Comm System.

Items/Page: 200 | All: 1

Comm System
<input checked="" type="radio"/> sbctest05

Business Groups

Please select a Business Group.

Items/Page: 200 | All: 19

Business Group
<input type="radio"/> 1NR_BG4
<input type="radio"/> Acme
<input type="radio"/> BG003
<input type="radio"/> BG004
<input type="radio"/> BG006
<input checked="" type="radio"/> BG1

This checkbox will be unchecked the first time a unit is installed. If subsequent installations are required it must be manually unchecked again.

When you click “OK” the OS-SBC will then be added to the “OpenScope SBC list” as shown below.

UNIFY Common Management Platform Domain: system User: administrator@system | Settings | Help | Logout

Configuration Maintenance User Management Fault Management Performance Management Accounting 4 33 6

OpenScope Voice OpenScope Branch OpenScope SBC RG8700 Unified Communications CMP Device Management

Administration

Job Management

General Settings

Licensing

All systems

OpenScope SBC list

Select OpenScope SBC

Management

OpenScope SBC Overview - All systems

Use the Refresh selected button to update the status of selected OpenScope SBC appliances. To update the status of all OpenScope SBC appliances use the Refresh all button.

Filter: for OpenScope SBC Go Clear

Manage Password... Refresh Selected Refresh All Add... Edit... Delete

Set: 0 Items/Page: 100 All: 9

OpenScope SBC	IP Address	Comm System	Business Group	Version	Status	Last Update	Last Configuration
C-SBC-63-230	10.232.63.230	sbctest05	BG1	V7R1.14.00	Normal	2013/12/24 12:29:16	---
C-SBC-65-215	10.232.65.215	sbctest05	BG1	V8 R0.01.00	Normal	2013/12/24 12:29:16	Thu, 19 Dec 2013 15:10:28
sbclv8media	10.232.63.163	sbctest05	BG1	V8 R0.01.00	Normal	2013/12/24 12:29:16	Sat, 21 Dec 2013 01:06:00
CSBC_split	10.232.63.70	sbctest05	BG1	V8 R0.01.00	Unknown	2013/12/24 12:29:16	Sat, 21 Dec 2013 01:06:00
SBC63_76_v7	10.232.63.76	sbctest05	BG-CSBC	V7R1.14.00	Normal	2014/01/09 08:32:17	---
SBC-213	10.232.65.213	sbctest05	BG-CSBC	V8 R0.01.00	Normal	2014/01/02 04:17:04	Thu, 02 Jan 2014 16:16:40
OSS_202155	10.232.202.155	sbctest05	BG_HUSIM	---	Unknown	2014/01/06 10:11:07	---
Vm_SBC_222	10.232.65.222	sbctest05	BG1	---	Unknown	2014/01/10 11:03:46	---
CSBC_63_94	10.232.63.94	sbctest05	BG1	V8 R0.01.00	Normal	2014/01/13 10:40:31	Sun, 02 Feb 2014 03:00:23

Note:

When an OS-SBC is added via the procedure above, if the administrator has provided an appliance name (host name) on the “general” tab, this name will be applied to the node, otherwise the node will retain the hostname created during installation of the node.

If the endpoint address used is the VIP of a cluster then both nodes will have their “hostname” changed. The nodes involved will perform a restart.

3.3 Centralized Licensing On CMP

Licensing of OS-SBC can be accomplished via the CMP/OpenScape SBC Assistant with a Centralized license file/pool or via a Standalone license file directly on the OS-SBC. In order to use Centralized licensing via the CMP, the license file provided by Unify Technical Support should have been created with the MAC address for eth0 of the CMP server as the locking ID. If the license file was created with the MAC address of interface eth0 of OS-SBC, then this is a standalone license file, so refer to section [Standalone licenses for OS-SBC](#).

If Unify Technical Support provided a License Authorization Code (LAC) and Central License Server (CLS) address instead of a license file, then you must use this LAC via the CMP → Maintenance → Licenses → Information → Online Activation to access an online Central License Server (CLS) to get the license file for your CMP. Refer to the current issue of the OpenScape SBC V9, Installation Guide, in E-Doku.

If a license file (.lic extension) was provided with the MAC ID of the CMP/OpenScape SBC Assistant, then this file must be applied to the CMP via offline activation at CM → Maintenance → Licenses → Information → Offline Activation → browse to file location and select it and click Activate.

To determine if OS-SBC licenses are installed on this CMP the path is:
CMP → Maintenance → Licenses → Information → <filter on “[OpenScape Branch/SBC](#)”>



System	Product Name	Feature Name	Number of used licenses	Validity
offboard	OpenScape Branch/SBC V9	Circuit Telephony Connector	0 of 100	unlimited
offboard	OpenScape Branch/SBC V9	OpenScape SBC/CTC Session (per Session)	6949 of 37000	unlimited
offboard	OpenScape Branch/SBC V9	OpenScape SBC/CTC Base	15 of 100	unlimited

At this point a license pool is created on the OpenScape SBC Assistant and licenses may be allocated to individual SBC(s).

Refer to section [Add an appliance to OpenScape SBC list](#) for how to add the Central SBC to the SBC List on the OpenScape SBC Assistant. The centralized licensing communication process between the CMP and the OS-SBC relies on three main ingredients:

1. Exchange of authentication statements
2. Logical ID of OS-SBC, and
3. Hardware ID of OS-SBC

When OS-SBC is created in OpenScape SBC Assistant, the logical ID is automatically generated by the CMP. The logical ID consists of the “<OSV Name>:<BG Groupname>:<SBC Endpoint name>”. Also verify that the OS-SBC has Security Status of “Unsecured Mode” in SBC List on OpenScape SBC Assistant.

When it is in unsecured mode, the OS-SBC can communicate with the CMP and request an authentication statement to enter “secured mode”. **During any SBC installation, remember to uncheck the flag “Communicating over Secured channel” in the SBC entry in the SBC List to return to the unsecured mode to re-establish secure communication.**

Also check the “installation” check box under CMP→configuration→OpenScape SBC→ OpenScape SBC list → <select the OS-SBC and Click “edit”> → configure installation → general tab..

To manage OS-SBC licenses the path is CMP→configuration→OpenScape SBC→OpenScape SBC list. Then select the OS-SBC and click “Manage”.

These are read only fields.

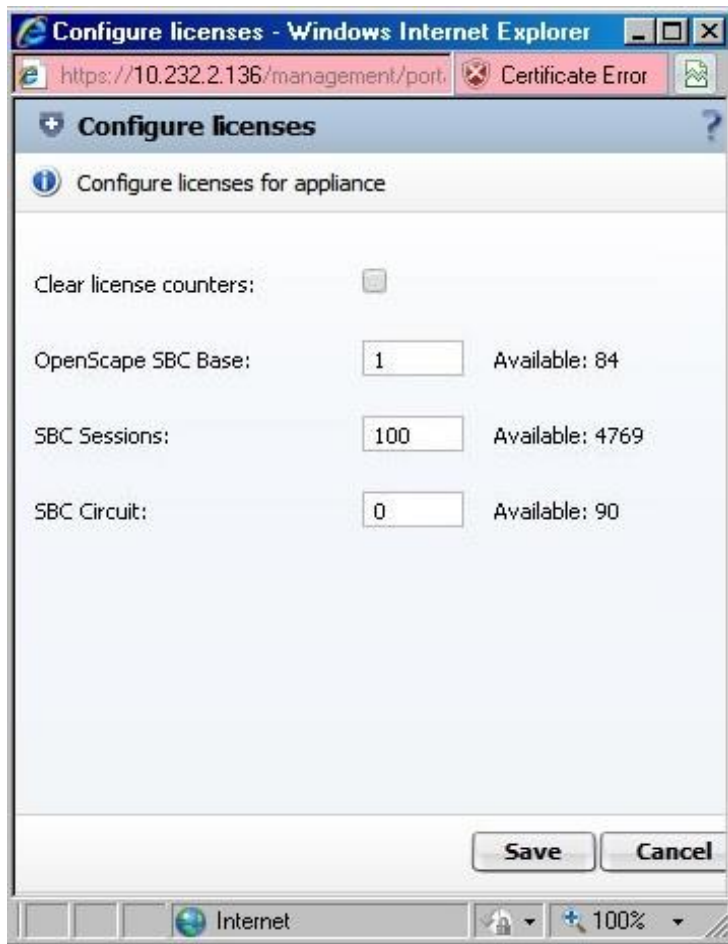
“Configured” shows licenses assigned to this OS-SBC in the OpenScape SBC Assistant database.
 “Reported Locally” shows license information from the OS-SBC.
 “Usage” shows the peak licenses used in the OS-SBC, for the past calendar month.

This will “refresh” the “Configured” column data from the OS-SBC assistant database.

This will update the OS-SBC with current information and receive updated information from the OS-SBC. This will also set the **security status** to secured mode in the OS-SBC assistant.

This will open the window shown on the next page to assign licenses to this device.

License type	Configured	Reported locally	Usage(Peak)
OpenScape SBC Base	1	1	1
SBC Sessions	100	100	9
SBC Circuit	0	0	0



To verify on the OS-SBC that licenses were assigned, from the OS-SBC Local GUI →System → Licenses → License Information, you should see License Type as “Floating” with Days to Expire set to some number or “unlimited” and the actual type of license and quantity should be listed in the table.

3.3.1 Software Subscription License Usage on CMP

CMP License Management service (CMP→Maintenance →Licenses→Software Subscription) displays the “high watermark” of “SBC sessions” usage, for the month. This number is the sum of the “high watermarks” from each of the SBCs administered by this CMP. The data is updated each day around 23:00.

At the first of each month the current “high watermark” is saved and the CMP License Management service will reset the usage counter to the current value collected. The respective high watermarks for each month are available for display for a “rolling” year.

This screen also shows the unique Product ID and valid remaining days for the license. There is also an indication showing if there was a problem collecting current values.

3.3.2 SBC sessions peak usage on OS-SBC

Each OS-SBC calculates and records a “peak usage” value of SBC sessions. The value is saved as a “high watermark” and made available to the OpenScape SBC Assistant.

The value is cleared and new calculations started on the first day of each month. Refer to Licenses for more information.

3.3.3 Standalone licenses for OS-SBC

The standalone license is used when the procedure to provide a license via the CMP is not available.

1. Obtain the “standalone” license through the regular customer service channels. The name of the file must end in “.lic”. For example “mySBCstandalone.lic”
2. OS-SBC Local GUI → System → Licenses → License information → browse and select the license file provided → Upload. Wait for the file to be uploaded.
3. After the file is uploaded close the current window.
4. Wait one or two minutes for the licenses to be “activated”.
5. OS-SBC Local GUI → System → Licenses → License information
6. Verify the “License type” is “Stand Alone” and the correct quantity of individual licenses is displayed in the column “Licenses configured”. If the acquired license file is for regular licenses (i.e. no expiration date) then the “Days till license expires” will indicate “unlimited”.
7. If there is an error in this procedure, such as the wrong MAC being used in the license file, collect the process manager log to aid in trouble shooting the problem.

An established SBC session where no RTP packages are not exchanged for 3 min will be dropped after (15~18 min), no alarm is generated, only ssm logs in certain level will show dropped sessions.

This is valid for sessions using RTP(anchored and/or transcode and or transrating).

For sessions with media optimization where the RTP packages are exchanged directly there is no audit, therefore is always recommend to use session timers between parties, this will avoid hung session is case of missing BYEs. To overcome this in the Port and Signaling Settings a configurable timer to drop sessions after time was included, this timer called Maximal call session time will drop sbc sessions and release its license counter.

3.4 OS-SBC Configuration / Displays

3.4.1 Dashboard

The screenshot shows the 'General - SBCConfigGuideDemo' page in the Atos Unify OpenScape SBC Management Portal. The top navigation bar includes the Atos logo and the user name 'administrator'. The left sidebar lists various management categories: Administration, System, Network/Net Services, VoIP, Features, Security, Diagnostics & logs, Alarms, and Maintenance. The main content area is divided into several sections:

- Alarms:** Displays an alarm summary with Critical, Major, and Minor counts, all currently at 0. A 'Show alarm details' button is available.
- System Status:** Shows the branch mode as 'Centralized SBC' and the auto refresh timer set to '20 seconds'. It lists the operational state as 'normal' and provides details for two nodes (Com Node 1 and Com Node 2), including primary and backup server IP addresses and their respective penalty box states (Active).
- System Info:** Displays hardware and software information. Hardware details include CPU (3.25% - 4 x 1995 MHz), Memory (13.79% - 4 Gb), and Disk (13.08% - 42 Gb). Software details include the version (V10 R2.00.00) and partition information (Active/Backup).
- Services status:** A grid of buttons to view the status of various services, including Registered subscribers, SSP status, Dynamic port mapping, Dynamic IP remote endpoints, Denial of Service Mitigation, TURN Allocations, Telephony Connector status, and SIP Loadbalancer status.

At the bottom right, there are 'Apply Changes' and 'Cancel Changes' buttons.

3.4.1.1 System Status and info

This screenshot provides a detailed view of the 'System Info' panel. It features progress bars and numerical data for system resources:

- CPU:** 20.73% - 2 x 2667 MHz (5000 MHz Reserved in VM)
- Memory:** 11.41% - 4 Gb (4 Gb Reserved in VM)
- Disk:** 11.28% - 42 Gb

Additional system metrics shown include a system uptime of 3 minutes and a hardware type of 'Virtual OSS 250'. The hostname is listed as 'VM'. The 'Software Info' section shows the current software version as 'V10 R3.01.01' and provides buttons to manage the software partition information, currently set to 'Active'.

Operational state shows the system connectivity with the central SIP Server. The state "normal" indicates full connectivity to primary and/or backup server. 'Survivable' mode status is only relevant internally and transition to survivability mode (when OSV nodes become unreachable) does not initiate any 'operational mode' notifications.

A Penalty Box Mechanism is implemented to determine the currently active binding.

When **Redundancy** is enabled, the state shows the status of Redundancy system. The state "MASTER" indicates that the system is the current active system.

The state "BACKUP" indicates that the system is in a standby mode (all services are disabled). The state "FAULT" indicates no networkconnectivity.

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 vmsettings.txt file which is in info.tar in rapidstat.

3.4.1.2 Service status and alarms

Services Status

Current status of available services.

Alarm Manager	<div></div> running	NTP	<div></div> running
Audit	<div></div> running	Process Manager	<div></div> running
B2BUA	<div></div> not running	Push Notification	<div></div> not running
Continuous Symptom Collector	<div></div> not running	QoS Application	<div></div> not running
Continuous Tracing	<div></div> stand-by	RTP Proxy	<div></div> running
Cron	<div></div> not running	Redundancy	<div></div> stand-by
DBMS	<div></div> running	Reverse Proxy	<div></div> not running
DHCP	<div></div> not running	SIP Loadbalancer	<div></div> not running
DNS	<div></div> not running	SIP Server	<div></div> running
Eth0	<div></div> running	SNMP	<div></div> running
Eth1	<div></div> running	SSH	<div></div> running
GTC App	<div></div> not running	SSM	<div></div> running
GTC Database	<div></div> running	Service	<div></div> not running
GTC Loader	<div></div> not running	Survivability Provider	<div></div> running
IPsec	<div></div> not running	Syslog	<div></div> running
Kernel Console Collector	<div></div> not running	TURN Server	<div></div> not running
MS Adapter	<div></div> running	Web Server	<div></div> running
Media Server	<div></div> not running		

NOTE: some services are not enabled by default

These service will run in **Backup mode**: syslog, network, apache2, postgresql, alarm, ctrace, redmng, nettrace, snmpdx, ntp, ganglia, rtpproxy, ssm, mediaserver, qos_sendtrap

These services will **NOT** run in **Backup mode**: ipsec, named, zooclient, kamailio, sp, bcfMonitor, push, msadapter, redis, haproxy, turnserver, gtc, siplb, gtcloader

Alarm Details											
<div> Information about current list of alarms. </div>											
<div> <div>Clear all</div> <div>Clear</div> </div>											
<div> <div>Items/Page: 10</div> <div> <div><<</div> <div><</div> <div>1</div> <div>></div> <div>>></div> </div> <div>All : 2</div> <div> CSV Export </div> </div>											
Clear	Group ID	Event ID	Group name	Event name	Monitored value	Time	Threshold	Trigger	Severity	Flow timer	
<input type="checkbox"/>	7	1	Admin	Wrong user ID or password entered	1	2014-02-04T08:58:21+0000	0	Greater than	Major	60	
<input type="checkbox"/>	9	6	Security	TLS certificate expiration warning	1	2014-02-03T09:13:03+0000	0	Greater than	Warning	0	

3.4.1.3 Registered subscribers and Dynamic port mapping

Registered Subscribers				
Registered Subscribers				
Search for <input type="text"/> in Username Search Show All				
Items/Page: 10 << < 1 > >> All : 13 CSV Export				
Username	Contact	OSV expiry	Subscriber expiry	Mapped port
15615597203	sip:15615597203@166.20.100.102:5060;transport=tcp	114 seconds	114 seconds	10641
15615597204	sip:15615597204@166.20.100.102:5060;transport=tcp	114 seconds	114 seconds	10641
15615597202	sip:15615597202@166.20.100.102:5060;transport=tcp	114 seconds	114 seconds	10641
15615597202	sip:15615597202@166.20.100.101:5060;transport=tcp	183 seconds	183 seconds	10640
15615597203	sip:15615597203@166.20.100.101:5060;transport=tcp	167 seconds	167 seconds	10640
15615597204	sip:15615597204@166.20.100.100:5060;transport=tcp	341 seconds	341 seconds	10639
15615597203	sip:15615597203@166.20.100.100:5060;transport=tcp	218 seconds	218 seconds	10639
15615597202	sip:15615597202@166.20.100.100:5060;transport=tcp	111 seconds	111 seconds	10639
15615597201	sip:15615597201@166.20.100.100:5060;transport=tcp	207 seconds	207 seconds	10639
15615597206	sip:15615597206@166.20.100.103:5060;transport=tcp	341 seconds	341 seconds	10638

Port Mapping								
Port Mapping								
<input type="checkbox"/> Select all Delete								
Search for <input type="text"/> in Contact Search Show All								
Items/Page: 10 << < 1 > >> All : 13 CSV Export								
Delete	Contact	External IP	External port	SBC access IP	SBC core port	Map time	Expire time from server	
<input type="checkbox"/>	sip:15615597203@166.20.100.102:5060;transport=tcp	166.20.100.50	58731	10.191.0.11	10641	234 seconds		300
<input type="checkbox"/>	sip:15615597204@166.20.100.102:5060;transport=tcp	166.20.100.50	58731	10.191.0.11	10641	234 seconds		300
<input type="checkbox"/>	sip:15615597202@166.20.100.102:5060;transport=tcp	166.20.100.50	58731	10.191.0.11	10641	234 seconds		300
<input type="checkbox"/>	sip:15615597202@166.20.100.101:5060;transport=tcp	166.20.100.50	58731	10.191.0.11	10640	192 seconds		327
<input type="checkbox"/>	sip:15615597203@166.20.100.101:5060;transport=tcp	166.20.100.50	58731	10.191.0.11	10640	235 seconds		354
<input type="checkbox"/>	sip:15615597204@166.20.100.100:5060;transport=tcp	166.20.100.50	58731	10.191.0.11	10639	53 seconds		346
<input type="checkbox"/>	sip:15615597203@166.20.100.100:5060;transport=tcp	166.20.100.50	58731	10.191.0.11	10639	133 seconds		303
<input type="checkbox"/>	sip:15615597202@166.20.100.100:5060;transport=tcp	166.20.100.50	58731	10.191.0.11	10639	8 seconds		348
<input type="checkbox"/>	sip:15615597201@166.20.100.100:5060;transport=tcp	166.20.100.50	58731	10.191.0.11	10639	186 seconds		345
<input type="checkbox"/>	sip:15615597206@166.20.100.103:5060;transport=tcp	166.20.100.103	58348	10.191.0.11	10638	59 seconds		352

Note: Each registered key appearance counts toward the platform limit for registered subscribers.

Example:

Three devices each have the same three key appearances assigned, would count as nine registered users on the OS-SBC.

This button clears port mapping for selected entries. Unregister is sent to the OSV to clear the registration cash on the OSV. Active calls are affected and subscribers must register again.

3.4.1.4 SSP Connectivity Status

The SSPs status can be seen on the SSP Connectivity Status page, which is accessible from SBC's main page. On this page it is possible to check the registration status, the connectivity status, which concerns the OPTIONS requests, and also trigger register requests for those SSPs that the registration is required.

IMPORTANT: The registration status and the send register functionality are only available for those SSPs that are configured with a profile that the registration is required.

The screenshot shows the Atos Unify OpenScope SBC Management Portal. The top navigation bar includes the Atos logo and the user name 'administrator'. The left sidebar lists various management categories like Administration, System, Network/Net Services, VoIP, Features, Security, Diagnostics & logs, Alarms, and Maintenance. The main content area is titled 'General - SBCConfigGuideDemo' and contains an 'Alarms' section with a summary of critical, major, and minor alarms. Below this, there are sections for 'System Status' and 'System Info'. The 'System Status' section includes details about the branch mode, operational state, and two core nodes (Com Node 1 and Com Node 2) with their primary and backup servers. A red box highlights the 'SSP status' link in the 'Services status' section. The 'System Info' section displays hardware and software details. At the bottom, the 'SSP Connectivity Status' section shows a table of SSPs with their registration status and connectivity check results.

Status	SSP Trunk Name	Default Home DN	URI	SSP Connectivity Check	SSP Registration Status	Register/Unregister
Not Available	SSP_Register_3	156120001903	sip:173.16.105.200:5061;transport=tls	Not Available	Not Registered	<input type="checkbox"/>
Registered	SSP_Register_2	554420181902	sip:173.16.105.200:5060;transport=tcp	Not Available	Registered	<input type="checkbox"/>
Registered	SSP_Register_1	554420181900	sip:173.16.105.200:5060;transport=udp	Not Available	Registered	<input type="checkbox"/>
Not Available	SSPFAX		sip:173.16.6.11:5060;transport=tcp	Not Available	Not Available	<input type="checkbox"/>

3.4.1.5 Dynamic IP Remote Endpoints

Dynamic IP Remote Endpoints		
Dynamic IP Remote Endpoints		
Logical-Endpoint-ID	External IP	SBC Access IP
OSV:BG:89012345678901234567890123456789012345	none	10.232.63.94
1234567890	none	10.232.63.94
OSV:bg:branch:another	none	10.232.63.94
10.191.1.243	none	10.232.63.94
123456789012345678901234567890123456789012345	none	10.232.63.94
sbctest03:BG1_MAIN:Branch_SBCProxy	10.191.1.242	10.232.63.94

Dynamic IP remote endpoints
Shows relationship between “logical Endpoint-ID” and current IP address of dynamic endpoints.

3.4.1.6 Denial of Service Mitigation display

This shows the “Quarantine Grid” of Source IP addresses affected by denial of service blocking due to message rate limit violations only. The list may be searched by IP, quarantine TTL or network ID. Selected devices may be unblocked from this screen.

Refer to [Denial of Service Mitigation](#)

Quarantine Grid for Unauthorized/Unknown Users shows the IP:Port and Expire time of Unauthorized/Unknown Users.

3.4.2 System Settings

System

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

Settings

License

Branding

General

SBC Mode

Centralized SBC

Hostname

SBCConfigGuideDemo

Domain name

unify.com

Administration

Session expiry timer

1 hour

Default language

English

Watchdog Configuration

☐ Watchdog expiry timer

Watchdog information

Watchdog expiry timer

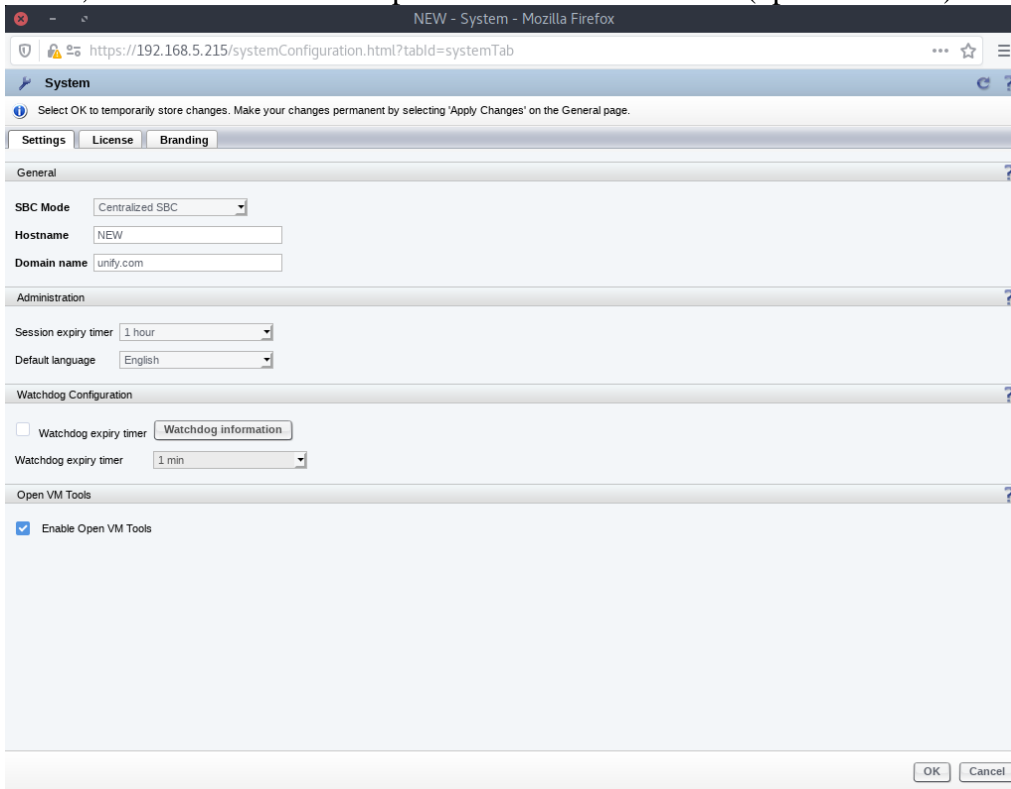
1 min

Open VM Tools

☒ Enable Open VM Tools

3.4.2.1 Enable Open VM Tools

If checked, this field enables the Open Virtual Machine Tools (open-vm-tools)



NEW - System - Mozilla Firefox

https://192.168.5.215/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

SBC Mode: Centralized SBC

Hostname: NEW

Domain name: unify.com

Administration

Session expiry timer: 1 hour

Default language: English

Watchdog Configuration

☐ Watchdog expiry timer Watchdog information

Watchdog expiry timer: 1 min

Open VM Tools

☒ Enable Open VM Tools

OK Cancel

After enabling this feature, VM Ware will show that VM Tools is enabled and running.

Console | Power on | Shut down | Suspend | Restart | Edit settings | Refresh | Actions



OSS douglas 1

Guest OS	Other 2.6.x Linux (64-bit)
Compatibility	ESXi 5.0 and later (VM version 8)
VMware Tools	Yes
CPU	2
Memory	2 GB
Host name	sbc94

General Information	
Networking	sbc94
VMware Tools	Installed and running
Storage	1 disk
Notes	Edit notes

Hardware Config	
CPU	
Memory	
Hard disk 1	
Network adapte	
Network adapte	

3.4.2.2 Licenses

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: 192.168.96.64 License server port: 4709

Hardware ID: 00:0C:29:65:9E:17

Logical ID: senhora:BG_RD_OSB_OSSBC:SBC_Configdemo

Advanced Locking ID: L3DJDR3M+:CCU7YKCU7YKQV Refresh

License Information

License Version: V10 SIEL ID: SID:152135222399

License type: Floating Days till license expires: unlimited

Stand alone license file:

Choose File No file chosen Upload

Refresh from License Server

License type	License configured	Licenses usage (peak)
OSS Base	1	1
Circuit SBC Sessions	0	0
SBC sessions	100	0
SBC BCF	0	0
SBC MS Direct Routing	0	0

This is a configurable Field which allows the setting of a license Server.

Must match logical ID in OpenScape SBC assistant.

Used to upload a "standalone" license if the license is not obtained from the license server (CMP).

This column shows peak usage for the current month. At the start of each month the values are reset to zero.

SIEL-ID: This field shows the Standardized Integrated Equipment Life-cycle (SIEL) that is delivered to each network element with licenses file from the Central License Server (CLS). The SIEL ID is also retrievable over a specific SNMP get request. Depending on the Licence type (CMP assigned or local Licence) the SIEL ID will read:

for CMP assigned Licences:

CMP will provide the SIEL ID thru the WSDL interface along with the Licence Version (V9, V10 etc.)

SIEL ID is received from CMP: SID: received siel ID

SIEL ID is NOT received from CMP: SID: CMP assigned

for locally applied License

SID: SIEL ID retrieved from CLS

The IP address of the node that will execute the snmpget commands needs to be included under Alarms > SNMP Configuration > SNMP v2c Read-Only IP

3.4.2.3 Branding

3.4.2.3.1 Entering Branding Information using Local GUI:

Local GUI → System→Branding

Company name can be entered here. This name can be made up of upper or lower case letters, digits, or special characters. Special characters can be any of the following set: !@#%&()_+{}|:;'/=,^\$.*[]™©äÄüÜöÖ€µß and the white space.

Even though the company name is entered here, it is not visible in any of the pages of the GUI. It is reserved for future use.

System

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

Settings License Branding

Branding Settings

Company name Unify Software and Solutions

Product name OpenScope SBC

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

Logo picture default Import Delete

An existing logo picture can be chosen from here, or a new logo picture can be imported using the Import button.

The Logo Picture is presented on Local Management for the login screen and title bar. The file must be a valid image (png, jpg, gif) and should use the recommended dimension (160x40) for proper display. Note: file size is recommended to be smaller than 5Kb. The Import button is used for uploading a new picture file, which becomes afterwards visible at the Logo Picture combo box.

The Delete button is used for deleting the selected picture file.

The option "default" is used to select the original logo picture.

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 the clear of browsing history may be needed.

Trademark License Agreement can be entered here. This name can be made up of upper or lower case letters, digits, or special characters. Special characters can be any of the following set: !@#%&()_+{}|:;'/=,^\$.*[]™©äÄüÜöÖ€µß and the white space.

TLA is visible on the login screen and by clicking on the Trademark & License link, which can be found at the bottom left corner of the help screen.

Product name can be entered here. This name can be made up of upper or lower case letters, digits, or special characters. Special characters can be any of the following set: !@#%&()_+{}|:;'/=,^\$.*[]™©äÄüÜöÖ€µß and the white space.

3.4.3 Network / Net Services

3.4.3.1 Physical Network Interfaces

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	1000	Full
eth3	<input type="checkbox"/>	1500	Auto	Auto
eth4	<input type="checkbox"/>	1500	Auto	Auto
eth5	<input type="checkbox"/>	1500	Auto	Auto

☐ Single armed

☐ Interface bonding

If the "speed" is set to Auto, the "duplex mode" must be Auto.
If the "speed" is set to 1000, then the "duplex mode" is disabled the speed option is shown as "Full".

In Single armed configuration, the SBC's LAN and WAN interfaces are connected to the same IP subnet instead of being connected between two different IP networks or subnets. It is also desirable for both the LAN and WAN connection of OS SBC to use a single physical Ethernet interface, rather than two. Refer to appendix Single Armed SBC.

3.4.3.2 Ethernet Bonding on LAN and/or WAN interfaces

Local GUI → Network / Net Services → Physical Network Interface → Interface bonding

☒ Interface bonding

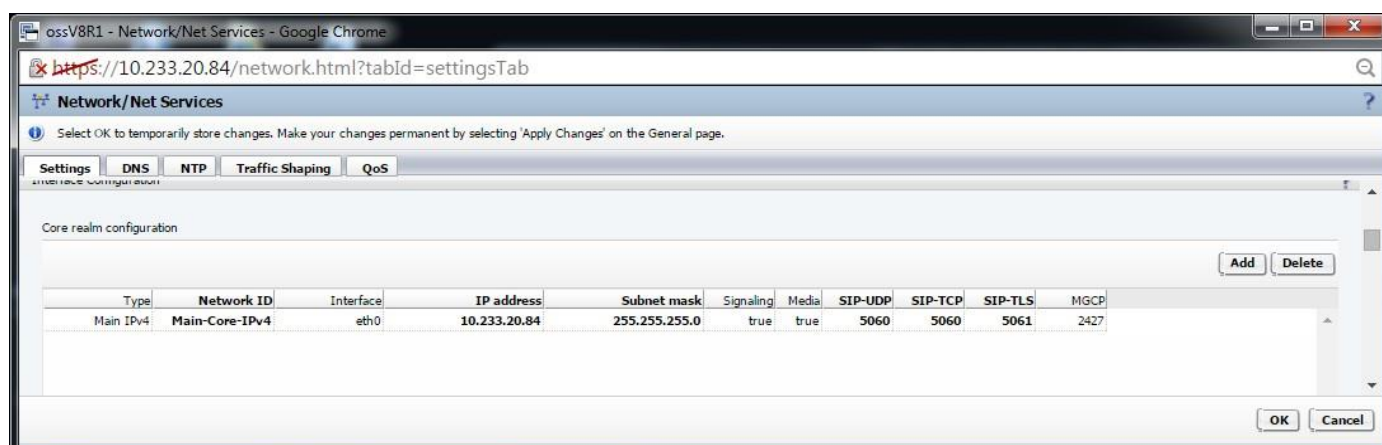
Bond interface	Enabled	Type	eth0	eth1	eth2	eth3
bond0	<input type="checkbox"/>	Redundancy	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
bond1	<input type="checkbox"/>	Redundancy	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>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

This allows the *available* Ethernet network interfaces to be bonded or teamed together to support network interface redundancy helping to prevent an SBC node Loss of Service in the event of a single EthernetNIC failure, local switching network failure.

This also has an effect on the selection of interfaces in the "access and Admin realm configuration" section, in that the interfaces (eth0, eth1....ethx) will be replaced with a selection of bond interfaces (bond0 ...bondx).

3.4.3.3 Core realm configuration

Multi-arm OS-SBC



Type – select from Main IPV4, Main IPV6 or Non VlanIP

Network ID – enter a name for the core realm

Interface – only eth0 is allowed

IP address – enter the IP address

Subnet mask – enter the Subnet Mask

Signaling - if signaling allowed on this interface

Media – if media is allowed on this interface

SIP-UDP – port used for UDP signaling

SIP-TCP – port used for TCP signaling

SIP-TLS – port used for TLS signaling

MGCP – port used for MGCP signaling

Single-Armed SBC – Refer to Appendix [Single-Armed-SBC](#)

3.4.3.4 Configuring separate management interface in an isolated subnet

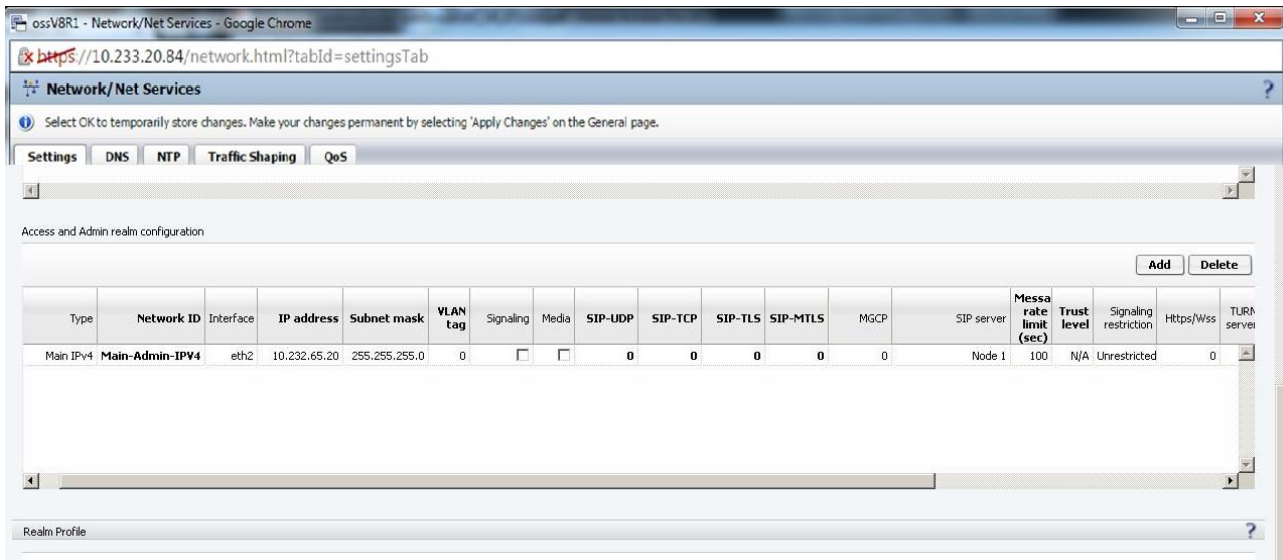
If a separate management interface is desired on the SBC and the physical hardware supports more than 2 interfaces, interface eth2 may be used. After connecting interface eth2 to the new management network, the SBC must be configured as follows to separate the management interface from the LAN interface. This can also be done with Virtual SBC(s) after adding an additional ethernet card to the Virtual Machine and mapping it to the new management subnet.

This feature should be configured using the LOCAL GUI of the SBC. The SBC cannot be administered via the SBC Assistant once a separate management interface is created and enabled on the SBC.

If Ethernet bonding/teaming is also being used, then eth4 should be used for the separate management interface. Five NICs must be configured and “adminNode1eth4” or “adminVirtualeth4” would be used in the Network ID field below.

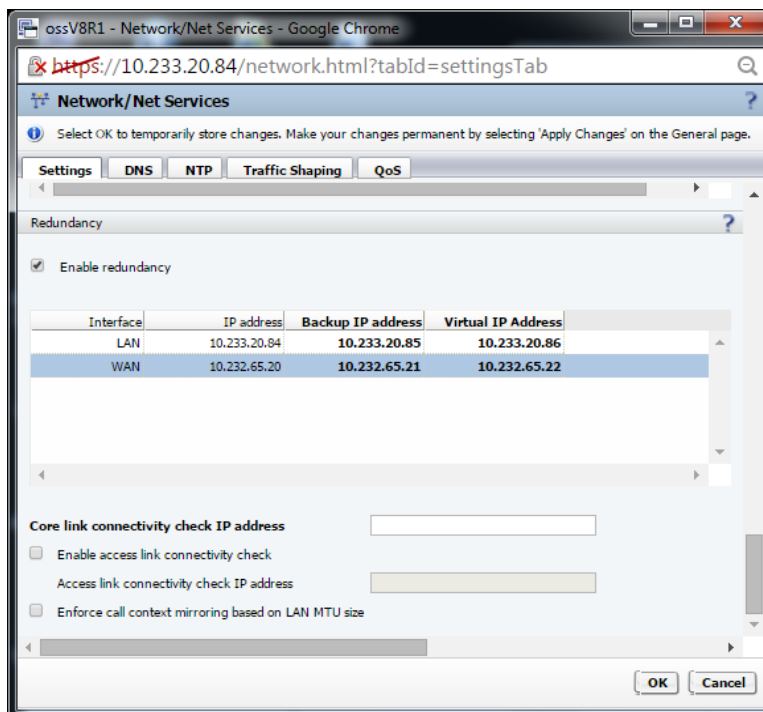
1. Use the capability in the “Access and Admin realm configuration” Network to configure the admin network interfaces.
2. Create a network ID with the type of “Main admin IPV4”

- a. The fields “SIP-UDP”, “SIP-TCP”, “SIP-TLS”, “SIP-MTLS” and “MGCP” must be 0.
- b. The fields “Signaling” and “Media” must be unchecked.



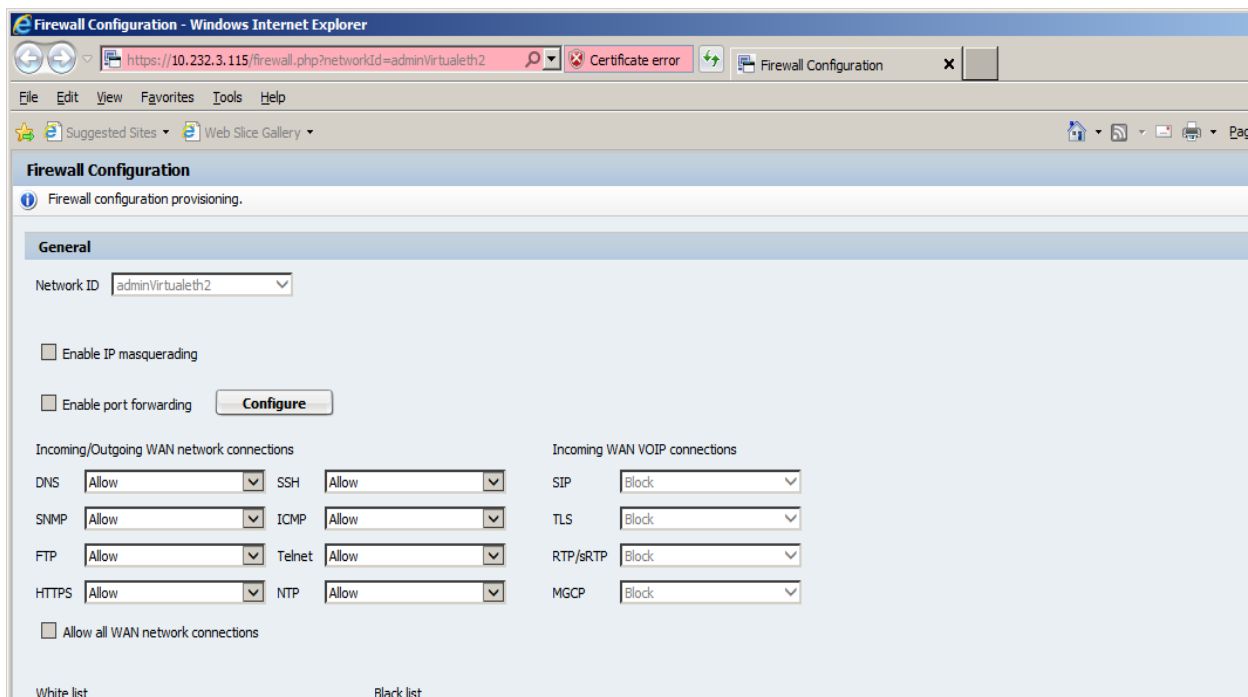
3. Speed, Duplex and MTU settings would be picked up from the eth1/Access interface.
4. If this is a redundant system click “OK”. The following error will be shown and is expected”
There are invalid field values: Enter a valid Backup IP address for Interface ADMIN in Redundancy list at row 3.

At this point scroll down and fill in the backup and VIP address for the second admin interface.



5. At this point, administrator must Apply Changes. SBC will reboot and new interface will be provisioned. In a redundant SBC pair, the backup node will also reboot a few minutes after the master node reboots.
6. In the security tab, administrator would then configure the firewall for this new NetworkID.
7. By default LAN interface has the admin services enabled.

8. By default everything is blocked on the new Admin interface and any necessary service must be manually enabled in the new Admin firewall. If NTP is “Allowed” on the new Admin interface, then the SBC pair will reboot when the changes are applied. If NTP is not allowed, then no reboot will occur. Close Internet browser and start a new browser session to the new Admin Interface.
9. All the VoIP related protocols are blocked on the new Admin firewall and cannot be enabled.



10. Once new Admin Firewall is configured then all unknown admin access on the LAN interface from outside is blocked.
11. If HTTPS access is not allowed on the new Admin firewall then it would be automatically enabled on the LAN interface in order to avoid no Admin access.
12. Since NTP or DNS servers could be residing on the LAN or Admin network, if the NTP or DNS services are enabled on the new Admin network then it is automatically blocked on the LAN network. Similarly, if the NTP or DNS services are disabled on the new Admin network then they are automatically enabled on the LAN network.
13. Internal processes would still continue to run on the LAN and WAN interfaces.
14. SSH/SFTP is used internally across the redundant pair communication over the LAN interface and hence firewall rules are restricted to allow communication from the known redundant pair IP.
15. ICMP would always be enabled on the LAN interface and allowing or blocking it from the new Admin interface has no effect on the functionality on the LAN interface.
16. Any outgoing admin traffic (e.g. Syslog and SNMP traps) would be sent out by the internal processes and as long as the destination is in the Admin subnet which is different than the LAN subnet, packets would go out over the Admin interface.

If SBC licenses are assigned from the SBC Assistant prior to feature being enabled, the SBC may still be able to refresh its license information from the SBC Assistant after the feature is enabled provided Assistant and Admin IP are in the same subnet. Standalone license file for the SBC is the recommended way to license this SBC with this feature.

NOTE:

1. Static routes could be created that will use the new Admin interface from the Net Services tab.

3.4.3.5 Access and Admin realm configuration

Access and Admin realm configuration

AddDelete

Type	Network ID	Interface	IP address	Subnet mask	VLAN tag	Signaling	Media	SIP-UDP	SIP-TCP	SIP-TLS	SIP-MTLS	MGCP	MSRP	SIP server	Messa rate limit (sec)	Trust level	Signaling restriction
Main IPv4	Main-Access-IPv4	eth1	193.0.0.139	255.255.255.0	0	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	5060	5060	5061	5161	2727		Node 1	100	N/A	Unrestricted

Type – select from Main IPV4, VLAN IP, Main IPV6 or Non VLANIP

When Single armed is set (enabled) the selectable values are:

- SA Main IPv4
- SA Main IPv6
- Non-VLAN IP
- VLAN IP

Forward Main - The IP address field is populated with the IP address of Main_IP and can't be changed. VLAN tag is set to 0, Signaling and Media checkboxes are unchecked and cannot be checked. A port must be set in at least one of the columns reserved to protocol.

Forward Non VLAN - The IP address field must be entered, VLAN tag is set to 0, Signaling and Media checkboxes are unchecked and cannot be checked. A port must be set in at least one of the columns reserved to protocol.

Forward VLAN - The IP address field must be entered, the VLAN tag must be entered with a value different to 0, Signaling and Media checkboxes are unchecked and cannot be checked. A port must be set in at least one of the columns reserved to protocol.

Network ID – enter a name for the corerealm

Interface – select from eth1, eth2 or eth3 IP address

Subnet mask

VLAN tag

Signaling - if signaling allowed on this

interface Media – if media is allowed on this

interface SIP-UDP – port used for UDP signaling

SIP-TCP – port used for TCP signaling

SIP-TLS – port used for TLS signaling

MGCP - port used for MGCP signaling

MSRP - The MSRP listening port. Recommended port is 2855.

SIP server - Comm. System Node. Default is Primary Comm System Node i.e. Node 1. In case of Active-Active Comm. System configuration, Node 2 could be selected to route the traffic received on this IP to Comm. System Node 2.

Message rate limit – select from drop down values

* Trust level – select from the pulldown *

Signaling restriction – restricts the type of endpoint allowed

* Trusted level is associated to the Denial of Service. The “Enable gateway message rate limit” feature is enabled on the Security → Denial of Service Mitigation tab.

Then if the feature is enabled, the message rate limit value selected is the number of messages per second received from the same source IP address. If the number of messages received exceeds this limit, then the source IP will be quarantined for the interval specified by the trust level assigned to the interface, i.e., the time to be released from quarantine depends on the configured value in trust level quarantine intervals.

The minimal is 60 seconds, the range is from 60 to 3600 seconds.

The medium is 10 seconds, the range is from 10 to 3600 seconds.

When the OS-SBC is in simplex mode the total number of VLANs possible is 1000. The total IPs possible is 1010, one IP per VLAN, and up to 10 IPs for the main Access interface (VLAN=0)

When the OS-SBC is in collocated mode the total number of VLANs possible is 2000. The total IPs possible is 2020, one IP per VLAN per node, and up to 20 IPs for the Access interface (VLAN=0)

Vlans are used in the case of VLAN tagged branches or networks. They are not used for SSPs unless traffic is tagged by the SSP.

Tag the main access interface requires the creation of a new realm with a VLAN type with IP 0.0.0.0 then an alias is created to eth1 and eth1 can be accessed tagged or not tagged. This allows accessing of access realm with and the without tag.

Access and Admin realm configuration

Type	Network ID	Interface	IP address	Subnet mask	VLAN tag	Signaling	Media	SIP-UDP	SIP-TCP	SIP-TLS	SIP-MTLS	MGCP	MSRP
Main IPv4	Main-Access-IPv4	eth1	173.16.57.10	255.255.0.0	0	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	5060	5060	5061	5161	2727	
VLAN IP	Main-Access-VLANIP	eth1	0.0.0.0	0.0.0.0	173	<input type="checkbox"/>	<input type="checkbox"/>	0	0	0	0	0	

Realm Profile

Realm profile	Realm	Signaling network ID	Media network ID	Forward network ID
Main-Core-Realm - ipv4	core	Main-Core-IPv4	Main-Core-IPv4	
Main-Access-Realm - ipv4	access	Main-Access-IPv4	Main-Access-IPv4	

Routing configuration

Row	Destination	Gateway	Netmask	Interface	VLAN tag
1	173.16.0.0	173.16.0.1	255.255.0.0	eth1	173

Note: There is a need for an additional entry in the routing Table for routing this traffic tagged with the VLAN ID.

For Access realms in a “Single-armed-SBC” refer to [Single-Armed-SBC](#).

SBC can support several VLANs to the same access Ethernet interface. Each VLAN will have its own IP address tagged with the specific VLAN ID.

For each created VLAN IP there is a need to add the routing table entry, so that SBC routes the traffic to the specific VLAN.

Additional details about the configuration are given in the following picture:

Configuration using Forward Main, Forward NON VLAN and Forward VLAN

Three new types of Network were created in the Network settings for Access side: Forward Main, Forwarded NON VLAN and Forward VLAN. The forwarded network types apply for UDP and TCP/TLS protocols too.

If the Type is set to forwarded Main then the IP address field is populated with the IP address of Main IP and cannot be changed, Vlan tag is set to 0 and signaling and Media checkbox are unchecked and cannot be checked. A port must be mandatory set in at least one of the columns reserved to protocol.

If the Type is set to forwarded NON VLAN then the IP address field must be entered, Vlan tag is set to 0 and signaling and Media checkbox are unchecked and cannot be checked. A port must be mandatory set in at least one of the columns reserved to protocol.

If the Type is set to forwarded VLAN then the IP address field must be entered, the Vlan tag must be entered with a value different from 0 and signaling and Media checkbox are unchecked and cannot be checked. A port must be mandatory set in at least one of the columns reserved to protocol.

The restriction of a maximal 10 IPs for Non VLAN must not be used to Forwarded network types, in this case the limit is the same as the maximal VLAN (1.000).

From now, the Ports configured in Access realm should not be in the range from 60000 to 62000. This range was reserved for internal system usage.

Additionally, for each Forward network, an entry in Realm Profile should be created (mandatory to associate the "Network ID" with new field "Forward Network ID" in Realm Profile)

Network/Net Services

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

Settings DNS NTP Traffic Shaping QoS

Access and Admin realm configuration

Type	Network ID	Interface	IP address	Subnet mask	VLAN tag	Signaling	Media	SIP-UDP	SIP-TCP	SIP-TLS	SIP-MTLS	NGCP	MSRP	SIP server	Message rate limit (sec)	Trust level	Signaling restriction	Https/Was
Main IPv4	Main-Access-IPv4	eth1	173.16.10.121	255.255.0.0	0	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	5060	5060	5061	5161	2727		Node 1	100	N/A	Unrestricted	0
Forward Main	fwmainits	eth1	173.16.10.121	255.255.0.0	0	<input type="checkbox"/>	<input type="checkbox"/>	0	0	50072	0	2727		Node 1	100	N/A	Unrestricted	0
Forward Main	fwmaintcp	eth1	173.16.10.121	255.255.0.0	0	<input type="checkbox"/>	<input type="checkbox"/>	0	50071	0	0	2727		Node 1	100	N/A	Unrestricted	0
Forward Non-VLAN	fwnonvlantcp	eth1	173.16.10.222	255.255.0.0	0	<input type="checkbox"/>	<input type="checkbox"/>	0	50061	0	0	2727		Node 1	100	N/A	Unrestricted	0
Forward Non-VLAN	fwnonvlanits	eth1	173.16.10.223	255.255.0.0	0	<input type="checkbox"/>	<input type="checkbox"/>	0	0	50062	0	2727		Node 1	100	N/A	Unrestricted	0
Forward Non-VLAN	fwnonvlanudp	eth1	173.16.10.221	255.255.0.0	0	<input type="checkbox"/>	<input type="checkbox"/>	50060	0	0	0	2727		Node 1	100	N/A	Unrestricted	0

Realm Profile

Realm profile	Realm	Signaling network ID	Media network ID	Forward network ID
Main-Core-Realm - ipv4	core	Main-Core-IPv4	Main-Core-IPv4	
Main-Access-Realm - ipv4	access	Main-Access-IPv4	Main-Access-IPv4	
fwnonvlanudp	access	Main-Access-IPv4	Main-Access-IPv4	fwnonvlanudp
fwnonvlantcp	access	Main-Access-IPv4	Main-Access-IPv4	fwnonvlantcp
fwnonvlanits	access	Main-Access-IPv4	Main-Access-IPv4	fwnonvlanits
fwmainudp	access	Main-Access-IPv4	Main-Access-IPv4	fwmainudp
fwmaintcp	access	Main-Access-IPv4	Main-Access-IPv4	fwmaintcp
fwmainits	access	Main-Access-IPv4	Main-Access-IPv4	fwmainits

Now, it is possible to configure the Forward Main, Forward Non-VLAN and Forward VLAN using the same IP address and different ports.

Then, it is also possible to configure the SSP using the same IP address or URL(fqdn) or SRV and different core realm ports. Associate the respective access realm profile in the remote endpoint configuration.

See the following example:

Network/Net Services

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

Settings DNS NTP Traffic Shaping QoS

Access and Admin realm configuration

Type	Network ID	Interface	IP address	Subnet mask	VLAN tag	Signaling	Media	SIP-UDP	SIP-TCP	SIP-TLS	SIP-MTLS	MGCP	MSRP	SIP server	Message rate limit (sec)	Trust level	Signaling restriction	Https/Was
Forward Non-VLAN	fwnonvlanp1	eth1	173.16.10.224	255.255.0.0	0	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	50080	0	0	0	2727		Node 1	100	N/A	Unrestricted	0
Forward Non-VLAN	fwnonvlanp2	eth1	173.16.10.224	255.255.0.0	0	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	50081	0	0	0	2727		Node 1	100	N/A	Unrestricted	0
Forward Non-VLAN	fwnonvlanp3	eth1	173.16.10.225	255.255.0.0	0	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	50082	0	0	0	2727		Node 1	100	N/A	Unrestricted	0
Forward Non-VLAN	fwnonvlanp4	eth1	173.16.10.225	255.255.0.0	0	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	50083	0	0	0	2727		Node 1	100	N/A	Unrestricted	0
Forward Non-VLAN	fwnonvlanp5	eth1	173.16.10.226	255.255.0.0	0	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	50084	0	0	0	2727		Node 1	100	N/A	Unrestricted	0
Forward Non-VLAN	fwnonvlanp6	eth1	173.16.10.226	255.255.0.0	0	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	50085	0	0	0	2727		Node 1	100	N/A	Unrestricted	0

Realm Profile

Realm profile	Realm	Signaling network ID	Media network ID	Forward network ID
fwnonvlanp1	access	Main-Access-IPv4	Main-Access-IPv4	fwnonvlanp1
fwnonvlanp2	access	Main-Access-IPv4	Main-Access-IPv4	fwnonvlanp2
fwnonvlanp3	access	Main-Access-IPv4	Main-Access-IPv4	fwnonvlanp3
fwnonvlanp4	access	Main-Access-IPv4	Main-Access-IPv4	fwnonvlanp4
fwnonvlanp5	access	Main-Access-IPv4	Main-Access-IPv4	fwnonvlanp5
fwnonvlanp6	access	Main-Access-IPv4	Main-Access-IPv4	fwnonvlanp6

Remote Endpoints

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

Remote endpoint configuration

Row	Name	Access realm profile	Type	Profile / Circuit ID	Remote IP address / Logical Endpoint ID / Circuit URL	Remote port	Remote transport	Associated Endpoint	Linked Endpoint	Core realm profile	Core PQDN	Core realm port	Routing prefix
22	SSP_ONE	fwnonvlanp1	SSP	ssp	173.16.105.140	5060	UDP			Main-Core-Realm - ipv4		50718	477718%
23	SSP_TWO	fwnonvlanp2	SSP	ssp	173.16.105.140	5060	UDP			Main-Core-Realm - ipv4		50719	477719%
24	SSP_THREE	fwnonvlanp3	SSP	ssp	sgnnonlan741.sbc2.com.br	5060	UDP			Main-Core-Realm - ipv4		50726	477726%
25	SSP_FOUR	fwnonvlanp4	SSP	ssp	sgnnonlan741.sbc2.com.br	5060	UDP			Main-Core-Realm - ipv4		50727	477727%
26	SSP_FIVE	fwnonvlanp5	SSP	ssp	abc2.com.br	0	UDP			Main-Core-Realm - ipv4		50724	477724%
27	SSP_SIX	fwnonvlanp6	SSP	ssp	abc2.com.br	0	UDP			Main-Core-Realm - ipv4		50725	477725%
28	SSP_SIX	Main-Access-Realm - ipv4	SSP	Register	173.16.105.143	5060	TCP			Main-Core-Realm - ipv4		50739	477500%
29	SSP_SIX	Main-Access-Realm - ipv4	SSP	Register	173.16.105.143	5060	TCP			Main-Core-Realm - ipv4		50740	477501%
30	SSP_SEVEN	fwnonvlanp7	SSP	ssp	173.16.105.140	5060	UDP			Main-Core-Realm - ipv4		50741	477741%
31	SSP_EIGHT	fwnonvlanp8	SSP	ssp	173.16.105.140	5060	UDP			Main-Core-Realm - ipv4		50742	477742%
32	SSP_EIGHT	fwnonvlanp8	SSP	ssp	abc3.com.br	0	TLS			Main-Core-Realm - ipv4		54163	477603%

NOTICE: When creating a Realm Profile: if a forward non-vlan Network is to be used (even if different network interfaces are used) such network must be configured only as the "Forward network id" and the Signaling network ID must be "Main Access network ID"

Network/Net Services

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

Settings DNS NTP Traffic Shaping QoS

Access and Admin realm configuration

Type	Network ID	Interface	IP address	Subnet mask	VLAN tag	Signaling	Media	SIP-UDP	SIP-TCP	SIP-TLS	SIP-MTLS	MGCP	MSRP	SIP server	Message rate limit (sec)	Trust level	Signaling restriction	Https/Was
Main IPv4	Main-Access-IPv4	eth1	173.16.10.121	255.255.0.0	0	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	5060	5060	5161	5161	2727		Node 1	100	N/A	Unrestricted	0
Forward Main	fwmaintrp	eth1	173.16.10.121	255.255.0.0	0	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	0	50071	0	0	2727		Node 1	100	N/A	Unrestricted	0
Forward non-VLAN	fwnonvlanp	eth1	173.16.10.221	255.255.0.0	0	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	50060	0	0	0	2727		Node 1	100	N/A	Unrestricted	0
Forward non-VLAN	fwnonvlanp13	eth2	172.16.10.241	255.255.0.0	0	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	0	50299	0	0	2727		Node 1	100	N/A	Unrestricted	0
Forward non-VLAN	fwnonvlanp14	eth2	172.16.10.241	255.255.0.0	0	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	0	50300	0	0	2727		Node 1	100	N/A	Unrestricted	0

Realm Profile

Realm profile	Realm	Signaling network ID	Media network ID	Forward network ID
Main-Core-Realm - ipv4	core	Main-Core-IPv4	Main-Core-IPv4	
Main-Access-Realm - ipv4	access	Main-Access-IPv4	Main-Access-IPv4	
fwnonvlanp	access	Main-Access-IPv4	Main-Access-IPv4	fwnonvlanp
fwmaintrp	access	Main-Access-IPv4	Main-Access-IPv4	fwmaintrp
fwnonvlanp13	access	Main-Access-IPv4	Main-Access-IPv4	fwnonvlanp13
fwnonvlanp14	access	Main-Access-IPv4	Main-Access-IPv4	fwnonvlanp14

Flag Shared Domain

Due to ticket SBC-6436, the new flag Shared Domain was created in Folder Features/Remote Endpoints/Remote Location Domain. This is valid only to Remote Endpoint configured as SSP Type. When enabled this flag indicates that the configured FQDN uses shared domain. In other words, there are more SSPs configured with different FQDNs resolving the same address, and only the first part of FQDN (hostname) is different. The flag is only used for forward realms in order to identify shared domains and differ forward rules that use a same address.

All SSPs that share the same resolved address and use different FQDNs must have this flag enabled.

The image shows the 'Remote Endpoints' configuration page. At the top, there's a section for 'Remote endpoint configuration' with a table listing endpoints. Below this, there are two detailed views of the 'Remote Location Domain' settings for specific endpoints.

Row	Name	Registration protocol	Registration interval (sec)
1	ssp	SSP	3600

Row	Name	Access realm profile	Type	Profile / Config ID	Remote SP address / Logical-Endpoint-ID / Remote URL	Remote port	Remote transport	Associated Endpoint	Linked Endpoint	Core realm profile	Core FQDN	Core realm port	Routing profile	Default for
25	SSP_TWOVE	funcomfaria2	SSP	ssp	abcc.com.br	0	TLS			Main-Core-Realm - gwt		50759		
26	SSP_THRO	funcomfaria2	SSP	ssp	abcc.com.br	5061	TLS			Main-Core-Realm - gwt		50759	477228%	
27	SSP_THREE	funcomfaria2	SSP	ssp	sspronfari4.abcc.com.br	5061	TLS			Main-Core-Realm - gwt		50759	477228%	
28	SSP_FOUR	funcomfaria1	SSP	ssp	sspronfari5.abcc.com.br	5061	TLS			Main-Core-Realm - gwt		50759	477228%	
29	SSP_FIVE	funcomfaria5	SSP	ssp	sspronfari6.abcc.com.br	0	TLS			Main-Core-Realm - gwt		50759	477228%	

Remote Location Domain

General

Remote URL: ☒ Shared domain

Remote port:

Remote transport:

OK Cancel

Remote Location Domain

General

Remote URL: ☒ Shared domain

Remote port:

Remote transport:

OK Cancel

RESTRICTIONS:

- Different SIP Service Providers cannot be associated to the same Forward Network ID if the SIP Service Provider address is configured in more than one remote endpoint.
- Not available in Single Armed mode, using MTLS and IPV6 environment.
- The user must not configure different FQDNs that are resolving the same IP address for different SSP endpoints that are using this feature.

3.4.3.6 SIP listening ports for LAN and WAN Main IP Addresses

Type	Network ID	Interface	IP address	Subnet mask	Signaling	Media	SIP-UDP	SIP-TCP	SIP-TLS	MGCP
Main IPv4	Main-Core-IPV4	eth0	21.21.100.51	255.255.0.0	true	true	5060	5060	5161	2427

Type	Network ID	Interface	IP address	Subnet mask	VLAN tag	Signaling	Media	SIP-UDP	SIP-TCP	SIP-TLS	SIP-MTLS	MGCP	MSRP	SIP server	Message rate limit (sec)	Trust level	Signal restrict
Main IPv4	Main-Access-IPV4	eth1	173.16.100.51	255.255.0.0	0	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	5060	5060	5061	5161	2727		Node 1	100	N/A	Unre



To help prevent DoS (Denial of Service) attacks, it is **strongly recommended** that the network listening ports be set to something other than the defaults of 5060 and 5061. The port SIP MTLS for Access realm configuration in OS SBC is 5161. Configure this port in accordance to the access side necessity. Use any port range between 65000 to 65535, for example use

TCP : 65060

UDP: 65060

TLS : 65061

This will require devices which communicate with the OS-SBC to use these ports.

Possible devices affected by this setting include, but are not limited to:

- The OSV system which this OS-SBC connects to
- Remote end points which connect to the OS-SBC
- SIP phones which connect to this OS-SBC

For example to “harden” the WAN side of the OS-SBC for remote subscribers:

1. Change the “listening ports” on the OS-SBC (local GUI → Network services → settings → select each interface)
2. DO NOT change the port for the voice server (local GUI → VOIP-Sip Server Settings). This is the LAN side communications.
3. On the OSV, update the port associated with the OS-SBC endpoint
4. On the OSV, update the aliases for the new private port
5. On the remote user phone, update the port configuration for the new private port

In versions prior to OSV V9, OSV challenged OPTIONS requests coming from the SIP proxy endpoint (OSB, SBC). In that case, it was recommended to configure the SBC IP address + port as trusted in the OSV.

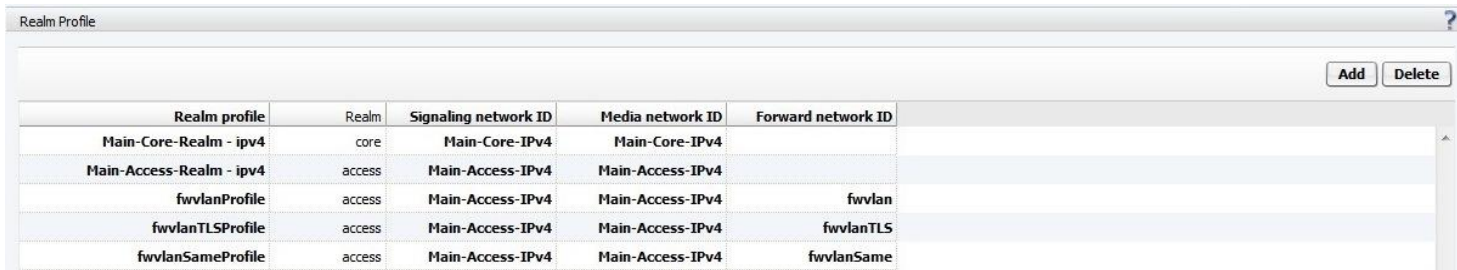
From OSV V9, OPTIONS requests will not be contested if the 'SIP Proxy' endpoint attribute is set and **there is a recommendation to configure SBC IP address + port as non-trusted in the OSV.**

This configuration is preferred in order to avoid having security issues regarding the registration of the remote users. The remote subscribers should be always challenged, even if they are configured as trusted in OSV.

Note: In the case of remote endpoints (OpenScape Branch, etc.) similar changes are required. The remote endpoints in the OS-SBC and the listening ports and voice server port in the OSB need to be updated with the new private port information. It is “highly recommended” to use TLS as the transport for all remote endpoints.

Note: If you are using a firewall remember to update it for the new private port.

3.4.3.7 Realm Profile



Realm profile	Realm	Signaling network ID	Media network ID	Forward network ID
Main-Core-Realm - ipv4	core	Main-Core-IPv4	Main-Core-IPv4	
Main-Access-Realm - ipv4	access	Main-Access-IPv4	Main-Access-IPv4	
fwvlanProfile	access	Main-Access-IPv4	Main-Access-IPv4	fwvlan
fwvlanTLSProfile	access	Main-Access-IPv4	Main-Access-IPv4	fwvlanTLS
fwvlanSameProfile	access	Main-Access-IPv4	Main-Access-IPv4	fwvlanSame

The realm profile merges the signaling and media realms into one entity which will be used when creating remote endpoints and the settings for remote subscribers.

Realm profiles associate signaling and media network interfaces with network realms to support multimedia sessions. Once a realm profile is defined, routing and identify objects may be configured to identify their realm association to support signaling and media flows between the OS-SBC access and core realm network interfaces.

The user may add a new realm profile, edit an existing realm profile in-line or delete a realm profile row entry. The user follows the same in-line edit options as used in other network services configuration sections.

Each realm profile section row has the following fields:

- **Realm Profile** - A unique identity to identify the realm profile. Network ID must be associated to a new realm profile that will be used in the remote endpoint configuration. Available options:

- *Main-Core-Realm-ipv4*
- *Main-Access-Realm-ipv4*
- *Second_Access*
- *Third_Access*

- **Realm** - Identifies the realm the realm profile is associated; either Access or Core may be selected, e.g., from a pull-down list.

- **Signaling Network-ID** - The user is presented a list of signaling capable Network-ID's for selection. Alternatively the user may be provided a list of Network-ID's filtered by the chosen association.

- **Media Network ID** - By default, selecting a signaling and media capable network interface in the Signaling Network-ID provisioning step shall automatically show the same Network-ID as a preferred selection for this field.

- **Forward Network ID** - Forward network ID ties a Realm profile to an existent Forward VLAN. It is mandatory to have an entry in Realm Profile for each configured Forward VLAN.

INFO: Before a realm profile deletion is allowed to proceed, a crosscheck SHALL be performed to ensure that there are no existing associations or relationships with routing or identify objects

3.4.3.8 Routing

ossV8R1 - Network/Net Services - Google Chrome

<https://10.233.20.84/network.html?tabId=settingsTab>

Network/Net Services

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

Settings DNS NTP Traffic Shaping QoS

Routing

Default gateway address: 10.233.20.1

Default gateway IPv6 address:

Routing configuration

Row	Destination	Gateway	Netmask	Interface	VLAN tag
-----	-------------	---------	---------	-----------	----------

Buttons: Add, Delete, OK, Cancel

This defines the IP address to be used as a default gateway for the OS-SBC. As a result of the "USBstick installation" the default will be set to the LAN. Users should fill in the default gateway address for the WAN.

A new route is added using the add button. In this case a new row in the routing table is created and is possible to configure the destination IP address, gateway IP address, network mask and choose which interface and Vlan Tag that will be used to route the IP packets. To delete a route select the route and then use the delete button. Once the routes are entered or deleted the save button will save the configuration and the window will close. To apply this configuration the user must click on "Apply Changes" button.

The default gateway should be changed to the WAN after the USB installation

Therefore enter a route for each subnet on the LAN (data-center). Then make the WAN the default gateway address.

NOTE: If it becomes necessary to add a route on the LAN manually from the CLI the following example is provided.

1 – SSH to the OS-SBC as root

2 - route add 192.168.59.1/32 dev eth0

3 - route add -net 192.168.59.0 gw 192.168.59.1 netmask 255.255.255.0

Here we are adding routing for the 192.168.59.0/24 network to the LAN interface

3.4.3.9 OS-SBC Redundancy

3.4.3.9.1 IP addresses required for various OS-SBC / OSV configurations



Note 1: The row labeled OSV refers to the mode of communicating with the OpenScape Voice, NOT the logical or architectural configuration of the OpenScape voice. (Local GUI → VOIP → Sip Server Settings → “Comm System Type”).



Note 2: It is recommended to only use this “Comm System Type” when traffic separation or load sharing, between two OSV nodes, is required.

SBC / OSV note 1:	Simplex	Collocated note 2:	Geo-Separated
Simplex	2 IP addresses; 1 LAN 1 WAN	3 IP addresses; 1 LAN 1 WAN + 1 under WAN Access side to be used for OS-SBC Access IP on VOIP tab	2 IP addresses; 1 LAN 1 WAN
Active-Active	6 IP addresses; 1 LAN for each OS-SBC + LAN VIP 1 WAN for each OS- SBC + 1 WAN VIPs (1 under redundancy, to be used for OS- SBC Access IP on VOIP tab)	7 IP addresses; 1 LAN for each OS- SBC + LAN VIP 1 WAN for each OS- SBC + 2 WAN VIPs (1 under redundancy, 1 under WAN Access side to be used for OS-SBC Access IP on VOIP tab)	7 IP addresses; 1 LAN for each OS- SBC + LAN VIP 1 WAN for each OS- SBC + 2 WAN VIPs (1 under redundancy, 1 under WAN Access side to be used for OS-SBC Access IP on VOIP tab)

Table 1 IP Address Calculations: The above assumes using “single core” address.

In an active-active scenario OSS needs a second IP on WAN interface to load balancing the requests towards OSV.

Depending on the IP where the message arrives it will go to node 1 or node 2 depending on the configuration.

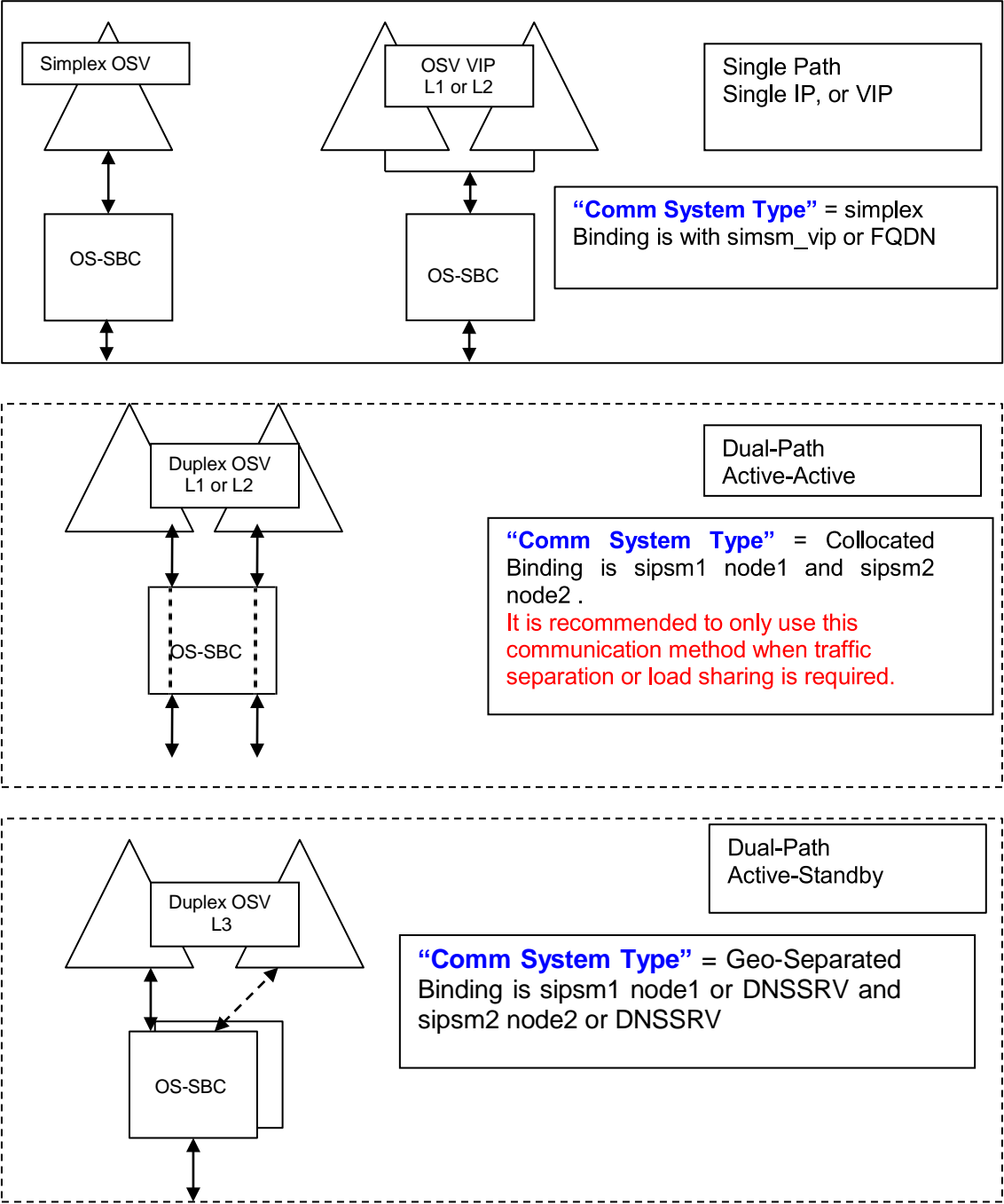
If Redundancy is used the second IP (and other additional ones) is “transferred” from the master to the new master when switchover occurs.

The redundancy connectivity checks on WAN is done by send arping to the configured IP.

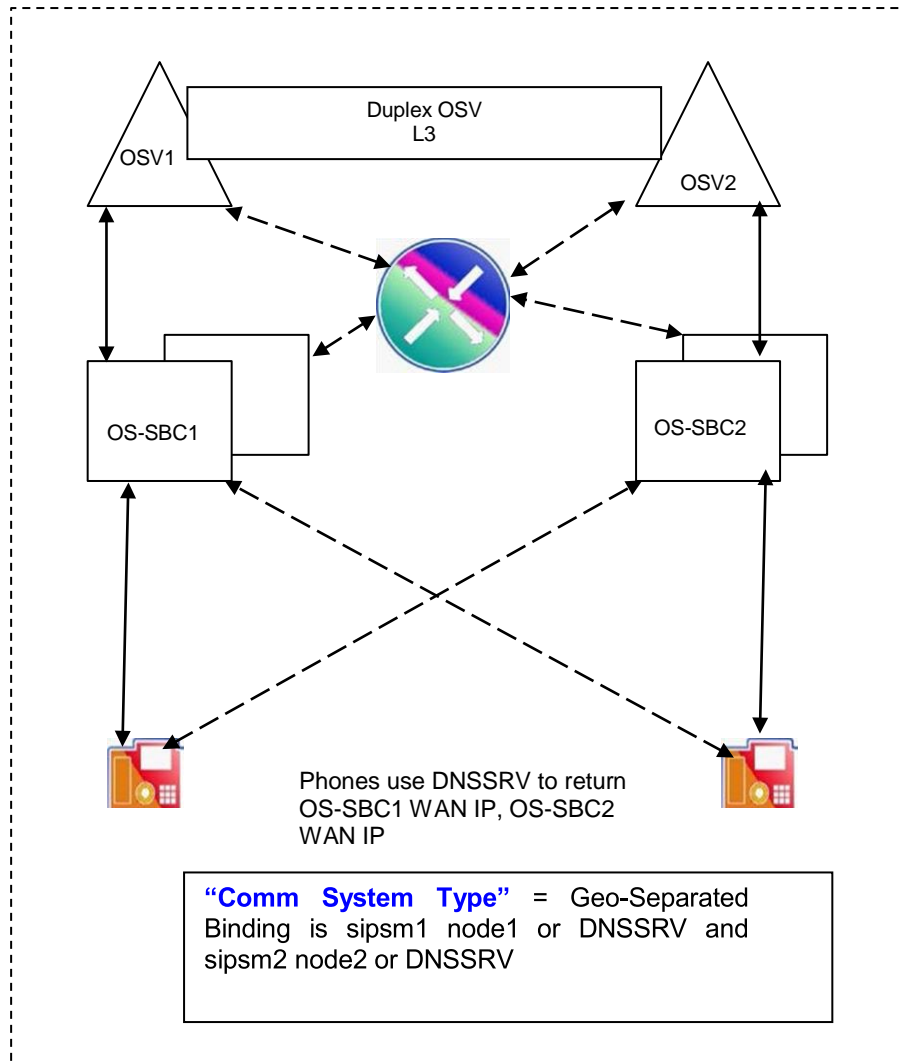
Is sent every 10s, and wait for 3s for a response. New arp ping is sent if the response is not arrived within 3s. After 3 consecutive failures the system will switchover.

The time to complete the switchover depends on the startup of sipserver in the new active node, reconnections of TCP and the response of OPTIONS by the main sipserver usually this process takes less than a minute.

3.4.3.9.2 Examples of connections to OSV



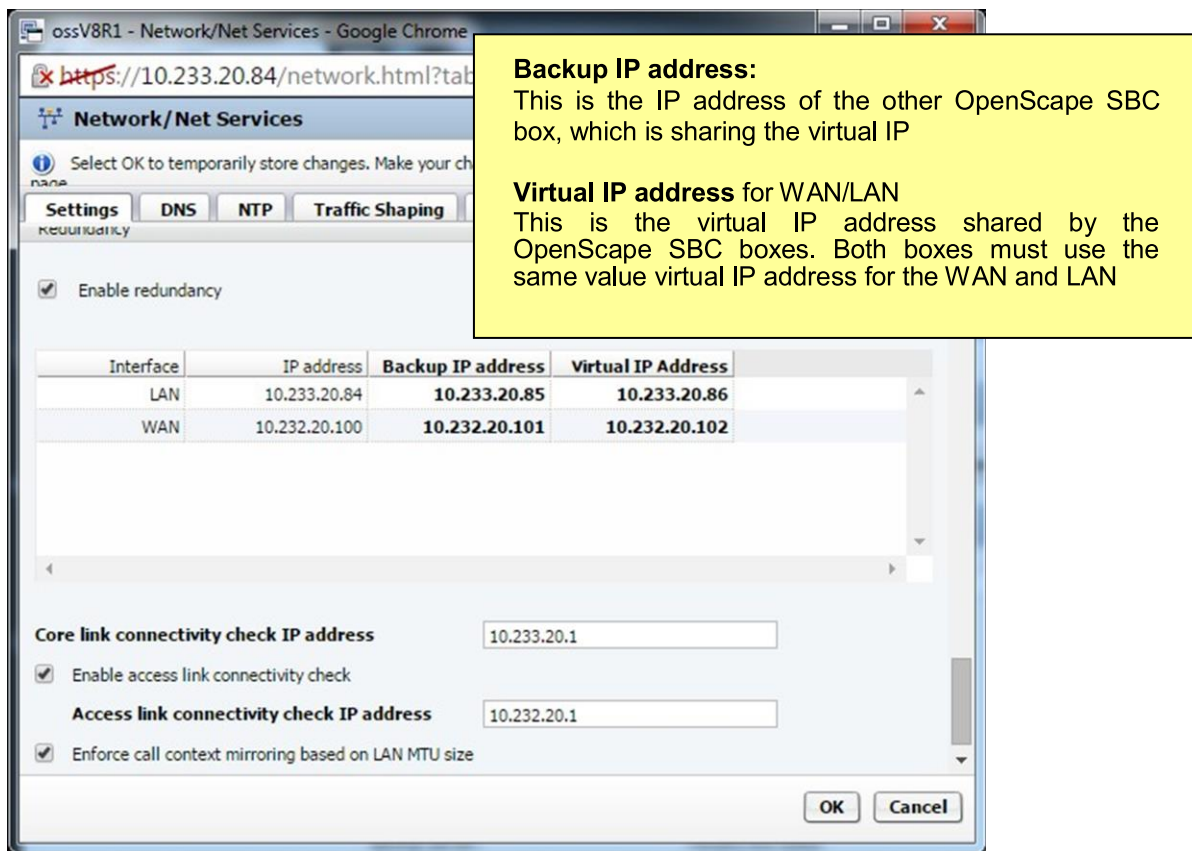
Example OSV Connections



Example OSV Connections

This is the model for the Geo-Separated OSV with fully redundant OS- SBCs. In this model the OS-SBC pairs are independent.

3.4.3.9.3 OS-SBC - Collocated Redundancy



Redundancy uses a non-proprietary protocol which is used to increase the availability of the OS-SBC. This is based on a virtual IP address in the same subnet of the OpenScapeSBC used for redundancy. The check box enables the Redundancy protocol.

Enabling/Disabling Redundancy:

In order for two nodes to be a redundant OS-SBC system, both nodes must have the same hardware configuration.

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.

Upgrading a redundant system:

The Local GUI/CMP shows the upgrade progress only while upgrading the Master node. The upgrade

P31003-S53A0-M101-30-76A9 76 OpenScape SBC V10 Configuration Guide

completion on the other node must be further verified by checking the software information(version).
The upgrade process is started in the master node and could take around 30 minutes to complete in both nodes.

Virtual IP address for WAN/LAN

This is the virtual IP address shared by the OpenScape SBC boxes. Both boxes must use the same value for the virtual WAN and LAN.

3.4.3.9.4 Access Link connectivity check (WAN redundancy)

Customer Responsibilities for WAN redundancy

The customer SHALL be responsible for providing a redundant network infrastructure which prevents the feature from detecting the same WAN failure condition in both OS-SBC redundant nodes. Insufficient redundancy for key network elements would not be improved by this feature and would continue to lead to OS-SBC network isolation.

The customer SHALL be responsible for providing unrestricted access to a WAN gateway which can support the ARP ping request.

The customer SHALL be responsible for providing an OS-SBC WAN IP address for each OS-SBC server node. This means 3 addresses are required, two additional IP addresses in addition to the VIP address.

3.4.3.10 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** **Traffic Shaping** **QoS**

Client

Refresh DNS

DNS server IP address **Add** Alias **Add**

Delete **Delete**

☐ Enable DNS server **DNS configuration**

☐ Enable customization **Administer custom files**

DNS server list - List of DNS server IP addresses to be used by this client (maximum of 3 DNS servers).

3.4.3.11 NTP

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 OpenScape SBC must be added to NTP Server firewall list

The screenshot shows the 'Network/Net Services' configuration window with the 'NTP' tab selected. The 'NTP Settings' section includes a 'Region' dropdown (set to 'Asia'), a 'Timezone' dropdown (set to '(GMT +07:00) Jakarta'), and three radio buttons: 'Enable local NTP server' (checked), 'Manual configuration', and 'Synchronize with NTP server'. Below these are fields for 'Date' (02.26.2019) and 'Time' (16:20), an 'Apply' button, and an 'NTP server' list containing '192.168.100.4' with 'Add' and 'Delete' buttons. A 'Synchronize now' button is also present.

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

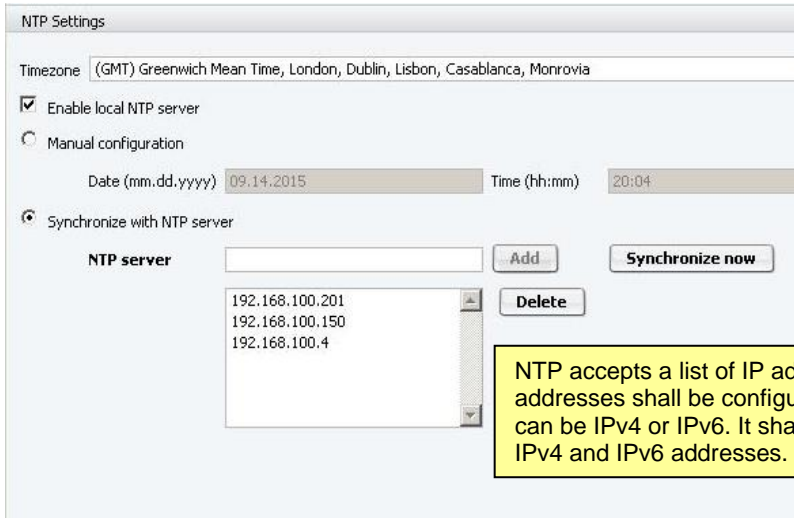
Drop list with the available **Regions** that relates to the **Timezones** in the selected region.

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.

3.4.3.11.1 Support_Multiple_NTP_Servers



NTP Settings

Timezone: (GMT) Greenwich Mean Time, London, Dublin, Lisbon, Casablanca, Monrovia

☒ Enable local NTP server

☐ Manual configuration

Date (mm.dd.yyyy): 09.14.2015 Time (hh:mm): 20:04 Apply

☒ Synchronize with NTP server

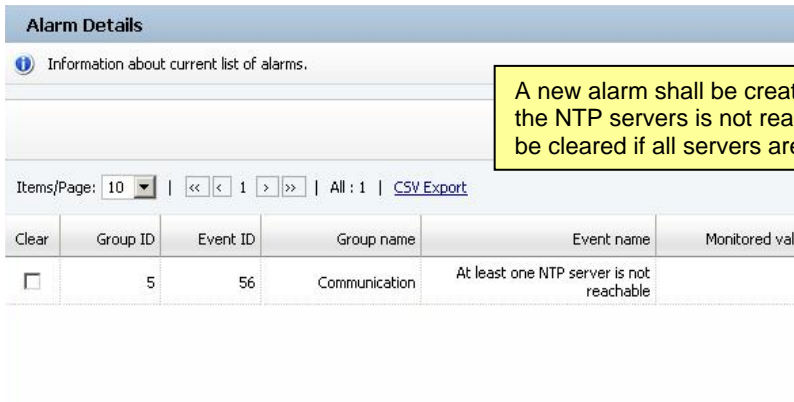
NTP server Add Synchronize now

192.168.100.201
 192.168.100.150
 192.168.100.4

Delete

By configuring more than one NTP server in the NTP client, it will select the most precise NTP server. If the selected NTP server gets unreachable it will adjust to the remaining NTP servers.

NTP accepts a list of IP addresses. Up to 3 IP addresses shall be configured. The IP addresses can be IPv4 or IPv6. It shall not be possible to mix IPv4 and IPv6 addresses.



Alarm Details

Information about current list of alarms.

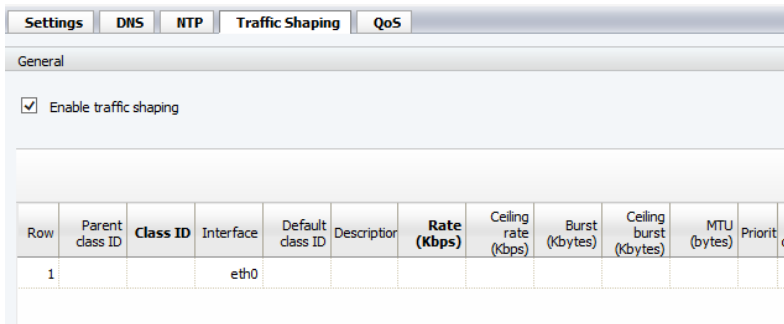
Clear all Clear

Items/Page: 10 | << < 1 > >> | All: 1 | [CSV Export](#)

Clear	Group ID	Event ID	Group name	Event name	Monitored value	Time (yyyy-mm-ddThh:mm:ss)	Threshold	Trigger
<input type="checkbox"/>	5	56	Communication	At least one NTP server is not reachable	1	2015-09-14T19:45:01+	0	Greater than

A new alarm shall be created to inform that one of the NTP servers is not reachable. The alarm shall be cleared if all servers are reachable again.

3.4.3.12 Traffic Shaping



Traffic Shaping

☒ 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 (bytes)	Priorit	Leaf queueing	SFQ quantum (bytes)	SFQ perturbation (sec)	Packet FIFO limit	Byte FIFO limit	Rule filters (separated by ;)	Mark filters (separated by ;)
1			eth0									none						

Here rules may be created which influence traffic thru the SBC. Refer to the online help.

3.4.3.13 QOS 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 Traffic Shaping QoS

QoS Settings

☐ Enable QoS

DSCP for SIP 26

DSCP for MGCP 26

DSCP for RTP (Audio) 46

DSCP for RTP (Video) 34

DSCP for SIP
DSCP value to be set in the IP packets of SIP protocol sent by OS SBC SIP Server.
DSCP for RTP
DSCP value to be set in the IP packets of RTP protocol sent by OS SBC Media services.

Add Delete

Row	Protocol	In interface	Out interface	Port	DSCP	Mark
-----	----------	--------------	---------------	------	------	------

A new line in QoS table is created using "Add" button, in this case a new QoS rule can be configured.

It can set the DSCP value for IP packets filtered according to the configured parameters and/or set the mark for traffic shaping. The QoS rule is deleted from table using "Delete" button.

Protocol - This box defines the protocol for the QoS rule. (all, TCP, UDP, ICMP)

In Interface - This box defines the incoming interface for the QoS rule. (eth0, eth1, eth2, eth3)

Out Interface - This box is used to configure the outgoing interface for the QoS rule. (eth0, eth1, eth2, eth3)

Port - This box defines the port or a port range (start_port:end_port) for the QoS rule (input or output).

DSCP - This box defines the DSCP value to be set in the IP packets for the QoS rule.

Mark - This box defines the mark for the QoS rule in order to use with traffic shaping.

Note: DSCP values of QoS configuration table rule can overwrite the values set by SIP and RTP protocols when conflicting rules are set.

See online help for more information of the DSCP field.

3.4.4 VOIP / SIP Server Settings

3.4.4.1 SIP Server Settings none clustered

The screenshot shows the 'VOIP' configuration page for 'SIP Server Settings'. It includes tabs for 'Sip Server Settings', 'Port and Signaling Settings', 'Media', and 'QoS Monitoring'. The 'General' section has a 'Comm System Type' dropdown set to 'Simplex' and a checked checkbox for 'Allow Register from SERVER'. Below this is a button for 'Other trusted servers'. The 'Node 1' section contains fields for 'Target type' (Binding), 'Primary server' (10.200.0.108), 'Backup server', and 'SRV record', each with a 'Transport' dropdown (all set to TCP) and a 'Port' field (5060 for Primary). The 'Node 2' section has similar fields but they are empty. The 'Timers and Thresholds' section at the bottom has four input fields: 'Failure threshold (pings)' (2), 'Success threshold (pings)' (1), 'Transition mode threshold (pings)' (1), 'OPTIONS interval (sec)' (300), 'OPTIONS timeout (sec)' (4), and 'Notification rate (per sec)' (100).

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 | Media | QoS Monitoring

General

Comm System Type: Simplex

☒ Allow Register from SERVER

Other trusted servers

Node 1

Target type: Binding

Primary server: 10.200.0.108 Transport: TCP Port: 5060

Backup server: Transport: TCP Port:

SRV record: Transport: TCP

Node 2

Target type: Binding

Primary server: Transport: TCP Port:

Backup server: Transport: TCP Port:

SRV record: Transport: TCP

Timers and Thresholds

Failure threshold (pings)	2	OPTIONS interval (sec)	300
Success threshold (pings)	1	OPTIONS timeout (sec)	4
Transition mode threshold (pings)	1	Notification rate (per sec)	100

The OpenScape Voice mode determines how OpenScape SBC is connected to the OpenScape Voice network

- Simplex : Supported
- Active-Active(formerly Collocated) : Supported
- Active-Standby : Supported

Allow Register from SERVER - Select the checkbox, if the remote endpoint is allowed registration via the server.

Bond TCP connections to SLB - Select this checkbox in order to reuse the TCP connections.

Other Trusted Servers - This configuration edits the list of trusted SIP Servers from which Requests can be accepted.

(Node 1/ Node 2)

- If the configuration is "Binding" then the SRV Record field will be grayed- out and the user has to enter in the Primary and Backup (depending on OpenScape Voice mode) the IP or FQDN, the Transport and the Port (the last fields are mandatory).
- If the configuration is "Service", a DNS SRV Record query will search the addresses automatically (SRV Record field) using the respective Transport (Transport field).
- Primary server is the preferred SIP server where the OpenScape SBC is connected to. In this box either sipsmx_vip or FQDN of the server is configured. The transport defines the SIP protocol used to communicate with server, port is the SIP port used.If TLS is selected the primary IP should be pointing to sipsm3_vip for Node1 and if applicable sipms4_vip for Node2 (which are the OSV's MTLS addresses, see below table).

Simplex is a single node configuration.

Active-Active (formerly Collocated) mode in SBC means Active-Active load balancing configuration of Comm System i.e. traffic coming in on Access IP 1 goes to Comm System node 1 and traffic on Access IP 2 goes to Comm System node 2.

INFO: When in Active-Active mode, additional Access IP configuration is a must for load balancing.

Active-Standby mode means that two nodes are in different locations.

INFO: If the configuration is set to Active-Active or Active-Standby, the Primary server field for Node 2 will be enabled.

OSV Mode	OSV V7R1 and V9R1	
	TCP/UDP/TLS	MTLS
Simplex		
Node 1	sipsm1_vip	sipsm3_vip
Collocated		
Node 1	sipsm1_vip	sipsm3_vip
Node 2	sipsm2_vip	sipsm4_vip
Geo-Separated		
Node 1 Primary server	sipsm1_vip	sipsm3_vip
Node 1 Secondary server	sipsm2_vip	sipsm4_vip
Node 2 Primary server	sipsm2_vip	sipsm4_vip
Node 2 Secondary server	sipsm1_vip	sipsm3_vip

3.4.4.2 VOIP / SIP server Settings Clustered

The screenshot shows a web browser window titled "BCF2 - VOIP - Google Chrome" with the address bar displaying "21.21.100.191/voip.html?tabId=sipTab". The page has a blue header with the "VOIP" logo and a warning icon. 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 content area is divided into tabs: "Sip Server Settings", "Port and Signaling Settings", "Error Codes", "Media", and "QoS Monitoring". The "Sip Server Settings" tab is active, showing a "General" section with a "Comm System Type" dropdown set to "Clustered". Below this are three checkboxes: "Allow Register from SERVER" (checked), "Use RURI to Route to Comm System" (unchecked), and "Bond TCP Connection to SLB" (unchecked). A "Clustered servers" button is also present. The "Clustered Nodes settings" section is expanded, showing "Ping Method" set to "OPTIONS", "OPTIONS interval (sec)" set to "300", "Failure threshold (pings)" set to "10", and "No Destination Error Code" set to "403 Forbidden". A dropdown menu for "No Destination Error Code" is open, showing options: "403 Forbidden", "403 Forbidden", "480 Temporarily Unavailable", and "503 Service Unavailable". The bottom of the page has "OK" and "Cancel" buttons.

Allow Register from SERVER- Select the checkbox, if the remote endpoint is allowed registration via the server.

Use RURI to Route to Comm System - Select this checkbox to route the calls to the Communication System server nodes based on RURI.

Note that, when this flag is set, the SIP messages containing a RURI with FQDN will be only routed to the Communication System if the FQDN matches the clustered servers FQDN.

Bond TCP connections to SLB - Select this checkbox in order to reuse the TCP connections.

In the **Clustered Nodes settings** area, configure the following parameters:

- **Failure threshold (pings)**

This is the number of failure attempts that SBC will count until consider a node failure.

- This defines the number of positive responses to wait until consider a node active again.


- This is the number of failure attempts during Transition Mode that SBC will count until switch to Survivable Mode.


- This box defines the time interval to send OPTIONS to the server.

- This box defines the timeout when waiting for 200OK from SIP server.

- This is the number of notifications per second sent to phones after state transition.

- Select which error response will be sent in case no destination is available when in Clustered Server mode.
Available values are:

- 
clustered Servers


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

Add

Delete

Group ID	Group name	Node Name	Priority	Routing prefix	IP address or FQDN	Port	Transport	No Answer timer (msec)	No Reply timer (msec)
1						5060	TCP	360000	3000
1						5060	TCP	360000	3000
1						5060	TCP	360000	3000
1						5060	TCP	360000	3000

- P31003-S53A0-M101-30-76A9

3.4.4.2.1 VOIP / Error codes Clustered

VOIP

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

Sip Server SettingsPort and Signaling SettingsError CodesMediaQoS Monitoring

Error Code Settings

Error codes for Clustered Servers

☒ Enable routing for all codes

☐ Disable routing for all codes

Items/Page: 10 | << < 1 > >> | All : 31 | [CSV Export](#)

Error code	Description	Enable routing in Normal Mode
300	Multiple Choices	<input checked="" type="checkbox"/>
301	Moved Permanently	<input checked="" type="checkbox"/>
302	Moved Temporarily	<input checked="" type="checkbox"/>
305	Use Proxy	<input checked="" type="checkbox"/>
380	Alternative Service	<input checked="" type="checkbox"/>
402	Payment Required	<input checked="" type="checkbox"/>
403	Forbidden	<input checked="" type="checkbox"/>
404	Not Found	<input checked="" type="checkbox"/>
405	Method Not Allowed	<input checked="" type="checkbox"/>
406	Not Acceptable	<input checked="" type="checkbox"/>

If SBS is in Cluster mode, then you have the option to choose error codes that would trigger a rerouting. You could either set error codes individually or set them all at once by checking the "Enable routing for all codes". You could also disable all by checking the flag "Disable routing for all codes"

3.4.4.3 Timers and thresholds

Timers and Thresholds

Failure threshold (pings)

2

OPTIONS interval (sec)

60

Success threshold (pings)

1

OPTIONS timeout (sec)

4

Transition mode threshold (pings)

1

Notification rate (per sec)

100

3.4.4.4 Port and Signaling 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** | Media | QoS Monitoring

Port Range

Media independent RTP ports

Port min: 10000 Port max: 49999

☐ Enable Media Specific Ports

Audio Port min: 10000 Audio Port max: 37499

Video Port min: 37500 Video Port max: 49999

Subscribers dynamic SIP ports

Port min: 10000 Port max: 49999

Remote Endpoints Static SIP Ports

Port min: 50000 Port max: 54999

TCP/BFCP ports

Port min: 10000 Port max: 14999

Number of reserved SIP ports: 100

Signaling and Transport Settings

TCP connect timeout (sec): 3

TCP connection lifetime (sec): 3

BFCP connection timer (min): 720

☐ Maximal call session time (hr): 12

Miscellaneous

☐ SIP SSL single context

Annotations:

- This section allows allocation of a range of ports the OSS will use for audio and video calls.
- Number of ports to be reserved for remote endpoints to avoid restart of sipserver in case of adding or removing an endpoint.
- Used for control of remote video devices
- Used for dropping the sessions after time.

Since V9R2, the Core realm port value configured in Folder Features/Remote Endpoints Configuration/ Remote Location Identification/Routing is verified against the remote endpoint valid range configured in Folder VOIP/Port and Signaling Settings/Remote Endpoints Static SIP Ports.

In this case, the warning message is shown. There is the option to change the range in VOIP/Port and Signaling Settings from 10000 to 65000. For Single Armed operation, the ranges will be

configured separately for Core and Access. The range for core side is from 10.000 to 19.999 and for access side is from 20.000 to 49.999.

The validation will be enforced anytime a new configuration is applied, so if the core ports configured for remote endpoints are out of range they must be changed, also the remote endpoint port configuration in OSV must match the new core port configuration.

If the flag Enable Media Specific ports is enabled, then Audio and Video port ranges can be changed as well. Default for audio at core side is from 10.000 to 23.749 and for audio at access side is from 23.750 to 37.499. For video, the default for core side is from 37.500 to 43749 and for access side is from 43.750 to 49.999.

Miscellaneous

- **SIP SSL single context**

It is used to share the same SSL context among the SIP Server child processes in order to save SIP Server shared memory.

If the flag is disabled, there is an increase in memory usage by the SIP server compared to if it is enabled. It may increase up to 1% of total system memory usage.

If the system has memory enough for multiple TLS processing or has multiple local addresses pointing to the same remote address using TLS protocol, it is recommended to disable it.

The default value is disabled.

3.4.4.5 Media

The screenshot shows the VOIP configuration interface. The 'Media Handling' section has the following options:

- ☐ 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

The 'Core Side Media Configuration' section has a 'Media profile' dropdown menu set to 'default'.

The 'Media Profiles' section contains a table with the following data:

Name	Codecs	Media protocol	SRTP crypto context negotiation	Mark SRTP Call-leg as Secure
default		Best Effort SRTP	sdes	✓
webrtc_default		SRTP only	dtls	✓
WE_Phone_default		Best Effort SRTP	mikey + sdes	

Buttons for 'Add', 'Edit', 'Delete', 'OK', and 'Cancel' are visible.

When a call originates from a device with a listed user agent the associated media profile is used to build the SDP, regardless of the original SDP from the device. A match is performed on the characters in the user agent list.

For example, "open" would match openstage and openscape. If no match is found, the SDP is not modified.

- **Replace the SDP Origin (o) field:** enable the replacement of SDP Origin (o) field with the SBC addresses and username OSSBC.
- **Reset SRTP context upon key change:** when enabled, the SRTP context (for Mikey and SDES) will be recreated upon a cryptographic key change. Otherwise, the SRTP context will be just updated with the new key. The configuration is enabled by default to avoid breaking flows with already supported SSPs.

IMPORTANT: According to the RFCs, the context must not be recreated if only the key has changed. Despite being enabled by default, the flag implies a non-RFC behavior.

- **Use single bridge/port for audio media:** when enabled, a single bridge will be used for audio m-lines. The consequence is that all audio m-lines will use a single port. The configuration is disabled by default.

IMPORTANT: The single bridge usage gives the possibility to maintain the same SRTP context even after changing the media negotiation with the other peer. For example, if peer A has an active SRTP context with SBC and on a reINVITE peer B changes from a secure m-line to a non-secure, the formerly used bridge will be replaced by a new one, losing/recreating the SRTP context with peer A. This can eventually affect the speech between peers.

After selecting the codecs in Features Enable Codecs Support for transcoding, add the codecs in desired media profile and define the priority.

A list of codecs may be associated with a media profile here. The list of codecs allowed are configured at GUI → features → Enable codec support for transcoding → configure.

For remote subscribers assign the media profile at: GUI → features → Remote Subscriber configuration → remote subscriber configuration → add / edit → media profile.

For remote endpoints assign the media profile at: GUI → features → Remote Endpoints configuration → add/edit → Remote Location domain list → media profile

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

RTP only

☐ Direct Media Support

☐ Support ICE

☐ Support NGTC Trickle ICE

☐ Enable NGTC WebRTC Compatibility

☐ Enable TURN Client

☒ RTP/ RTCP Multiplex in offer

☐ SDP Compatibility Mode

☐ Support Mid Attribute

☐ Do not set port to zero on session

Media Protocol: drop-down selection list

– **Strict Pass-Thru** - Incoming SDP received from the originating side would be sent out as is with the exception of doing the NAT on the IP addresses and Port i.e. number of m lines remains the same.

– **Best Effort SRTP** - Incoming SDP would be converted to the Best Effort SRTP SDP based on the SRTP configuration.

– **SRTP only** - Incoming SDP would be converted to the SRTP only SDP based on the SRTP configuration.

– **RTP only** - Incoming SDP would be converted to the RTP only SDP

Direct Media Support: Direct Media Support can be enabled when using DTLS as a SRTP crypto negotiation and when Suppress ICE Candidates is unset. Once direct media is enabled, it will be possible to choose a SBC ICE priority and DTLS cannot be disabled.

Support ICE: Adds ICE support to outgoing SDP. If the remote peer does not support ICE it can ignore the ICE attributes and the call will be completed in the traditional way.

INFO: Only IPv4 ICE candidates are supported.

Support NGTC Trickle ICE: Adds NGTC Trickle ICE support to outgoing SDP.

Enable NGTC WebRTC Compatibility: This flag changes the SDP for NGTC WebRTC compatibility.

Enable TURN Client: Enable the addition of system ICE candidates of type reflexive or relayed in a message to the GTC endpoint associated to the media profile. The STUN/TURN servers are provided by the GTC endpoint during the SIP negotiation. And an additional candidate will only be included in a message to GTC endpoint if it is different from a host address.

RTP/RTCP Multiplex in offer: Adds rtp-mux support to outgoing SDP. If the remote peer does not support rtp-mux it can ignore the attribute and the call will be completed in the traditional way.

SDP Compatibility Mode: Some SIP Service Providers do not accept certain codecs or unknown attributes in the SDP. Use this flag to remove extra fields from the SDP. If this flag is enabled, the codec list of the respective Media Profile cannot be empty and the Allow unconfigured codecs flag must be disabled. The flag is disabled by default.

Support Mid Attribute: This flag sets the attribute "mid" in the media lines of SDP. When enabled, the same mid attributes received in the SDP offer will be included in the SDP answer.

INFO: If the flag **Support Mid Attribute** is disabled, the attribute "mid" is removed from the SDP towards the endpoint/subscribe associated to the respective media profile.

For media profiles associated to remote endpoints of type GTC, the flag is required to be enabled.

The Real-time Transport Protocol comprises two components, a data transfer protocol and an associated control protocol (RTCP). RTP and RTCP have been run on separate UDP ports. With the introduction of the **RTP/RTCP multiplex in offer** flag, they will now run on a single port.

During the SDP negotiation phase, if the endpoint doesn't support Multiplex a fallback to dual port is still possible however this is only possible if the media is anchored in SBC. In case of direct media this is not possible.

If endpoints have different RTCP mux capabilities then the media optimization will have precedence over the RTCP mux. If media optimization is allowed between endpoints there is no guarantee that the RTCP mux will be offered/accepted, because the SDPs will be passed transparent from one endpoint to another. If the user wants to force RTCP mux over media optimization then the media profile/media realm group should have the force anchor media for the subnets of the corresponding endpoints.

To select the packetization interval, uncheck the flag **Allow unconfigured codecs**.

SBC-DAN - Media Profile - Google Chrome

Not secure | 21.21.100.198/mediaProfileConfiguration.html?name=default&coreSideMedia=default

Media Profile

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

General

Name default

Media protocol

- ☐ Support ICE
- ☐ Enable TURN Client
- ☒ RTP/ RTCP Multiplex in offer
- ☐ SDP Compatibility Mode
- ☐ Support Mid Attribute
- ☐ Do not set port to zero on session timer answer SDP

Media protocol dropdown:

- Best Effort SRTP
- Strict Pass-Thru
- Best Effort SRTP
- Single m-line Best Effort SRTP**
- SRTP only
- RTP only

SRTP configuration

SRTP crypto context negotiation ☒ MIKEY ☒ SDES

☐ Mark SRTP Call-leg as Secure

RTCP configuration

rtcpMode 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
- ☐ Enforce Packetization Interval

Codec Add

Priority	Codec
4	

Single m-line SRTP - This flag shows whether the SDP offer will have a single m-line SRTP, based on the media profile configuration.

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.

Mark sRTP Call-leg as Secure - if a secure media is negotiated, the call will be indicated as secure (ST-.....-Call-Type: secure).

Note: this flag will add a X-.....- call type header with an indication of ST-secure to INVITE and ANSWER messages **exiting** this interface.

Refer to the current release notes for support of this flag.

SRTP Configuration

IMPORTANT: When the selected SBC 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.

Codec Configuration

Allow unconfigured codecs: Enabled by default. When enabled, codecs received in the SDP Offer that are not configured in the profile are presented to the called Party in addition to the configured codecs.

Enforce codec priority in profile: The codec order in the media profile is enforced with this option regardless of the codec preference in the SDP offer.

Send Telephony Event in Invite without SDP: When this profile is used by SIP Service Provider configured with Do not send Invite without SDP flag, enabling this checkbox allows sending the INVITE with RFC2833 telephone-event indication in the SDP built by the OSSBC.

Use payload type 101 for telephony event/8000:

Disabled by default. This flag allows SBC to convert the payload type for telephone-event rate 8000 to 101 in the SDP offer and restore the original payload type when sending the SDP answer. Some SIP Service Providers send the payload type 101 for the telephone-event/8000 in the SDP, even if another payload type was used in the SDP offer to negotiate the telephone-event payload type. As a result, the DTMF tones between the parties may not be recognized. This flag should be enabled in the Media Profile of the destination endpoint. This Media profile's codec list CANNOT be empty.

This flag should be used to prevent conflicts in the SDP m-line if the codecs iLBC (PT 97), iSAC (PT 103) or OPUS (PT 96) are present in the codec list and there is a telephone-event using a conflicting payload type (PT) in the same SDP m-line.

Enforce packetization interval: Disabled by default. It is necessary at least one codec configured to enable this feature. When this flag is enabled, all codecs must have the same "Packetization interval" and it can not be set as Auto. As 'Allow unconfigured codecs' requires that 'Packetization Interval' be set to Auto, the two features can not be activated at the same time.

Codec: The user shall be able to select a codec from a drop-down list and click **Add** to add it to the bottom of the list of codecs for this media profile. If a codec is already in the list of codecs for this media profile then it shall not appear in the drop-down list for adding codecs. The user shall also be able to select a codec from the list and Move up or Move down in terms of priority or Delete it. In these cases the priority numbering shall be updated.

Each codec has its own packetization interval that can be selected from a drop down list with the following available options: 10ms, 20ms, 30ms, 40ms, 50ms, 60ms, and pass-through (auto) with default value auto.

Up to 3 different packetization interval values are allowed per Media Profile.

IMPORTANT: If the Allow unconfigured codecs checkbox is selected, then Packetization interval can only be auto for each and every codec. If it is not selected, then other options are allowed, as long as the codec is compatible with the assigned time value.

3.4.4.6 Core Side Media 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

Error Codes

Media

QoS Monitoring

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

Core Side Media Configuration

Media profile default

AddDelete

User agent

mediaProfile

Media Profiles

AddEditDelete

Name	Codecs	Media protocol	SRTP crypto context negotiation	Mark SRTP Call-leg as Secure
default	G722,G711A	RTP only	none	
webrtc_default		SRTP only	dtls	✓
WE_Phone_default		Best Effort SRTP	mikey + sdes	
Unify_Phone_default		SRTP only	dtls	

Cloud Support

☐ Support OpenScape Cloud

Media Realm Groups

☐ Distributed Media Realm Group

After full installation, there are four Media Profile configured:

- default, with media protocol as Best Effort SRTP, key exchange method as mikey+sdes.
- Webrtc_default. This is the media profile used in Circuit.
- WE_Phone_default. This is the media profile with direct media enabled.
- Unify_Phone_default. This media profile is recommended for NGTC (Next Generation Telephony Connector).

The available Media Protocol values are:

Strict Pass-Thru - Incoming SDP received from the originating side would be sent out as is with the exception of doing the NAT on the IP addresses and Port, i.e., number of m lines remains the same.

Best Effort SRTP - Incoming SDP would be converted to the Best Effort SRTP SDP based on the SRTP configuration.

mikey - Multimedia Internet KEYing

sdes - Session Descriptions Protocol Security Descriptions

dtls - Datagram Transport Layer Security

- SRTP only - Incoming SDP would be converted to the SRTP only SDP based on the SRTP configuration.
- RTP only - Incoming SDP would be converted to the RTP only SDP

IMPORTANT: If users have their speech path optimized they will face problems regarding REINVITES (hold/retrieve, consult, etc) if the flag "**Do not send invite in SDP**" is enabled on OSVoice. In order to avoid this issue, either the media must be anchored or the OSV flag must be disabled.

Media Protocol Value	Key exchange method	default
Best Effort SRTP	mikey+sdes, mikey, sdes,dtls	mikey+sdes
Strict Pass-Thru	none	none(grayed out)
SRTP Only	mikey,sdes, dtls,mikey+sdes	sdes
RTP	none	none(grayed out)

3.4.4.7 Media Realm Groups

GUI → VOIP → Media →

The Media Realm Groups allow the customer to have some control over media connectivity between network media domains (or network segments) without L3 NAT.

To support the needed flexibility, the customer is required to identify network segments (media realms) in a group (Media Realm Groups), identifying the media anchoring requirements for the media realm group. Additionally each media realm has its own intra-realm media anchoring requirements.

Media connections outside the media realm group are automatically anchored by the OpenScape SBC. A maximum of 1024 Media Realm Groups can be defined.

Distributed Media Realm Group - The Distributed Media Realm Group is used when more than one SBC is in the media path and the media can be anchored in only one SBC. Depending on media capabilities on peers, the media can even not be anchored at all meaning the direct media will be used.

Media Realm Groups

☐ Distributed Media Realm Group

Name	Anchoring media	Force media anchoring on transcoding

Media Realm Groups may be made up of one or multiple network segments. This screen is display only. By selecting "edit" or "add" the next screen is opened

Media Realm Optimization Settings

Name

Anchoring Media Across Subnets

☐ Allow Force Anchoring On Transcoding Across Subnets

Media Optimization Subnets

Row	Physical Interface	VLAN	IP address, Subnet or Logical Endpoint ID	Subnet	Anchor Media	Allow Force Anchoring on Transcoding
1	eth1	0	10.191.0.6	255.255.255.255	forced	<input type="checkbox"/>
2	eth1	0	OSV:BG:branch1	255.255.255.255	auto	<input checked="" type="checkbox"/>

This section controls calls made **inter network segment**. ***See caution

In this section the **network segments are defined** by clicking the "Add" button.

The IP address, Subnet or Logical IP ID are the network elements identification corresponding to remote endpoints or remote subscribers configured in Remote Endpoint Session or Remote Subscriber Session, meaning their remote URL (IPs or FQDN) or logical ID in case of NAT. See Remote URL on chapter 3.5 Example Configurations. The optimization or anchoring for calls, **intra network**, is also configured.

For networks where no NAT is involved the IP address of the end device (phones, GW) is used.

For networks behind a dynamic NAT, the logical ID is used. (all devices behind the dynamic NAT are defined by the logical ID of that NAT).

For networks behind a static NAT, the address of the NAT is used. (all devices behind the static NAT are defined by the address of that NAT).

There may be up to 1024 network segments defined in the system.



*** Care must be taken not to configure media realm groups to include network segments which can not communicate directly as it may result in no speech path problems. (for example a media realm group with one segment behind NAT#1 and a second segment behind NAT#2)

IP address, Subnet or Logical-ENDPOINT-ID – enter the following IP address of the domain subnet.

Endpoint Type	Use IP address of
Remote subscribers no NAT	phones
Phones via Proxy	Phone network
Branch SBC	Branch
Gateway	Gateway
SSP	SSP
If static NAT involved	Address of the NAT
Branch behind dynamic NAT	Logical-Endpoint-ID

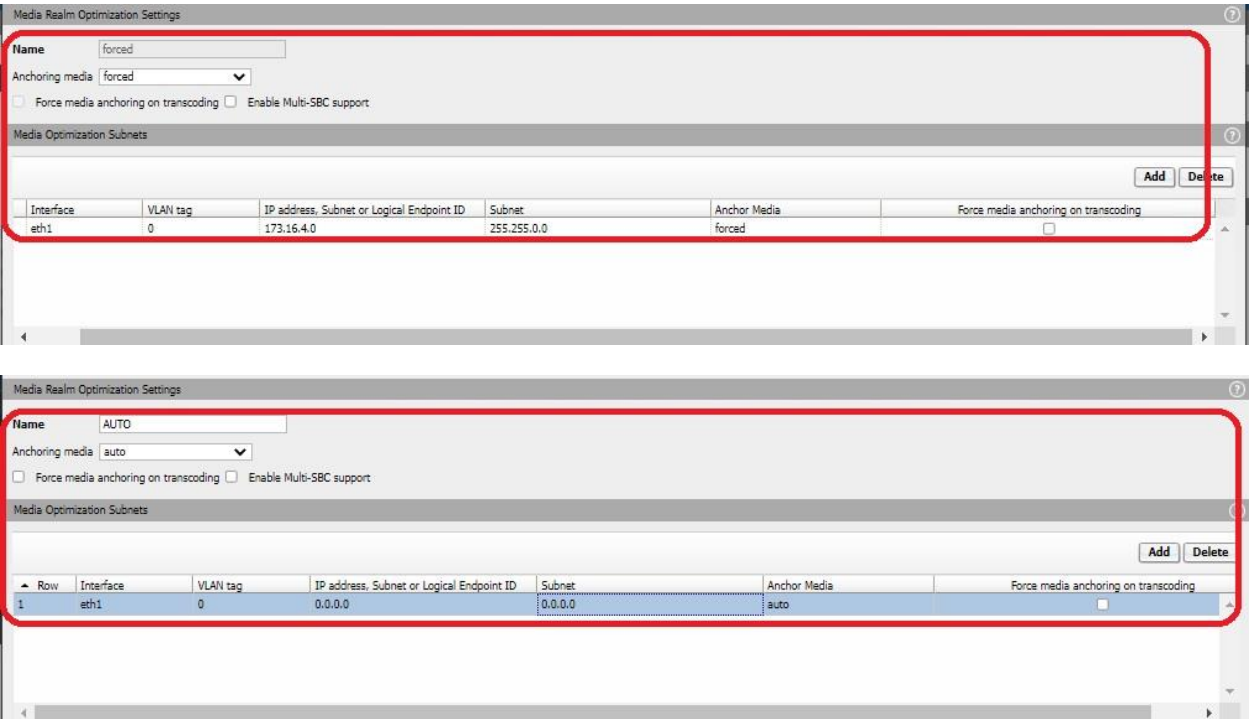
Media anchoring for overlapping subnets

When there is a need to anchor media for a specific subnet, it is necessary to create separate Media Realm Groups.

- One Realm Group to Anchor media
- The second Realm Group to not Anchor media

Select the subnet (example 173.16.4.0) with the option Anchor Media set to forced

Select the subnet (example 0.0.0.0) and option Anchor Media set to auto



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
Media
QoS Monitoring

default	G711A,G711U,G729	Best Effort SRTP	mikey + sdes	
webrtc_default		SRTP only	dtls	
WE_Phone_default		Best Effort SRTP	mikey + sdes	
TESTPTIME	G711A,G711U,G729	Best Effort SRTP	mikey + sdes	

Cloud Support

☐ Support OpenScape Cloud

Media Realm Groups

☐ Distributed Media Realm Group

Add Edit Delete

Name	Anchoring media	Force media anchoring on transcoding
forced	forced	
AUTO	auto	

3.4.4.8 Media Optimization

The purpose of this chapter is to give a better explanation of all media optimization possibilities in a way that the user has the full knowledge to properly configure the SBC. SBC provides two main possibilities to optimize the media path, the Media Realm Groups and Direct Media. These features are independent, which means that, depending on the environment, both can be configured.

1. Media Realm Groups

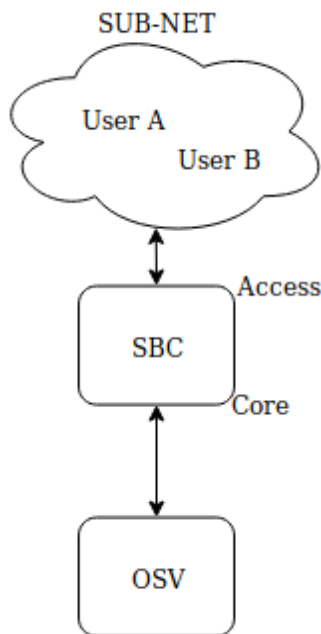
Use cases: this feature was designed for peers in the same sub-net, endpoint, or NAT. It's most commonly used when the peers are devices, such as CP phones and OpenStage.

Target: the target of this feature is not only to optimize the media, but to have some control over it. The user can configure it to either force the anchoring or to optimize it.

Limitations:

- SBC tries to establish direct media between the peers by copying the peers' SDP to send to the other, which means that both peers must have the same configuration regarding media, e.g., codec, m-lines, etc.
- This feature **does not work** with Circuit, refer to Direct Media optimization if that is the case.

Configuration: VoIP→Media on Media Realm Groups section.



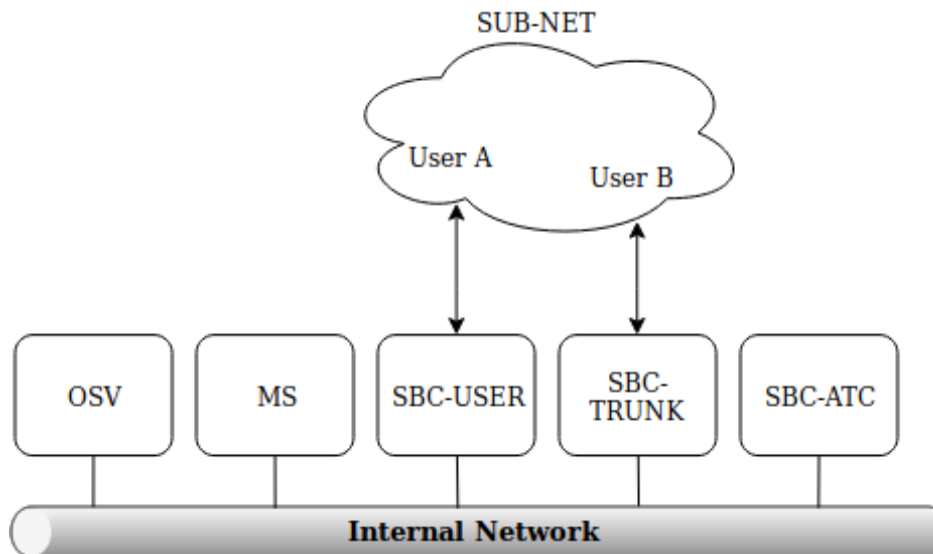
A Sub-net is configured to identify each group. The 'auto' option for 'Anchoring Media' must be chosen in order to optimize the media path. In that way, if both legs of the call are in the configured sub-net, SBC will try to establish the media directly between the endpoints.

Distributed Media Realm Group (DMRG)

Distributed Media Realm Groups allows the Media Realm Group feature to work along with different SBCs. The SBCs use the SDP to exchange information regarding the peers.

NOTE: It's important to mention that the DMRG works because the SDPs are exchanged directly between the SBCs (core side), since OSV only forward the SDPs. This functionality **will not work** if the SDPs are modified by some component in the middle. The exception for this is the Cascaded SBCs design that will be mentioned on this same chapter.

Take the example bellow, where both users A and B are in the same sub-net but connected to different SBCs, User A connected to SBC-USER and User B connected to SBC-TRUNK.



The Media Realm Group **will not** optimize the media by itself because each SBC would handle one leg of the call. The optimization can be done by enabling the DMRG checkbox in **both** SBCs. In this case, if the media cannot be established directly between the endpoints (different media setup), the call **will only be anchored in one SBC**, reducing the media path. The criteria for anchoring in one SBC is the CPU usage.

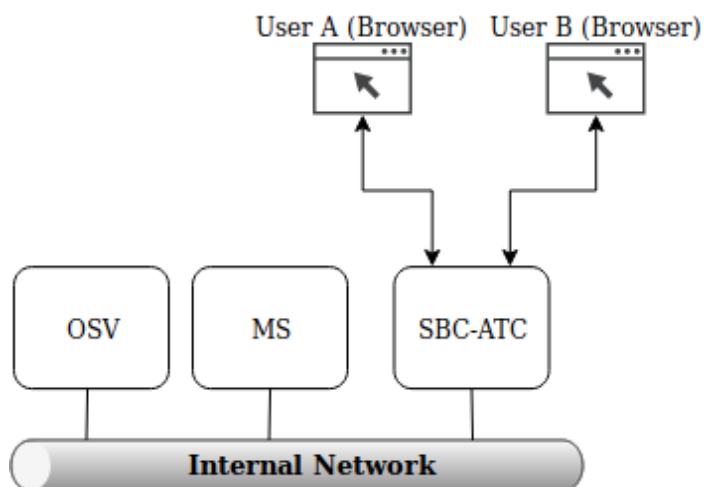
2. Direct Media

Use cases: this feature was designed for peers that, beside reaching each other, support ICE and have the same rtcp setup. It's most commonly used with CP phones and Circuit.

Target: optimize the media path.

Limitations: peers must support ICE, have the same rtcp setup (rtcp-mux or not) and have a common media path excluding the SBC.

Configuration: This feature is configured on the media profiles, VoIP→Media→Media Profiles. Media profile for both sides (core and access) must be configured with Direct Media.



When enabled for both peers, SBC will forward the ICE and rtcp attributes from one peer to another. The rest is handled by ICE itself, which will establish the media with the pair candidates with the highest priority that can reach each other.

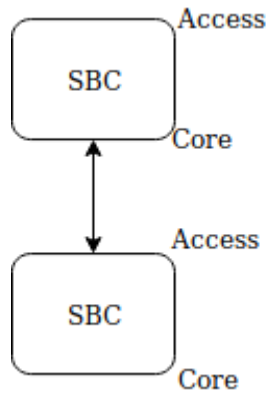
CASCADED SBCs

Cascaded SBCs consist of two SBCs connected to each other. This design have a

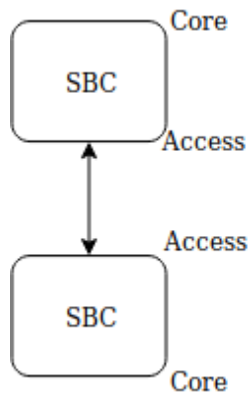
particularity regarding the media optimization because more than two components may interfere on the call negotiation (SDP).

There are two possible designs:

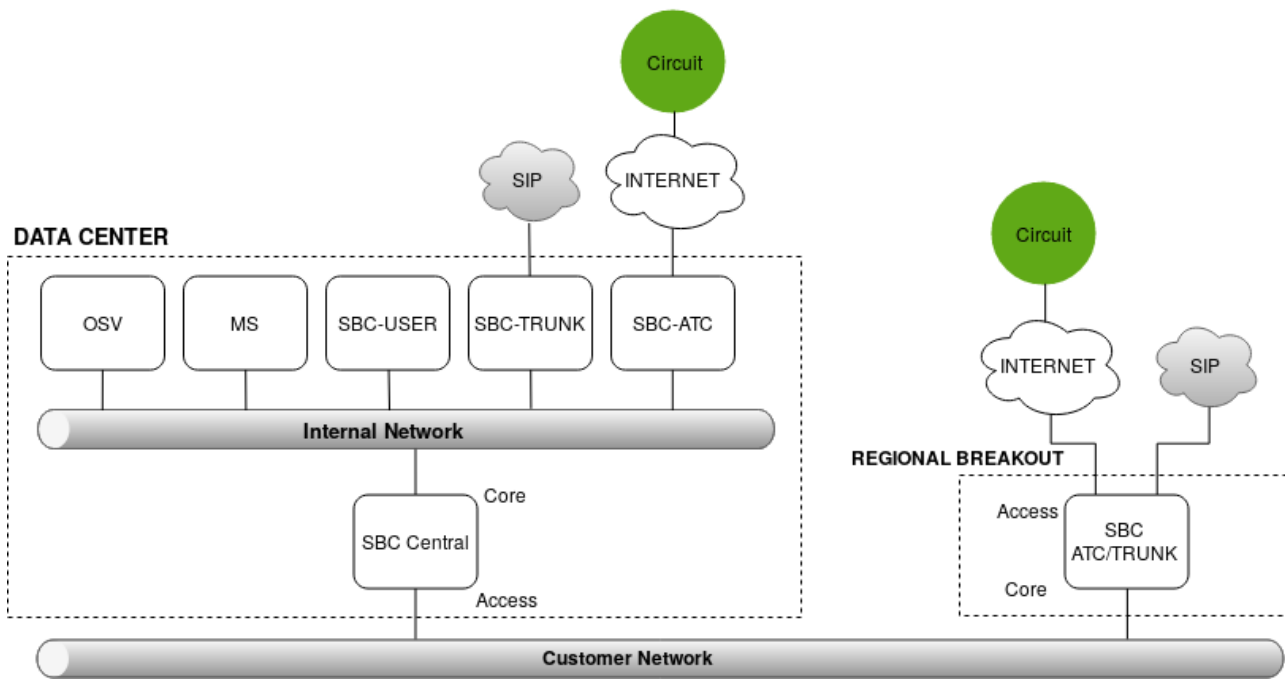
1 - **Core-Access** interaction



2 - **Access-Access** interaction



Take as an example the following solution:



In this example, the customer has a Data Center, where the core structure is, and a Regional Breakout, which could be another site located in a different region. This Regional breakout is connected to the Data Center via the customer network. The cascaded SBCs are formed by the SBC on the Regional Breakout and the SBC Central. The design is the first one mentioned above, Core-Access. Take as an example a call between a Sip Client connected to the Regional Breakout and a Sip Client connected to the Data Center. The flow of the first invite would be the following:

Sip Client A -> SBC on Regional Breakout -> SBC Central -> OSV -> SBC-TRUNK (DataCenter) -> Sip Client B

As explained before, the Distributed Media Realm Group will not work by itself since SBC Central will modify the SDP. In order for DMRG to work, the following configurations must be done:

1. Enable the DMRG on the SBC at the Regional Breakout;
2. Enable the DMRG on SBC-TRUNK (DataCenter);
3. On SBC Central, configure an endpoint type 'SBC' with the 'DMRG' profile for the SBC on the Regional Breakout.

This DMRG profile determines that this SBC endpoint has the DMRG feature enabled and the DMRG optimization must not be interfered.

The DMRG optimization may be the best choice for the example mentioned above, but, on

Remote endpoint configuration

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

Remote Endpoint Settings

Name

SBC 1

Type

SBC

Profile

DMRG

Access realm profile

Main-Access-Realm-ipv4

Core realm profile

Main-Core-Realm-ipv4

Associated Endpoint

☐ Enable Call Limits

Maximum Permitted Calls

0

Reserved Calls

0

Remote Location Information

☐ URI based routing

☐ Enable access control

Signaling address type

IP address or FQDN

Remote Location domain list

AddEditDelete

Row	Remote URL	Remote port	Remote transport	Media IP	Media profile	TLS mode	Certificate profile	TLS keep-alive
-----	------------	-------------	------------------	----------	---------------	----------	---------------------	----------------

OKCancel

this same environment, another optimization may suit better depending on the scenario.

NOTE: The DMRG for cascaded SBC is only supported when the interaction is Core-Access, the feature is not supported for Access-Access interaction.

3.4.4.9 Support of Media optimization across multiple SBCs

So far, Media Optimization (Media between SIP-Endpoints in the same Subnet) is possible per SBC only. Media optimization across multiple SBCs supporting the same Subnets is now available & supported.

In order to optimize the path of subscribers residing in the same subnet, there are some configuration requirements.

The following Configurations have to be identical in all SBCs:

- a) Subnet definition
- b) Media Profile Access
- c) Media Profile Core
- d) Media Profiles Access and Core can be still differ

In order to utilize the feature there are some requirements regarding the **Media Profiles**

Core media profile:

- ☐ Allow "Strict Pass-Thru" and "Besteffort (rtp + srtp)" only;
- ☐ Flag: "Allow unconfigured codecs" needs to be checked;
- ☐ Codec list: empty, no transcoding.

Access media profile:

- ☐ Allow "RTP only", "sRTP only" and "Besteffort (rtp + srtp)" only;
- ☐ Flag: "Allow unconfigured codecs" needs to be checked;
- ☐ Codec list: empty, no transcoding

These settings should ensure that optimization is possible among SBCs.

How to forward media information

A media attribute "**prtnrinfo**" must be used to hold relevant information from one SBC to another. The said attribute will be present in every m-line with an m-line equivalent on the original SDP. SBC must send this information in this order:

- ☐ Original IP
- ☐ Original RTP port
- ☐ Original RTCP port ("0" if non-existent)
- ☐ Codecs added (if any)

Examples:

```
a=prtnrinfo:10.0.0.1 5060 5061
a=prtnrinfo:192.168.0.15 40500 5000 cod 9
9 (G722) is the added, it should be removed in the other
end in case of optimization
```

Here is an example of how the it should work:

1. SDP arriving in SBC1 (Original SDP)

```

v=0
o=OpenStage-Line_0 1202801581 1175310705 IN IP4
192.168.110.52
s=SIP Call
c=IN IP4 192.168.110.52
t=0 0
m=audio 54768 RTP/AVP 0 8 18 101
a=rtpmap:0 PCMU/8000
a=rtpmap:8 PCMA/8000
a=rtpmap:18 G729/8000
a=rtpmap:101 telephone-event/8000
a=silenceSupp:off - - - -
a=fmtp:18 annexb=no
a=fmtp:101 0-15
a=sendrecv
a=rtcp:55765

```

2. SDP leaving SBC1 going to OSV. SBC generates 2 m-lines, one of them which has an equivalent on the original SDP (RTP/AVP). At this stage SBC inserts the “prtnrinfo” attribute.

```

v= 0
o=OpenStage-Line_0 1202801581 1175310705 IN IP4
10.10.170.103
s=SIP Call
c=IN IP4 10.10.170.103
t=0 0
m=audio 4000 RTP/AVP 0 8 18 101 9
a=prtnrinfo:192.168.110.52 54768 55765
a=rtpmap:0 PCMU/8000
a=rtpmap:8 PCMA/8000
a=rtpmap:18 G729/8000
a=rtpmap:101 telephone-event/8000
a=silenceSupp:off - - - -
a=fmtp:18 annexb=no
a=fmtp:101 0-15
a=sendrecv
a=rtcp:4001
m=audio 40002 RTP/SAVP 0 8 101
a=rtpmap:0 PCMU/8000
a=rtpmap:8 PCMA/8000
a=rtpmap:101 telephone-event/8000
a=silenceSupp:off - - - -
a=fmtp:101 0-15
a=sendrecv
a=crypto:1 AES_CM_128_HMAC_SHA1_80 inline:
+c/qnMqzxKDb647ISyJ2c42rmGKLcdKvcric/zmSi
a=key-mgmt:mikey

```

```

AQAVgNCfGY4CAAAAAAAAAAAAAABE1EGcAAAAAUBAAVtaWtleQsA20XazwAA
AA
AKFETL/
+S5pSctgaHaThAq3Hmg3Gm0AQAAADYCAQEEDBAAAAKAEBAAAAHALBAAAAFAAA
Q
EBBAAAAIAJAQAGAQAFAQAIAQEKAQEHAQEMBAAAAAAAAAAAAkABAAEOCNHUuw
zR5eU2YxgqSrhN4ADsBX1lJ6WxBZvu0Pw13ZAA==

```

3. OSV should not change the SDP when forwarding it to the next SBC:

```
v=0
o=OpenStage-Line_0 1202801581 1175310705 IN IP4
10.10.170.103
s=SIP Call
c=IN IP4 10.10.170.103
t=0 0
m=audio 4000 RTP/AVP 0 8 18 101 9
a=prtnrinfo:192.168.110.52 54768 55765
a=rtpmap:0 PCMU/8000
a=rtpmap:8 PCMA/8000
a=rtpmap:18 G729/8000
a=rtpmap:101 telephone-event/8000
a=silenceSupp:off - - - -
a=fmtp:18 annexb=no
a=fmtp:101 0-15
a=sendrecv
a=rtcp:4001
m=audio 40002 RTP/SAVP 0 8 101
a=rtpmap:0 PCMU/8000
a=rtpmap:8 PCMA/8000
a=rtpmap:101 telephone-event/8000
a=silenceSupp:off - - - -
a=fmtp:101 0-15
a=sendrecv
a=crypto:1 AES_CM_128_HMAC_SHA1_80 inline:
+c/qnMqzxKDb647ISyJ2c42rmGKLcdKvcrl/zmSi
a=key-mgmt:mikey
AQAVgNCfGY4CAAAAAAAAAAAAAABELEGcAAAAAUBAAVtaWtleQsA20Xazw
AAAA
AKFETL/
+S5pSctgaHaThAq3Hmg3Gm0AQAAADYCAQEDBAAAAKAEBAAAAHALBAAAAFA
AAQ
EBBAAAAIAJAQAGAQAFAQAIAQEKAQEHAQEMBAAAAAAAAAAAkABAAEOCNHUuw
zR5eU2YxgqSrhN4ADsBX1lJ6WxBZvu0Pwl3ZAA==
```

4. Now SBC2 can check the m-lines with the attribute “partnerfsm” verifying if media optimization is possible and if it is SBC rebuilds the original SDP and send it to the destination:

```
v=0
o=OpenStage-Line_0 1202801581 1175310705 IN IP4
192.168.110.52
s=SIP Call
c=IN IP4 192.168.110.52
t=0 0
m=audio 54768 RTP/AVP 0 8 18 101
a=rtpmap:0 PCMU/8000
a=rtpmap:8 PCMA/8000
a=rtpmap:18 G729/8000
a=rtpmap:101 telephone-event/8000
a=silenceSupp:off - - - -
a=fmtp:18 annexb=no
a=fmtp:101 0-15
a=sendrecv
a=rtcp:55765
```

This procedure can be used to forward up to 2 m-lines (one RTP/AVP and another RTP/SAVP).

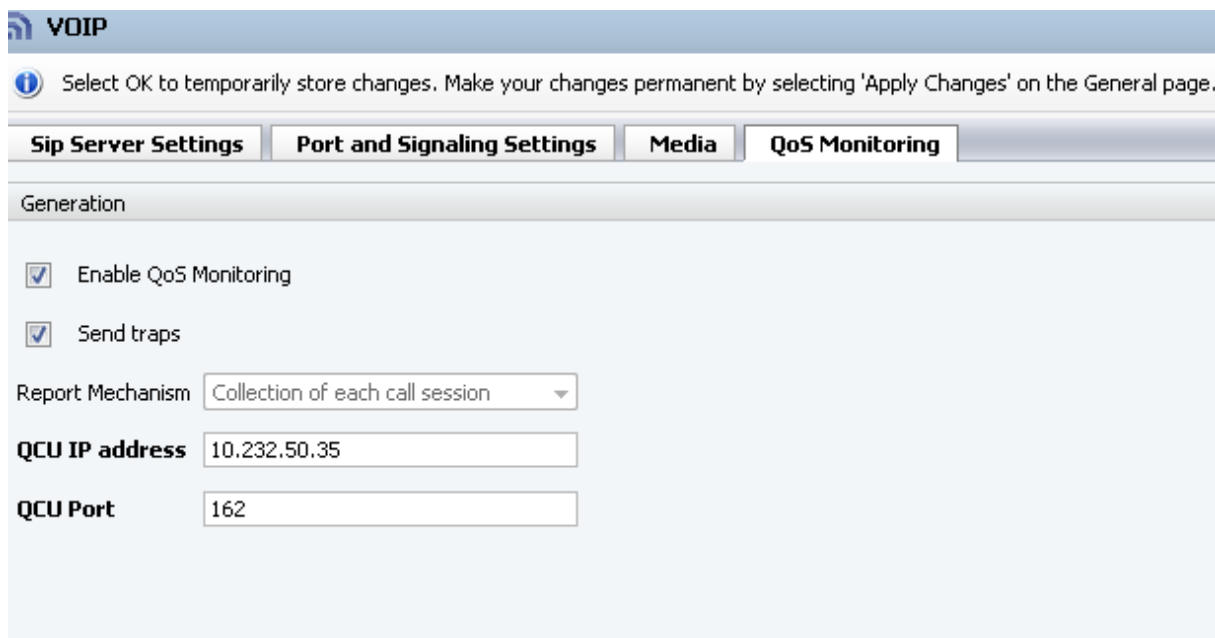
3.4.4.10 QoS Monitoring

QoS Monitoring is enabled by checking the Enable QoS Monitoring checkbox. This flag must be enabled in order to perform media statistic calculations.

Send traps flag enables / disables the generation of traps to the QDC server. The QDC trap is generated at the end of the media session with QoS statistics report for the Access Side, the Core Side and the Remote Endpoint. The default status of this flag is unchecked.

Report mechanism is hardcoded to Collection of each call session. This parameter is not configurable and is be grayed out.

QCU IP address and port specifies the IP and port of QCU servers which the QDC traps are sent on the QCU server.



The screenshot shows the 'VOIP' configuration page with the 'QoS Monitoring' tab selected. At the top, a message states: 'Select OK to temporarily store changes. Make your changes permanent by selecting 'Apply Changes' on the General page.' Below this are four tabs: 'Sip Server Settings', 'Port and Signaling Settings', 'Media', and 'QoS Monitoring'. The 'QoS Monitoring' tab is active and shows a 'Generation' section with the following settings:

- ☒ Enable QoS Monitoring
- ☒ Send traps
- Report Mechanism: Collection of each call session (dropdown menu)
- QCU IP address: 10.232.50.35
- QCU Port: 162

3.4.5 Features

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

Features configuration

<input checked="" type="checkbox"/> Enable Remote Subscribers	Configure	See Remote Subscribers
<input checked="" type="checkbox"/> Enable Remote Endpoints	Configure	See Remote Endpoints
<input checked="" type="checkbox"/> Enable Codec Support for transcoding	Configure	See Transcoding
<input type="checkbox"/> Enable TURN Server	Configure	See TURN Server
<input type="checkbox"/> Enable Circuit Telephony Connector	Configure	See Circuit Telephony Connector
<input type="checkbox"/> Enable Sip Load Balancer	Configure	See SIP Load Balancer
<input type="checkbox"/> Enable Border Control Function	Configure	
<input type="checkbox"/> Enable Push Notification Service	Configure	
<input type="checkbox"/> Enable Ganglia Monitoring Daemon		
<input checked="" type="checkbox"/> Enable Circuit Zookeeper Client		
<input type="checkbox"/> Enable THIG		
<input type="checkbox"/> Enable Standalone		

Enable Standalone

The Feature Standalone is to allow the SBC to be used without sending all traffic to a PBX Node; it will instead send traffic from one configured endpoint to its associated counterpart. In this operation mode there is no connection to any PBX at the core side, SBC will send OPTIONS to the loopback interface that gets responded by itself; in this way it stays in "normal mode" and the access side interfaces aren't locked. The activation of the feature is by a simple checkbox on the Features Screen. To use the feature it is necessary to configure pairs of Associated Remote Endpoints - such configuration is only made available with the activation of the feature.

3.4.5.1 Remote Subscribers

For the purposes of this document "Remote Subscribers" are subscribers which connect to the OS-SBC, either directly or via a NAT device. They do not connect via a branch.

By design, throttling of Registrations for TLS OSMO devices is not performed.

Core realm profile - For the core realm, the “Main-Core-Realm” profile is always selected by the system and cannot be modified by the user (grayed out).
Access realm profile - For the access realm, the “Main-Access-Realm” profile is always selected by the system and cannot be modified by the user (grayed out).

Enable register throttling - Enables register throttling timers for UDP and TCP.
Enable register throttling for TLS - Enables register throttling timers for TLS.
By design in OSS version 8, throttling for TLS OSMO devices is not performed.
Timer value towards subscriber (sec) - It is the expiry timer that CSBC uses towards the phone. Possible values are within the range 30 to 1800. This only applies to remote subscribers behind a NAT.
Maximum throttling timer threshold (sec) - It is the maximum timer for throttling mechanism to control the expiry timer indicated in the Register request from the phone. Possible values are within the range 300 to 3000.
Maximum registration expiry time (sec) - It is the maximum acceptable expiry time for a Register request. Possible values are in range 3600 to 86400.
Port Mapping TTL timer (hours) - It is the timer for Port Mapping Time To Live. Possible values are within the range 1 to 48 hours or never (meaning port mappings persist once they occur).

The checkbox “**Enable remap internal error code**” allows the replacement of internal error code 500 to 504 or 408 for calls to remote subscribers. Default is disabled.

Insert Location Header: This configuration applies to all remote subscribers under the SBC. When enabled, SBC adds the ‘X-Simeens-Location’ header towards OSV. Default is disabled.

Remote Subscribers

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

General Settings

☒ Enable register throttling
Timer value towards subscriber - UDP (sec) 300
☐ Enable register throttling for TLS
Timer value towards subscriber (sec) TCP/TLS 300
Maximum throttling timer threshold (sec) 1800
Maximum registration expiry time (sec) 5000
Minimum registration interval (sec) 300
Port Mapping TTL timer (hours) 2
Core realm profile Main-Core-Realm - ipv4
Access realm profile fwnonvlantcp2
INVITE No Answer timeout (msec) 360000
INVITE No Reply timeout (msec) 30000
☐ Enable remap internal error code 504
☐ Open external firewall pinhole
☐ Send RTP dummy packets
☐ Insert Location Header

Remote Subscribers configuration

Row	Name	Location Domain Name	Location Domain Subnet/IP	Location Domain Subnet Mask	Firewall Allowed List
1	remoteUsersVlan173	remoteusers.com	173.16.101.0	255.255.255.0	Not Enabled
2	TestPtime	ptime.com	173.16.105.0	255.255.255.0	Not Enabled
3	fax	fax.com	173.16.6.0	255.255.255.0	Not Enabled
4	551138176050	551138176050.com	173.16.5.150	255.255.255.255	Not Enabled

Note: By design, throttling of Registrations for TLS OSMO devices is not performed.

3.4.5.1.1 Remote Subscriber Settings

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

name

sgurgurndi

OK

Remote Subscriber Location Domain

Location Domain Name

remote.user.labdq

☐ Subnet

☒ DN List

Subnet IP address

173.16.4.1

Subnet mask

255.255.0.0

Certificate profile

OSV Solution

Media profile

webrtc_default

TLS mode

☒ Fallback TLS

☐ From HEADER

☒ Contact HEADER

Add

75675678

Delete

Access Side Firewall Settings

☐ Enable Firewall Settings

Firewall Settings

Emergency configuration

See [Firewall Settings](#)

Emergency numbers

Add

Delete

Emergency call routing

Add numbers to be considered emergency such as 911 in the United States.

See [Emergency Calling Subnets](#)

Name - user defined name of the remote subscriber, ([branch or subnet name](#))
Location Domain Name - user defined location of the phone, must be a valid IP address or FQDN
Subnet - Selected by default. Subnet configuration items are editable and Subnet configuration is used for Location Domain.
Note: When selected, DN List items are grayed out.
Subnet IP Address - IP address or subnet of the phone, for example 173.16.4.1
Subnet Mask - Domain subnet mask, for example 255.255.255.0
Certificate profile – Select the TLS certificate profile. Default value is None.
Media profile – Select a Media Profile which is configured with the Media protocol, codecs, and packetization interval suited for remote subscriber.
TLS mode – Set the mode for the authentication. Available values are: Client Authentication, Server Authentication and Mutual authentication

3.4.5.1.2 Firewall Settings

Firewall Settings

Firewall Settings provisioning.

- ☐ enable SIP UDP
- ☐ enable SIP TCP
- ☒ enable SIP TLS
- ☐ enable MGCP
- ☐ enable DNS

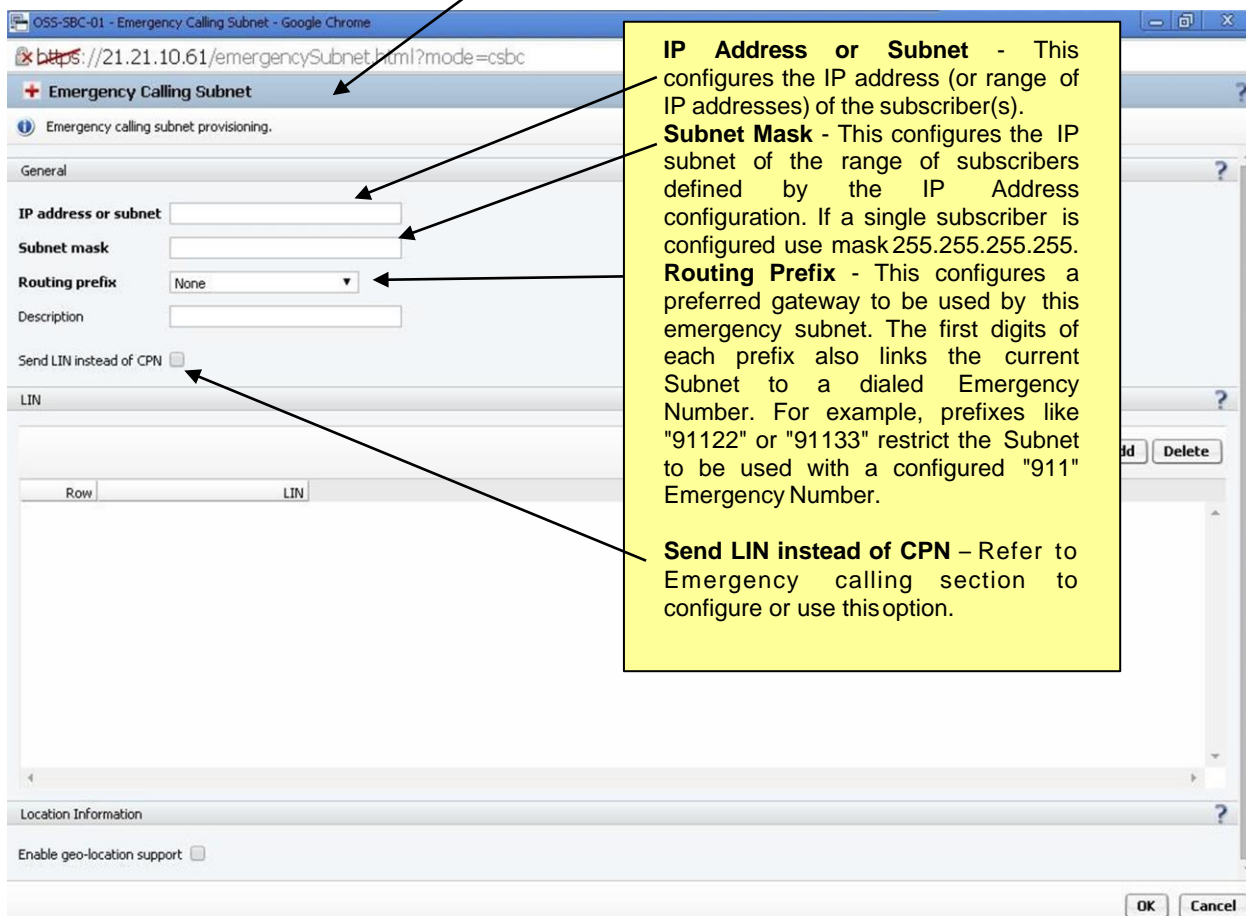
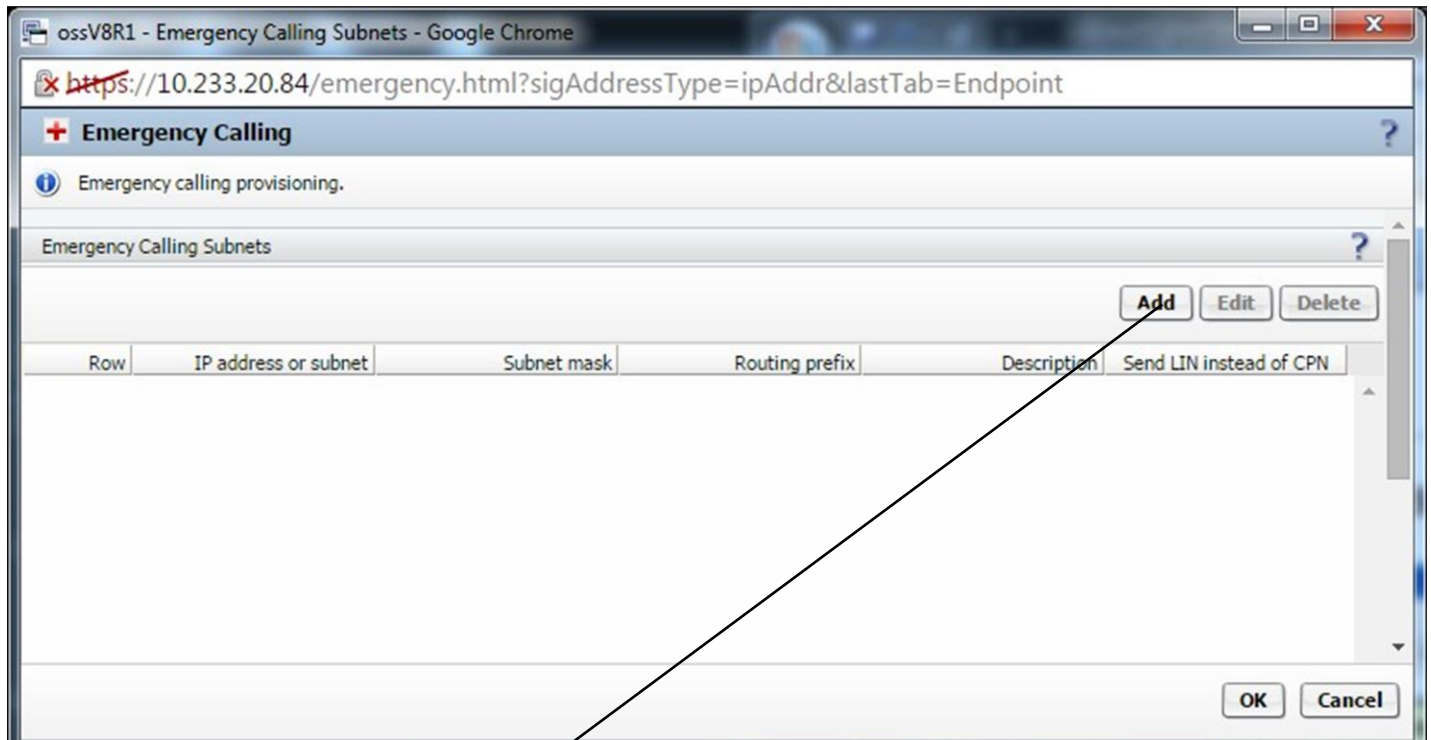
Message rate threshold

White list		Black list	
IP address or subnet	Port	IP address or subnet	Port

White List
Allow Incoming/Outgoing WAN network connections for a specific IP/Port. If the Port field is empty, all ports will be allowed.

Black List
Block Incoming/Outgoing WAN network connections for a specific IP/Port. If the Port field is empty, all ports will be blocked.

3.4.5.1.3 Emergency Calling Subnets



3.4.5.2 Remote Endpoints

There are there 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.

A new SIP Service Provider is configured using the **Add** button.(see section [SIP Service Provider \(SSP\) Profiles](#)) An existing SIP Service Provider can be changed using the **Edit** button, and deleted using the **Delete** button.

Remote Endpoints

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

SIP Service Provider Profile

Hostname

Port

Remote directory

User name

Password

[Download New Profile List](#)

Add Edit Delete

Row	Name	Registration required	Registration interval (sec)
1	dynregssp	<input type="checkbox"/>	3600

Remote endpoint configuration

Add Edit Delete Export Logical IDs

Row	Name	Access realm profile	Type	Profile / Circuit ID	Remote IP address / Logical-Endpoint-ID / Circuit URL	Remote port	Remote transport	Associ
1	SSP_4000	Main-Access-Realm - ipv4	SSP	dynregssp	192.168.111.224	5060	TCP	

OK Cancel

A new Remote Endpoint is configured using the **Add** button. (see [Remote Endpoint Configuration](#)). An existing Remote Endpoint can be changed using the **Edit** button and deleted using the **Delete** button. Notice the "D" in the "remote IP address/Logical endpoint ID" column indicates a dynamic IP address endpoint. The **Export Logical IDs** button is used to download a CSV file containing all the Endpoints using Logical ID with the Row Index of Remote Endpoint table, the Logical IDs and the Logical ID hash code, and the Access Network Realm.

3.4.5.2.1 Remote endpoints using TLS/MTLS

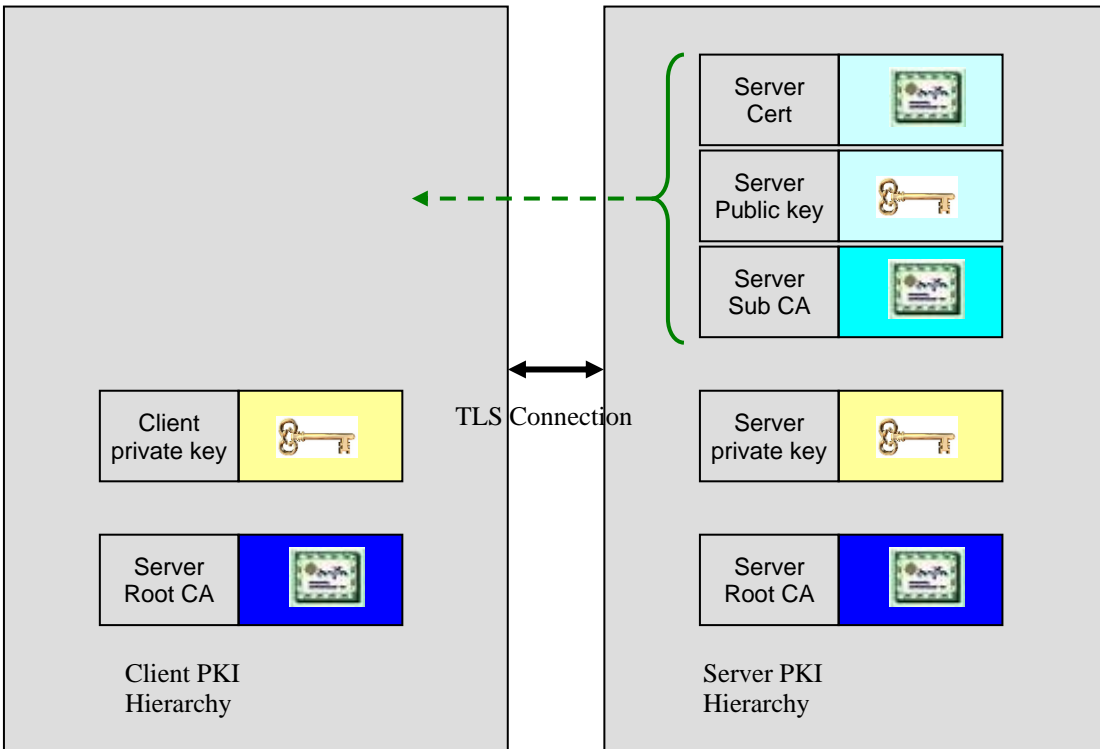
In the case of a TLS connection in which the TLS server provides its certificates, the following certificates must be stored in the client and in the server:

In the TLS Server:

- The following information shall be sent to the client during the establishment of the TLS connection:
 - o The server Certificate;
 - o The server intermediate CA Certificates;
 - o The server public key;
- The server private key;
- Optional - The server Root CA Certificate may be stored in the server in order to be able to verify the validity of its own certificate and its certificate CA chain.

In the TLS Client:

- The client private key;
- The Server Root CA Certificate which will be used to validate the CA chain of the received server certificate.



In the case of an MTLS connection in which both the TLS client and the TLS server provide their certificates, the following certificates must be stored in the client and in the server:

In the TLS Server:

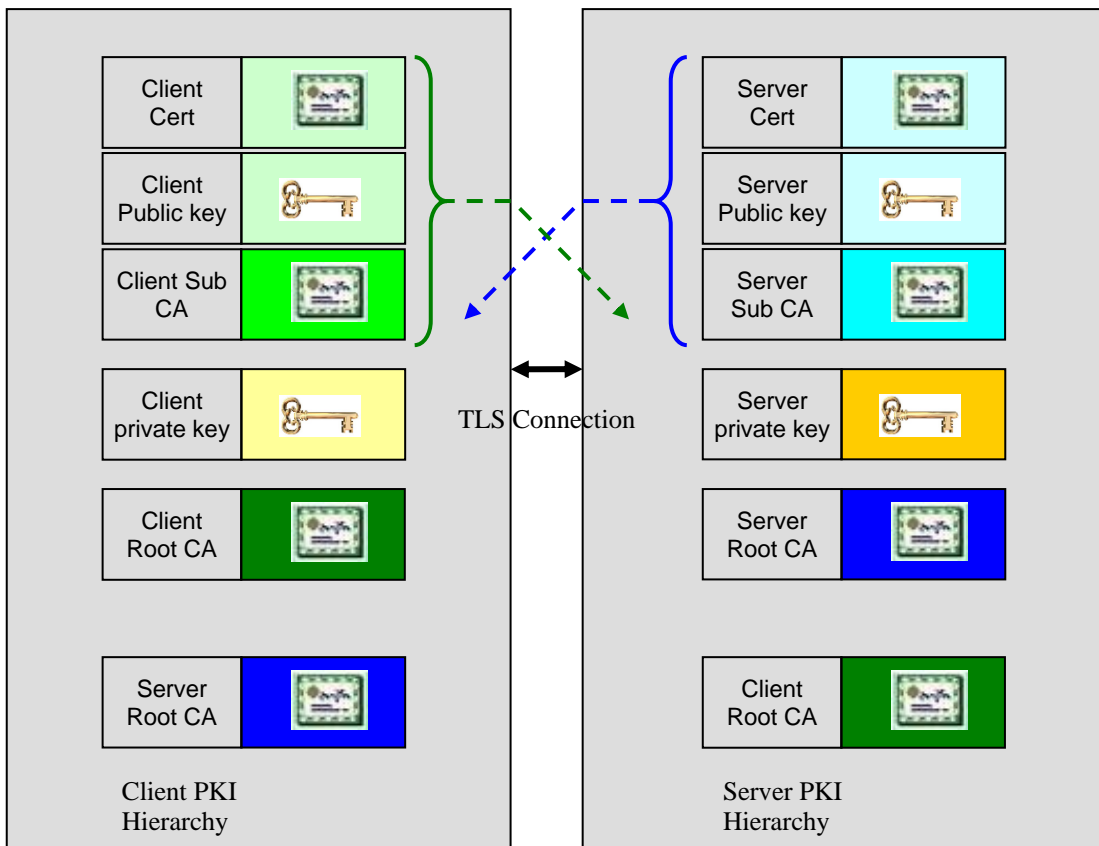
- The following information shall be sent to the client during the establishment of the TLS connection:
 - o The server Certificate;
 - o The server intermediate CA Certificates, if any;
 - o The server public key;
- The server private key;
- Optional - The server Root CA Certificate may be stored in the server in order to be able to verify the validity of its own certificate and its certificate CA chain.
- The client Root CA Certificate which will be used to validate the CA chain of the received client certificate.

In the TLS Client:

- The following information shall be sent to the server during the establishment of the TLS connection:
 - o The client Certificate;
 - o The client intermediate CA Certificates, if any;
 - o The client public key;

- The client private key;
- Optional - The client Root CA Certificate may be stored in the client in order to be able to verify the validity of its own certificate and its certificate CA chain.

The Server Root CA Certificate which will be used to validate the CA chain of the received server certificate.



3.4.5.2.1.1 Certificate Creation

The certificate shall be created according to the following conditions:

- CA file is used – the created certificate will be chained to this CA certificate. A private key will also be created. The CA file should contain the private key of CA certificate.
- CA file is not used (Self Signed) – a new root certificate will be created and the certificate and the key will be generated from this root certificate.

In SBC/OSB management portal, under **Security >General > Certificate Management >Certificate Creation**.

Validation of Received Certificate

During the establishment of TLS / MTLS, certificates are exchanged between the endpoints. The certificates carry the public key, the sender identification, information about the validity period of the certificate and extensions.

For security purposes, a certificate received from the peer shall be validated by:

- Making sure that the certificate has been signed by a CA with an intact chain to a CA certificate configured in the node.
- Making sure that the certificate is within its validity period (between the dates defined by not before and not after).
- Verifying that the certificate has not been revoked by using a Certificate Revocation List.
- Verifying critical extensions – the only supported critical extension is Basic Constraints.
- Certificate Subject Authentication - Authenticating the Subject – Common Name of the received certificate against the configured endpoint FQDN / IP address. If it is not possible to authenticate the Subject – Common Name, it shall be tried to authenticate the extension Subject Alternative Authentication – Common Name.

Certificate profile Setup

The configuration of a cascaded SBC (SBC as remote endpoint of another SBC) the remote endpoint configuration is not different from other endpoint.

In case of MTLS the certificates have to be distributed in both nodes (as client and as server) as described before.

The server and client certificates can be created using the same CA certificate in this case, in Certificate profile of both endpoints the Local CA file will be the same.

If the server and client uses different CA certificates then the certificate profile should have the remote CA file configured in certificate profile and stored in the system. Each remote endpoint have to its own remote CA file which corresponds to the other endpoint.

Below an example of same CA file used on both endpoints:

Name	Certificate service	Client certificate file	Server certificate file	Local CA file	Remote CA file	Local Key file	Attach to Cfg file
OSV Solution	SIP-TLS		servercert.pem	serverCA.pem		serverkey.pem	NO
HTTPS System Default	HTTPS		server.crt			server.key	NO
CircuitLab	GTC				x3e1-AnsibleCA.pem		NO
SBC_CPE	SIP-TLS		altTLSCertcert.pem	dtlsCA.pem		altTLSCertkey.pem	NO

And here with different CA file:

3.4.5.4 SIP Service Provider (SSP) Profiles

SBC-DAN - SIP Service Provider Profile - Google Chrome

Not secure | 21.21.100.198/serviceProvider.html?mode=csbc&name=SSP

SIP Service Provider Profile

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

General

Name: SSP Default SSP profile MS Teams

☒ Use SIP Service Address for identity headers

SIP service address: sbcdan.br

☐ Use SIP Service Address in Request-URI header

☒ Use SIP Service Address in From header

☐ Use SIP Service Address in To header

☒ Use SIP Service Address in P-Asserted-Identity header

☒ Use SIP Service Address in Diversion header

☒ Use SIP Service Address in Contact header

☒ Use SIP Service Address in Via header

☐ Use SIP Service Address in P-Preferred-Identity header

SIP User Agent

SIP User Agent towards SSP: Passthru SIP User Agent:

Registration

☐ Registration required

Registration interval (sec): 3600

Business Identity

☐ Business identity required

Business identity DN:

Outgoing SIP manipulation

☐ Insert anonymous caller ID for blocked Caller-ID

Manipulation

Incoming SIP manipulation

Calling Party Number: From header user and disp

Flags

☐ FQDN in TO header to SSP

☐ Use To DN to populate the RURI

☐ Send Default Home DN in Contact for Call messages

☐ Allow SDP changes from SSP without session version update

Activate Windows
Go to Settings to activate Windows.

OK Cancel

Name - SIP Service Provider name

Default SSP Profile - list of default SIP Service Providers profiles. When a default profile is selected the SSP configuration is automatically loaded to the page

- **Use SIP Service Address for identity headers** - When enabled, for both normal and survivability modes, identity header fields are modified to include the SIP Service Address network domain field
- **SIP service address** - FQDN or IP address identifying the network domain for the SIP Service Provider
- **Use SIP Service Address in Request-URI header** - Modifies Request-URI header to include the SIP Service Address network domain
- **Use SIP Service Address in From header** - Modifies From header to include the SIP Service Address network domain
- **Use SIP Service Address in To header** - Modifies To header to include the SIP Service Address network domain
- **Use SIP Service Address in P-Asserted-Identity header** - Modifies P-Asserted-Identity header to include the SIP Service Address network domain
- **Use SIP Service Address in Diversion header** - Modifies Diversion header to include the SIP Service Address network domain
- **Use SIP Service Address in Contact header** - Modifies Contact header to include the SIP Service

Address network domain

- **Use SIP Service Address in Via header** - Modifies Via header to include the SIP Service Address network domain
- **Use SIP Service Address in P-Preferred-Identity header** - Modifies P-Preferred-Identity header to include the SIP Service Address network domain

Registration required - If selected (enabled), the OpenScape SBC will attempt to register with the SSP.

Registration interval (sec) - Configures the expiration time for the registration performed by the OpenScape SBC in the SIP SP. Will be used by the system only if 'Registration required' option is selected.

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

SIP Manipulation - Opens new configuration window allowing creation/modification/deletion of specific SIP manipulation rules

Digest Authentication credentials specified in the OS-SBC SSP profiles are **only** used for the **SSP trunk surrogate registration** (the OS-SBC trunk will attempt to register with the SSP)
This information is not used for subsequent calls only the registration process.

TLS Signaling - This box is used to configure how TLS as a transport type will be signaled in the SIP messages of remote endpoint calls.

The possible values are: transport=tls, SIPS Scheme, Endpoint config or Pass-Thru

transport=tls - Uses parameter "transport=tls" in SIP messages and does not accept SIPS URI.

SIPS Scheme - Uses the TLS connection to identify the transport type of registration, uses SIPS URI in Record-Route header of remote endpoint requests.

Endpoint config - Uses the remote endpoint configuration to determine the transport and does not use "transport=tls" nor SIPS URI in the SIP Message.

Pass-Thru - Accept or Send transport=tls or SIPS in SIP Message.

SIP User Agent

SIP User Agent towards SSP - Default value is "Passthru" for all SSP profiles. Available options:

– Passthru - the SIP User Agent configuration box is grayed out. If no SIP User Agent is received from the LAN side, nothing will be added.

– Add if non received - the received User Agent from the LAN side is passed on unchanged.

– Add or Replace - the received User Agent from the LAN side will be replaced with the configured User Agent.

IMPORTANT: If no User Agent is received from the LAN side, the configured User Agent will be added

SIP User Agent - Configurable SIP User Agent able to recognize a SIP soft switch and apply dynamically a profile to this SIP soft switch and monitor it.

Up to 32 alphanumeric characters allowed, e.g "OSBC-test-24"

Flags

Flags	
<input type="checkbox"/>	FQDN in TO header to SSP
<input type="checkbox"/>	Use To DN to populate the RURI
<input type="checkbox"/>	Send Default Home DN in Contact for Call messages
<input type="checkbox"/>	Allow SDP changes from SSP without session version update
<input type="checkbox"/>	Do not send INVITE with sendonly media attribute
<input type="checkbox"/>	Do not send INVITE with inactive media attribute
<input type="checkbox"/>	Do not send INVITE with video media line
<input checked="" type="checkbox"/>	Do not send Invite without SDP
<input checked="" type="checkbox"/>	Renew core side crypto keys
<input type="checkbox"/>	Do not send Re-Invite when no media type change
<input type="checkbox"/>	Do not send Re-Invite
<input type="checkbox"/>	Remove Silence Suppression parameter from SDP
<input type="checkbox"/>	Enable pass-through of Optional parameters
<input type="checkbox"/>	Force direction attribute to sendrcv
<input type="checkbox"/>	Send default Home DN in PAI
<input type="checkbox"/>	Send default Home DN in PPI
<input type="checkbox"/>	Preserve To and From headers per RFC2543
<input type="checkbox"/>	Disable FQDN pass-through in FROM header
<input type="checkbox"/>	Keep Digest Authentication Header
<input type="checkbox"/>	Send Contact header in OPTIONS
<input type="checkbox"/>	Do not send Privacy header in response messages
<input type="checkbox"/>	Remove bandwidth (b) lines from SDP
<input type="checkbox"/>	Keep P-Asserted-Identity from access side
<input type="checkbox"/>	Avoid sending 183 messages
<input type="checkbox"/>	Avoid sending 180 message (for 60s)

- **FQDN in TO header to SSP** - If selected (enabled), To header is modified for the in-dialog SIP Requests sent to SSP with FQDN configured for SSP.
- **Use To DN to populate the R-URI** - Enable if the SIP Service Provider is sending the Account information in the Request URI and the destination information in the To header. Disabled by default.
- **Send Default Home DN in Contact for Call messages** - If enabled, the configured default home DN is used to set the Contact header only for call messages. It is not applicable for REGISTER message. Disabled by default.
- **Allow SDP changes from SSP without session version update** - Flag to take care of SSP which are incorrectly keeping the same session id and session version but changing the contents of the

SDP.

- **Do not send INVITE with sendonly media attribute** - Do not send INVITE with sendonly media attribute to SSP.
- **Do not send INVITE with inactive media attribute** – Change inactive media attribute to sendrecv.
- **Do not send INVITE with video media line** - Do not send INVITE with video media line to SSP.
- **Do not send Invite without SDP** - Do not send INVITE without SDP to SSP. When enabled, the SBC interworks an INVITE without SDP to an INVITE with SDP towards the SSP, which does not support INVITE requests without SDP. All re-invites originating from the core side that include SDP, will be delivered to the access side using normal processing procedures such as transcoding and m-line type modifications. However, if a re-invite without SDP is sent from the core side to the access side, SSM will retrieve the most recent SDP sent to the access side, remove the media attribute (sendrecv, inactive, sendonly, or recvonly) and send the re-invite to the access side.

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: Starting from V10R3.03.00.

- **Renew core side crypto keys** - Starting from V10R3.1.3, with this feature every answer generated by the system is assigned a new crypto key on the core side.

Important: This flag is used only when the flag **Do not send invite without SDP** is activated. If not, this flag is grayed out.

If a new crypto context is necessary, it is recommended to activate the flag **Reset SRTP context upon key change** in folder VOIP/Media for long calls with SRTP.

When the flags **Renew core side crypto keys** and **Reset SRTP context upon key change** are enabled, after each re-invite with SDP, the crypto context is recreated. This implies a new sequence number and a reset of the Roll-Over Counter. This flag only changes the crypto in the SDP. If the endpoint does not support a crypto refresh, do not use this flag.

Note: The combination of the flags **Renew core side crypto keys** and **Reset SRTP context upon key change** implies non-RFC behavior.

- **Do not send Re-Invite when no media type change** - Do not send re invite to SSP if there is no change in the media type characteristics towards SSP (e.g. audio to audio re-invite).

NOTE: Old Codecs from the SSP would be reused towards the core and hence requires that at least one common codec should exist between all endpoints including SSP.

- **Do not send Re-Invite** - Do not send re invite at all to the SSP. 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.

- **Remove Silence Supression parameter from SDP** - Remove the attribute for silence suppression in the SDP towards the SIP Service Provider. Disabled by default.
- **Enable pass-through of Optional parameters**- When enabled, you may configure up to 10 optional SIP - Header parameters pass-through for Call handling to / from SIP Service Providers (SSPs). You only need to add the parameter name (e.g. "alias").Disabled by default.
- **Force direction attribute to sendrcv** - This flag is used to force sending the SDP media direction attribute. This configuration is recommended for providers that do not accept to receive SDP without media direction attribute.

NOTE: This configuration only applies to SIP responses.

- **Send default Home DN in PAI** - When enabled, the respective configured Home DN is replaced in the user part of the P-Asserted-Identity header if available for the message to the SSP.
- **Send default Home DN in PPI** - When enabled, the respective configured Home DN is replaced in the user part of the P-Preferred-Identity header if available for the message to the SSP.
- **Preserve To and From headers per RFC2543** - When set the To and From header to the SSP would match the URI received from the SSP in order to meet the RFC2543 dialog matching requirements.
- **Disable FQDN pass-through in FROM header**
When FQDN is received in FROM header if this flag is enabled the appropriate IP interface address will be used in the core to access side mapping. If the flag is disabled the FQDN received will be passed transparently to the other side.

NOTE: When "Disable FQDN Passthrough in FROM header" is enabled and FQDN is received in FROM header the "SIP Service Address" is not used in FROM header even if "Use SIP Service Address for all identity headers" is enabled.

- **Keep Digest Authentication Header** - after receiving the first challenge, SBC will keep sending the authentication header, incrementing the nonce count each time. The SSP must challenge again if the registration fails at some point.
- **Send Contact header in OPTIONS** - This flag modifies the OPTIONS messages to include the Contact header when it is not present.
When the option Use SIP Service Address in Contact header is set, the SIP service Address will be used in the Contact header. Otherwise, the external firewall, when enabled, or the endpoint IP will be used.
- **Do not send Privacy header in response messages** - This flag removes Privacy header from SIP response messages 183 and 200.
When the option Do not send Privacy header in response messages is set, the responses to original INVITE sent with Privacy header will have this header removed.
- **Remove bandwidth (b) lines from SDP** - Remove the bandwidth parameters from the SDP session and media lines present in the messages sent to the SSP.
- **Keep P-Asserted-Identify from access side** - This flag keeps the original P-Asserted-Identity (PAI) header received from the access side. This flag prevents the PAI header to be changed

by OS-SBC.

NOTE: This flag is not directly associated with emergency calls and can be used in other situation

- **Avoid sending 183 messages** - When this flag is set, the SBC does not forward the 183 Session Progress response messages received by the SSP to the core side.
- **Avoid sending 180 message (for 60s)** - This flag prevents 180 Ringing multiple response messages. The SBC avoids sending a new 180 Ringing message for 60 seconds after sending the previous message.

INFO:

The previous flags "Allow single SSP with different home DN prefix based handling" and "Ignore last digit in Default home DN for incoming calls from SIP trunk" were removed as they are no longer needed.

During the system re-configuration due a user change or upgrade if the flag " Allow single SSP with different home DN prefix based handling" were set then the prefix table is populated with Home DN and if the "Ignore last digit in Default home DN for incoming calls from SIP trunk" is also set then the prefix table is populated with home DN with last digit stripped. The duplicated rules are not allowed, even for remote endpoints with different remote ip addresses.

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 SBC adds "user=phone" in SIP URIs towards SSP.
- **1TR118** - Technical Specification of the SIP Trunking Interface between a SIP-PBX with DDI and the NGN Platform of Telekom Deutschland (DT-AG). If this flag is enabled, then many SIP messages will be in accordance with Deutsch Telekom requirements for SIP Connect 1.1 described under https://www.telekom.de/hilfe/downloads/1tr118_v10_.pdf
- **Registration Mode** - When Registration Mode flag is enabled, SBC will be sending Register message with Registration Mode format of SIP Connect that will add the following headers:
 - Proxy-Require: gin
 - Require: gin
 - Supported: path
 - Allow-Events: vq-rtcp
- **Bulk registration required** - When checked, then the Registration AOR must also be configured. In this case the OSB/SBC shall use the configured Registration AOR in the FROM and TO headers of the REGISTER request towards the SSP.
- **Registration AOR** - The SIP-PBX must be capable of provisioning any format of SIP-URI as the Registration AOR, in order to accommodate SP-SSE requirements

DTAG/Company Flex

When the default SSP profile "DTAG/Company Flex" is selected, the parameter for specification 1TR119 is automatically selected. It requires that the associated SSP uses media profile with SRTP/SDS, and will include in the methods REGISTER, INVITE, and UPDATE, the following SIP headers:

- Proxy-Require: mediasec
- Require: mediasec
- Security-Verify: msrp-tls;mediasec
- Security-Verify: sdes-srtp;mediasec
- Security-Verify: dtls-srtp;mediasec

The header "Security-Verify" will be included in the method REGISTER only when the authorization is sent after the challenge.

For the method REGISTER, the following SIP header will also be included:

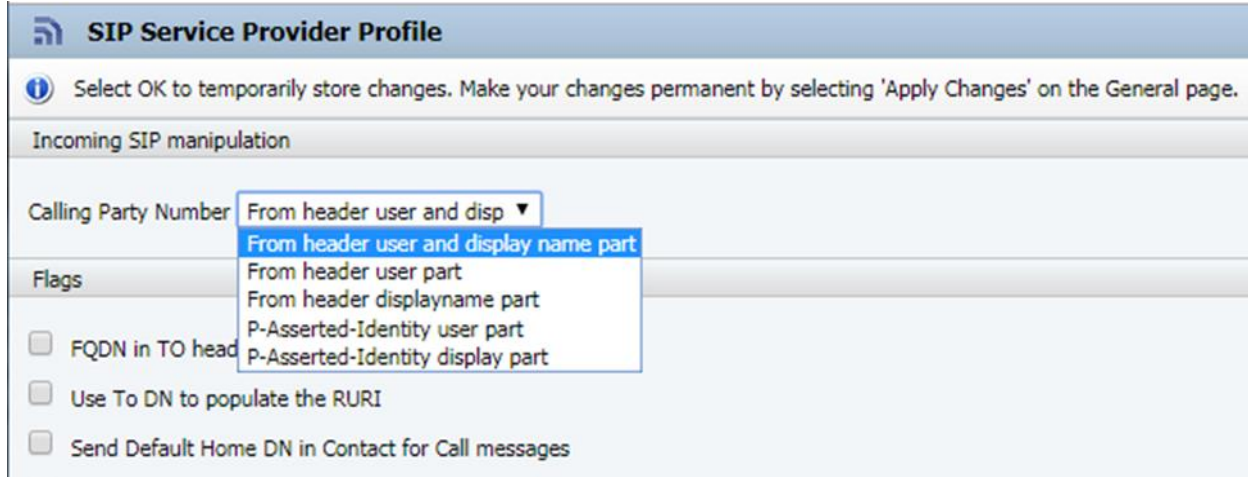
- Security-Client: sdes-srtp;mediasec

In addition, the attribute "3ge2ae: requested" will be included in the SDP offer to the SSP

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 providers 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
- ☐ Use To DN to populate the RURI
- ☐ Send Default Home DN in Contact for Call messages

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.

SIP Service Provider Profile

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

Flags

- ☐ FQDN in TO header to SSP
- ☐ Use To DN to populate the RURI
- ☐ Send Default Home DN in Contact for Call messages
- ☐ 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
- ☐ Do not send Re-Invite when no media type change
- ☐ Do not send Re-Invite
- ☐ Remove Silence Suppression parameter from SDP
- ☐ Enable pass-through of Optional parameters
- ☐ Force direction attribute to sendrcv
- ☒ Send default Home DN in PAI
- ☒ Send default Home DN in PPI
- ☐ Preserve To and From headers per RFC2543
- ☐ Disable FQDN pass-through in FROM header
- ☐ Keep Digest Authentication Header
- ☐ Send Contact header in OPTIONS
- ☐ Do not send Privacy header in response messages
- ☐ Remove bandwidth (b) lines from SDP

Setting the flag Send default Home DN in PAI, the OS SBC shall overwrite any received authentication number in a P-Asserted-Identity header in a SIP INVITE from OSV with the default Home DN configured for the SIP SP for outgoing INVITE messages towards a SIP SP. The same behavior is valid for the flag Send default Home DN in PPI in relation to the P-Preferred-Identity header.

The default Home DN is configured in Remote endpoint configuration.

Remote endpoint configuration

Remote endpoint provisioning.

Signing source type: [dropdown]

Remote Location domain list

Remote URL	Remote SIP/MGCP port	Remote transport	Media IP	Media profile	TLS mode	Certificate profile	TLS Keep-Alive
<div style="text-align: right;"> <input type="button" value="Add"/> <input type="button" value="Delete"/> </div>							

Remote Location Identification/Routing

Core FQDN: [text box]

Core realm port: [text box]

Default core realm location domain name: [text box]

Routing Prefix: [text box]

Default Home DN: [text box]

OS SBC shall support all the allowed characters for the user part of a SIP URI per section 25.1. of RFC 3261 in the FROM and TO headers and RURI in registration messages towards a SIP Service provider.

The following characters shall be supported: "-", "_", ".", "!", "~", "*", "(", ")", "&", "=", "+", "\$", "%", ";", "?", "/"

3.4.5.4.1 Additional information on digest Authentication for SSP

In the case of a SSP, the SSP MAY challenge the OSV when an INVITE is received in an attempt to setup a call (SIP 407 proxy authentication required).

The challenge is passed to the OSV by the OSS. To respond to the challenge the information needs to be configured on the OSV.

CMP→OpenScope Voice→ <select business group> members→endpoints <endpoint which represents the trunk to the SSP> SIP →Security→trusted→edit. Here the port range, local realm, local user name, and local password must be set up. This information is then used to respond to the challenge.

The information configured on the OSS is used only for configuration, not subsequent calls.

3.4.5.4.2 Incoming Route Prefixes for Common SSP

Some SIP service providers can support several customers with different numbering plan. When making an outgoing calls to SSP the remote endpoint is selected by OSV based on routing rules. It creates a request to SBC using a specific core port and this port is used to match the remote endpoint. Then the default homeDN is used as caller.

In incoming calls from SSP, some providers use the R-URI as the Default Home DN or specific range of numbers. It is used to identify the remote source endpoint when there is more than one endpoint associated to the same Sip Service Provider. It only shows if the gateway/trunk type is set to SIP Trunk.

This table stores up to 10 prefixes associated to a remote endpoint, the query for the endpoint is then based on a best match of configured prefixes. Any configured prefixes must not overlap another previously configured prefix, thus avoiding any duplication.

A maximum 30 character string of alphanumeric characters as well as the supported set of symbols (" - ' _ . " ~ " * " (") " = " + " \$ " ; " ? " / ").

3.4.5.4.3 SSP Profiles Special Conditions Related to “Do not send INVITE without SDP” and “Do not send Re-Invite”

The OS SBC now supports a new configuration item per SIP Service Provider profile which allows setting an indication whether the SSP supports receiving INVITE without SDP or not. This is controlled by “Do not send INVITE without SDP” in the SSP Profile.

When OS SBC receives an initial INVITE without SDP targeted for a remote endpoint which has this flag set, it selects a free RTP port and/or SRTP port and CODECS based in the profile assigned to the SSP, on the Access side of the SBC to be included in the SDP offer.

The CODEC selection that goes on the SDP of the INVITE message is specified with a media profile that gets assigned to the SSP remote endpoint.

The SSP must offer at a minimum an unsecure audio stream.

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.

NOTE: 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.

3.4.5.5 Remote Endpoint Configuration

Remote endpoint configuration

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

Remote Endpoint Settings

Name

Type

Profile

Access realm profile

Core realm profile

Associated Endpoint

☐ Enable Call Limits

Maximum Permitted Calls

Reserved Calls

Associated endpoint pull-down box is enabled when the remote endpoint type is "Media Server" or "Gateway". The user is then given the opportunity to associate this remote endpoint with another remote endpoint Name of type "Proxy" or "Branch SBC". This association provides the ability to associate a gateway as well as a media server to a specific Branch. With this association you could now have gateways with the exact same private IP behind a different OSB.
For example branch1 and branch2 could both have a gateway with an IP address of 192.168.4.4 behind the branch.

Remote Location Information

☐ Support Peer Domains

☐ Support Foreign Peer Domains

☐ Enable access control

Signaling address type See the note below regarding this field

Remote Location domain list

Row	Remote URL	Remote port	Remote transport	Media IP	Media profile	TLS mode	Certificate profile	TLS keep-al
Click Add to add a new Remote Location Domain to the Remote Endpoint (see Remote Location Domain). You may edit the new or existing Remote Location domain by pressing the Edit button. To delete an existing Remote Location domain, select the row entry followed by the Delete button.								

Remote Location Identification/Routing

Core FQDN

Core realm port

Default core realm location domain name

Core realm port – Must match the unique port defined for this endpoint in the OSV



If the "signaling address type" = "dynamic IP" then the Logical-Endpoint-ID **MUST** equal the "Logical branch office ID" of the branch behind the NAT. The "Logical branch office ID" of the branch may be found at: local GUI → System → OpenScope Branch Licenses

Support Peers Domains: Enables the usage of URI based routing, which means that the OSS routes the call based on the Request URI that is contained in the INVITE received from the OSV. When this box is not checked, the OSS routes the call based on the static remote endpoint configuration.

Note: When a connection with a Foreign Peer Domain is established, if the Sip Server is restarted, the connection information is lost and in-dialog requests will not be routed correctly.

Note: When an external firewall is used, the firewall port must be the same as the SBC access interface port. Otherwise some problems can occur with the ports inside the sip message

Support Foreign Peer Domains: Enables the usage of URI based routing without having the remote URL configured in Remote Location domain list. For incoming calls from the Access side (WAN), the call will be accepted when the destination in the request URI matches any entry in the whitelist. When the white list is empty, only outgoing calls coming from the Core side are allowed. This configuration is available only when remote endpoint type is set to Gateway.

Note: Foreign Peers Domains will use the Default media profile

Note: By default, only calls with video m-line will be accepted for Support Peers Domains and Support Foreign Peer Domains endpoints. This configuration may be changed disabling flag Accept only Video Calls from Peer Domains in security->general tab.

Note: Only one remote endpoint with the flag "Support Foreign Peer Domains" can be configured in the system.

Whitelist: Enables the configuration of allowed URLs in the destination R-URI for the incoming calls, when the attribute Support Foreign Peer Domains is enabled.

The possible items added to the whitelist to match the destination are :

- Only exact match: sip:user@domain or [sip:user@IPAddress](#)
- Wildcard match *@video.unify.com or *.video.unify.com for all video devices in video.unify.com realm
- Regular expression e.g. sip\:sub\d\d\d\d\d@video\.unify\.com to match string [sip:sub12345@video.unify.com](#)
- The wildcard on both user and domain part is not allowed for complete fields i.e. *@*
- The entry must begin with "*", "sip\:." or "sips\:"
- IPv6 entries are allowed, use [and] to indicate IPv6 entry.
- Allowed characters: A-Z a-z 0-9 . - _ + \ [] : @ ? & = () +
- Ending character must match \$? + * A-Z a-z 0-9)]

White list

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


White list for trusted peers **Add**


Delete

OK **Cancel**

Enable Access Control: You can activate this check box only when the Support Peers Domains check box is checked. Otherwise, this field is deactivated. When you check this box is, the access control functionality is enabled by allowing multiple entries in the Remote Location Domain list. Calls are only possible when the source or the destination remote URL is configured. Incoming calls from the Access side are authenticated by source IP address authentication. When you disable the Enable access control flag and the remote endpoint is configured with the flag Support Peer Domains, incoming calls are accepted from unknown peers if the MTLS negotiations are successful. The Remote Location Domain list contains exactly one entry with a blank remote URL in this case. Otherwise, multiple entries are allowed. When he incoming call, in this case, is not (M)TLS, then a search for a remote endpoint with a whitelist match is executed.

Warning: URI based routing and Allow Open Alphanumeric Access are deprecated.


clustered Servers


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

AddDelete

Group ID	Group name	Node Name	Priority	Routing prefix	IP address or FQDN	Port	Transport	Stick with CommServer	No Answer timer (msec)	No Reply timer (msec)
1	Group	SSP	1	+55	1.1.1.1	5060	TCP	<input type="checkbox"/>	360000	3000
2	Group	GTC	2	+55	2.2.2.2	5060	TCP	<input type="checkbox"/>	360000	3000

Endpoint on clustered mode works following the configuration presented on the clustered servers screen, exception for the endpoint type GTC. In the scenario that GTC range number and SSP range number are in the same routing prefix and cant be changed, the following configuration can be used, changing the priorities for the SSP being the higher the call will try that server first and enabling the "Enable Cluster Server" flag on the GTC endpoint configuration to use the GTC rule will maintain each endpoint going to its designed server.

☐ Enable Call Limits

Maximum Permitted Calls

Reserved Calls

Enable Call Limits : Enable/Disable limit sessions for this specific endpoint based on the values configured.

Maximum Permitted Calls : Maximum allowed number of simultaneous calls for this endpoint.

Reserved Calls : Number of calls guaranteed for this endpoint at any time. This number must be lower than the

overall licensed sessions and the SUM of all reservations across multiple endpoints MUST not exceed the overall sessions limit.

Notes : Emergency calls are not subjected to rejection even after limit is reached

Access side firewall settings for Remote endpoints

The Firewall Settings are enabled using the Enable Firewall Settings check box. The button "Firewall Settings" is used to open the Firewall configuration window.

These firewall settings are specifically for this remote endpoint regardless of the system wide firewall settings.

The remote endpoint firewall does not currently function if the remote endpoint is behind a dynamic NAT. (Defined with a logical-ID rather than an IP address)

Emergency configuration Emergency numbers

This is the list of Emergency numbers, that when dialed will allow the OpenScape SBC to identify an Emergency Call.

Emergency Calling Subnets

Opens a new window where it is possible to configure the emergency calling subnets.

IP address or subnet / Logical-Endpoint-ID (Dynamic IP) - This configures the IP address (or range of IP addresses) or the Logical-Endpoint-ID (Dynamic IP) of the subscriber(s).

Subnet mask - This configures the IP subnet of the range of subscribers defined by the IP Address configuration. If a single subscriber is configured use mask 255.255.255.255.

Routing prefix - This configures a preferred gateway to be used by this emergency subnet. The first digits of each prefix also links the current Subnet to a dialed Emergency Number. For example, prefixes like "91122" or "91133" restrict the Subnet to be used with a configured "911" EmergencyNumber.



“Send LIN instead of CPN” – **DO NOT** use this option. Routing of emergency calls should be based on “Default core location domain name” as configured in the “remote Location Identification/ Routing” section of the “Remote endpoint configuration” with coordinated configuration of “Emergency Calling Subnets” on the OpenScape Voice.

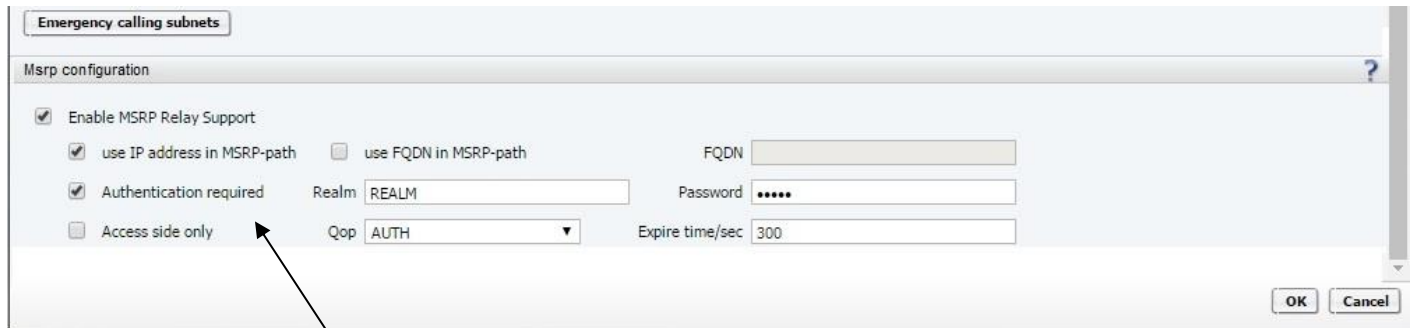
Note: OS SBC recognizes the NG911 emergency call and supports multipart MIME body and the Content-ID and Message-ID Uniform Resource Locators.

The PIDF-LO in the message body of a SIP message is transparently passed through.

The Geolocation header fields specified in the OSCAR location conveyance specification are transparently passed through.

In case of missing location information, the OS SBC does not insert a Geolocation header or PIDF-LO.

The Message Session Relay Protocol is used for transmitting a series of related instant messages. The MSRP Configuration provisioning window is displayed with the following options.



The screenshot shows the 'Emergency calling subnets' window with the 'Msrp configuration' tab selected. The configuration options are as follows:

- ☒ Enable MSRP Relay Support
- ☒ use IP address in MSRP-path ☐ use FQDN in MSRP-path
- ☒ Authentication required
- ☐ Access side only
- Realm: REALM
- Password: *****
- FQDN: [empty field]
- Qop: AUTH
- Expire time/sec: 300
- Buttons: OK, Cancel

An arrow points from the 'Access side only' checkbox to a yellow box containing detailed descriptions of the configuration options.

Enable MSRP relay support: Checkbox for enabling MSRP relay support.

use IP address in MSRP-path: Checkbox for using IP in the MSRP-path

use FQDN in MSRP-path: Checkbox for using FQDN in the MSRP-path.

FQDN: This is the Fully Qualified Domain Name to be used in the MSRP-path

Authentication required: Checkbox for selecting whether authentication is required or not.

Realm: Realm to be used in the authentication challenge on both sides of the path - Access and Core.

Password: Password to be used on both sides of the path through the OSS.

Access side only: Checkbox for selecting whether authentication is in the access side only.

Qop: Select the Quality of protection.

Expire time/sec: Expire default maximum and minimum values. Min: 60, Max: 3600

Enable routing based on domain

The screenshot shows a web browser window titled "SBC-DAN - Remote endpoint configuration - Google Chrome". The address bar shows a "Not secure" warning and the URL "21.21.100.198/remoteEndpointConfiguration.html?name=SSP_DAN&status=false&standalone=false". The page title is "Remote endpoint configuration". A message at the top states: "Select OK to temporarily store changes. Make your changes permanent by selecting 'Apply Changes' on the General page." The main configuration area is titled "Remote Location Identification/Routing". It contains the following fields and controls:

- Core FQDN**: A text input field.
- Core realm port**: A text input field with the value "50198".
- Default core realm location domain name**: A text input field.
- Default home DN**: A text input field.
- Enable routing based on domain**: A checked checkbox.
- FQDN**: A text input field with the value "branch1.bt.com".
- Incoming Routing prefix**: A text input field with the value "123". To its right are "Add" and "Delete" buttons.

Below this section is the "Digest Authentication" section, which includes:

- Digest authentication supported**: An unchecked checkbox.
- Digest authentication realm**: A text input field.
- Digest authentication user ID**: A text input field.
- Digest authentication password**: A text input field.

Next is the "Access Side Firewall Settings" section, which includes:

- Enable Firewall Settings**: A checked checkbox, with a "Firewall Settings" button next to it.

Below that is the "Emergency configuration" section, which includes:

- Emergency numbers**: A text input field with "Add" and "Delete" buttons.
- Emergency call routing**: A button.

At the bottom is the "MSRP Data Configuration" section, which includes:

- Enable MSRP Relay Support**: An unchecked checkbox, with a "(not licensed)" status indicator.

The Windows taskbar is visible at the bottom of the screen, showing the Start button, a search bar, and several application icons. The system tray on the right shows the date and time as "08:01/06".

This configuration applies when the endpoint is an SSP. It allows the incoming calls to be routed according to the destination FQDN present in the To header. When enabled, a unique FQDN can be assigned to the SSP, which will be used as selection criteria when more than one SSP is associated with the same SIP Service Provider. This configuration disables the incoming routing by prefixes.

3.4.5.5.1 Remote Location Domain

Remote Location Domain ⓘ

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

General ⓘ

Remote URL ☐ Shared domain Logical ID Code

Remote port

Remote transport

Signaling ⓘ

INVITE No Answer timeout (msec)

INVITE No Reply timeout (msec)

TLS ⓘ

TLS mode

Certificate profile

☐ TLS keep-alive

Keep-alive interval (seconds)

Keep-Alive timeout (sec)

Media Configuration ⓘ

Media profile

Media realm subnet IP address

Outbound Proxy Configuration ⓘ

Outbound Proxy

Outbound Proxy Port

Registrar Server Configuration ⓘ

Registrar Server

Registrar Server Port

Remote URL - URL of the remote endpoint or domain. The URL can be entered as IP address (IPv4/IPv6), as domain (FQDN or domain name) or as Logical-Endpoint-ID. By using DNS SRV (domain name) the remote port is automatically set to 0. The port configuration is received by DNS SRV.

Remote SIP/MGCP port - Defines the port to be used in communication with the endpoint.

Remote transport - Defines the transport protocol to be used in communication with the endpoint. For a Media Server endpoint, Transport must be UDP.

Logical ID Code (only visible if the “signaling address type” = “dynamic IP”) - Previews the Logical ID hash code for the Remote URL.

INVITE No Answer Timeout (msec) - Final response timeout (in milliseconds) to an INVITE request that has not received a final reply. Range is 120000 to 600000 milliseconds. Default is 360000.

INVITE No Reply Timeout (msec) - Timeout (in milliseconds) for an INVITE request or a non-INVITE transaction that has not received a provisional response. Range is 1000 to 32000 milliseconds. Default is 3000 msec.

TLS mode - Allow the selection between Server Authentication, Mutual Authentication and Client Mode (valid only if transport type is TLS).

Certificate profile - Select the TLS certificate profile.

TLS Keep-Alive - Enable the keep-alive mechanism if the connection was established by the SBC as TLS client.

Keep-Alive interval (sec) - Determines the interval between sending the keep-alive requests. Valid values: 60 - 3600 seconds, default: 120.

Keep-Alive timeout (sec) - Determines how long the TLS client shall wait for the keep-alive response before considering the TLS connection to be broken. Valid values: 5 - 120 seconds, default: 10.

Media profile - Select a Media Profile which is configured with the Media protocol, codecs, and packetization interval suited for the remote subscriber.

Media realm subnet IP address - Some endpoints do not use the same address for SIP and media (RTP) and can also use different subnet and network interfaces. This parameter is optional and is used to identify the endpoint in terms of media address.

Outbound Proxy - URL of the outbound proxy. The URL can be entered as IP address (IPv4/IPv6), as domain (FQDN or domain name). If configured, the SIP messages are sent via outbound proxy to the remote endpoint.

Outbound Proxy Port - Defines the port to be used in communication with the outbound proxy.

Registrar Server - URL of the registrar server. The URL can be entered as IP address (IPv4/IPv6), as domain (FQDN or domain name). If configured, this address is used to populate the SIP Request-URI and other header fields of the REGISTER request.

Registrar Server Port - Defines the port to be used in communication with the registrar server.

3.4.5.6 Transcoding

This section allows enabling of what codecs are supported for the purpose of transcoding. They can then be assigned for use in media profiles. (GUI → Media → Media profiles)

Features

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

Features configuration

- ☒ Enable Remote Subscribers **Configure**
- ☒ Enable Remote Endpoints **Configure**
- ☒ Enable Codec Support for transcoding **Configure**
- ☐ Enable TURN Server **Configure**
- ☒ Enable Circuit Telephony Connector **Configure**
- ☐ Enable Sip Load Balancer **Configure**
- ☐ Enable Border Control Function **Configure** (not licensed)
- ☐ Enable Push Notification Service **Configure**
- ☐ Enable Ganglia Monitoring Daemon
- ☒ Enable Circuit Zookeeper Client
- ☐ Enable THIG

Codecs

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

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

OK Cancel

The available codes are:

- G.711 PCMA/PCMU
- G.729 AB Functions
- G.722 Sub-Band ADPCM Speech Codec Functions
- Support media transcoding with webrtc lib (or equivalent) for codecs:
 - OPUS
 - iLBC
 - iSAC

3.4.5.7 Enable THIG

In order to integrate the OpenScape SBC into the OpenScape Enterprise Express (OSEE) as a core application, the THIG (stands for Topology Hiding Interworking Gateway) feature is enabled, using the Enable THIG checkbox.

The integration of the OS SBC into the OSEE is to introduce support for:

- Topology hiding. Provide only one point of access to the OSEE Solution.
- Provide Fixed IP address schema for OSEE Core applications (OSV, UC, Xpressions, OSCC, OSCC-E, DLS, OSTM)
- Allow the deployment of Virtual Appliances for OSEE Core Applications
- Reduce the number of IP addresses that should be reserved on customer LAN
- Provide extra firewall security for OSEE Core applications
- Easy transformation to Voice Redundancy Systems

When THIG is enabled, the way that SBC handles the NAT is changed to provide the THIG functionality. So instead of changing the source IP as its own IP, THIG will bypass the IP and just change the port according to port forwarding rules. That way network elements will point to SBC WAN address as destination and the package will be forwarded to LAN preserving the original Source IP address. All network packages of LAN interface with the destination not belonging to the subnet of originating address will see SBC THIG as destination since it's the network gateway. SBC THIG will forward the package to WAN using its own WAN address, the network elements on the WAN will not even notice that they are not talking directly to the destination.

IMPORTANT: For OS-4K deployments, THIG is disabled

The port forwarding rules along with the rest of the THIG configuration are provided by WebCDC during the initial staging.

3.4.5.8 Enable Standalone

For Openscape Cloud the standalone SBC is a remote endpoint of type and profile as SBC configured at TRUNK-SBC as in the example below.

Remote endpoint configuration

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

Remote Endpoint Settings

Name

SBC6000-SA-OSV

Edit

Type

SBC

Profile

SBC

Access realm profile

Main-Access-Realm - ipv4

Core realm profile

Main-Core-Realm - ipv4

Associated Endpoint

☐ Enable Call Limits

Maximum Permitted Calls

0

Reserved Calls

0

Remote Location Information

☐ URI based routing

☐ Enable access control

signaling address type

IP address or FQDN

Remote Location domain list

Add

Edit

Delete

At OSV the configuration is as any other regular SBC the SIP port just have to match the core port of remote endpoint configured in the TRUNK-SBC corresponding to the Stand Alone SBC.

[WoWarcraft] - [BG_RD_OSB_OSSBC] - [Main Office] - Edit Endpoint : SBC6000-SA-OSV

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: SBC6000-SA-OSV

Remark:

Registered: ☒

Profile: EP_RD_OSB50i_113 ...

Branch Office: ...

Associated Endpoint: ...

Default Home DN: ...

Location Domain:

Endpoint Template: ...

Endpoint Type: Central SBC

Max number of users:

Last Update: 2018-05-16 18:28:02.0

In the Stand Alone SBC itself we have at least one endpoint that should point to the TRUNK-SBC endpoint as explained above, and a second endpoint that is used to connect to SSP or Gateway/Proxy, both endpoints as linked together as can be seen in the picture below (see endpoints blue colored). In a practical way this means that every call coming in the endpoint associated to SSP will go to endpoint of Standalone SBC on TRUNK-SBC on OpenScape Cloud and vice-versa.

Add Edit Delete

Name	Access realm profile	Type	Profile / Circuit ID	Remote IP address / Logical-Endpoint-ID / Circuit URL	Remote port	Remote transport	Associated Endpoint	Linked Endpoint	
SSP09	Main-Access-Realm - ipv4	SSP	Telefonica	192.168.105.27	5060	TCP		SBC6000-SA-OSV	
SSP01	Main-Access-Realm - ipv4	SSP	Telefonica	192.168.105.19	5060	TCP		SSP02	
SSP03	Main-Access-Realm - ipv4	SSP	Telefonica	192.168.105.21	5060	UDP		SSP04	
SSP04	Main-Access-Realm - ipv4	SSP	Telefonica	192.168.105.22	5060	UDP		SSP03	
SSP05	Main-Access-Realm - ipv4	SSP	Telefonica	192.168.105.23	5061	TLS		SSP06	
SSP06	Main-Access-Realm - ipv4	SSP	Telefonica	192.168.105.24	5061	TLS		SSP05	
SSP07	Main-Access-Realm - ipv4	SSP	Telefonica	192.168.105.25	5060	TCP		SSP08	
SSP08	Main-Access-Realm - ipv4	SSP	Telefonica	192.168.105.26	5061	TLS		SSP07	
SSP02	Main-Access-Realm - ipv4	SSP	Telefonica	192.168.105.20	5060	TCP		SSP01	
SBC6000-SA-OSV	Main-Access-Realm - ipv4	SBC	SBC	192.168.100.146	5060	TCP		SSP09	
SSP-fqdn1	Main-Access-Realm - ipv4	SSP	Telefonica	Standalone1.sbc.com.br	5060	TCP		SSP10	

3.4.5.9 Enable Turn Server

TURN Server and Relay settings

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

General

☐ Enable Standalone TURN Server

Max TURN Server UDP instances

Relay Port min

Relay Port max

TURN Network Realm

TURN REST API Separator

TURN Relay Server Security

☒ Require periodic re-authentication

Certificate Profile

Max allocate timeout (secs)

Static authentication secret

Secret authentication timeout (secs)

Per-user allocation quota

Total allocation quota

Per-session bandwidth quota (bytes per sec)

TURN Server and Relay settings Configuration

Enable Standalone TURN Server - Checkbox for enabling Standalone TURN Server

• **Max TURN Server UDP instances** - From 1 to max number of CPU's available.

• **Per-user allocation quota** - From 0 - 100 (0 means no limit)

• **Total allocation quota** -

With Telephony Connector disabled:

– Hardware type: Virtual OSS 6000 - Default: 200. Valid from 100 to 1000

– Hardware type: Virtual OSS 20000 - Default: 1000. Valid from 100 to 5000

With Telephony Connector enabled:

– Hardware type: Virtual OSS 6000 - Default: 200. Valid from 100 to 200

– Hardware type: Virtual OSS 20000 - Default: 1000. Valid from 100 to 1000

Per-session bandwidth quota (bytes per sec) - From 0 to 1000 bytes per sec. 0 means no limit.

TURN Network Realm - Valid FQDN

Enable REST API - The Turn Server will support a REST API interface to authentications for allocating and creating of media connections

TURN REST API Separator - This is the timestamp / username separator symbol (character) in TURN REST API. The default value is ':'.

Server NW realm - Select the interface realm from Settings.

Allow UDP - Checkbox for enabling the configuration of UDP

UDP Start port - Start port for UDP, will be incremented by one for each additional instance. Default value: 3478

Allow TCP/TLS -Checkbox for enabling the configuration of TCP/TLS

• **TCP/TLS port** - Default value:5349


Certificate Profile - TURN certificate profile

Max allocate timeout (secs) - Default value:60 sec. Range:10 - 60 sec

Static authentication secret - TURN Authentication secret string

Secret authentication timeout (secs) - Default value:86400. Range: 60-518400 sec

3.4.5.10 Enable Circuit Telephony Connector

 **Circuit Telephony Connector**

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

General

General Settings

☒ Enable On-Premise Circuit Telephony Connector

☐ Enable Hosted Circuit Telephony Connector

☒ Enable Dynamic Connector Registrations

☐ Enable Early Media

☐ Allow local re-invite handling

☒ Enable TCP Port reuse

Dynamic Reg Realm

Retry After (sec)

Initial Invite delay (sec)

Pre-SDP Codec

HTTPS Proxy IP

HTTPS Proxy Port

Telephony Connector status

TC running version [View Status](#)

Telephony Connector Common Settings

Certificate Profile (with Remote CA) [Open Certificate Management](#)

Circuit Telephony Connector URL (https)

Circuit Telephony Connector Configuration

General

Enable On-Premise Circuit Telephony Connector - Set Circuit Telephony Connector as On-Premise, the SBC is inside the customer private network (datacenter).

Enable Hosted Circuit Telephony Connector - Set Circuit Telephony Connector as Hosted, the SBC is inside the Circuit cloud

Enable Dynamic Connector Registrations -Dynamically create pairs of remote endpoints, each pair consists of a Telephony connector plus an SSP. The pairs are created using the first pair GTC.Trunk/SSP already present in the Remote Endpoint table as a reference but their fields are slightly different. The SSP used as a reference must have its profile named "dynregssp", the copies of this endpoint will be available for dynamic registration to OSBiz customers.

Dynamic Reg Realm - This field must contain the realm used by the gtcClient to execute the Login method "digest".

Retry - After (sec) - This configuration only has effect for dynamically registered OSBiz SSPs. This Item configures the Retry After header that will be informed in 503 replies to REGISTER messages. The 503 reply will be generated in case the system has an alarm due to high CPU Usage or high RAM usage. The valid range for this field is 30 to 650 sec, and the default value is 140 sec.

Enable TCP Port reuse (for dynamic Endpoints only) - When this flag is enabled, the TCP/TLS port used by remote endpoints to register dynamically in Telephony Connector will be reused by SBC to send messages to these remote endpoints.It requires the Enable Dynamic Connector Registrations flag enabled.

Enable Early Media - Enable the initial invite delay and pre-SDP Codec for incoming calls from Circuit Telephony connector.

Initial Invite Delay (sec) - Time in seconds to delay the initial INVITE from Circuit Telephony connector call. This time should be used to reduce the user perception of media setup delays in the media connection.

Pre-SDP Codec - Codec used to pre-define the codec selected by the called party in order to reduce the media changes for the Circuit client. It is recommended to adjust the codec, at least on the Announcement Servers to minimize the codec changes.

Allow local re-invite handling - Re-invite messages to Telephony connector will be handled locally if the media is not changed.

HTTPS Proxy IP - Configure the HTTPS Proxy IP

HTTPS Proxy Port - Configure the HTTPS Proxy Port

For **Circuit Telephony Connector** and **Clustered mode** a flag **Enable Cluster Server** can be configured. When set is possible to chose in a drop down menu a specific group of cluster (configured in the clustered Servers screen) to be bounded to that Telephony Connector Endpoint, meaning that the Circuit devices will use exclusively that cluster group configuration(not being affected by other cluster groups prefixes and priorities).

Telephony Connector Status

TC running version -Display the current running Circuit Telephony Connector version

IMPORTANT: Applied configuration in this window affects the Remote Endpoint configuration. Do not use both at the same time. The last configuration applied will be valid.

View Status- Click the View Status button. A new window will open to display the current status of Telephony Connector. The following parameters are displayed on the Telephony Connector status screen.

INFO: When Circuit Telephony Connector is enabled, the Telephony Connector status is shown

Status - Display the overall status, presenting the final indication of the TC functionality.

Circuit Tenant Company - Display the Circuit Tenant Company configured on Circuit.

Circuit Trunk Name - Display the Circuit Trunk Name configured on SBC.

Circuit Trunk Type - Display the Circuit Trunk Type. Dynamic trunks are presented as DYN.

Circuit Connectivity - Show information about the current connectivity with Circuit.

SSP Trunk Name - When in Hosted mode, display the associated SSP Trunk Name configured on SBC.

SSP Connectivity - When Hosted Circuit Telephony Connector and SSP connectivity check flags are enabled, the SSP status is displayed

Telephony Connector Common settings

IMPORTANT: The common connector settings no longer overwrite the url and certificate fields on the connector list. When a new connector is created, the url and certificate fields are used as default initial values for the connector

Certificate Profile (with remote CA) -Configures the Certificate for all GTC endpoints. The profile must have a Remote CA.

Circuit Telephony Connector URL (https)- Configures the Circuit URL for all GTC endpoints. Possible values:URL with maximum 255 characters.

Open Certificate Management - Launches the Certificate Management window.Refer to [Certificate Management](#)

3.4.5.11 Enable SIP Load Balancer

The SIP Load Balancer (SIP-LB) distributes the SIP traffic among a set of SBCs based on establishing a TCP / TLS connection (Round-Robin mechanism).TheSIP-Load Balancer is used in Circuit deployments as well as Cloud Telephony (OSV based) deployments. Once the Load Balancer is activated, the other SBC functionalities are disabled. Also the core realm settings are obsolete.

The SIP Load Balancer is checking the SBC availability in the cluster based on a background script sending ICMP pings to each of the configured SBC in the cluster. The pings will be send to all as "active" marked SBCs, whereas manually marked "in-active" (down) will not be pinged. If the ping is not responded the SBC will be marked as "down" in the Cluster configuration and the configuration file will be reloaded without influencing the existing connections.

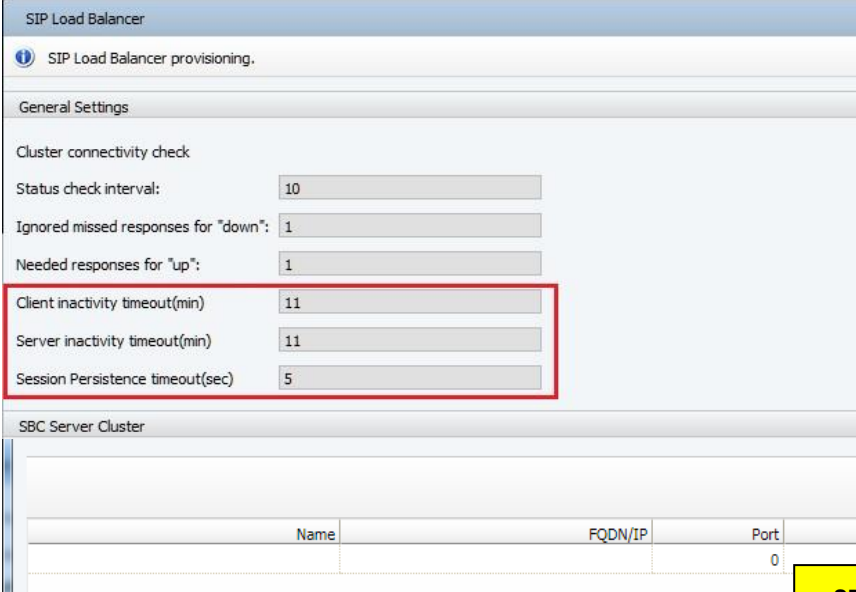
IMPORTANT: For OS-4K deployments, SIP Load Balancer is Disabled

The **HAProxy** Open Source is used as the main application for SIP-LB, providing a high availability Load Balancer and proxy server for TCP and HTTP-based applications.

For an SBC Server Cluster entry, the entry port is the port configurable as SIPTCP under **Network / Net Services > Settings > Interface Configuration > Access realm configuration**.

Requests coming in this port will be distributed to the IPs / FQDNs and ports configured in the Cluster settings.

INFO: The SBC port is used to check the SBC connectivity. SIP Load Balancer will send periodically iCMP messages to each pair address: port configured in the cluster.



SIP Load Balancer Configuration

General Settings

Cluster Connectivity check

Status Check interval - Range: 5sec - 60sec.Default value:10sec.

Ignored missed responses for "down" - Range: 1- 4. Default value:1

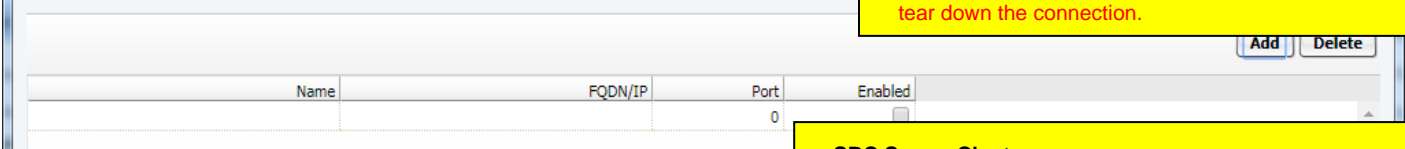
Needed responses for "up"- Range: 1- 4. Default value:1

Client inactivity timeout (min) - Set the value of the timeout for inactivity of the TCP connection at the client side (**HAProxy**). Range: 1- 60 min.

Server Client inactivity timeout (min) - Set the value of the timeout for inactivity of the TCP connection at the server side (**HAProxy**). Range: 1- 60 min.

Session Persistence timeout (min) - set the time that the data related to the connection between clients (Front-end) and the SBCs (Back-end) will remain on the Load Balance table

INFO:After the timeout, if no activity at TCP level was performed for the existing connections, HAProxy will tear down the connection.



SBC Server Cluster

INFO: You can add a total up to 100 servers

- Name - 24 alpha numeric characters
- FQDN/IP - 24 alpha numeric characters
- Port - 10 numeric characters
- Enabled - Default value: unchecked

Planning your load-balancing needs

- Determine how many trunks and users are required.
- Determine how many SBCs you will need for your SBC-SIP load-balancer (hereafter referred to as SBC-LB). For example, each SBC can handle up to 200 dynamic trunks. Each trunk belongs to a different tenant with multiple users.
- For documentation purposes, let us assume we are configuring one SBC-LB with two SBCs.

Planning your network

Assuming that the SBC-LB and SBCs are in a NAT'ed network, note down the following information and make a table if necessary, as shown, for reference.

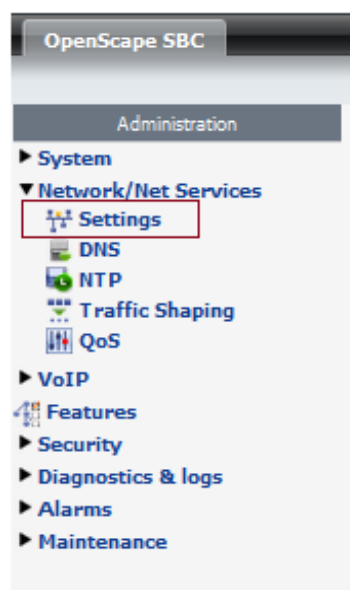
- LAN IP for management access of SBC-LB and the SBCs
- NAT IP address of the SBC-LB and the SBCs
- Public IP address of the SBC-LB and the SBCs ("External firewall IP")

- Port open for signaling (TCP) - Please note this information from the host provider's IP Firewall rules
- Port range open for UDP (RTP) - Please note this information from the host provider's IP Firewall rules
- External Firewall IP for "Signaling" will be the external firewall IP of the SBC-LB.
- External Firewall IP for "Media" IP of the SBCs will be the external firewall IP of the SBC itself.

	LAN(Core) -IP	WAN(Access) NAT IP	WAN(Access) External firewall IP	WAN signalin g TCP port	VOIP port range setting s for RTP	External IP Signalling	External IP Media
SBC -LB	10.20.200.8 2	10.20.100.82	80.157.193.193	23120	11000- 49999	80.157.193.19 3	N/A
SBC -1	10.20.200.8 6	10.20.100.86	80.157.193.125	23120	11000- 49999	80.157.193.19 3	80.157.193.12 5
SBC -2	10.20.200.8 7	10.20.100.87	80.157.193.196	23120	11000- 49999	80.157.193.19 3	80.157.193.12 5

Installing and configuring the SBC as a SIP(TCP) load-balancer [SBC-LB]

1. Download and install an SBC with version equal to greater than 09.00.06.01-1 from SWS
2. Please read [this](#) article about load-balancer.
3. Using the information from the above table, configure the SBC-LB
4. From the SBC management GUI Select "Network/Net Services"->Settings.



5. The above step will take you to the Network Services Window. Here, configure the Core and Access realm configuration as shown below. Click "OK". In the main window click "Apply Changes"

Network/Net Services

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

settingsLM DNS NTP trafficShapingLM 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

☐ Single armed

☐ Interface bonding

Interface Configuration

Core realm configuration

Type	Network ID	Interface	IP address	Subnet mask	Signaling	Media	SEP-UDP	SEP-TCP	SEP-TLS	HQCP
Main IPv4	Main-Core-IPv4	eth0	10.20.200.82	255.255.255.0	true	true	5060	5060	5061	2427

Access and Admin realm configuration

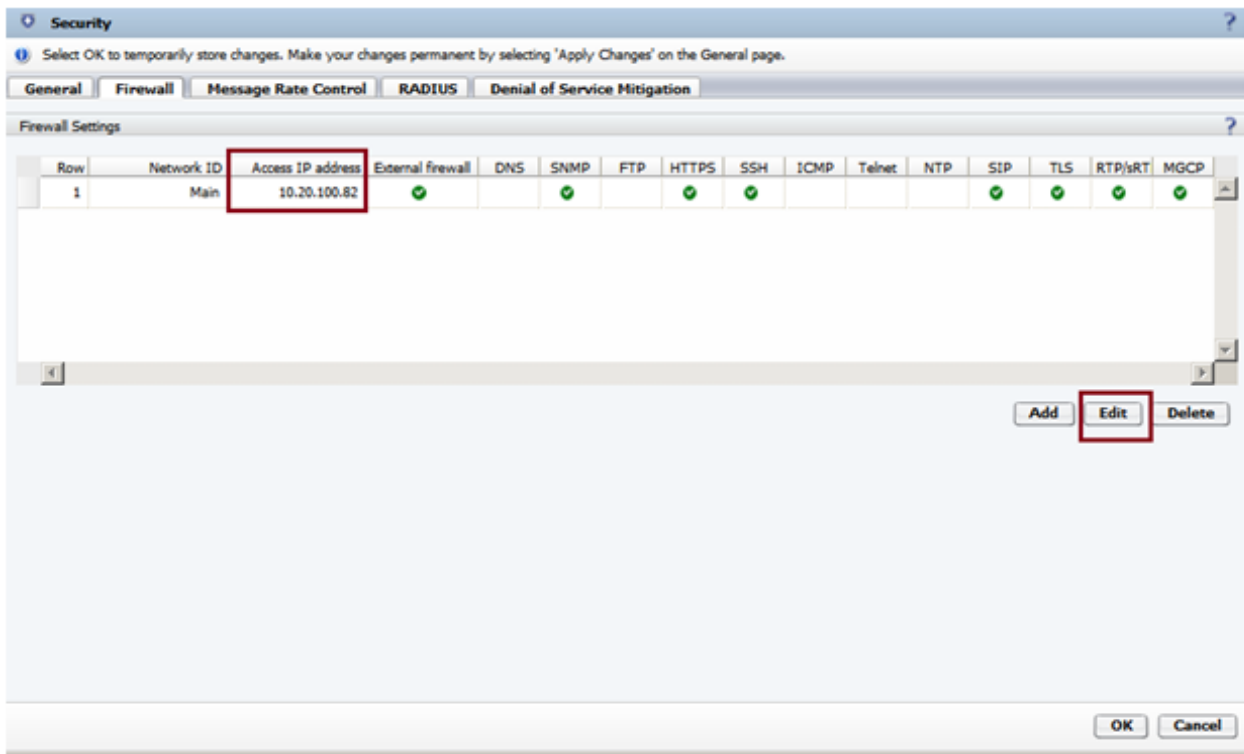
Type	Network ID	Interface	IP address	Subnet mask	VLAN tag	Signaling	Media	SEP-UDP	SEP-TCP	SEP-TLS	SEP-MTLS	HQCP	SP server	Message rate limit (sec)	Trust level	Signaling restriction	HTTP/VoIP	TURN server	TURN relay	STUN
Main IPv4	Main-Access-IPv4	eth0	10.20.100.82	255.255.255.0	0	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	65060	23120	65061	65161	2727	Node 1	100	N/A	Unrestricted	0	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

OK Cancel

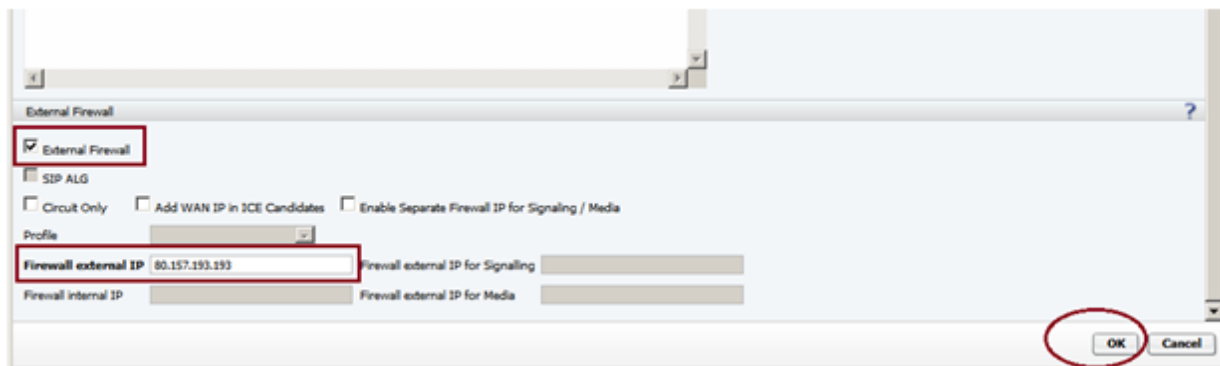
- When the Management interface has successfully applied the network settings. Click on the Security->Firewall configuration.



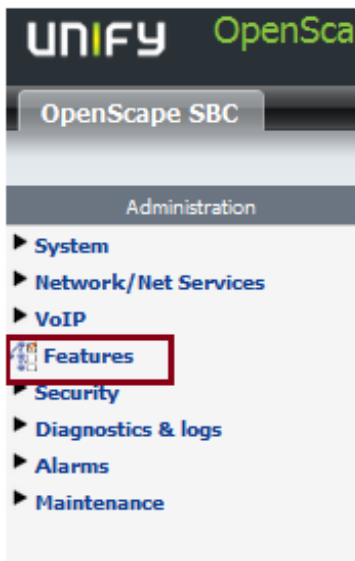
- This will open the "Firewall" tab of the security settings. Select the first and *only* item in the list and click "Edit".



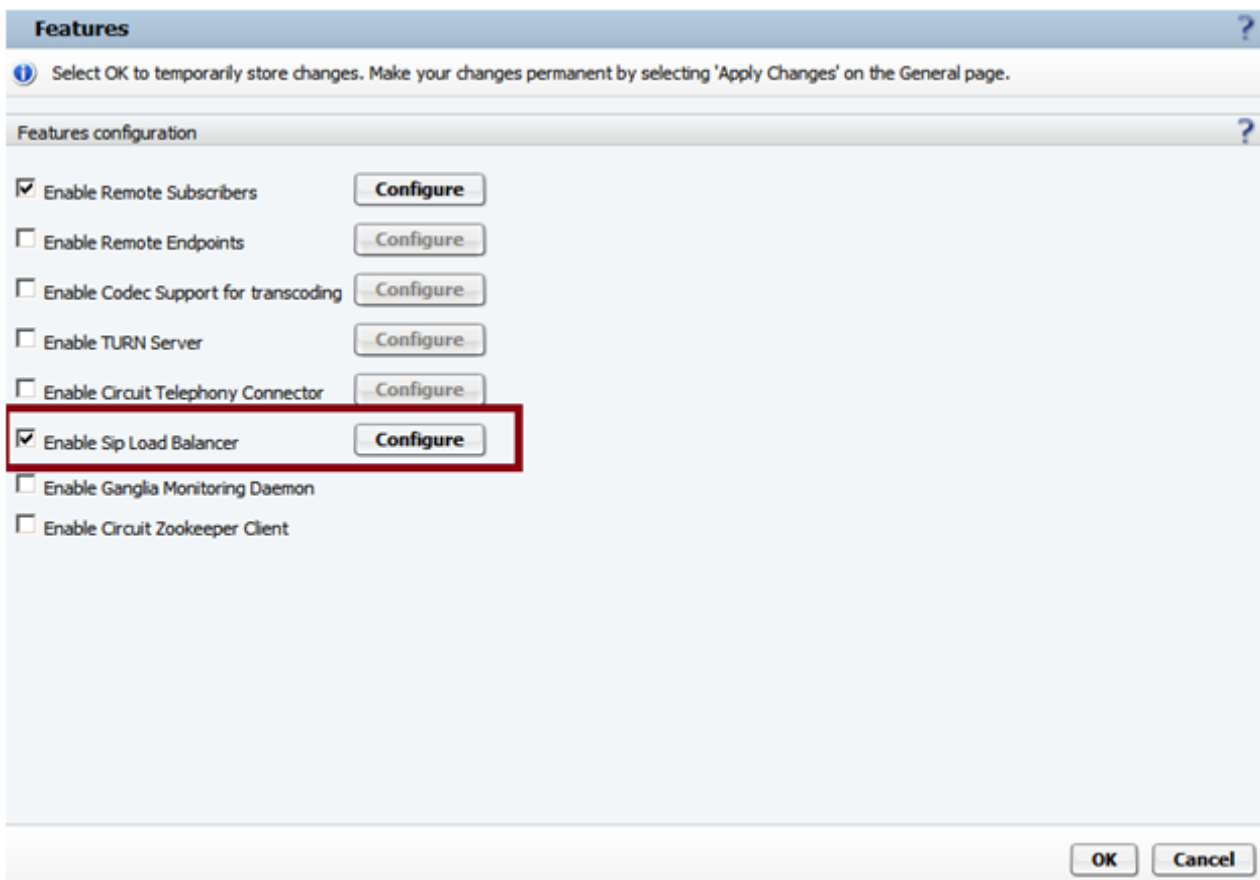
8. Scroll down to the section “External Firewall” . Check the box “External Firewall” . Add your public IP to “Firewall external IP” and click OK



9. This will take you back to the Security window. Click OK. In the main window click “Apply Changes”
10. When the Management interface has successfully applied the security settings, Select “Features”.



11. When the “Features” window opens Check the box “Enable Sip Load Balancer” and click “Configure...”



12. Within the load-balancer configuration window, add the IP address of the SBCs and make sure the WAN ports are entered correctly. Click “Save

SIP Load Balancer ?

! SIP Load Balancer provisioning.

General Settings ?

Cluster connectivity check

Status check interval:

Ignored missed responses for "down":

Needed responses for "up":

SBC Server Cluster ?

Name	FQDN/IP	Port	Enabled
SBC-06	10.20.100.86	23120	<input checked="" type="checkbox"/>
SBC-07	10.20.100.87	23120	<input checked="" type="checkbox"/>

13. Clicking "Save" in the above step will take you back to the "Features" Window. Here, please click "OK". On the main page, click "Apply Changes"
14. When the Management interface has successfully applied the Feature changes, go to the next steps to configure the SBCs. (If you checked the "SIP Loadbalancer status" at this stage, the connection will be down. You have to configure the SBCs)

3.4.5.12 Sip Enable Push Notification Service

The Push Notification Service feature supports sending Notifications to an Apple Push Notification Server and Firebase Cloud Messaging Server.

Push Notification Service

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

Registration

Register expire time (secs)

Register Hold time (days)

Outbound calls

Call hold time (secs)

☒ Send Session Progress (183) during hold time

Send Session Progress (183) after: (secs)

Notification Server (iOS)

Push Certificate Passphrase

Account Team Id

Mobile Application Bundle Id

Notification Server (Android)

Firebase Database URL

Security

☐ Disable certificate validation

Push Notification Service Configuration

Registration

Register expire time (secs) - Available options: 600-3600sec. Default value: 3600sec.

Register Hold time (days) - Default value: 1. Available options: 1-7 days

Outbound calls

Call hold time (secs) - When an INVITE is sent from OSV to OSMO client passing through SBC, this INVITE will be held and SBC will send a push notification to OSMO client in an Android/iOS device (in order to wake it up). After receiving the push notification at Android/iOS device, OSMO client sends an OPTIONS message to SBC which says that it is ready to receive VoIP calls, then the SBC releases the INVITE towards OSMO client. Default value: 5sec. Available options: 3-15sec

Send Ringing (180) during hold time - Enabled by default.

Send Ringing (180) after: (secs) - This is a timeout to wait for the OSMO message OPTIONS to arrive before sending backwards the 183 Session Progress to OSV.

Default value: 5 sec. Available options: 1-10sec.

IMPORTANT: Set to a value less than the value set in the OSV.

Notification Server (iOS)

Push Certificate Passphrase - it is the .p12 certificate key file or the .p8 token key file password.

Apple Account Team Id - when using a .p8 token key file, an Apple Account Team ID is required.

Mobile Application Bundle Id - the Mobile Application bundle ID to be used on push notifications (if VoIP is not used, suffix will add it on VoIP notifications). e.g. com.unify.iOSMO

Notification Server (Android)

Firebase Database - Must be filled with the client Firebase Database URL in case of user certificate upload. Otherwise, there is no need to change, because it already has a default value.

INFO: APN Push Notification API uses Push Server Port 443 by default.

3.4.5.13 Enable Ganglia Monitoring Daemon

Ganglia monitoring allows several metrics being retrieved from OpenScape SBC periodically. This is used in Circuit deployments where the OpenScape SBC node health is constantly checked. The daemon is already pre-configured to accept connections from monitoring system, so no further settings is necessary.

3.4.5.14 Enable Circuit Zookeeper Client

Zookeeper client is used in Circuit deployments where the OpenScape SBC configuration is stored in the Management Node and is pushed to SBC

3.4.6 Security

3.4.6.1 Certificate Management

The System Certificate has the default Certificate Profile configured and the default certificates are associated with them:

- System TLS certificate: OSV Solution
- HTTPS certificate profile: HTTPS System Default
- Media DTLS certificate profile: Not Configured
- IOS Push certificate profile: IOS Push Default
- Android Push certificate profile: Android Push Default
- Service API certificate profile: Service API Default

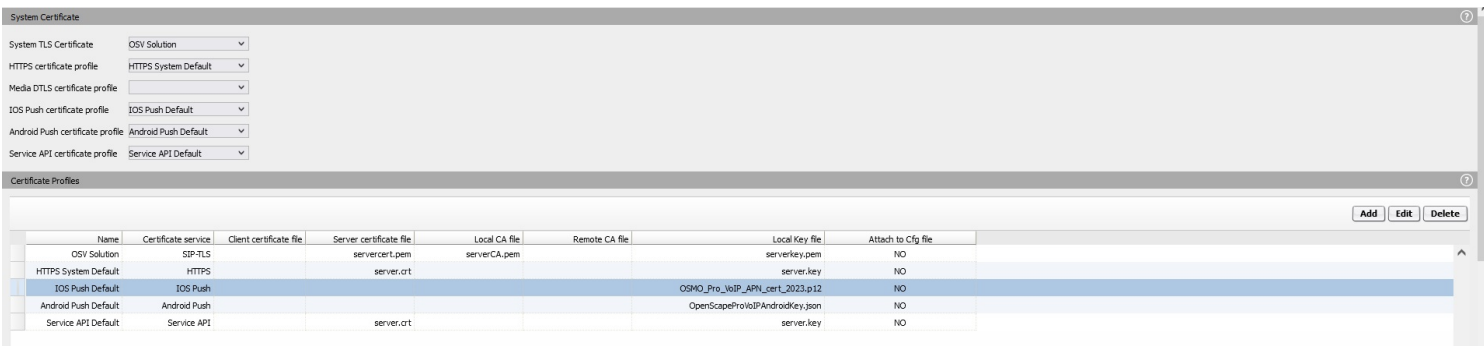
Note: For OSMO the default client credentials are configured in IOS Push certificate profile and Android Push certificate profile.

Note: When the new certificate is released in SBC version, the IOS Push certificate or Android Push certificate will be updated automatically only when the previous certificate is configured in the profile "IOS Push Default" or "Android Push Default".

For example: If the current certificate used on the profile "IOS Push Default" is OSMO_Pro_VoIP_APN_cert_2023.p12, after upgrading to V10R3.2.0, it will be automatically replaced by the OSMO_Pro_VoIP_APN_cert_2024.p12 certificate.

If the OSMO_Pro_VoIP_APN_cert_2023.p12 certificate is used in another IOS Push certificate profile, it will not be updated automatically; In such case, It is mandatory to manually change this certificate to the new OSMO_Pro_VoIP_APN_cert_2024.p12 certificate (in "Local Key file" column) and **Apply Changes**.

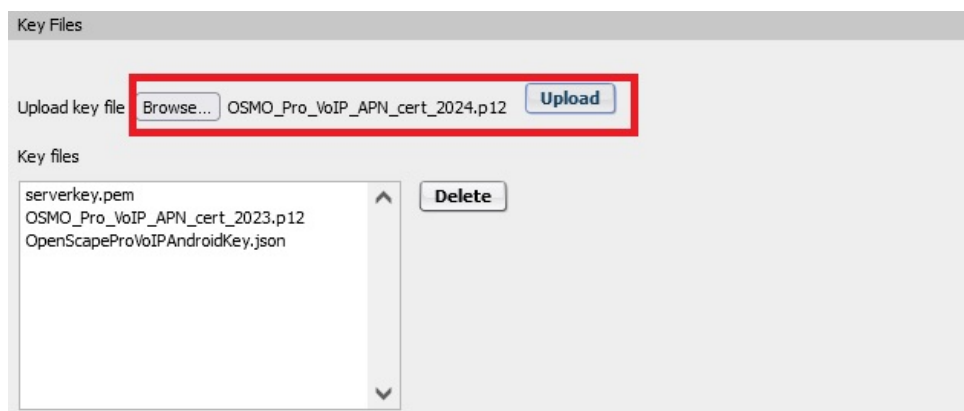
If you need to upload a new certificate, navigate to the **Security->General->Certificate Management** page. There you will find the default profile and certificate of the feature. For example the new IOS Push certificate:



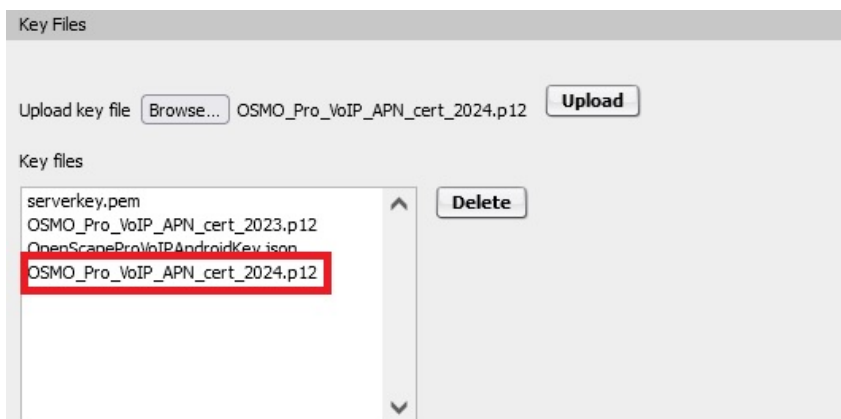
The screenshot shows the 'System Certificate' configuration page. At the top, there are dropdown menus for 'System TLS Certificate' (OSV Solution), 'HTTPS certificate profile' (HTTPS System Default), 'Media DTLS certificate profile' (empty), 'IOS Push certificate profile' (IOS Push Default), 'Android Push certificate profile' (Android Push Default), and 'Service API certificate profile' (Service API Default). Below this is the 'Certificate Profiles' section, which contains a table with columns: Name, Certificate service, Client certificate file, Server certificate file, Local CA file, Remote CA file, Local Key file, and Attach to Cfg file. The table lists several profiles, with the 'IOS Push Default' profile highlighted in blue. This profile is associated with the 'IOS Push' service and has 'OSMO_Pro_VoIP_APN_cert_2023.p12' in the 'Local Key file' column. Other profiles include 'OSV Solution', 'HTTPS System Default', 'Android Push Default', and 'Service API Default'.

Name	Certificate service	Client certificate file	Server certificate file	Local CA file	Remote CA file	Local Key file	Attach to Cfg file
OSV Solution	SP-TLS		servercert.pem	serverCA.pem		serverkey.pem	NO
HTTPS System Default	HTTPS		server.crt			server.key	NO
IOS Push Default	IOS Push					OSMO_Pro_VoIP_APN_cert_2023.p12	NO
Android Push Default	Android Push					OpenScopeProVoIPAndroidkey.pson	NO
Service API Default	Service API		server.crt			server.key	NO

Scroll down to the **Key Files** section.
Click **Browse** to select the new file.
Click **Upload** to upload the new **Local Key** file.



If the upload is completed successfully, the new certificate will be listed in the **Key files** section.



In the **Certificate Profiles** section, select the profile you want to edit, and then click **Edit**.



A new **Certificate profile** pop-up window is displayed.
Select the new certificate in the **Local key file** option. Press **OK** and, in the main page, click **Apply Changes**.

The screenshot shows the 'Certificate Profile' configuration window. The 'Certificate profile name' is 'IOS Push Default'. The 'Certificate service' is 'IOS Push'. The 'Local client certificate file', 'Local server certificate file', 'Local CA file', and 'Remote CA file' are all set to empty, with 'Show' buttons next to them. The 'Local key file' dropdown is open, showing a list of certificates: 'OSMO_Pro_VoIP_APN_cert_2024.p12' (highlighted with a red box), 'serverkey.pem', 'OSMO_Pro_VoIP_APN_cert_2023.p12', and 'OpenScapeProVoIPAndroidKey.json'. The 'EC param' is 'serverkey.pem'. The 'Attach to Config file' is 'OSMO_Pro_VoIP_APN_cert_2023.p12'. The 'Validation' section is empty. The 'Certificate Verification' is 'None'. The 'Renegotiation' section has 'Enforce TLS session renegotiation' checked and 'TLS session renegotiation interval (minutes)' set to '60'. The 'TLS version' section has 'Minimum TLS version' set to 'TLS V1.2'. The 'DTLS version' section has 'Minimum DTLS version' set to 'DTLS V1.0'. The 'Cipher Suites' section has 'Perfect Forward Secrecy' set to 'Preferred PFS' and 'Encryption' set to 'Preferred AES-128'. The 'OK' button at the bottom right is highlighted with a red box.

The new configuration will restart the Push Notification service.

3.4.6.1.1 Certificate profile configuration:

Pressing the **Show** button near each certificate/CA file opens a new screen with a view of the certificate fields.

Certificate profile name – Name of certificate profile

Certificate service – There are two selections to indicate if the certificate profile service is SIP-TLS or VPN. For the default profile, only SIP-TLS is allowed.

Local client certificate file – Local client certificate field is used only for Mutual Authentication. It is used when establishing a TLS connection as TLS client. As this field is optional, if the Local client certificate is not configured, the Local server certificate shall be used.

Local server certificate file – This certificate file is used when establishing a TLS connection as TLS server.

Local CA file – This is the CA file with the root CA certificate which signed the local certificates.

Remote CA file – This is the CA file for path validation of the certificate received from the remote endpoint. This is required only when a remote endpoint uses a different certificate issuer.

Local key file – This file contains the private key

EC param - Elliptical Curve which is used with ECDH and ECDHE cipher suites. This parameter is hardcoded with value secp256r1

Attach to Config file - If set, the certificate file defined in **Remote CA file** will be saved/restored to/from the xml configuration file. Available only if **Remote CA file** is filled up.

Certificate validation – Checking this box enables validation of the CA chain and CA signature, Validity Period, and Critical Extensions.

Revocation status – This checkbox enables verification of revoked certificates according to CRL of the CA.

Subject authentication – Checking this box enables validation of certificate Subject CN or Subject Alternative Name according to the configured remote endpoint FQDN or IP address

Enforce TLS session renegotiation - This checkbox indicates if renegotiation of an established TLS session is enabled for the endpoint.

TLS session renegotiation interval (minutes) – This field indicates how long a negotiated key is valid in a TLS connection. Valid values are between 15 and 1440 minutes, the default value is 60 minutes.

Certificate Profile

TLS version

Minimum TLS version

TLS V1.0

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

Minimum TLS Version:

Indicate the minimum version supported. Available options are TLS V1.2, TLS V1.1 and TLS V1.0.



Note: For security reasons SSLv23 and SSLv3 are not supported after V9R1



Note: 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.

Minimum TLS Version Configured in SBC/OSB	TLS Version in Remote Endpoint as Client	SBC as TLS Server	SBC 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	

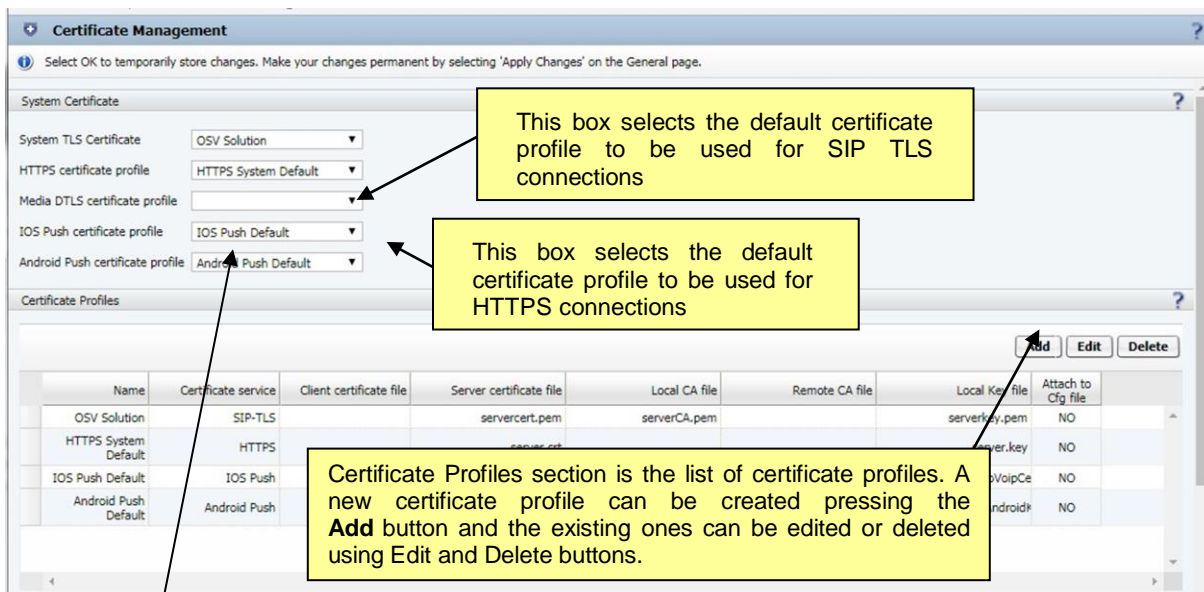
	SSLv23/SSLv3	Reject	
--	--------------	--------	--

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 Without PFS.
- 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.

3.4.6.1.2 Creation of certificate profiles using local GUI:



Media DTLS certificate profile : This box selects the default certificate profile to be used for Media DTLS connections. If the option Media DTLS certificate profile was chosen under Certificate service, the supported **DTLS version** is configurable.

IMPORTANT: An invalid DTLS certificate can cause rtpproxy failure. Additional certificate validation protection is planned to next release. If not setting Media DTLS configuration, rtpproxy uses the default internal certificate.

The number of security certificate profiles were increased from 5 to 50 for small OS SBC models and from 10 to 100 for medium and large OS SBC models. (Folder Security General → Certificate Management → Certificate Profiles). The SIP Trunks can be added using different certificate profiles.

3.4.6.1.3 Create/Upload TLS Certificates for OpenScapeSBC (Using openssl)

Purpose: Secure communication between the OpenScape SBC and all other security enabled products.

Certificate format: PEM – Key not encrypted.

The OpenScape SBC is installed with certificates signed using the default root CA certificate of OSV which contains certificate and private key.

Following certificates are required

- ossservercert.pem
- ossserverkey.pem
- serverCA.pem
- ossclientcert.pem (optional)

Note: The ossclientcert.pem file is designed for users who distinguish the usage of their certificates between server and client only connections. This requires the server.pem certificate contain an extended key usage setting for “TLS Web server authentication” or extension nsCertType =server and for client.pem to contain an extended key usage setting for “TLS Web client authentication” or extension nsCertType=client. In practice, most people do not set these values, or they contain both values. This allows the certificate to be used for both purposes. If you did not set these values or do not know then simply copy server.pem to client.pem.

Generate CSR and Install New Certificates

Create CSR and sign with CA and install the certificates in OpenScapeSBC. Refer to [Generate a Certificate Sign Request file \(CSR\)](#) and Install the CA generated certificate in OpenScapeSBC.

Note: The default OSV CA certificate (root.pem) shall be used only for Lab test purpose where user wants to change certificate parameters (eg: adding DNS or IP) for OpenscapeSBC or to avoid recreating certificates for all other devices in the lab network. Refer to [CHANGE CERTIFICATE PARAMETERS FOR OSS DEFAULT CERTIFICATE](#).

Note: OpenScape SBC accept only certificate in pem format. If the certificate is in different format refer [Converting certificate format](#) to pemformat.

Reference: For more details refer **Certificate Management and Transport Layer Security (TLS) for OpenScape Solution Set V10** at E-Doku.

After all three files are uploaded, create your profile using certificates profile section. Please refer to [Creation of certificate profiles using local GUI](#):

3.4.6.1.4 Saving current security files if replacing an OS SBC



If you are going to completely reload or replace a working OS SBC which has non-default security files, they must be saved before reloading the current OS SBC.

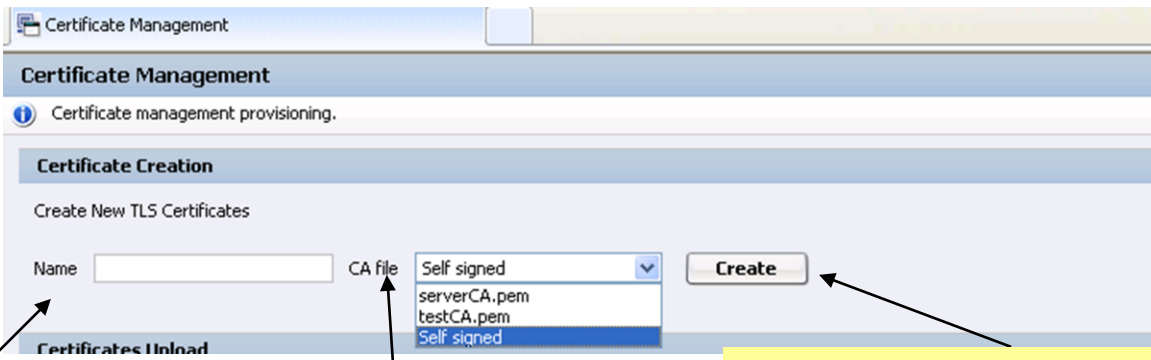
The saving of the xml will save the certificate profiles but not the files they refer to, so the user should save/restore these files using the following procedure.

1. Use SFTP to save the contents of /etc/openbranch/ssl to a secure location.
2. after the new device has been loaded restore the saved files to the same location on that new device.

3.4.6.1.5 Creation of certificates using local GUI:

New certificates with self sign CAs (Certificate Authority) or based on existing CAs can be created using the “Certificate Creation” section of the Certificate Management screen on the local GUI.

Local GUI → Security → General → Certificate management



Name - Indicates the name of the certificate which will be created.

CA file - Allows the selection of a CA file used to sign the certificate that is being created. If CA file option 'Self Signed' is chosen, all 3 files are created: CA Certificate file, X.509 Certificate file and Key file.

Create – A new certificate is created based on name and CA selection.
Certificate files can only be created based on a CA file with certificate and key.

Certificates generated using GUI will be created with default parameters of OpenscapeSBC.

If you want to create the certificate with different company information and FQDN/IP in subject Alt Name, you need to create it using the openssl command.

If extra parameters for certificate creation are required, please refer to Create/Upload TLS Certificates for OpenScapeSBC (Using openssl).

3.4.6.1.6 Downloading of certificates using local GUI:

The certificates and key files can be downloaded from the system using the local GUI.

Certificate Download

Certificate file: serverCA.pem [v] [Download]

Key file: serverkey.pem [v] [Download]

Certificate file - A certificate file (CA or X.509) can be downloaded browsing an entry in the Certificate file list and using the download button.

Key file - A key file can be downloaded browsing an entry in the Key file list and using the download button.

Certificate Expiration Checking

Certificate expiration warning period (days): 60

Certificate expiration warning interval (days): 7

Certificate expiration time of day (hh:mm): 00:00

Certificate expiration warning period (days) - The number of days before a certificate expires at which an alarm is generated to warn the administrator about the impending expiration of the certificate. The valid values are between 0 and 300 days, and the default value is 60 days.

Certificate expiration warning interval (days) - The number of days after when to repeat the Certificate expiration warning alarm. The valid values are between 0 and 60 days, and the default value is 7 days.

Certificate expiration time of day (hh:mm) - The time of day at which to run the certificate expiration check. The valid values are between 00:00 and 23:59, and the default value is 00:00.

NOTE:

OpenScope SBC supports X.509 Certificates with Digital Signature using hash algorithm SHA-2 (SHA-256) for SIP over TLS, HTTPS and IPSec

Due to backwards compatibility OS SBC will keep supporting certificates signed with SHA-1

It is possible to define a Certificate Profile for each Remote Endpoint.

One certificate profile can be defined for HTTPS

3.4.6.1.7 Certificate Revocation Configuration

Certificate Revocation

Certificate Revocation configuration.

Certificate Revocation Configuration

Name

CRL URL

Manual update

CRL download interval (hours)

24

CRL short download interval (minutes)

60

CRL time of day (hh:mm)

00:00

Name - Internal name for reference of certification revocation list for root CA. CRL URL – The URL from which the CRL file can be downloaded.

Manual update – This button allows the download of the CRL from the configured URL and uploads the CRL to the system. A manual update can be performed only after the CRL configuration is applied to the system.

CRL download interval (hours) – This interval defines the maximum time between two CRL downloads. If this interval is set to 0, the Next Update field is used instead for the automatic CRL downloads. The valid values are between 0 and 168 hours, and the default value is 24.

CRL short download interval (minutes) - This is the interval at which a CRL check will occur in case of a download of a CRL fails. The valid values are between 15 and 1440 minutes, and the default value is 60 minutes.

CRL time of day (hh:mm) - Time of day at when to start the CRL check. This variable is only checked if the CRL download interval is 24 or a multiple of 24. The valid values are between 00:00 and 23:59, and the default value is 00:00.

3.4.6.2 Users/Password Recovery/Change

Local GUI→Security → General → Passwords - Change/Reset password

☒ Account Enabled

User name

administrator

Privilege

Administrator

Expires (days)

99999

☒ SSH login

Change password

Reset password

Press the **Reset password** button to set the password to default for the selected user.

Default users/passwords for OS-SBC:

User: administrator, Password: Asd123!
User: service, Password: BF0bpt@x
User: assistant, Password: 2GwN!gb4

User: root, Password: T@R63dis
User: guest, Password: 1cIENtk=
User : redundancy, Password Asd!.123



For security purposes it is recommended to change **ALL** passwords from their defaults as delivered with a new system.



Warning: In case you change the redundancy password on the master node and have a collocated redundant OSS system, the information gets updated after data synchronization. No change is necessary in the backup node.

3.4.6.3 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.

	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"/>

Administrator Account

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

Administrator Profile

☒ Account Enabled

User name:

Password:

Confirm password:

Privilege:

- Administrator
- Network Administrator
- Security Administrator
- Network and Security Administrator
- Read Only

Expires (days):

☐ SSH login

☒ Change Password in first login

OK Cancel

Administrator Profile

Account enabled - This flag is used to grant login rights (SSH and Management Portal) to users. Enabled by default.

The flag is disabled & grayed out for assistant & redundancy users.

User Name - User name of the Administrator account.

Password - The password for the Administrator account user name.

Confirm Password - Confirm & verify the Administrator account user name password.

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

Expires (days) - The password expiration timeslot. Possible values: **7 -99999.**

SSH login - Login to the Linux open source application that allows data to be exchanged using a secure channel between two networked devices. Disabled by default.

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

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.

3.4.6.4 SIP/SDP Information Filtering

- **"Warning Info on Error Responses removal"** - will remove Warnings 399 and 488 Header from SIP messages
- **"Internal names and additional headers removal"** - will remove the UA names, server names and X-Siemens headers from SIP messages

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

Certificates
?

Certificate management

Administrator Accounts
?

Add
Edit
Delete

	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"/>

SIP/SDP Information Filtering
?

☐ Warning info on Error Responses removal
☐ Internal names and additional headers removal

Advanced
?

☒ Accept only Video Calls from Peer Domains

OK
Cancel

3.4.6.5 Advanced

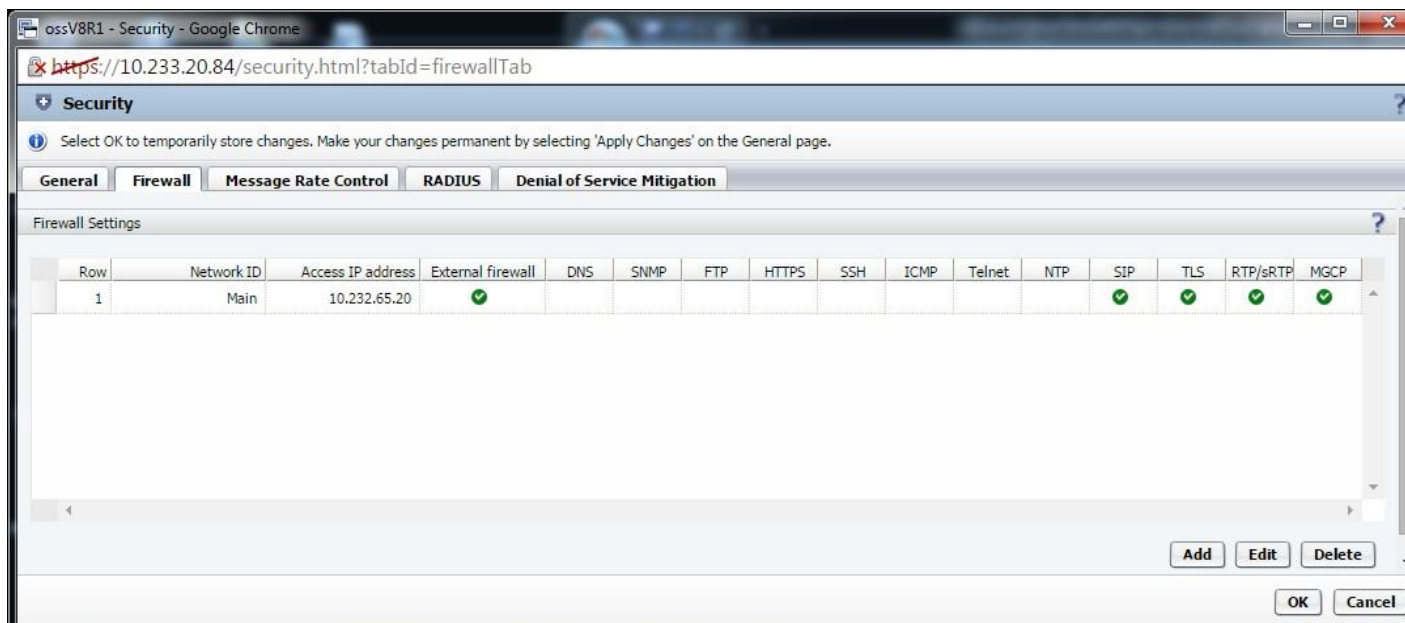
Accept only Video Calls from Peer Domains: When this flag is enabled, only INVITE messages containing a video m-line in the SDP is accepted from calls coming from the Access side (WAN) if Support Peer Domains or Support Foreign Peer Domains is the endpoint to be used. When no video m-line is received in the INVITE message, the call is rejected. You can change this behavior by disabling this flag. This flag is enabled by default.

3.4.6.6 Firewalls

3.4.6.6.1 Internal firewalls

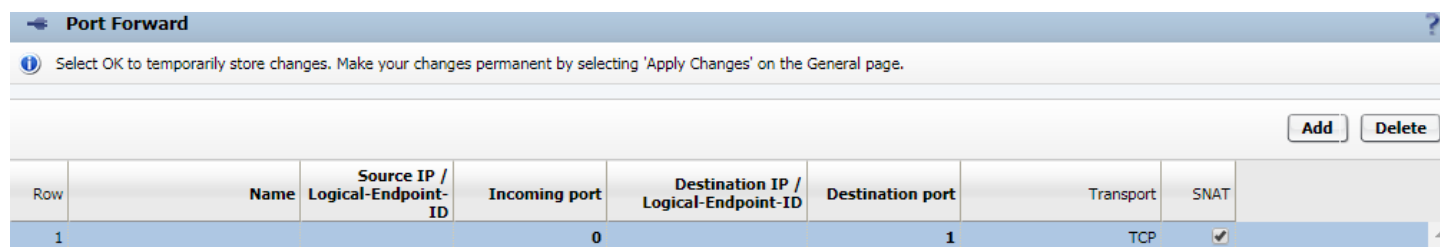
Each “Network Id” may have individual firewall

Local GUI → Security → Firewall



3.4.6.6.2 Port forwarding

Local GUI → Security → Firewall → Select the network and Edit → Enable Port Forwarding → Configure



SNAT: this flag indicates that SBC acts as network gateway for the specific rule.

It is not recommended to activate port forwarding for a port which is equal to a default listening port set up on the OSS.

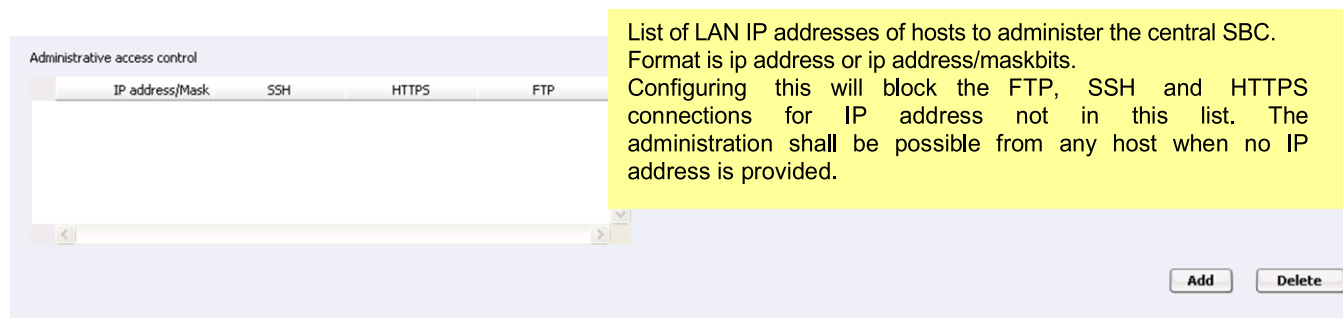
If port forwarding is administered for a TCP connection it will not take affect till the TCP connection is reestablished.

Currently port forwarding is only effective from the WAN interface (as the source) to the LAN interface.

An example of a use for port forwarding is the OpenScope desk top client using port 8443 to communicate with the CMP via the OS-SBC. OpenScope desktop functions.

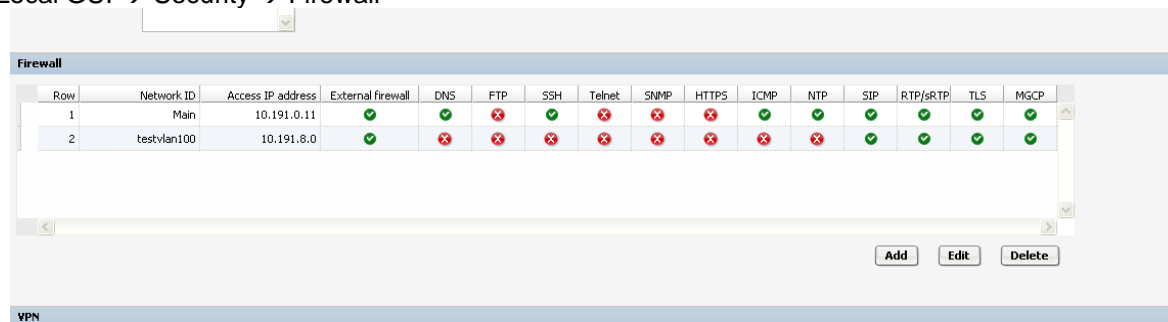
3.4.6.6.3 Administrative Access Control

Local GUI → Security → Firewall → Select the network and Edit → Administrative Access Control → Add



3.4.6.6.4 WAN Interface External firewalls TCP non TLS

Local GUI → Security → Firewall



- There may be an external firewall for each Network ID address (VLANs)
- Enabling the external firewall does NOT disable the internal firewall.

Local GUI → Security → Firewall → Add

The screenshot shows the 'Firewall Configuration' window in a web browser. The window title is 'ossV8R1 - Firewall Configuration - Google Chrome'. The address bar shows a URL starting with 'https://10.233.20.84/firewall.html?'. The main content area has a header 'Firewall Configuration' and a sub-header 'Firewall configuration provisioning.' Below this, there are several options: 'External Firewall' (checked), 'SIP ALG' (unchecked), and 'Circuit Only' (checked). There is a 'Profile' dropdown menu. Below these are two input fields: 'Firewall external IP' with the value '65.222.73.102' and 'Firewall internal IP' which is empty. Two callout boxes are present: one at the top right stating 'When the **External Firewall** flag is checked, the parameter Firewall external IP must be configured.' and another on the right side listing features: '“External firewall” - when enabled, the IP address of firewall shall be used in the SIP headers and SDP towards access side instead of the SBC access IP.', 'SIP ALG - for future use.', 'Circuit Only – New feature', 'Profile - for future use.', 'Firewall external IP - the public IP address of external near end firewall.', and 'Firewall internal IP - the internal IP address of external near end firewall towards SBC (for future use).'. At the bottom right are 'OK' and 'Cancel' buttons.



Use routing configuration (GUI→ Network /Net Services → Settings → Routing configuration to ensure messages intended for the public side of the firewall use the private or core side of the firewall as a gateway.

Configuration of the external firewall is beyond the scope of this document. Please refer to the configuration guide for each individual type of firewall used.



When configuring an external firewall, “rules” must be defined to allow messages, related to services, to pass in both directions. These services include but are not limited to:

- TCP
- UDP
- MGCP
- DNS



The firewall must **NOT** be SIP aware or MGCP aware.



For messages being sent from the WAN side to the “core” side, the concept of **port forwarding** is required. (The message sent to the external side of the firewall, from an external device, should be forwarded to the WAN of the OS-SBC with the same port as in the original message.

See [Table A: Fixed/Configurable Port Information](#) for information on dynamic ports used by the OS-SBC.



Note: The values shown in the table are default values and may have been modified for security reasons. If so, corresponding changes will be required in the port forwarding “rules” of the firewall.



** If there is an external firewall on the WAN interface, the number of ports required to be open can be calculated as follows: $\text{number of sessions} \times 5$ gives the number of required ports to be opened. $100 \times 5 = 500$, Min Port ==55000 Max Port==55499

Limited information on the Fortigate 310B is available in [Appendix FortiNet Firewall model 310B Version 4 non TLS](#)



Provisioning devices “outside” the firewall.

Devices outside the firewall must communicate with the OS-SBC via the firewall.

For example: On phones the fields for “SIP server address” , “SIP registrar address” need to be the external address of the firewall, not the WAN address of the OSS. *These devices can not communicate directly with the OSS.*

For branches outside the firewall “Node 1” and “Node 2” “primary” and “backup” server addresses must be this external firewall address.

If the DNS used by these devices is on the core side of the firewall, the fields “primary DNS” and “secondary DNS” must point to the firewall.

When the firewall is correctly configured, the firewall will “forward” messages from the remote device to the OSS.



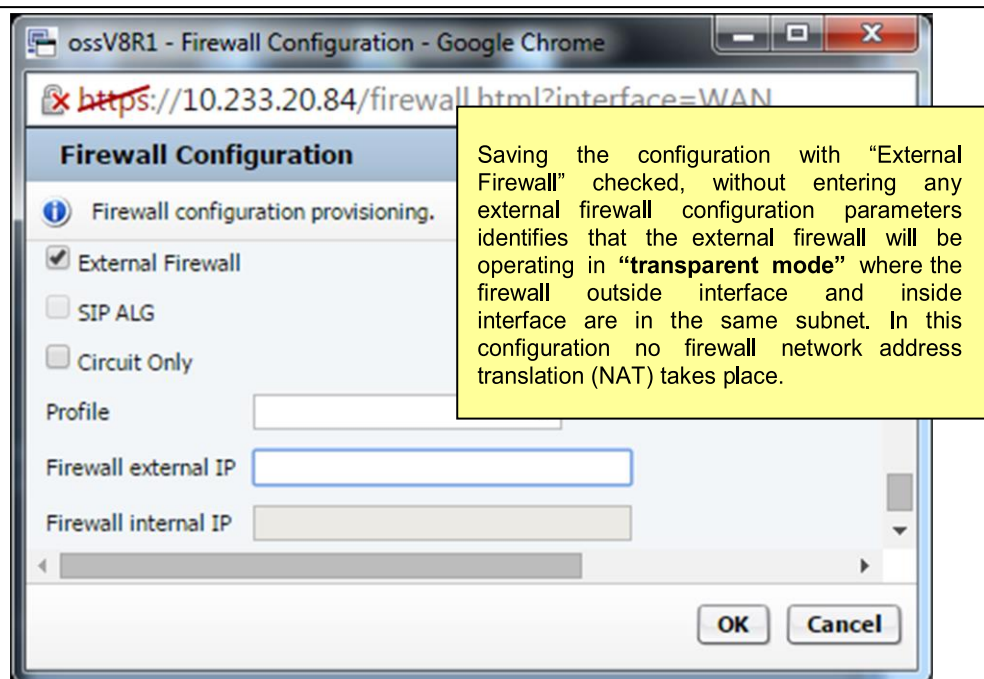
Using a firewall within the internal network.

If a customer DMZ is used within the internal network requiring a separate firewall interface, it is required that this firewall operate in “transparent mode”, i.e., without any NAT.

3.4.6.6.5 WAN Interface External firewalls support of TLS

For this configuration the Firewall must have the following attributes:

- ALG must be enabled.
- SIP and MGCP helpers must be disabled
- The firewall must work in the transparent mode



This information is based on FortiGate FW 5.0(build3608).

Limited information on the Fortigate 310B is available in [Appendix FortiNet Firewall model 310B Version 5 TLS](#)

3.4.6.7 Message Rate Control

When Message Rate Control is enabled and Message Rate Threshold is reached, Message Rate Control 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.

The user must configure a Message Rate Control threshold value for VoIP operation following one of the procedures below:

1. The Message Rate Control threshold of 20000 must be used during system upgrades if the network server interface IP address used for performing the file uploading during system upgrade cannot be identified. Once the system upgrade is complete, the Message Rate Control limit of 20000 must be lowered to the VoIP PPS threshold (recommended value of 300).
2. The Message Rate Control threshold is configured to the VoIP PPS threshold (recommended value of 300) and all network interface(s) used for the system upgrade file upload are configured in the Message Rate Control white-list. By placing these network interface address(es) into the white-list, they are not subject to any packet filtering with Message Rate Control.
3. If the user finds that calls are still being blocked by Message Rate Control (check the Firewall & Msg Rate Control log – Diagnostics & Logs → Debugging → select the Firewall & Msg Rate Control log → show), the user will need to either increase the limit for blocking or add the IP address which is being blocked to the white list.

Message Rate Control Settings

☒ Enable Message Rate Control

Message rate threshold: 20000

Block period (sec): 60

White list:

10.232.1.127

Add Delete

This window lists all IPs which will **not** be blocked by Message Rate Control.

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

3.4.6.8 RADIUS

RADIUS Settings

☐ Enable RADIUS

	Address:	Port:	Secret:	Timeout (sec):
Server 1:			
Server 2:			

☐ Enable RADIUS Authentication

Apply To: ☐ CLI ☐ SSH ☐ WEB

☐ Enable RADIUS Accounting

Apply To: ☐ CLI ☐ SSH ☐ WEB

The Address field may be a IP or FQDN.

If the port field is left blank the default value of 1812 is used for authentication and the authorization port+1 is used for accounting.

The secret field **must be** 16 characters.

The timeout field is optional with a default value of 3 seconds with a valid range of 1-10 seconds.

Note: CLI refers to login from the console, SSH refers to login via utilities like Putty, WEB refers to login via https session.

3.4.6.9 Denial of Service Mitigation

Dynamic Blacklist

☐ Block unauthorized users Unauthorized user quarantine interval (sec) 300

☐ Block unknown users Unknown user quarantine interval (sec) 300

☐ Process initial registration

☐ Enable gateway message rate limit

Trust Level Quarantine Intervals

Minimal (sec) 60

Medium (sec) 10

User Agent Allowed List

User Agent

**If the Agent allowed list is empty, all agents are allowed.
If there is any entry on the Agent Allowed list then any agents to be allowed **MUST** be on the list.**

Dynamic Blacklist

- **Block Unauthorized users**

If the checkbox is enabled, upon receiving a “401 unauthorized” response from the OSV, the response is forwarded to the SIP UA. The OS-SBC must supervise subsequent SIP REGISTER messages from the same SIP UA’s Source IP. If three (fixed) successive failure attempts occur, it is flagged as “User Authentication Violation” which leads to quarantining the violating Source IP for the **Unauthorized user quarantine interval**. A “403 Forbidden” response is returned to the offending endpoint instead of forwarding the “401 unauthorized” response.

- **Block Unknown users**

If the checkbox is enabled, upon receiving a “404 Not Found” response from the OSV to a SIP REGISTER message, a “403 Forbidden” response with a Warning is returned to the offending endpoint instead of forwarding the “404 Not Found” response.

The OS-SBC shall flag the occurrence as an “Unknown User Violation” which leads to quarantining the violating Source IP for the **Unknown user quarantine interval**.

- **Process initial registration**

If the checkbox is enabled, the initial SIP REGISTER message received from a SIP UA without a valid OS- SBC contact address binding is allowed to proceed as normal towards the SIP server. Otherwise, if not checked, a 503 Server unavailable is returned.

- **Unauthorized user quarantine interval**

Quarantine interval for unauthorized users.

Valid range: 60 to 36,000 seconds (default: 300sec.)

- **Unknown user quarantine interval**

Quarantine interval for unknown users.

Valid range: 60 to 90,000 seconds (default: 300sec.)

- **Enable gateway message rate limit**

By default the checkbox is unchecked. When checked (feature enabled) the system applies message rate limiting and quarantining according to the configuration of the OS-SBC Access SIP listening IP:Port address.

The message rate limit is configured via GUI in **Network/Net Services -> Settings** and **Admin realm configuration**.

- **Trust Level Quarantine Intervals**

An array of quarantine interval settings is administered under this section

- **Minimal** - default is 60 seconds; integer of range 60-3600
- **Medium** - default is 10 seconds; integer of range 10-3600

User Agent Allowed List

This will allow only requests which have a "User-Agent" Header which matches with the allowed user agent list. The Validation shall not take place if the Allowed User Agent List is empty or notpresent.

1. Each user agent shall be in a separate line. For Example
OpenStage Polycom Tandberg Lifesize
2. The user agent can be specified to match exactly or partly.
 - a.) For an exact match with the user agent name, use \$ sign as suffix to the word
For Example
Polycom\$ - This will exactly match the user agent name Polycom, not PolyCom-V1.
 - b.) To match a user agent starting with a prefixname.
For Example
Polycom - This will match the user agent name PolyCom-V1 and PolyCom-V2

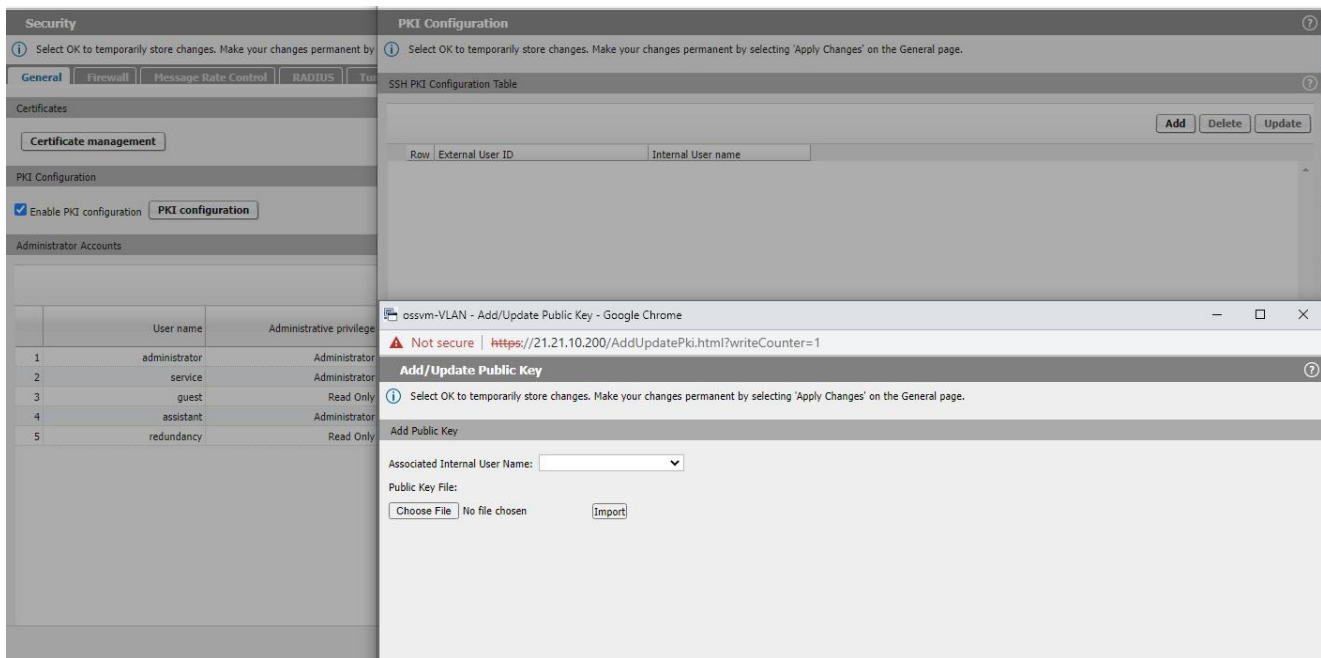
Note: The Denial of Service mitigation can be overridden by Firewall White List or Message Rate Control White List.

3.4.6.10 PKI Configuration for SSH

Configuration of PKI for SSH allows external users to log into other systems, such as PCs or other Linux servers, to execute scripts or other commands on an OpenScope SBC without having to explicitly log into the OpenScope SBC using a password. This is achieved by storing the external user's public key on the OpenScope SBC.

In order to configure a PKI for SSH follow the steps below:

1. Check the checkbox **Enable PKI Configuration**.
2. Click **PKI Configuration**.
 - ➔ A new PKI Configuration screen is displayed.
3. Click on the **Add** button.
 - ➔ A new **Add/Update Public Key** screen is displayed.
4. Select from the **Associated Internal User Name** dropdown list the internal user (administrator or service) to which the key will be associated.
5. Click **Choose File** to select the public key file and click **Import** to import it.
6. Apply the configuration.



3.4.7 Diagnostics & Logs

3.4.7.1 Settings

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.

The screenshot shows the 'Diagnostics & logs' configuration window. It has tabs for 'Settings', 'Debugging', 'Continuous Tracing', 'On Demand Trace', and 'Statistics'. The 'Settings' tab is active, showing fields for 'Log size (kbytes)' (1024) and 'Syslog server'. Below are 'Log Levels' for various services: Alarm Manager (Error), Logging Client (Error), Continuous Tracing (Error), Survivability Provider (Error), Media Server (Error), Process Manager (Notice), Redundancy (Notice), RTP Proxy (Error), SIP Server (Error), SSM (Error), QoS Application (Error), GTC App (Notice), ZooKeeper Client (Error), SIP Service Provider (Error), and BCF NIF (Error), BCF LIF (Error). There is a checkbox for 'Signature on Log Files' and a 'Signature Key' field. The 'Fallback' section has a checked checkbox for 'Fallback to default log level' and a 'Fallback time (hh:mm)' field set to '01:06'. The 'Call Log Settings' section includes checkboxes for logging call details (started from number, to destination number, initiated from remote address, received on host address, for SIP methods) and a checkbox for 'Invert SIP Methods match'. At the bottom, there are checkboxes for 'REGISTER', 'OPTIONS', 'NOTIFY', and 'SUBSCRIBE'. Arrows point from yellow callout boxes to specific settings: 'Signature on Log Files', 'Fallback time (hh:mm)', 'Log for SIP methods', and 'Invert SIP Methods match'.

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: SIP Server Info and Debug level will produce the ↑same output.

This flag is used to provide an MD5 signature to the compressed log files that are exported or internally stored.

↑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.

This setting upgrades the log level to DEBUG for applications SIP Server, SSM, and RTP Proxy, based on each criterion selected.

Log Data	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 the Alarm manager application. Useful when an alarm is not being triggered, a false alarm is being activated or not cleared accordingly.
Boot	Log of the last system boot. It is useful to debug problems of processes or driver modules not being correctly installed and, to identify hardware failure indications. Additionally, it provides system capabilities are correctly detected and configured.
Continuous Tracing	Continuous trace is the application that collects the logs from the applications does the log rotation, compression and aging.
Current Processes	A list of the current processes running on the SBC.
Denial of service	The log will show hosts that sent DoS messages and are blocked by the system.
Firewall & Msg Rate Control	This log contains the details of packets that are blocked by the Firewall and Msg Rate control.
GTC App	Logs for the GTC Client application, which are needed for troubleshooting failures related to phone calls to/from Circuit.
GTC Database	Logs for the database application which is mainly used to coordinate GTC applications. They are only needed when database errors is reported by any application that utilizes it.
GTC Loader	Logs for the GTC Loader application, which are needed for troubleshooting failures related to GTC Client auto-update procedures.
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.
Media Server Adapter	Log of Media server, MGCP Adapter and SIPMGCP converter applications.
Process Manager	Log of the Process Manager application responsible for the system sanity monitoring and also for license management. It includes processes status checking and starting or stopping them if applicable. It is also responsible for the configuration deployment, it includes the fallback to previous system partition when there is an upgrade issue, the configuration is not valid or the current system partition is corrupted.
Push Notification	The logs related to notifications to an Apple Push Notification Server and Firebase Cloud Messaging Server.
QoS Application	This is the log of QoS send TRAP application that sends over SNMP the QoS information to the QDC server that monitors the quality of voice calls.

QoS Monitoring	This is the QoS data that was collected for the voice calls.
Redundancy	This log show details about the redundancy manager application. It is useful to debug issues related to redundancy process functionalities, like switchover failures.
Registration Blacklist	This table stores the subscribers that try to register but fails due not configured or wrong credentials.
RTP Proxy	The RTP Proxy is the component responsible to relay RTP packets between different interfaces and some VoIP features interworking like transcoding, transrating, SRTP, ICE, STUN, etc. RTP Proxy logs are useful debugging issues involving these features, specially voice quality issues, DTMF, FAX T.38, rtcp-mux, etc.
Simplified Installation	The log of simplified installation is similar to the installation tool logs but in this case the installation procedure uses the easy install concept where the software and the system configuration is done almost with no intervention from the user.
SIP Server	SIP Server is a Kamalio application running in the system. It provides the SIP signaling, being always the system external SIP interface. This log is useful to debug call processing issues, SIP connection issues and many other problems in registration, port mapping, number modification, DNS, NAT, Options Heartbeat, etc.
SIP Service Provider	This log shows details about the SSPs Registration process.
SSM	SSM works together with SIPserver, it's used to provide some SIP functionalities and interworking with SIP Service providers. Usually their logs are needed for call failures related to SSPs, MoH for subscribers on SM, SipRec, call using anchored SBC sessions i.e. codec transcoding.
Sip Load Balancer	The logs related to Sip Load Balancer issue.
Survivability Provider	Log of the Survivability provider application. This application is responsible for the OPTIONS heartbeat functionality, that indicates the system operational mode (SM, NM, etc). This application is also responsible for SSP registration and BCF Notifications functionalities.
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.
System	This log contains the Kernel logs. Useful to debug operational system and device drivers (sensors, ethernet, etc) related issues.
Turn Server	These are the logs of the Turnserver which is the application that implements Traversal Using Relays around NAT (TURN) which is used to allow multimedia applications to traverse the NAT and or firewalls of customer network.
Web Server	Log of the local web server application. Useful to debug the local management, GUI interface and XML issues.

Note: After activating ssm trace (Level ERROR or DEBUG), the SBC removes all active registered subscribers due to tcp connections reset. All subscribers are registered again.
The, to debug already existent calls activates the ssm trace via commands:
ssmctl trace_on level=7
ssmctl trace_off"


3.4.7.2 Debugging

The screenshot shows the 'Debugging' tab of the OpenScape SBC V10 Configuration Guide. The interface is divided into three main sections: 'Log Viewer', 'Debugging Tools', and 'Rapid Stat'. The 'Log Viewer' section has a 'Log data' dropdown menu set to 'Alarm History', with 'Show', 'Clear', and 'Clear all logs' buttons. The 'Debugging Tools' section has a 'Tool' dropdown menu set to 'ICMP', an 'Options' text input field, 'Start' and 'Stop' buttons, and 'Results' with 'View' and 'Export' buttons. The 'Rapid Stat' section has an 'Info level' dropdown menu set to 'Level 2' and a 'Get file' button.

Settings	Debugging	Continuous Tracing	On Demand Trace	Statistic
Log Viewer				
Log data: Alarm History Show Clear Clear all logs				
Debugging Tools				
Tool: ICMP				
Options: <input type="text"/>				
Start Stop				
Results: View Export				
Rapid Stat				
Info level: Level 2 Get file				

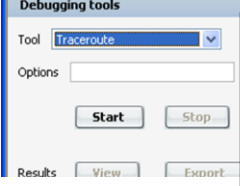
User can select a logfile and **Show** it, or **Clear** the selected logfile. While "showing" a file, the user may export the data to a save file. It is also possible to **Clear All** logfiles. **Note: certain logfiles are read only and can not be cleared (ex. Alarm History, Boot log)**

The user has access to ICMP, Traceroute, and Network Tracer debugging capabilities.



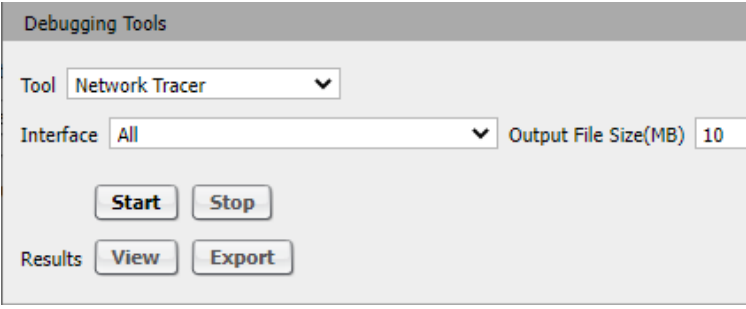
ICMP: can have its own options entered in "Options" box. In this case the minimal option is one IP address. The given options are not parsed, because the user may want to configure some specific ping options

Example
 Network: **10.234.2.11/255.255.255.0**
 Field value: "**10.234.2.11 -b**"



TraceRoute: can have its own options entered in "Options" 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**"



Network Tracer: A 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 will be created as *.pcap. The user can also select the maximum file size. The size should range between 1MB and 100MB. **Only Applicable to the option "All".**

Note: Ethereal or Wireshark is required to open the Network Tracer file.

Tracing with TLS: The user can collect decoded network traces by selecting the "SIP/MGCP/Q931 trace" option from the Network Tracer Menu. System collects decoded TLS traces from OS-SBC with this option.

The SIP/MGCP trace option is used to capture network trace in the application level. (SIP and MGCP protocols are shown as UDP messages. Q931 is shown as TCP and is only applicable for Integrated Gateway.)

Use the SIP/MGCP/RTP trace option to capture RTP for debug of speech problems.

Rapidstat: tool that collects system information for system debugging.

s

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 Level 5 to report problems against the OS-SBC.

According to the level the following information will be stored in the compressed file:

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, Survivability Provider logs + Level1.

Level 3 – audit logs + Level ½.

Level 4 – Management logs + Level 1/2/3.

Level 5 – Media server logs + Rapidstat Level 1/2/3/4

Log data: SIP Server [Show] [Clear] [Clear all logs]

Rapid Stat

Info level: Level 2 [Get file]

Administer: Level 1, Level 2, Level 3, Level 4, Level 5

[Restart] [Restart to backup]

Debugging tools

Tool: ICMP

Note: Select **Level** and **Get File**. After a few seconds user has the option to open/save/cancel collected "sys_info.tar" file.
Note: Rapidstat will not include OSVTM traces files available on disk (ex. SIP/MGCP Wireshark)

3.4.7.3 Continuous tracing

Continuous Tracing user can configure a trace manager server (OSVTM) so that traces/logs are captured 24x7. Log level categories are set under Log Settings (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

Continuous Tracing

☒ Enable

Server: 10.232.1.158 System name: sbctest03prim

File size threshold (kbytes): 256 SFTP username: tracedata

Time interval threshold (min): 5 SFTP password:

SIP/Q931 trace: ☒

MGCP trace: ☒

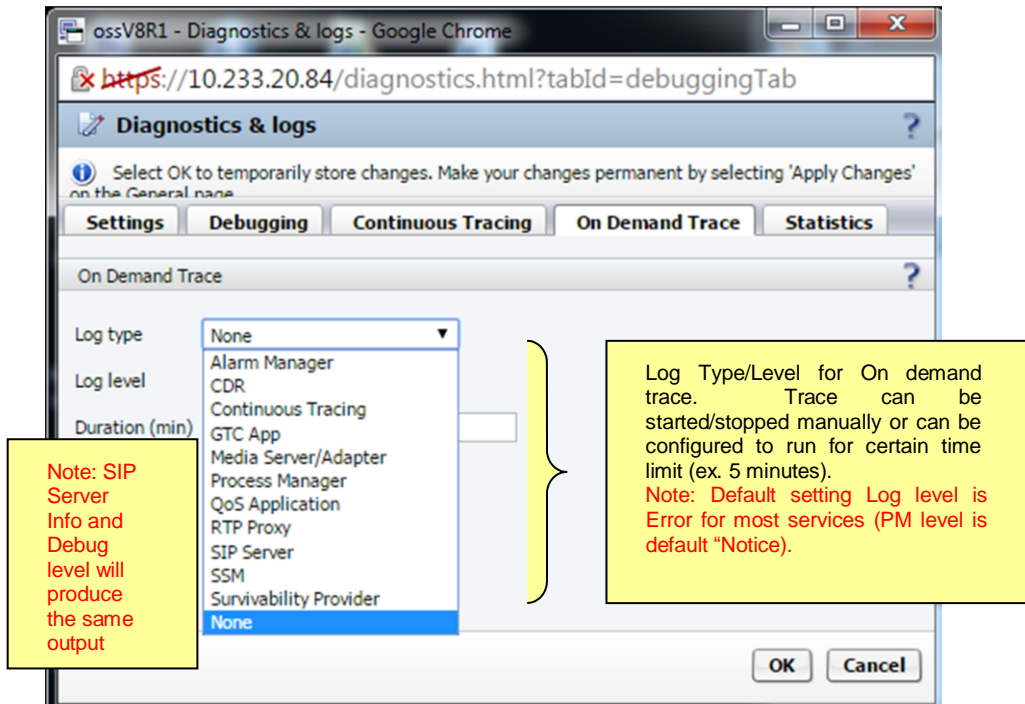
System Name: OSV System name configured on the OSV-TM Server.
Username/Password: Login information used to connect OSS SFTP server to OSV-TM server.
Note: logs/traces are sent (push) as *.gz by the OSS

Enable: Flag to enable/disable Continuous Tracing.
IP Address: IP Address or FQDN of OSV-TM Server.
File Size/Time Interval: log/trace files are sent to OSV-TM server when File Size or Time Interval Threshold is elapsed.
Note: polling time is about 10 seconds so file sizes may vary if the amount of log data is increasing too fast.
SIP/Q931 Trace: enables SIP/Q931 trace Capture.
MGCP Trace: enables MGCP trace Capture.

NOTE: RTP cannot be logged in the trace manager server. In order to trace RTP, use local GUI network trace

3.4.7.4 On Demand Trace

On Demand Trace allows selecting a log type and log level manually or for a specific time period. The "on demand trace" overwrites the log level configuration for a specified interval of time. After that the log level configuration goes back to the configured one. The Continuous Tracing file size and time parameters still control when files are sent (via SFTP).



3.4.7.5 Statistics

This tab has only read only fields. No configuration performed on this tab.

3.4.7.6 Serviceability

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 **Serviceability**

Rest API Server ⓘ

☒ Enable

Server Port

Client Credentials ⓘ

Add Delete

Client ID	Client Password
1234567890	*****

Rest API Server

Enable- enable the Rest API feature

Server Port - The default Server Port is 8000. You may change the Server Port from 8000 to another Port number and verify it.

Client Credentials - It is necessary to authenticate for accessing the API routes and must be configured the ClientID and Client Password to be used on this authentication. After the client sends an authentication request with a valid ClientID/Client password on Authorization Header or into the Body of the request, the Service API will provide an access token to be used in each next request. This received token must be sent in Authorization Header.

Client ID - Unique ID with at least 10 characters.

Client Password - Password with at least 10 characters.

IMPORTANT:

The Rest API will be available only on the SBC LAN side (for dual-armed configuration) in the port specified in the configuration. This is the server address that will listen for requests:
`https://<SBC-LAN-IP>:<port>`

3.4.8 Alarms

3.4.8.1 Alarm Settings

This allows configuration of alarm thresholds, severity level, flow timer, reporting class and if the reporting of the alarm is activated.

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	Minor	0	1	HW-Sensors	Equipment

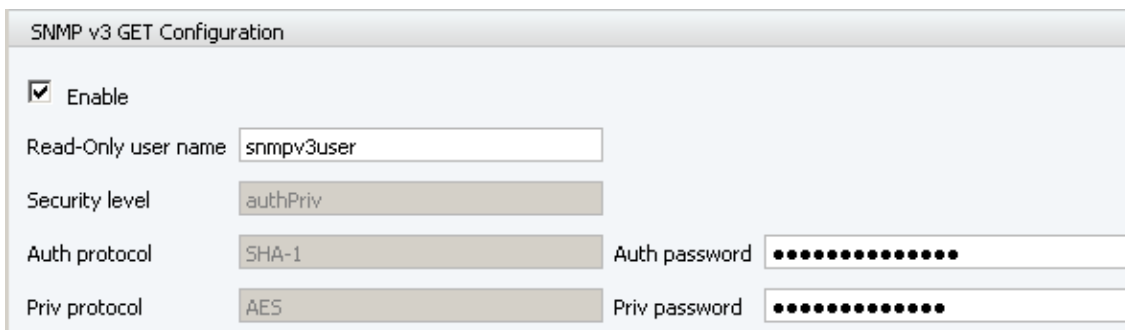
When configuring flow timer as 0, then alarm traps to clear an alarm are reported every time. If configured as 60, then same alarm trap to clear alarm is repeated only after timer expires.

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. **Faulty Object** character string that defines the object that is at fault.
11. **Event Type** classifies alarms into: communications, environmental, equipment, processingError, and qualityOfService.

3.4.8.2 SNMP v3 GET Configuration

Local GUI → Alarms → SNMP Configuration → SNMP v3 GET Configuration

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



The image shows a web-based configuration form titled "SNMP v3 GET Configuration". It contains several fields: a checked "Enable" checkbox, a "Read-Only user name" text box with the value "snmpv3user", a "Security level" dropdown menu with "authPriv" selected, an "Auth protocol" dropdown menu with "SHA-1" selected, an "Auth password" masked text box, a "Priv protocol" dropdown menu with "AES" selected, and a "Priv password" masked text box. The "authPriv", "SHA-1", and "AES" options are grayed out, indicating they are default or locked values.

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.

3.4.8.3 Trap Destinations

Local GUI → Alarms → SNMP Configuration → trap destinations → add

Alarms can be routed to a remote device using SNMP v2c or SMP v3. The IP address and port of the receiving device may be configured. The user can also configure the “reporting class” of alarm to be sent to limit the alarms sent.

The SNMP community string for Alarm traps can be changed by a new file `/etc/snmp/snmptraps.conf`. It will automatically update the SNMP community string of alarm traps after a few seconds.

The following format should be used in the file:

```
alarm_trap[index]_community="[newSnmpCommunityString]"
```

where [index] is the trap index (1 to 5) which refers to the same Row index in the GUI (a max of 5 trap destinations are allowed) , and [newSnmpCommunityString] is the new SNMP community string.

The SNMP string must be between double quotes. The default SNMP community string “public” will be used if it is not recognized as a valid SNMP string. An Alarm Manager log in WARN level is generated when the SNMP community string is changed.

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

Row	IP address	Port	Trap community name	Blocked	Reporting class set	Type	Read-Only community name
1	10.200.0.100	162	public	<input type="checkbox"/>	1;2;3;4;5;6;7	alarm	
2	10.200.0.101	162	public	<input type="checkbox"/>	1;2;5;6;7	alarm	test12567
3	10.200.0.102	162	public	<input type="checkbox"/>	7	alarm	
4	10.200.0.103	162	public	<input type="checkbox"/>	7	alarm	
5	10.200.0.104	162	public	<input type="checkbox"/>	1;2;3;4;5;6;7	alarm	test1234567

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 OS SBC /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):

SNMP v3 Trap Destinations

Row	IP address	Port	Security name	Security level	Auth protocol	Auth password	Priv protocol	Priv password	Blocked	Reporting class set	Type
1	10.200.0.100	162	OSFM	authPriv	sha1	*****	aes	*****	<input type="checkbox"/>	1;2;3;4;5;6;7	alarm
2	10.200.0.101	162	OSFM	authPriv	sha1	*****	aes	*****	<input type="checkbox"/>	1;2;3;4;5;6;7	alarm
3	10.200.0.102	162	OSFM	none					<input type="checkbox"/>	1;2;5;6;7	alarm
4	10.200.0.103	162	OSFM	auth	md5	*****			<input type="checkbox"/>	7	alarm
5	10.200.0.104	162	OSFM	auth	sha1	*****			<input type="checkbox"/>	7	alarm

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

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.

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.

Note: up to 5 trap destinations can be configured.

3.4.8.4 Alarm for Malformed SIP Message Received

1 - First of all, it is necessary to check if the alarm is enabled for use since it is disabled by default. To check this, go to the Alarm Settings menu and look for the alarm with the Group Id / Event Id 9/20 and check if Active is selected, otherwise select and then apply the changes.

The screenshot shows the OpenScape SBC Management Portal interface. The left sidebar contains navigation menus for Administration, System, Network/Net Services, VoIP, Security, Diagnostics & logs, Alarms, Alarm Settings, SNMP Configuration, and Maintenance. The main content area displays the 'General - SBC-Test-fermando' page, which includes system status, system info, and a table of alarm settings. The 'Alarm Settings' tab is selected, and the 'SNMP Configuration' sub-tab is active. The table lists various alarms, including 'SIP Malformed Message Received' (Group ID 9, Event ID 20). The 'Active' checkbox for this alarm is highlighted with a red box. The 'Apply Changes' button is also highlighted with a red box.

Row	Group ID	Event ID	Group name	Event name	Active	Threshold	Trigger	Severity	Flow timer	Reporting class	Faulty object	Event type
123	9	11	Security	CRL download failure	<input type="checkbox"/>	0	Greater than	Warning	0	7	TLS Certificate	Communications
124	9	12	Security	CRL download failure due to invalid signature	<input checked="" type="checkbox"/>	0	Greater than	Major	0	7	TLS Certificate	Communications
125	9	13	Security	Subscriber/DA synchronization failure	<input checked="" type="checkbox"/>	0	Greater than	Critical	0	7	SIP Server Subscriber Authentication	Communications
126	9	14	Security	Wrong Digest Authentication exchange key	<input checked="" type="checkbox"/>	0	Greater than	Critical	0	7	SIP Server Subscriber Authentication	Communications
127	9	15	Security	Invalid Certificate Purpose	<input checked="" type="checkbox"/>	0	Greater than	Critical	0	7	TLS Certificate	Communications
128	9	16	Security	BCF-SUSBCRIBE received from non configured partners	<input checked="" type="checkbox"/>	0	Greater than	Minor	0	7	BCF	Communications
129	9	17	Security	BCF Security Posture: Yellow	<input checked="" type="checkbox"/>	0	Greater than	Minor	0	7	BCF	Communications
130	9	18	Security	BCF Security Posture: Orange	<input checked="" type="checkbox"/>	0	Greater than	Major	0	7	BCF	Communications
131	9	19	Security	BCF Security Posture: Red	<input checked="" type="checkbox"/>	0	Greater than	Critical	0	7	BCF	Communications
132	9	20	Communication	SIP Malformed Message Received	<input type="checkbox"/>	0	Greater than	Critical	0	7	IP	Communications

2 - Now to check if the alarm was triggered and a malformed SIP message was received, go to Show Alarm Details and look for the Group Id / Event Id - 9/20. There will be some information, including the IP from which the malformed message was sent, in case an alarm has been generated.

UNIFY OpenScape SBC Management Portal

User name: administrator | Help | Logout

OpenScape SBC

Administration

- System
- Network/Net Services
- VoIP
- Features
- Security
- Diagnostics & logs
- Alarms
- Alarm Settings
- SNMP Configuration
- Maintenance

General - SBC-Test-fermando

SBC aggregated information and data.

Alarms

Alarm summary: Critical: 1 Major: 0 Minor: 0 [Show alarm details](#)

System Status

Branch mode: Centralized SBC Auto refresh timer: 10 seconds

Operational state: survivable

Com Node 1

Primary server: not configured Penalty box state: InPenaltyBox

Backup server: Penalty box state

Com Node 2

Primary server: Penalty box state

Backup server: Penalty box state

System Info

CPU: 7.72 % - 1 x 3093 MHz

Memory: 22.15 % - 0 Gb

Disk: 12.64 % - 43 Gb

System uptime: 3 days 22:39

Hardware type: Virtual OSS 20000

Hostname: SBC-Test-fermando

Software Info

Software version: V10 R1.00.00

Software Partition information: [Active](#) [Backup](#)

Services status: [Show](#) Registered subscribers: [Show](#)

SSP status: [Show](#) Dynamic port mapping: [Show](#)

Dynamic IP remote endpoints: [Show](#) Denial of Service Mitigation: [Show](#)

TURN Allocations: [Show](#) Telephony Connector status: [Show](#)

SIP Loadbalancer status: [Show](#)

Apply Changes Cancel Changes

Alarm Details

Information about current list of alarms.

Clear all Clear

Items/Page: 10 | < > 1 | All: 1 | CSV Export

Clear	Group ID	Event ID	Group name	Event name	Monitored value	Time (yyyy-mm-ddThh:mm:ss)	Threshold	Trigger	Severity	Flow timer	Reporting class	Faulty object	Event type
<input type="checkbox"/>	9	20	Communication	SIP Malformed Message Received	1	2020-06-08T19:57:25+0000	0	Greater than	Critical	0	7	IP-192.168.15.211	Communicati...

Close

3 – This alarm also can generate Trap messages (SNMP). Please refer SNMP configuration section in this guide.

3.4.9 Maintenance

3.4.9.1 How to import / export a file

Import / Export Tab under Maintenance includes the following fields:

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

Configuration file in use: config_178_20210318T014107.xml **Current Running config File**

Load

Select a configuration file: config_178_20210318T014107.xml **Load**

Import

Select a file to upload: Choose File No file chosen **Upload**

Export

Select a configuration file: config_178_20210318T014107.xml **Export** **Export all**

History

Last configuration time: Thu, 18 Mar 2021 01:41:07 User: User IP address: **Show last changes**

Compare with previous version: config_178_20210318T014107.xml **Compare**

This function will compare the selected XML file to the current version.

This will open a window which will show the latest changes made to the xml file.

Load/ Import: user can load a previous existing config file (Load) or import a new one into SBC (Import)

Export: user can export current config file or all config files

Close

- **Load**

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_178_.xml** is configured as **Config_179_.xml**).

- **Import**

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_178.xml** is configured as **Config_179.xml**).

- **Export**

Export Config (DB XML File). The **Export** button shows two options: save or open the selected xml config file.

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

3.4.9.2 How to install / upgrade a file

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

3.4.9.2.1 Install

The screenshot shows the 'Maintenance' tab with a sub-tab 'Install/Upgrade'. The 'Installation' section is highlighted with a red box. It contains a checkbox for 'UEFI Bootloader (UEFI Bios NOT detected)', a text field for 'Number of Code Partitions (2..5)' with the value '2', and an 'Install' button. Below this is the 'Upgrade' section with a 'Software source' dropdown set to 'USB stick' and an 'Upgrade' button.

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**



The screenshot shows the 'Maintenance' window with the 'Install/Upgrade' tab selected. Under the 'Installation' section, the 'UEFI Bootloader (UEFI Bios NOT detected)' checkbox is unchecked. The 'Number of Code Partitions (2..5)' field is highlighted with a red box and contains the number '5'. Below this is an 'Install' button. The 'Upgrade' section below it shows a 'Software source' dropdown menu set to 'USB stick' and an 'Upgrade' button.

By default, the system disk has 2 partitions:

- 2) Partition “A” is used to hold one copy of the uncompressed OpenScape SBC software.
- 3) Partition “B” is used to hold a second copy of the uncompressed OpenScape SBC software.

A Data partition is used to hold data.

The “A” and “B” partitions provide the possibility of falling back to a previous software release in the event of a problem when upgrading to a new software release.

Upon initial installation, the “A” partition holds the “active” file system which is loaded into RAM whenever the OpenScape SBC is restarted. When 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 SBC is restarted.

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

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	Unlock 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.

3.4.9.2.2 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

New Code Activation

Partition	Version
P1	oss-10.02.04.00-1

☒ Reboot only when all calls are disconnected

Time to wait for all calls be disconnected (between 1 to 72 hours) 24

Activate now **Abandon** **Remove**

Activate at date 20 / 06 / 2022 14 : 29 **+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**

Close

1. 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 a web interface titled "Upgrade". Under "Software source", "Local file" is selected in a dropdown menu. Below this, there is a "File" input field with a "Browse..." button next to it. Under the "Files:" section, a file path is displayed: "Z:\OSS\OPENSAPESBC_V10.01.00_01.00.02.04\image_oss-01.00.02.4.tar", with a "Remove" button to its right. At the bottom of the interface 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' tab with the 'Upgrade' sub-tab selected. The 'Software source' is set to 'HTTPS'. The 'Hostname' field contains '10.80.0.20'. The 'Remote directory' field contains '/bcf'. The 'Software version' dropdown is set to 'bcf-10.09.00.00-1'. The 'List Versions' button is highlighted. The 'Upgrade' button is at the bottom.

- 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_SBC-10.09.00.00-1.tar.
- Click **List Versions** and select the available software version to upgrade.

4. SFTP

The screenshot shows the 'Maintenance' tab with the 'Upgrade' sub-tab selected. The 'Software source' is set to 'SFTP'. The 'Hostname' field contains '25.25.130.53'. The 'Port' field contains '22'. The 'Remote directory' field contains '/root/upgrade'. The 'User name' field contains 'root'. The 'Password' field contains '*****'. The 'Software version' dropdown is set to 'bcf-10.09.00.00-1'. The 'List Versions' button is highlighted. The 'Upgrade' button is at the bottom.

- 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_SBC-10.09.00.00-1.tar.
- Click **List Versions** and select the available software version to upgrade.

2. New code activation field

Partition	Version
P1	oss-10.02.04.00-1

☒ Reboot only when all calls are disconnected

Time to wait for all calls be disconnected (between 1 to 72 hours) 24

Activate now Abandon Remove

Activate at date 20 / 06 / 2022 14 : 29 +1 Day +1 Hour Now

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.

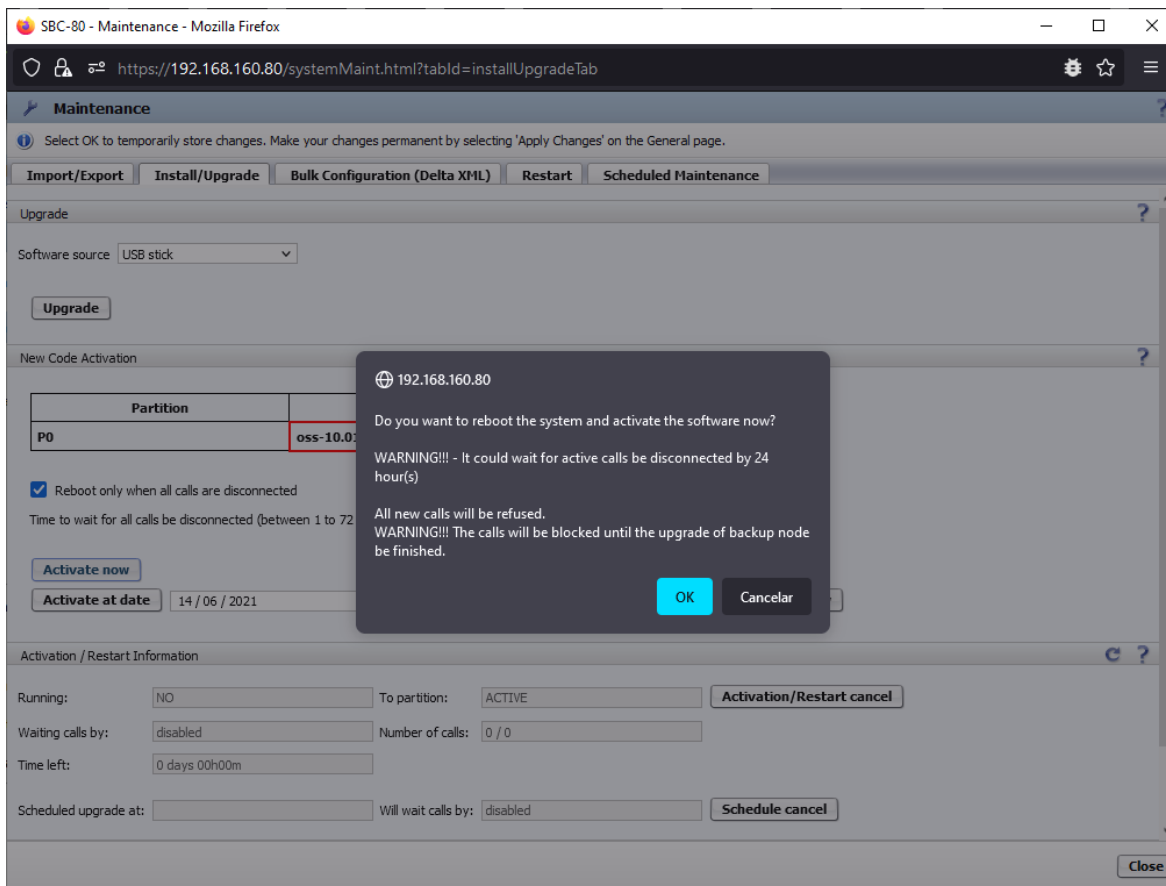
It is also possible to request the system to wait for running calls before reboot to activate the new code. For redundant system, when the flag **Reboot only when all calls are disconnected** is selected and upgrade is activated, the calls will be blocked until the end of upgrade process in both nodes (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 SBC.

When the **Abandon** button is used, an installed new partition will be ignored but left in the disk to be used if necessary (see the restart window). If a restart to it is done in the future, it will not upgrade a redundant node if the system is configured as a redundant pair.

When the **Remove** button is used, an installed new partition is set as empty, and it cannot be used later.

By activating the upgrade, a warning message is displayed indicating the upgrade.



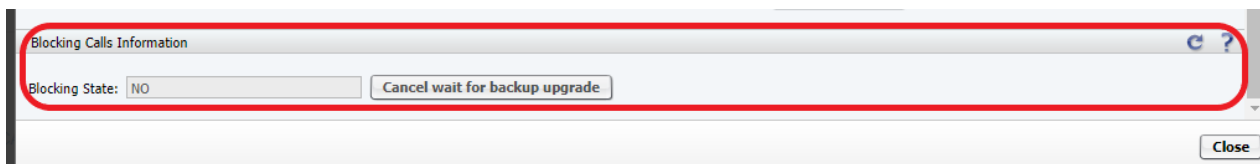
3. Activation / Restart Information field

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.

- **Blocking Calls information**



During activation, it is not possible to receive or generate calls and register subscribers.

However, it is possible to unlock the calls when the master node has already performed the upgrade and the backup node is not finished yet. For this, it is necessary to use the **Cancel wait for backup upgrade** button.

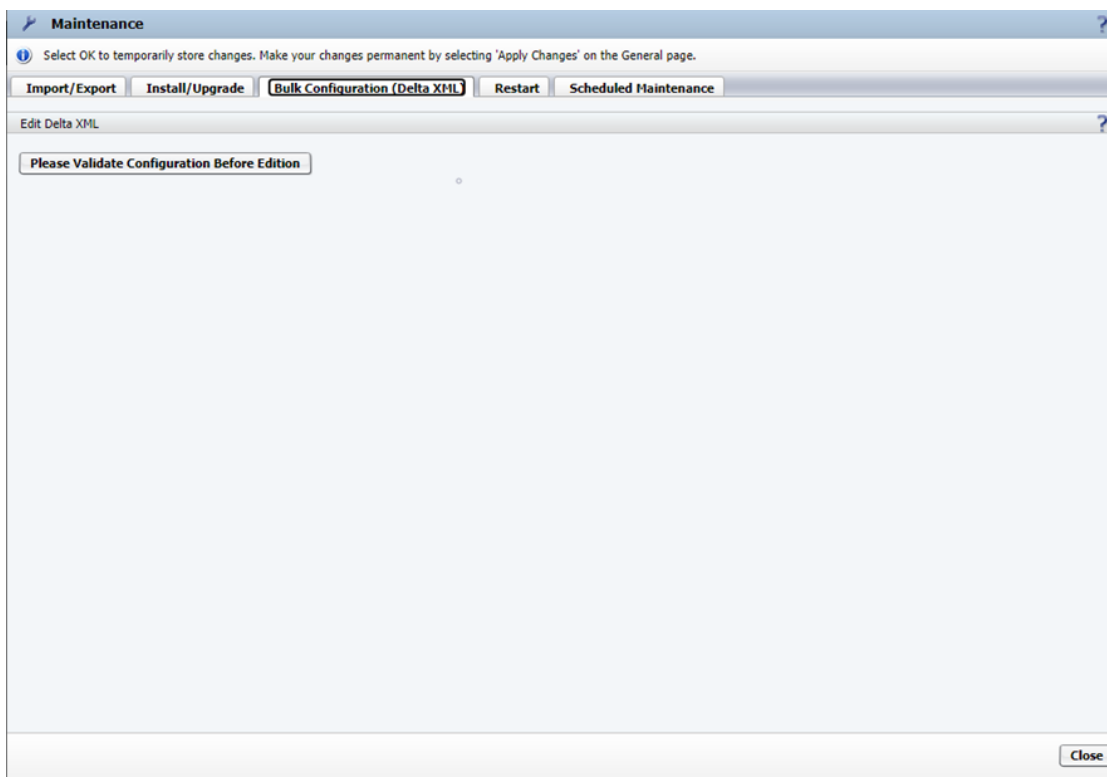
The **Cancel wait for backup upgrade** button is only available when calls are being blocked on the system by "pmc block" command.

- **Abandoning or removing an upgrade partition**



The **Abandon** button will remove the new flag from the new partition. It will stay in the disk and can be selected again to be used in the restart TAB. The **Remove** button will clear the partition and it will not be available for usage, it is set an empty.

3.4.9.3 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.

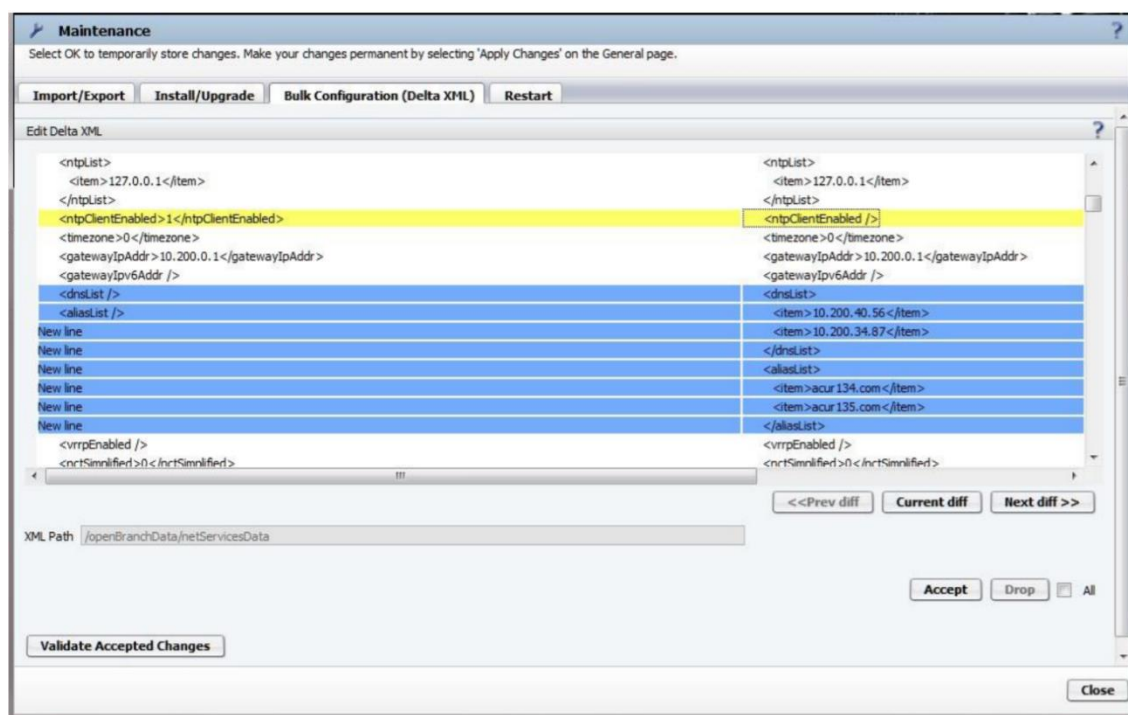
Note: Changes done on configuration after this step are detected only when reloading the "Bulk Configuration (Delta XML)" tab.

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).

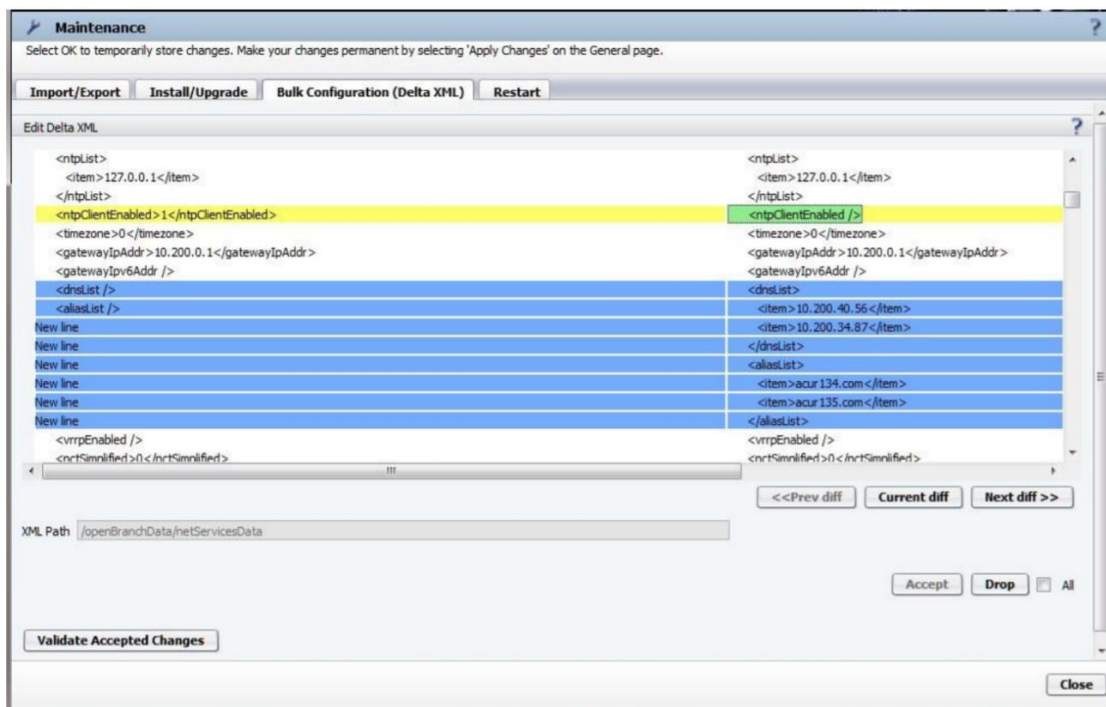
Note: In normal configuration task this feature can be used to have a preview of modifications on xml before the **Apply Changes**.



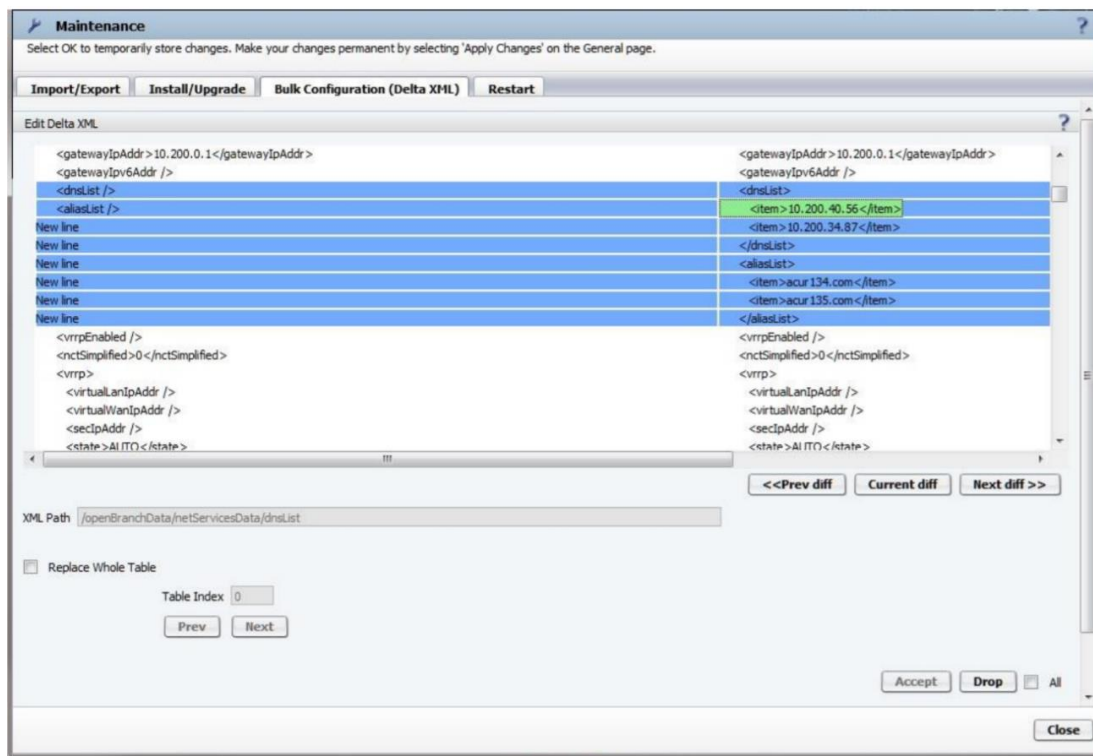
Only "accepted" changes are included on Delta XML files. It is possible to include/exclude changes on Delta XML file individually or in groups ("item" elements (lists or tables)).

Accept and **Drop** acts over currently selected change (checkbox **All** unchecked).

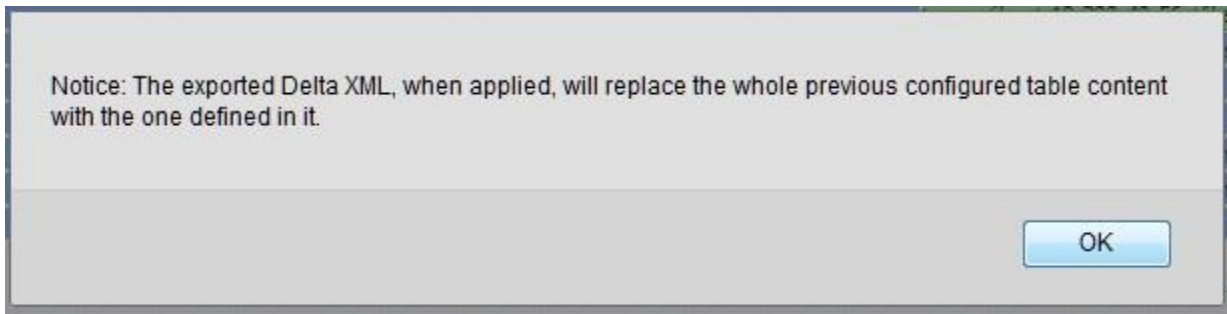
Accepted changes are marked with a green background. Dropping an accepted change returns its background to the original color. Original background colors are the same ones used on the **Compare** on **Import / Export** tab.



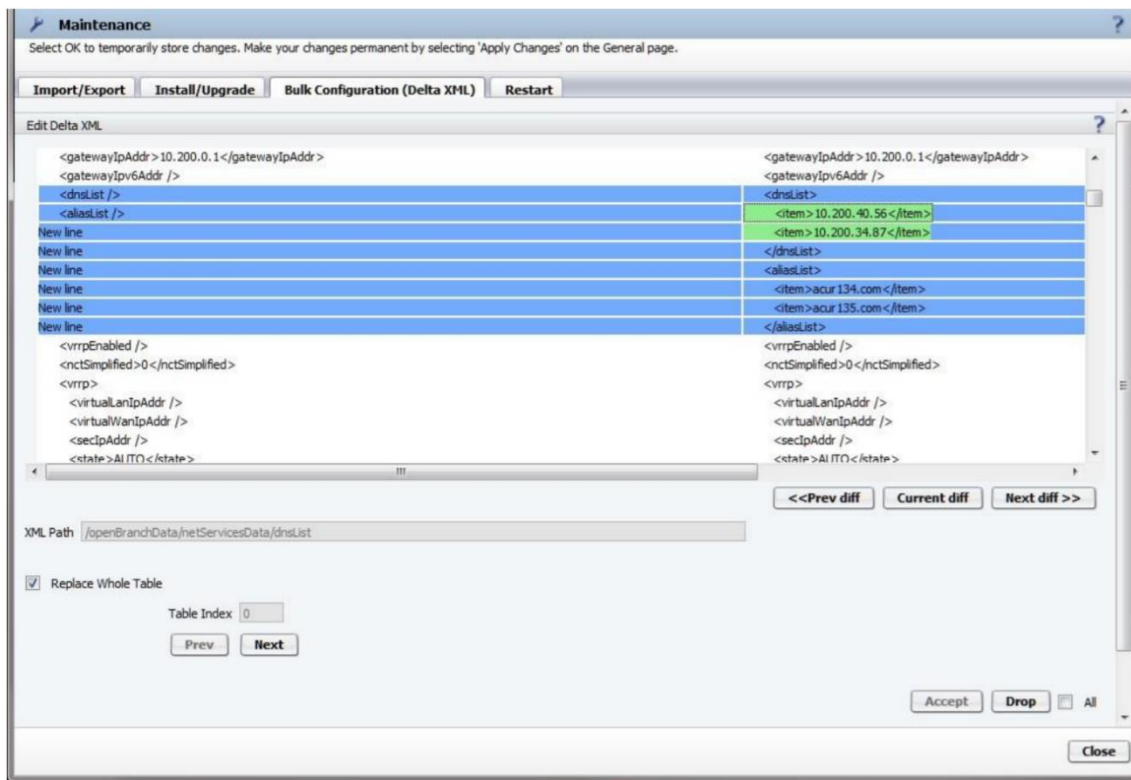
For lists and tables ("item" elements) there are additional operations shown at the left area below the "XML Path".



This Notice is presented the first time **Replace Whole Table** is checked:



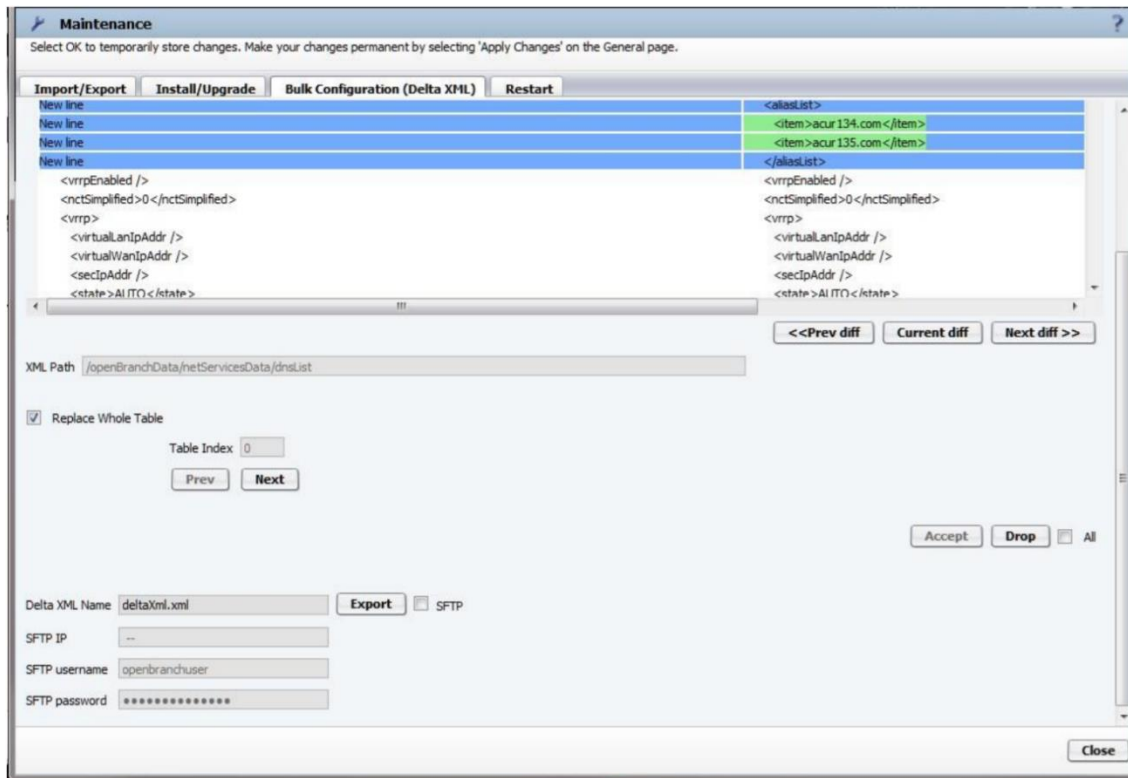
If the **Replace Whole Table** is checked, all "item" elements in the same level are colored in green. The exported Delta XML, when applied, replaces the whole previous configured table content by the one in green. **Table Index** informs the position of the "item" element (starts with 0). **Prev** and **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

- logicalBranchOfficeld
- hwld
- saveCounter
- openBranchNetwork
- mode
- voipData.

3.4.9.4 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) 24

Minimal number of calls 0

Code partitions

Name	Version	State	Status
P0	bcf-10.09.00.00-91	ready	
P1	bcf-10.09.00.00-92	ready	
P2	bcf-10.09.00.00-94	ready	backup
P3	bcf-10.09.02.00-80	ready	next-boot,running

Unblock all Refresh

Block/Unblock Restart from P0

Block/Unblock Restart from P1

Block/Unblock Restart from P2

Block/Unblock Restart from P3

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

Close

4. 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.

5. 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.

6. 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.

7. 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](#).

8. 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.

3.4.9.5 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 SBC is a way to set the SBC call processing in an out of service state, so the traffic can be handled by another server, without shutting down the server. In that way, the upgrade and configuration functionalities can still be done.

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 SBC (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 reject new calls when the system activates the maintenance state, the flag "In Maintenance only after all calls are disconnected" is selected and there are active calls. Sipserver is still running.

This message is also valid for remote subscribers trying to register during this period.

When the system is effectively in maintenance state, the sipserver is blocked and the message is not sent.

This is also verified in Upgrade or Restart when the flag "Reboot only when all calls are disconnected" is selected and there are active calls.

3.4.10 Open External Firewall-Pinhole

When the SBC is under an external firewall, dummy UDP or 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.

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 **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***

3.4.10.1 Send RTP dummy packets

As some providers were having issues with the dummy UDP packets a new flag **Send RTP dummy packets** is added to send RPT packets instead.

Same way as the **Open External Firewall Pinhole**, the dummy RTP packets are sent towards the endpoint media destination (connection address and port in the SDP) in order to dynamically open the firewall for the incoming media streaming.

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:

Remote Subscribers (Administration → Features → Enable Remote Subscribers → Configure)

Remote Subscribers

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

General Settings

☒ Enable register throttling

Timer value towards subscriber - UDP (sec)

☒ Enable register throttling for TLS

Timer value towards subscriber (sec) TCP/TLS

Maximum throttling timer threshold (sec)

Maximum registration expiry time (sec)

Minimum registration interval (sec)

Port Mapping TTL timer (hours)

Core realm profile

Access realm profile

INVITE No Answer timeout (msec)

INVITE No Reply timeout (msec)

☐ Enable remap internal error code

☒ Open external firewall pinhole

☒ Send RTP dummy packets

☐ Insert Location Header

☐ Quarantine registration rate violators

Remote Subscribers configuration

Row	Name	Location Domain Name	Location Domain Subnet/IP	Location

Remote Endpoint

Administration→Features→Enable Remote Endpoints→Configure→Remote Endpoint Configuration→Miscellaneous

Remote endpoint configuration

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

MSRP Data Configuration

☐ Enable MSRP Relay Support (not licensed)

☒ use IP address in MSRP-path ☐ use FQDN in MSRP-path FQDN

☒ Authentication required Realm Password

☐ Access side only Qop AUTH Expire time/sec 300

Miscellaneous

☒ Open external firewall pinhole

☒ Send RTP dummy packets

Configuration per Remote Endpoint.

Telephony Connector

Administration → Features → Enable Circuit Telephony Connector → Configure → Miscellaneous

Circuit Telephony Connector

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

General

HTTPS Proxy IP

HTTPS Proxy Port

Telephony Connector status

TC running version 1.2.8602

Telephony Connector Common Settings

Certificate Profile (with Remote CA)

Circuit Telephony Connector URL (https)

Telephony Connector List

Row	Name	Access Realm Profile	Type	Circuit ID	GTC Type	Digest Enabled

Miscellaneous

☒ Open external firewall pinhole

☒ Send RTP dummy packets

Example of UDP packet (pinhole) that is sent when only **Open external firewall pinhole** is enabled:

P31003-S53A0-M101-30-76A9

214 OpenScape SBC V10 Configuration Guide

3.5 Example configurations

Object	OS SBC endpoint configuration (See 3.5.1)				OSV endpoint configuration (See 3.5.2)	
	Remote URL	Remote SIP/MGCP port	Core FQDN	Core realm port	IP address	port
OS SBC				5060	10.232.63.94	5060
OSB proxy mode "A" (See 3.5.2.1)	10.191.0.20	5060		50010	10.232.63.94	50010
OSB proxy mode "B" (See 3.5.2.1)	10.191.0.30	5060		50020	10.232.63.94	50020
Gateway behind OSB proxy "B" (See 3.5.2.2 and 3.5.3)	10.191.0.30	5096		50021	10.232.63.94	50021
OSB "SBC-proxy" mode (See 3.5.3.1)	10.191.0.40	5060		50030	10.232.63.94	50030
Gateway behind OSB "SBC-proxy" (See 3.5.2.2 and 3.5.3)	10.191.0.40	5096		50031	10.232.63.94	50031
OSB in "Branch-SBC" mode (See 3.5.3.2)	10.191.0.50	5060		50040	10.232.63.94	50040
Gateway behind OSB in "Branch-SBC mode (See 3.5.2.2 and 3.5.3)	10.191.0.50	5096		50041	10.232.63.94	50041
OSB behind static NAT (See 3.5.4.1)	192.168.1.150	5060		50050	10.232.63.94	50050
OSB behind dynamic NAT (See 3.5.4.2)	osv.bg.branch	5060		50060	10.232.63.94	50060
Standalone Gateway directly on OS SBC (See 3.5.2.2)	10.191.0.100	5060		50070	10.232.63.94	50070
OSB "A" with "auto Attendant" (See 3.5.2.4)	10.191.0.20	5096 udp		50011	10.232.63.94	50011
OSB "A" with local media server (See 3.5.5)	10.191.0.20	2427 udp		2427	10.232.63.93 (See 3.5.5)	

This assumes the OSS has been created using information in General steps to add a OS-SBC.

Note 1:

Unless noted these values are configured under the "remote endpoints" configuration" section of the OSS. Local GUI-> VOIP-> "Enable Remote Endpoints" -> click on "Remote Endpointsconfiguration".

Under "Remote Endpoints Configuration" clickAdd.

Under "Remote Endpoint Settings" enter the Name, Type and Profile.

Under "Remote Location Information" enter the Signaling address type, IP address, port and Transport of the remote endpoint.

Under “Remote Location Identification/Routing” enter the core side address and **unique ports**, as defined in the OSV, for the remote endpoint.

Under “Remote Location Domain List” click Add. See section [Remote Endpoint Configuration](#) for details.

Under “Access Side Firewall Settings” check “enable Firewall Settings”, click on “Firewall Settings” See section [Remote Endpoints](#) for details.

Note 2:

These values are configured on the CMP under OpenScape Voice →business group →members →endpoints

Note 3:

These values are configured on the OSS under remote endpoints settings →Remote Location Identification/Routing →core Realm port. Not required if the default IP address of the OSS is to be used.

Note 4:

SBC-proxy mode enables the WAN interface of the OSB

For SBC-Proxy mode, the WAN interface is used to access SIP Service Providers. Subscribers and OpenScape Voice are in LANas in Proxy mode.

Local GUI→ VOIP →OpenScape Branch Mode →select “SBC-Proxy” (this will enable interface 2)

Local GUI→VOIP →check “Branch behind SBC

Local GUI→Network Services→Interface 2 →check box “Interface enabled”, enter the IP address of node 1 and the Subnet mask for this interface.

Local GUI→VOIP →check box “enable Gateways/Trunks” Local GUI→VOIP →click “Gateways/Trunks”

Local GUI→VOIP→ “Enable Gateways/Trunks” →click on “Gateways/Trunks configuration”. Note that the gateway is created on the WAN interface enabled in the first step.

For more details on the OpenScape Branch please refer to the OpenScape Branch configuration Guide. <https://www.g-dms.com/livelink/llisapi.dll/view/inf-13-000221>

Note 5:

The gateway is created in the branch office the OSB represents in the OSV Create the gateway under the branch office

CMP→OpenScape Voice→<select business group> →<branch office created above>→Members→Endpoints→Add

On the General tab enter the Name, Profile and Endpoint template.

On the Sip tab, click “SIP trunking”, set the “Type” to “Static”, set the “signaling address type”, enter the “Endpoint address” (this will be the same address of the OS-SBC.

On the Sip tab enter a unique port number which will define the OSB in both the OSV and OS-SBC, also add this port to the list of “trusted entities”.

On the “Attributes tab” set the attributes of “Route via Proxy”.

On the “Aliases tab” add any IP address and port combination which may be used to communicate with the OSB. The entry is in the form of <IP address>:<port>

On the General tab click “Registered”

Note 6:

Additional configuration is required on the OSB refer to the OSB configuration guide.

Refer to the OSB Configuration guide <https://www.g-dms.com/livelink/llisapi.dll/view/inf-13-000221> for information

Note 7:

Branch SBC mode enables the WAN interface of the OSB. The WAN interface of the OSB is used to

connect to the OSS while the LAN interface is used for subscribers and gateways

On the Branch Phones

The checkmark for Outbound Proxy should be set.

The SIP server address should be the WAN address of the OS-SBC. The SIP registrar address should be the WAN address of the OS-SBC.

The SIP gateway address should be the LAN address of the OpenScape Branch. (not the LAN gateway IP)

Note if an external firewall is between the phones and the OS-SBC, then the external address of the firewall would be used in place of the WAN address of the OS-SBC.

Note 8:

This is the address of the address of the branch not the address of the NAT

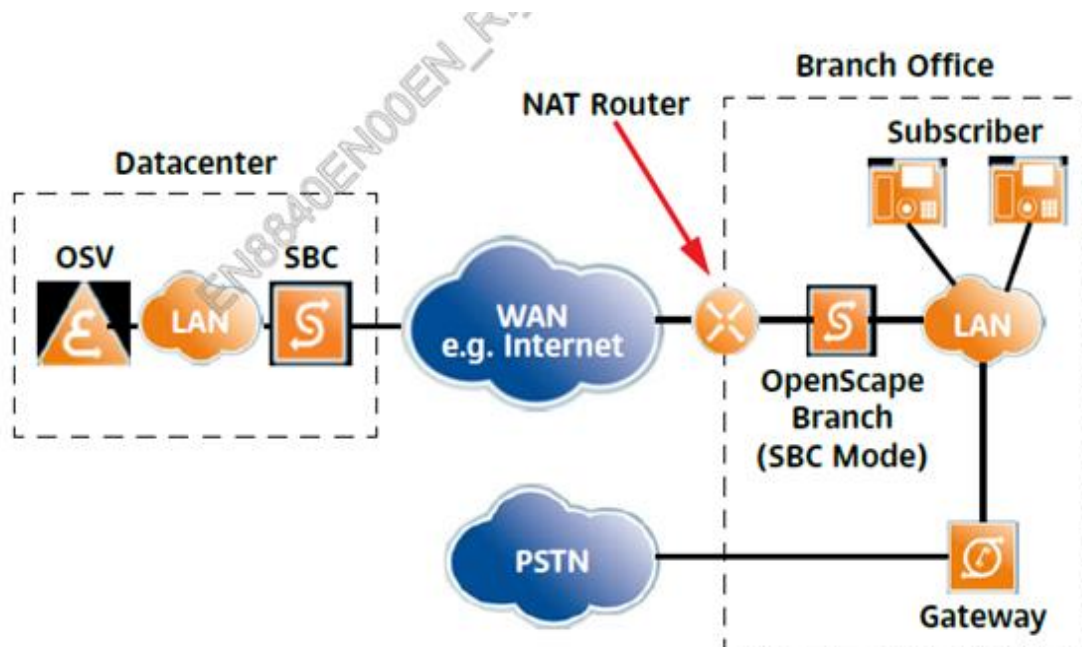
1. Local GUI → VOIP → "Enable Remote Endpoints" → click on "Remote Endpoints configuration". Under "Remote Endpoints Configuration", click Add.
2. Under "Remote Endpoint Settings" enter the Name, Type and Profile.
3. Under "Remote Location Information" enter the Signaling address type, IP address, port and Transport of the remote endpoint. **(not the address of the NAT)**
4. Under "Remote Location Identification/Routing" enter the core side address and unique ports, as defined in the OSV, for the remote endpoint.
5. Under "Remote Location Domain List" click Add. See section [Remote Endpoints](#) for details. **(use the address of the NAT not the address of the branch)**.
6. Under "Access Side Firewall Settings" check "enable Firewall Settings", click on "Firewall Settings" See section [Remote Endpoints](#) for details.

On the OpenScape Branch

Local GUI → VOIP → Node 1 primary server → set the address, transport and port of the WAN interface of the OS-SBC. <https://www.g-dms.com/livelink/lisapi.dll/view/inf-13-000221>

Add in Bold provisioning of Branch Office behind NAT and with Gateways.

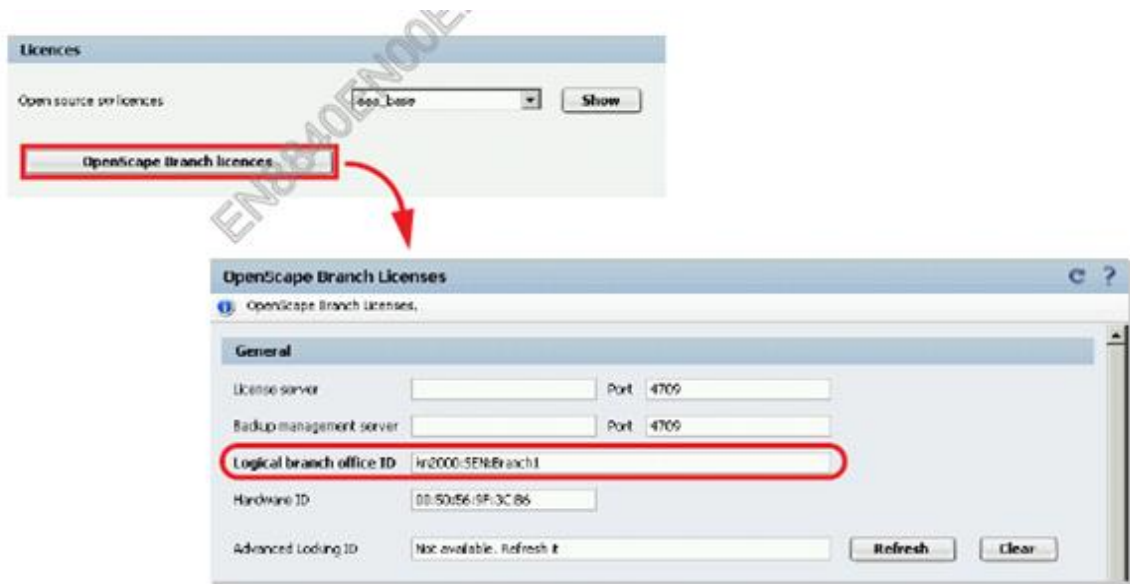
The following diagram provides an overview of the scenario which will be configured on the following pages :



First, the OpenScape Branch's WAN interface (which is connected to the NAT Router) must be configured under the **Network Services** menu as well as the default route should point to the NAT router:

The screenshot shows the configuration for **Interface 2**. The **Interface enabled** checkbox is checked. The **Type** is set to **WAN**, highlighted with a red dashed box and a green note: "This will indicate the „External“ interface (mostly the 2nd)". The **Main IP address node 1** is **1.20.250.187** and the **Subnet mask** is **255.255.255.0**, both highlighted with a red box. The **Default gateway address** is **1.20.250.254**, also highlighted with a red box. Other fields include **Admin IP address**, **Main IP address node 2**, **Main Virtual IP address**, and **Speed** (set to Auto). Buttons for **VLAN configuration** and **Routes configuration** are visible at the bottom.

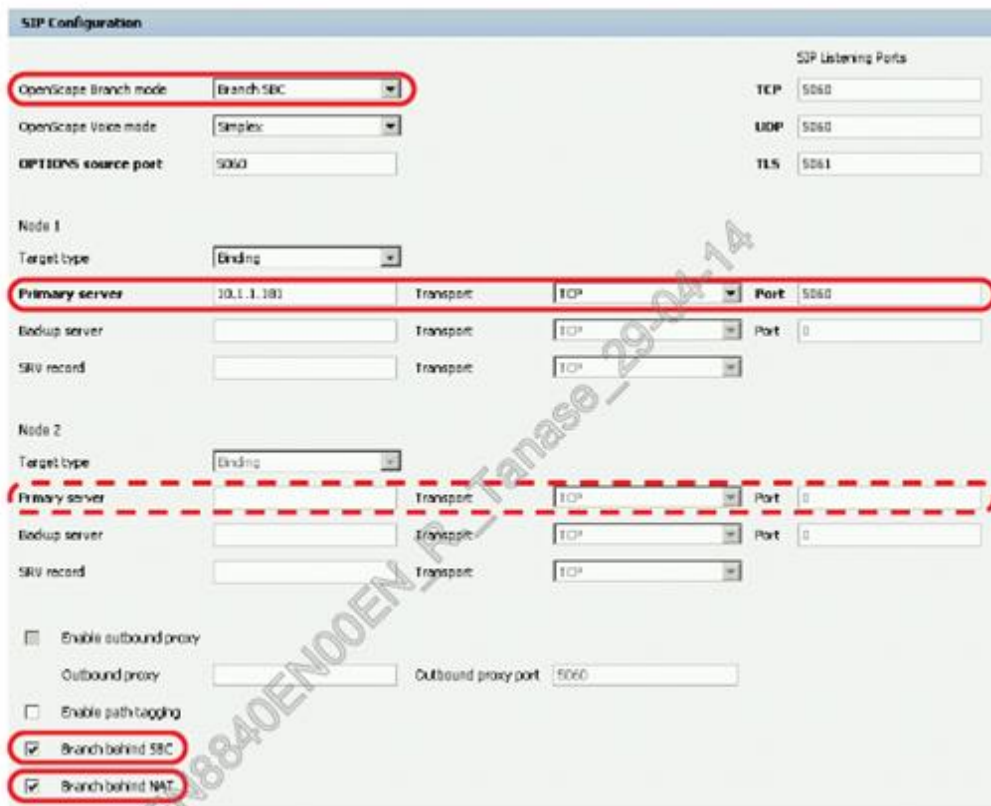
Next, under the **Licenses** tab of the **System** menu, verify that the Logical branch office ID is configured:



This will be done normally from the OSB Assistant. In the case where the device is operated in standalone mode, the Logical branch office ID can be entered manually in the following format:

<Cluster Name>:<Business Group Name>:<Branch Office Name>

Now the operating mode can be changed to **Branch SBC** as well the **Branch behind SBC** and **Branch behind NAT** must be activated. Under Primary server of Node 1 and 2 the OpenScope SBC's WAN IP or FQDN must be configured:



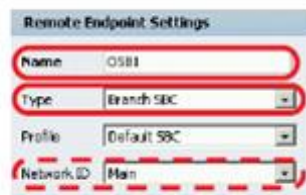
Click on **Apply Changes** to activate the new configuration.

Now, on the SBC, the OpenScope Branch device must be configured under **Remote Endpoints**
 P31003-S53A0-M101-30-76A9 220 OpenScope SBC V10 Configuration Guide

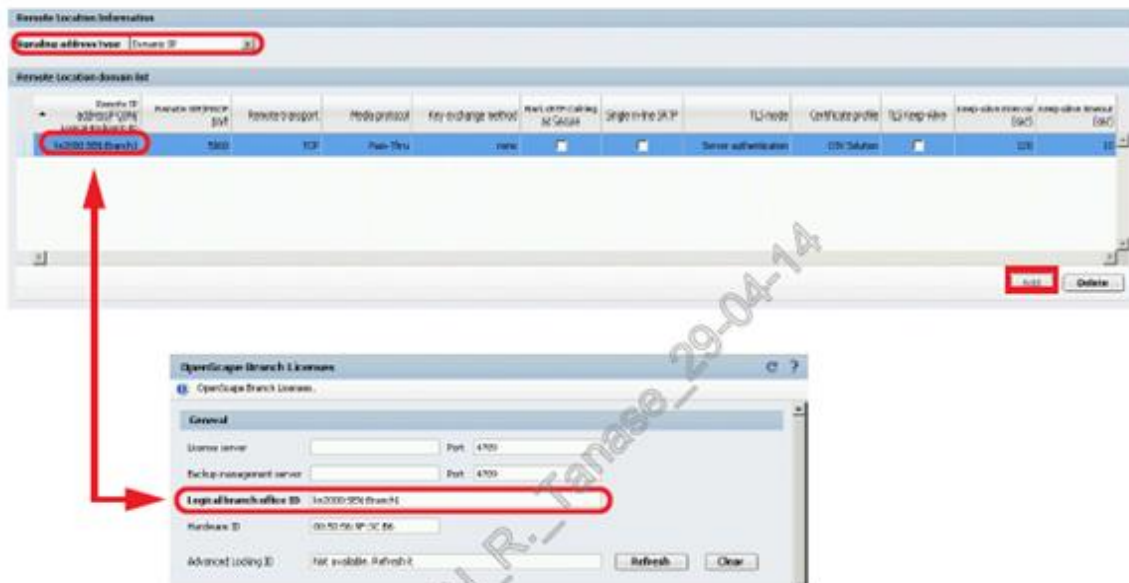
configuration. Click on **Add** under **Remote Endpoints configuration** in order to create a new endpoint mapping entry:



Enter a name for the entry and select the new type **Branch SBC** (this will automatically select the profile **Default SBC**). Optionally, select the VLAN under which the OSB can be reached:

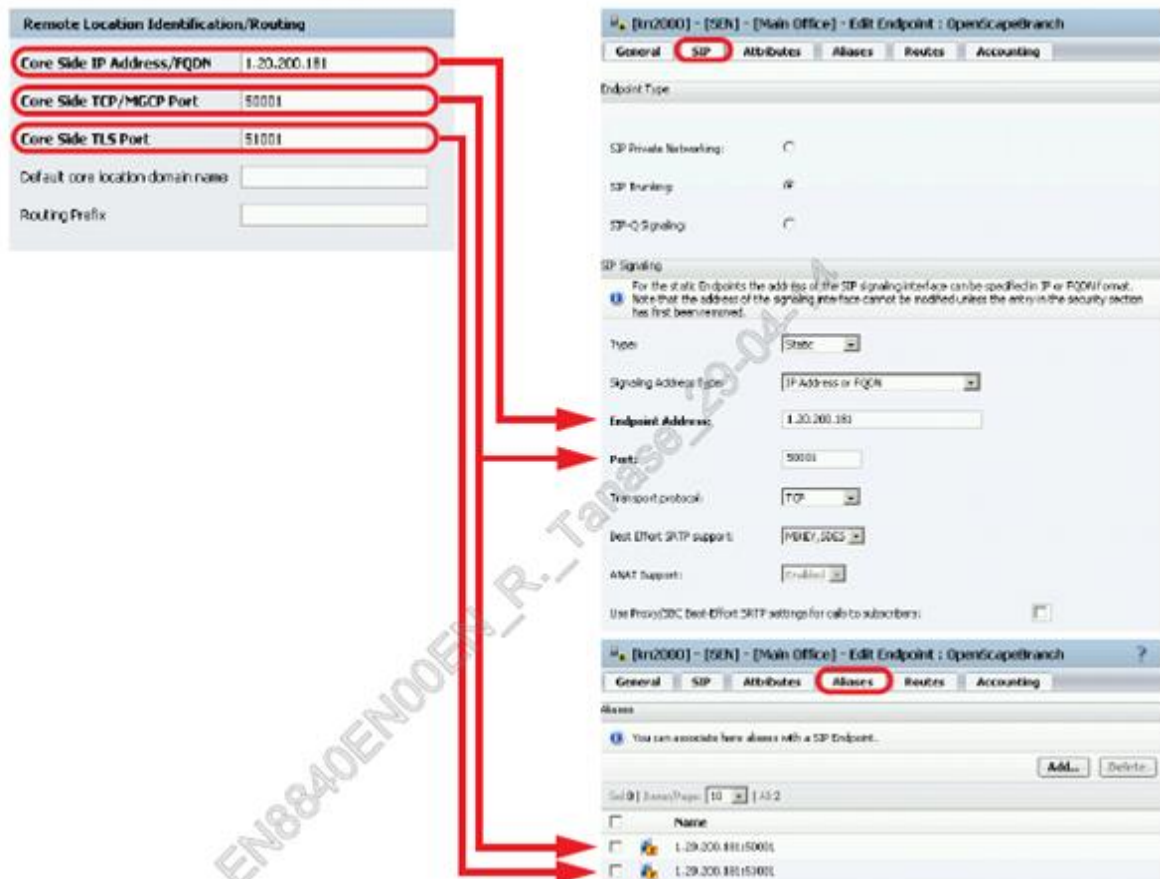


Under **Remote Location information**, select the new Signalling address type **Dynamic IP** and enter the **Logical branch office ID** which has been retrieved /configured earlier on the OSB.



Please note that the **Logical branch office ID** will be used later from the SBC to match the OSB's **dynamic IP** to this entry and must match on both sides!

Enter the SBC's LAN IP which should be used to forward traffic from this device to the OSV and assign a unique TCP/TLS port from the static endpoint port range:



Save all configurations and click on **Apply Changes** to activate the new configuration. The OSB should switch to **Normal Mode** shortly:

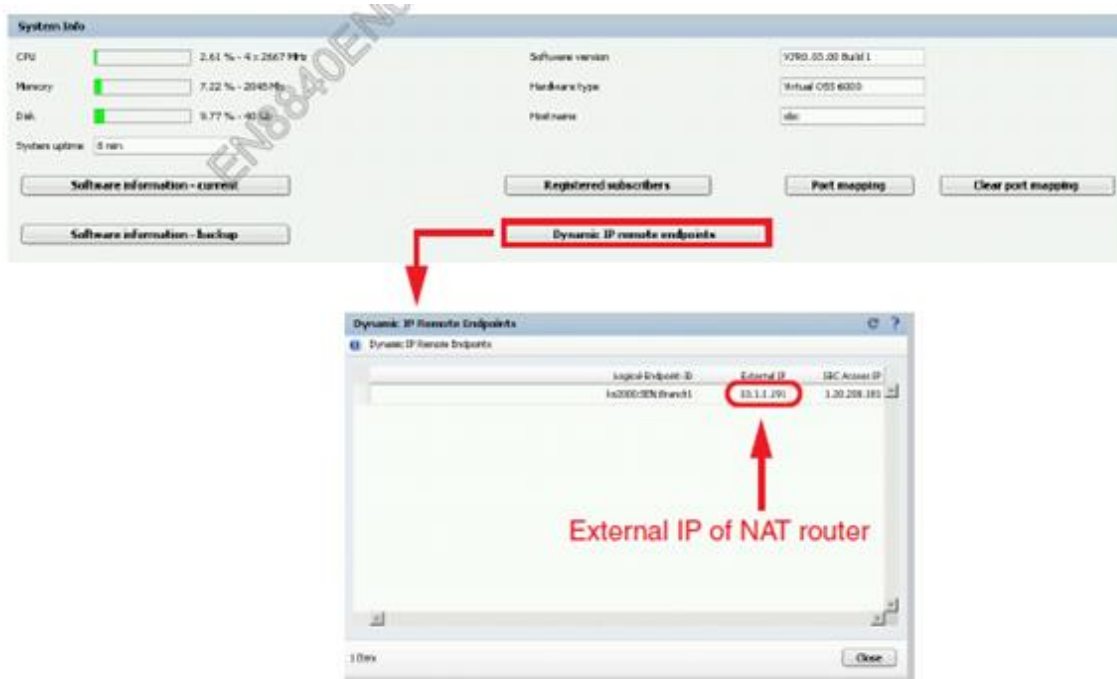


The SBC can reach the branch office, the OSB will send a SIP OPTIONS message with its Logical-Endpoint-ID encrypted (MD5 encoding using an internal shared secret) in a new **X-Siemens-Identity** header:

```
OPTIONS sip:sipserver@10.1.1.181:5060;transport=TCP SIP/2.0
Via: SIP/2.0/TCP 1.20.250.187;branch=z9hG4bK94585B59240F0F04.40373755;i=1
Via: SIP/2.0/TCP 1.20.250.187;branch=z9hG4bK8ce3f2c
Via: SIP/2.0/TCP 1.20.250.187:5060;branch=z9hG4bK4a706f18
X-Siemens-Identity: SS-nAGsUjPdwXO4F1QN.p4RIAm9
Call-ID: 2592fba6
From: <sip:survivabilityprovider@1.20.250.187>;tag=403737553
CSeq: 1 OPTIONS
Content-Length: 0
Max-Forwards: 70
To: <sip:sipserver@10.1.1.181:5060;transport=TCP>
User-Agent: SIP alive check
X-Siemens-Proxy-State: normal
```

If the decrypted Logical-Endpoint-ID matches a remote endpoint, the OS-SBC will update the external IP for the remote endpoint.

This can be monitored on the SBC's **Maintenance & diagnostics** menu with the new button **Dynamic IP remote endpoints** under the **System Info** section:



This process is automatic and requires no further action on the part of the user.

On the NAT

The NAT should use a static IP toward the OS-SBC.

The NAT should NOT be SIP aware. If it is turn off SIP aware. The NAT also acts as the DHCP server for the phones.

On the OpenScape Branch

Local GUI-> VOIP-> Node 1 primary server-> set the address, transport and port of the WAN interface of the OS-SBC. <https://www.g-dms.com/livelink/lisapi.dll/view/inf-13-000221>

Note 9:

This must match the Logical ID created in the OSB

Local GUI-> VOIP-> "Enable Remote Endpoints" -> click on "Remote Endpoints configuration". Under "Remote Endpoints Configuration" click Add.

Under "Remote Endpoint Settings" enter the Name, Type and Profile.

Under "Remote Location Information" enter the Signaling address type as **"dynamic IP"**, **"Logical-endpoint-ID"** (this must be identical to the logical-endpoint-ID of the branch, port and Transport of the remote endpoint. **(not the address of the NAT)**)

Under "Remote Location Identification/Routing" enter the core side address and unique ports, as defined in the OSV, for the remote endpoint.

Under "Remote Location Domain List" click Add. See section [Remote Endpoints](#) for details. **(use the address of the NAT not the address of the branch)**.

Under "Access Side Firewall Settings" check "enable Firewall Settings", click on "Firewall Settings" See section [Remote Endpoints](#) for details.

On the NAT

The NAT may dynamically change it's IP address toward the OS-SBC. The NAT should NOT be SIP

aware. If it is turn off SIP aware.
The NAT also acts as the DHCP server for the phones.

On the OpenScape Branch

Local GUI->VOIP-> Node 1 primary server-> set the address, transport and port of the WAN interface of the OS-SBC. Verify the check box for "branch behind NAT" is set.

Verify the "Logical-endpoint-ID" is equal to the "Logical-endpoint-ID" used in the OS-SBC.

Port Mapping Table on the OS-SBC with devices registered

Local GUI-> Maintenance & Diagnostics-> Port Mapping.

The "external IP" address of the devices via the NAT, shows the address of the NAT.

Dynamic IP remote endpoints on the OS-SBC

Local GUI-> Maintenance & Diagnostics-> Port Mapping.

This should show the current relationship between the "Logical-endpoint-ID" and the current IP address of the NAT.

Note 10:

The core side IP address/ FQDN MUST be defined on the OS-SBC and be unique (it can not match the main core address of the OS-SBC or be used for SIP communications). This is then the address used in the OSV for the mediaserver.

On the OSV

Refer to the following description (three modes of configuring the media server).

3.5.9 OpenScape SBC remote endpoint configuration

These remote endpoints can be configured using Local GUI or CMP under Folder Features → Enable Remote Endpoints → Remote Endpoints Configuration.

Under Remote Endpoints configuration click **Add**.

Under Remote Endpoint Settings enter the Name, Type and Profile.

Type: This box defines the remote endpoint type.

Available options: **Gateway, Proxy, Branch SBC, Media Server, SSP, SBC, OSBIZ**.

Profile - In this box it is possible to choose a profile according to the remote endpoint Type assigned.

Possible options: **Gateway, Proxy, Branch SBC, Media Server, SSP, SBC, OSBIZ**.

For types Gateway, Proxy and Branch SBC a default profile is assigned,

for types Media Server and SSP, pre-configured profiles can be chosen.

For SBC, this configuration shall be used also in case of THIG where the SBC is configured behind SBC THIG.

For OSBIZ, it will validate incoming requests to the SBC access side based on the IP address or FQDN from the OSBIZ remote endpoint and it will not consider the remote port configured, because at OSBIZ it can be an ephemeral port. It will also perform the port mapping to the core side of multiple Via Headers.

Under Remote Location domain list enter the Remote URL (IP address, domain or Logical Endpoint ID), Remote SIP/MGCP port and Remote transport of the remote endpoint. See section [Remote Endpoint Configuration](#) for details.

Under Remote Location Identification/Routing enter the core Realm port. Not required if the default IP address of the OS SBC is to be used.

Remote Endpoints configuration

Add
Edit
Delete

▲ Row	Name	Access realm profile	Type	Profile / Circuit ID	Remote IP address / Logical-Endpoint-ID / Circuit URL	Remote port	Remote transport	Associated EP	Core realm profile	Core FQDN	Core port	Routing prefix	Default home DN
1	Gateway_Behind_OSB_Branch_SI	Main-Access-Realm - ipv4	Gateway	Gateway	10.191.0.50	5060	TCP		Main-Core-Realm - ipv4		50041		
2	OSB_Proxy_A	Main-Access-Realm - ipv4	Proxy	Default Proxy	10.191.0.20	5060	TCP		Main-Core-Realm - ipv4		50010		
3	Gateway_Behind_OSB_Proxy_B	Main-Access-Realm - ipv4	Gateway	Gateway	10.191.0.20	5096	TCP		Main-Core-Realm - ipv4		50021		
4	OSB_SBC_Proxy_mode	Main-Access-Realm - ipv4	Proxy	Default Proxy	10.191.0.40	5060	TCP		Main-Core-Realm - ipv4		50030		
5	Gateway_Behind_OSB_SBC_Prox	Main-Access-Realm - ipv4	Gateway	Gateway	10.191.0.40	5096	TCP		Main-Core-Realm - ipv4		50031		
6	OSB_Branch_SBC_mode	Main-Access-Realm - ipv4	BranchSBC	Default SBC	10.191.0.50	5060	TCP		Main-Core-Realm - ipv4		50040		
7	OSB_Proxy_B	Main-Access-Realm - ipv4	Proxy	Default Proxy	10.191.0.30	5060	TCP		Main-Core-Realm - ipv4		50020		
8	OSB_Behind_Static_NAT	Main-Access-Realm - ipv4	Proxy	Default Proxy	192.168.1.150	5060	TCP		Main-Core-Realm - ipv4		50050		
9	OSB_Behind_Dynamic_NAT	Main-Access-Realm - ipv4	Proxy	Default Proxy	osv.bg.branch	5060	TCP		Main-Core-Realm - ipv4		50060		
10	Standalone_Gateway_SBC	Main-Access-Realm - ipv4	Gateway	Gateway	10.191.0.100	5060	TCP		Main-Core-Realm - ipv4		50070		
11	OSB_A_AutoAttendant	Main-Access-Realm - ipv4	Proxy	Default Proxy	10.191.0.20	5096	UDP		Main-Core-Realm - ipv4		50011		
12	OSB_A_MediaServer	Main-Access-Realm - ipv4	MediaServer	Media_Server	10.191.0.20	2427	UDP		Main-Core-Realm - 2		2427		

Media Server Profiles

Add
Edit
Delete

▲ Row	Name	Time to live	Maximum conference time	Maximum announcement time	MGCP over SIP
1	Media_Server	30	18000	1800	<input type="checkbox"/>

Save
Cancel

3.5.10 OpenScape Voice endpoint configuration

These endpoints can be configured on the CMP under OpenScape Voice → Business Group → Members → Endpoints. Configure the endpoint Name, Profile, Endpoint Address and Port/Transport protocol, Aliases.

3.5.10.1 OpenScape Branch (OSB) configuration in OpenScape Voice

Create the Openscape Branch under the mainoffice.

CMP → OpenScape Voice → <select business group> → Main Office → Members → Endpoints → Add

On the General tab enter the Name, Profile and Endpoint template.

On the Sip tab, click “SIP trunking”, set the “Type” to “Static”, set the “signaling address type”, enter the “Endpoint address” (this will be the same address of the OS-SBC).

On the Sip tab enter a unique port number which will define the OSB in both the OSV and OS-SBC, also add this port to the list of “trusted entities”.

On the “Attributes tab” set the attributes of “Survivable Endpoint”, “SIP proxy” and “Route via Proxy”. On the “Aliases tab” add any IP address and port combination which may be used to communicate with the OSB. The entry is in the form of <IP address>:<port>

On the General tab click “Registered”

3.5.10.2 Gateway in OSB branch office configuration in OpenScape Voice

Create the gateway under the branch office.

CMP → OpenScape Voice → <select business group> → <branch office created above> → Members → Endpoints → Add

On the General tab enter the Name, Profile and Endpoint template.

On the Sip tab, click “SIP trunking”, set the “Type” to “Static”, set the “signaling address type”, enter the “Endpoint address” (this will be the same address of the OS-SBC).

On the Sip tab enter a unique port number which will define the OSB in both the OSV and OS-SBC, also add this port to the list of “trusted entities”.

On the “Attributes tab” set the attributes of “Route via Proxy”.

On the “Aliases tab” add any IP address and port combination which may be used to communicate with the OSB. The entry is in the form of <IP address>:<port>

On the General tab click “Registered”

3.5.10.3 Standalone Gateway directly in OS SBC configuration in OpenScape Voice

Create the Gateway under the main office.

CMP → OpenScape Voice → <select business group> → Main Office → Members → Endpoints → Add

On the General tab enter the Name, Profile and Endpoint template.

On the Sip tab, set the endpoint type, set the “Signaling type”, set the “signaling address type”, enter the “Endpoint address” (this will be the same address of the OS-SBC).

On the Sip tab enter a unique port number which will define the gateway in both the OSV and OS-SBC, also add this port to the list of “trusted entities”.

On the “Attributes tab” set the attributes of “Route via Proxy”

On the “Aliases tab” add any IP address and port combination which may be used to communicate with the OSB. The entry is in the form of <IP address>:<port>

3.5.10.4 Auto Attendant configuration in OpenScape Voice

There must also be routing created, which represents the DN of the auto attendant, pointing to this new endpoint.

In addition, a unique endpoint needs to be created, in the branch office, for the Auto Attendant in the branch. This must also use the concept of unique ports.

The associated end point should be the endpoint for the branch office. The transport should be UDP. The attributes should be “Survivable

Endpoint”, “Route via Proxy”, “Allow Proxy bypass” and “Public/Offnet traffic” The alias needs to be set with the OS-SBC address and port

3.5.11 *OpenScape Branch configuration*

Additional configuration is required on the OSB refer to the OSB configuration guide.
Refer to the OSB Configuration guide for more information.

3.5.11.1 OSB SBC-Proxy mode configuration

SBC-proxy mode enables the WAN interface of the OSB

For SBC-Proxy mode, the WAN interface is used to access SIP Service Providers. Subscribers and OpenScape Voice are in LAN in Proxy mode.

Local GUI → VOIP → OpenScape Branch Mode → select “SBC-Proxy” (this will enable interface 2) Local GUI → VOIP → check “Branch behind SBC

Local GUI → Network Services → Interface 2 → check box “Interface enabled”, enter the IP address of node 1 and the Subnet mask for this interface.

Local GUI → VOIP → check box “enable Gateways/Trunks” Local GUI → VOIP → click “Gateways/Trunks”

Local GUI → VOIP → “Enable Gateways/Trunks” → click on “Gateways/Trunks configuration”. Note that the gateway is created on the WAN interface enabled in the first step.

3.5.11.2 OSB Branch SBC mode configuration

Branch SBC mode enables the WAN interface of the OSB. The WAN interface of the OSB is used to connect to the OSS while the LAN interface is used for subscribers and gateways

On the Branch Phones

The checkmark for Outbound Proxy should be set.

The SIP server address should be the WAN address of the OS-SBC. The SIP registrar address should be the WAN address of the OS-SBC.

The SIP gateway address should be the LAN address of the OpenScape Branch. (not the LAN gateway IP)

Note if an external firewall is between the phones and the OS-SBC, then the external address of the firewall would be used in place of the WAN address of the OS-SBC.

3.5.12 *NAT configuration*

3.5.12.1 OSB SBC configuration using static NAT

On the OS SBC:

Local GUI → VOIP → “Enable Remote Endpoints” → click on “Remote Endpoints configuration”. Under “Remote Endpoints Configuration” click Add.

Under “Remote Endpoint Settings” enter the Name, Type and Profile.

Under “Remote Location Information” enter the Signaling address type, IP address, port and Transport of the remote endpoint. **(not the address of the NAT)**

Under “Remote Location Identification/Routing” enter the core side address and unique ports, as defined in

the OSV, for the remote endpoint.

Under “Remote Location Domain List” click Add. See section [Remote Endpoints](#) for details. (**use the address of the NAT not the address of the branch**).

Under “Access Side Firewall Settings” check “enable Firewall Settings”, click on “Firewall Settings” See section [Remote Endpoints](#) for details.

On the NAT

The NAT should use a static IP toward the OS-SBC.

The NAT should NOT be SIP aware. If it is turn off SIP aware. The NAT also acts as the DHCP server for the phones.

On the OpenScape Branch

Local GUI → VOIP → Node 1 primary server → set the address, transport and port of the WAN interface of the OS-SBC. <https://www.q-dms.com/livelink/lisapi.dll/view/inf-13-000221>

3.5.12.2 OSB SBC configuration using dynamic NAT

On the OS SBC:

Local GUI → VOIP → “Enable Remote Endpoints” → click on “Remote Endpoints configuration”. Under “Remote Endpoints Configuration” click Add.

Under “Remote Endpoint Settings” enter the Name, Type and Profile.

Under “Remote Location Information” enter the Signaling address type as “**dynamic IP**”, “**Logical- endpoint-ID**” (this must be identical to the logical-endpoint-ID of the branch, port and Transport of the remote endpoint. (**not the address of the NAT**))

Under “Remote Location Identification/Routing” enter the core side address and unique ports, as defined in the OSV, for the remote endpoint.

Under “Remote Location Domain List” click Add. See section [Remote Endpoints](#) for details. (**use the address of the NAT not the address of the branch**).

Under “Access Side Firewall Settings” check “enable Firewall Settings”, click on “Firewall Settings” See section [Remote Endpoints](#) for details.

On the NAT

The NAT may dynamically change it’s IP address toward the OS-SBC. The NAT should NOT be SIP aware. If it is turn off SIP aware.

The NAT also acts as the DHCP server for the phones.

On the OpenScape Branch

Local GUI → VOIP → Node 1 primary server → set the address, transport and port of the WAN interface of the OS-SBC. Verify the check box for “branch behind NAT” is set.

Verify the “Logical-endpoint-ID” is equal to the “Logical-endpoint-ID” used in the OS-SBC.

Port Mapping Table on the OS-SBC with devices registered

Local GUI → Maintenance & Diagnostics → Port Mapping.

The “external IP” address of the devices via the NAT, shows the address of the NAT.

Dynamic IP remote endpoints on the OS-SBC

Local GUI → Maintenance & Diagnostics → Port Mapping.

This should show the current relationship between the “Logical-endpoint-ID” and the current IP address of the NAT.

3.5.13 *Media server configuration*

On the OSV

NOTE: For more information related to Media Services in OpenScape Voice see the OpenScape Voice Administration Documentation, chapter 5 – Media Services.

3.5.13.1 **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 V10, Administration, Administrator Documentation**” or “**OpenScape Voice V10, Installation and Upgrades, Installation Guide**”.

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.

1. Under **Configuration > OpenScape Voice > Administration > Media Servers**, select **List** and Press **Add**:

UNIFY Common Management Platform Domain: system

Configuration Maintenance User Management Fault Management Performance Management

OpenScope Voice OpenScope Branch OpenScope SBC RG8700 Unified Communications CMP

[[BOCAST1]-]List Switch Settings for Media Servers

[WoWarcraft] - Media Server - Google Chrome

https://10.100.123.84/management/portal/Applications/Operation/OSV/Ad

[[BOCAST1]-]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

Name: OSB527

Fully Qualified Domain Name: [10.232.63.93]

Assign Method: Node Primary

Protocol Type: MGCP


Protocol Version: MGCP 1.0 NCS 1.0


MG Signaling IP Address Allocation Method: Static

MG Signaling: 10.232.63.93


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



[WoW Warcraft]-Media Server


 Configure Media Gateway Options

General
Extended
 Circuits


 In the Extended Section, you can configure the extended options of the Media Server.

Extended Options


 Extended options are listed below

Initial Retransmission Timer (ms):

Number Of Retransmissions:

Maximum Retransmission Time (s):

Final Response Timer (s):


History Timer Duration (s):

MG Receive Port:

MG Listen Port:

Keep Alive:

Overload Options


 Overload options are listed below

Overload Support:

Allow Surveillance Connections During Overload:

Overload Levels	Gap Interval (s)	Associated Return Code
Level 1	<input type="text" value="5"/>	<input type="text" value="406"/>

2. Depending on the traffic type being served 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: 10

<div></div>	Circuit ID	Circuit End Id	Circuit Type	
<div></div>	<div><div></div>ann/\$</div>	ann/\$	Announcement	<div></div>
<div></div>	<div><div></div>cnf/\$</div>	cnf/\$	Conference	<div></div>
<div></div>	<div><div></div>es/\$</div>	es/\$	Surveillance	<div></div>

Circuit Type: for media server. Possible circuit types Any, Announcement, Surveillance (US only), Conference, and Audit

P31003-S53A0-M101-30-76A9

234 OpenScape SBC V10 Configuration Guide

3. Create an **Origin** Destination for each traffic type: Announcements, Conference and Electronic Surveillance.
OSV -> Global Translation and Routing -> Destinations and Routes -> Origin Destinations.

[BOCAST1]-Origin Destinations

General Routes Intercepts

Origin Destinations description

Origin Destinations

Name: AnnOrigDest

Configuration Maintenance User Management

OpenScope Voice OpenScope Branch RG8700 Unified Communications CMP

[BOCAST1]

Global Translation and Routing

- Directory Numbers
- Translation
- Destinations and Routes
 - Destinations
 - Origin Destinations
 - Time Destinations
 - Routes
- Endpoint Management
- Display Number Modification
- ENUM

[BOCAST1] - Origin Destinations

This list shows all origin destinations:

Set:0 | Items/Page: 200 | All:3

Name
AnnOrigDest
CalOrigDest
CnfOrigDest

Following must be created:

- AnnOrigDest
- CnfOrigDest
- CalOrigDest (US only)

4. 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

[BOCAST1] - Edit Destination: DefDestAnn

Destinations are used to route a call to an endpoint.

General Routes Route Lists Destination Codes Origin Destinations

Name: DefDestAnn

is a media server: ☒

[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

1 Item

Add... Edit... Delete

ID	Endpoint	Route Type	Delete	Insert	Nature of Address
1	OSB527.ann/\$	MGCP-Media-Service	0		Undefined

OSB configured as main media server

[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 have integrated media server, OSB can function as secondary media server for load balancing.
- If Prioritized is check, 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

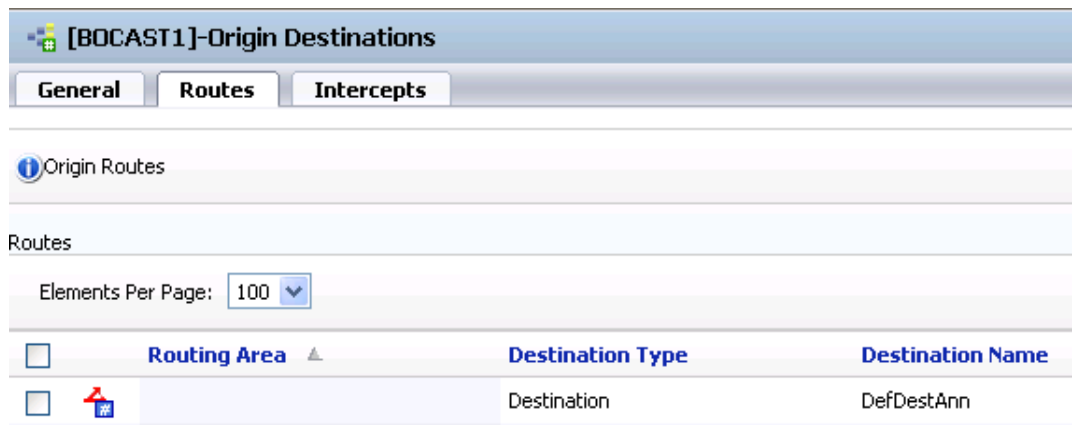
Note: When Routing Area is used only the matching Routing Area subscribers will have access to OSB Media Server.

[BOCAST1]-Origin Route

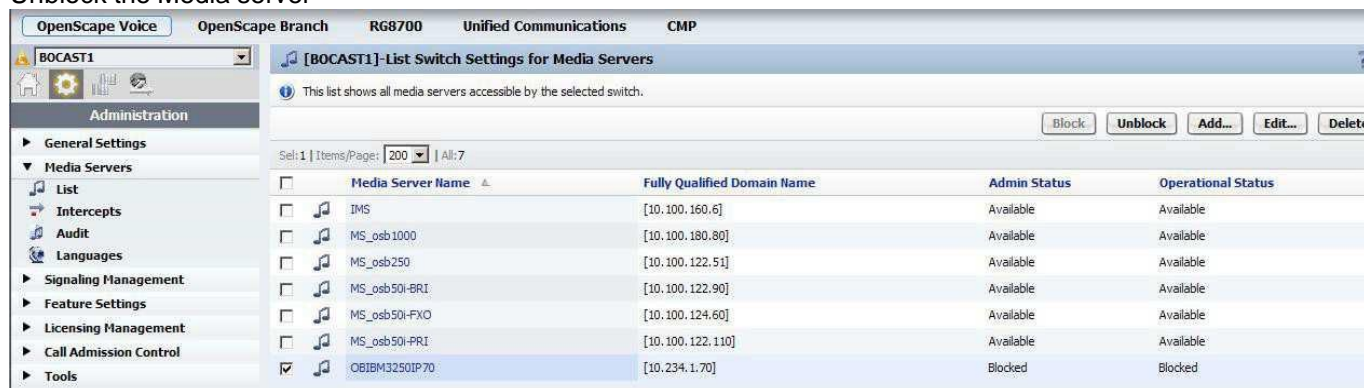
Routing Area: **...**

Destination Type: **▼**

Destination Name: **...**



7. 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:

/unisphre/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.

3.5.13.2 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.
Got 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_OS8527cnf

is a media server: ☒

10 Items

Name	Media Server
DEST_RAG0_ANN	True
DEST_RAG0_CNF	True
DefDestAnn	True
DefDestCal	True
DefDestCnf	True
Dest_41130B	True
Dest_OS8527ann	True
Dest_OS8527cal	True
Dest_OS8527cnf	True
Orig_Dest	True

Default destination from previous section

Destination for the Routing Area

4. Add Route to the Destination. Repeat for conference and surveillance.

[NodeV5] - Edit Destination: Dest_OSB527ann

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	OSB527.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.

Set: 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
	Destination	DefDestAnn
RA527	Destination	Dest_OSB527ann
RA_MS1	Destination	Orig_Dest
RA_OBMS1205	Destination	DEST_RAG0_ANN
RA_OBMS4113	Destination	Dest_4113OB

Routing Area that was created

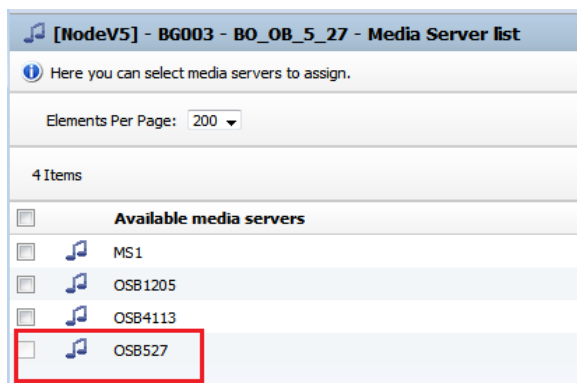
7. There are two ways to assign the OSB media server as a media server for a subscriber. The first is to assign the RA directly to the subscriber: Openscape Voice -> Business group -> Members -> Subscribers -> edit Sub -> Routing Tab -> Assign Rate Area (Routing Area)

The screenshot shows the 'Edit Subscriber' window for subscriber 9546660007. The 'Routing Information' tab is active. 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'.

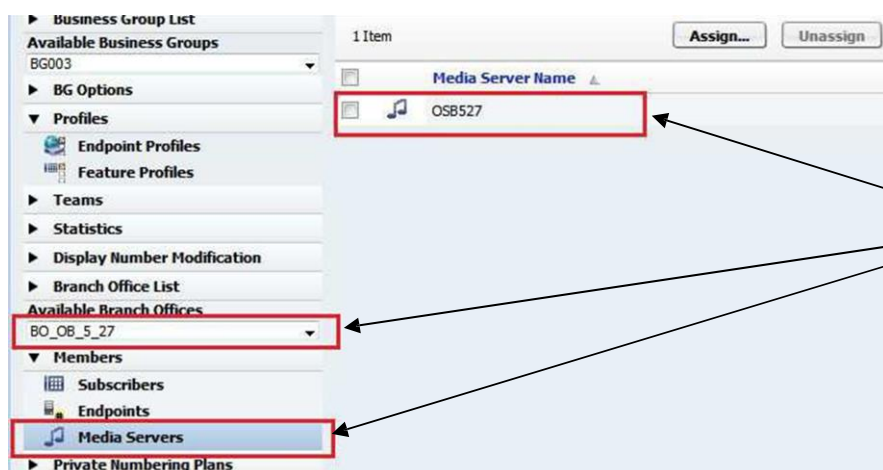
8. The second way is to assign the Rate Area for the entire Branch: Assign the newly added Routing Area to the Endpoint Profile of the Proxy serving the Branch Office. OSV -> Business Group -> BG(x) -> Profiles -> Endpoint

The screenshot shows the 'Edit Endpoint Profile' window for profile EPP_OB527. The 'Management Information' tab is active. The 'Routing Area' field is highlighted with a red box and contains the value 'RA527'. Other fields include 'Name' (EPP_OB527), 'Remark', 'Numbering Plan' (NPBG003), 'Class of Service', 'Calling Location', 'Time Zone' (LOCAL), 'SIP Privacy Support' (Basic), and 'Failed Calls Intercept Treatment' (Disabled). The 'Save' and 'Cancel' buttons are at the bottom.

9. Assign the Media Server that will serve the Branch Office.
 - 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 server the Branch Office as Media Server.



OSB is now a default media server for all members of this branch

****Note:** Can add more media server for this branch in case the branch can't handle all the media server needs.

10. Edit Intersect Treatment for Conference
 - Openscape Voice -> Administration -> Media Servers -> Intercepts -> Conference -> Treatments -> Add

11. 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).

12. Unblock the Media server (Branch Media Server configuration is completed)

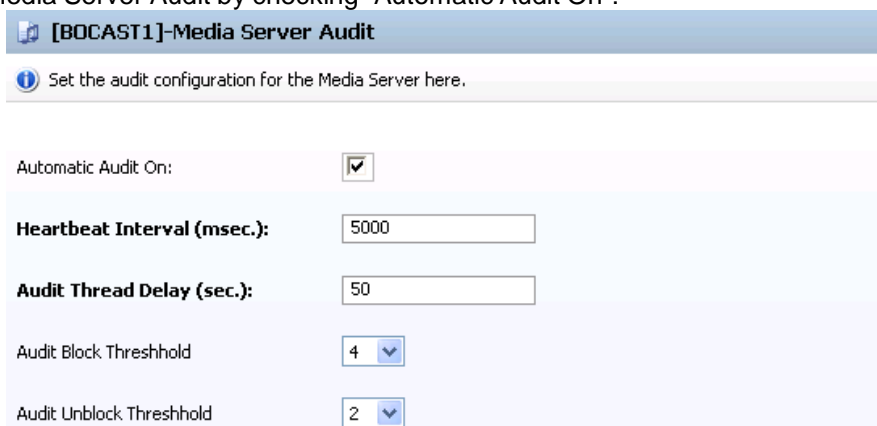
3.5.13.3 Configuring the main Media Server as a backup of the Branch MS:

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:

Enable Media Server Audit in the OSV:

Via CMP go to **OSV -> Administration -> Media Servers > Audit**

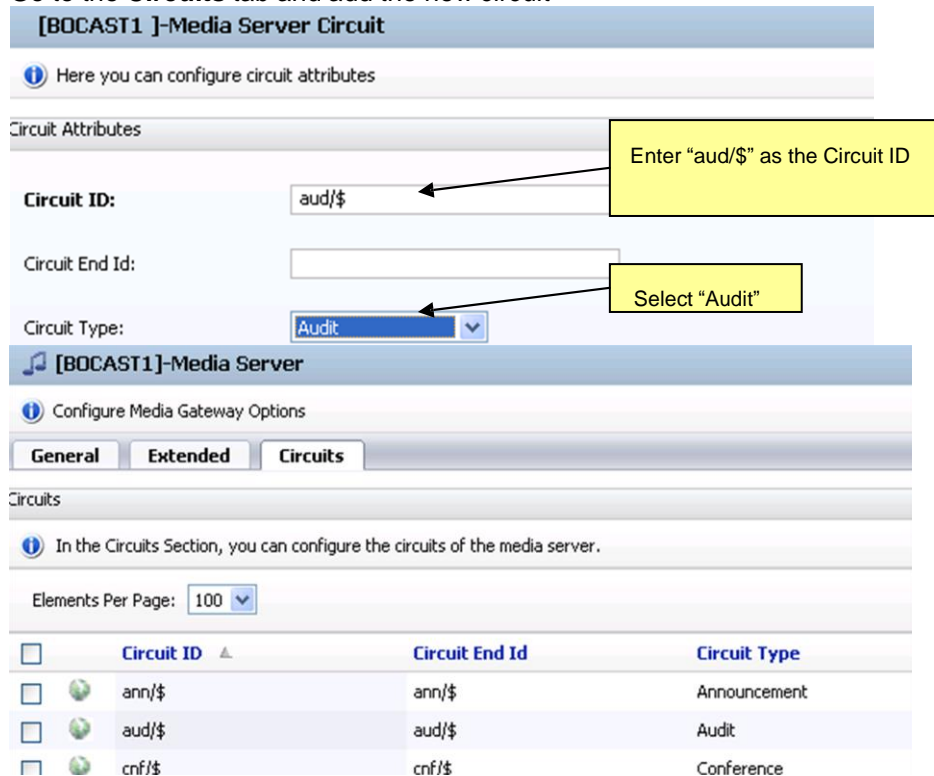
1. Enable the Media Server Audit by checking "Automatic Audit On":



2. Create the Audit circuit in the Branch Media Server.

Go to **OSV -> Administration -> Media Servers -> List** and click on the desired Branch Media Server.

3. Go to the **Circuits** tab and add the new circuit



	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

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 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

Routes

Elements Per Page: 100

<input type="checkbox"/>	Routing Area	Destination Type	Destination Name
<input type="checkbox"/>		Destination	DefDestAnn
<input type="checkbox"/>	bocaOB20_RA	Destination	DEST_RAG2_ANN
<input type="checkbox"/>	bocaOB21_RA	Destination	DEST_RAG3_ANN

Open the Destination from the above step.

Got to 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 an 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

<input type="checkbox"/>	ID	Endpoint	Route Type	Delete	Insert	Nature of Address
<input type="checkbox"/>	3	bocaOB21.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"/>

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”.

For more information about Media Services in OpenScape Voice see the OpenScape Voice Administration Documentation, chapter 5 – Media Services.

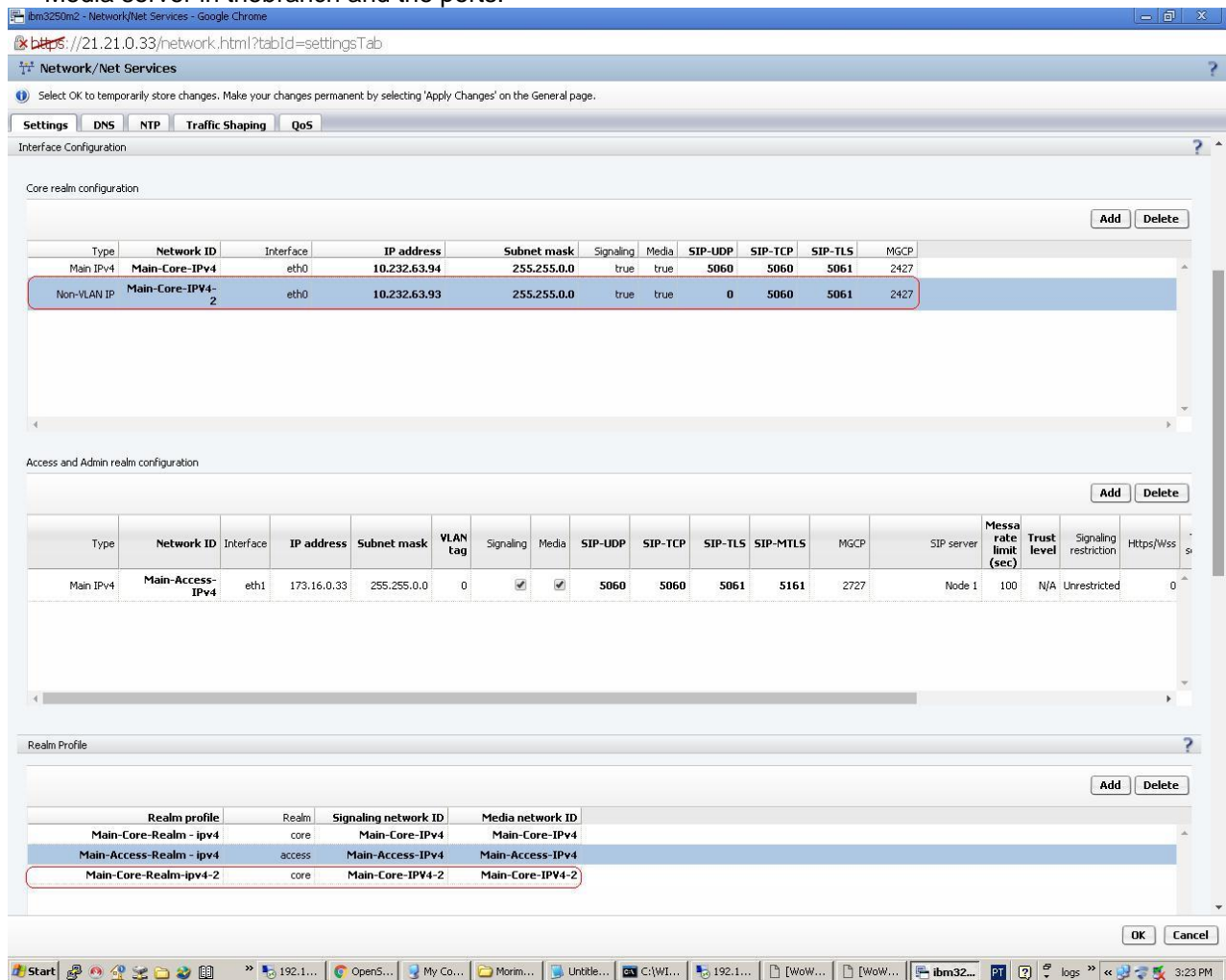
In the OS-SBC

1. Create the Media Server profile

Local GUI → Features → Remote Endpoints Configuration → Media Server Profiles → Add → select the name of the profile and parameters (in this case do not check MGCP over SIP)

2. Create the core realm for the MS.

Local GUI → Network / Net Services → Interface Configuration → Core realm configuration → Add
Pick non-Vlan IP, assign a name, interface = eth0, the IP address used in the OSV setup for the Media server in the branch and the ports.



3. Create a Realm Profile to be used

Local GUI → Network / Net Services → Realm Profile → Add

Pick a name, select the realm type as core, pick the network ID from step 2.

4. Create the remote endpoint for the Media Server in the branch.

Local GUI → Features → Remote Endpoints Configuration → Remote endpoints Configuration → Add

Under Remote endpoint Settings: Set the name, type = Media Server, Profile = the profile created in step 1, select the Access realm profile, select Core realm profile = from step 2.

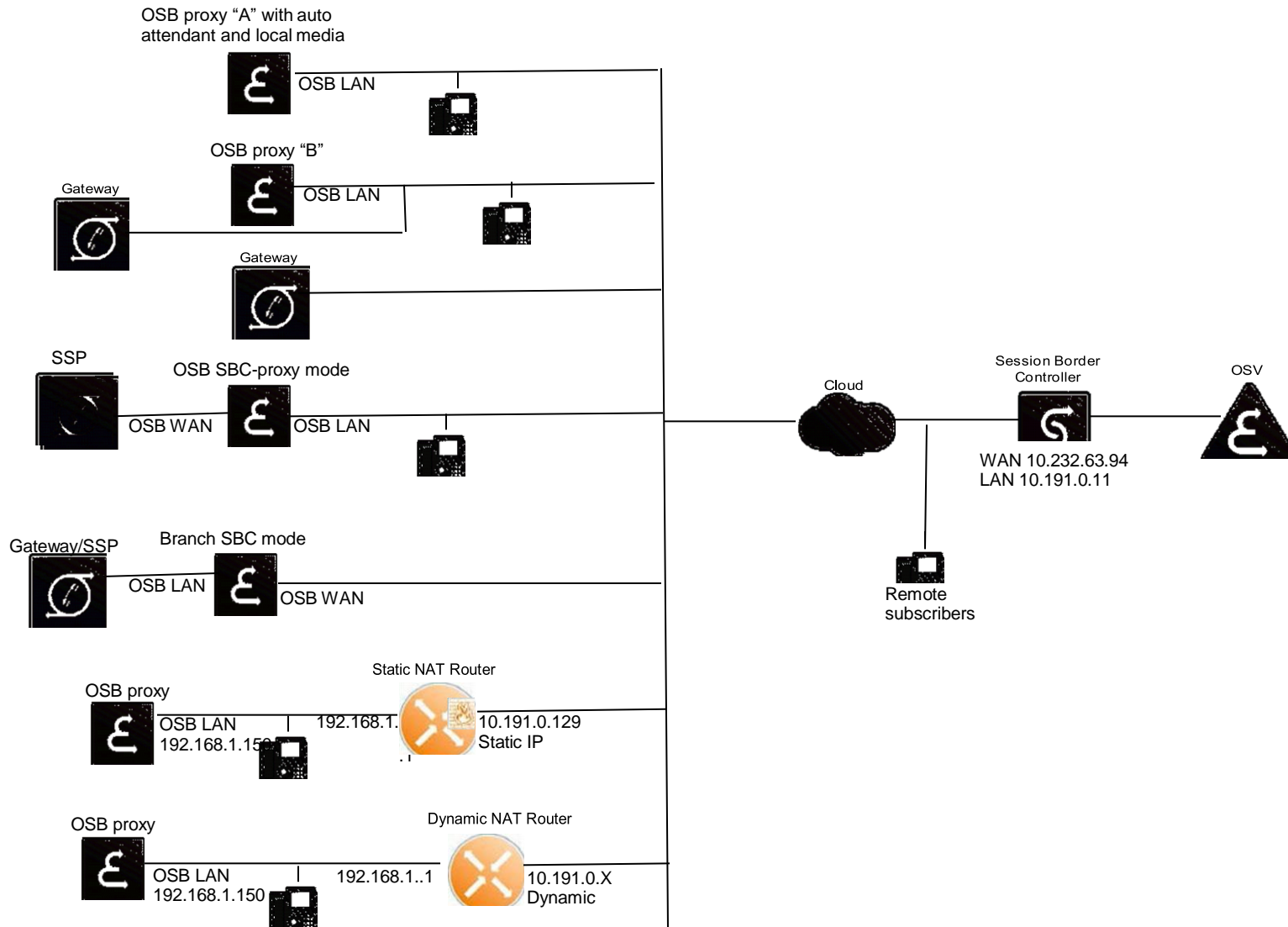
Under Remote Location Information: core realm port = 2427.

The core side IP address/ FQDN MUST be defined on the OS-SBC and be unique (it can not match the main core address of the OS-SBC or be used for SIP communications). This is then the address used in the OSV for the mediaserver.

In the OS-OSB

There is specific configuration required on the OSB to enable the media server. Refer to the OpenScape Branch (OSB) configuration Guide. <https://www.g-dms.com/livelink/llisapi.dll/view/inf-13-000221>

The media files required must be available on the OS-OSB.



Caution: For Gateways which need to register with the OSV via the OS-SBC:

Complete the configuration of the gateway, in the OSV and OS-SBC, (as shown on the next pages) prior to connecting the gateway and allowing it to register.
Failure to do so may cause the registration of the gateway to be challenged and fail.

3.6 SBC using OpenScape 4000 as SIP Server

3.6.9 Installation

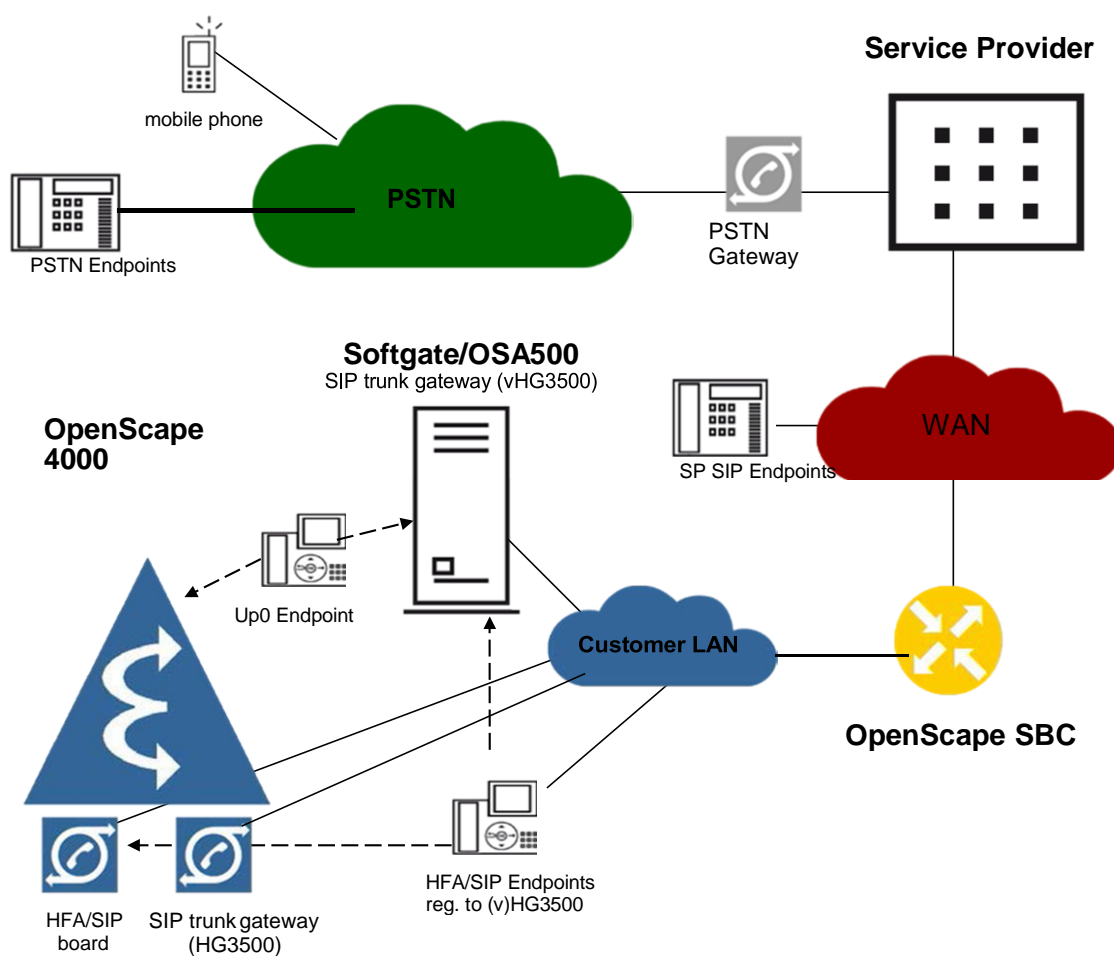
The picture shows the topology of OpenScape 4000 system, connected to SIP service provider over OpenScape SBC.

The OpenScape 4000 may consist of Host/AP and Softgate/OSA500 with e.g. HFA/SIP/Up0/analog endpoints.

A native SIP trunk gateway can be configured using a common gateway board (HG3500) or as virtual board on the Softgate (vHG3500) with provider specific profile.

IP address/Hostname (Registrar, Server) of the Provider is part of OpenScape SBC configuration.

The service provider may have a connection to the public PSTN network and to SIP endpoints, directly registered to the service provider.

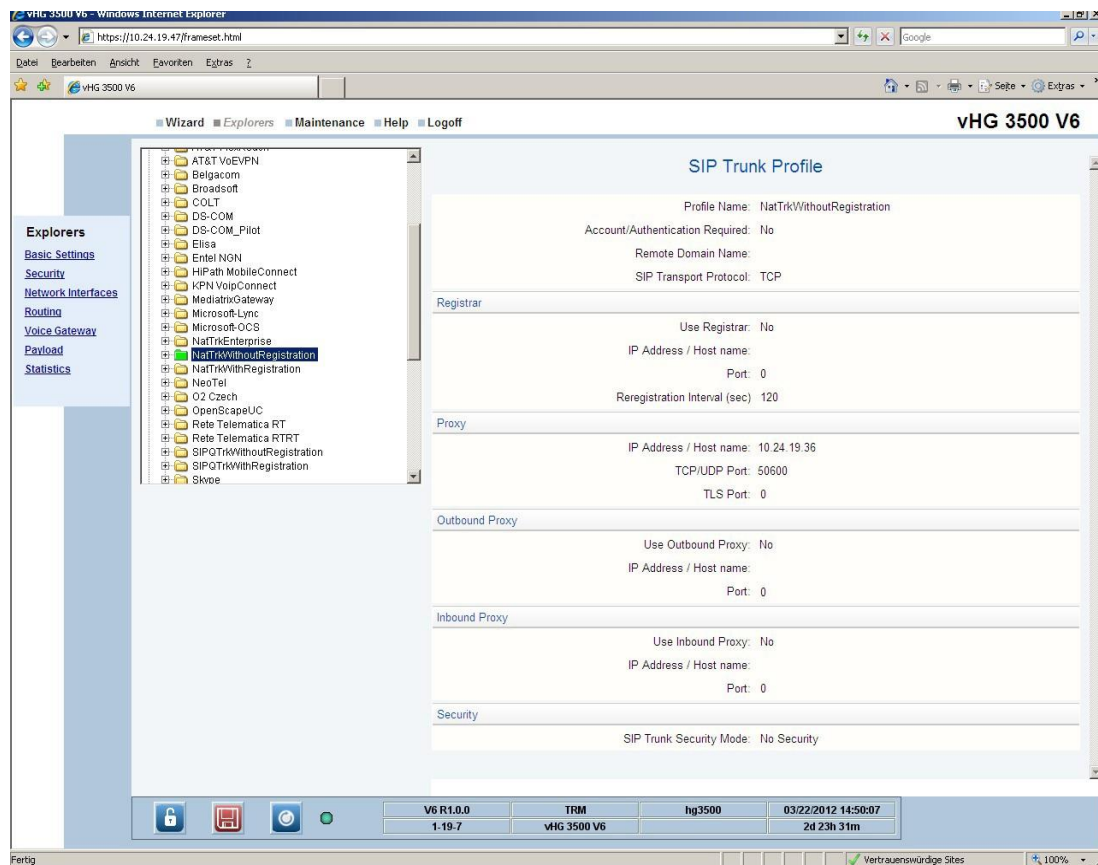


3.6.10 Configuration change at OpenScape 4000/HG3500 w/ OpenScape SBC

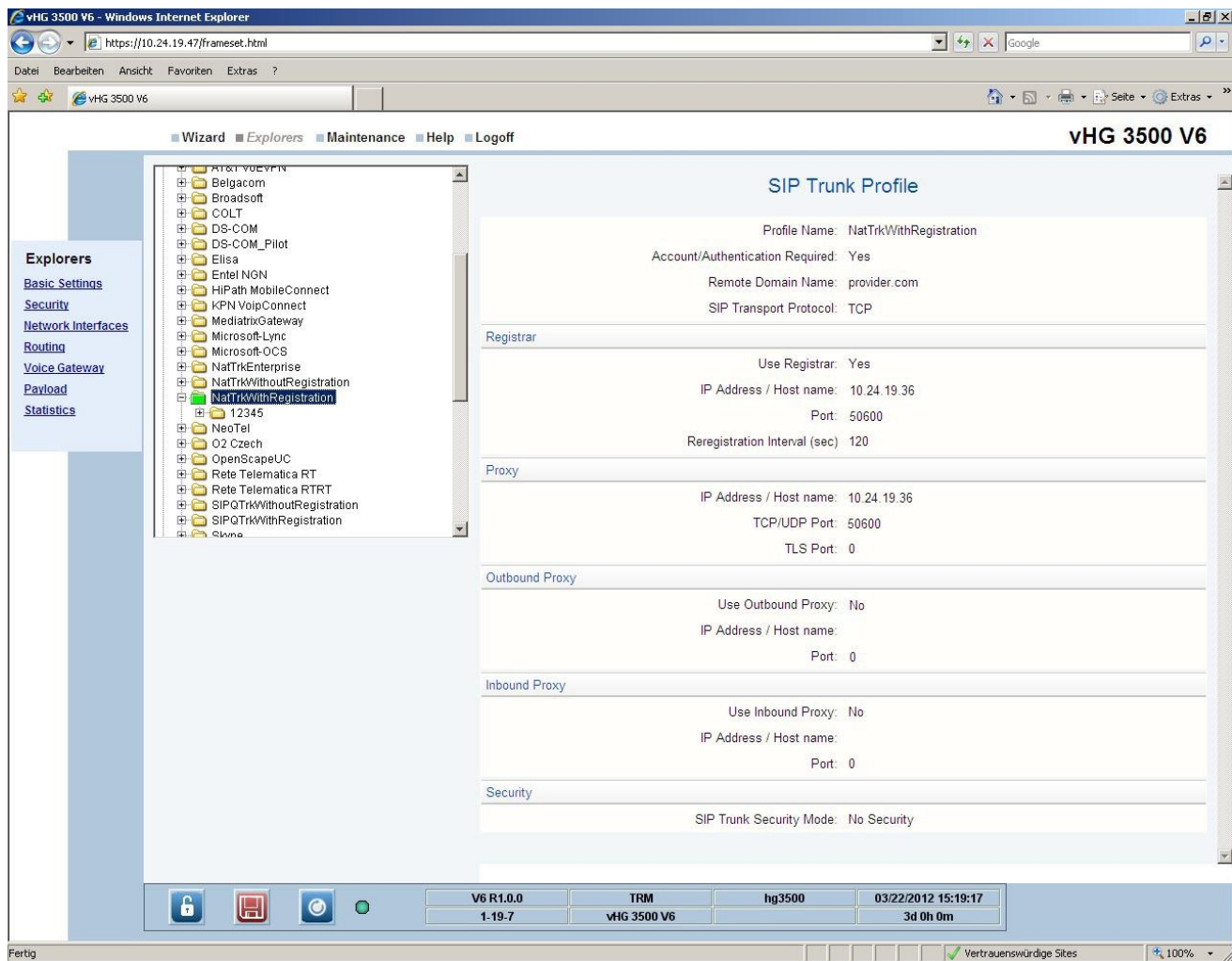
The configuration change at OpenScape 4000/HG3500 with OpenScape SBC has to be done within (v)HG3500.

The LAN interface between OpenScape 4000 HG3500/vHG3500 requires TCP, though the SIP Transport Protocol for the selected provider has to be set to TCP.

Registrar and Proxy, IP Address/ Host name and port has to be replaced with the LAN IP address and listen port of the OpenScape SBC.



The screenshot shows an example using a profile without registration, where 10.24.19.36 is the OpenScape SBC LAN IP and 50600 the OpenScape SBC listenport.



The screenshot shows an example with a profile with registration, where 10.24.19.36 is the OpenScape SBC LAN IP and 50600 the OpenScape SBC LAN listen port.

3.6.11 Configuration on OpenScape SBC

3.6.11.1 SIP Server Settings

The OpenScape 4000 connection can either be configured with Simplex or Clustered mode:

- Simplex (Primary server) with one single OpenScape 4000 (v)HG3500 gateway
- Clustered (Clustered servers) with several OpenScape 4000 (v)HG3500 gateways to bypass the OpenScape 4000 gateway limitation of 120 channels per gateway. In this case, the SBC is connected to multiple SIP servers at the core side and logically group the SIP server nodes into clusters. E.g. in the application scenario shown above there are N clusters (Group 1, Group 2, ... Group N) each containing up to N' nodes.

1) Simplex

Choose 'Simplex' as 'Comm System Type' and configure the OpenScape 4000 (v)HG3500 gateway ip address as 'Primary Server'. Set the transport protocol and port accordingly to the OpenScape 4000 gateway configuration.

ossV8R1 - VOIP - Google Chrome

<https://10.233.20.84/voip.html?tabId=sipTab>

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 | Media | QoS Monitoring

General

Comm System Type: Simplex

☒ Allow Register from SERVER

Other trusted servers

Node 1

Target type: Binding

Primary server: 10.233.20.106 Transport: TCP Port: 5060

Backup server: Transport: TCP Port:

SRV record: Transport: TCP

Node 2

Target type: Binding

Primary server: Transport: TCP Port:

Backup server: Transport: TCP Port:

SRV record: Transport: TCP

OK Cancel

Allow Register from SERVER: this has to be checked, if a provider profile with registration is activated in the (v)HG3500 WBM, see above.

2) Clustered

Choose 'Clustered' as 'Comm System Type' and switch to 'Clustered servers' configuration dialog. In this dialog the needed clusters may be configured.

Sip Server Settings | Port and Signaling Settings | Error Codes | Media | QoS Monitoring

General

Comm System Type: Clustered

☐ Allow Register from SERVER

☐ Use RURI to Route to Comm System

☐ Bond TCP Connection to SLB

Clustered servers

Clustered Nodes settings

Ping Method: OPTIONS OPTIONS interval (sec): 30

Failure threshold (pings): 2

Each rule is treated as own node, therefore, Group Name, Priority, Routing Prefix, Ip/FQDN, Port must be
P31003-S53A0-M101-30-76A9 253 OpenScape SBC V10 Configuration Guide

configured individually for each gateway rule.

clustered Servers ?										
Select OK to temporarily store changes. Make your changes permanent by selecting 'Apply Changes' on the General page.										
										Add Delete
Group ID	Group name	Node Name	Priority	Routing prefix	IP address or FQDN	Port	Transport	Stick with CommServer	No Answer timer (msec)	No Reply timer (msec)
1	4g_grp1_anl7	sg33_vhG1	1	+55	192.1.33.75	5060	TCP	<input type="checkbox"/>	360000	3000
2	4g_grp1_anl7	sg33_vhG1	1	970	192.1.33.76	5060	TCP	<input checked="" type="checkbox"/>	360000	3000
3	4g_grp1_anl7	sg33_vhG1	1	970	192.1.50.79	5061	TLS	<input type="checkbox"/>	360000	3000

Subsequent to the cluster configuration the 'SIP server' in the 'Access and Admin realm configuration can be configured accordingly, for each interface rule a specific group can be configured or "Any" to allow all groups to be used by the interface

Network/Net Services

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

Settings **DNS** NTP Traffic Shaping QoS

Interface Configuration

Core realm configuration

Add Delete

Type	Network ID	Interface	IP address	Subnet mask	Signaling	Media	SIP-UDP	SIP-TCP	SIP-TLS	MGCP
Main IPv4	Main-Core-IPv4	eth0	192.1.33.99	255.255.255.0	true	true	5060	5060	5061	2427

Access and Admin realm configuration

Add Delete

Type	Network ID	Interface	IP address	Subnet mask	VLAN tag	Signaling	Media	SIP-UDP	SIP-TCP	SIP-TLS	SIP-MTLS	MGCP	SIP server	Messa rate limit (sec)	Ti k
Main IPv4	Main-Access-IPv4	eth1	214.18.44.199	255.255.255.0	0	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	5060	5060	5061	5161	2727	4k grp1 - anl7	100	




After these configuration steps the configuration may be applied with 'Apply changes'.

Note: Every applying of changes to the cluster will restart the SIP server in the OS-SBC. This means that all active and ongoing connections will be affected/terminated.

The availability of the single cluster nodes can be monitored from the OS-SBC dashboard by switching to the 'Show clustered nodes' dialog.

clustered Servers

clustered servers provisioning.

St	State	Group Name	Node Name	Routing Prefix	IP Address
	Active	4k grp1 - anl7	sg33 vHG1	+55	192.1.33.75
	Active	4k grp1 - anl7	sg33 vHG2	970	192.1.33.76
	Active	4k grp1 - anl7	sg50 vHG1	970	192.1.50.79

Routing Prefix configuration for Clustered mode

For "clustered mode" the Routing prefix does not use regular expression. It just checks the prefix and uses the best match criteria.

The validation is described in RFC3986 for userinfo:

userinfo = *(unreserved / pct-encoded / sub-delims)


unreserved = ALPHA / DIGIT / "-" / "." / "_" / "~"


ALPHA = A-Z | a-z

DIGIT = 0-9

pct-encoded = "%" HEXDIG HEXDIG

sub-delims = "!" / "\$" / "&" / "'" / "(" / ")" / "*" / "+" / "," / ";" / "="


clustered Servers


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

Add

Delete

Group ID	Group name	Node Name	Priority	Routing prefix	IP address or FQDN	Port	Transport	Stick with CommServer	No Answer timer (msec)	No Reply timer (msec)
1	Group_1	Default	1		1.1.1.1	5060	TCP	<input type="checkbox"/>	360000	3000
2	Group_2	General_1	1	+22	2.2.2.1	5061	TLS	<input checked="" type="checkbox"/>	360000	3000
3	Group_2	General_2	2	+22	2.2.2.2	5060	TCP	<input checked="" type="checkbox"/>	360000	3000
4	Group_2	General_2	3	+22	2.2.2.3	5060	TCP	<input checked="" type="checkbox"/>	360000	3000
5	Group_3	Gw_1	1	+33	3.3.3.1	5060	TCP	<input type="checkbox"/>	360000	3000
6	Group_3	Gw_2	1	+33	3.3.3.2	5060	TCP	<input type="checkbox"/>	360000	3000
7	Group_4	Specific_1	1	+44	4.4.4.1	5060	TCP	<input type="checkbox"/>	360000	3000
8	Group_5	GTC	1	+55	5.5.5.1	5060	TCP	<input type="checkbox"/>	360000	3000

Following the example configuration given, several groups are configured for different purposes. Group_1 works as a default rule for every call that doesn't match any other rule. Group_2 has three rules with the same routing prefix and different priority, the behavior will be that every call with that matching prefix will go in the order of the priority, this group also has the stick with commserver set this mean that the device after registering in one of the servers available in this group the device will keep sending its requests to that server ignoring the other rules of the group. Group_3 has two rules with the same priorities and routing prefix, in this group the calls will work in a round robin logic, the calls matching the prefix will rotate between the two servers. Group_4 works for a specific range of numbers that match +44 prefix and needs to go to the specific server 4.4.4.1. Group_5 works for GTC, GTC can demand its own group, it can be done by configuring a specific routing prefix or activating the flag Enable Cluster Server on the GTC endpoint configuration. Keep in mind that if the SipServer field on the access interface is set to 'any' the system will consider all rules as part of the same group, meaning that the priorities and routing prefixes becomes the main configuration to differentiate each group behavior.

3.6.11.2 Remote Endpoints Configuration

The SIP service provider related data is configured under RemoteEndpoints.

SIP Service Profile:

At first, create a service provider profile, that is generally used for SIP provider connectivity with OpenScape 4000;

General ?

Name4kDefaultProfileDefault SSP profile▼

☐ Use SIP Service Address for all identity headers

SIP service address

SIP User Agent

SIP User Agent towards SSPPassthru▼SIP User Agent(not licensed)

Registration ?

☐ Registration required

Registration interval (sec)3600

Business Identity ?

☐ 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

☐ Use To DN to populate the RURI

☐ Send Default Home DN in Contact for Call messages

☐ 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 pass-through of Optional parameters(not licensed)

☐ Send default Home DN in PAI/PPI

☐ Preserve To and From headers per RFC2543

☐ Allow single SSP with different home DN prefix based handling

☐ Ignore last digit in Default home DN for incoming calls from SIP trunk

Digest Authentication ?

☐ Digest authentication supported

Digest authentication realm

Digest authentication user ID

Digest authentication password

TLS ?

TLS SignalingPass-Thru▼

Sip Connect ?

☐ Use tel URI

☐ Send user=phone in SIP URI

☐ Registration mode

☐ ITR 118

There is no special selection necessary in that profile for OpenScape 4000 as the OS4K SIP Provider Profile Settings will be used anyway from OS4K through the OS-SBC. Just create it as default profile.

P31003-S53A0-M101-30-76A9

257 OpenScape SBC V10 Configuration Guide

Remote Endpoints Configuration:

In the next step the Remote Endpoint pointing to the SIP Service Provider must be added. Click **Add**.

Remote Endpoint Settings:

- **Name:** Please define a name for the SIP Service Provider
- **Type:** Please choose type "SSP"
- **Profile:** Please choose the previously defined SIP Service Provider Profile e. g. `4kDefaultProfile`
- **Signaling address type:** Depending on SIP Service Provider the corresponding setting (IP or FQDN or DNS SRV) must be chosen.
- **Remote Location domain list:** Please click "Add" and configure the SIP Service Provider data like IP or DNS name (Remote URL) of the SSP.
- **Core realm port:** Please enter the used (v)HG port used in WBM e. g. 50600 (see chapter **3.6.2**)

Using DNS SRV (domain name) the remote port is automatically set to 0. The port configuration is received by DNS SRV.

Remote Endpoint Settings
?

Name
SIP-Service-Provider-Name
Type
SSP
Profile
4#DefaultProfile
Access realm profile
Main-Access-Realm - ipv4
Core realm profile
Main-Core-Realm - ipv4
Associated Endpoint
Enable Call Limits
Maximum Permitted Calls
0
Reserved Calls
0

This screenshot shows an example, where the SIP Service Provider is configured with a DNS SRV name. "Remote URL" can be used also for IP addresses in case SSP provides IP. Please change "Signaling address type" accordingly.

Remote Location Information
?

URI based routing
Enable access control
Signaling address type
DNS SRV

Remote Location domain list
?

Add
Delete

Remote URL	Remote SIP/MGCP port	Remote transport	Media IP	Media profile	TLS mode	Certificate profile	TLS keep-aliv
provider.com	5060	TCP		webrtc_default	Server authentication	OSV Solution	

Remote Location Identification/Routing
?

Core FQDN
Core realm port
50600
Default core realm location domain name
Routing prefix
Default home DN

Access Side Firewall Settings
?

Enable Firewall Settings
Firewall Settings

Emergency configuration
?

Emergency numbers
Add
Delete
Emergency calling subnets

MSRP Data Configuration
?

Enable MSRP Relay Support (not licensed)
use IP address in MSRP-path
use FQDN in MSRP-path
FQDN
Authentication required
Realm
Password
Show
Access side only
Qop
AUTH
Expire time/sec
300

3.6.11.3 Remote Endpoint configuration for OpenScape 4000

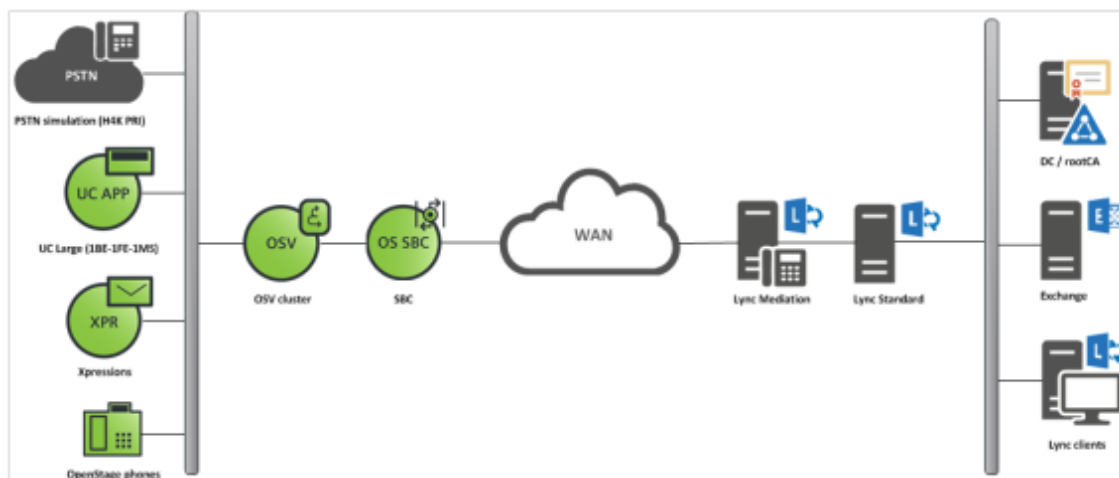
The configuration of remote endpoints to work with OpenScape 4000 as SIP server is no different from remote subscriber configuration as described in 3.4.5.1. The only exception is, if OpenScape 4000 is used in cluster mode, in this case the routing prefix is used to send the request to a specific OpenScape 4000 node or a group and the remote subscriber should belong to the numbering plan to this node or group.

3.6.12 Restrictions

UPDATE with SDP data is not supported by OpenScapeSBC;

- DMC has to be disabled (AMO TDCSU: DMCALLWD=N) for the SIP trunk, UPDATE w/ SDP is not sent by OpenScape 4000/(v)HG3500.
- UPDATE is offered in the Allow header, a provider might send UPDATE w/ SDP; in this case a special profile has to be provided by OpenScape 4000 as workaround (CR created for OpenScape SBC).

3.7 Support secure calls to Microsoft Lync Mediation Server



The OpenScape SBC is configured with a Remote Endpoint for each Mediation Server.

1. From SBC Management portal, go to **Network/Net Services >Settings:**

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

Settings | DNS | NTP | Traffic Shaping | QoS

Interface Configuration

Core realm configuration

Add Delete

Type	Network ID	Interface	IP address	Subnet mask	Signaling	Media	SIP-UDP	SIP-TCP	SIP-TLS	MGCP
Main IPv4	Main-Core-IPv4	eth0	10.6.5.205	255.255.255.192	true	true	5060	5060	5161	2427

Access and Admin realm configuration

Add Delete

Type	Network ID	Interface	IP address	Subnet mask	VLAN tag	Signaling	Media	SIP-UDP	SIP-TCP	SIP-TLS	SIP-MTLS	MGCP	SIP server	Message rate limit (sec)
Main IPv4	Main-Access-IPv4	eth1	10.10.170.195	255.255.255.0	0	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	5060	5060	5061	5067	2727	Node 1	100

OK Cancel

- a. At **Core realm configuration**, set e.g., SIP-TLS=5161
 - b. At **Access and Admin realm configuration**, set e.g., SIP-MTLS=5067 (Lync mediation Server port in accordance to configuration at Lync)
2. From SBC Management portal, go to **VOIP >Sip Server Settings:**
 - a. We may use the OSV SIPSM1 and OSV SIPSM2 IP values for MTLS, but we need to add OSV SIPSM3 and OSV SIPSM4 IPs for MTLS in the **other trusted servers** field.
 - b. Set port value e.g., "5161"

3. Under **Media** create two different "Media Profiles"; one for the SBC-OSV connection (e.g. OSV) and one for P31003-S53A0-M101-30-76A9

SBC-Lync Mediation (e.g. Lync).

The screenshot shows the VOIP configuration window with the 'Media' tab selected. The 'Core Side Media Configuration' section has 'Media profile' set to 'OSV'. Below this is a table for 'Media Profiles' with the following data:

Profile name	Codecs	Media protocol	Key exchange method	Mark sRTP Call-leg as Secure	Single m-line SRTP
default		Best Effort SRTP	mikey + sdes		
webrtc_default		SRTP only	dtls	✓	
OSV		Best Effort SRTP	mikey + sdes	✓	
Lync		Best Effort SRTP	sdes		✓

- Under **Core Side Media Configuration**, select the value e.g. “OSV” (custom).
- Under **Media Profiles** for the “OSV” profile, select:

The **Media Protocol** should be “Best Effort SRTP”.

The **Key exchange method** should be “mikey + sdes” (set based on OSV domain equipment preference).

The **Mark SRTP Call-leg as Secure** should be “enabled/checked”.

- Under **Media Profiles** for the “Lync” profile, select:
 - The **Media Protocol** should be “Best Effort SRTP”.
 - The **Key exchange method** should be “mikey + sdes”.
 - The **Single m-line SRTP** should be “enabled/checked”.

- From SBC Management portal, under **Features>Enable Remote Endpoints** create the trunk between SBC and Lync Mediation Server. A Remote Endpoint should be created for each Mediation Server. An example:

Remote Endpoints ?

Remote Endpoints provisioning.

Service Provider Profiles ? ^

Add Edit Delete

Row	Name	Registration required	Registration interval
1	LyncCon	<input type="checkbox"/>	3600

Remote Endpoints configuration ?

Add Edit Delete

Row	Name	Access realm profile	Type	Profile / Circuit ID	Remote IP address / Logical-Endpoint-ID / Circuit URL	Remote port	Remote transport	Associated
1	LyncMED	Main-Access-Realm - ipv4	SSP	LyncCon	10.10.170.185	5067	TLS	

Save Cancel

5. A new Service Provider Profile is required:

SIP Service Provider ?

SIP Service Provider Provisioning.

General ? ^

Name Default SSP profile

☐ Use SIP Service Address for all identity headers

SIP service address

Registration ?

☐ Registration required

Registration interval (sec)

Business Identity ?

☐ Business identity required

Business identity DN

Manipulation ?

☐ Insert anonymous caller ID for blocked Caller-ID

Manipulation

Flags ? v

OK Cancel

- a. Select for “**Default SSP Profile**” the option “Lync Mediation Server”.

6. Add to “Remote Endpoint configuration” table:

Remote endpoint provisioning.

Remote Endpoint Settings

Name

LyncMED

Edit

Type

SSP

Profile

LyncCon

Access realm profile

Main-Access-Realm - ipv4

Core realm profile

Main-Core-Realm - ipv4

Associated Endpoint

☐ Enable Call Limits

Maximum Permitted Calls

0

Reserved Calls

0

Remote Location Information

☐ URI based routing

☐ Enable access control

Signaling address type

IP address or FQDN

Remote Location domain list

Add

Delete

Remote URL	Remote SIP/MGCP port	Remote transport	Media IP	Media profile	TLS mode	Certificate profile	TLS Keep-Alive	Keep-Alive
10.10.170.185	5067	TLS		Lync	Mutual authentication	OSV Solution	<input type="checkbox"/>	

Remote Location Identification/Routing

Core FQDN

Core realm port

5161

Save

Cancel

- a. Select for **Type** the option “SSP”.
- b. Select for **Profile** the option “LyncCon” (the one created previously at step 3).
- c. At **Remote URL**, enter the value e.g., “10.10.170.185” (the Lync mediation Server IP)
- d. At **Remote SIP/MGCP port**, enter the value e.g., “5067” (Lync mediation Server port)
- e. At **Remote transport**, use “TLS”.
- f. At **Media profile**, select e.g., “Lync” (custom media profile).
- g. At **TLS mode**, select “Mutual authentication”.

- h. At **Certificate profile**, select a value e.g. "OSV Solution" (it could be a custom one)
- i. The value **TLS Keep-Alive** should be "disabled/unchecked".
- j. For **Core realm port**, set the value e.g., "5161" (setting at OSV port)

There are three different approaches in order to create and distribute the certificates in the secure SIP trunking environment of FRN10055.

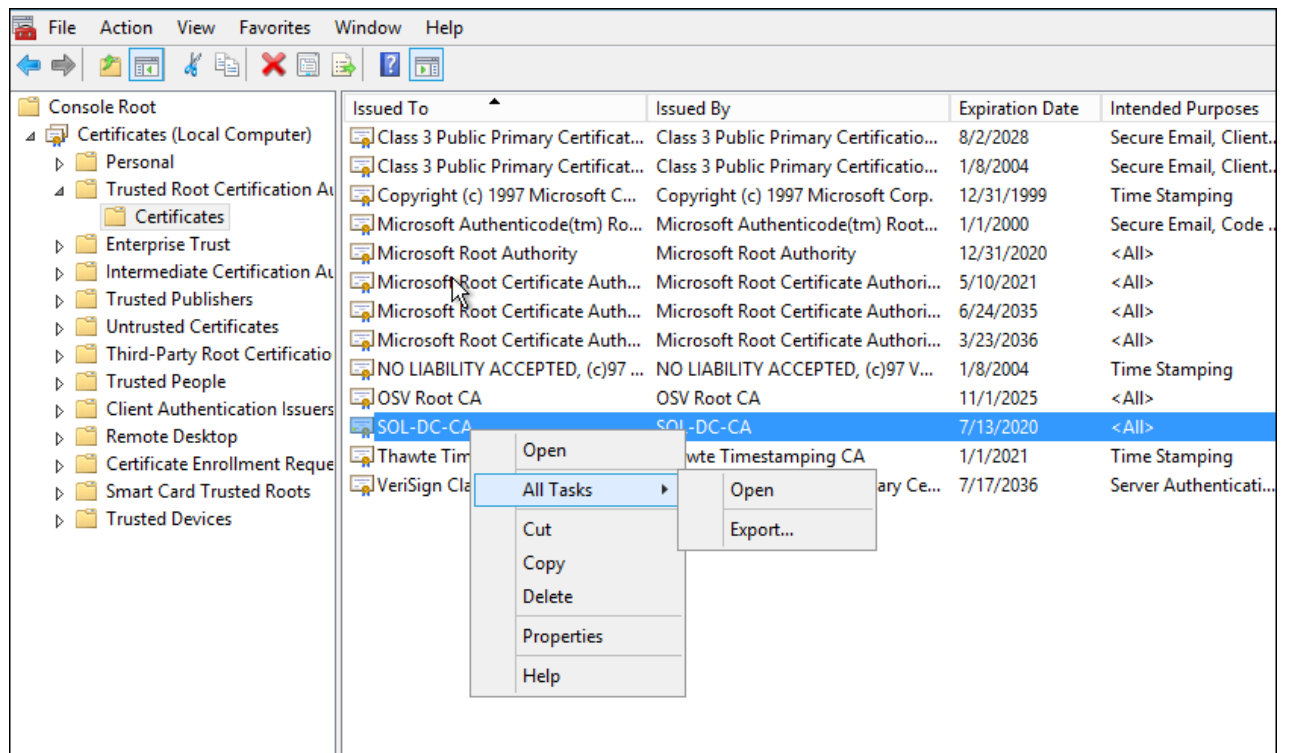
Notwithstanding, which of the following approaches is going to be used the principles for the certificates are the same.

A first approach is that OpenScape Servers and Microsoft Servers to have the same CA. This is the more probable scenario in customer environment.

Another approach is to have a different CA for OSV and a different CA for Lync + SBC.

The third approach is the one used in the current Lab environment for secure media interworking. OSV domain (including SBC) has a custom CA and Lync domain has a different CA. This is the one to be analyzed in the subsequent steps.

1. The OSV rootCA certificate file need to be imported in the trusted CA store of Lync Mediation server in order to trust the SBC server certificate during MTLS handshake.
 - a. At OSV's folder /usr/local/ssl/certs convert "root.pem" to e.g. "rootOSV_CA.crt" with openssl command: `openssl x509 -in root.pem -out rootOSV_CA.crt -outform DER`
 - b. Import "rootOSV_CA.crt" in Lync Mediation Server's "Trusted Root Certification Authorities" store
2. The Lync domain root CA certificate should be imported in the trusted CA store of SBC so as SBC to trust Lync Mediation's server certificate during MTLS handshake
 - a. Export from a Lync server with the use of MMC the RootCA certificate file (with private key) in DER format (e.g. LyncCA.cer)



- b. Convert LyncCA.cer to LyncCA.pem to import to SBC with openssl command: `openssl x509 -inform der -in LyncCA.cer -out LyncCA.pem`

3. At OSV, create the necessary server certificate for SBC.

During TLS handshake between SBC and Lync, the SBC server certificate will be presented to Lync Mediation for validation. In order Lync Mediation to accept SBC server cert, the latter needs to satisfy the following:

For **Common Name** or in the **SAN** field, the FQDN used in the configuration for Lync Mediation (step 1 section 3.3.1.2) e.g., "sbc10055.h8k.sec".

In **SAN** field the IP of SBC WAN interface must also be included e.g. "10.10.170.195"

The SBC server certificate must also have the following extensions, which are required from Lync :

The "X509v3 Key Usage".

The "X509v3 Extended Key Usage".

The "X509v3 CRL Distribution Points"; a dummy URI may be used e.g., "URI:http://cert_auth.com/CA_crl", since Lync doesn't check the URL to verify if it's reachable.

The contents of the certificate can be viewed with openssl command e.g.
`openssl x509 -in server-cert.pem -text -noout`

4. From SBC Management portal, go to **Security>General>Certificate management** and upload the certificate files:

+

Certificate Management

?

?

Certificate management provisioning.

Certificates Upload

?

^

CA Certificates

Upload CA certificate file

Browse...

Upload

CA certificates

LyncCA.pem
root.pem
serverCA.pem

Delete

X.509 Certificates

Upload X.509 certificate file

Browse...

Upload

X.509 certificates

server-cert.pem
servercert.pem

Delete

Key Files

Upload key file

Browse...

Upload

Key files

clientserver-key.pem
serverkey.pem

Delete

OK

Cancel

a. The **CA certificates** contain:

P31003-S53A0-M101-30-76A9

- The file `root.pem` (CA file for OSV domain)
 - The file e.g., `LyncCA.pem` (created in step 2)
- b. The **X.509 certificates** contain the SBC server certificate e.g., `server-cert.pem`.
- c. The **Key files** contain the SBC client-server certificate private key e.g., `clientserver-key.pem`.
5. At **Security > General > Certificate management > Certificate Profiles** configure **OSV Solution** profile or create a custom one.

Certificate Management

System Certificate

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		server-cert.pem	root.pem	LyncCA.pem	clientserver-key.pem
HTTPS System Default	HTTPS		server.crt			server.key

Certificate Creation

Create New TLS Certificates

Name: CA file: Self signed Create

Certificates Upload

CA Certificates

Upload Unload

OK Cancel

At **Server certificate file** use e.g., “`server-cert.pem`”

At **Local CA file** use e.g., “`root.pem`”

At **Remote CA file** use e.g., “`LyncCA.pem`”

At **Key files** use e.g., “`clientserver-key.pem`”

3.8 Phone Configuration as Remote user

The following configuration is used for all versions of OpenStage phones.

The screenshot shows the 'SIP interface' configuration page. The left sidebar contains a menu with 'Administrator Pages' selected. The main content area has a yellow callout box with the text: 'Check and fill in if phone is behind OSB. If for remote subscriber do not check this box'. An arrow points from this box to the 'Outbound proxy' checkbox, which is checked. The configuration fields are as follows:

SIP interface	
Outbound proxy	<input checked="" type="checkbox"/>
Default OBP domain	10.191.0.20
SIP transport	TCP
Response timer (ms)	32000
NonCall trans. (ms)	32000
Reg. backoff (seconds)	60
Connectivity check timer (seconds)	0
Keep alive format	Sequence
Media Negotiation	Single IP
Media IP Mode	IPv4
<input type="button" value="Submit"/> <input type="button" value="Reset"/>	

The screenshot shows the 'Registration' configuration page. The left sidebar contains a menu with 'Administrator Pages' selected. The main content area has two yellow callout boxes. The first box, with the text: 'If phone is behind branch in "proxy" or "branch-SBC" mode, fill in the branch LAN address. If for remote subscriber this field should be left blank.', has an arrow pointing to the 'SIP gateway address' field. The second box, with the text: 'SIP server address = OS-SBC WAN IP. SIP registrar address = OS-SBC WAN IP', has an arrow pointing to the 'SIP server address' and 'SIP registrar address' fields. The configuration fields are as follows:

Registration	
SIP Addresses	
SIP server address	10.191.0.11
SIP registrar address	10.191.0.11
SIP gateway address	10.191.0.20
SIP Session	
Session timer enabled	<input checked="" type="checkbox"/>
Session duration (seconds)	0
Registration timer (seconds)	300
Server type	OS Voice
Realm	realm
User ID	15615597202
Password	*****
MLPP base	Local
MLPP Domain	dsn+uc
Other Domain	
SIP Survivability	
Backup registration allowed	<input type="checkbox"/>
Backup proxy address	
Backup registration timer (seconds)	3600
Backup transport	UDP
Backup OBP flag	<input type="checkbox"/>
<input type="button" value="Submit"/> <input type="button" value="Reset"/>	

Administrator Pages
User Pages
Logout

Admin Login
Applications
Bluetooth
Network
General IP configuration
IPv4 configuration
IPv6 configuration
Update Service (DLS)
QoS
Port configuration
LLDP-MED operation
System
File transfer
Local functions
Date and time
Speech
General information
Security and Policies
Ringer setting
Mobility
Diagnostics
Maintenance

Port configuration

SIP server65060
SIP registrar65060
SIP gateway65060
SIP local65060
Backup proxy5060
RTP base5010
Download server (default)21
LDAP server389
HTTP proxy0
LAN port speedAutomatic
PC port speedAutomatic
PC port modedisabled
PC port autoMDIX
SubmitReset

Administrator Pages
User Pages
Logout

Admin Login
Applications
Bluetooth
Network
System
File transfer
Local functions
Date and time
Speech
General information
Security and Policies
Ringer setting
Mobility
Diagnostics
Maintenance

Date and time

Time source
SNTP IP address10.191.0.101
Timezone offset (hours)0
Daylight saving
Daylight saving
Difference (minutes)60
Auto time change
DST zone
SubmitReset

The phone must have it's time sync'ed with the NTP server if SRTP mikey is to be used.

3.9 OpenScape Mobile Configuration

Please refer to the OpenScape Mobile Android Devices User Guide, available in e-Doku under the following link: http://apps.g-dms.com:8081/techdoc/search_en.htm or the OpenScape Mobile Android Devices User Guide available in E-Doku under the following link: http://apps.g-dms.com:8081/techdoc/search_en.htm

Once there, please select the Product “OpenScape Mobile” and hit *Create List*.

As with other devices the address of the SIP server (either the OSV or OS-SBC should contain the IP address and the port. Refer to [Core realm configuration](#)

3.10 Generating an effective OS-SBC Ticket

3.10.9 *Describe the setup and problem.*

What version of OSS is being used?
Physical or virtual machine?
What type of Hardware platform?
What device originates the call? (IP address and phone number)?
What digits are dialed? Is call forwarding, serial ringing or some other feature involved?
What device is terminated to? (IP address and phonenumber)
Is the problem reproducible?
What device is not accessible?
Is redundancy involved? If so what type of redundancy? If a network diagram is available, please provide it.

3.10.10 *Gather information (some information may not apply)*

IP addresses of devices involved (OSV, OS-SBC-LAN, OS-SBC-WAN, OSB, Gateway, phones)
Versions of devices (OSV, OS-SBC-LAN, OS-SBC-WAN, OSB, Gateway, phones)
Protocols involved (TCP, TLS, SRTP)

3.10.11 *Gather traces, logfiles and Configuration files*

Wireshark traces refer to [Debugging](#)
Associated log files of the problem refer to [Settings](#)
Rapidstat refer to [Debugging](#)
Configuration file refer to [Import/Export](#)

4 Trouble shooting hints---what if?

4.4 The OS-SBC is in survivable mode.

Verify the server IP address, Transport and port match what is created in the OSV. Local GUI → VOIP → SIP Server Settings → Node 1/2 information.

Verify the “Alias” information for this OS-SBC in the OSV.

4.5 A node server is “in penalty box” state

Verify the server IP address, Transport and port match what is created in the OSV. Local GUI → VOIP → SIP Server Settings

Verify the “Alias” information for this OS-SBC in the OSV.

4.6 A redundant node is in “FAULT” state

Verify the “redundancy” configuration in BOTH OS-SBCs Local GUI → Network Net Services → Settings → Redundancy

4.7 Call processing is “slow” even for single calls

Verify that the log level for some function has not been left at “Info” or “Debug”. Local GUI → Diagnostics & Logs → Log Levels

4.8 Remote subscribers can not register

Verify Remote Subscribers are enabled in the OS-SBC
Local GUI → Features → enable Remote Subscribers → Remote Subscribers configuration

4.9 Remote endpoints are in survivable mode

Verify the server IP address, transport and port match what is created in the OSV. Local GUI → Features → Remote Endpoints configuration <check the following>

Remote IP address
Remote Port
Remote transport
Core TCP or TLS port

On the Remote device check the following:

Server IP address
Server transport
Server port

4.10 Calls of some protocols do not pass through the OS-SBC

Verify the firewall settings allow the protocol desired.

Local GUI → Features → Remote Subscribers → <select the remote configuration> edit → Firewall Settings → check the protocols allowed.

Local GUI → Features → Remote Endpoints → <select the remote endpoint configuration> edit → Firewall Settings → check the protocols allowed.

Local GUI → Security → Firewall

4.11 Lines receive a code 606 when attempting a call

Verify the OpenScape SBC Licenses are loaded and not expired. Local GUI → System → Licenses

4.12 Line receives code 401 Unauthorized when attempting to register

Verify the realm and password created in the OSV and the phone.

4.13 Line receives code 403 Forbidden when attempting to register

Verify the transport type used by the phone matches the transport created in the OSV

4.14 Line receives code 404 Not Found when attempting to register

Verify the subscriber is created in the OSV with the same phone number

4.15 Lines receive a code 406 when attempting a call

Using Wireshark verify the codecs offered by the A party. Verify the B party can support that codec.

4.16 Line receives code 503 service unavailable when attempting to register

This is normal the first time a line attempts to register via the OS-SBC. The first time the OS-SBC will return code 503 with a field "Retry-After: <seconds>", but as the phone attempts to re-register, after the Retry period, the OS-SBC will pass the register on to the OSV to allow the registration attempt.

4.17 Errors report Not possible to get authentication statement during simplified installation

CMP → configuration → OpenScape SBC → OpenScape SBC list → <select the OS-SBC → <click edit> → <uncheck the box "Communicating over Secured channel"> → OK Attempt the installation again

4.18 Devices can not communicate with the OS-SBC

Verify the listening ports on the OS-SBC. Refer to [General steps to add a OS-SBC](#) step 4.

Verify the ports other devices are sending to, for communications with the OS-SBC.

4.19 Trouble doing an "Import" of a XML configuration file

Open the "Web Server" log file to see the reported error.

4.20 You see the alarm "License using temporary grace period" on SBC, when centralized licensing is in use

This means the SBC is not able to communicate with the CMP, to refresh its license data. Every 24 hours, the SBC syncs up its license information with the CMP. If it fails to successfully communicate with the CMP, then this alarm is generated. If it is not corrected within 30 days, then calls may be blocked on the SBC. One possible solution could be to access the SBC Assistant and edit the SBC entry in the Branch Office list to uncheck the "Communicating over Secured channel" flag and save the entry, then "Manage" that SBC from the CMP and select the "device license update" to allow the CMP and SBC to exchange new authentication statements and re-establish secure communication.

4.21 Can not upload a local file for upgrade

Verify the sending device is in the "white list" for Message Rate control.

4.22 Calls which did work, are blocked at times.

If the user finds that calls are still being blocked by Message Rate control (check the firewall & Msg rate control log – Diagnostics & Logs -> Debugging -> select the firewall & Msg rate control log -> show), the user will need to either increase the limit for blocking or add the IP address which is being blocked to the white list.

4.23 Receive a message indicating invalid HW type during XML validation

In the XML file, verify both the "hwType" field and the "product" field.

In the "product" field the value of 1 equates to IBM x3250 and a value of 2 equates to IBMx3550.

4.24 Receive a message indicating a file problem when booting a VM

The message may indicate a file corruption or a problem with the checksum of a file. In this case first verify the VM was created with the correct resource values.

See [Configuration of Virtual OS-SBC \(VM-OS-SBC\)](#) for the suggested values.

4.25 Branch behind a “dynamic IP address NAT stays in penalty box.

Verify OS-SBC remote endpoint “Logical-Endpoint-ID” is equal to the “Logical Branch office ID” of the branch.

On branch GUI→system→Licenses

On OS-SBC GUI→.Features→Remote Endpoints configuration

Verify the “Branch behind NAT” flag is set on the OSB GUI →VOIP -. Sip Server Settings →check the box

4.26 A redundant system must have redundancy disabled

A redundant system may need to be “split” at times. One example may be to replace a defective node.

To disable **Redundancy** it is required to configure Node 1 and Node 2 separately as follows: First configure a temporary IP in the Master node and uncheck the **Redundancy Enable** checkbox, so that the system will restart with Redundancy disabled and the other system will be unable to take the control (unable to reach the system as the IP address has been changed). The other node will remain in Backup state for about 9 minutes and then will become the master node. Now it is possible to change the configuration on this node, so configure a temporary IP and uncheck the Redundancy Enable checkbox (system will restart). Now both systems are operating with Redundancy disabled and it is possible to restore the IP configuration.

4.27 Can not login to OS-SBC

This can happen if the default gateway is set to the WAN interface but there is no routing to allow communications with the LAN.

To resolve this the user must add a route on LAN manually from CLI of the OS-SBC.

1 - route add 192.168.59.1/32 dev eth0

2 - route add -net 192.168.59.0 gw 192.168.59.1 netmask 255.255.255.0 Here we are adding

192.168.59.0/24 network to the LAN interface

4.28 Cannot upgrade due to old license version

The V10R2 software will start to block an upgrade if the installed license version is not V9 or later. Clients upgrading to V10R2 need to request a new license file. The old license files will not be accepted after a full installation.

NOTE: If the license file version is V8 but the license file contains the component id "EMSS_Check" (Extended Manufacturer Software Support) which is still valid, the upgrade procedure will be executed, and the license file will be accepted.

5 Table A: Fixed/Configurable Port Information:

This table shows specific ports used by OpenScapeSBC

Mode / Application	Port information
static	DNS server
	53
	SNMP Set/Get
	161
	NTP/SNTP
	123
	SSH/SFTP
	22
	HTTPS over TLS/SSL
	443
	B2BUA (for integrated gateways)
Configurable / dynamic Default values shown	5096
	ISAKMP (Key management)
	500
	Syslog Server (used for system logging)
	514
	Ipssec Nat-Transversal (RFC3947)
	4500
	Secure HTTPS (used by Fusion)
	8443
	Proxy SIP TCP/UDP
	5060 *
	Proxy SIP TLS
	5061 *
	SBC RTP
	55000-65000 **
	Subscriber Dynamic SIP ports
	10000-49999 **
	Remote endpoints Static SIP ports
	50000-54999



* It is highly recommended that the default values be changed for security reasons. Refer to section [SIP listening ports for LAN and WAN Main IP Addresses](#).



** If there is an external firewall on either the WAN or LAN interface or both, the number of ports required to be open can be calculated as follows: $\text{number of sessions} \times 5$ gives the number of required ports to be opened. $100 \times 5 = 500$, Min Port ==55000 Max Port==55499

6 OS-SBC Performance Configuration Limits:

For performance information related to this version of OS-SBC, please refer to the "OpenScape SBC V9, Data Sheet, Issue 2" in E-Doku.

6.4 SIP Requests Limits

SBC has mechanisms that limits the SIP request messages based on rate and resources to avoid potential issues. They are based on sipserver and control the message rate limit, CPU load limit, and network limit. All these limits are dependent on the HW model and can be affected by configuration (number of remote subscribers, log level, etc).

These limits do not have any relation with the message rate control and gateway message rate limit

(DOS Mitigation), both from security configuration. These configurations act in firewall and the SIP request limits are handled by sipserver. Thus, the message rate control and gateway message rate limit can block message at the network level and override the SIP request limit.

6.4.9 Message rate limit

The message rate limit controls different message methods: REGISTER, NOTIFY, SUBSCRIBE, and INVITE. And, each method has a different limit which is dependent on HW type. The algorithm uses an internal counter which is checked and restarted every 10s and incremented for each received message by the sipserver (including internal messages). Once the counter hits the stated limit, SBC will reject a SIP request from access side with 503 “Server Unavailable” and add a warning header indicating “Overload Rate Limiting”. In addition, a random value between 10s and 30s is included in the header Retry-after.

6.4.10 CPU load limit

This mechanism uses the PID Controller model, the drop rate is adjusted dynamically based on the load factor so that the load factor always drifts towards the specified limit (or setpoint, in PID terms). As reading the CPU load average is relatively expensive, this only happens once every 10 seconds and consequently the value is only at these intervals recomputed. Once the load factor reaches the stated limit, SBC will reject a SIP request from access side with 503 “Server Unavailable” and add a warning header indicating “Overload System Limiting”. In addition, a random value between 10s and 30s is included in the header Retry-after.

6.4.11 Network limit

This algorithm relies on information provided by network interfaces. The total amount of bytes waiting to be consumed on all the network interfaces is retrieved once every 10 seconds. If the returned amount exceeds the limit specified SBC will reject a SIP request from access side with 503 “Server Unavailable” and add a warning header indicating “Overload Network Limiting”. In addition, a random value between 10s and 30s is included in the header Retry-after.

6.4.12 Limits per HW type

The following table presents the limits for each HW type.

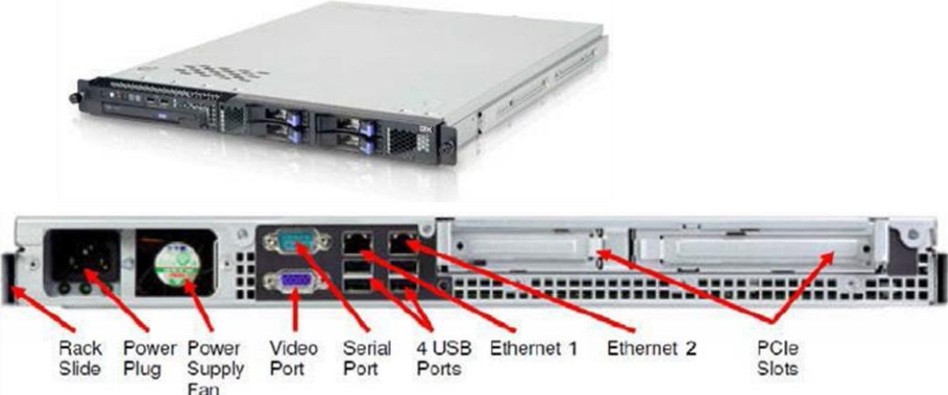
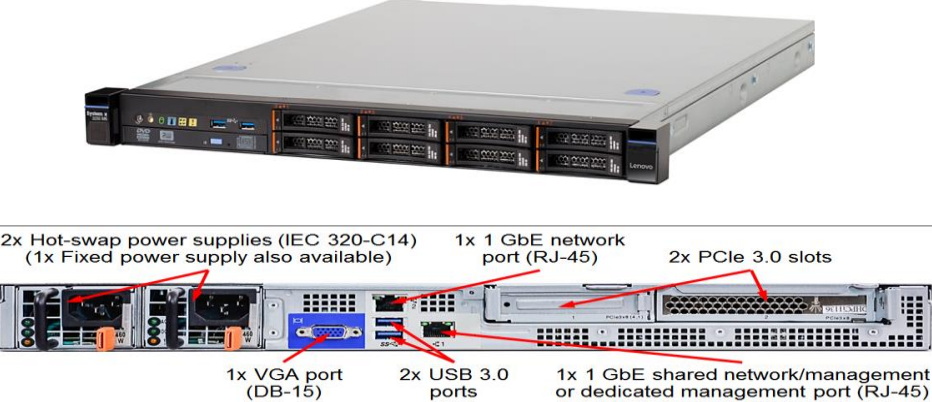
Limit Mechanism\HW type	x3250	sr250	x3550	rx330	rx200	sr530	advantech	advantech250	LXC (does not depend on HW type)
REGISTER message rate	150 msg/s		1000 msg/s			20 msg/s			100 msg/s
INVITE message rate	100 msg/s		200 msg/s			20 msg/s			60 msg/s
SUBSCRIBE message rate	150 msg/s		1000 msg/s			20 msg/s			100 msg/s
NOTIFY message rate	150 msg/s		1000 msg/s			20 msg/s			100 msg/s
CPU Load	80%		80%			80%			80%
Network	50000 bytes		200000 bytes			10000 bytes			30000 bytes

From build 09.04.12.02, new configurable sipserver parameters are available to control message rate. These parameters are maxRegisterRate, maxCallRate, maxNotifyRate, and maxSubscribeRate. And, they are configurable only via XML file. The value "0" indicates that the parameter is disabled, and the default value will be applied. All parameters are dependent on the HW type and will be applied only if they are set with valid values for the respective HW type. These parameters should not be changed except in some specific scenarios, for example, when the server has a limitation of REGISTER message rate, which is lower than the SBC HW limit. The technical support can provide the recommended and valid values if necessary. The new fields will appear in the xml in two situations:

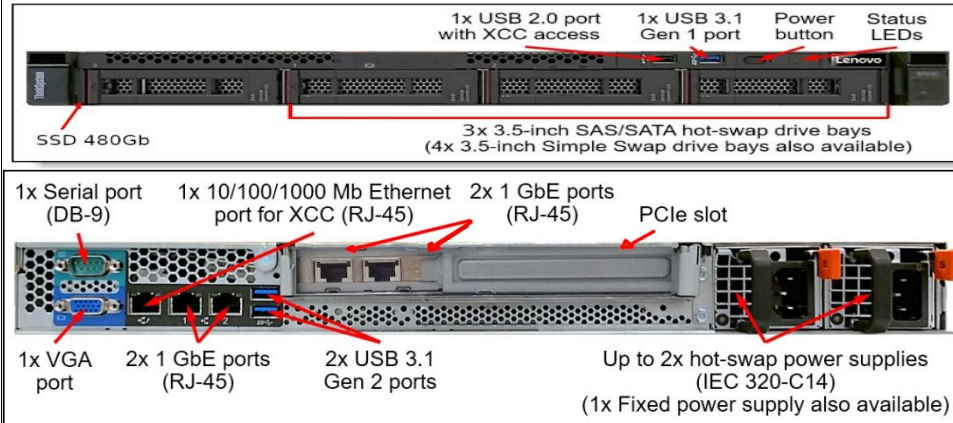
- 1)Update from a different release (for instance V9R3 to V9R4);
- 2)Any change is made to the current database.

Once you have an xml file with the fields available, edit it to modify the parameters as desired and then import it.

7 Table B: Hardware Types Table

OpenScape SBC Model	Details
<p data-bbox="558 386 721 415">3250-M3/M5</p>  <p data-bbox="224 758 964 814"> Rack Slide Power Plug Power Supply Fan Video Port Serial Port 4 USB Ports Ethernet 1 Ethernet 2 PCIe Slots </p>	<p data-bbox="1143 386 1484 415">IBM x3250 M3/M5 server</p> <p data-bbox="1143 449 1523 701"> Physical Dimension (W x H x D): 440 x 44.5 x 559 mm (17.3" x 1.75" x 22.0") Power: 351 W, 100~127/ 200~240 V AC input Part number: ADA41 / L30220- D600-A601 </p> <div data-bbox="1143 709 1479 835" style="background-color: yellow; border: 1px solid black; padding: 5px;"> <p data-bbox="1159 722 1451 827">For x3250 M5, only 2 ethernet interfaces are available.</p> </div>
<p data-bbox="581 911 698 940">3250-M6</p>  <p data-bbox="168 1213 1094 1388"> 2x Hot-swap power supplies (IEC 320-C14) (1x Fixed power supply also available) 1x 1 GbE network port (RJ-45) 2x PCIe 3.0 slots 1x VGA port (DB-15) 2x USB 3.0 ports 1x 1 GbE shared network/management or dedicated management port (RJ-45) (set by a jumper on the system board) </p>	<p data-bbox="1143 911 1435 940">IBM x3250 M6 server</p> <p data-bbox="1143 974 1523 1226"> 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> <div data-bbox="1143 1234 1479 1360" style="background-color: yellow; border: 1px solid black; padding: 5px;"> <p data-bbox="1159 1247 1451 1352">For x3250 M6, only 2 ethernet interfaces are available.</p> </div>

Lenovo-SR250



Lenovo SR250 (Replacement for IBM x3250 M3/M5/M6)

Physical Dimension (W x H x D): 434 x 43 x 498 mm (17.1" x 1.7" x 19.6")

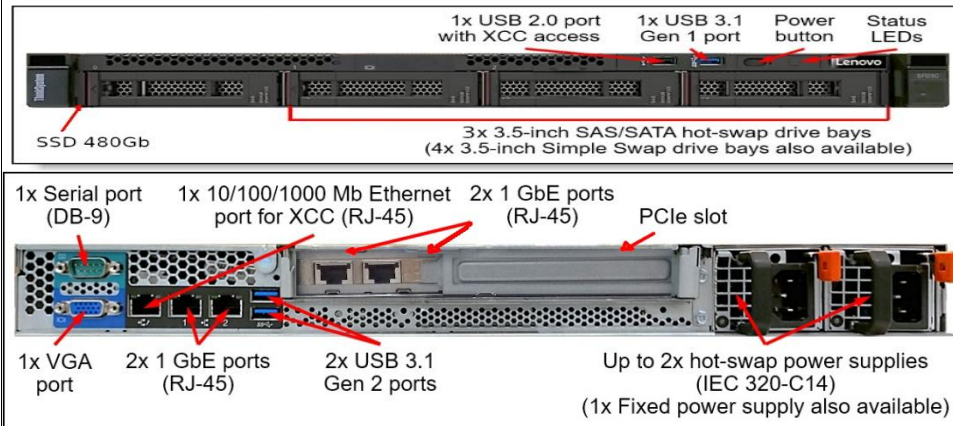
Weight: up to 12.3 kg (27.1 lb)

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

3550-M3



IBM x3550 M3

Physical Dimension (W x H x D): 440 x 44 x 711 mm (17.3" x 1.7" x 28.0")

Weight: up to 15.4 Kg (34.0 lb)

Rated Power: 100~127 / 200~240 V AC, 50-60 Hz, 351W

ADA569 / L30220-D600-A569

BZF101 / L30280-Z600-F101

(Power Cord, USA Variant)

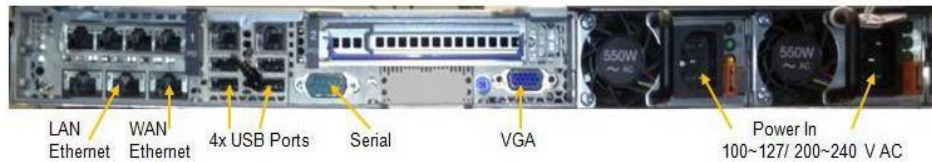
BZF105 / L30280-Z600-F105

(Power Cord with Straight Appliance Connector, EURO Variant)

BZF107 / L30280-Z600-F107

(Power Cord, BRA Variant)

3550-M4



IBM x3550 M4

Physical Dimension (W x H x D): 440 x 43 x 711 mm
(17.32" x 1.69" x 27.99")

Weight: up to 15.4 kg (34.0 lb)
Rated Power: 100-127 / 200-240 V AC , 50-60 Hz, 351 W

Average Power

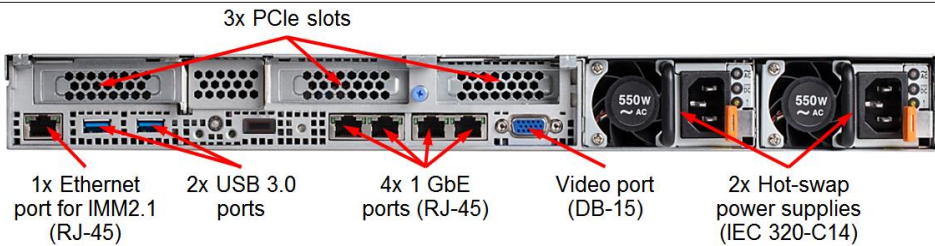
Consumption : 180 W

Rated Heat Emission: 1263.7 kJ/h (1197.7 BTU)

Operating Temperature: 10-35°C (50-95°F)

Part Number : L30220-D600- A604

3550-M5



IBM x3550 M5

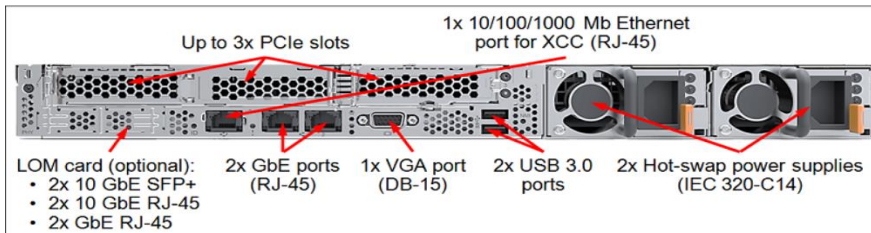
Physical Dimension (W x H x D): 434 x 43 x 734 mm (17.1" x 1.69" x 28.9")

Weight: up to 19.3 kg (42.5 lb)

Rated Power: 100-127 / 200-240 V AC , 50-60 Hz, 351 W

Operating Temperature: 5-40°C (41-104°F)

Part Number :to be supplied



Lenovo SR530 (Replacement for IBM x3550 M5)

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),

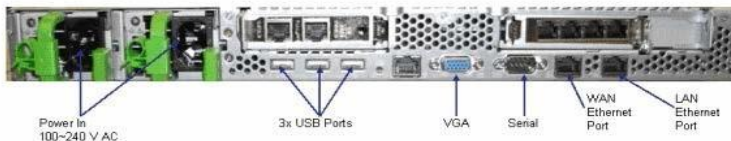
maximum: 16 kg (35.3 lb)

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

Fujitsu – Rx200 S6



Fujitsu Primergy RX200 S6

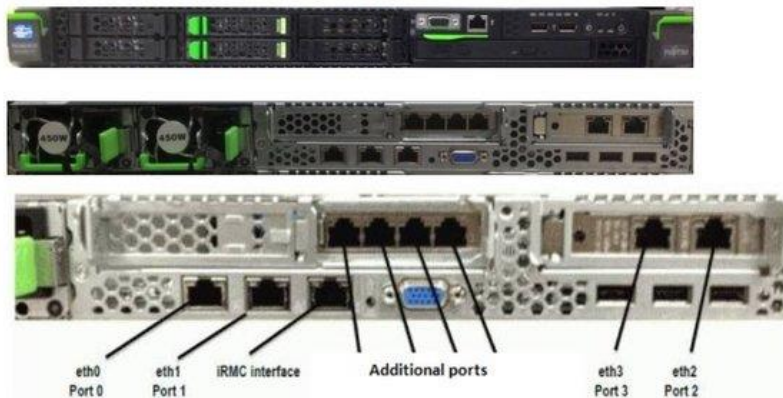
Physical Dimension (W x H x D): 431 x 43 x 762mm (18" x 1.69" x 30.0")

Weight: up to 17 Kg (37.5 lb)
Average Power Consumption: 193W

Unify Part number: ADA603 / L30220-D600-A603

Fujitsu – Rx200 S7

OpenScape Session Border Controller - Fujitsu Primergy RX200 S7



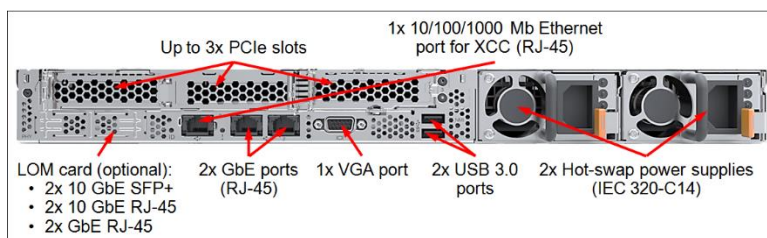
Fujitsu: Rx200 S7

Physical Dimension (W x D x H): 482mm x 431 x 43

Power: 100~240 V AC, 47-63Hz, 549W

Fujitsu RX200 S7 server :
Part Number : to be supplied

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)

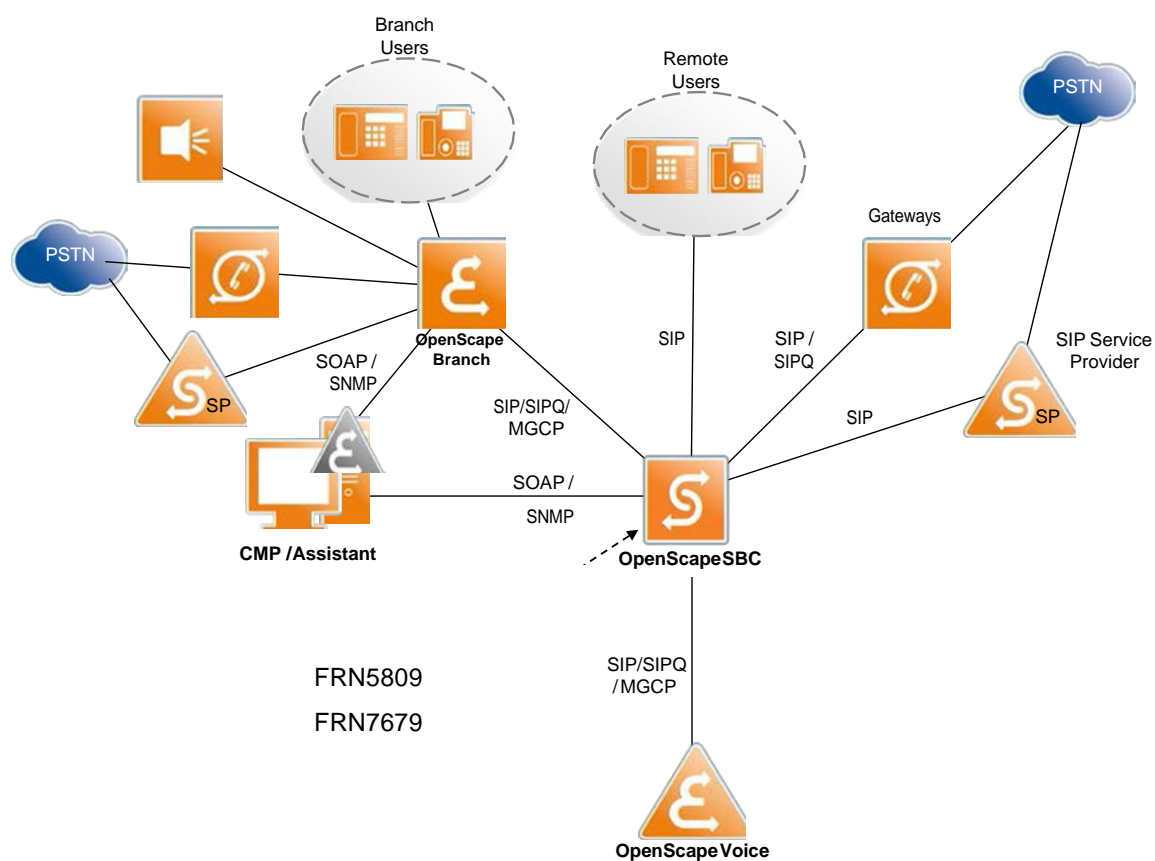
Physical Dimension (W x H x D):
440 x 43 x 773 mm (17.3" x 1.7"
x 30.4")

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

8 Appendix C: OS-SBC External Interfaces



9 Create Certificate

9.4 Create Server Configuration file

CREATE SERVER CONFIGURATION FILE

Generating the private/public key pair and the certificate sign request file is done through the OpenSSL library via the *openssl req* command (Sample configuration template is provided in step 3).

Note: The file name used for server.cnf and certificates can be changed according to your convention.

Specific steps:

- SSH to OpenScape Branch or system which support openssl commands .
- Make the working directory that will hold all the configuration files of certificate sign request files.

```
mkdir /tmp/config cd  
/tmp/config
```

- Create the server configuration file. Copy the contents of the below text into a file named osbserver.cnf.

```
#  
# Server configuration file.  
# If you are creating certificates for more then one Server and  
# are using subAltName then you should create a copy of this file for  
# each server.  
#
```

```
[req]
```

```
default_bits = 2048  
encrypt_key = no  
default_md = sha1  
distinguished_name = req_distinguished_name  
req_extensions = v3_req
```

[req_distinguished_name]

countryName = Country Name (2 letter code)

countryName_default = US

countryName_min = 2

countryName_max = 2

stateOrProvinceName = State or Province Name (fullname)

localityName = Locality Name (eg, city) organizationName =

Organization Name (eg, company) organizationalUnitName =

Organizational Unit Name (eg, section) commonName = Common

Name (eg, FQDN) commonName_max = 64

[v3_req]

keyUsage = keyEncipherment, dataEncipherment

subjectKeyIdentifier = hash

basicConstraints = CA:false

nsCertType= client,server

README: If you decide to use subjectAltName you must uncomment
the following line and AT LEAST one of the lines under [alt_names].

#subjectAltName = @alt_names

[alt_names]

#You can define more IP and DNS names. Just follow the order.

#DNS.1 = www.foo.com

#DNS.2 = www.bar.org

#IP.1 = 192.168.1.1

#IP.2 = 192.168.69.144

#EOF

- Copy the server.cnf template file to the config directory while renaming it to the specific purpose for which the certificate will be used.

E.g. if a certificate is created for SIP Endpoint Server Authentication, use the name `osbserver.cnf`. If a certificate is created for the client side of SIP Mutual Authentication, use the name `osbclient.cnf`, etc. Let's assume the first case:

`osbserver.cnf`

- There are 2 options to modify the `osbserver.cnf` file:
 - If using a local editor, simply open the template file using e.g. the vi editor:

`vi osbserver.cnf`

- If using an off-line editor to modify the template file, transfer `osbserver.cnf` to the PC, running the editor and open the file there.
- Modify the `osbserver.cnf` file by following the instructions in the file. Typically, most of the defaults in this file should be left untouched. There is however a variable portion to this file that needs to be changed to suit the needs of the deployment. The following is a list of the more common changes that need to be made to the file:
 - `[req]` section: is used to generate the certificate sign request:
 - `default_bits`: per default OSV generates a 2048 bit key. This is sufficiently secure for most deployments.
 - `encrypt_key`: leave this option set to no. OpenScape Branch does not support loading keys that are pass-phrase protected. Only the root user can access the private key, so the key itself is actually sufficiently protected via Linux access rights.
 - `[req_distinguished_name]` sub-section: is used to generate an X509 Distinguished Name for the certificate. All elements are optional except the common name. Usually though, most elements receive a value. Set the Common Name to something meaningful. For web servers this would usually be set to the www URI. For SIP this is usually set to the FQDN or IP address of the device (note that this will be overwritten anyway through the use of the Subject Alternate Name extension).
 - `[v3_req]` sub-section: contains the extension fields that will be populated in the certificate sign request.

The nsCertType (netscapeCertificateType) is used if users who distinguish the usage of their certificates between server and client only connections. This requires the serverCert.pem certificate contain an extension nsCertType =server and for clientCert.pem to contain an extension nsCertType =client.

The current template includes the Subject Key Identifier extension and the Subject Alternate Names extension. For the Subject Alternate Names extension a new sub-section is created where the IP addresses and FQDNs of the server can be entered:

- [alt_names] sub-section contains 0 or more IP addresses and FQDNs. These are the FQDNs and IP (IPv4 and IPv6) addresses by which the server can be reached. For example, this would be the IP address/FQDN of the OpenScape Branch)
- o Save the osbserver.cnf file after the modifications. If an off-line editor was used, copy the modified osbserver.cnf file to the config directory (/tmp/config). If the editor was running on a windows PC, the dos2unix command needs to be run on the osbserver.cnf file in the private directory as follows:

```
dos2unix osbserver.cnf
```

VALIDATE THE CERTIFICATE

The certificate received from the CA should contain the entire certificate chain or CA certificate (ServerCA.pem) and Certificate (osbservercert.pem) signed by CA from CSR. Use the 'openssl x509' command of Viewing a Certificate or Certificate Sign Request to view the received certificate. Unfortunately that just shows the first certificate in the chain (assuming a certificate together with its CA certificates up to the Root CA was delivered).

Always, make sure that the current directory is the config directory:

```
cd /tmp/config
```

To verify whether the received certificate also contains other certificates, run:

```
more osbservercert.pem
```

One should observe the PEM formatted certificate received as follows:

```
-----BEGIN CERTIFICATE-----  
MIIDejCCAuOgAwIBAgIJANRO4Lwz1cO6MA0GCSqGSIb3DQEBBQUAMIHMMQswC  
QYD
```

```
VQQGEwJVUzEQMA4GA1UECBMHRmxvcmlkYTETMBEGA1UEBxMKQm9jYSBSYXRvbjEq
MCgGA1UEChMhU2lbWVucy1FbnRlcnByaXNlIENvbW11bmljYXRpb25zMRgwFgYD
-----END CERTIFICATE-----
```

Or, it could be a concatenation of the certificate together with the signing
CAs certificate:

```
-----BEGIN CERTIFICATE-----
MIIESzCCA7SgAwIBAgIJAIXewvQNWUL/MA0GCSqGSIb3DQEBBQUAMIHKMqswC
QYD
VQQGEwJVUzEQMA4GA1UECBMHRmxvcmlkYTETMBEGA1UEBxMKQm9jYSBSY
XRvbjEq
MCgGA1UEChMhU2lbWVucy1FbnRlcnByaXNlIENvbW11bmljYXRpb25zMRgwFgYD
...
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
MIESTCCA7KgAwIBAgIJAOPiOzYWpgITMA0GCSqGSIb3DQEBBQUAMIHKMqswC
QYD
VQQGEwJVUzEQMA4GA1UECBMHRmxvcmlkYTETMBEGA1UEBxMKQm9jYSBSYXRvbjEq
MCgGA1UEChMhU2lbWVucy1FbnRlcnByaXNlIENvbW11bmljYXRpb25zMRgwFgYD
...
-----END CERTIFICATE-----
```

For OpenScape Branch it is necessary to have separate CA and
server certificate. For example as below

```
CA.pem
osbservcert.pe
m
osbservkey.pe
m
```

If it is concatenated, make sure to separate CA and server certificate from the CA
supplied file. You can copy the content between --BEGIN CERTIFICATE-- and ---
END CERTIFICATE--- to file and validate the certificate for the supplied CSR and key to
determine the observer certificate.

The following commands will check whether a private key matches a certificate
or whether a certificate matches a certificate signing request. It generates the
md5 hash of Modulus from the certificate, private key and CSR.

```
openssl x509 -noout -modulus -in osbservcert.pem |
openssl md5 openssl rsa -noout -modulus -in
osbservkey.pem | openssl md5 openssl req -noout -
modulus -in osbserv.csr | openssl md5
```

SERVER CONFIGURATION FILE TEMPLATE

The following is an OpenSSL server configuration file template that can be used to create CSR. It is available in the OpenScape Voice server as /usr/local/ssl/server.cnf.

```
# server certificate example configuration file.
# This file is based on the OpenSSL example configuration file
#

# This definition stops the following lines choking if HOME isn't
# defined.
HOME                = .

[ req ]
distinguished_name  = req_distinguished_name
attributes          = req_attributes
x509_extensions     = v3_req # The extensions to add to the self signed cert

[ req_distinguished_name ]

# If prompting has been switched off, remove _min, _max and _default lines
# in this section and set values to those that are required.
countryName         = Country Name (2 letter code)
countryName_default = AU
countryName_min      = 2
countryName_max      = 2

stateOrProvinceName = State or Province Name (full name)
stateOrProvinceName_default = Some-State

localityName         = Locality Name (eg, city)

0.organizationName   = Organization Name (eg, company)
0.organizationName_default = Internet Widgits Pty Ltd

# we can do this but it is not needed normally :-)
#1.organizationName   = Second Organization Name (eg, company)
#1.organizationName_default = World Wide Web Pty Ltd

organizationalUnitName = Organizational Unit Name (eg, section)

commonName           = Common Name (eg, YOUR name)
commonName_max        = 64

[ req_attributes ]

challengePassword     = A challenge password
challengePassword_min = 4 challengePassword_max
                     = 20

unstructuredName       = An optional company name

[ v3_req ]

# Extensions to add to certificate

basicConstraints = CA:FALSE
keyUsage = nonRepudiation, digitalSignature, keyEncipherment
# example of FQDN is sever.myco.com
# subjectAltName=DNS:<insert FQDN here>
#
```

9.5 Create Certificate Sign Request (CSR) and Install Certificates

9.5.9 Generate a Certificate Sign Request file (CSR)

9.5.9.1 Create the server configuration file, Refer to the section above.

- Create the Certificate Sign Request using the ossserver.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 ossserver and store the private key in ossserverkey.pem and enter the public key in a file called ossserver.csr.

```
openssl req -new -config ossserver.cnf -keyout  
osserverkey.pem -out ossserver.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
SBC'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 ossserver.cnf -keyout ossserverkey.pem -out ossserver.csr
```

Note: Keep the private key (eg: ossserverkey.pem) in secure place as it will be required to install the certificates for OpenScape SBC.

9.5.10 *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.

The same happens when the CA is on a OpenScape Voice than where the Certificate Sign Request was created.

Note: User must not send the private key (ossserverkey.pem) to CA or anyone else that matter.

9.5.11 *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 asosssservercert.pem

The same happens when the CA is on a OpenScape Voice than where the Certificate Sign Request was created.

9.5.12 *Validate the Certificate*

The certificate received from the CA should contain the entire certificate chain or CA certificate (ServerCA.pem) and Certificate (osbservercert.pem) signed by CA from CSR. Use the 'openssl x509' command of Viewing a Certificate or Certificate Sign Request to view the received certificate. Unfortunately that just shows the first certificate in the chain (assuming a certificate together with its CA certificates up to the Root CA was delivered).

Always, make sure that the current directory is the config directory:

```
cd /tmp/config
```

To verify whether the received certificate also contains other certificates, run:

```
more osbsservercert.pem
```

One should observe the PEM formatted certificate received as follows:

```
-----BEGIN CERTIFICATE-----
```

```
MIIDejCCAuoGAWIBAgIJANRO4Lwz1cO6MA0GCSqGSIb3DQEBBQUAMIHMMQswC  
QYD
```

```
VQQGEwJVUzEQMA4GA1UECBMHRmxvcmlkYTETMBEGA1UEBxMKQm9jYSBSYXRvbjEq
MCgGA1UEChMhU2lbWVucy1FbnRlcnByaXNlIENvbW11bmljYXRpb25zMRgwFgYD
-----END CERTIFICATE-----
```

Or, it could be a concatenation of the certificate together with the signing
CAs certificate:

```
-----BEGIN CERTIFICATE-----
MIIESzCCA7SgAwIBAgIJAIXewvQNWUL/MA0GCSqGSIb3DQEBBQUAMIHKMqswC
QYD
VQQGEwJVUzEQMA4GA1UECBMHRmxvcmlkYTETMBEGA1UEBxMKQm9jYSBSY
XRvbjEq
MCgGA1UEChMhU2lbWVucy1FbnRlcnByaXNlIENvbW11bmljYXRpb25zMRgwFgYD
...
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
MIESTCCA7KgAwIBAgIJAOPiOzYWpgITMA0GCSqGSIb3DQEBBQUAMIHKMqswC
QYD
VQQGEwJVUzEQMA4GA1UECBMHRmxvcmlkYTETMBEGA1UEBxMKQm9jYSBSYXRvbjEq
MCgGA1UEChMhU2lbWVucy1FbnRlcnByaXNlIENvbW11bmljYXRpb25zMRgwFgYD
...
-----END CERTIFICATE-----
```

For OpenScape Branch it is necessary to have separate CA and
server certificate. For example as below

```
CA.pem
osbservcert.pe
m
osbservkey.pe
m
```

If it is concatenated, make sure to separate CA and server certificate from the CA
supplied file. You can copy the content between --BEGIN CERTIFICATE-- and ---
END CERTIFICATE— to file and validate the certificate for the supplied CSR and key to
determine the observer certificate.

The following commands will check whether a private key matches a certificate or
whether a certificate matches a certificate signing request. It generates the md5 hash
of Modulus from the certificate, private key and CSR.

```
openssl x509 -noout -modulus -in osbservcert.pem | openssl
```

```
md5 openssl rsa -noout -modulus -in osbservkey.pem | openssl
```

```
md5 openssl req -noout -modulus -in osbserv.csr | openssl md5
```

9.6 Change Certificate Parameters for OSS default certificate.

Note: SSH to OSV, Create temp directory and run the commands below from the tempdirectory.

1. Get the root certificate from OSV (/usr/local/ssl/certs/root.pem) and copy it in the temp directory. Make sure the root.pem contains certificate and private key.
2. Create the server configuration file and add the required parameters, Refer [section 1](#)
3. *Generate a Certificate Sign Request file, Refer [section 2.1](#)*
4. *The step 3 generate key ossserverkey.pem and certificate signing request ossserver.csr*
5. *Sign certificate using root.pem of OSV*

```
openssl x509 -req -in ossserver.csr -sha1 -CA root.pem -CAkey root.pem -CAcreateserial-out servercert.pem -days 3650
```

6. Copy root.pem to serverCA.pem within temp directory. (ossserverkey.pem, ossservercert.pem and ossserverCA.pem needed for step 7)
7. Upload the TLS Certificates to the OpenScape SBC.
OpenScape SBC → Security → Certificate Management → Certificates Upload

9.7 Formatting Certificates

9.7.9 Viewing a Certificate or Certificate Sign Request

Certificates and Certificate Sign requests can always be viewed using the openssl library by using the following commands:

- Certificate Sign Request (PEM format):

```
openssl req -in  
osserver.csr -noout -
```

- text ○ Certificate Sign

Request (DER format):

```
openssl req -inform DER -in oserver.csr -noout
```

- text ○ Certificate (PEM format):

```
openssl x509 -in  
certificate.pem -noout -text
```

- Certificate (DER format):

```
openssl x509 -inform DER -in certificate.der -noout -text
```

9.7.10 Converting certificate format

Convert DER to PEM

```
openssl x509 -inform der -in  
certificate.cer -out certificate.pem ○
```

Convert P7B to PEM

```
openssl pkcs7 -print_certs -in certificate.p7b -out  
certificate.pem
```

Convert PFX to PEM

```
openssl pkcs12 -in certificate.pfx -nokeys -  
clcerts -out certificate.pem
```

9.7.11 *Validate Certificates*

This will check whether a private key matches a certificate or whether a certificate matches a certificate signing request. It generates the md5 hash of Modulus from the certificate, private key and CSR.

```
openssl x509 -noout -modulus -in ossservercert.pem |  
openssl md5 openssl rsa -noout -modulus -in  
ossserverkey.pem | openssl md5 openssl req -noout -  
modulus -in ossserver.csr | openssl md5
```

9.8 Terminology

CA - Certificate Authority. CA is an entity that issues digital certificates for use by other parties. It is an example of a trusted third party. CAs are characteristic of many public key infrastructure (PKI) schemes.

CSR - Certificate Signing Request. CSR is a message sent from an applicant to a certificate authority in order to apply for a digital identity certificate.

PEM - Privacy-enhanced Electronic Mail. The .pem file name extension is used for a Base64- encoded X.509 certificate.

9.9 Server Configuration File Template

The following is an OpenSSL server configuration file template that can be used to create CSR. It is available in the OpenScape Voice server as /usr/local/ssl/server.cnf.

```
# server certificate example configuration file.  
# This file is based on the OpenSSL example configuration file  
#  
# This definition stops the following lines choking if HOME isn't  
# defined.  
HOME = .  
  
[ req ]  
distinguished_name = req_distinguished_name  
attributes = req_attributes  
x509_extensions = v3_req # The extensions to add to the self  
signed cert  
  
[ req_distinguished_name ]  
# If prompting has been switched off, remove _min, _max and  
# default lines  
# in this section and set values to those that are required.  
countryName = Country Name (2 letter code)  
countryName_default = AU  
countryName_min = 2  
countryName_max = 2  
  
stateOrProvinceName = State or Province Name (full name)  
stateOrProvinceName_default = Some-State
```

```

localityName          = Locality Name (eg, city)
0.organizationName    = Organization Name (eg, company)
0.organizationName_default=Internet Widgits Pty Ltd
# we can do this but it is not needed normally :-
#1.organizationName    = Second Organization Name (eg, company)
#1.organizationName_default    = World Wide Web Pty Ltd

organizationalUnitName = Organizational Unit Name (eg, section)

commonName            = Common Name (eg, YOUR name)
commonName_max        = 64

[ req_attributes ]

challengePassword= A
challenge password
challengePassword_min    = 4
challengePassword_max    =
20

unstructuredName = An optional company name

[ v3_req ]

# Extensions to add to

certificate basicConstraints

= CA:FALSE
keyUsage = nonRepudiation, digitalSignature, keyEncipherment
# example of FQDN is sever.myco.com
# subjectAltName=DNS:<insert FQDN here>
#

```

10 OS SBC Support of IPV6

Supported configurations information:

OS-SBC Access or Outside Network Interface:

- o Remote Subscribers which support dynamic registration as IPv4-only or IPv6-only:
 - o Remote Subscribers may be in a private or public network without a NAT.
 - o Remote Subscribers in a private network behind a NAT. Only private networks of the same IP version as the public NAT interface are supported.
- o Remote Subscribers which are statically configured as IPv4-only or IPv6-only
- o Remote Gateways (e.g., OpenScape 4000) which are statically configured as IPv4-only or IPv6-only
- o Session establishment between IPv4-only or IPv6-only Remote Subscribers with other SIP interfaces using the same or different IP version.
- o Session establishment between IPv4-only or IPv6-only Remote Gateways with other SIP interfaces using the same or different IP version
- o SRTP/RTP Media bridging between media endpoints using different IP versions

- o SRTP/RTP Media session optimization between media endpoints within the same subnet
- o OS-SBC V1 and V2 network scenarios for the OS-SBC Access network continue to be supported as IPv4-only:
- o OpenScape Branch Proxy / Proxy (SBC) users are supported as IPv4-only or IPv6-only.
 - o OpenScape Branch Proxy / Proxy (SBC) external or integrated Media Gateways
- o Support of OpenScape Branch Proxy / Proxy SBC remote media servers require the OS-SBC Core network be IPv4-only or IPv6-only, because the MGCP IPv4/IPv6 interworking is supported in this feature.
- o SIP Service Providers with IPv6 is supported.

OS-SBC Core or Inside Network Interface

For VoIP communications (SIP, SIP-Q, (s)RTP) the network interface may be configured as IPv4-only or IPv6-only.

If the VoIP communications is configured for IPv6, the network interface will support IPv4 for non-VoIP Applications, e.g., administrative services including CMP, Trace Manager, etc.

INFO:By default, IPv6 will create a link-local IP. To completely disable it, you must use this command line: `sysctl -w net.ipv6.conf.all.disable_ipv6=1`. It will not survive reboots.

To make it permanently, you must edit `/etc/sysctl.conf` and add the following line at the end of the file: `net.ipv6.conf.all.disable_ipv6=1`. It will not survive SBC upgrades, so you must do the same process again after upgrades.

If OS-SBC core side uses 1Pv6 network then in the OSV you create your endpoint using 1Pv6 address. This requires you add management 1Pv4 address in order to manage OS-SBC from CMP.

[SOLT16] - [BG1] - [Main Office] - Edit Endpoint: SBCIPV6 - Mozilla Firefox

10.232.2.136 https://10.232.2.136/management/portal/Applications/Operation/OSV/BusinessGroup/Members/PopUps/m

[SOLT16] - [BG1] - [Main Office] - Edit Endpoint : SBCIPV6

General SIP Attributes Aliases Routes Accounting

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: fd00:10:232:51::51

Port: 5060

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: 10.232.51.51

Security

Save Cancel

OS-SBC IPv6 Support for hosted branch offices configuration

OSV configuration

Create an endpoint for OS SBC as follows:

The following steps are shown in the screenshots:

- General Tab:** The 'Name' field is set to 'acur1h128_IPV6'. The 'Registered' checkbox is checked. The 'Endpoint Type' is set to 'Central SBC'.
- SIP Tab:** The 'SIP Trunking' checkbox is checked. The 'Endpoint Address' is set to 'fd04::128'. The 'Port' is set to '5061'. The 'Transport protocol' is set to 'TLS'. The 'Best Effort SRTP support' is set to 'MDKEY,SDS'. The 'ANAT Support' is set to 'Enabled'.
- Attributes Tab:** The 'SIP Proxy' checkbox is checked. The 'Central SBC' checkbox is checked.
- Aliases Tab:** The 'Name' field is set to 'fd04::128:5060'. The 'port' field is set to '5061'.

Create an endpoint for OSB as follows:

The image displays two screenshots of the OpenScape SBC V10 configuration interface, specifically the 'Edit Endpoint' form for the endpoint named 'acur1h138'.

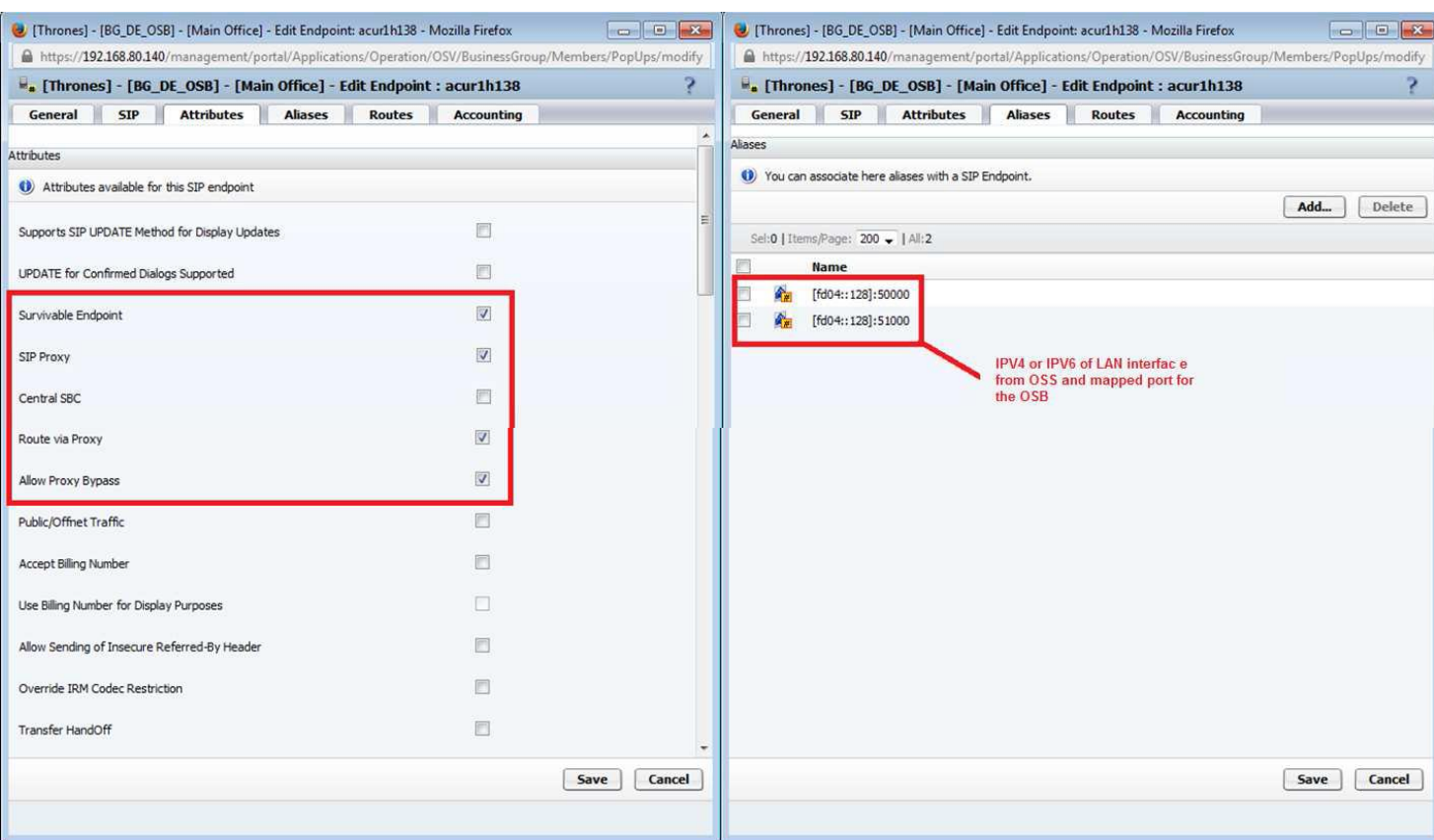
Left Screenshot (General Tab):

- Name:** acur1h138
- Remark:** (empty)
- Registered:** ☒ (highlighted with a red box)
- Profile:** EPP_acur1h138
- Branch Office:** (empty)
- Associated Endpoint:** (empty)
- Default Home DN:** (empty)
- Location Domain:** (empty)
- Endpoint Template:** (empty)
- Endpoint Type:** OpenScape Branch Proxy
- Max number of users:** 50
- Last Update:** 2015-09-02 17:20:01.0
- CSTA Device ID:** (empty)

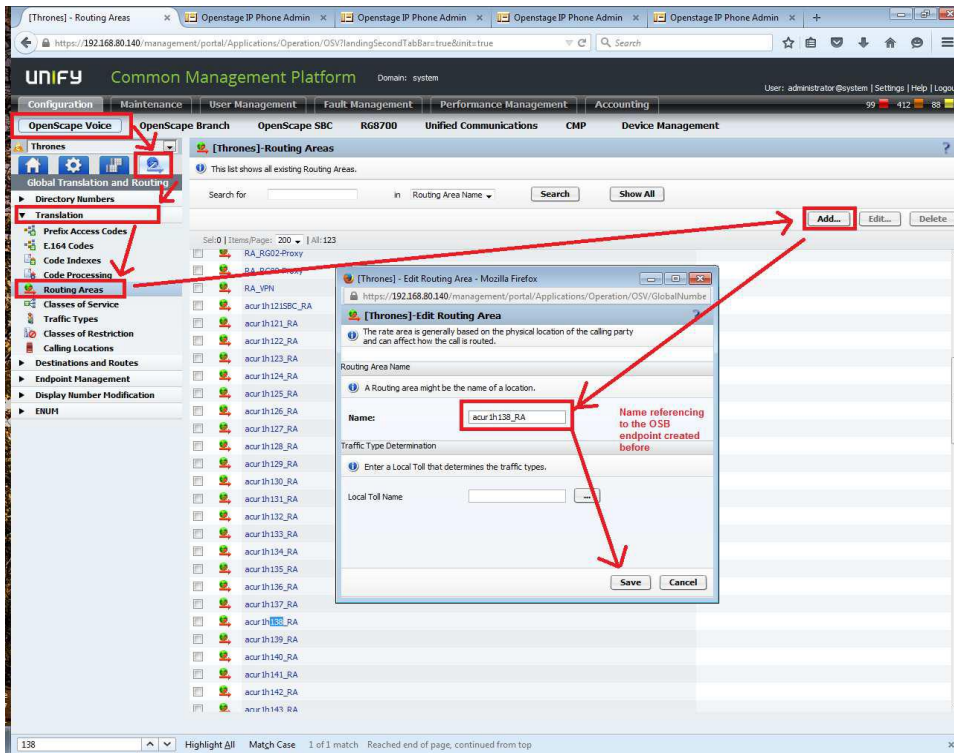
Right Screenshot (SIP Tab):

- Endpoint Type:**
- SIP Private Networking:** ☐
- SIP Trunking:** ☒ (highlighted with a red box)
- SIP-Q Signaling:** ☐
- SIP Signaling:**
- Type:** Static
- Signaling Address Type:** IP Address or FQDN
- Endpoint Address:** fd04::128 (highlighted with a red box)
- Port:** 51000 (highlighted with a red box)
- Transport protocol:** TLS
- Endpoint does not accept incoming TLS connections:** ☐
- Best Effort SRTP support:** MIKEY,SDES
- ANAT Support:** Enabled
- Security:**
- Set the Realm, Username and Password for digest authentication or configure the signaling address as a trusted one.**
- Trusted:** ☒ (highlighted with a red box)

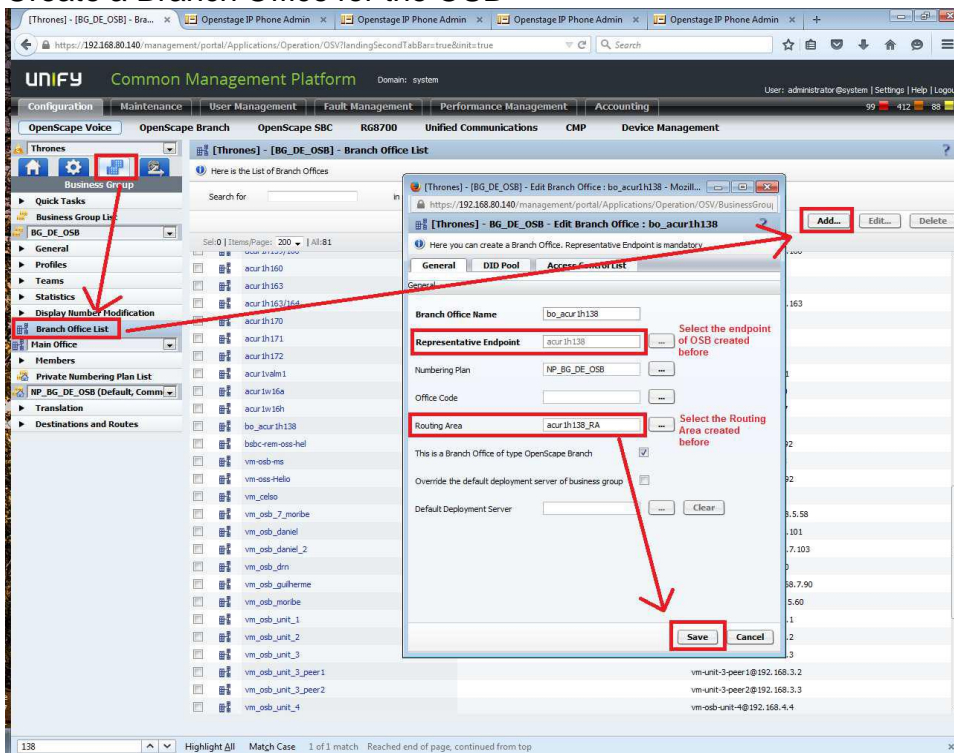
A red arrow points from the text "IPV4 or IPV6 of LAN interface from OSS and mapped port for the OSB" to the 'Endpoint Address' and 'Port' fields.



Create a Routing Area for the OSB endpoint



Create a Branch Office for the OSB



Create the subscribers

Screenshot 1: General Tab

Subscriber Information

Business Group: BG_DE_OSB

Branch Office: **bo_acur1h138** (Select the Branch Office created before)

Directory Number: 55 (42) 3341-3356

Screenshot 2: Routing Tab

Routing Information

Numbering Plan: NP_BG_DE_OSB

Routing Area: **acur1h138_RA** (Select the Routing Area created before)

Class of Service:

Calling Location Code:

Subscriber Attributes

Transfer Hand Off: ☐

Support Media Redirection: ☐

Create the Media Server for the Branch

Screenshot 1: General Tab

(Thrones) Media Server - Media Firefox

Configure Media Gateway Options

General Options

Name: **MS_acur1h138**

Fully Qualified Domain Name: **f004:128**

Assign Method: Node Primary

Protocol Type: **HGCP** (Name referencing the OSB created before and the IP address of OSS LAN interface)

Protocol Version: **HGCP 1.0 HCS 1.0**

MS Signaling IP Address Allocation Method: Static

MS Signaling: **f004:128**

Admin Status: ☐ Sub-usable

Operational Status: ☐ Sub-usable

Location Domain:

Screenshot 2: Circuits Tab

Configure Media Gateway Options

Circuits

In the Circuits Section, you can configure the circuits of the Media Server.

Set 0 | Items/Page: 200 | 1 of 4

Circuit Type

Announcement

Audio

Video

Surveillance

Add all kind of desired announcements for this Media Server

Don't forget to unblock the Media Server

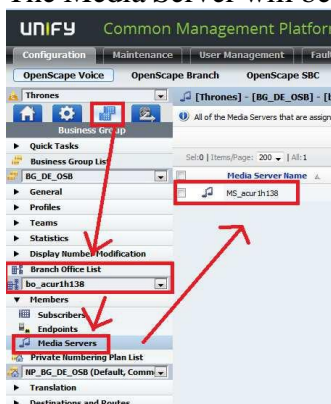
(Thrones) - List Switch Settings for Media Servers

This list shows all Media Servers accessible by the selected switch.

Block Unblock Add... Edit... Delete

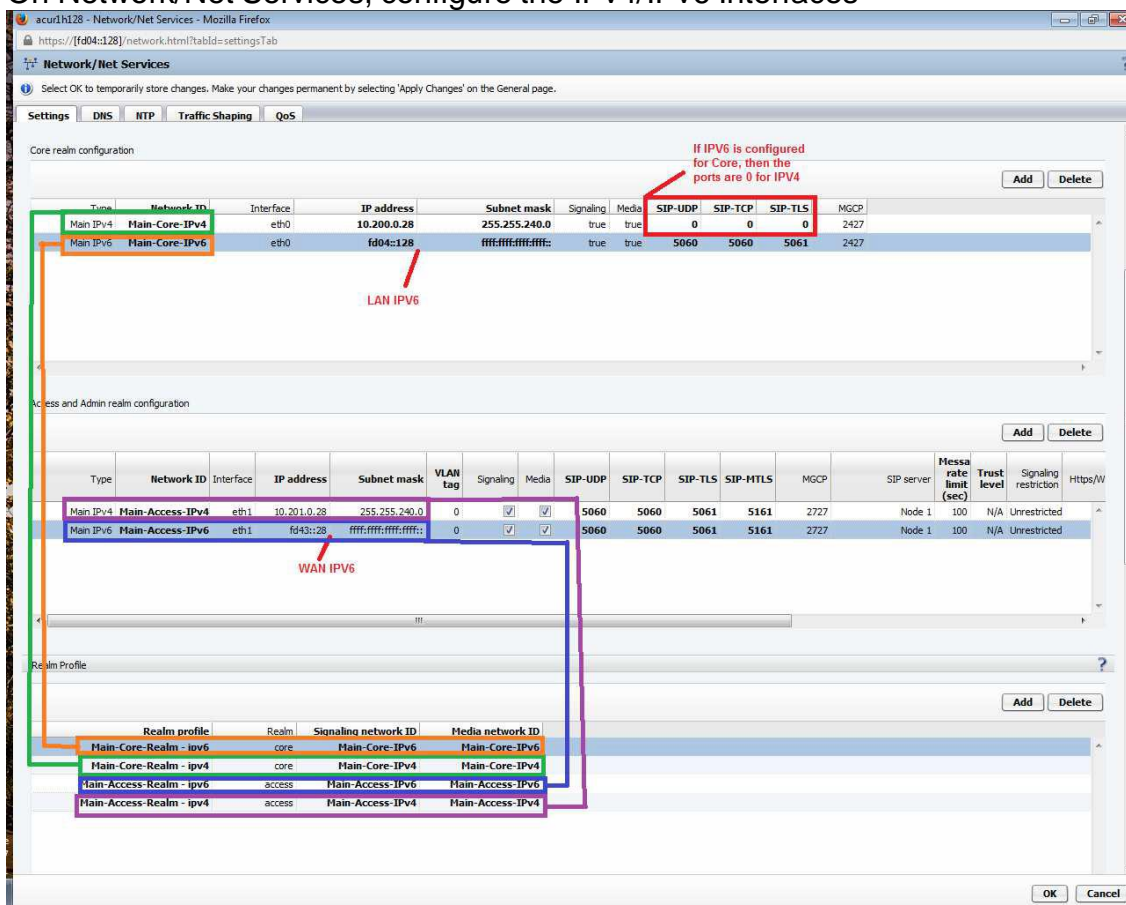
Media Server	IP Address	Status	Available
MS_acur1h126	[10.200.0.26]	Available	Available
MS_acur1h131	[10.200.0.31]	Available	Available
MS_acur1h132	[10.200.0.32]	Available	Available
MS_acur1h134	[10.200.0.34]	Available	Available
MS_acur1h137	[10.201.0.37]	Available	Available
MS_acur1h138	[f004:128]	Available	Available
MS_acur1h149	[10.200.0.49]	Available	Available

The Media Server will be assigned to the Branch Office created before

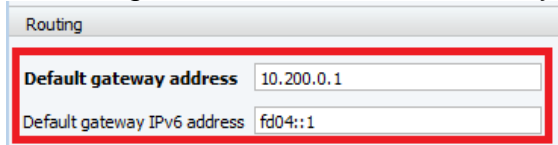


OS SBC Configuration

On Network/Net Services, configure the IPv4/IPv6 Interfaces



Don't forget to set the Default Gateway IPv4/IPv6



On VoIP > Sip Server Settings, configure the IP address of your PBX

acur1h128 - VOIP - Mozilla Firefox

https://[fd04::128]/voip.html?tabid=sipTab

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 Media QoS Monitoring

General

Comm System Type Simplex

Allow Register from SERVER

Other trusted servers

Node 1

Target type Binding

Primary server fed1:182::56 Transport TLS Port 5061

Backup server Transport TCP Port

SRV record Transport TCP

On Features > Remote Endpoints, create an endpoint for the OSB

acur1h128 - Remote Endpoints - Mozilla Firefox

https://[fd04::128]/remoteEndpointConfiguration.html?name=acur1h128

Remote endpoint configuration

Remote endpoint provisioning

Remote endpoint settings

Name acur1h128

Type Proxy

Profile Non-Core-Realm-ipv4

Associated endpoint

Enable Call Limits

Maximum Permitted Calls

Reserved Calls

Remote location information

URI based routing

Enable access control

Signaling address type IP address or FQDN

Remote location domain list

Remote ID	Remote IP (NCP)	Remote transport	Media IP	Media profile	TLS mode	Certificate profile	TLS keep-alive	Keep-alive interval (sec)	Keep-alive timeout (sec)	Dest
10.201.8.38	5061	TLS	default	Server authentication	CDI Solution			120	30	

Remote location identification routing

Core FQDN

Core realm port 5000

Default core realm location domain name

Routing prefix

On Features > Remote Endpoints, create a Media Server profile

acur1h128 - Media Server Profile - Mozilla Firefox

https://[fd04::128]/msProfile.html?name=MS_profile

Media Server Profile

Media server profile provisioning

Name MS_profile

Time to live (sec) 30

Maximum conference time (sec) 18000

Maximum announcement time (sec) 1800

MGCP over SIP

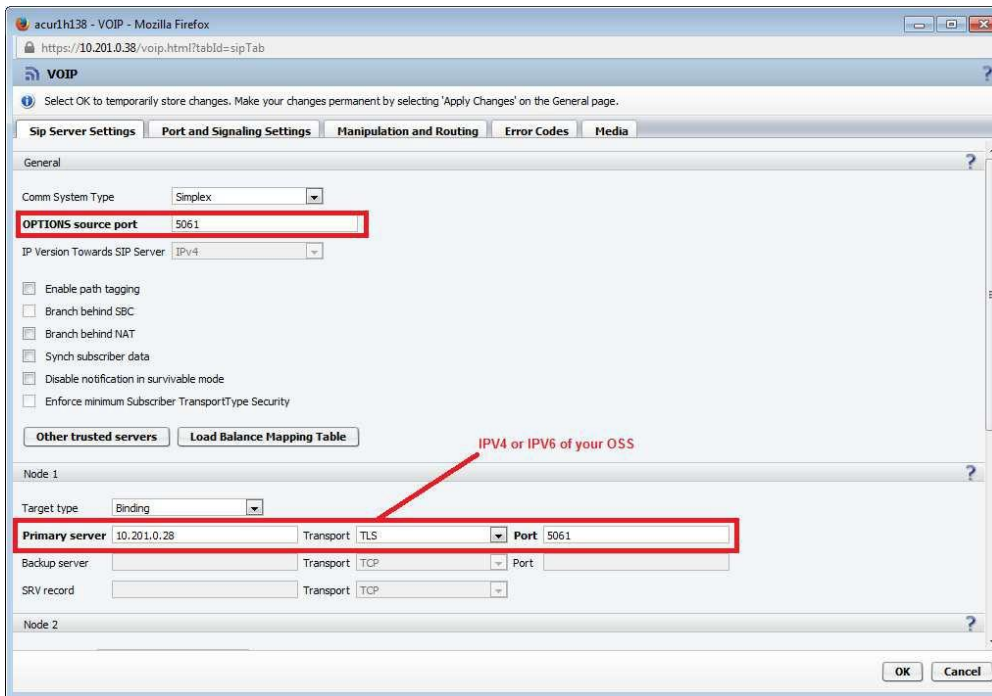
On Features > Remote Endpoints, create an endpoint for the Media Server

Apply the configuration, a reboot may be required.

1.1.3.3 OSB Configuration

On Network/Net Services > Settings, enable the eth1 and configure the IPV4 address on LAN Configuration and IPV6 address on WAN Configuration.

Don't forget to set the Default Gateway IPV4/IPV6



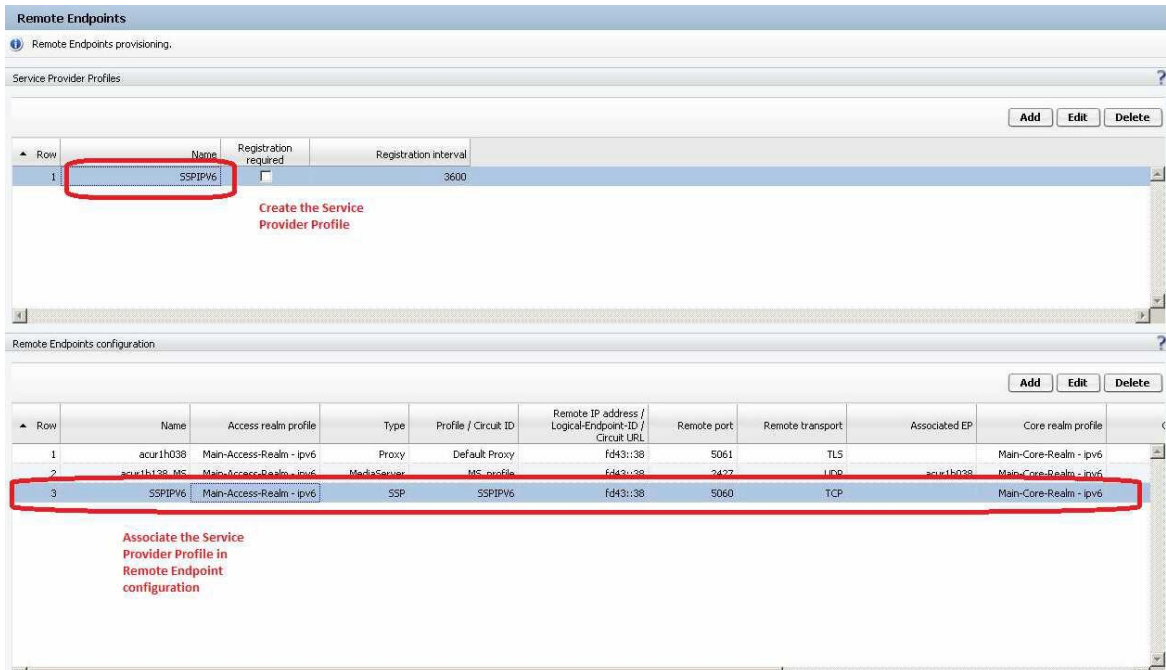
On Features, check the flag Enable Media Server.



Apply the configuration, a reboot may be required.

1.1.4. OS SBC with SIP Server Provider using IPv6

The OpenScope SBC supports the SIP Service Providers with IPv6.



11 Generating SBC Configuration XML file via CDC Tool

The Customer Data Collection (CDC) Tool is an Excel spreadsheet based tool that allows Unify, its channel partners and its customers to work together to plan and record all aspects of an Openscape Voice (OSV) installation, including other Unify components and third party components that are included in the OpenScape Voice network.

The CDC Tool makes configuration of Openscape Voice solutions significantly easier by producing configuration files that can be used for Openscape SBC.

In order to generate an SBC Configuration file with the CDC Tool, the CDC Standard Edition of the tool should be retrieved from SWS and used. The CDC Tool consists of a series of worksheets designed to be populated with the entire OSV solution. Various pieces of information from these various sheets have an impact on the generated SBC Configuration file. Besides data for the SBC itself that must be entered, data identifying the OSV Signaling IP addresses, transport protocol and subscriber data must also be provided and is used to generate the corresponding OSV configuration file and SBC configuration file.

Once all the relevant data is entered, the CDC Tool can generate the configuration files. This includes the OSV configuration data (MP2) file to create the necessary data on the Openscape Voice Server and the SBC configuration file to install and configure physical or virtual SBC(s). With the vApp option, it will also generate the necessary vApp ISO image with SBC configuration files to install a single SBC or multiple SBCs.

Relevant sheets in the CDC tool for SBC Configuration file generation include:

- Quick Start Sheet
- Std. General Sheet
- Std. IP Sheet
- Std. Site Sheet
- Std. Endpoints Sheet
- Std. Subscribers Sheet

Please refer to the Openscape Voice V7R1, Design and Planning Manual: Customer Data Collection document for more general information on how to use the CDC Tool.

Quick Start Sheet

The Quick Start sheet is used to select the Deployment Architecture to be used and set the Openscape Voice Version, Openscape SBC version.

- Deployment Architecture

- Select either "Standard Solution" (default) or "Standard Solution/vApp".
Use the vApp option if generating virtual SBC's with vApp ISO image.
- OpenScape Voice Version
 - Select appropriate version for the solution: 7R1 or 7R0
- OpenScape SBC version
 - Select appropriate version for the planned SBC: 7R1 or 7R0

Refer to Section 4.1.3, Quick Start Worksheet, of the Design and Planning Manual for more information.

Std. General Sheet

This is the sheet to set the switch configuration. Many of the settings here will affect the settings in the SBC configuration file. Some of the fields here are mandatory and so data must be provided, like Openscape Voice Type, Node Separation, Hardware Platform, OpenScape Switch ID, Company Name, Business Group Name, Business Group Default Display Number, User Digest Password Generation. The values entered in these fields may affect other fields on other sheets within the CDC tool and ultimately the data generated in the SBC configuration file, regarding the OSV mode and node configuration.

The SIP transport type field will dictate the transport protocol used between the SBC and the OSV and the default port numbers (5060 for TCP/UDP or 5061 for TLS)

Other SBC related fields include:

- Enable FQDN support on OSV
 - "yes/no" to use FQDNs to identify the SBC in the OSV and to identify the OSV in the SBC configuration.
- SBC: Media Protocol
 - Pass-thru : if chosen, SRTP method below is irrelevant
 - SRTP+RTP
 - RTP
- SRTP method:
 - mikey
 - sdes
- SBC: Enable Remote Endpoints
 - "yes/no" to enable configuring Remote endpoints behind the SBC.
The only Remote endpoint type supported via the CDC tool is the SSP type.
- SBC: Enable Remote Subscribers
 - "yes/no" to enable Remote subscribers behind the SBC.

- DSCP QOS for SIP/MGCP
- DSCP QOS for RTP

Refer to Section 4.3.1, Std. General Worksheet, of the Design and Planning Manual for more detailed information on the parameters in this sheet.

Std. IP Sheet

The IP Sheet is used to identify the OSV subnets and IP information for the nodes of the OSV for TCP or TLS, as well as provide the License server and media server IP/FQDNs, as well as the DNS server, NTP server and domain name for the solution.

The DNS server IP and NTP server IP provided here are populated in the SBC configuration file as well as the Domain Name field.

The OSV signaling IP/FQDNs provided here are also propagated to the SBC configuration file to configure the SBC to OSV (Core side) communication.

Refer to Section 4.3.2, Std. IP Worksheet, of the Design and Planning Manual for more detailed information on the parameters in this sheet.

Std Site Sheet

The Std Site sheet defines some basic parameters to be used in the Dialing Plan, Routing Plan, Voicemail (Xpressions) and Subscriber Data sheets. Please note that the first site, also known as the Headquarters, is the only site allowed to have one or more Central SBC(s) associated with it on the Std Endpoint sheet.

Below is a bare minimum of what fields should be populated.

Topic	Headquarters / Site 1
Site Name	CDC1
Site Component in the Domain Name (FQDN)	
DNS SRV Record Of The Site Proxy (DNS SRV)	
Extension ranges	1010-1020
Access code for outgoing line	8
Time Zone	US/Eastern
Make default subscribers for the extension range	no
Make the created subscribers also UC App. users	no
Make default Xpressions voice mailboxes for the extension range	no
Site prefix	123
Local NTP server	

Backup Gateway for Local Gateway	
Central Gateway	
Default Device Type for the Subscribers	OpenStage 40
Default Dialing Permissions for the Subscribers	International
Default Prompt Language for the Subscribers	
Second Language for Announcements (optional)	
Xpressions Direct Access Number	
Xpressions Guest/Forward Access Number	
Xpressions Callback Access Number (UC VoiceMail)	
Xpressions Transfer Access Number	
Media Server Conference Number	
Auto Attendant Public Number	
Use Local Toll Tables	no
Default First Speed Dial List	
Default Second Speed Dial List	

Refer to Section 4.3.3, Std. Site Worksheet, of the Design and Planning Manual for more detailed information on the parameters in this sheet.

Std. Endpoint Sheet

This is the sheet to define the Central SBC as an endpoint in the Openscape Voice Solution. On this sheet the endpoint name, hostname, type and usage are defined. The endpoint is also associated with a site from the Site sheet, and the LAN and WAN IP addresses of the C-SBC are configured. Also an SSP remote endpoint can be configured behind the C-SBC.

Please note that if no other endpoint types are configured on this page (such as gateways, proxies, OSBs) then a dummy entry (with Endpoint Usage = Dummy) must be created to specify a Country code, Area code and subscriber DN data range in order for the CDC tool to generate the SBC configuration file. If a SSP is optionally provisioned behind the C-SBC then a Country code, Area code and DN range should be provided with that C-SBC entry and therefore a dummy entry is not necessary.

The relevant parameters on this sheet include:

- Endpoint Name
 - Name of the SBC endpoint, up to 12 characters. For a Central SBC, the CDC Tool will append a "_OP" to this value to make the OPTIONS (i.e. main) endpoint name in the endpoint data on the OSV. If an optional SSP is configured on this C-SBC, then the CDC Tool will also create the endpoint data in the OSV for the SSP using this name.
- Site Name

- select which site this endpoint is for. Central SBC's are only allowed in the headquarters site.
- Hostname
 - SBC Hostname will be propagated to the SBC Configuration XML.
- Endpoint Type
 - select one of five types for the Central SBC. If using the "Standard Solution/vApp" Deployment Architecture, then select one of the Virtual SBC types below.
 - OpenScape SBC [IBM x3250]
 - OpenScape SBC [IBM x3550]
 - OpenScape SBC [Fujitsu RX200]
 - OpenScape SBC 6000 [Virtual SBC/vApp]
 - OpenScape SBC 20000 [Virtual SBC/vApp]
- Endpoint Signalling Type
 - select SIP
- Endpoint Usage
 - describes how the endpoint is used. For Central SBC, select "Central SBC".
 - If no other endpoint types are added to this sheet AND no SSP is configured on the SBC, a second entry must be created with endpoint type of "Dummy".
- Country Code
 - The remote site's country code. At least one entry on this sheet must specify a value for this field or else the CDC Tool will not generate an SBC configuration file.
- Area Code
 - The remote site's area code. At least one entry on this sheet must specify a value for this field or else the CDC Tool will not generate an SBC configuration file.
- Local Exchange Code
 - The local exchange (office code) for the remote site. At least one entry on this sheet must specify a value for this field or else the CDC Tool will not generate an SBC configuration file.
- DID Extension Range
 - The Direct Inward Dialing extension range.
- Default Home DN

- This is an optional field included in the SBC configuration when an SSP is configured behind this Central SBC. Also appears in the OSV endpoint data for the Central SBC and the SSP.
- Signaling Endpoint IP
 - The LAN/Core side (Admin) IP address to be used for the Central SBC.
- Signaling Endpoint Netmask
 - The netmask of the signaling network used for the Central SBC.
- Signaling Endpoint Default GW
 - The default gateway IP address of the LAN/Core side network used by the Central SBC.
- WAN IP
 - The WAN/Public side IP address to be used for the Central SBC. This is mandatory for Central SBCs.
- WAN Netmask
 - The netmask of the WAN signaling network of the Central SBC. This is mandatory for Central SBCs.
- WAN Default GW
 - The default gateway IP address of the WAN signaling network used by the Central SBC. This is mandatory for Central SBCs.
- SIP Service Provider (SSP)
 - This is optional and only used for Central SBC endpoint types to configure an SSP behind the Central SBC. Select any one of the predefined values in the pull down list. Certain flags will be set in the SSP Profile in the SBC Configuration file based on the selection made.
 - Even if the desired SSP is not in the pre-defined list, select any one from the list and proceed to fill in the IP address, port and transport protocol for the desired SSP. This will ensure that the OSV data is created with the remote endpoint and the SBC Configuration file is created with the remote endpoint.
 - For the Skype SSP, further configuration is required after installation of the Central SBC to configure the sip service address and digest authentication user id and password.
- SSP IP Address
 - Only relevant for SSP behind Central SBC. The IP address/FQDN of the SSP.

- **SSP SIP Port**
 - Only relevant for SSP behind Central SBC. This is the SIP port used by the SIP Service Provider. Where there is an SSP but this field is empty, the default port 5060 for UDP/TCP or 5061 for TLS is used.
- **SSP SIP Transport**
 - Only relevant for SSP behind Central SBC. This is the SIP transport protocol used by the SIP Service Provider. When there is an SSP and this field is empty, then the value of the SIP Transport Std General Sheet is used.

Here is a sample configuration of an Central SBC without an SSP:

M	M	M	M
Endpoint Name (Gateway or Proxy Name)	Site Name	Hostname	Endpoint Type
CDC-SBC-212	CDC1	sbc-212	OpenScope SBC 6000 [Virtual SBC/vApp]
dd1	CDC1	dumm	Other

M	M	M [E]	M [E]	M [E]	M [E]
Endpoint Signalling Type	Endpoint Usage	Country Code	Area Code	Local Exchange Code	DID Extension Range
SIP	CentralSBC				
SIP	Dummy	1	314	544	1010-1020

M [E]			M	M	M
Default Home DN	PSTN Provider Name	Line Channel Selection	Signaling Endpoint LAN IP	Signaling Endpoint LAN Netmask	Signaling Endpoint LAN Default GW
			10.232.65.212	255.255.255.0	10.232.65.1
13145441010					

M (SBC)	M (SBC)	M (SBC)	SBC relevant only			
WAN IP	WAN Netmas	WAN Default	SIP Service Provider	SSP IP Address	SSP SIP	SSP SIP Transport
10.191.0.41	255.255.0.0	10.191.0.1				

Here is a sample configuration with an SSP.

M	M	M	M
Endpoint Name (Gateway or			

CDC-SBC-212

CDC1

sbc212

OpenScape SBC 6000 [Virtual SBC/vApp]

M	M	M [E]	M [E]	M [E]	M [E]
Endpoint Signalling Type	Endpoint Usage	Country Code	Area Code	Local Exchange Code	DID Extension Range
SIP	CentralSBC	1	314	544	1010-1020

M [E]			M	M	M
Default Home DN	PSTN Provider Name	Line Channel Selection	Signaling Endpoint LAN IP	Signaling Endpoint LAN Netmask	Signaling Endpoint LAN Default GW
13145441010			10.232.65.212	255.255.255.0	10.232.65.1

M (SBC)

M (SBC)

M (SBC)

			SIP			
WAN IP	WAN Netmask	WAN Default GW	Service Provider (SSP) Address	SSP IP	SSP SIP Port	SSP Transport
10.191.0.41	255.255.0.0	10.191.0.1	Qwest	wansbc98.osstest.com	5061	TLS

Refer to Section 4.3.4, Std. Endpoints Worksheet, of the Design and Planning Manual for more detailed information on the parameters in this sheet.

Std Subscribers Sheet

Entering data in this worksheet is optional. Entering a subscriber in this sheet will add a new subscriber or modify a default generated subscriber. Any data entered in this sheet

overwrites the automatically generated data created by the option "Make default subscribers for the extension range" in the Std Site sheet. This creates the subscribers in the OSV and provides DLS Templates and Profiles for the DLS server to push out phone configurations to the individual phones.

In the case of Central SBC remote subscribers (i.e. subscribers behind the Central SBC), this page provides a column to indicate if the subscriber is a remote subscriber or not:

- Remote Subscriber: "yes/no" field.

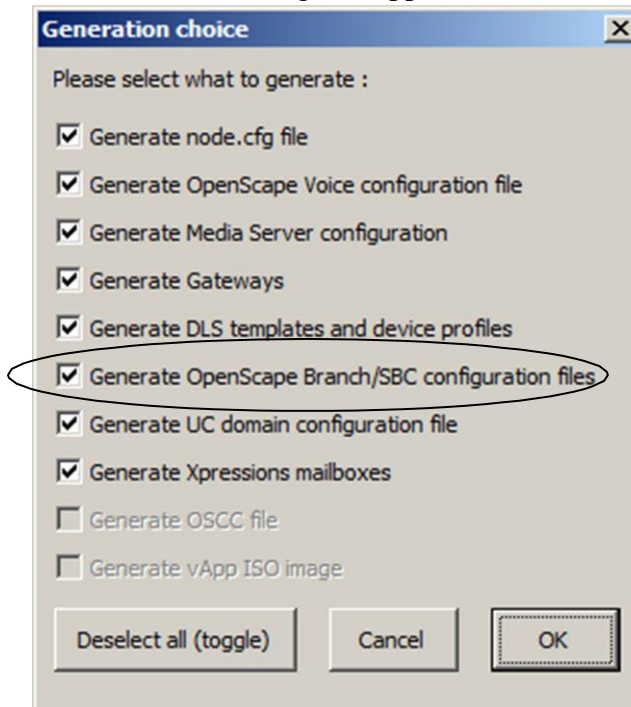
For remote subscribers, the phone must be configured with the WAN IP address of the SBC for the phones SIP Server Address and the SIP Registrar Address. The CDC Tool will provide the necessary DLS profiles with the preconfigured address information.

Refer to Section 4.3.7, Std. Subscriber Worksheet, of the Design and Planning Manual for more detailed information on the parameters in this sheet.

Generating the SBC Configuration XML

Once all the data has been entered on the various sheets in the CDC Tool, this data can be exported to an XML file to preserve the settings and share with others via the Std General worksheet "Export Configuration (XML)" button.

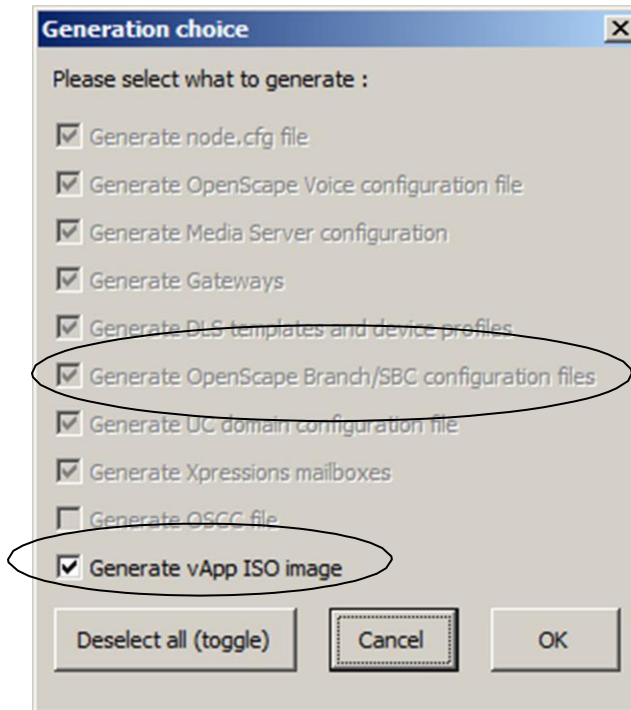
To generate all the configuration files, including the OSV data, DLS profiles, and SBC Configuration file, select the Std Site sheet and select the "Generate All Configuration Files". The following box appears (if Std Solution deployment architecture is used):



This will create a folder for all the configuration files in your working directory, which will include the

- openscapevoiceconfig.txt (MP2) file with the OSV data, and
- SBC_<endpoint_name>.XML, SBC configuration file, and
- DLS profiles.

For the vAPP deployment architecture, the following appears with everything selected including the vApp:



This will create a folder for all the configuration files in your working directory, which will include the

- openscapevoiceconfig.txt (MP2) file with the OSV data, and
- SBC_<endpoint_name>.XML, SBC configuration file, and
- DLS profiles, and
- vApp.iso file, with the necessary files to install and deploy C-SBC.

The SBC XML file can either be used to create a USB stick for SBC installation or can be directly imported into an existing SBC.

The vApp.iso file should be uploaded to the VM Datastore using the vSphere client software and should be assigned to the second DVD device after creating an SBC via the vSphere client "Deploy OVF template". See section X.X of this configuration guide for steps to deploy an SBC via vApp.

12 Security considerations for the OS-SBC

It is very highly recommended that the following steps be taken to secure a OS-SBC which has just been brought up:

1. Change **ALL** default passwords. See [Users/Password Recovery/Change](#).
2. Change the default listening ports. See [SIP listening ports for LAN and WAN Main IP Addresses](#).
3. Enable and configure [Message Rate Control](#) and [Denial of Service Mitigation](#).
4. Configure the internal firewall for the “Main” access interface. See [Internal firewalls](#). This step will need to be performed when ever any new access interface is defined.
5. Configure Administrative Access Control. See [Security and administrative access control](#).
6. Configure the internal firewall for any remote endpoints. See [Internal firewalls](#). This step will need to be performed when ever any new access interface is defined.
7. Change the default gateway from the LAN used during loading to the WAN and setup routing. See [Routing](#).

In a scenario that integrates MS Teams with an Unify OpenScape Voice or OpenScape 4000 using the OpenScape SBC particular care needs to be taken in order to avoid misconfiguration that facilitates toll fraud. The reason is that there is no authentication of the MS Teams subscriber when connecting to the SBC. The security mainly relies on a trust relationship that is established between MS Teams and the SBC during the TLS connection.

The following measures are strongly recommended to reduce the risk for toll fraud when connecting to MS Teams:

1. Import the Trusted CA's proposed by Microsoft (Comment for Dev: include corresponding links).
2. Restrict import of additional CA's to the minimum required for additional SBC Trunk connections (Note: Support of a wide range of Trusted CA's increases the risk of compromise through spoofed certificates).
3. Always use mTLS with full certificate validation of the certificates.
4. Restrict access from MS Teams in the SBC firewall to IP address ranges for MS Teams as published by Microsoft (Comment for Dev: include the corresponding ip address ranges).

Note: Any deviation from the recommended practices should be explicitly accepted by the customer as a risk as this will increase the risk of toll fraud.

12.4 Configuration of “allowed user agent” for OS-SBC

Refer to Denial of Service Mitigation

13 Appendix FortiNet Firewall model 310B Version 4 non TLS



The firewall must **NOT** be SIP aware or MGCP aware.

FortiNet Firewall model 310B

This information is based on FortiGate model 310B, firmware version V4.0 build 0521 (MR 3 Patch 6)

Currently SIP/TLS is not supported by the FortiOS and therefore not part of this document.

The firewall **must not** be SIP-aware or MGCP-aware.

These awareness functions are implemented in the system with session helpers

Use this command to determine if any of the pre-defined session-helpers are in use. [get system session-helper](#)

You can view the session helpers enabled on your FortiGate unit in the CLI using the commands below. The following output shows the first two session helpers. The number of session helpers can vary to around 20.

```
show system session-helper
config system session-
helper
edit 1
set name
pptp set port
1723
set protocol 6
end
next
set name
```



```
h323 set port
1720 set
protocol 6
next
end
```

The configuration for each session helper includes the name of the session helper and the port and protocol number on which the session helper listens for sessions.

Disabling and enable the SIP session helper

You can use the following steps to disable the SIP session helper. You might want to disable the SIP session helper if you don't want the FortiGate unit to apply NAT or other SIP session help features to SIP traffic. With the SIP session helper disabled, the FortiGate unit can still accept SIP sessions if they are allowed by a security policy.

To disable the sip session helper

Enter the following command to find the sip session helper entry in the session-helper list:

```
show system session-helper
```

```
.
```

```
.
```

```
edit 13
```

```
set name sip
```

```
set port 5060
```

```
set protocol
```

```
17 next
```

```
.
```

This command output shows that the sip session helper listens in UDP port 5060 for SIP sessions.

Enter the following command to delete session-helper list entry number 13 to disable the sip session helper:

```
config system session-
```

```
helper delete 13
```

```
end
```

If you want to use the SIP session helper you can verify whether it is enabled or disabled using the [show system session-helper command](#).

To enable the sip session helper

You do not have to disable the SIP session helper to use the SIP ALG.(SIP application layer gateway)

If the SIP session helper has been disabled by being removed from the session-helper list you can use the following command to enable the SIP session helper by adding it back to the session helper list:

```
config system session-
```

```
helper edit 0
```

```
set name sip
```

```
set port 5060
```

```
set protocol
```

```
17 end
```

The same procedure can be used to disable the MGCP helper.

Packet tracings with the FortiGate

Some FortiGate units are equipped with an ASIC. That means that any successfully established session is offloaded from CPU to the ASIC and no traffic will be seen on CPU as long as this session is valid. Normally you will see the first few packets of a new session. Therefore you have to use an external mirror port on a switch or use the fastpath-sniffer command on the FortiGate to see the all packets with the integrated sniffer.

Example to enable the fastpath-sniffer for port 5 and 8

```
# diagnose npu np2 fastpath-sniffer enable port5
```

```
# diagnose npu np2 fastpath-sniffer enable port8
```

Trace the call you are interested

```
# diag sniffer packet <interface_name> <'filter'> <verbose> <count>
```

<interface_name>	The name of the interface to sniff, such as "port1" or "internal". This can also be "any" to sniff all interfaces.
<'filter'>	What to look for in the information the sniffer reads. "none" indicates no filtering, and all packets will be displayed as the other arguments indicate. The filter must be inside single quotes (').
<verbose>	The level of verbosity as one of: 1 - print header of packets 2 - print header and data from IP of packets 3 - print header and data from Ethernet of packets 4 the sniffer trace will display the interface names where traffic enters or leaves the FortiGate unit.
<count>	The number of packets the sniffer reads before stopping. If you don't put a number here, the sniffer will run forever until you stop it with <CTRL C>.

To stop the sniffer, type CTRL+C.

For more information refer to the FortiGate manual.

14 Appendix FortiNet Firewall model 310B Version 5 TLS

14.4 Overview

This document describes the needed configuration settings on the FortiGate to get the voice related SIP/RTP/RTCP working for an OpenScape Solution.

The focus of this guide is the SIP application layer gateway (ALG) of the FortiGate providing the security functionality for SIP/RTP/RTCP. All further needed protocols like HTTPS, DLS, SSH, SNMP, etc. with its attendant configuration for legacy firewall rules follow the common configuration of the FortiGate product and is not repeated here.

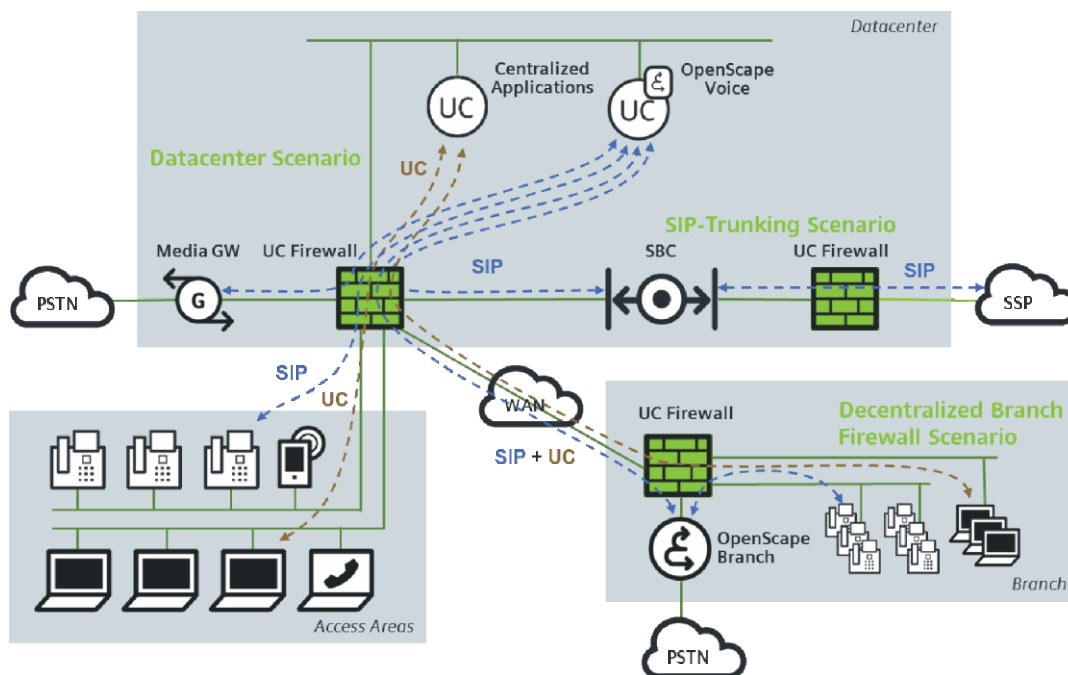


Figure 1: General overview

Dynamic pin-holing is done by the FortiGate to allow the needed (S)RTP/(S)RTCP traffic to pass according to the SIP session initiating the media stream.

The configuration and parameter values of this configuration guide cover the solution scenarios of OpenScape UC Firewall for:

Datacenter / Managed Services

Decentralized Branch Firewall

The configuration needed for the deployment model OpenScape UC Firewall (VPN only mode) as used within the scenarios of OpenScape Video is described in the specific chapter 8.

NOTE:

VoIP connection based upon the H.323 protocol family - like HFA / CorNet - is not subject of this document nor is it supported by the FortiGate on application layer.

14.5 Requirements

The following is required

To have the hardware acceleration for RTP/RTCP packet forwarding one of these hardware models is needed: e.g. 200D, 600C, 1000C, 3600C.

Software version 5.0 build 271 (GA Patch 6) or later on the FortiGate appliance

The currently known minimum required and recommended software version of the OpenScape Solution can be checked in the release notes¹

SIP request and response traffic has to pass the same firewall (symmetric IP routing).

For dynamic pin-holing of RTP/RTCP traffic the SIP signaling has to pass the same firewall as the media stream.

14.6 Restrictions

Dynamic pin-holing for MGCP traffic is not supported as needed by the OpenScape solution. Therefore the setup of a media pin-hole must be done based upon the decisions of the SIP state machine processing the corresponding SIP dialog.

Activating any sort of UTM options on a firewall rule will cause the FortiGate to clear the DSCP field of passing traffic to „0“². This will happen as soon as the described SIP configuration is applied on the firewall. A workaround is available by setting a DSCP value.

FortiGate's HA implementation does not synchronize TCP & TLS states of the UTM for state full failover, this affects SIP. The TCP or TLS session needs to be reestablished first before the next SIP transactions can be processed. This does not apply to UDP encapsulation.

The SIP over TLS software feature is not available on all FortiGate hardware platforms. Please check hardware feature list from Fortinet or release notes of UC Firewall³.

Please check the current version of the release notes of OpenScape UC Firewall regarding further limitations.¹

14.7 Constraints

Although there are some features regarding network address translation in the FortiGate, the usage is not released with the UC Firewall in an OpenScape solution with all aspects of it.

Currently the feature to limit the amount of SIP messages per second is not addressed in this configuration guide. There are no general valid settings for this feature which can be used not having the metered maximum values of the individual setup.

The configuration for the current release is restricted for the usage of with IP version 4.

NOTE:

If any of the excluded/undescribed features is required within a customer project request a NPR for this feature.

¹ Release Notes of OpenScape UC Firewall: please request from thomas.toelg@unify.com

² Technical Note 13587: <http://kb.fortinet.com/kb/viewContent.do?externalId=13587>

³ Known non-supported platforms (not complete): 60D, 90D, 300C

14.8 VoIP Configuration

14.8.9 *Operation modes*

14.8.9.1 Network operation mode

Both “transparent mode” and “NAT mode” are possible to use together with the SIP ALG functionality. Nevertheless it is recommended to use “NAT mode”.

NOTE:

“NAT” mode does not mean the firewall is doing address translation. It is the name of the mode where the FortiGate firewall is integrated as L3 device.

14.8.9.2 Virtualization (VDOM)

The FortiGate can be configured with VDOMs for virtualization in combination with the SIP ALG's functionality of the UTM. The configuration steps of the SIP ALG need to be repeated within each VDOM serving SIP traffic. **Specific global configuration sections are shared by all VDOMs like the configuration of the session-helper and the high availability.** Please consult the FortiGate Guides and documentation regarding VDOMs.

14.8.9.3 SIP ALG / session-helper

It is absolutely important to use the SIP ALG and turn off the former SIP implementation which was realized by a session-helper. The session-helper is enabled by default and must be switched off to enable the SIP ALG which is used for the OpenScape UC Firewall. The actual SIP ALG is enabled through the binding of a voice profile on a firewall rule. For technical details see chapter 6.1: “Deactivate legacy session-helper on FortiGate (CLI)”.

14.8.9.4 Service objects and session expiration (TTL)

For SIP-UDP there is a predefined service object in the default configuration. For SIP-TCP and SIP-TLS the service objects have to be defined with TCP Destination Port Range 5060-5060 respectively 5061-5061 and Source Port range 1-65535. The TCP session expiration timer should be increased from default to 4500 seconds to be long enough for the randomized default SIP expiration timer of 3600.

Name	Protocol	Source Port	Destination Port	TTL
SIP-TCP	TCP	1-65535	5060	4500
SIP-TLS	TCP	1-65535	5061	4500

Table 1: Firewall services

NOTE:

In contrast to TCP the UDP session expiration time must not be changed from default! Otherwise the SIP-ALG will not maintain the pinhole any longer.

14.8.9.5 Firewall rule set

The firewall policy has to fit to the individual deployment. The two tables with a building block are an example illustrating how the rule base could be structured. The first table shows the interface between phones and the SIP server and the second table shows the communication between two SIP servers. The most important task is the assignment of the defined UTM VOIP Profile to the individual firewall rule. The assignment to the rule connects the traffic with the SIP ALG. The assignment of the UTM IPS sensor is recommended, but not required for functionality. The service objects SIP and SIP-TCP have to be selected as needed by the encapsulation of the deployed VoIP installation. If either UDP or TCP is not used the firewall should forbid access by the corresponding encapsulation. Same applies to rules for encrypted/unencrypted SIP traffic.

The following rules show how to allow phone clients to access their SIP server by UDP, TCP or TLS. In case of TLS the selected VoIP profiles additionally binds the certificates being shown and verified within the connection (Therefore individual VoIP profiles "OpenScape-VoIP-Profile-TLS-OSV" and "OpenScape-VoIP-Profile-TLS-OSB" are selected for different destinations).

Source	Destination	Service	UTM VOIP	UTM IPS	Log
SIP-Clients	SIP-OSV SIP-OSB	SIP, SIP-TCP	OpenScape- VoIP-Profile	OpenScape- IPS-Sensor	Accept/Log
SIP-OSV SIP-OSB	SIP-Clients	SIP, SIP-TCP	OpenScape- VoIP-Profile	OpenScape- IPS-Sensor	Accept/Log
SIP-Clients	SIP-OSV	SIP-TLS	OpenScape- VoIP-Profile- TLS-OSV	OpenScape- IPS-Sensor	Accept/Log
SIP-Clients	SIP-OSB	SIP-TLS	OpenScape- VoIP-Profile- TLS- OSB	OpenScape- IPS-Sensor	Accept/Log

Table 2: Firewall policy for SIP traffic from endpoint to server

The next set of rules demonstrates how to allow bidirectional communication between an OSB and an OSV by UDP, TCP and TLS (only one encapsulation will normally be deployed). In case of SIP-TLS the selected VoIP profiles binds the certificates being shown and verified within the MTLS connection (This requires selecting individual VoIP profiles "OpenScape-VoIP-Profile-MTLS-B2V" and "OpenScape-VoIP-Profile-MTLS-V2B" for each direction of the communication).

Source	Destination	Service	UTM VOIP	UTM IPS	Log
SIP-OSB	SIP-OSV	SIP, SIP-TCP	OpenScape- VoIP-Profile	OpenScape- IPS-Sensor	Accept/Log
SIP-OSV	SIP-OSB	SIP, SIP-TCP	OpenScape- VoIP-Profile	OpenScape- IPS-Sensor	Accept/Log
SIP-OSB	SIP-OSV	SIP-TLS	OpenScape- VoIP-Profile- MTLS-B2V	OpenScape- IPS-Sensor	Accept/Log
SIP-OSV	SIP-OSB	SIP-TLS	OpenScape- VoIP-Profile- MTLS-V2B	OpenScape- IPS-Sensor	Accept/Log

Table 3: Firewall policy for SIP traffic from server to server

14.8.10 *Parameters UTM Voice Profile*

14.8.10.1 General profile for UDP, TCP and TLS/MTLS

This table lists the detailed parameters for the setting of the general voice profile “OpenScape-VolIP-Profile”. The parameters described in this table are valid for clear text SIP (UDP, TCP) and for encrypted SIP (SIP-TLS). For encrypted SIP the parameters of the voice profiles are enhanced by additional SSL/TLS settings, described separately. The defined voice profile is referenced by each SIP firewall rule (see above) in the UTM option section of the rule.

Having the knowledge of the exact configuration of the OpenScape Voice some timers may be reduced (see chapter 7: Recommended settings for OpenScape Voice).

Parameter	Value	Comment
ack-rate	0	0 = unlimited / no limitation
block-ack	Disable	
block-bye	Disable	
block-cancel	Disable	
block-geo-red-options	Disable	
block-info	Disable	
block-invite	Disable	
block-long-lines	Enable	The limit is 998 characters defined by parameter “max-line-length”
block-message	Disable	
block-notify	Disable	
block-options	Disable	
block-prack	Disable	
block-publish	Disable	
block-refer	Disable	
block-register	Disable	
block-subscribe	Disable	
block-unknown	Enable	Enable = only defined known SIP methods
block-update	Disable	
bye-rate	0	0 = unlimited / no limitation
call-keepalive	735	Amount of minutes to track the SIP dialog in the firewall table without having seen any RTP traffic.

Parameter	Value	Comment
		735 minutes = 1/2 day + 15 minutes (default: 0 = inactive / do not monitor RTP stream to terminate the SIP dialog if RTP is idle)
cancel-rate	0	0 = unlimited / no limitation
contact-fixup	Disable	for NAT / not applicable
hnt-restrict-source-ip	Enable	for NAT / not applicable restrict expected source IP address for arriving RTP media to that IP address which has been learned from previous signaling (assuming signaling and media are NATed to the same IP address but with individual port numbers)
hosted-nat-traversal	Disable	for NAT / not applicable
info-rate	0	0 = unlimited / no limitation
invite-rate	0	0 = unlimited / no limitation
ips-rtp	Disable	put RTP traffic back to ASIC
log-call-summary	Enable	write log messages that record SIP call progress SIP logging: Log&Report > Log Access > Event SIP archiving: Log&Report > Archive Access > VoIP
log-violations	Enable	logging of SIP violations
malformed-header-allow	Discard	drop message with syntax error in header line
malformed-header-call-id	Discard	drop message with syntax error in header line
malformed-header-contact	Discard	drop message with syntax error in header line
malformed-header-content-length	Discard	drop message with syntax error in header line
malformed-header-content-type	Discard	drop message with syntax error in header line
malformed-header-cseq	Discard	drop message with syntax error in header line
malformed-header-expires	Discard	drop message with syntax error in header line
malformed-header-from	Discard	drop message with syntax error in header line
malformed-header-max-forwards	Discard	drop message with syntax error in header line
malformed-header-p-asserted-identity	Discard	drop message with syntax error in header line
malformed-header-rack	Discard	drop message with syntax error in header line

Parameter	Value	Comment
malformed-header-record-route	Discard	drop message with syntax error in header line
malformed-header-route	Discard	drop message with syntax error in header line
malformed-header-rseq	Discard	drop message with syntax error in header line
malformed-header-sdp-a	Discard	drop message with syntax error in sdp line
malformed-header-sdp-b	Discard	drop message with syntax error in sdp line
malformed-header-sdp-c	Discard	drop message with syntax error in sdp line
malformed-header-sdp-i	Discard	drop message with syntax error in sdp line
malformed-header-sdp-k	Discard	drop message with syntax error in sdp line
malformed-header-sdp-m	Discard	drop message with syntax error in sdp line
malformed-header-sdp-o	Discard	drop message with syntax error in sdp line
malformed-header-sdp-r	Discard	drop message with syntax error in sdp line
malformed-header-sdp-s	Discard	drop message with syntax error in sdp line
malformed-header-sdp-t	Discard	drop message with syntax error in sdp line
malformed-header-sdp-v	Discard	drop message with syntax error in sdp line
malformed-header-sdp-z	Discard	drop message with syntax error in sdp line
malformed-header-to	Discard	drop message with syntax error in header line
malformed-header-via	Discard	drop message with syntax error in header line
malformed-request-line	Discard	drop message with syntax error in request line
max-body-length	4094	maximum size of SIP message body
max-dialogs	0	0 = unlimited / do not limit the number of dialogs
max-idle-dialogs	0	0 = unlimited / do not limit amount of idle dialogs (do not drop idle calls until number is below)
max-line-length	998	Limit if “block-long-lines” is enabled
message-rate	0	0 = unlimited / no limitation
nat-trace	Disable	for NAT / not applicable
no-sdp-fixup	Enable	for NAT / not applicable
notify-rate	0	0 = unlimited / no limitation
open-contact-pinhole	Disable	We assume that each device is registered (📞 open-register-pinhole) and trunking connections are allowed bidirectional by

Parameter	Value	Comment
		firewall rule. Monitoring this is dispensable.
open-record-route-pinhole	Disable	Do not open pinholes according to information derived from record-route. Use explicit firewall rules for signaling.
open-register-pinhole	Enable	Keeps firewall session open for the signaling channel. This maintains the firewall session in case the transport protocol is UDP without adjusting TTL parameters.
open-via-pinhole	Disable	Do not open pinholes according to information derived from via headers. Use explicit firewall rules for signaling.
options-rate	0	0 = unlimited / no limitation
prack-rate	0	0 = unlimited / no limitation
preserve-override	Disable	for NAT / not applicable
provisional-invite-expiry-time	635	allow max 10 min for call setup / cancel (default value is 210 seconds) Some seconds are added on top in case a retransmission of SIP messages should occur.
publish-rate	0	0 = unlimited / no limitation
refer-rate	0	0 = unlimited / no limitation
register-contact-trace	Disable	for NAT / not applicable
register-rate	0	0 = unlimited / no limitation
rfc2543-branch	Disable	Disable = all sip proxies using RFC 3261
rtp	Enable	Enable = open RTP pinhole dynamically
ssl-mode	Off	Do not enable SIP/TLS for UDP and TCP encapsulation
status	Enable	Enable SIP inspection
strict-register	Enable	Enable = SIP Proxy and SIP Registrar must be the same (this conforms to OpenScape) In case a signaling pinhole is created in the firewall (session expectation) the source ip address is restricted to the ip address used for register. If set to disable any ip address will be accepted by the provisioned signaling pinhole.
subscribe-rate	0	0 = unlimited / no limitation
unknown-header	pass	Pass = to allow the unknown header including the X-Siemens header to pass the ALG

Parameter	Value	Comment
update-rate	0	0 = unlimited / no limitation

Table 4: Parameter list for voice profile

14.8.10.2 Profile extension for TLS

This table lists the additional parameters for the voice profile “OpenScape-VoIP-Profile-TLS”. This profile is dedicated to connections using TLS like a phone to the server. It is rather a template as it needs to be completed with two individual references to certificates:

ssl-server-certificate
ssl-auth-server

As this profile binds a specific server certificate to the profile multiple similar profiles may be needed (one for each individual SIP server).

Parameter	Value	Comment
ssl-client-certificate	<empty>	for MTLS / not applicable
ssl-auth-client	<empty>	for MTLS / not applicable
ssl-client-renegotiation	allow	Allow client renegotiation
ssl-pfs	allow	Enable Perfect Forward Secrecy
ssl-server-certificate	<individual>	Reference of the certificate to be returned to the client establishing a new TLS connection
ssl-send-empty-frags	Enable	Send empty fragments to avoid attack on CBC IV (Compatible with SSL 3.0 and TLS 1.0 only)
ssl-mode	full	Enable SIP/TLS support
ssl-client-renegotiation	secure	Reject any SSL connection that does not offer a RFC 5746 Secure Renegotiation Indication
ssl-algorithm	High	Only allow AES and 3DES
ssl-auth-server	<individual>	Authenticate the presented server's certificate with the referenced peer/peergrp
ssl-min-version	tls-1.0	Lowest SSL/TLS protocol version to be negotiated will be TLS 1.0
ssl-max-version	tls-1.1	Highest SSL/TLS protocol version to be negotiated will be TLS 1.1 (max supported)

Table 5: Parameter list for voice profile extensions for TLS

14.8.10.3 Profile extension for MTLS

This table lists the additional parameters for the voice profile “OpenScape-VoIP-Profile-MTLS”. This profile is dedicated to connections using MTLS which is used between two servers within an OpenScape installation. It is rather a template as it needs to be completed with four individual references to certificates:

ssl-server-certificate
ssl-auth-server
ssl-client-certificate
ssl-auth-client

As this profile binds specific certificates to the profile for client and server side, two separate profiles are needed for one SIP connection between two servers, one for each direction in which the communication needs to be able to initiate the communication.

Parameter	Value	Comment
ssl-client-certificate	<individual>	Reference of the certificate to be offered from client to the server when establishing a new TLS connection
ssl-auth-client	<individual>	Enable MTLS and authenticate the presented clients's certificate against the referenced peer/peergrp
ssl-client-renegotiation	allow	Allow client renegotiation
ssl-pfs	allow	Enable Perfect Forward Secrecy
ssl-server-certificate	<individual>	Reference of the certificate to be returned to the client establishing a new TLS connection
ssl-send-empty-frags	Enable	Send empty fragments to avoid attack on CBC IV (Compatible with SSL 3.0 and TLS 1.0 only)
ssl-mode	full	Enable SIP/TLS support
ssl-client-renegotiation	secure	Reject any SSL connection that does not offer a RFC 5746 Secure Renegotiation Indication
ssl-algorithm	High	Only allow AES and 3DES
ssl-auth-server	<individual>	Authenticate the presented server's certificate with the referenced peer/peergrp
ssl-min-version	tls-1.0	Lowest SSL/TLS protocol version to be negotiated will be TLS 1.0
ssl-max-version	tls-1.1	Highest SSL/TLS protocol version to be negotiated will be TLS 1.1 (max supported)

Table 6: Parameter list for voice profile extensions for MTLS

14.8.10.4 Parameters UTM IPS Sensor

On the VoIP rules an IPS sensor can be applied in the UTM section. An example for a simple sensor profile that can be used is given here.

Parameter	Value	Comment
Severity	All	
Target	All	All = client and server
OS	All	
Protocol	SIP, RTP, RTCP, SSL	Some very concerned security people might add "UDP" and "TCP" here. They also can select some specific IDs of IPS pattern.
Application	All	
Quarantine Attackers	No	
Signature settings – Enable	Enable All	
Signature settings – Action	Block all	
Signature settings – Logging	Enable all	
Signature settings – Packet Logging	Disable all	

Table 7: Parameter list for IPS sensor

14.8.10.5 Certificates for SIP-TLS

To use SIP over TLS on the UC Firewall requires the FortiGate to become part of the same Public Key Infrastructure (PKI) which is being used for SIP/TLS of the OpenScape installation. The UC Firewall needs to trust and to know how to validate the certificates presented by the OpenScape's server. And on the other side it does need proper certificates to present to the OpenScape servers or clients like OpenStage phones.

NOTE:

The UC Firewall does not terminate the SRTP or RTP media stream. Therefore it is independent from the used media encryption mechanism. This means RTP without encryption, SRTP with MIKEY#0 or SRTP with SDES are all handled as negotiated by signaling.

The FortiGate terminates the TLS session on the incoming side and establish a new TLS session on the outgoing side. This affects only the TLS layer. To do so the UC Firewall must be equipped with own, individual certificates for TLS/MTLS. Each certificate must meet the certificate profile requirements being valid for the certificate of the original server respectively client. Do not copy the certificates from the original device as it corrupts revocation mechanism and render identification of the original server useless for diagnostic purpose.

The following gives an overview how the UC Firewall integrates into the TLS respectively MTLS connection and which certificates are needed by the FortiGate firewall.

14.8.10.6 Client – Server connection (TLS)

This type of connection address the way a phone (OpenStage, Deskphone, optiPoint, a softclient, etc.) connects to its SIP server (OpenScape Voice, OpenScape Branch). Thereby the IP, TCP and further up the SIP layers are kept. The TLS layer in between is being broken up to be able to read and inspect the SIP messages. The FortiGate tie the two separate TLS sessions logically together to forward SIP messages.

For resilience the connectivity check mechanism for TLS should be activated on the phones. This type of keep alive is supported by the UC Firewall.

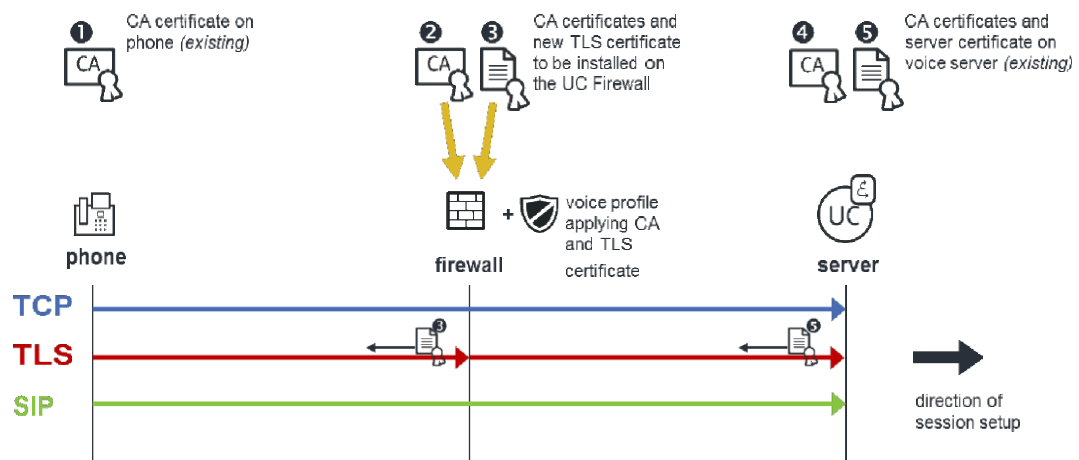


Figure 2: Firewall integration for TLS with certificates

Certificate assignment and usage within the TLS connection:

- ☐ CA certificate to verify presented server certificate ②.
- 🔗 CA certificates to verify presented server certificate ☐ and to be included into the certificate chain of ② on presenting to client. All CA certificates of the chain need to be imported into the FortiGate.
- ② Individual (server) certificate plus private key for the UC Firewall device, having the same identity and identical certificate profile like the (server) certificate ☐. This server certificate is being sent to the client (phone) together with CA certificate chain 🔗 instead of the original certificate ☐.
- 🔗 CA certificates to be included into the certificate chain of ☐ on presenting to client.
- ☐ Certificate plus private key of the OpenScape server being sent to the client together with the CA certificate chain 🔗.

The referenced CA certificates ☐, 🔗, and 🔗 represent the same CA certificate, as long as no PKI hiding is to be realized. In case of a multi-tier CA hierarchy these are multiple CA certificates according to the PKI (here referenced as one for simplicity).

14.8.10.7 Server – Server connection (MTLS)

This type of connection address the way two SIP servers (OpenScape Voice, OpenScape Branch, ...) are connecting to each other. Thereby the IP, TCP and further up the SIP layers are kept. The TLS layer in between is being broken up to be able to read and inspect the SIP messages. The FortiGate tie the two separate TLS sessions logically together to forward SIP messages.

The setup of a new connection can be initiated in both directions. Depending of the direction the TLS role for authentication regarding server and clients are swapped. Both possible directions need to be reflected by the policy with its voice profiles.

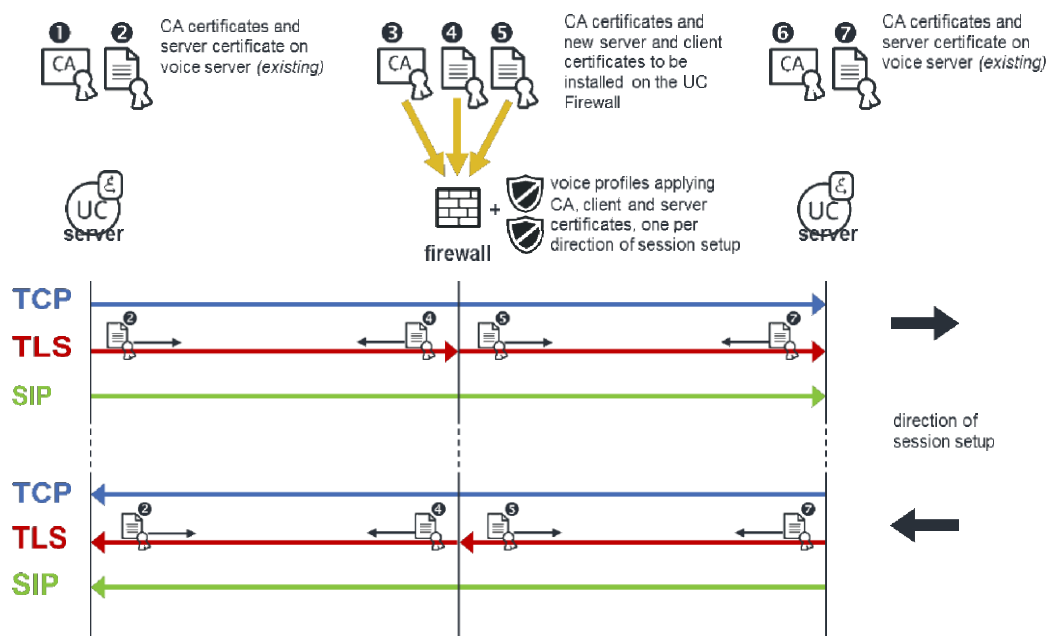












Figure 3: Firewall integration for TLS with certificates

Certificate assignment and usage within the TLS connection during session setup:

- Chain of CA certificates to verify presented certificate and to be included to the certificate on presenting to client or server.
- Certificate plus private key of the OpenScape server being sent to the UC Firewall together with CA certificate chain for client side authentication (session setup from left to right) or server side authentication (session setup from right to left).
- CA certificates to verify presented certificates and . They are also included into the certificate chain of and on presenting them to client or server. All CA certificates of the chain need to be imported into the FortiGate.
- Individual certificate plus private key for the UC Firewall device, having the same identity and identical certificate profile like the certificate . This certificate is being sent to the OpenScape server together with the CA certificate chain instead of the original certificate for server side authentication (session setup from left to right) or client side authentication (session setup from right to left).
- Individual certificate plus private key for the UC Firewall device, having the same identity and identical certificate profile like the certificate .

This certificate is being sent to the OpenScape server together with the CA certificate chain  instead of the original certificate  for client side authentication (session setup from left to right) or server side authentication (session setup from right to left).

-  Chain of CA certificates to verify presented certificate  and to be included to the certificate  on presenting to client or server.
-  Certificate plus private key of the OpenScape server being sent to the UC Firewall together with CA certificate chain  for server side authentication (session setup from left to right) or client side authentication (session setup from right to left).

The referenced CA certificates , , and  represent the same CA certificate, as long as no PKI hiding is to be realized. In case of a multi-tier CA hierarchy these are multiple CA certificates according to the PKI (here referenced as one for simplicity).

14.8.10.8 Using High-Availability (HA) with VoIP

Implementing a UC Firewall within the OpenScape Solution is a crucial component as all traffic passes through it. Implementing it as a standalone firewall would lead to a single point of failure caused by any simple hardware problem. To unravel the security gateway as single point of failure two FortiGate units can be implemented as a high availability cluster using the FortiGate Cluster protocol (FGCP). The FortiGate HA cluster needs to be operated in active-passive HA mode. Setup details for HA configuration can be found in the vendor's configuration manual⁴.

For SIP and RTP Traffic of the OpenScape Voice it is recommended to enable the option "Session Pickup" within the FortiGate's HA configuration. Session pickup must be enabled explicitly and provides session failover. In case of a failover the established stable SIP calls and dynamically opened RTP/RTCP pinholes are available on the backup unit which can take over the traffic.

The outage to media stream and signaling traffic will be the time which takes the backup unit to detect the failure of the active one and to announce it as new active unit.

If TCP is used for SIP encapsulation the TCP session of the signaling channel gets out of sync during failover, which results in drops of SIP messages until TCP is reestablished⁵.

Established SSL/TLS sessions are lost during failover. This requires reestablishing new SIP-TLS signaling connections after failover.

⁴ FortiOS Handbook (FortiOS 5.0) <http://docs.fortinet.com/fgt.html>

⁵ UTM traffic does not avail itself of active "Session Pickup" feature

14.8.10.9 DiffServ Configuration

The SIP ALG is activated by using a VoIP protection profile of the UTM. Having an UTM profile enabled the FortiGate is acting as a transparent proxy, creating a new session from itself to the destination device where the IP packets have the DSCP field set to 0. To overcome this, the DSCP values can be configured on a SIP rule base to apply a defined value.

NOTE:

The DSCP value configured on the rule for the SIP traffic is passed to the media streams descending of this! Currently the configuration cannot distinguish between signaling and media.

14.8.10.10 Alternate/Additional service port for SIP

In case the deployment is using SIP on a different port than the standard port 5060 respectively 5061 it is necessary to configure the alternate port in the FortiGate. For each encapsulation protocol it is possible to configure up to two ports in parallel for SIP traffic inspection globally on the firewall. Only ports defined as SIP ports are inspected by the firewall rules having a voice profile attached.

NOTE:

In configuration examples given within this document we assume that standard port number 5060 is used for SIP respectively 5061 for SIP-TLS.

14.8.11 *Configuration blocks*

This chapter contains the configuration steps to configure the previous described settings of the FortiGate.

14.8.11.1 Deactivate legacy session-helper on FortiGate (CLI)

In the default configuration of the FortiGate a couple of session-helpers are active. Among them following legacy session-helpers need to be disabled: SIP, MGCP, H323, RAS. The corresponding steps to disable the SIP session-helper can be found in the technical note FD31530⁶.

First you have to figure out the correct id number of each session-helper in the individual configuration. In this example these are number "13" for SIP, "2" for H323, "3" for RAS and "19"+"20" for MGCP (defaults for the used release 5.0)

```
config system session-helper
```

```
....
edit 2
    set name h323
    set port 1720
    set protocol 6
next
edit 3
    set name ras set
    port 1719 set
    protocol 17
next
....
edit 13
    set name sip set
    port 5060 set
    protocol 17
next
....
edit 19
    set name mgcp
    set port 2427
    set protocol 17
next
edit 20
    set name mgcp
    set port 2727
    set protocol 17
next
end
```

⁶ Technical Note FD31530: <http://kb.fortinet.com/kb/viewContent.do?externalId=FD31530>

To disable the session-helpers you can use the “delete” command as shown below. Perform this in descending sequence of the id numbers as ids are changed afterwards.

```
fgt # config system session-helper
fgt (session-helper) # delete 20
fgt (session-helper) # delete 19
fgt (session-helper) # delete 13
fgt (session-helper) # delete 3
fgt (session-helper) # delete 2
fgt (session-helper) # end
fgt #
```

Additionally you have to disable the two parameter “sip-helper” and “sip-nat-trace”.

```
config system settings
    set sip-helper disable
    set sip-nat-trace disable
end
```

ATTENTION:

It is necessary to reboot the unit after having done these changes!

14.8.11.2 Service objects and service session timer (CLI)

If TCP or TLS is used for SIP the service has to be defined manually. The definition is a regular FortiGate definition like it is for other services.

```
config firewall service custom
    edit "SIP-TCP"
        set protocol TCP/UDP/SCTP
        set tcp-portrange 5060
    next
    edit "SIP-TLS"
        set protocol TCP/UDP/SCTP
        set tcp-portrange 5061
    next
end
```

Additionally increase the default expiration timer of TCP sessions for the SIP-TCP and SIP-TLS service to 4500 seconds:

```
config system session-ttl
    config port
        edit 5060
            set protocol 6 set
            timeout 4500 set
            end-port 5060
            set start-port 5060
        next
    end
```

```

        edit 5061
            set protocol 6 set
            timeout 4500 set
            end-port 5061
            set start-port 5061
        next
    end
end

```

14.8.11.3 Certificates for SIP-TLS

The CA certificate files – Root CA and its Subordinated CAs – needs to be imported to the FortiGate via the web based interface as base-64 encoded X.509 (PEM) formatted files:

System  Certificates  CA Certificates: Import (Local PC)

All needed CA files of the CA chain must be imported. The result will show up via CLI in section “vpn certificate ca”:

```

config vpn certificate ca
    edit "Root_CA_Certificate"
        . . . .
    next
    edit "Sub_CA_Certificate"
        . . . .
    next
end

```

These imported CA certificates needs to be mapped to “user peer” objects via CLI using the following commands (Example for Root and Sub CA):

```

config user peer
    edit "My_Root_CA"
        set ca "Root_CA_Certificate"
        set mandatory-ca-verify enable
    next
    edit "My_Sub_CA"
        set ca "Sub_CA_Certificate"
        set mandatory-ca-verify enable
    next
end

```

The list of all valid issuing CAs, which are allowed to be accepted when connecting to a server, needs to be populated into a group. The name of this group is in turn referenced within the voice profile.

```

config user peergrp
    edit "Group-CA-Accepted"
        set member "My_Sub_CA"
    next
end

```

The certificate including private key dedicated for the FortiGate device itself needs to be imported via the web based interface as base-64 encoded X.509 (PEM) files split into certificate and key file:

System  Certificates  Local Certificates: Import (Type: Certificate)

This task needs to be repeated for all further certificates of the UC Firewall. The result will show up via CLI in section “vpn certificate local”:

```
config vpn certificate local
    edit "UCFW-as-OSV"
        . . . .
    next
    edit "UCFW-as-OSB"
        . . . .
    next
end
```

14.8.11.4 Voice profile (CLI)

This is the corresponding SIP profile as defined in chapter 5.5.1: “General profile for UDP, TCP and TLS/MTLS”. Remember: only the non-default values are visible in the configuration.

```
config voip profile
    edit "OpenScape-VoIP-Profile"
        set extended-utm-log enable
        config sip
            set open-contact-pinhole disable
            set strict-register enable
            set call-keepalive 735
            set open-record-route-pinhole disable
            set log-violations enable
            set nat-trace disable
            set contact-fixup disable
            set hnt-restrict-source-ip enable
            set max-body-length 4094
            set malformed-request-line discard
            set malformed-header-via discard
            set malformed-header-from discard
            set malformed-header-to discard
            set malformed-header-call-id discard
            set malformed-header-cseq discard
            set malformed-header-rack discard
            set malformed-header-rseq discard
            set malformed-header-contact discard
            set malformed-header-record-route discard
            set malformed-header-route discard
            set malformed-header-expires discard
            set malformed-header-content-type discard
            set malformed-header-content-length discard
            set malformed-header-max-forwards discard
            set malformed-header-allow discard
            set malformed-header-p-asserted-identity discard
            set malformed-header-sdp-v discard
```

```

        set malformed-header-sdp-o discard
        set malformed-header-sdp-s discard
        set malformed-header-sdp-i discard
        set malformed-header-sdp-c discard
        set malformed-header-sdp-b discard
        set malformed-header-sdp-z discard
        set malformed-header-sdp-k discard
        set malformed-header-sdp-a discard
        set malformed-header-sdp-t discard
        set malformed-header-sdp-r discard
        set malformed-header-sdp-m discard
        set provisional-invite-expiry-time 635
        set ips-rtp disable
    end
    config sccp
        set status disable
    end
next
end

```

For SIP/TLS protected communication between endpoint “EP” and OpenScape Voice “OSV” the profile assigning “UCFW-as-OSV” as certificate to “OSV” and grouping PKI CA certificates into “Group-CA-Accepted” extends the profile with the parameter described in chapter 5.5.2: “Profile extension for TLS”:

```

config voip profile
    edit "TLS-EP-to-OSV"
        set extended-utm-log enable
        config sip
            set open-contact-pinhole disable
            set strict-register enable
            set call-keepalive 735
            set open-record-route-pinhole disable
            set log-violations enable
            set nat-trace disable
            set contact-fixup disable
            set hnt-restrict-source-ip enable
            set max-body-length 4094
            set malformed-request-line discard
            set malformed-header-via discard
            set malformed-header-from discard
            set malformed-header-to discard
            set malformed-header-call-id discard
            set malformed-header-cseq discard
            set malformed-header-rack discard
            set malformed-header-rseq discard
            set malformed-header-contact discard
            set malformed-header-record-route discard
            set malformed-header-route discard
            set malformed-header-expires discard
            set malformed-header-content-type discard
            set malformed-header-content-length discard
            set malformed-header-max-forwards discard
            set malformed-header-allow discard
            set malformed-header-p-asserted-identity discard
            set malformed-header-sdp-v discard
        end
    end
end

```

```

        set malformed-header-sdp-o discard
        set malformed-header-sdp-s discard
        set malformed-header-sdp-i discard
        set malformed-header-sdp-c discard
        set malformed-header-sdp-b discard
        set malformed-header-sdp-z discard
        set malformed-header-sdp-k discard
        set malformed-header-sdp-a discard
        set malformed-header-sdp-t discard
        set malformed-header-sdp-r discard
        set malformed-header-sdp-m discard
        set provisional-invite-expiry-time 635
        set ips-rtp disable
        set ssl-mode full
        set ssl-client-renegotiation secure
        set ssl-min-version tls-1.0
        set ssl-server-certificate "UCFW-as-OSV"
    end set ssl-auth-server "Group-CA-Accepted"
    config sccp
        set status disable
    end
next
end

```

Having a SIP/TLS protected communication between two servers like an OpenScape Branch “OSB” and an OpenScape Voice “OSV” the pair of profiles assigning “UCFW-as-OSB” as certificate to “OSB”, “UCFW-as-OSV” as certificate to “OSV” and grouping PKI CA certificates into “Group-CA-Accepted” are the two following profiles. These are extended by the parameters defined in chapter 5.5.3: “Profile extension for MTLs”.

```

config voip profile
    edit "TLS-OSB-to-OSV"
        set extended-utm-log enable
        config sip
            set open-contact-pinhole disable
            set strict-register enable
            set call-keepalive 735
            set open-record-route-pinhole disable
            set log-violations enable
            set nat-trace disable
            set contact-fixup disable
            set hnt-restrict-source-ip enable
            set max-body-length 4094
            set malformed-request-line discard
            set malformed-header-via discard
            set malformed-header-from discard
            set malformed-header-to discard
            set malformed-header-call-id discard
            set malformed-header-cseq discard
            set malformed-header-rack discard
            set malformed-header-rseq discard
            set malformed-header-contact discard
            set malformed-header-record-route discard
            set malformed-header-route discard
            set malformed-header-expires discard
            set malformed-header-content-type discard
        end
    end
end

```



```

        set malformed-header-content-length discard
        set malformed-header-max-forwards discard
        set malformed-header-allow discard
        set malformed-header-p-asserted-identity discard
        set malformed-header-sdp-v discard
        set malformed-header-sdp-o discard
        set malformed-header-sdp-s discard
        set malformed-header-sdp-i discard
        set malformed-header-sdp-c discard
        set malformed-header-sdp-b discard
        set malformed-header-sdp-z discard
        set malformed-header-sdp-k discard
        set malformed-header-sdp-a discard
        set malformed-header-sdp-t discard
        set malformed-header-sdp-r discard
        set malformed-header-sdp-m discard
        set provisional-invite-expiry-time 635
        set ips-rtp disable
        set ssl-mode full
        set ssl-client-renegotiation secure
        set ssl-min-version tls-1.0
        set ssl-client-certificate "UCFW-as-OSB"
        set ssl-server-certificate "UCFW-as-OSV"
        set ssl-auth-client "Group-CA-Accepted"
    end set ssl-auth-server "Group-CA-Accepted"
    config sccp
        set status disable
    end
next
edit "TLS-OSV-to-OSB"
    set extended-utm-log enable
    config sip
        set open-contact-pinhole disable
        set strict-register enable
        set call-keepalive 735
        set open-record-route-pinhole disable
        set log-violations enable
        set nat-trace disable
        set contact-fixup disable
        set hnt-restrict-source-ip enable
        set max-body-length 4094
        set malformed-request-line discard
        set malformed-header-via discard
        set malformed-header-from discard
        set malformed-header-to discard
        set malformed-header-call-id discard
        set malformed-header-cseq discard
        set malformed-header-rack discard
        set malformed-header-rseq discard
        set malformed-header-contact discard
        set malformed-header-record-route discard
        set malformed-header-route discard
        set malformed-header-expires discard
        set malformed-header-content-type discard
        set malformed-header-content-length discard
        set malformed-header-max-forwards discard
        set malformed-header-allow discard

```

```

        set malformed-header-p-asserted-identity discard
        set malformed-header-sdp-v discard
        set malformed-header-sdp-o discard
        set malformed-header-sdp-s discard
        set malformed-header-sdp-i discard
        set malformed-header-sdp-c discard
        set malformed-header-sdp-b discard
        set malformed-header-sdp-z discard
        set malformed-header-sdp-k discard
        set malformed-header-sdp-a discard
        set malformed-header-sdp-t discard
        set malformed-header-sdp-r discard
        set malformed-header-sdp-m discard
        set provisional-invite-expiry-time 635
        set ips-rtp disable
        set ssl-mode full
        set ssl-client-renegotiation secure
        set ssl-min-version tls-1.0
        set ssl-client-certificate "UCFW-as-OSV"
        set ssl-server-certificate "UCFW-as-OSB"
        set ssl-auth-client "Group-CA-Accepted"
    end set ssl-auth-server "Group-CA-Accepted"
    config sccp
        set status disable
    end
next
end

```

14.8.11.5 IPS sensor (CLI)

This configuration block defines the IPS sensor for VoIP with previously described parameters.

```

config ips sensor
    edit "OpenScape-IPS-Sensor"
        config entries
            edit 1
                set action block
                set log-packet enable
                set protocol SIP SSL RTP RTCP
                set status enable
            next
        end
    next
end

```

14.8.11.6 Activate the SIP ALG with firewall rule set (CLI)

The following rules are for reference only. The exact rules have to be written individually to the required policy. Most likely the GUI is being used for this step.

```
config firewall policy
  edit 1
    set srcintf "any"
    set dstintf "any"
    set srcaddr "grp-v-phones"
    set dstaddr "grp-v-sipsm"
    set action accept
    set utm-status enable
    set schedule "always"
    set service "SIP" "SIP-TCP"
    set ips-sensor "OpenScape-IPS-Sensor"
    set voip-profile "OpenScape-VoIP-Profile"
    set logtraffic enable
  next
  edit 2
    set srcintf "any"
    set dstintf "any"
    set srcaddr "grp-v-sipsm"
    set dstaddr "grp-v-phones"
    set action accept
    set utm-status enable
    set schedule "always"
    set service "SIP" "SIP-TCP"
    set ips-sensor "OpenScape-IPS-Sensor"
    set voip-profile "OpenScape-VoIP-Profile"
    set logtraffic enable
  next
end
```

For SIP/TLS there is one rule for phones connecting to the server. The opposite direction does not exist for phones with SIP/TLS.

```
config firewall policy
  edit 3
    set srcintf "any"
    set dstintf "any"
    set srcaddr "grp-v-phones"
    set dstaddr "grp-v-sipsm"
    set action accept
    set utm-status enable
    set schedule "always"
    set service "SIP-TLS"
    set ips-sensor "OpenScape-IPS-Sensor"
    set voip-profile "OpenScape-VoIP-Profile-TLS"
    set logtraffic enable
  next
```

Having a server to server connection using SIP/TLS there are two rules each with an individual voice profile assigned.

```

config firewall policy
  edit 4
    set srcintf "any"
    set dstintf "any"
    set srcaddr "osb01"
    set dstaddr "osv-sipsm3" "osv-sipsm4"
    set action accept
    set utm-status enable
    set schedule "always"
    set service "SIP-TLS"
    set ips-sensor "OpenScape-IPS-Sensor"
    set voip-profile "MTLS-OSB01-to-OSV"
    set logtraffic enable
  next
  edit 5
    set srcintf "any"
    set dstintf "any"
    set srcaddr "osv-sipsm3" "osv-sipsm4"
    set dstaddr "osb01"
    set action accept
    set utm-status enable
    set schedule "always"
    set service "SIP-TLS"
    set ips-sensor "OpenScape-IPS-Sensor"
    set voip-profile "MTLS-OSV-to-OSB01"
    set logtraffic enable
  next

```

14.8.11.7 Certificate Revocation Checking for SIP-TLS

The revocation check for certificates needs to be explicitly configured to enforce it. It could be done by evaluating a downloaded CRL or querying an OCSP server. The FortiGate applies this check to all certificate issued by the specific CA – not only to TLS protected SIP sessions.

To enable revocation checking via CRL the download URL needs to be configured:

```

config vpn certificate crl
  edit "UCFW-CRL"
    set http-url "http://<server>/<path>/<file>.crl"
    set update-interval 3600
  next
end

```

To enable revocation checking via OCSP the responder URI needs to be configured:

```

config vpn certificate ocsp-server
  edit "UCFW-OCSP"
    set url "http://<server>/<path>"
  next
end

```

14.8.11.8 High-Availability settings

The HA configuration can be done via Web GUI or CLI. The most important options (CLI) for VoIP are:

```
config system ha
  set .....
  set mode a-p
  set password <password>
  set .....
  set session-pickup enable
  set .....
end
```

14.8.11.9 Optional DiffServ Configuration (CLI)

To set the DSCP values of forwarded IP packets to a certain value the following commands can be configured on each rule. The values can be set individually for each direction as shown below. Values are applied to all streams signaling and media originating from this rule.

```
config firewall policy
  edit <rule number>
    set .....
    set diffserv-forward enable
    set diffserv-reverse enable
    set diffservcode-forward 011010
    set diffservcode-rev 011010
    set .....
  next
```

The values have to be specified binary.

Example: 011010 = DSCP 26 = AF31 (Assured Forwarding Class 3, Low Drop)

14.8.11.10 Alternate/Additional service port for SIP

The following configuration steps are only needed in case an alternate or additional service port needs to be inspected by the SIP-ALG. The configuration needs to be done individually for each encapsulation protocol. It is an additional step to the firewall policy.

Example for UDP encapsulation with alternate port for SIP inspection:

```
config system settings
  set sip-udp-port 6050
end
```

Example for TCP encapsulation with alternate port for SIP inspection:

```
config system settings
    set sip-tcp-port 15060
end
```

Example for TLS encapsulation with alternate port for SIP inspection:

```
config system settings
    set sip-ssl-port 15061
end
```

14.8.12 Recommended settings for OpenScape Voice

There are some parameter settings in the configuration of the OpenScape Voice which are helpful to align for resilience of the integrated solution.

14.8.12.1 Maximum time for call in provisional state “AlertTimer”

The RTP parameter “Srx/Sip/AlertTimer” defines the maximum time (in milliseconds) a call to remain in ringing state before it will be released by the OSV. On SIP protocol level this is the amount of time after the “180 Ringing” message has been transmitted.

For the OpenScape UC Firewall the following two timers should be aligned:

System	Configuration section	Parameter name
OpenScape Voice	RTP	Srx/Sip/AlertTimer
FortiGate	VoIP Profile	provisional-invite-expiry-time

Table 8: Timer parameter for provisional state

The default values may depend on the installed software version. It is recommended to have the RTP parameter “Srx/Sip/AlertTimer” set to a defined value on the OSV and to adapt this value to the configuration of the FortiGate VoIP-Profile parameter “provisional-invite-expiry-time”. The value used in the VoIP-Profile should be slightly higher than the configured RTP value.

Example:

```
Srx/Sip/AlertTimer = 180000  
provisional-invite-expiry-time = 215
```

NOTE:

The values should be larger than all CFNR timers.

14.8.12.2 Session timers

The use of session timers is recommended for SIP sessions passing the firewall. The use of session timers causes SIP signaling messages to be exchanged on a regular interval between two active SIP endpoints. Especially for the datacenter scenario where no RTP media of an active call can be seen by the firewall, the firewall can recognize that the call is still active and valid.

Using session timers allows a smaller value in the VoIP profile of the parameter “call-keepalive”. This parameter defines the amount of time the dialog is held in the firewall state table without seeing any traffic (SIP, RTP, RTCP) of the related call. The “call-keepalive” must be higher than the interval used by the session timer.

14.8.12.3 Maximum time for an established call

This measure only applies if session timers are not used. Using session timers makes this alignment futile.

Starting a phone call causes the firewall to set up an entry in the firewall sip dialog state table. In case the media traffic does not cross the firewall, session timers are not used and no signaling traffic is generated on the active SIP dialog the firewall must decide when to timeout the entry in the firewall state table in case the dialog has been terminated but the end message has not arrived at the firewall for some reason.

To ensure that the firewall still hadn't freed the state entry the timer in the firewall should be large enough to exceed the duration of the call or the maximum length allowed by the UCE – whatever comes first. This ensures that the firewall has the state entry when the release signaling arrives.

For the OpenScape UC Firewall the following timers should be aligned:

System	Configuration section	Parameter name
OpenScape Voice	RTP	Srx/Main/LongCallTime
	RTP	Srx/Sip/LongCallTimer ⁷
	RTP	Srx/Sip/LongCall_disconnect_enabled ⁷
FortiGate	VoIP Profile	call-keepalive

Table 9: Timer parameter for long calls

The default values and presence of the parameters may depend on the installed software version of OpenScape Voice. It is recommended to have the RTP parameters configured to a defined value on the OSV and to adapt this value to the configuration of the FortiGate VoIP-Profile parameter "call-keepalive". The value used in the VoIP-Profile should be slightly higher than the configured RTP value.

Example:

```
Srx/Main/LongCallTime = 12
call-keepalive = 735
```

⁷ Starting with version V4 of OSV this parameter is obsolete. This is for reference for the older versions (V3).

14.8.13 *OpenScape UC Firewall (VPN only mode)*

With OpenScape Video the FortiGate firewall can be utilized to create an interface based IPSec VPN between two sites. Deploying it as “VPN only mode” device means not to use the advanced security inspection of the SIP ALG and the other application level security functionalities as it is used by the OpenScape UC Firewall. It will not limit the traffic passing the firewall as the firewall is configured not to restrict traffic originated from the VPN tunnel.

The following scenarios of OpenScape Video V7 are using the FortiGate in VPN only mode:

Scenario A4: “Corporate Network – Multiple Sites – VPN secured”

Scenario B3: “Data Centre – SBC protected with VPN”

Scenario R3: “Remote Worker – Remote Worker with VPN”

General setup and VPN configuration of the FortiGate follows the standard procedures as documented in the vendor’s configuration manual⁸. These steps are not repeated here.

As this “VPN only mode” deployment does not take advantage of the application layer inspection the firmer restrictions and constraints of the standard scenarios do not apply.

The only specific configuration task that needs to be performed is the configuration step described in chapter 6.1: “Deactivate legacy session-helper on FortiGate (CLI)”. This will deactivate the by default enabled VoIP protocol evaluation and its interference towards video traffic.

NOTE:

As the firewall is validating the TCP handshake and state of any passing TCP session it must be assured that the devices using the VPN tunnel are assigning distinct source port numbers for each initiated TCP session.

⁸ FortiOS Handbook (FortiOS 5.0) <http://docs.fortinet.com/fgt.html>

14.8.14 *Abbreviations*

ALG	Application Layer Gateway
ASIC	Application Specific Integrated Circuit
CLI	Command Line Interface CorNet “Corporate Network” protocol DLS Deployment Service
DSCP	Differentiated Services Code Point
FGCP	FortiGate Cluster protocol
HA	High-Availability
HTTP	Hypertext Transfer Protocol
HTTPS	TLS secured HTTP IP Internet Protocol
IPS	Intrusion Prevention System
IPSec	Internet Protocol Security
MGCP	Media Gateway Control Protocol
NPR	Non Portfolio Release
OCSP	Online Certificate Status Protocol
PKI	Public-Key-Infrastruktur
PEM	Privacy Enhanced Mail (in context of X.509 format to use base64 encoding) PSR Project Specific Release
RTCP	RTP Control Protocol
RTP	Real-time Transport Protocol SBC Session Border Controller SIP Session Initiation Protocol
SNMP	Simple Network Management Protocol SRTP Secure Real-Time Transport Protocol SRTCP Secure RTP Control Protocol
SSH	Secure Shell
SSL	Secure Sockets Layer
TCP	Transmission Control Protocol
TLS	Transport Layer Security
TTL	Time to live
UDP	User Datagram Protocol UTM Unified Threat Management VoIP Voice over IP
VPN	Virtual Private Network

15 Simplified Installation

Simplified Installation

Load the current released OS-SBC software to the CMP repository

CMP-> Maintenance-> Inventory ->Repository->Add

Note: this is for the files which make up the software load, not configuration or media files.

Add to software repository

Please upload a single ZIP archive containing all the necessary files, or the individual files that make up the software update. In either case, please make sure you upload the mandatory SPA file for the software update which also contains the meta information that appears on the main grid list.

File	Filename	Progress	Action
File 1:	image_oss-02.00.01.10.spa	100%	Browse... Cancel
File 2:	image_oss-02.00.01.10.tar	4%	Browse... Cancel
File 3:			Browse...
File 4:			
File 5:			
File 6:			
File 7:			Browse...
File 8:			Browse...
File 9:			Browse...
File 10:			Browse...

Add another File **Add**

Uploading (3%)...

Save **Cancel**

The SPA file must be the first file in the list. The information in the SPA is used to create the directory where the other files are stored.

When all selected files are uploaded, the “save” button will become active. Click on “save” to complete the upload process.

Configuration **Maintenance** **User Management**

Inventory **Monitoring** **Recovery** **Licenses**

Nodes & Applications

Nodes

Applications

Repository

Software Repository

Product name and Version data are extracted from the SPA file of the corresponding software update. Size is the actual size of the uploaded files.

Search for: in **Product Name** **Search** **Show All**

Add... **Delete**

Product Name	Version	Size
OpenScope SBC V2 R0	V2R0.01.0	286771

Option 1 (zero touch)

Installation Option	USB Stick contents	Description	Comments
1 – Zero touch (must install the right HW box to match the MAC configured in CMP + must pre-configure DHCP servers to return CMP URL)	<ul style="list-style-type: none">• Generic sw used to perform loading, may not be final sw load on the appliance	<ul style="list-style-type: none">• MAC pre-configured in CMP• Use temporary dynamic IP from DHCP for OSB• Fetch CMP URL from DHCP (option 43)• MAC from HW used in getinstallationinfo msg to CMP to fetch sw/config list	Zero touch at site but not at data center (must pre-configure DHCP servers to return CMP URL)

Create the EndPoint for the OS-SBC.

CMP-> Configuration->OpenScape Voice-><business group>-><main Office>->Endpoints->Add

Data is required on the General, SIP, Attributes and Aliases tabs.

It is necessary that the “Endpoint Template” of “Central SBC” be selected. This will cause the “Endpoint Type” to be set to “Central SBC”.

Add the OS-SBC to the OpenScape SBC list

CMP->Configuration->OpenScape SBC->OpenScape SBC list->Add

These will be filled in when the bottom three are filled in from the dropdowns.

Comm Systems

Please select a Comm System.

Items/Page: 200 | All: 1

Comm System
sbctest02

Business Groups

Please select a Business Group.

Items/Page: 200 | All: 19

Business Group
1NR_BG4
Acme
BG-EP-HG1500
BG-HPPC
BG-Vz
BG003
BG004
BG006
BG1

Endpoint

Items/Page: 200 | All: 18

EndpointName	IP Address
OSS-236	10.232.65.236
C-SBC-65-240	10.232.65.240
cSBC-Skype-Main	10.232.63.95
cSBC-Skype	10.232.63.95
C-SBC-RG8700	10.232.65.228
C-SBC-Branch	10.232.65.228
C-SBC-SSPto130	10.232.65.228

Endpoint

Items/Page: 200 | All: 18

EndpointName	IP Address
OSS-236	10.232.65.236
C-SBC-65-240	10.232.65.240
cSBC-Skype-Main	10.232.63.95
cSBC-Skype	10.232.63.95
C-SBC-RG8700	10.232.65.228
C-SBC-Branch	10.232.65.228
C-SBC-SSPto130	10.232.65.228

This will be unchecked the first time a unit is installed. If subsequent installations are required it must be unchecked again

When you click “OK” the OS-SBC will then be added to the “OpenScape SBC list” as shown on the next page.

UNIFY Common Management Platform Domain: system User: administrator@system | Settings | Help | Logout

Configuration Maintenance User Management Fault Management Performance Management Accounting

OpenScape Voice OpenScape Branch **OpenScape SBC** R68700 Unified Communications CMP Device Management

Administration

- Job Management
- General Settings
- Licensing
 - All systems
 - OpenScape SBC list**
 - Select OpenScape SBC
- Management

OpenScape SBC Overview - All systems

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

Filter: for OpenScape SBC

Sel:0 | Items/Page: 100 | All:10

<input type="checkbox"/>	OpenScape SBC	IP Address	Comm System	Business Group	Version	Status	Last Update	Last Configuration
<input type="checkbox"/>	C-SBC-63-230	10.232.63.230	sbctest05	BG1	V8 R0.01.00	Normal	2014/01/15 04:28:16	Wed, 15 Jan 2014 09:55:22
<input type="checkbox"/>	C-SBC-65-215	10.232.65.215	sbctest05	BG1	V8 R0.01.00	Normal	2014/01/15 04:28:16	Thu, 02 Jan 2014 14:27:53
<input type="checkbox"/>	sbcv8media	10.232.63.163	sbctest05	BG1	V8 R0.01.00	Unknown	2014/01/15 04:28:16	Fri, 03 Jan 2014 10:27:18
<input type="checkbox"/>	CSBC_split	10.232.63.70	sbctest05	BG1	V8 R0.01.00	Normal	2014/01/15 04:28:16	Fri, 03 Jan 2014 10:27:18
<input type="checkbox"/>	SBC63_76_v7	10.232.63.76	sbctest05	BG-CSBC	V7R1.14.00	Normal	2014/01/15 04:28:16	---
<input type="checkbox"/>	SBC-213	10.232.65.213	sbctest05	BG-CSBC	V8 R0.01.00	Normal	2014/01/15 04:28:16	Wed, 15 Jan 2014 14:11:41
<input type="checkbox"/>	OSS_202155	10.232.202.155	sbctest05	BG_HUSIM	V7R1.14.00	Normal	2014/01/15 04:28:16	---
<input type="checkbox"/>	Vm_SBC_222	10.232.65.222	sbctest05	BG1	V8 R0.01.00	Normal	2014/01/15 04:28:17	Wed, 15 Jan 2014 15:40:37
<input type="checkbox"/>	CSBC_63_94	10.232.63.94	sbctest05	BG1	V8 R0.01.00	Normal	2014/01/15 04:28:18	Sun, 02 Feb 2014 04:00:23
<input type="checkbox"/>	SBC-Col-IPv4	10.232.51.53	sbctest05	BG1	V7R1.14.00	Normal	2014/01/15 04:28:28	---

Select the checkbox to the left of the OS-SBC and click on “Edit” to open the next window.

Edit the configuration data for the OS-SBC

CMP->OpenScape SBC->OpenScapeSBC list-> select the OS-SBC and Click Edit

OpenScape SBC - Windows Internet Explorer

https://10.232.2.157/management/portal/Applications/Operation/ Certificate error

Edit OpenScape SBC

Enter OpenScape SBC appliance information and select its users.

General

OpenScape SBC Name: CSBC_63_94

IP Address or FQDN: 10.232.63.94

Comm System Type: OpenScape Voice

Comm System: sbctest05


Business Group: BG1


Endpoint: CSBC_63_94


Communicating over Secured channel: ☒

Click here to get the window on the next page

General

 An outage may occur by changing or clearing the MAC Address

Software load: 

Hardware type: 

MAC address:

MAC Address Node 2:

Installation: ☐

Select these from the dropdowns

This is the MAC for the LAN interface of the box to be loaded. The second MAC has to do with licenses for a redundant system.

Check this box to allow installation from the CMP

Click “OK” and “OK” to complete the configuration process.

Upload xml file, for the system to be loaded, to the CMP.

This procedure will upload the desired xml file to the CMP.

CMP->OpenScape SBC->OpenScape SBC list-> select the OS-SBC and Click Edit -> click configure Installation -> select "Data configuration File" tab -> browse for the xml file desired for this SBC -> click Add -> OK -> OK

The xml file will be generated by the CDC tool.

Configuration of the DHCP server

this section allows for the response to the option 60 from the OS-SBC

#

option space Vendor;

option Vendor.swsupply1 code 1 = string;

class "Vendor" {

match if option vendor-class-identifier = "OpenScapeBranch";

vendor-option-space Vendor;

option Vendor.swsupply1 "10.232.2.12,10.232.3.254";

} *These are 2 possible CMPs ****

#

this section provides the temporary address used during the download process

#

subnet 10.232.63.0 netmask 255.255.255.0 {

range 10.232.63.81 10.232.63.89;

option domain-name-servers 10.232.3.122;

option domain-name "lab.dev.global-intra.net";

option routers 10.232.63.1;

default-lease-time 300;

max-lease-time 3600;



**** Note: The 2 CMPs returned do **Not** work in load sharing mode. They work in a true*

"failover"

mode.

For example if the first CMP returned is inaccessible or powered down the appliance will try to contact the

second CMP but if the first CMP responds, even with an error indication like "hardware id does not correspond to Branch office id" the appliance will NOT try to contact the second CMP it will just report the error and the loading will fail.

Creating the USB Stick

The path is <directory where load is stored> \usbsticksetup\ usbsticksetup.exe.
Make sure the “tar” file is copied to <directory where load is stored> \usbsticksetup\ob.

For option 1 (zero touch) check “**Automated**” and “**Preinstall**”
No other configuration needs to be filled in by the user.

If the OS-SBC to be loaded is a IBM 3250 M3 or 3550 M3 the box “Partitioned USB Stick” needs to be checked.

Note: if you are replacing a non-working unit, while keeping the same logical ID, you must allow communications to a non-secure unit on the OpenScape SBC Assistant.
CMP->configuration->OpenScape SBC->SBC list-><select the OS-SBC and Click “edit”>
Also check the “installation” check box under CMP->configuration->OpenScape SBC->SBC list-><select the OS-SBC and Click “edit”> -> configure installation -> general tab.

Installing the load

It is assumed that the unit has arrived at the site with the generic software pre-installed.

1. Connect the unit to be installed to the customer’s network and power.
2. Apply power to the unit.

Note: in the case of an error:

1. Record the number of beeps the unit sounds.
2. Gracefully shut down the unit. This allows the unit to write any remaining information and close the autoinstall.log file on the USB stick.

Note: If you are replacing a non-working unit with a unit of the same type, using options 2, 3 or 4, make sure to clear the MAC address in the OpenScape SBC Assistant first. [CMP->.configuration->Openscape SBC->OpenScape SBC List-><SBC>->edit->Configure Installation](#)

Also check the “installation” check box under CMP->configuration->OpenScape SBC->SBC list-><select the OS-SBC and Click “edit”> -> configure installation -> general tab.

Note: if you are replacing a non-working unit, while keeping the same logical ID, uncheck “Communicating over Secured channel” on the OpenScape SBC Assistant.

Also check the “installation” check box under CMP->configuration->OpenScape SBC->SBC list-><select the OS-SBC and Click “edit”> -> configure installation -> general tab.

Option 2 (HW independent)

General description (from the BO)

Installation Option	USB Stick contents	Description	Comments
2 – HW independent (must pre-configure DHCP servers to return CMP URL)	<ul style="list-style-type: none">Generic swBranch/OS-SBC Logical ID	<ul style="list-style-type: none">Logical ID pre-configured in CMPUse temporary dynamic IP from DHCP for OSBFetch CMP URL from DHCP (option 43)Logical ID used in msg to CMP to fetch sw/config list	must pre-configure DHCP servers to return CMP URL

Refer to [Option 1 \(zero touch\)](#) with the following exceptions

Edit the configuration data for the OS-SBC

Clear the field for the MAC in the OpenScape SBC Assistant

CMP->OpenScape SBC->OpenScape SBC list-> select the OS-SBC and Click Edit-> click Configure Installation

When creating the USB stick, click Automated , Netboot and DHCP. Fill in the Logical ID.

If the OS-SBC to be loaded is a IBM 3250 M3 or 3550 M3 the box “Partitioned USB Stick” needs to be checked.

Installing the load

1. Connect the unit to be installed to the customer’s network and power.
2. Connect the USB stick prepared above and apply power to the unit.
3. Remove the USB stick when directed.

Note: in the case of an error:

1. Record the number of beeps the unit sounds.
2. Gracefully shut down the unit. This allows the unit to write any remaining information and close the autoinstall.log file on the USB stick.

Note: If you are replacing a non-working unit with a unit of the same type, using options 2, 3 or 4, make sure to clear the MAC address in the OpenScape SBC Assistant first. [CMP-.configuration->Openscape SBC->SBC List-><SBC>->edit->Configure](#)

Installation

Also check the "installation" check box under CMP->configuration->OpenScape SBC->SBC list-><select the OS-SBC and Click "edit"> -> configure installation -> general tab.

Note: if you are replacing a non-working unit, while keeping the same logical ID, uncheck "Communicating over Secured channel" on the OpenScape SBC Assistant.

Option 3 (HW independent w/o option 43)

General description (from the BO)

Installation Option	USB Stick contents	Description	Comments
3 – HW independent (no need to pre-configure DHCP servers to return CMP URL)	<ul style="list-style-type: none">• Generic sw• Branch/OS-SBC Logical ID• CMP URL	<ul style="list-style-type: none">• Logical ID pre-configured in CMP• Use temporary dynamic IP from DHCP for OSB• Logical ID used in msg to CMP to fetch sw/config list	No need to go to DHCP server to get CMP URL – only Temporary Dynamic IP

Refer to [Option 1 \(zero touch\)](#) with the following exceptions

Edit the configuration data for the OS-SBC

Clear the field for the MAC in the OpenScape SBC Assistant.
CMP->OpenScape SBC->SBC list-> select the OS-SBC and Click Edit-> click Configure Installation

When creating the USB stick, click Automated , Netboot and DHCP. Fill in the Logical ID and the IP address of the CMP.

If the OS-SBC to be loaded is a IBM 3250 M3 or 3550 M3 the box “Partitioned USB Stick” needs to be checked.

If the OS-SBC to be loaded is a Lenovo SR250/SR250 V2 the “Partitioned USB” flag must be marked, otherwise Lenovo sr250/SR250 V2 won't boot.

Configuration of the DHCP server

For this case the DHCP server is not required to respond to a option 60 request with the address of the CMP (option 43). The address of the CMP is contained on the USB stick.

```
#
# this section provides the temporary address used during the download process
#
subnet 10.232.63.0 netmask 255.255.255.0 {
    range 10.232.63.81 10.232.63.89;
    option domain-name-servers 10.232.3.122;
    option domain-name "lab.dev.global-intra.net";
    option routers 10.232.63.1;
    default-lease-time 300;
    max-lease-time 3600;
```

Installing the load

1. Connect the unit to be installed to the customer's network and power.
2. Connect the USB stick prepared above and apply power to the unit.
3. Remove the USB stick when directed.

Note: in the case of an error:

1. Record the number of beeps the unit sounds.
2. Gracefully shut down the unit. This allows the unit to write any remaining information and close the autoinstall.log file on the USB stick.

Note: If you are replacing a non-working unit with a unit of the same type, using options 2, 3 or 4, make sure to clear the MAC address in the OpenScape SBC Assistant first. [CMP-.configuration->Openscape SBC->SBC List-><SBC>->edit->Configure Installation](#)

Also check the "installation" check box under CMP->configuration->OpenScape SBC->SBC list-><select the OS-SBC and Click "edit"> -> configure installation -> general tab.

Note: if you are replacing a non-working unit, while keeping the same logical ID, uncheck "Communicating over Secured channel" on the OpenScape SBC Assistant.

Option 4 (HW independent local config file)

General description (from the BO)

Installation Option	USB Stick contents	Description	Comments
4 – HW independent Local config file	<ul style="list-style-type: none">• Generic sw• Xml config file	<ul style="list-style-type: none">• Logical ID pre-configured in CMP• Use Static IP from config file for OS-SBC• Logical ID from Xml file used in msg to CMP to fetch sw list	No need to go to DHCP server to get OS-SBC Dynamic IP or CMP URL

Refer to [Option 1 \(zero touch\)](#) with the following exceptions

Configuration of the DHCP server

For this option the DHCP server is **not required**. The static IP address for loading and the IP address of the CMP are both obtained from the xml config file on the USB stick.

Creating the USB Stick

For option 4 a previously generated xml file is selected. Also select Automated and netboot.

If the OS-SBC to be loaded is a IBM 3250 M3 or 3550 M3 the box “Partitioned USB Stick” needs to be checked.

The xml file will be generated by the CDC tool.

Set default gateway for LAN and WAN to the LAN's gateway for the installation phase.

Installing the load

1. Connect the unit to be installed to the customer's network and power.
2. Connect the USB stick prepared above and apply power to the unit.
3. Remove the USB stick when directed.

Note: In the case of an error:

1. Record the number of beeps the unit sounds.

2. Gracefully shut down the unit. This allows the unit to write any remaining information and close the autoinstall.log file on the USB stick.

Note: If you are replacing a non-working unit with a unit of the same type, using options 2, 3 or 4, make sure to clear the MAC address in the OpenScape SBC Assistant first. [CMP-.configuration->Openscape SBC->SBC List-><SBC>->edit->Configure Installation](#)

Also check the “installation” check box under CMP->configuration->OpenScape SBC->SBC list-><select the OS-SBC and Click “edit”> -> configure installation -> general tab.

Note: if you are replacing a non-working unit, while keeping the same logical ID, uncheck “Communicating over Secured channel” on the OpenScape SBC Assistant.

Actual installation process

If the unit came to the field “pre-installed”, connect the unit to the customer’s network and power up the unit. (no USB stick required)

If the unit is not “pre-installed”, plug in the USB stick created for the selected option above, connect the unit to the customers network and power up the unit. When directed remove the USB stick and the unit will boot.

Audio indications of success or errors.

Different audible beeps, if hardware supports, will be provided to the installer so the installer can determine the nature of the problem.

Beeps will occur for 10 cycles.

When installation is successful OS-SBC will **beep once**, pause, and repeat)

2 Beeps, pause and repeat represent the following error conditions:

- Cannot contact DHCP
- DHCP server did not return temporary dynamic IP for OSB
- DHCP server not configured to return CMP URL

3 Beeps, pause and repeat represent the following error conditions:

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

4 Beeps, pause and repeat represent the following error conditions:

- Installation Info unavailable

- File Transfer unsuccessful
- Boot Failure Note: it may not be possible to provide the beeps depending on the nature of the boot failure
- SOAP Responses received with negative acks
- No Response to SOAP Requests sent by OSB
- SOAP Requests received that have invalid data

When possible information will also be logged and shown on the CMP.

Special steps for installation of redundant OS-SBC system using Simplified Installation

1. Create endpoint for node 1 in OSV using actual IP addresses
2. Create node 1 in OpenScape SBC assistant edit load, HW type and HW ID.
3. Save the xml file for node 1 under the logical ID
4. Create endpoint for node 2 in OSV using actual IP addresses
5. Create node 2 in OpenScape SBC assistant edit load, HW type and HW ID.
6. Save the xml file for node 2 under the logical ID
7. Use “zero touch” to install node 1
8. Use “zero touch” to install node 2
9. Enable the Redundancy on Node 1. 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.

Now that the loading is complete, the discrete node IPs are no longer required. The OSV will communicate with the redundant OS-SBC nodes via the Virtual IP address. The following steps remove the discrete IPs and creates the virtual IP. If this is not done the OSV will attempt to send OPTIONS message to each discrete node.

10. Delete node 1 from the OpenScape SBC assistant
11. Delete node 2 from the OpenScape SBC assistant
12. Delete node 1 from the OSV (prevent OSV from sending options to this IP address)
13. Delete node 2 from the OSV (prevent OSV from sending options to this IP address)
14. Create endpoint for the redundant pair, in the OSV, using the VIP address. This allows call processing.
15. Create the virtual node in the OpenScape SBC assistant. This will allow management of the virtual node. (master OS-SBC). Licenses etc.

The xml file will be generated by the CDC tool.

16 DNSSRV for TLS phones

How to setup for DNS SRV with PHONES using TLS

On your DNS server:

The screenshot shows a 'Service Location (SRV)' dialog box with the following fields and values:

- Domain:** siemens.com
- Service:** _sips
- Protocol:** _tcp
- Priority:** 1
- Weight:** 0
- Port number:** 65061
- Host offering this service:** nsn.siemens.com
- ☐ Delete this record when it becomes stale
- Record time stamp:** (empty field)
- Time to live (TTL):** 0 :0 :5 :0 (DDDD:HH.MM.SS)

At the bottom are buttons for OK, Cancel, Apply, and Help.

Create DNS SRV Record in your zone (siemens.com) for Service "_sips" using Protocol "_tcp" and provide a FQDN for the WAN side of your SBC (nsn.siemens.com) and the SBC WAN side Listening port (65061).

Host (A)

Host (uses parent domain if left blank):

Fully qualified domain name (FQDN):

IP address:

☒ Update associated pointer (PTR) record
☐ Delete this record when it becomes stale

Record time stamp:

Time to live (TTL): :0 :5 :0 (DDDDD:HH.MM.SS)

OK Cancel Apply

Create an A record entry in the DNS server for the FQDN of your SBC's WAN side.

On each phone using administrator privileges:

Registration

SIP Addresses

SIP server address	siemens.com
SIP registrar address	siemens.com
SIP gateway address	

SIP Session

Session timer enabled	<input type="checkbox"/>
Session duration (seconds)	408
Registration timer (seconds)	408
Server type	OS Voice
Realm	realm
User ID	15615591029
Password	*****
MLPP base	Local
MLPP Domain	dsn+uc
Other Domain	

SIP Survivability

Backup registration allowed	<input checked="" type="checkbox"/>
Backup proxy address	
Backup registration timer (seconds)	3600
Backup transport	UDP
Backup OBP flag	<input type="checkbox"/>

Submit Reset

On the phone, set the SIP server address and SIP Registrar address to your domain.

Port configuration

SIP server	0
SIP registrar	0
SIP gateway	0
SIP local	5061
Backup proxy	0
RTP base	5010
Download server (default)	21
LDAP server	389
LAN port speed	Automatic
PC port speed	Automatic
PC port mode	disabled
PC port autoMDIX	<input type="checkbox"/>

Submit Reset

Set the Ports to 0 except for the SIP local port on the Phone.

Administrator Pages
User Pages
Logout

Admin Login
Network
General IP configuration
IPv4 configuration
IPv6 configuration
Update Service (DLS)
QoS
Port configuration
LLDP-MED operation
System
System Identity
SIP interface
Registration
SNMP
Features
Security
File transfer
Local functions
Date and time
Speech
General information
Security and Policies
Ringer Setting
Mobility
Diagnostics
Maintenance

General IP configuration

Protocol Mode
IPv4_IPv6
LLDP-MED Enabled
DHCP Enabled
DHCPv6 Enabled
VLAN discovery
Manual
VLAN ID
DNS domain
siemens.com
Primary DNS
10.232.3.122
Secondary DNS
Submit
Reset

Set the DNS domain and Primary DNS on the phone.

Administrator Pages
User Pages
Logout

Admin Login
Network
General IP configuration
IPv4 configuration
IPv6 configuration
Update Service (DLS)
QoS
Port configuration
LLDP-MED operation
System
System Identity
SIP interface
Registration
SNMP
Features
Security
File transfer
Local functions
Date and time
Speech
General information
Security and Policies
Ringer Setting
Mobility
Diagnostics
Maintenance

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
Keep alive format
Sequence
Media Negotiation
Single IP
Media IP Mode
IPv4
Submit
Reset

This is what the REGISTER msg looks like from the phone to the SBC:

%BREGISTER sip:unify.com;transport=tls SIP/2.0
Accept: application/dls-contact-me
Via: SIP/2.0/TLS 10.232.3.117:5061;branch=z9hG4bKf401e6002c80924de
Max-Forwards: 70
From: "15615591029" <sip:15615591027@unify.com>;tag=227688a3fa
To:
<sip:15615591027@unify.com>
Call-ID: 3bb03a2a7d2d20d4
CSeq: 2026383700 REGISTER
Contact:"15615591029"<sip:15615591027@10.232.3.117:5061;transport=tls>;ex
pires=4
08
Supported: X-Siemens-Proxy-State
User-Agent: OpenStage_40_V3 R1.41.0 SIP 130205 simple-
uaCSTA X-Siemens-IID: 802MAC=001ae802a7d2
Content-Length: 0

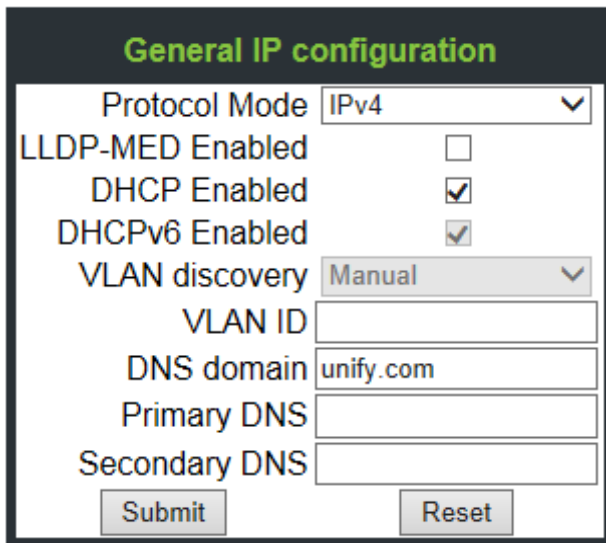
17 Configuration of location for emergency calls

Setting Location of “remote subscribers” for emergency calls

Using DHCP option 120

This provides the greatest granularity for locations.

1. Set the phone to use DHCP



The screenshot shows a web-based configuration interface titled "General IP configuration". It contains several settings for network configuration:

- Protocol Mode: A dropdown menu set to "IPv4".
- LLDP-MED Enabled: A checkbox that is currently unchecked.
- DHCP Enabled: A checkbox that is checked.
- DHCPv6 Enabled: A checkbox that is checked.
- VLAN discovery: A dropdown menu set to "Manual".
- VLAN ID: An empty text input field.
- DNS domain: A text input field containing "unify.com".
- Primary DNS: An empty text input field.
- Secondary DNS: An empty text input field.

At the bottom of the form are two buttons: "Submit" and "Reset".

2. The DHCP server must support DHCP option 120
The DHCP server returns something like building1.unify.com per RFC 3361.

00 = the encoding for FQDN

03 = length of br1

627131 = br1

05 = length of unify

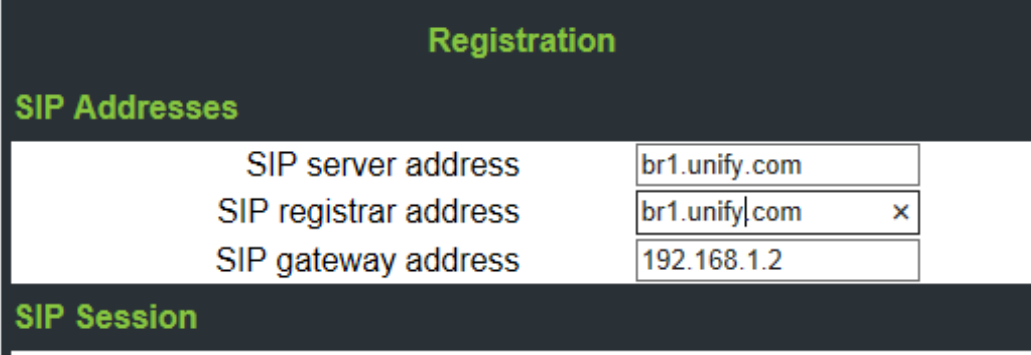
7563696679

03 = length of com

636F6

00 end of string

The phone will store that result as shown here.



The screenshot shows a configuration interface with a dark header and a light content area. The header is labeled 'Registration' in green. Below it, the section 'SIP Addresses' is also in green. There are three rows of configuration fields:

SIP Addresses	
SIP server address	br1.unify.com
SIP registrar address	br1.unify.com x
SIP gateway address	192.168.1.2

Below the SIP addresses section, the 'SIP Session' section is partially visible in green.

3. The DNS server must be set to return the WAN address of the SBC in response to the DNS query from the phone.

4. The SBC must be set to recognize the dialed digits as emergency (in the US this is 911).

Local GUI → Features → Remote Subscribers configuration → Add/Edit.

Remote subscriber configuration

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

name

Remote Subscriber Location Domain

Location Domain Name

☐ Subnet ☒ DN List

Subnet IP address

Subnet mask

Certificate profile

Media profile

TLS mode

☒ Fallback TLS ☐ From HEADER ☒ Contact HEADER

Access Side Firewall Settings

☐ Enable Firewall Settings

Emergency configuration

Emergency numbers

5. The OSV must be configured to resolve the location to the DN of the emergency services.
 CMPconfiguration → OpenScape Voice → select OSV → select business group
 → emergency calling → add

[sbctest05] - [BG1] - Add Emergency Calling Entry

Entries of the OpenScape Voice emergency call solution.

General **LIN**

Identification

Here you can set all values which identify the Emergency Calling Subnet. Use a valid "Department", "Address/Subnet" combination, and/or "IPv6 Address/Subnet" and/or a valid "Location Domain". The "Address/Subnet" and "IPv6 Address/Subnet" must be entered in CIDR format.

Department: ...

Location Domain:

IPv4 Address/Subnet:

IPv6 Address/Subnet:

Description:

Branch Office: ...

Configuration

Here you can set all values for the general configuration for this specific Emergency Calling entry.

Send LIN instead of CPN: ☐

Digits to append:

These digits are appended to the 911 phone to define the DN of the EMSB

6. The OSV must be able to translate the new DN from the previous step 5 (above). Prefix access code

9111111	7 / 7	Off-net Access	Unknown	None
---------	-------	----------------	---------	------

7. Destination code

911	Unknown	Emergency	Service	Emergency
9111111	Unknown	NONE	New Code	15615597219

This could be the pilot number of an MLHG representing the EMSB

7. /etc/hosts in OSV must be configured to resolve the location to the SIPSM for the OSV.

In the example shown below the name br1.unify.com, which is the FQDN provisioned into the phones, is set to resolve to the SIPSM of the OSV (10.232.202.32)

```
# tail /etc/hosts
10.232.2.15      v5_ms_2_15.unify.com
10.232.2.15      Assistant2-15
10.232.63.94     rgtls.unify.com
10.232.65.102    unify-osv1
10.232.65.102    C-SBC-3550-B2.csbc.unify.com
10.232.202.32 br1.unify.com
10.232.65.102    osv.obsbc.com
```

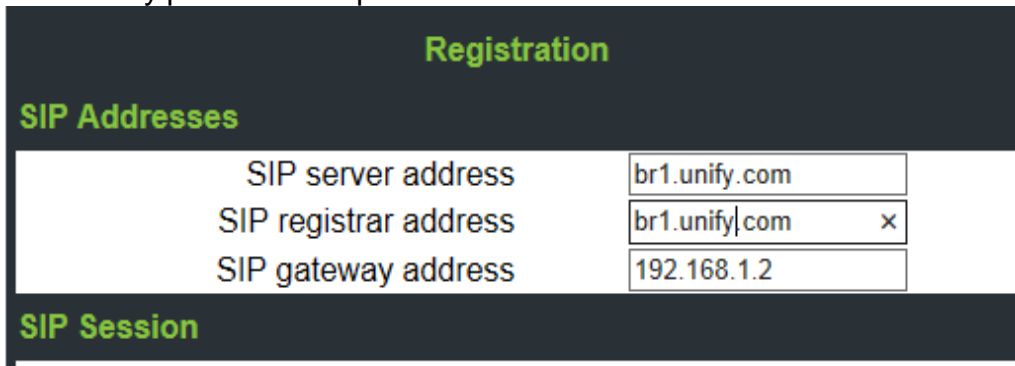
7. When the phone dials 911 the location information is passed in the INVITE to the OSS and on to the OSV.

```
⊕ Request-Line: INVITE sip:911@br1.siemens.com:5060;transport=tcp SIP/2.0
⊖ Message Header
⊕ Record-Route: <sip:166.20.100.50;transport=tcp;lr;ftag=fe17441dfb;otg=NM>
⊕ Via: SIP/2.0/TCP 166.20.100.50;branch=z9hG4bKe176.6b30ecf5.0;i=b77
⊕ Via: SIP/2.0/TCP 166.20.100.120;branch=z9hG4bK56ac54135b587b817
  Max-Forwards: 69
⊕ From: "15615597201" <sip:15615597201@br1.unify.com>;tag=fe17441dfb;epid=SC26aa1a
⊕ To: <sip:911@br1.unify.com> 5060>
  Call-ID: c28e7fb1e492c448
```

Manually provision the phone

This is a case where the DHCP option 120 is not supported either by the phone or the DHCP server.

1. Manually provision the phone with the desired "location."



The screenshot shows a configuration interface with a dark header labeled 'Registration'. Below the header is a section titled 'SIP Addresses' in green. It contains three rows of configuration fields:

SIP Addresses	
SIP server address	br1.unify.com
SIP registrar address	br1.unify.com x
SIP gateway address	192.168.1.2

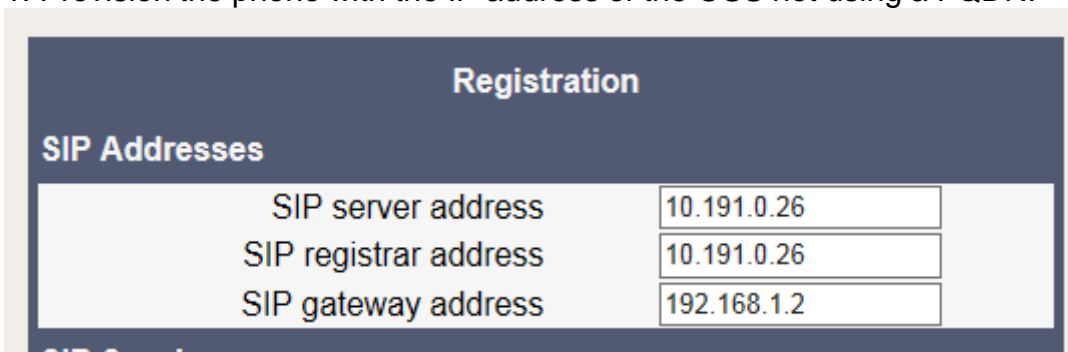
Below the 'SIP Addresses' section is another section titled 'SIP Session' in green.

2. Continue with step 3 of [Phone method #1: DHCP option 120](#)

Provision location in the OSS

In the case the finest granularity is the determined by the provisioning of the subnet in step 2.

1. Provision the phone with the IP address of the OSS not using a FQDN.



The screenshot shows a configuration interface with a dark header labeled 'Registration'. Below the header is a section titled 'SIP Addresses' in white. It contains three rows of configuration fields:

SIP Addresses	
SIP server address	10.191.0.26
SIP registrar address	10.191.0.26
SIP gateway address	192.168.1.2

Below the 'SIP Addresses' section is another section titled 'SIP Session' in white.

2. On the OSS provision the desired “Location Domain Name”. Also define the desired IP address and subnet this “Location domain Name” is used for.

Remote subscriber configuration

Remote Subscriber Location Domain

Location Domain Name remote.user.labdq

☐ Subnet ☒ DN List

Subnet IP address 173.16.4.1

Subnet mask 255.255.0.0

Certificate profile OSV Solution

Media profile webrtc_default

TLS mode

☒ Fallback TLS ☐ From HEADER ☒ Contact HEADER

75675678

Access Side Firewall Settings

☐ Enable Firewall Settings **Firewall Settings**

Emergency configuration

Emergency numbers

Emergency call routing

3. When the phone makes a 911 call the OSS will add the location information by adding a “X-Siemens-Location” header before forwarding the INVITE to the OSV.


```

+ Request-Line: INVITE sip:911@10.232.202.32:5060;transport=tcp SIP/2.0
+ Message Header
+ Record-Route: <sip:10.232.63.72:5060;transport=tcp;oss=oss-08.00.02.00>
+ Via: SIP/2.0/TCP 10.232.63.72;branch=z9hG4bK6cc9.837b2d9e17a55c30297f7
+ Via: SIP/2.0/TCP 10.232.63.72:10000;rport=55272;branch=z9hG4bK0ad1e5b7
  Max-Forwards: 69
+ Contact: "15615597208"<sip:15615597208@10.232.63.72:10000;transport=tcp>
+ To: <sip:911@10.232.202.32:5060>
+ From: "15615597208"<sip:15615597208@10.232.63.72:10000>;tag=fc84c5d9ff
  Call-ID: 697f59ef415def31
+ CSeq: 1073789421 INVITE
  Allow: INVITE, ACK, CANCEL, BYE, REFER, NOTIFY, UPDATE
  Content-Type: application/sdp
  Supported: replaces, 100rel
  User-Agent: OpenStage_80_V3 R1.44.2      SIP 130723
  Allow-Events: hold
+ X-Siemens-Location: remotes.com ←
  Content-Length: 356

```

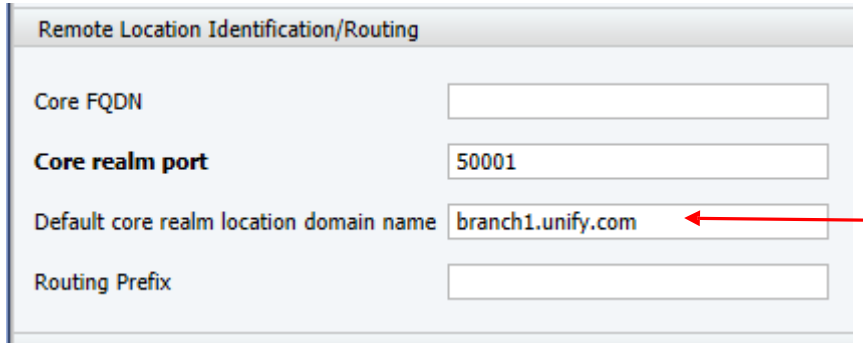
4. Continue with step 4 of [Using DHCP option 120](#)



E911 can determine location domain from either **X-Siemens-Location** header or **From** header. OSV cannot be configured to explicitly use one header or the other for determining location domain, it will always look up to both with the aforementioned order.

Setting Location of “branch subscribers” for emergency calls

GUI> Features> Remote Endpoints configuration> add/edit> Default core realm location domain name



Remote Location Identification/Routing

Core FQDN	<input type="text"/>
Core realm port	<input type="text" value="50001"/>
Default core realm location domain name	<input type="text" value="branch1.unify.com"/> ←
Routing Prefix	<input type="text"/>

With this configured, it works much like [Provision location in the OSS](#) for these branch subscribers

18 Single-Armed-OS SBC

In Single armed configuration, the OS SBC's LAN and WAN interfaces are connected to the same IP subnet instead of being connected between two different IP networks or subnets. It is also desirable for both the LAN and WAN connection of OS SBC to use a single physical Ethernet interface, rather than two.

The screenshot shows the 'USB Stick Setup' window. The 'Media Select' dropdown is set to 'E:\ (7.26 GB)' with a 'Refresh' button. A warning message states: 'WARNING: all data of the removable media will be erased.' Under 'Installation Method', 'Generate node.cfg file' is selected. Below this, 'Automated' is checked, and 'Single Armed SBC' is checked. The 'SBC Network Configuration' section has 'Hardware type' as a dropdown, 'Hostname' as 'One-Armed', and 'Interface' as 'WAN Interface'. The 'Disable interface' checkbox is unchecked. The IPv4 address is '10 . 232 . 63 . 94', the IPv4 netmask is '255 . 255 . 255 . 0', and the IPv4 gateway is '10 . 232 . 63 . 1'. There are empty fields for IPv6 address, netmask, and gateway. Below these are fields for 'Logical ID', 'CMP URL 1', 'CMP URL 2', 'DNS 1', and 'DNS 2'. At the bottom, there is a 'Change Branding Names and Logo' button, a 'Partitioned USB Stick' checkbox, and 'OK' and 'Cancel' buttons.

When “single Armed SBC” is selected the default is to create the LAN and WAN with the same IP address.

The “Single Armed SBC requires the use of an external firewall working in NAT mode.

This is the arrangement of the core and access realm after booting with a USB stick configured for “single armed”

☒ Single armed

☐ Interface bonding

Interface Configuration

Core realm configuration

AddDelete

Type	Network ID	Interface	IP address	Subnet mask	VLAN tag	Signaling	Media	SIP-UDP	SIP-TCP	SIP-TLS	MGCP
Main IPv4	Main-Core-IPv4	eth0	10.232.63.94	255.255.255.0	0	true	true	5060	5060	5061	2427

Note: The IP address of the core and access realms are the same. The ports for the access realm are unique. Also note the type is set to “SA Main IPv4”.

Access and Admin realm configuration

AddDelete

Type	Network ID	Interface	IP address	Subnet mask	VLAN tag	Signaling	Media	SIP-UDP	SIP-TCP	SIP-TLS	SIP-MTLS	MGCP	SIP server	Message rate
SA Main IPv4	Main-Access-IPv4	eth0	10.232.63.94	255.255.255.0	0	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	65060	65060	65061	65161	2727	Node 1	

Note: devices communicating with the access realm must use the correct port.

Network/Net Services

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

SettingsDNSNTPTraffic ShapingQoS

Interface Configuration

Core realm configuration

AddDelete

Type	Network ID	Interface	IP address	Subnet mask	VLAN tag	Signaling	Media	SIP-UDP	SIP-TCP	SIP-TLS	MGCP
Main IPv4	Main-Core-IPv4	eth0	10.232.63.94	255.255.255.0	0	true	true	5060	5060	5061	2427

Additional access realm may be added.
Note: The different selection of “types” from the normal “multi-arm” OS SBC.

Access and Admin realm configuration

AddDelete

Type	Network ID	Interface	IP address	Subnet mask	VLAN tag	Signaling	Media	SIP-UDP	SIP-TCP	SIP-TLS	SIP-MTLS	MGCP	SIP server	Message rate
SA Main IPv4	Main-Access-IPv4	eth0	10.232.63.94	255.255.255.0	0	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	65060	65060	65061	65161	2727	Node 1	
SA Main IPv6														
Non-VLAN IP														
VLAN IP														

Each additional external realm requires the configuration of an external firewall working in the NAT mode.

Normal configuration, using realm profiles, may continue from here.

19 SIP Connect 1.1

The SIP Connect 1.1 specification describes two modes of operation; the **Registration mode** and the **Static mode**.

These modes differ primarily in the way the Service Provider Network discovers the SIP signaling address of the SIP-PBX.

19.4 Registration Mode

Under **Remote Endpoints/Configure** add the **Service Provider Profiles**. Select in **Default SSP Profile** the option **DTAG/NGN Registration Mode**. Selecting this option, the flag **Registration required** will be activated. It is necessary to configure the Digest Authentication. The flag **Digest authentication supported** flag is also activated.

In the Sip Connect the following flags are activated: **Send user=phone in SIP URI, Registration mode, 1TR118**.

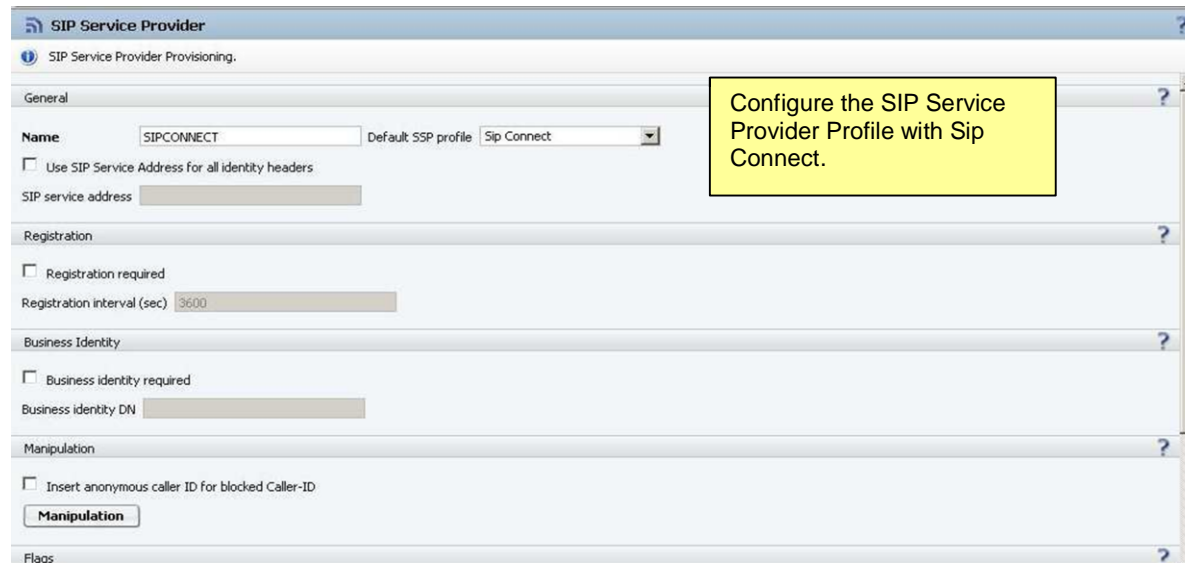
19.5 Static Mode

The Static mode is often used for larger Enterprises, where the size of the Enterprise warrants more explicit provisioning of connection and service information by the Service Provider. For example, large Enterprise trunks often have unique requirements for SLAs (Service Level Agreements), call routing, load balancing, codec support, etc., which make explicit provisioning necessary.

In the Static mode, the Service Provider Network views the SIP-PBX as a peer SIP-based network that is responsible for the Enterprise Public Identities that it serves. In this mode the Service Provider Network is either configured with the SIP-PBX signaling address, or it discovers the address using the Domain Name Service (DNS).

The Service Provider Network procedures for routing out-of-dialog requests to the SIP-PBX align closely with the SIP routing procedures defined in [RFC 3261] (and [RFC3263] if DNS is used). In Static mode the Enterprise Network can use DNS to advertise its publicly-reachable SIP-PBX SIP signaling address to the SP-SSE.

SIP Connect Configuration



The screenshot shows the 'SIP Service Provider' configuration window. The title bar reads 'SIP Service Provider'. Below the title bar, there is a status bar that says 'SIP Service Provider Provisioning.' The main configuration area is divided into several sections: 'General', 'Registration', 'Business Identity', 'Manipulation', and 'Flags'. In the 'General' section, the 'Name' field is set to 'SIPCONNECT', and the 'Default SSP profile' dropdown is set to 'Sip Connect'. There is a checkbox for 'Use SIP Service Address for all identity headers' which is unchecked. The 'SIP service address' field is empty. In the 'Registration' section, there is a checkbox for 'Registration required' which is unchecked, and the 'Registration interval (sec)' is set to '3600'. In the 'Business Identity' section, there is a checkbox for 'Business identity required' which is unchecked, and the 'Business identity DN' field is empty. In the 'Manipulation' section, there is a checkbox for 'Insert anonymous caller ID for blocked Caller-ID' which is unchecked, and a button labeled 'Manipulation'. In the 'Flags' section, there is a button labeled 'Flags'. A yellow callout box with a black border is positioned over the 'General' section, containing the text: 'Configure the SIP Service Provider Profile with Sip Connect.'

SIP Service Provider

SIP Service Provider Provisioning.

General

Name: SIPCONNECT Default SSP profile: Sip Connect

☐ Use SIP Service Address for all identity headers

SIP service address:

Registration

☐ Registration required

Registration interval (sec): 3600

Business Identity

☐ Business identity required

Business identity DN:

Manipulation

☐ Insert anonymous caller ID for blocked Caller-ID

Manipulation

Flags

Selects the flags in Sip Connect option in SIP Service Provider profile

Sip Connect

☐ Use tel URI

☐ Send user=phone in SIP URI

Use Tel URI - When the SIP-SP requires the use of tel URIs the user must check this check box. The SBC shall convert all SIP URIs to Tel URIs towards the SIP-SP and vice versa.

Send user=phone in SIP URI - When checked, the SBC adds “user=phone” in SIP URIs towards SIP-SP.

Remote Endpoints

Remote Endpoints provisioning.

Service Provider Profiles

Add Edit Delete

Row	Name	Registration required	Registration interval
1	SIPCONNECT	<input type="checkbox"/>	3600

After configured the Service Provider profile associated it in the Remote Endpoint Configuration.

Remote Endpoints configuration

Add Edit Delete

Row	Name	Access realm profile	Type	Profile / Circuit ID	Remote IP address / Logical-Endpoint-ID / Circuit URL	Remote port	Remote transport	Associated EP	Core realm profile
1	acur1h038	Main-Access-Realm - ipv6	Proxy	Default Proxy	fd43::38	5061	TLS		Main-Core-Realm - ipv6
2	acur1h138_MS	Main-Access-Realm - ipv6	MediaServer	MS_profile	fd43::38	2427	UDP	acur1h038	Main-Core-Realm - ipv6
3	SIPCONNECT	Main-Access-Realm - ipv4	SSP	SIPCONNECT	10.10.0.200	5060	TCP		Main-Core-Realm - ipv4

INFO: In order to be SIP Connect 1.1 compliant the certificates presented by the OS SBC shall use a SIP URI in the subjectAltName and Common Name fields, in accordance with [RFC 5280]. The OSV Solution recommended way to create certificates is to use OpenSSL where it shall be possible to specify the above fields using a SIP URI.OS-SBC Access or Outside Network Interface:

20 UCaaS Functionality

UCaaS, which stands for **Unified Communications as a Service**, integrates this communication through a cloud model, as well as integrating with cloud-based software applications.

20.4 Support Cascaded SBC configuration

20.4.9 Standalone mode

20.4.9.1 OSCloud Trunk SBC configuration

OSCloud trunk SBC should be configured to access standalone SBC. For Openscape Cloud the standalone SBC is a remote endpoint of type and profile as SBC.

SBC250upgrade - Remote endpoint configuration - Mozilla Firefox

https://10.10.170.112/remoteEndpointConfiguration.html?name=On_premise&status=false&standalone=false

Remote endpoint configuration

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

Remote Endpoint Settings

Name: On_premise [Edit]

Type: SBC

Profile: SBC

Access realm profile: Main-Access-Realm - ipv4

Core realm profile: Main-Core-Realm - ipv4

Associated Endpoint:

☐ Enable Call Limits

Maximum Permitted Calls: 0

Reserved Calls: 0

Remote Location Information

☐ URI based routing

☐ Enable access control

Signaling address type: IP address or FQDN

Remote Location domain list

Row	Remote URL	Remote port	Remote transport	Media IP	Media profile	TLS mode	Certificate profile	TLS keep-alive	Keep-alive interval (seconds)	Keep-Alive timeout (sec)
1	192.168.110.60	5060	TCP		default	Server authentication	OSV Solution	<input checked="" type="checkbox"/>	120	10

Remote Location Identification/Routing

Core FQDN:

Core realm port: 50011

Default core realm location domain name:

Routing prefix:

[OK] [Cancel]

Trunk SBC of OSCloud

In OSV the configuration is as any other regular SBC the SIP port just have to match the core port of remote endpoint configured in the TRUNK-SBC corresponding to the Stand Alone SBC.

The screenshot shows the 'Edit Endpoint: Trunk_onpremise' configuration window in the OpenScape SBC V10 management portal. The window is titled '[grp1019] - [Circuit] - [Main Office] - Edit Endpoint: Trunk_onpremise' and is running in Mozilla Firefox. The URL is 'https://10.10.153.2/management/portal/Applications/Operation/OSV/BusinessGroup/Members/PopUps/modifyBGEndpoint.psm?callPoi'. The 'SIP' tab is selected, showing the following configuration options:

- 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: 10.10.170.112
 - Port:** 50011 (highlighted with a red rectangle)
 - Transport protocol: MTLS
 - Endpoint does not accept incoming TLS connections: ☐
 - SRTP media mode: Enabled
 - ANAT Support: Enabled

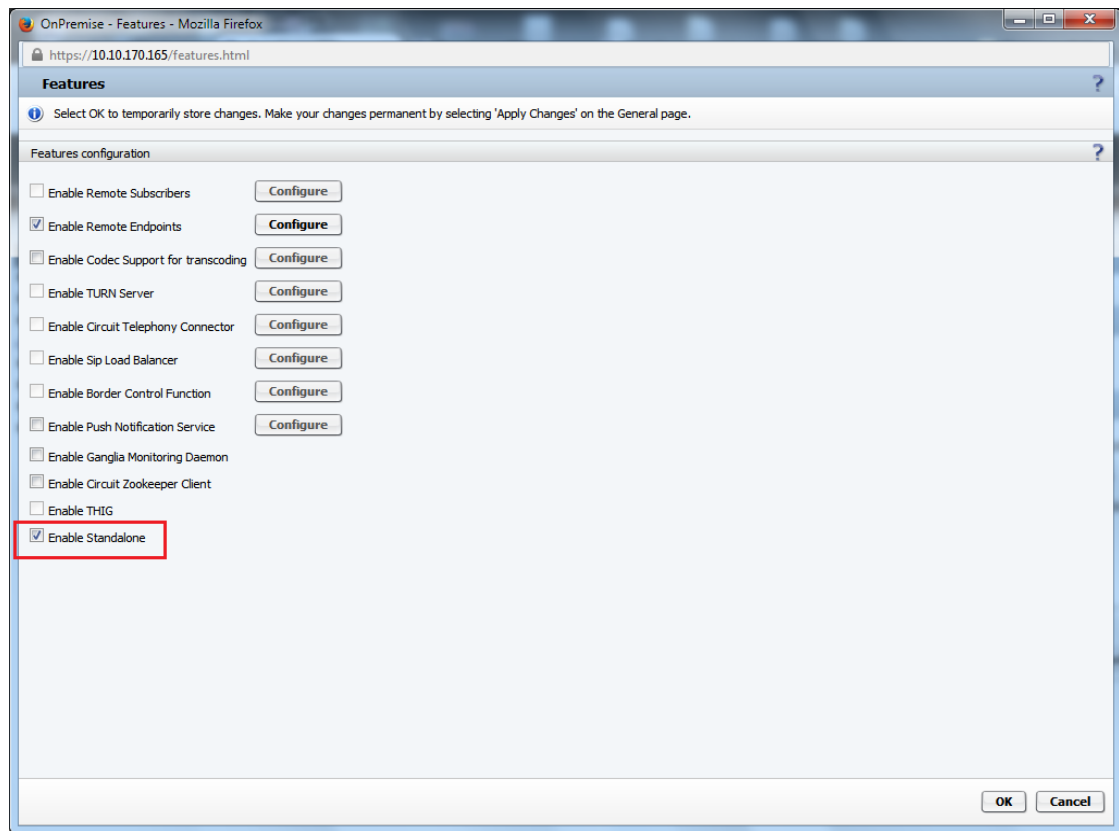
At the bottom right, there are 'Save' and 'Cancel' buttons.

Endpoint configuration of the OSV

20.4.10 Standalone SBC Configuration

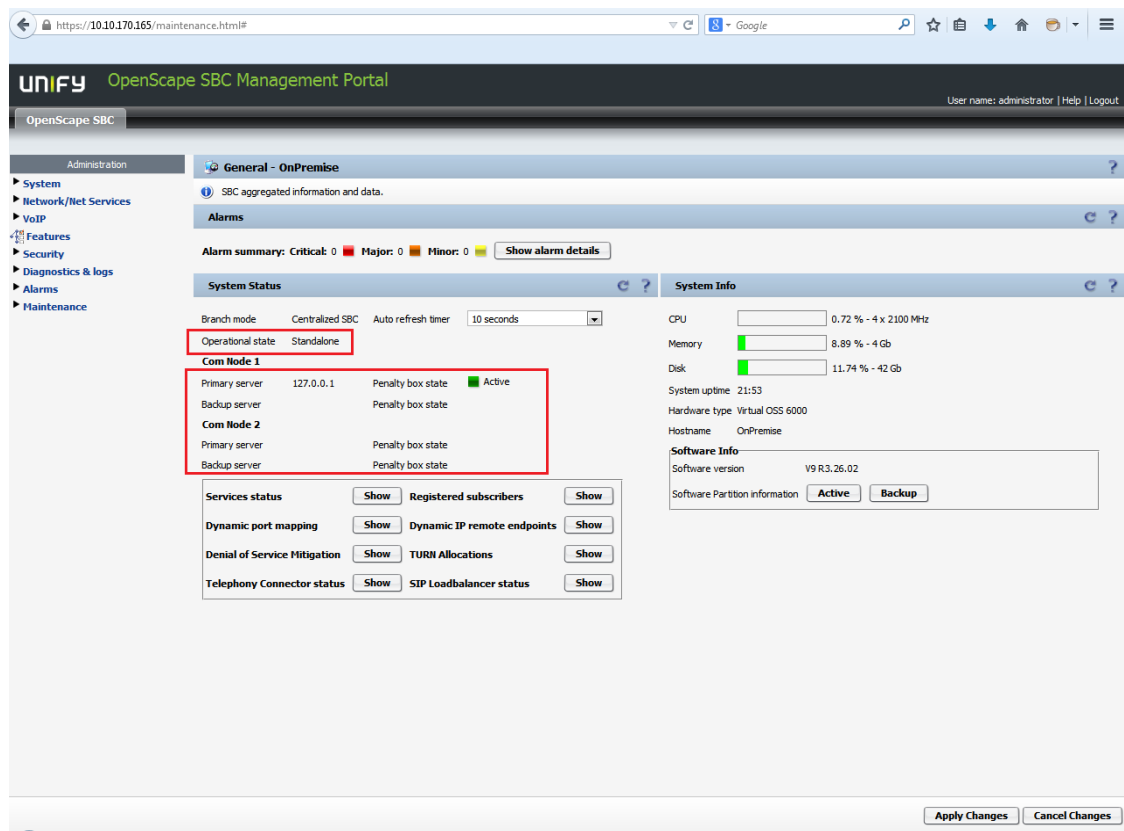
The SBC standalone mode is configurable in the "Features" windows as indicated below. Once the flag is set the following buttons became grayed out: Enable Remote Subscribers, Enable Turn Server, or Enable Sip Load Balancer and Enabled Border control function. In the same way the

Standalone Flag is grayed out if one of the previous mentioned flags is enabled.



Enable Standalone functionality of SBC

Once the flag is enable and the configuration is applied the Sip Server tab became empty and the dashboard will show in Operational mode the "Standalone". The Primary server is set to 127.0.0.1 and state should be green.



Standalone SBC dashboard

The remote endpoint configuration is changed to allow a remote endpoint of SSP type by linked to another endpoint of SSP type.
Create SSP profile.

OnPremise - SIP Service Provider Profile - Mozilla Firefox

https://10.10.170.165/serviceProvider.html?mode=csbc&name=ssp

SIP Service Provider Profile

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

General

Name: Default SSP profile:

☐ Use SIP Service Address for all identity headers

SIP service address:

SIP User Agent

SIP User Agent towards SSP: SIP User Agent:

Registration

☐ Registration required

Registration interval (sec):

Business Identity

☐ Business identity required

Business identity DN:

Outgoing SIP manipulation

☐ Insert anonymous caller ID for blocked Caller-ID

Manipulation

Incoming SIP manipulation

Calling Party Number:

Flags

OK Cancel

SBC Sip Service Provider Profile

“Linked endpoint” is used to identify that the endpoint is linked to another endpoint as the final destination. Link both trunks as below.

OnPremise - Remote Endpoints - Mozilla Firefox
 https://10.10.170.165/remoteEndpoints.html?status=false&standalone=true

Remote Endpoints

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

SIP Service Provider Profile

Hostname:
 Remote directory:
 User name:
 Password:

Row	Name	Registration required	Registration interval (sec)
1	ssp	<input type="checkbox"/>	3600

Remote endpoint configuration

Row	Name	Access realm profile	Type	Profile / Circuit ID	Remote IP address / Logical-Endpoint-ID / Circuit URL	Remote port	Remote transport	Associated Endpoint	Linked Endpoint	Cc
1	Trunk1	Main-Access-Realm - ipv4	SBC	SBC	192.168.110.6	5060	TCP		Trunk2	Main
2	Trunk2	Main-Access-Realm - ipv4	SSP	ssp	192.168.110.50	5060	TCP		Trunk1	Main

Media Server Profiles

Please note that the above configuration applies when standalone on premise SBC is connected to SSP through a SBC.
 If branch or gateway is used, SSP linked to a gateway behind a branch will have the branch as associated endpoint and the gateway as linked endpoint.

20.4.11 Cascaded SBC mode

20.4.12 OSCloud Trunk SBC configuration

OSCloud trunk SBC should be configured to access Cascaded SBC. For Openscape Cloud the Cascaded SBC is a remote endpoint of type and profile as SBC.

Remote endpoint configuration

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

Remote Endpoint Settings

Name: On_premise [Edit]

Type: SBC

Profile: SBC

Access realm profile: Main-Access-Realm - ipv4

Core realm profile: Main-Core-Realm - ipv4

Associated Endpoint:

☐ Enable Call Limits

Maximum Permitted Calls: 0

Reserved Calls: 0

Remote Location Information

☐ URI based routing

☐ Enable access control

Signaling address type: IP address or FQDN

Remote Location domain list

Row	Remote URL	Remote port	Remote transport	Media IP	Media profile	TLS mode	Certificate profile	TLS keep-alive	Keep-alive interval (seconds)	Keep-Alive timeout (sec)
1	192.168.110.60	5060	TCP		default	Server authentication	OSV Solution	<input type="checkbox"/>	120	10

Remote Location Identification/Routing

Core FQDN:

Core realm port: 50011

Default core realm location domain name:

Routing prefix:

OK Cancel

Trunk SBC of OSCloud

In OSV the configuration is as any other regular SBC the SIP port just have to match the core port of remote endpoint configured in the TRUNK-SBC corresponding to the Cascaded SBC.

The screenshot shows a web browser window with the URL `https://10.10.153.2/management/portal/Applications/Operation/OSV/BusinessGroup/Members/PopUps/modifyBGEndpoint.psml?callPoi`. The page title is "[grp1019] - [Circuit] - [Main Office] - Edit Endpoint : Trunk_onpremise". The interface has several tabs: General, SIP, Attributes, Aliases, Routes, and Accounting. The "SIP" tab is selected.

Under the "Endpoint Type" section, there are three radio buttons: "SIP Private Networking:" (unselected), "SIP Trunking:" (selected), and "SIP-Q Signaling:" (unselected).

The "SIP Signaling" section contains a note: "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."

Below the note, there are several configuration fields:

- Type: Static (dropdown)
- Signaling Address Type: IP Address or FQDN (dropdown)
- Endpoint Address: 10.10.170.112 (text input)
- Port: 50011 (text input, highlighted with a red box)**
- Transport protocol: MTLS (dropdown)
- Endpoint does not accept incoming TLS connections: ☐
- SRTP media mode: Enabled (dropdown)
- ANAT Support: Enabled (dropdown)

At the bottom right, there are "Save" and "Cancel" buttons.

Endpoint configuration of the OSV

20.4.13 Cascaded SBC configuration

The Cascaded SBC mode is configurable as regular sbc on customer's PBX side. Sip server should be configured in "sip server settings" to match customer sipsm of the PBX.

Communication system type should be Active-Standby and the register port 5060.

OnPremise - VOIP - Mozilla Firefox

https://10.10.170.165/voip.html?tabId=sipTab

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** **Media** **QoS Monitoring**

General

Comm System Type: Active-Standby

☐ Allow Register from SERVER

Other trusted servers

Node 1

Target type: Binding

Primary server: 10.10.32.116 Transport: TCP Port: 5060

Backup server: Transport: TCP Port:

SRV record: Transport: TCP

Node 2

Target type: Binding

Primary server: 10.10.32.126 Transport: TCP Port: 5060

Backup server: Transport: TCP Port:

SRV record: Transport: TCP

Timers and Thresholds

Failure threshold (pings): 2 **OPTIONS interval (sec)**: 60

Success threshold (pings): 1 **OPTIONS timeout (sec)**: 4

OK Cancel

Primary server is set to customer sipSMS active and standby, and the state should be green.

The screenshot shows the OpenScope SBC Management Portal interface. The left sidebar contains navigation links for Administration, System, Network/Net Services, VoIP, SIP Server Settings, Port and Signaling Settings, Media, QoS Monitoring, Features, Security, Diagnostics & logs, Alarms, and Maintenance. The main content area is titled 'General - OnPremise' and includes an 'Alarms' section with a summary (Critical: 0, Major: 0, Minor: 0) and a 'Show alarm details' button. Below this is the 'System Status' section, which includes a 'Branch mode' dropdown set to 'Centralized SBC' and an 'Auto refresh timer' set to '10 seconds'. Two red boxes highlight the 'Com Node 1' and 'Com Node 2' sections. 'Com Node 1' shows a primary server at 10.10.32.116 and a backup server, both with 'Penalty box state' set to 'Active'. 'Com Node 2' shows a primary server at 10.10.32.126 and a backup server, also with 'Penalty box state' set to 'Active'. To the right of the system status is the 'System Info' section, which displays CPU usage (0.84%), Memory usage (10.35%), Disk usage (11.76%), System uptime (5 days 1:23), Hardware type (Virtual OSS 6000), and Hostname (OnPremise). Below this is the 'Software Info' section, showing the software version (V9 R3.26.02) and software partition information (Active, Backup). At the bottom right of the page are 'Apply Changes' and 'Cancel Changes' buttons.

The remote endpoint configuration is changed to allow a remote endpoint of SSP type by connected to endpoint of TRUNK-SBC. Create default SSP profile and select “Cascaded SBC” from drop down menu. This profile will set as default outbound proxy port and registrar server port to 5060 in remote endpoint.

OnPremise - SIP Service Provider Profile - Mozilla Firefox

https://10.10.170.165/serviceProvider.html?mode=csbc&name=ssp1

SIP Service Provider Profile

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

General

Name: Default SSP profile:

☐ Use SIP Service Address for all identity headers

SIP service address:

SIP User Agent

SIP User Agent towards SSP: SIP User Agent:

Registration

☐ Registration required

Registration interval (sec):

Business Identity

☐ Business identity required

Business identity DN:

Outgoing SIP manipulation

☐ Insert anonymous caller ID for blocked Caller-ID

Manipulation

Incoming SIP manipulation

Calling Party Number:

Flags

OK Cancel

Create endpoint, select type SSP and assign the default ssp profile. Match the core port of remote endpoint configured in the customer PBX corresponding to the Cascaded SBC.

OnPremise - Remote endpoint configuration - Mozilla Firefox
 https://10.10.170.165/remotepointConfiguration.html?name=Trunk1&status=false&standalone=false

Remote endpoint configuration

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

Remote Endpoint Settings

Name: Trunk1 Edit

Type: SSP ▼

Profile: ssp ▼

Access realm profile: Main-Access-Realm - ipv4 ▼

Core realm profile: Main-Core-Realm - ipv4 ▼

Associated Endpoint: ▼

☐ Enable Call Limits

Maximum Permitted Calls: 0

Reserved Calls: 0

Remote Location Information

☐ URI based routing

☐ Enable access control

Signaling address type: IP address or FQDN ▼

Remote Location domain list

Add Edit Delete

Row	Remote URL	Remote port	Remote transport	Media IP	Media profile	TLS mode	Certificate profile	TLS keep-alive	Keep-alive interval (seconds)	Keep-Alive timeout (sec)	INV
1	192.168.110.6	5060	TCP		default	Server authentication	OSV Solution	<input type="checkbox"/>	120	10	

Remote Location Identification/Routing

Core FQDN:

Core realm port: 50011

Default core realm location domain name:

Routing prefix:

OK Cancel

The screenshot shows a web browser window with the address bar displaying `https://10.10.32.34/management/portal/Applications/Operation/OSV/BusinessGroup/Members/PopUps/modifyBGE`. The page title is "[GRP103C] - [athens] - [Main Office] - Edit Endpoint : On_Premise_mode". The interface has several tabs: General, SIP, Attributes, Aliases, Routes, and Accounting. The 'SIP' tab is active.

Under the 'Endpoint Type' section, there are three radio buttons: 'SIP Private Networking' (unselected), 'SIP Trunking' (selected), and 'SIP-Q Signaling' (unselected).

The 'SIP Signaling' section contains a note: "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."

Below the note, there are several configuration fields:

- Type:** A dropdown menu set to 'Static'.
- Signaling Address Type:** A dropdown menu set to 'IP Address or FQDN'.
- Endpoint Address:** A text input field containing '10.10.170.165'.
- Port:** A text input field containing '50011', which is highlighted with a red rectangular box.
- Transport protocol:** A dropdown menu set to 'TCP'.
- Endpoint does not accept incoming TLS connections:** An unchecked checkbox.
- SRTP media mode:** A dropdown menu set to 'Enabled'.
- ANAT Support:** A dropdown menu set to 'Enabled'.

At the bottom right of the form, there are two buttons: 'Save' and 'Cancel'.

Please note that the above configuration applies when Cascaded SBC is connected to SSP through a SBC and the customer's PBX is an OSV.

20.5 Support SBC on Premise configuration

20.5.9 Standalone mode

20.5.9.1 OSCloud Trunk SBC configuration

OSCloud trunk SBC should be configured to access standalone SBC. For Openscape Cloud the standalone SBC is a remote endpoint of type and profile as SBC.

Remote endpoint configuration

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

Remote Endpoint Settings

Name: On_premise [Edit]

Type: SBC

Profile: SBC

Access realm profile: Main-Access-Realm - ipv4

Core realm profile: Main-Core-Realm - ipv4

Associated Endpoint: [Select]

☐ Enable Call Limits

Maximum Permitted Calls: [0]

Reserved Calls: [0]

Remote Location Information

☐ URI based routing

☐ Enable access control

Signaling address type: IP address or FQDN

Remote Location domain list

Row	Remote URL	Remote port	Remote transport	Media IP	Media profile	TLS mode	Certificate profile	TLS keep-alive	Keep-alive interval (seconds)	Keep-Alive timeout (sec)
1	192.168.110.60	5060	TCP		default	Server authentication	OSV Solution	<input type="checkbox"/>	120	10

Remote Location Identification/Routing

Core FQDN: []

Core realm port: 50011

Default core realm location domain name: []

Routing prefix: []

[OK] [Cancel]

Trunk SBC of OSCloud

In OSV the configuration is as any other regular SBC the SIP port just have to match the core port of remote endpoint configured in the TRUNK-SBC corresponding to the Stand Alone SBC.

[grp1019] - [Circuit] - [Main Office] - Edit Endpoint: Trunk_onpremise - Mozilla Firefox

https://10.10.153.2/management/portal/Applications/Operation/OSV/BusinessGroup/Members/PopUps/modifyBGEndpoint.psm?callPoi

[grp1019] - [Circuit] - [Main Office] - Edit Endpoint : Trunk_onpremise

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: 10.10.170.112

Port: 50011

Transport protocol: MTLS

Endpoint does not accept incoming TLS connections: ☐

SRTP media mode: Enabled

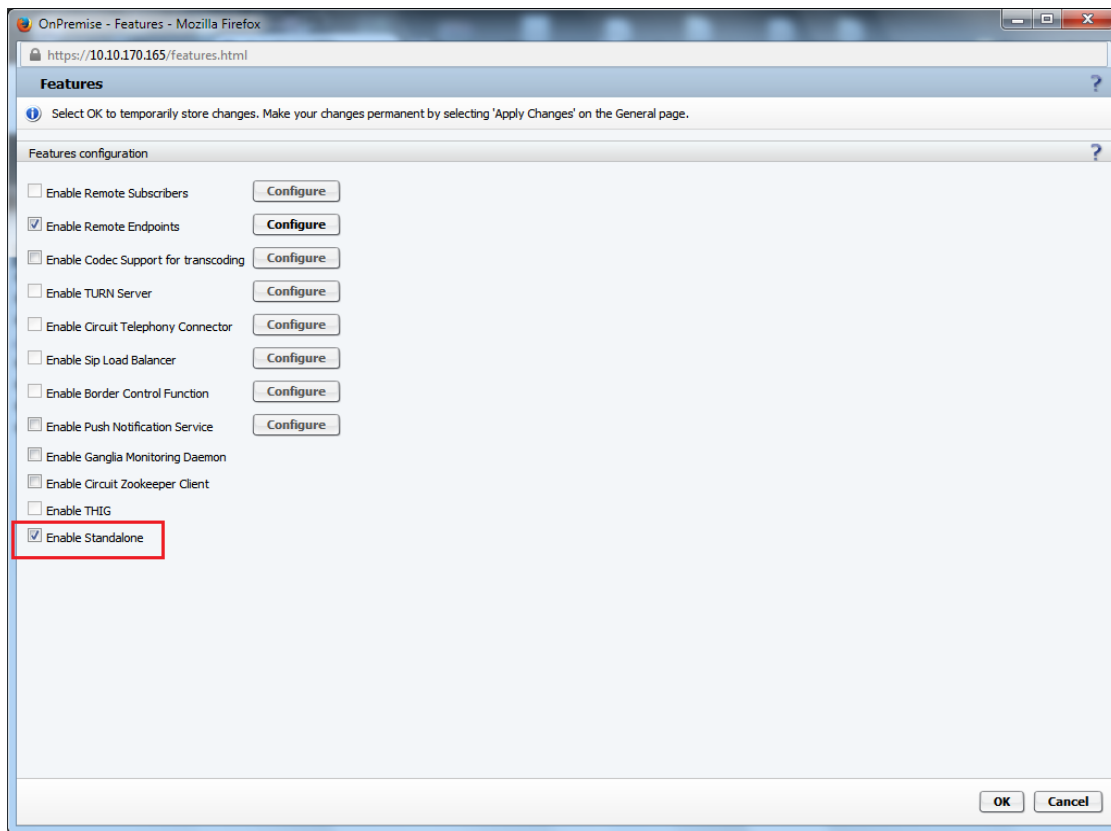
ANAT Support: Enabled

Save Cancel

Endpoint configuration of the OSV

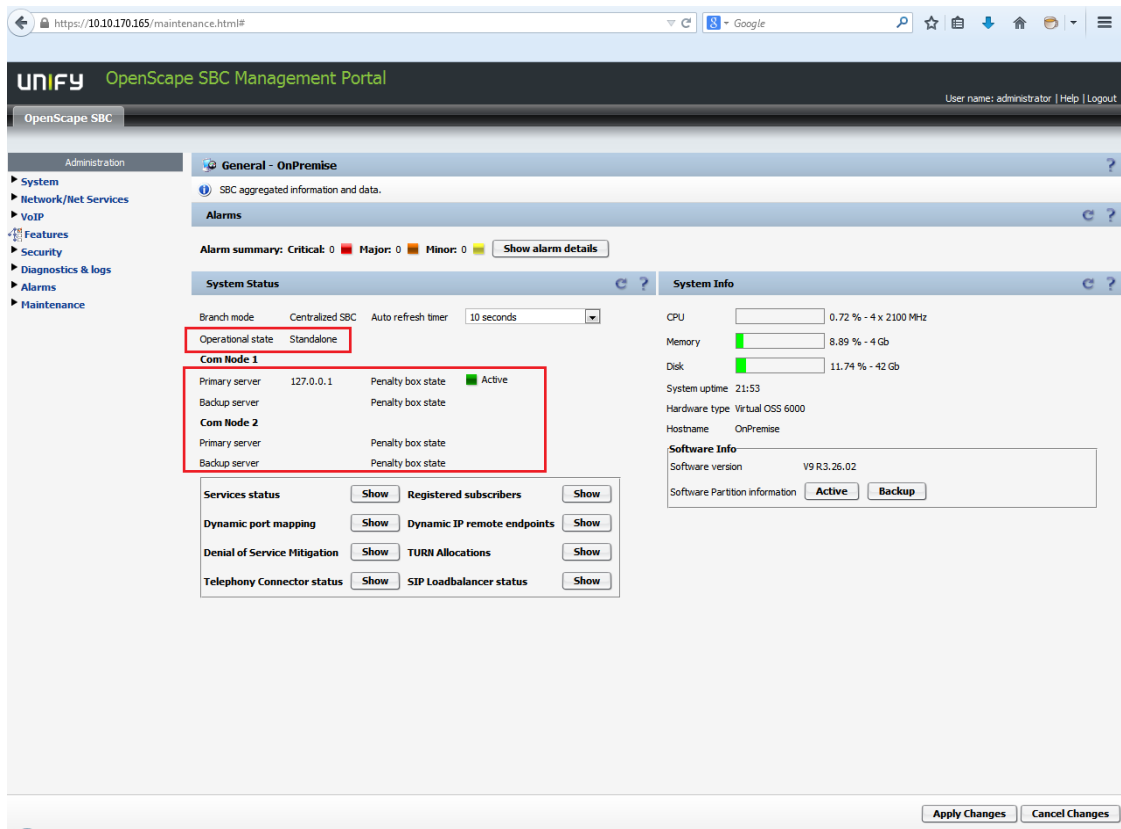
20.5.9.2 Standalone SBC Configuration

The SBC standalone mode is configurable in the "Features" windows as indicated below. Once the flag is set the following buttons became grayed out: Enable Remote Subscribers, Enable Turn Server, or Enable Sip Load Balancer and Enabled Border control function. In the same way the Standalone Flag is grayed out if one of the previous mentioned flags is enabled.



Enable Standalone functionality of SBC

Once the flag is enable and the configuration is applied the Sip Server tab became empty and the dashboard will show in Operational mode the "Standalone". The Primary server is set to 127.0.0.1 and state should be green.



Standalone SBC dashboard

The remote endpoint configuration is changed to allow a remote endpoint of SSP type by linked to another endpoint of SSP type.

Create SSP profile.

OnPremise - SIP Service Provider Profile - Mozilla Firefox

https://10.10.170.165/serviceProvider.html?mode=csbc&name=ssp

SIP Service Provider Profile

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

General

Name: Default SSP profile:

☐ Use SIP Service Address for all identity headers

SIP service address:

SIP User Agent

SIP User Agent towards SSP: SIP User Agent:

Registration

☐ Registration required

Registration interval (sec):

Business Identity

☐ Business identity required

Business identity DN:

Outgoing SIP manipulation

☐ Insert anonymous caller ID for blocked Caller-ID

Manipulation

Incoming SIP manipulation

Calling Party Number:

Flags

OK Cancel

SBC Sip Service Provider Profile

“Linked endpoint” is used to identify that the endpoint is linked to another endpoint as the final destination. Link both trunks as below.

OnPremise - Remote Endpoints - Mozilla Firefox
 https://10.10.170.165/remotEndpoints.html?status=false&standalone=true

Remote Endpoints

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

SIP Service Provider Profile

Hostname:
 Remote directory:
 User name:
 Password:

Row	Name	Registration required	Registration interval (sec)
1	ssp	<input type="checkbox"/>	3600

Remote endpoint configuration

Row	Name	Access realm profile	Type	Profile / Circuit ID	Remote IP address / Logical-Endpoint-ID / Circuit URL	Remote port	Remote transport	Associated Endpoint	Linked Endpoint
1	Trunk1	Main-Access-Realm - ipv4	SBC	SBC	192.168.110.6	5060	TCP		Trunk2
2	Trunk2	Main-Access-Realm - ipv4	SSP	ssp	192.168.110.50	5060	TCP		Trunk1

Media Server Profiles

OK Cancel

Please note that the above configuration applies when standalone on premise SBC is connected to SSP through a SBC.

If branch or gateway is used, SSP linked to a gateway behind a branch will have the branch as associated endpoint and the gateway as linked endpoint.

20.5.10 On premise SBC mode

20.5.10.1 OSCloud Trunk SBC configuration

OSCloud trunk SBC should be configured to access onpremise SBC. For Openscape Cloud the on premise SBC is a remote endpoint of type and profile as SBC.

Remote endpoint configuration - Mozilla Firefox

https://10.10.170.112/remotepointConfiguration.html?name=On_premise&status=false&standalone=false

Remote endpoint configuration

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

Remote Endpoint Settings

Name: On_premise [Edit]

Type: SBC

Profile: SBC

Access realm profile: Main-Access-Realm - ipv4

Core realm profile: Main-Core-Realm - ipv4

Associated Endpoint: [Empty]

☐ Enable Call Limits

Maximum Permitted Calls: [Empty]

Reserved Calls: [Empty]

Remote Location Information

☐ URI based routing

☐ Enable access control

Signaling address type: IP address or FQDN

Remote Location domain list

Row	Remote URL	Remote port	Remote transport	Media IP	Media profile	TLS mode	Certificate profile	TLS keep-alive	Keep-alive interval (seconds)	Keep-Alive timeout (sec)
1	192.168.110.60	5060	TCP		default	Server authentication	OSV Solution	<input type="checkbox"/>	120	10

Remote Location Identification/Routing

Core FQDN: [Empty]

Core realm port: 50011

Default core realm location domain name: [Empty]

Routing prefix: [Empty]

[OK] [Cancel]

Trunk SBC of OSCloud

In OSV the configuration is as any other regular SBC the SIP port just have to match the core port of remote endpoint configured in the TRUNK-SBC corresponding to the on premise SBC.

[grp1019] - [Circuit] - [Main Office] - Edit Endpoint: Trunk_onpremise - Mozilla Firefox

https://10.10.153.2/management/portal/Applications/Operation/OSV/BusinessGroup/Members/PopUps/modifyBGEndpoint.psml?callPoi

[grp1019] - [Circuit] - [Main Office] - Edit Endpoint : Trunk_onpremise

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: 10.10.170.112

Port: 50011

Transport protocol: MTLS

Endpoint does not accept incoming TLS connections: ☐

SRTP media mode: Enabled

ANAT Support: Enabled

Save Cancel

Endpoint configuration of the OSV

20.5.10.2 On premise SBC configuration

The SBC on premise mode is configurable as regular sbc on customer's PBX side. Sip server should be configured in "sip server settings" to match customer sipsm of the PBX.

Communication system type should be Active-Standby and the register port 5060.

OnPremise - VOIP - Mozilla Firefox

https://10.10.170.165/voip.html?tabId=sipTab

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 Media QoS Monitoring

General

Comm System Type: Active-Standby

Allow Register from SERVER

Other trusted servers

Node 1

Target type: Binding

Primary server: 10.10.32.116 Transport: TCP Port: 5060

Backup server: Transport: TCP Port:

SRV record: Transport: TCP

Node 2

Target type: Binding

Primary server: 10.10.32.126 Transport: TCP Port: 5060

Backup server: Transport: TCP Port:

SRV record: Transport: TCP

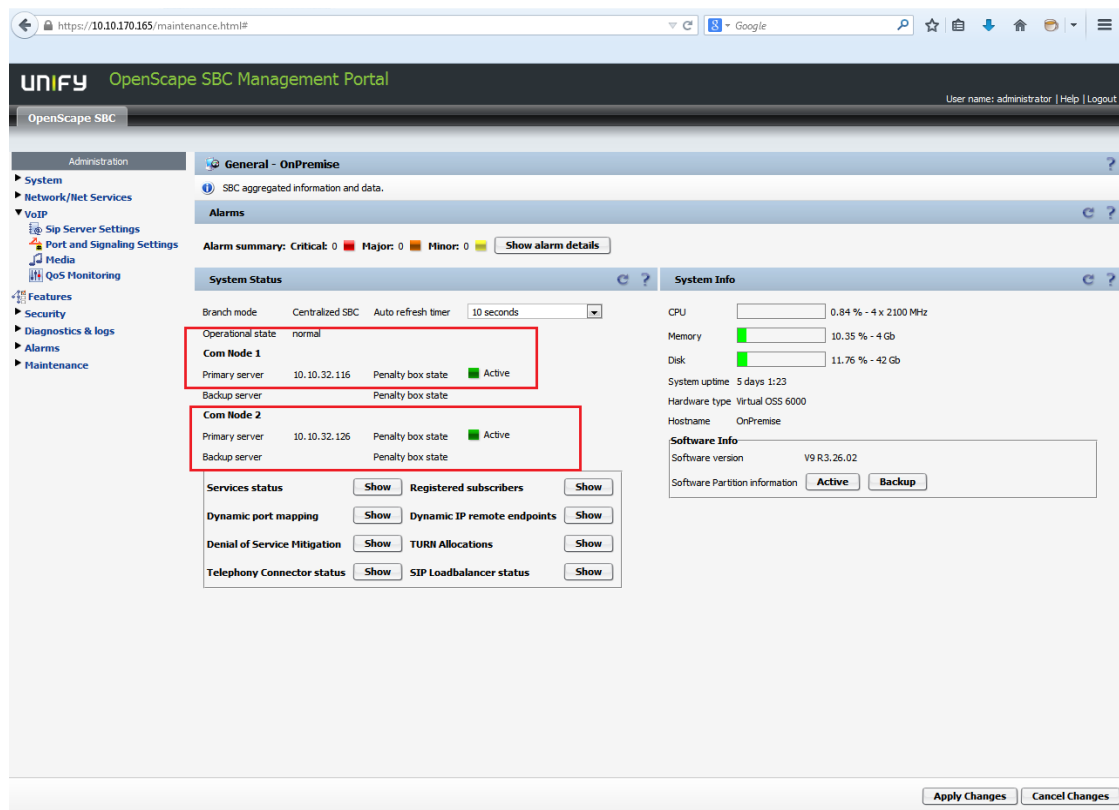
Timers and Thresholds

Failure threshold (pings): 2 OPTIONS interval (sec): 60

Success threshold (pings): 1 OPTIONS timeout (sec): 4

OK Cancel

Primary server is set to customer sipsm active and standby, and the state should be green.



The remote endpoint configuration is changed to allow a remote endpoint of SSP type by connected to endpoint of TRUNK-SBC.

Create default SSP profile and select “On Prem SBC” from drop down menu.

OnPremise - SIP Service Provider Profile - Mozilla Firefox

https://10.10.170.165/serviceProvider.html?mode=csbc&name=ssp

SIP Service Provider Profile

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

General

Name: Default SSP profile: On Prem SBC

☐ Use SIP Service Address for all identity headers

SIP service address:

SIP User Agent

SIP User Agent towards SSP: Passthru SIP User Agent:

Registration

☐ Registration required

Registration interval (sec):

Business Identity

☐ Business identity required

Business identity DN:

Outgoing SIP manipulation

☐ Insert anonymous caller ID for blocked Caller-ID

Manipulation

Incoming SIP manipulation

Calling Party Number: From header user and displ

Flags

☐

OK Cancel

Create endpoint, select type SSP and assign the default ssp profile. Match the core port of remote endpoint configured in the customer PBX corresponding to the on premise SBC.

OnPremise - Remote endpoint configuration - Mozilla Firefox
 https://10.10.170.165/remotepointConfiguration.html?name=Trunk1&status=false&standalone=false

Remote endpoint configuration

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

Remote Endpoint Settings

Name: Trunk1 Edit

Type: SSP ▼

Profile: ssp ▼

Access realm profile: Main-Access-Realm - ipv4 ▼

Core realm profile: Main-Core-Realm - ipv4 ▼

Associated Endpoint: ▼

☐ Enable Call Limits

Maximum Permitted Calls: 0

Reserved Calls: 0

Remote Location Information

☐ URI based routing

☐ Enable access control

Signaling address type: IP address or FQDN ▼

Remote Location domain list

Add Edit Delete

Row	Remote URL	Remote port	Remote transport	Media IP	Media profile	TLS mode	Certificate profile	TLS keep-alive	Keep-alive interval (seconds)	Keep-Alive timeout (sec)	INV
1	192.168.110.6	5060	TCP		default	Server authentication	OSV Solution	<input type="checkbox"/>	120	10	

Remote Location Identification/Routing

Core FQDN:

Core realm port: 50011

Default core realm location domain name:

Routing prefix:

OK Cancel

[GRP103C] - [athens] - [Main Office] - Edit Endpoint: On_Premise_mode - Mozilla Firefox

https://10.10.32.34/management/portal/Applications/Operation/OSV/BusinessGroup/Members/PopUps/modifyBGE

[GRP103C] - [athens] - [Main Office] - Edit Endpoint : On_Premise_mode

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: 10.10.170.165

Port: 50011

Transport protocol: TCP

Endpoint does not accept incoming TLS connections: ☐

SRTP media mode: Enabled

ANAT Support: Enabled

Save Cancel

Please note that the above configuration applies when on premise SBC is connected to SSP through a SBC and the customer's PBX is an OSV.

21 Glossary and Abbreviations

ACD	Automatic Call Distribution
AFD	Available For Development
ALI	Advanced Locking ID for SEN licensing Virtual deployments
AMI	Amazon Machine Image
ANAT	Alternative Network Address Types
AoR	Address of Record
API	Application Programming Interface
B10	PEPP Milestone where detailed analysis of a feature begins
B2BUA	Back-to-Back User Agent
B50	PEPP milestone at which a feature is defined
BG	Business Group
BGL	Business Group Line; a line that is a member of a business group
BO	Business Opportunity
BSM	Binding State Machine
CAC	Call Admission Control
CALEA	Communications Assistance for Law Enforcement
CCM	Connection Control Manager (MGCP)
CDR	Call Detail Record; an intermediate billing record generated by OpenScape Voice
CF	Call Forwarding
CF	Collection Function (for Electronic Surveillance)
CLI	Command Line Interface
CMP	Common Management Portal
CPU	Central Processing Unit
CR	Change Request
CSTA	Computer Supported Telecommunications Applications; ECMA open-standard interface definition to enable computing systems to control telephony systems (3rd party call control)
CSV	Comma Separated variables
DA	Digest Authentication
DF	Delivery Function (for Electronic Surveillance)
DFT	Digital Feature Telephone; a telephone that supports one line (i.e., has no line keys)
DHCP	Dynamic Host Configuration Protocol
DID	Direct Inward Dialing
DLS	Deployment and Licensing Tool
DMS	Document Management System
DMZ	Demilitarized Zone
DNS	Domain Name Server
DSCP	Differentiated Services Code Point
E.911	Enhanced Emergency Call system
EC2	Amazon Elastic Cloud (version 2)
E-Doku	Document Management System
ESXi	VMware product
ETSI	European Telecom Standardization Institute; international standards body, comparable to ANSI, that recommends standards for telephony, ISDN, wireless, plesiochronous, and synchronous transport in Europe
FDB1	Feature Design Building Block 1
FQDN	Fully Qualified Domain Name
FRDB	FRN Database
FRN	Feature Request Number (replaces LM Number); also used as the Feature Request object itself
FSC	Fujitsu-Siemens Computers
GUI	Graphical User Interface
HD	Hard Drive
HiPath	Unify line of PBXs
HiSPA	HiPath Serviceability Platform for Applications
HMS	HiPath Media Server
HW	Hardware
ICE	Interactive Connectivity Establishment
ICMP	Internet Control Message Protocol
iMS	Integrated Media Server – onboard media server on the Integrated OpenScape Voice solution.

IP Internet Protocol; IP specifies the format of packets, also called datagrams, and the addressing scheme.

ISAKMP Internet Security Association and Key Management Protocol

LAN Local Area Network

LEA Law Enforcement Agency

LI Lawful Interception - an ETSI framework used by the regional law enforcement, for their own regional specifications

LIN Location identification number

LIP Large IP

LM Leistungsmerkmal (German for "Feature"); This document uses the term FRN instead

MCU Media Control Unit

MG Media Gateway

MGC Media gateway Controller

MGCP Media Gateway Control Protocol; IETF standard RFC 2705

MIB Management Information Base

MIKEY0 Key Exchange Protocol

MLHG Multi-Line Hunt Group

MTLS Mutual Authentication TLS

MS Media Server

NAT Network Address Translator

NCPE Node Configuration Parameters Editor

NCS Network-based Call Signaling; PacketCable's MGCP variant for MTA control

NTP network Time Protocol

OAM Operation and maintenance functions

OEM Original Equipment Manufacturer

OMM Operational Measurements Management

ONS One Number Service

OSCAR SEN Communications Standards Organization

OSB OpenScape Branch

OSV OpenScape Voice

OSMO OpenScape MOBILE

OS-SBC OpenScape SBC

OSS OpenScape SBC

OVA Archive file containing OVF 1.0 descriptor and VMDK files

OVF A descriptor file that references VMDK-format virtual disk files

PBX Private Branch Exchange

PC Personal Computer

PIDF-LO Presence Information Data Format Location Object

PSTN Public Switched Telephone Network

QoS Quality of Service

QSIG Q (point of the ISDN model) Signaling; common channel signaling protocol based on ISDN Q.931 standards and used by many digital PBXs; used in the Enterprise market for the establishment and release of calls and for the control of a large number of features between PBXs

RG2700 An Enterprise Gateway

RG8700 An Enterprise Gateway

RSIP restart In Progress (MGCP)

RTP Real-Time Transport Protocol; IETF standard RFC-1889

RTP Resilient Telco Platform; OpenScape Voice middleware

RTT RealTime Trace

SBC Session border Controller

SDK Software Development Kit

SDP Session Description Protocol; IETF standard RFC-2327

SFTP Secure FTP

SIP Session Initiation Protocol; an IP-based protocol for distributed applications; IETF standard RFC-3261

SIRA Remote Service Access

SM Signaling Manager

SMR Software Maintenance Release

SMU Staff Month Unloaded

SNMP Simple Network Management Protocol; IETF standard

SOAP Simple Object Access Protocol

SOHO Small Home Office

SRTP Secure Real-Time Transport Protocol

SSP	SIP Service Provider
SW	Software
TCP	Transaction Control Protocol
TLS	Transport Layer Security
UA	User Agent
UAC	User Agent -Client
uaCSTA	User Agent -CSTA
UAS	User Agent -Server
UDP	User Datagram Protocol
UM	Unified Messaging
URI	Universal Resource Identifier
vApp	Virtual Appliance
Virtual	Appliance - An OVF descriptor file and one or more VMs that can be deployed and managed as as single entity by VMware tools
VIP	Virtual IP address
VM	Virtual Machine
VMDK	Virtual disk file used to store the contents of the virtual machine's hard disk drive
VM-OS-SBC	Virtual Machine OpenScape Session Border Controller
VoIP	Voice Over IP
VPN	Virtual Private network
VRRP	Virtual Router Redundancy Protocol
WAN	Wide Area Network
WSDL	Web Services Definition Language
XML	Extensible Markup Language