Unify OpenScape Session Border Controller

OpenScape SBC V11

Configuration Guide
July 2025

A31003-S53B0-M100-09-76A9

Mitel

Notices

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

Trademarks

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

Table of Contents

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	▪ Remote Endpoint configuration for OpenScape 4000 ▪ OpenScape Branch and SBC distribution via OVA
9.8.00	16/03/2018	▪ FRN 10620 - **IOS push feature**
9.9.00	11/05/2018	▪ Open External Firewall – **Pinhole feature**
9.10.00	24/05/2018	▪ **IOS push** feature enhancements
9.11.00	17/08/2018	▪ **Incoming SIP Manipulation** ▪ **Advanced Locking Id (ALI)**
9.12.00	28/09/2018	▪ **BCF Event Handling**
9.13.00	11/12/2018	▪ Minor enhancements & modifications
9.14.00	12/02/2019	▪ **UCaaS functionality** **a) On premise configuration** o **b) Cascaded configuration**
9.15.00	01/03/2019	▪ **Redesign of Time Zone configuration**
9.16.00	29/03/2019	▪ **Rest API**
9.17.00	12/04/2019	▪ Minor enhancements & modifications
9.18.00	05/07/2019	▪ Minor enhancements & modifications
9.19.00	15/11/2021	▪ Documentation enhancements and updates
9.20.00	13/12/2022	▪ Added note under Chapter 3.4.4.5 Media
9.21.00	11/1/2023	▪ Minor updates
9.22.00	20/4/2023	▪ Updated Section 3.4.5.1.1 Remote Subscriber Settings
9.23.00	26/06/2023	▪ Minor updates
9.24.00	01/08/23	▪ Updates and enhancements
9.25.00	22/07/2024	▪ Rebranded to Mitel layout
9.26.00	17/01/2025	▪ Added V11R2 content: o Configuring DNS NAPTR o *Administration Accounts* o Updated the content related to the **Export Logical IDs** function
9.27.00	18/02/2025	▪ Updated 2.1.5 Configuration of Virtual OS-SBC (VM-OS-SBC)
9.28.00	15/04/2025	▪ Added 3.4.4.9 Session Recording Client

Release Notes

Circuit Support in Version V11

SBC V11 does not support Circuit functionality.
We recommend that users who rely on Circuit features consider SBC V10 or explore the capabilities provided in Version V11 to meet their communication needs. For further information or assistance, please refer to the product documentation or contact our support team.

OpenScape UC Firewall

Please request release notes from thomas.toelg@unify.com

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 Manger" window select **Add Boot Option** and press **Enter.**
5. Select "USB Storage" and press **Enter**.
6. Press **Esc** to exit and go back to the "Boot Manager" window.
7. Select "Change Boot Order" and press **Enter.**
8. Press **Enter** again to change the order.
9. The order should be:
    - USB Storage
    - Hard Disk 0
10. Press **Enter**.
11. Select **Commit Changes** to save.
12. Press **Esc** to exit from all the windows.
13. Select **Y** when asked "Do you want to exit the Setup Utility?".

2.1.2 Change boot device for one time use: for IBM 3250M3/M5/M6 and 3550M3/M4/M5, Lenovo SR250/SR250 V2/V3, SR530 and SR630 V2/V3

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.

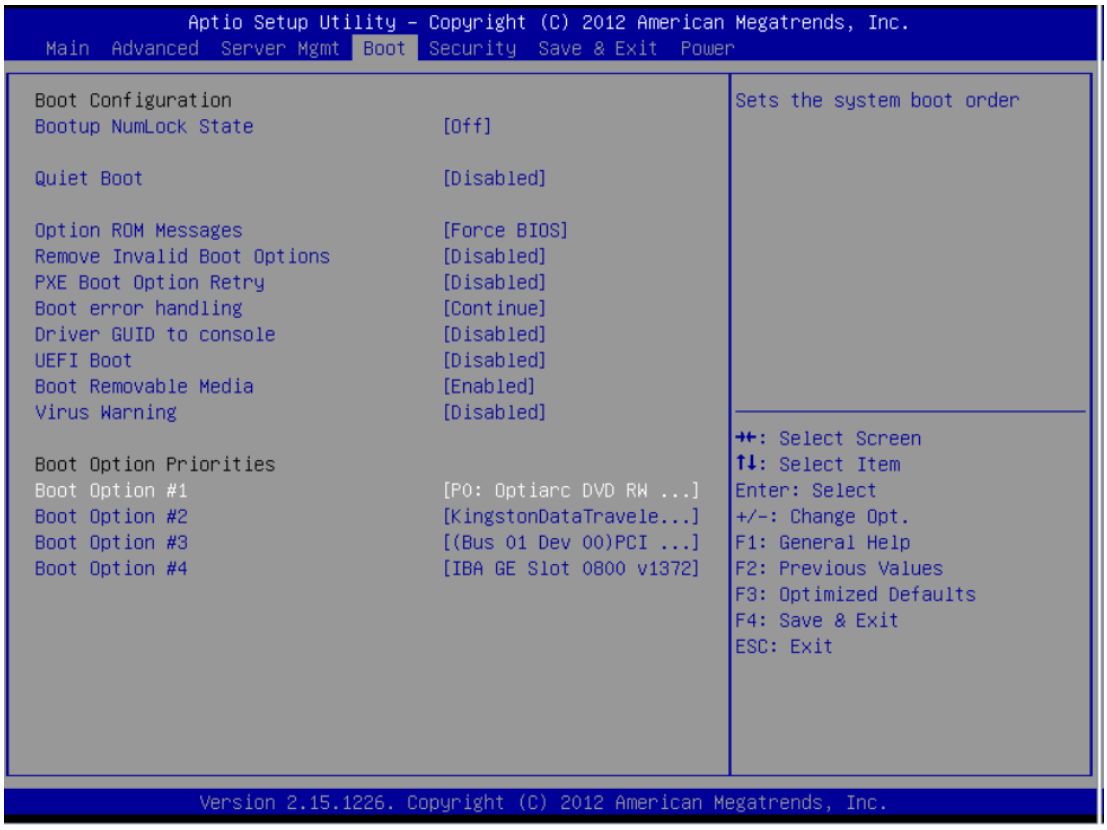
2.1.2.2 Lenovo SR530, SR630 V2/V3 and Lenovo SR250 / SR250 V2/V3 platforms

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/V3 and Lenovo SR630 V2/V3 are available starting from V10R3.3.0.
NOTE: Lenovo SR250 V3 and Lenovo SR630 V3 are available starting from V11R2.3.0.

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/V3 and Lenovo SR250 / SR250 V2/V3 platforms

LEGACY MODE:
1. Select **F1** to enter 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 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 parameters are supported:

VM-OSSBC size	OSSBC-250	OSSBC-6000	OSSBC-20000
Number of CPUs	**2**	**4**	**6 (<= 20000 subscribers)** **8 (<= 32000 subscribers)**
Memory size	**4Gb**	**4Gb**	**6Gb**
Hard disk size	**40Gb**	**40Gb**	**60Gb**
Network adapter type	**VMXNET3**	**VMXNET3**	**VMXNET3**
Number of network adaptors	**2**	**2**	**2**

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

Please refer to Deployment of a virtual OS-SBC on the OpenScape Solution Set V10, OpenScape Virtual Machine Resourcing and Configuration Guide, and Service Documentation.

Important: 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

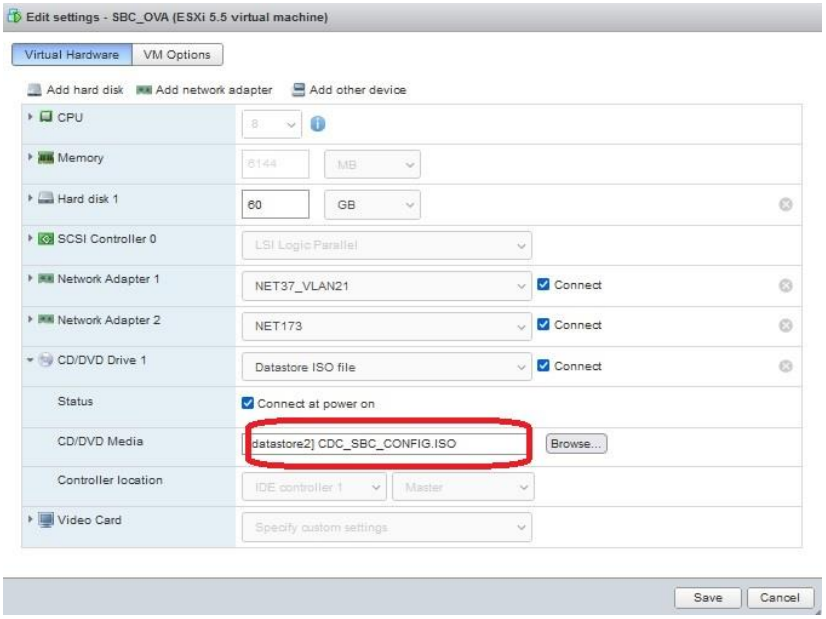
NOTE: In previous release, the OVA was used with OSEE/THIG(4 CPUs).

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.

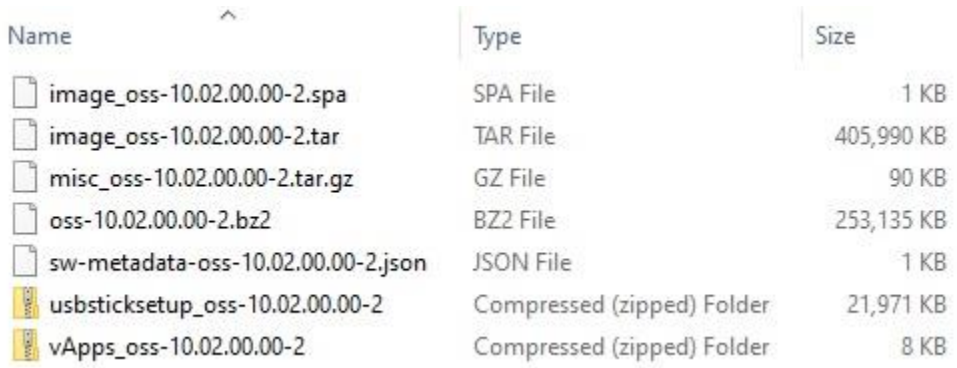
2.2 USB Stick Setup tool (classic method)

This application is distributed with the following files from SWS

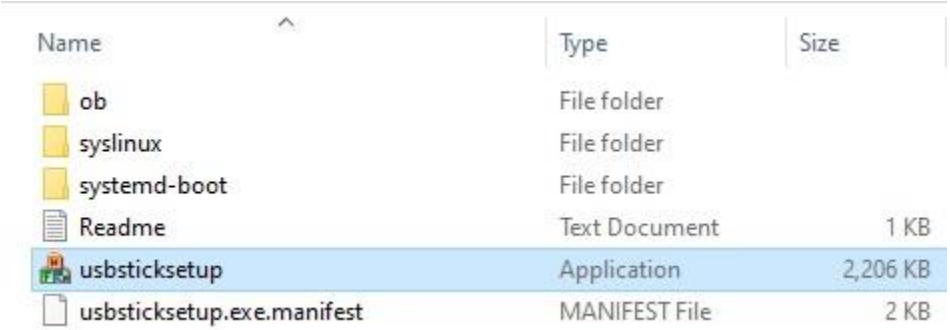
- **oss-10.02.*.*-*.zip**, that contains:
  - **image_oss-10.02.*.*-*.tar** – Software image file for upgrade or install.
  - **image_oss-10.02.*.*-*.spa** – File contains the compatibility information from the old release to new release for use by the CMP.
  - **usbsticksetup_oss-10.02.*.*-*.zip** - 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.

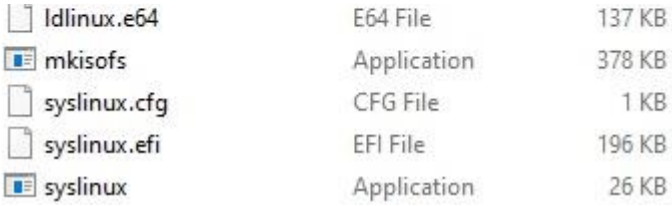


1. Unzip the file “usbsticksetup_oss-*.*.*.*.zip. The files will unzip into a folder called “usbsticksetup”. The contents of the “usbsticksetup” folder will look like:



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

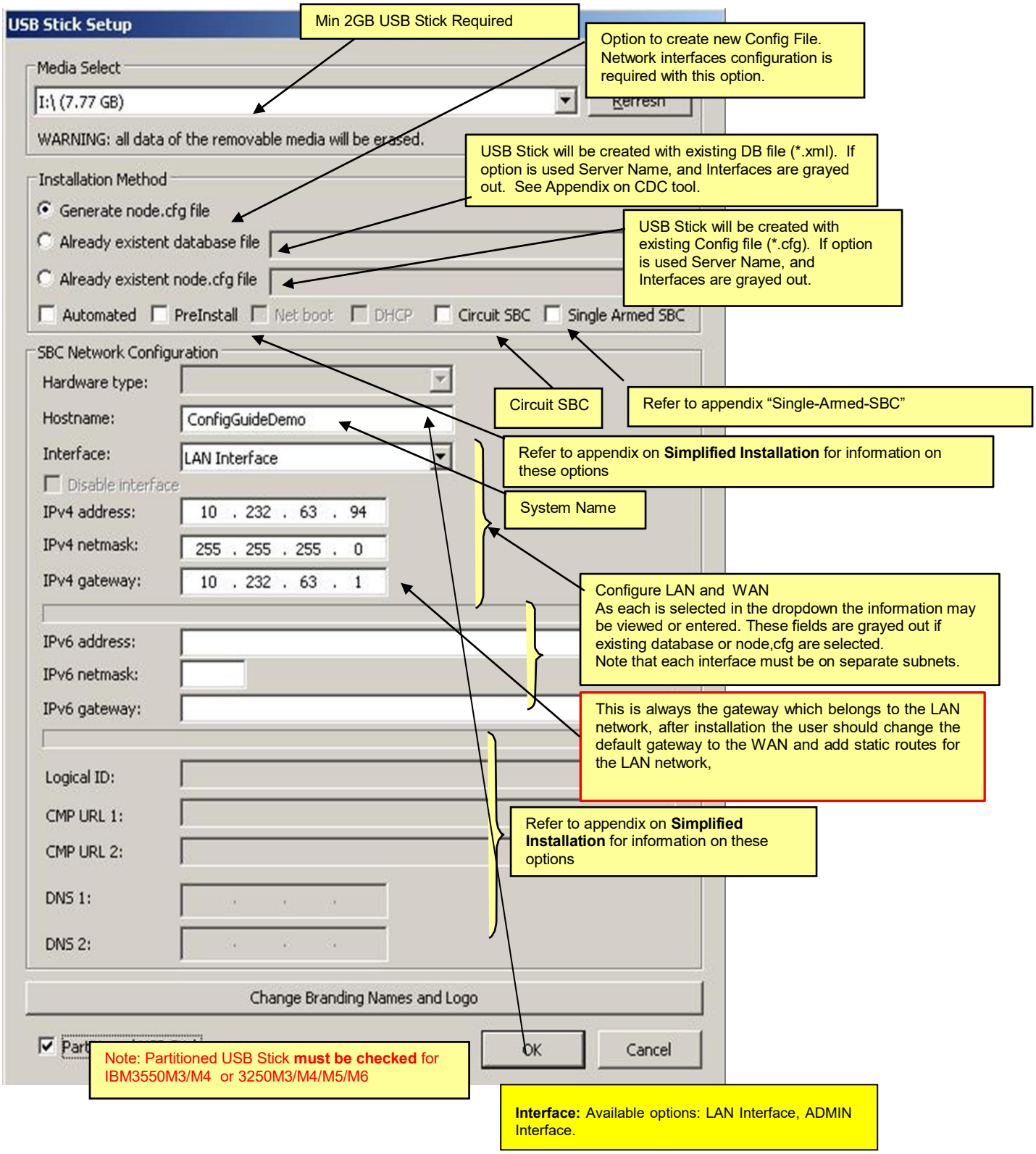
3. The “syslinux” folder will look like:



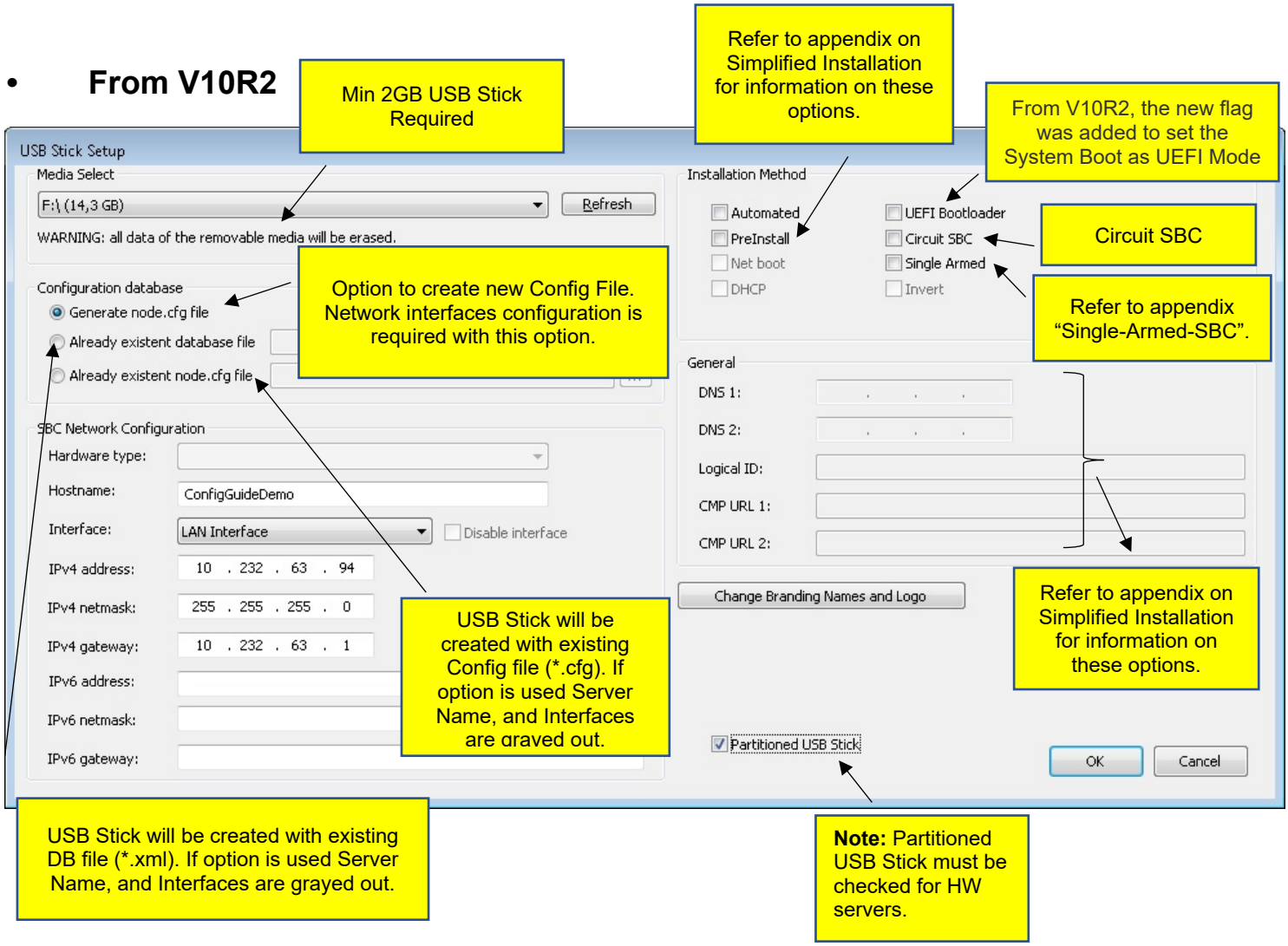
4. Proceed to the USB stick creation by running usbsticksetup.exe application.
5. After filling in the required information, press **OK** to create the USB Stick.
6. After the process is completed, the USB Stick can be removed and it will be ready for installation.

2.2.1 USB setup for single node system

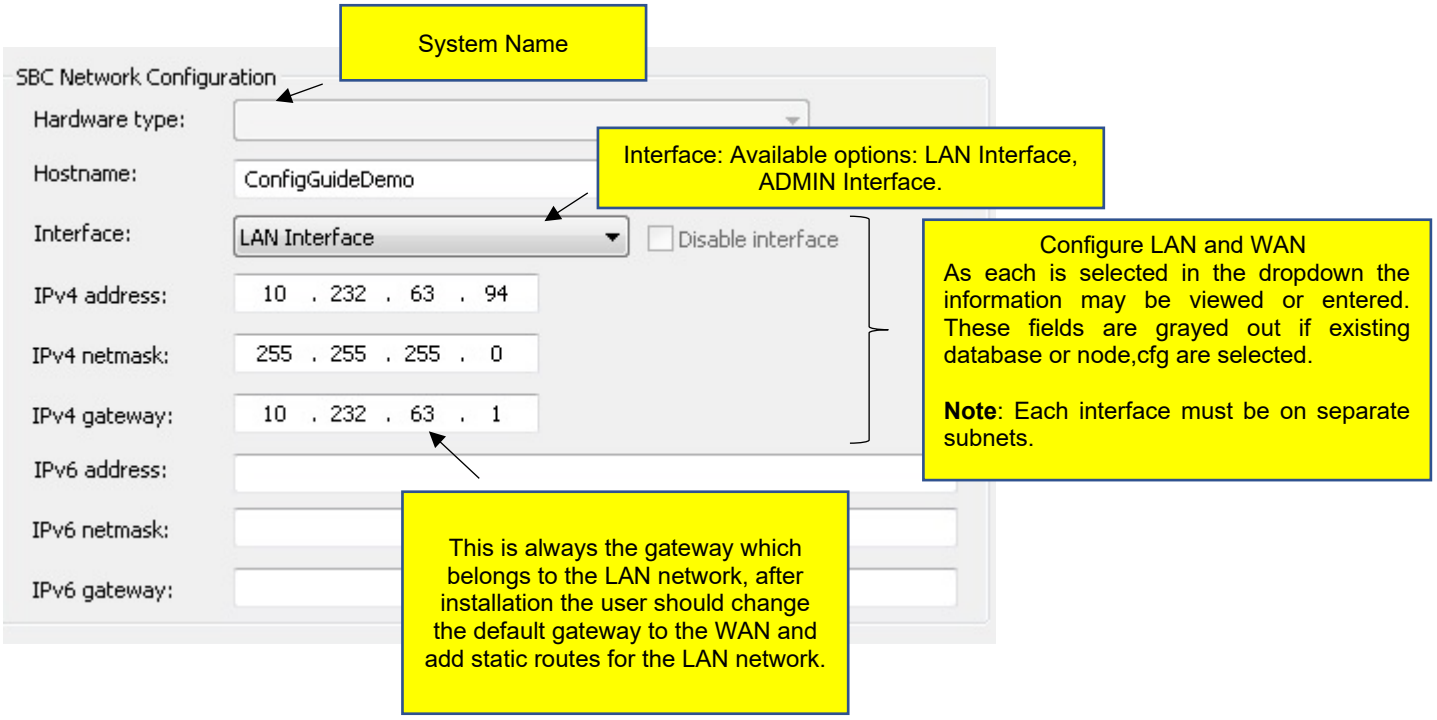
- **Up to V10R1**



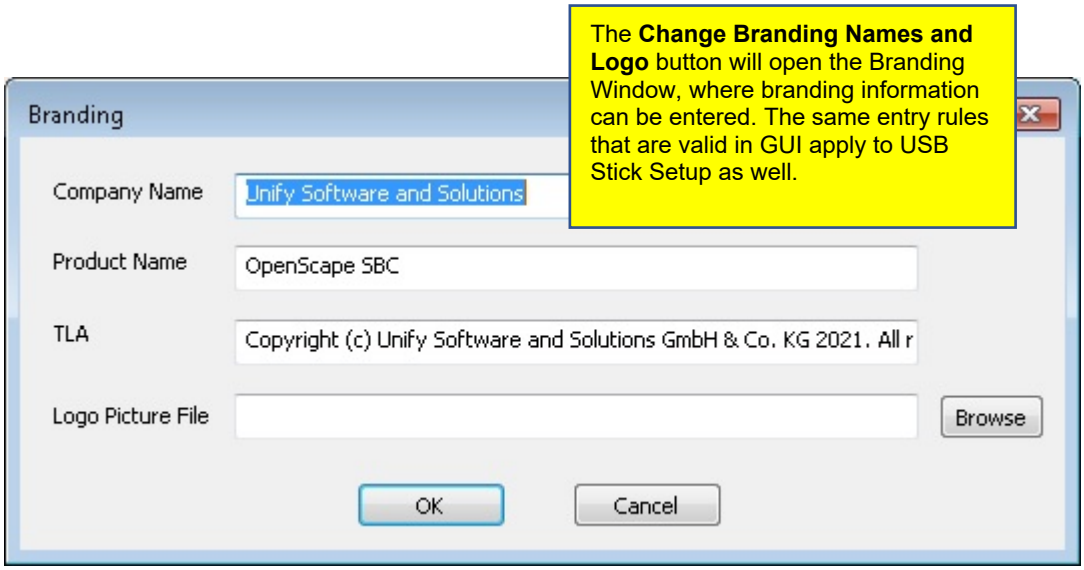
- **From V10R2**


Min 2GB USB Stick Required
Refer to appendix on Simplified Installation for information on these options.
From V10R2, the new flag was added to set the System Boot as UEFI Mode
USB Stick Setup
Media Select
F:\ (14,3 GB)
Refresh
WARNING: all data of the removable media will be erased.
Installation Method
Automated
PreInstall
Net boot
DHCP
UEFI Bootloader
Circuit SBC
Single Armed
Invert
Circuit SBC
Refer to appendix "Single-Armed-SBC".
Configuration database
Generate node.cfg file
Already existent database file
Already existent node.cfg file
Option to create new Config File. Network interfaces configuration is required with this option.
General
DNS 1:
DNS 2:
Logical ID:
CMP URL 1:
CMP URL 2:
SBC Network Configuration
Hardware type:
Hostname:
ConfigGuideDemo
Interface:
LAN Interface
Disable interface
IPv4 address:
10 . 232 . 63 . 94
IPv4 netmask:
255 . 255 . 255 . 0
IPv4 gateway:
10 . 232 . 63 . 1
IPv6 address:
IPv6 netmask:
IPv6 gateway:
Change Branding Names and Logo
Refer to appendix on Simplified Installation for information on these options.
USB Stick will be created with existing Config file (*.cfg). If option is used Server Name, and Interfaces are grayed out.
Partitioned USB Stick
OK
Cancel
USB Stick will be created with existing DB file (*.xml). If option is used Server Name, and Interfaces are grayed out.
Note: Partitioned USB Stick must be checked for HW servers.

SBC Network Configuration



2.2.1.1 Branding Information on the USB Stick Setup



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).

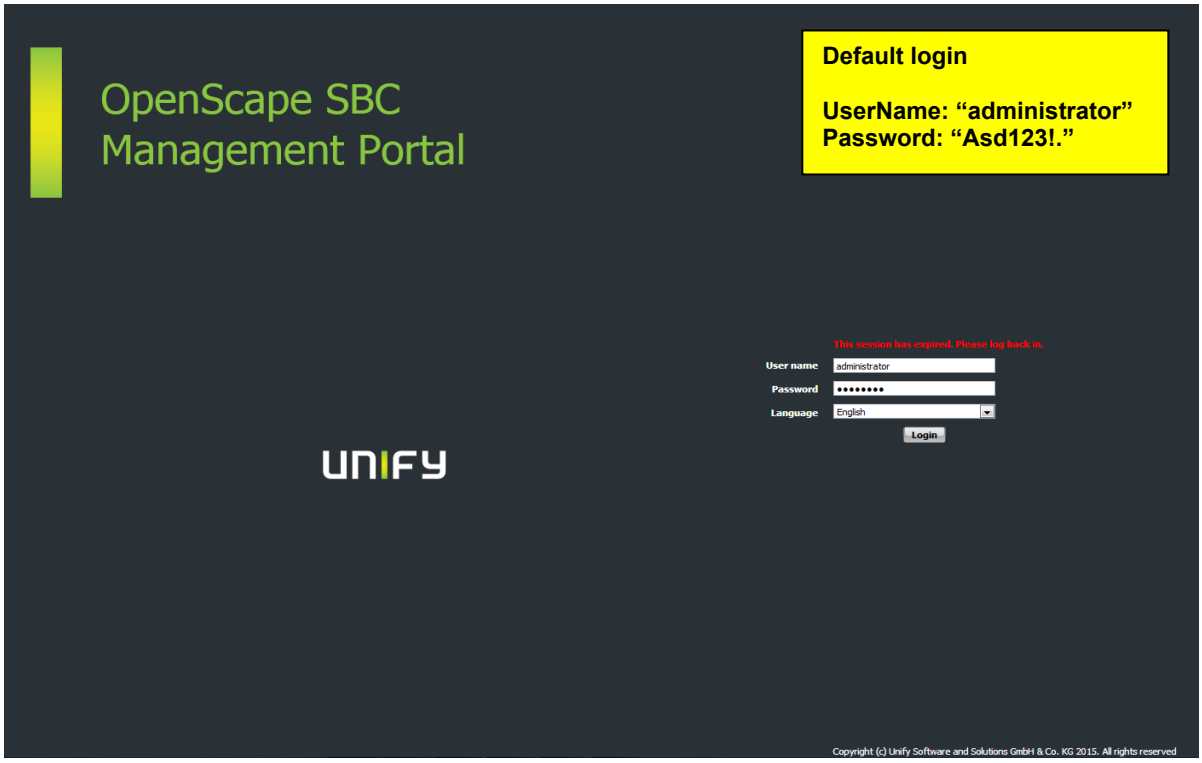
1. Restart OS-SBC with the USB connected.
2. Select the USB as the boot device during the power up sequence (F12).
3. Open the internet browser to the LAN IP (defined in the previous steps) via https:// and login as
    - User Name: “administrator”.
    - Password: “Asd123!.”

After the login OS-SBC will alert the user that OS-SBC is running with the USB stick.

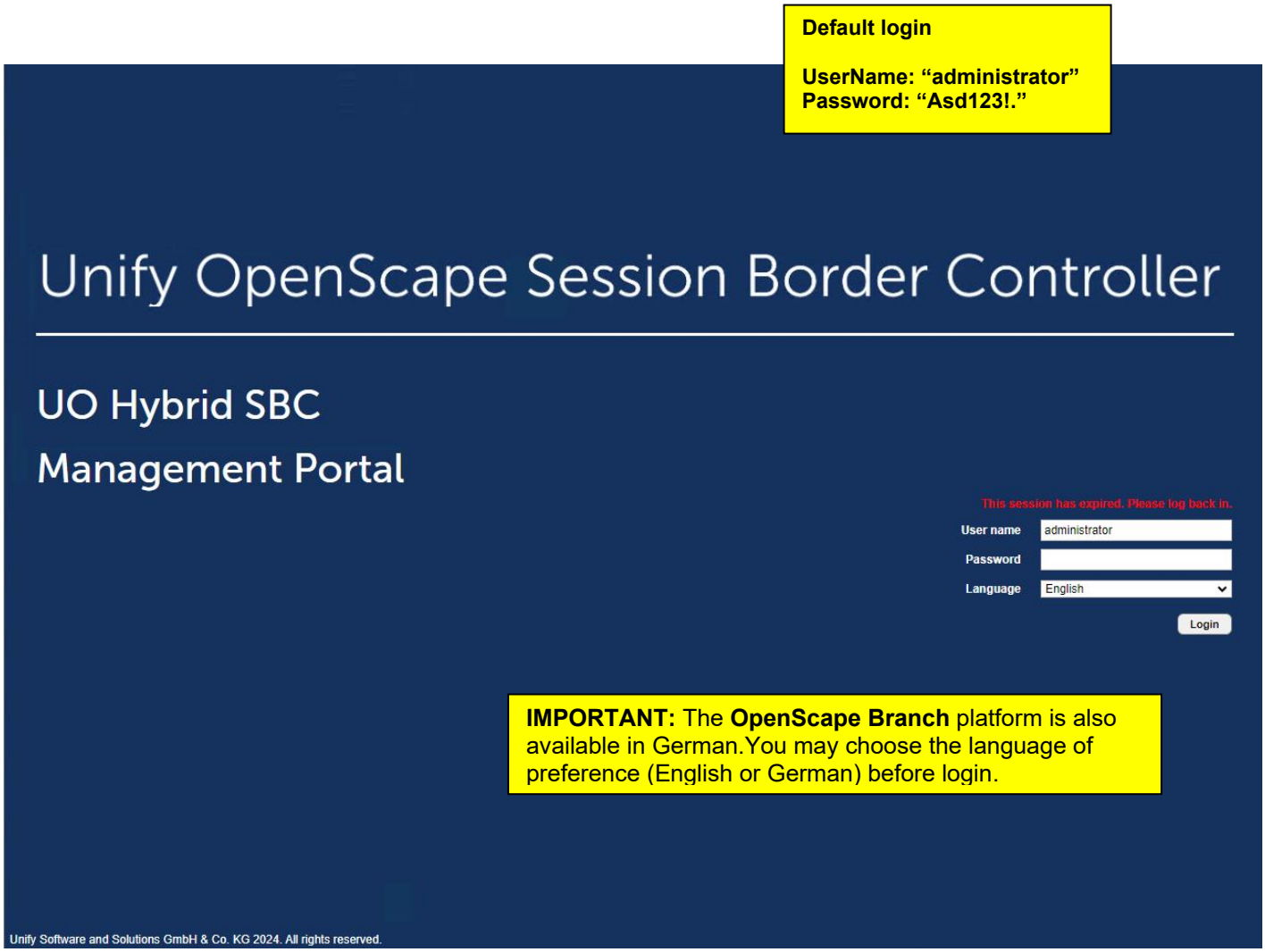
Note: From V10R2, the Local GUI is optimized for current versions of Chrome, Edge and Firefox. Please note that using IE or other browsers may lead to rendering errors and/or limited functionality.

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**



4. 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 itwas 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.

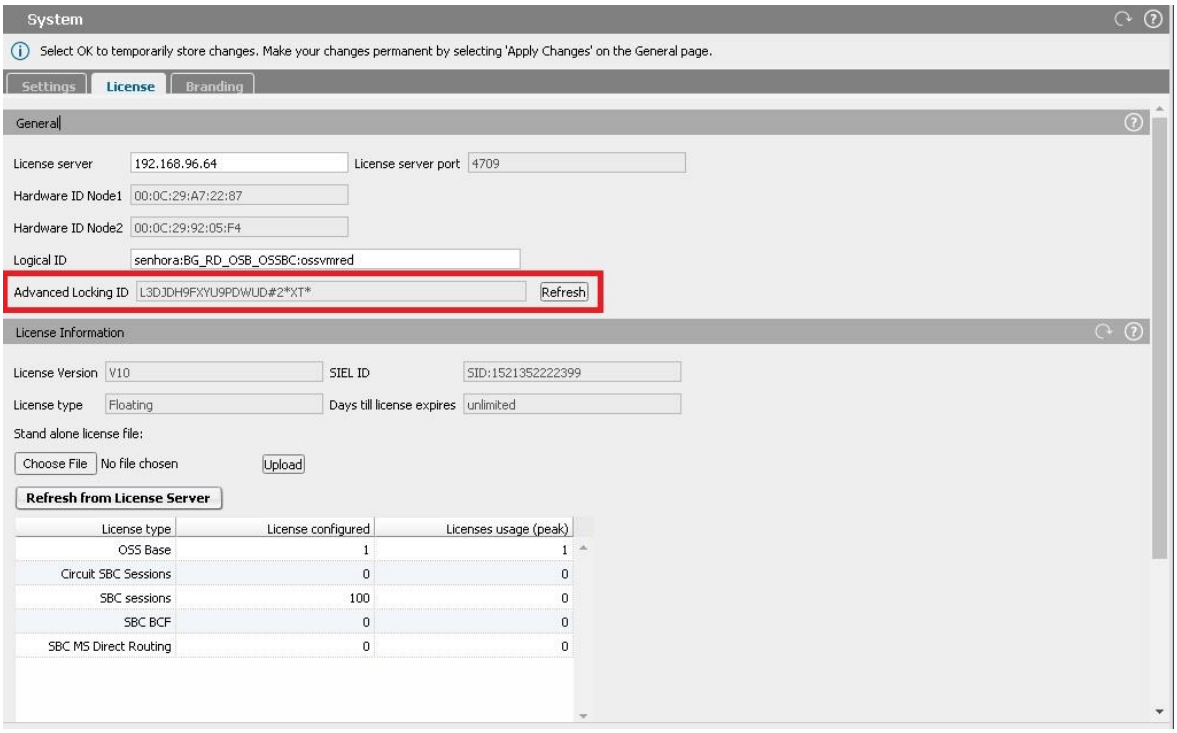
Timezone: from Local GUI of OS-SBC, navigate to Network/Net Services page → NTP → Timezone configuration

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.

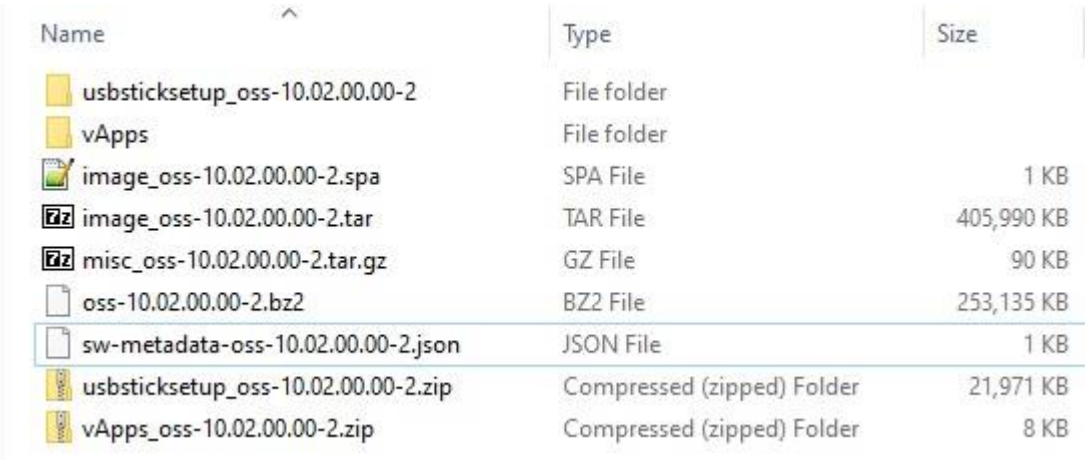
- This method of standalone licensing of Virtual OS-SBC is not the preferred method, but may still be used.
  - The **Advanced Locking ID** is also available in System → License folder.
  - Press **Refresh** in **Advanced Locking ID** option.

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

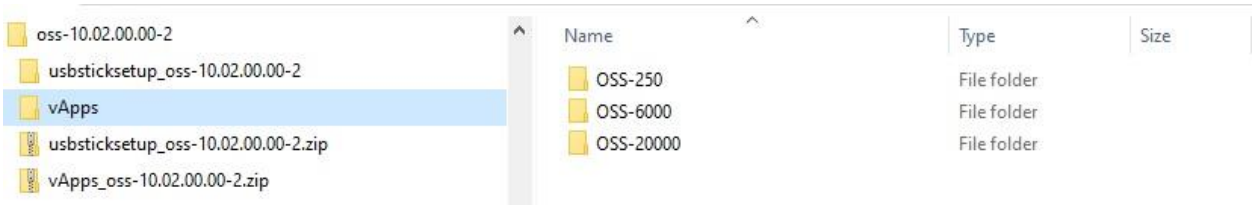


2.3.2 Detailed steps to deploy with a vApp

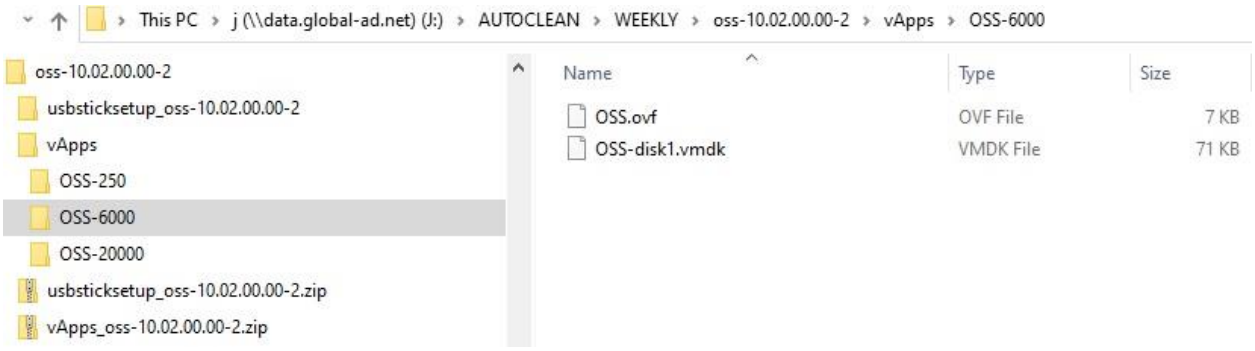
After unzipping the **usbsticksetup** and **vApps** archives your file folder should look like this:



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



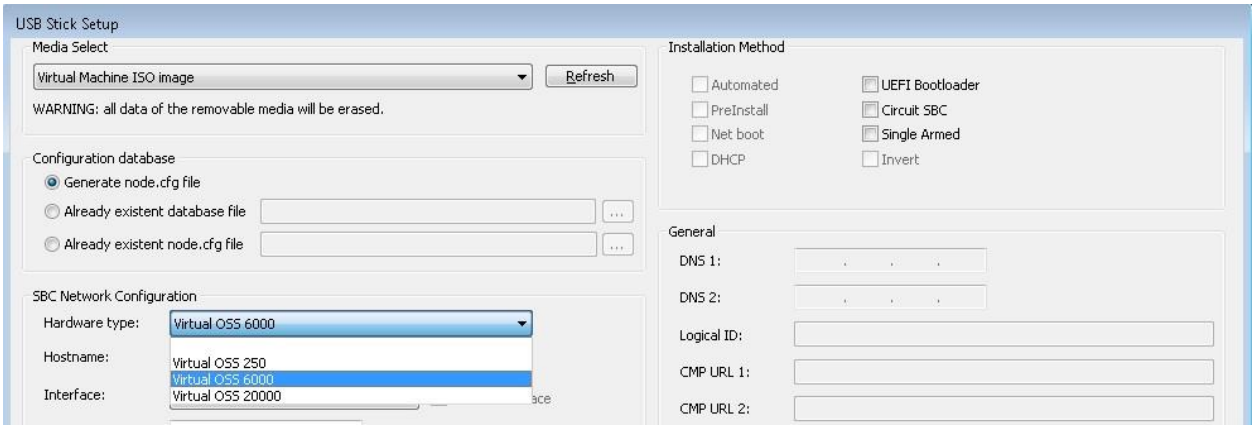
The **OSS.ovf** and **OSS-disk1.vmdk** files are used to deploy the vApps template for creating a OS-SBC VM in sizes 250, 6000 or 20000.



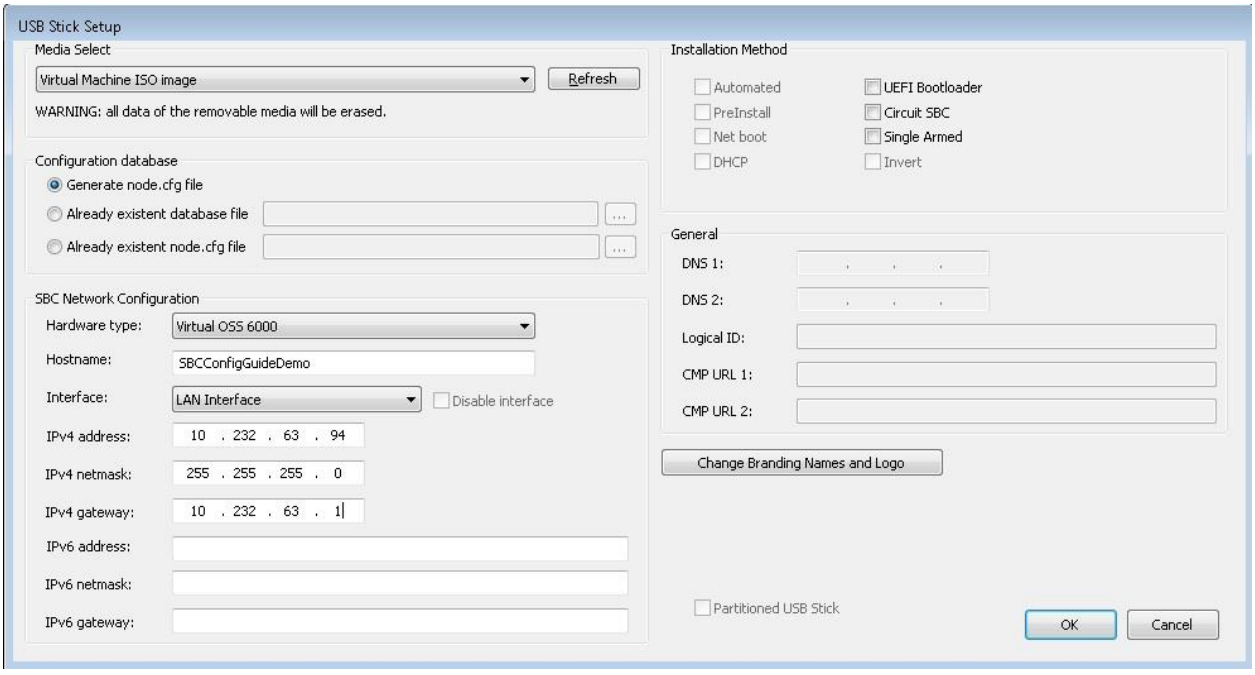
2.3.2.1 How to create the OS-SBC ISO image with the Software Load

1. Move the **image_oss-10.02.*.*-*.tar file** to the **ob** folder.

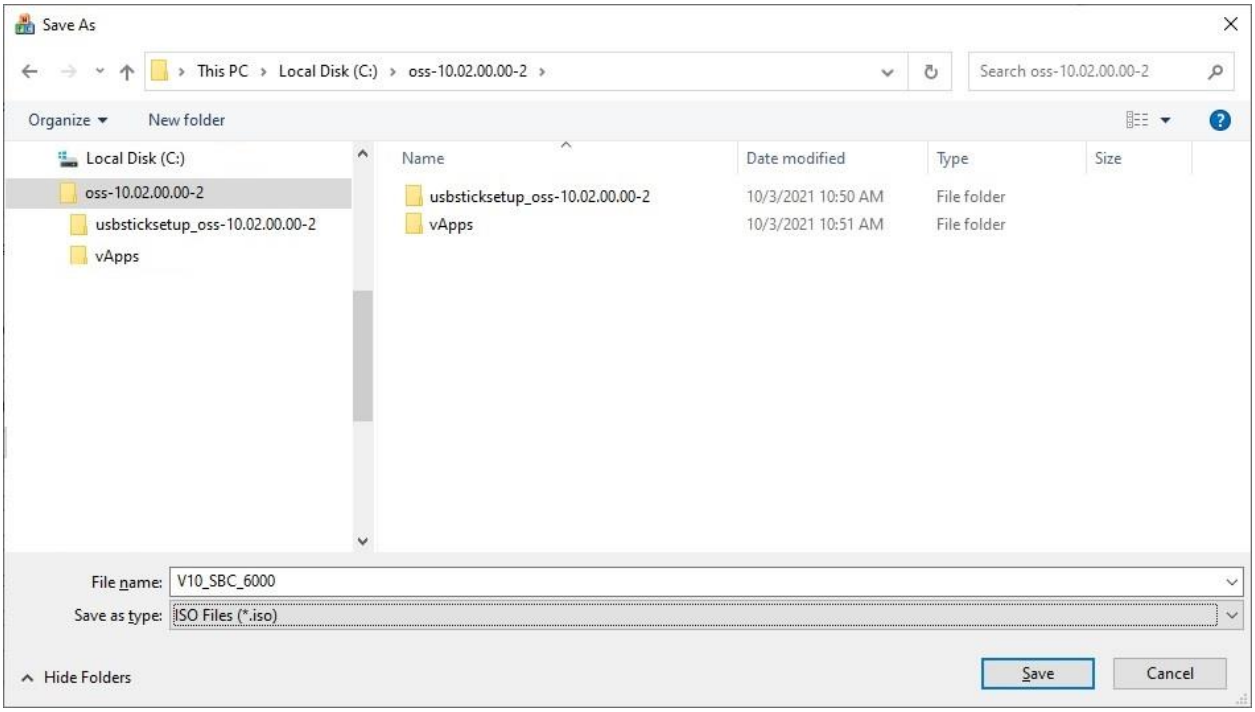
2. Run the **usbsticksetup.exe** program that was downloaded with the OS-SBC load from SWS:



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**.

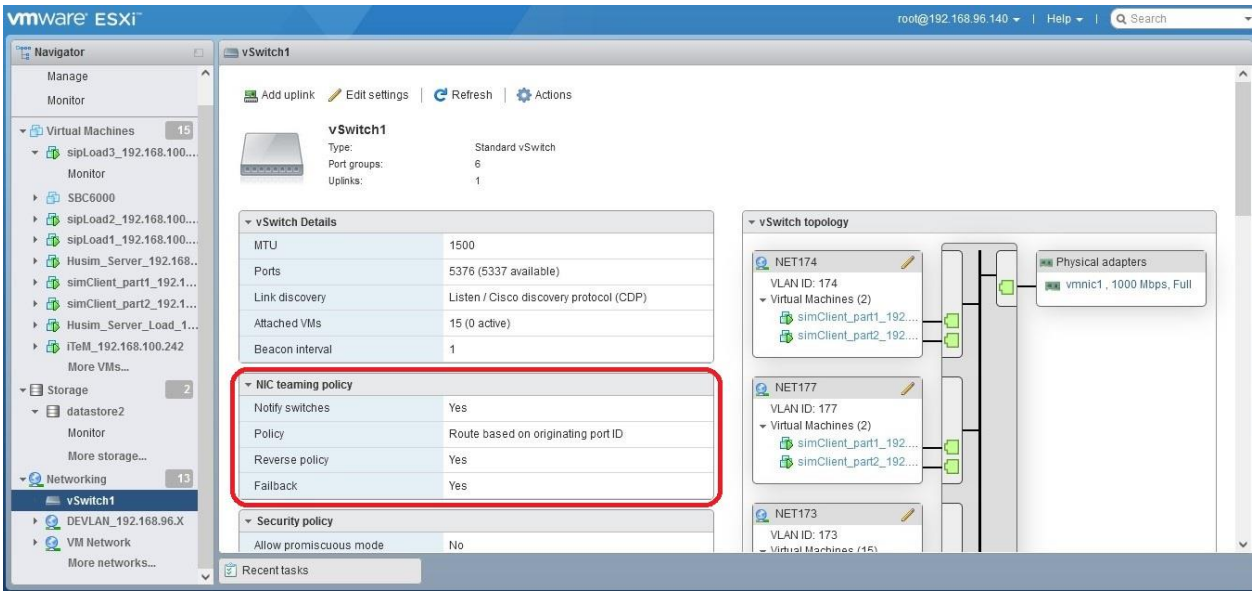


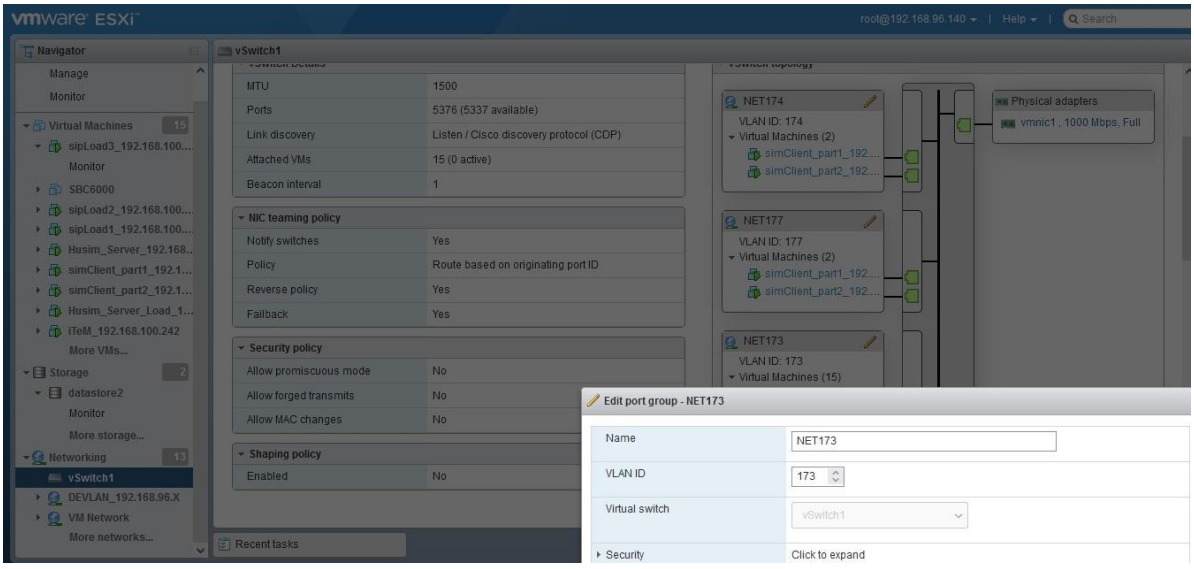
After clicking **OK**, you will be asked to configure where to save the resulting ISO file.



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.



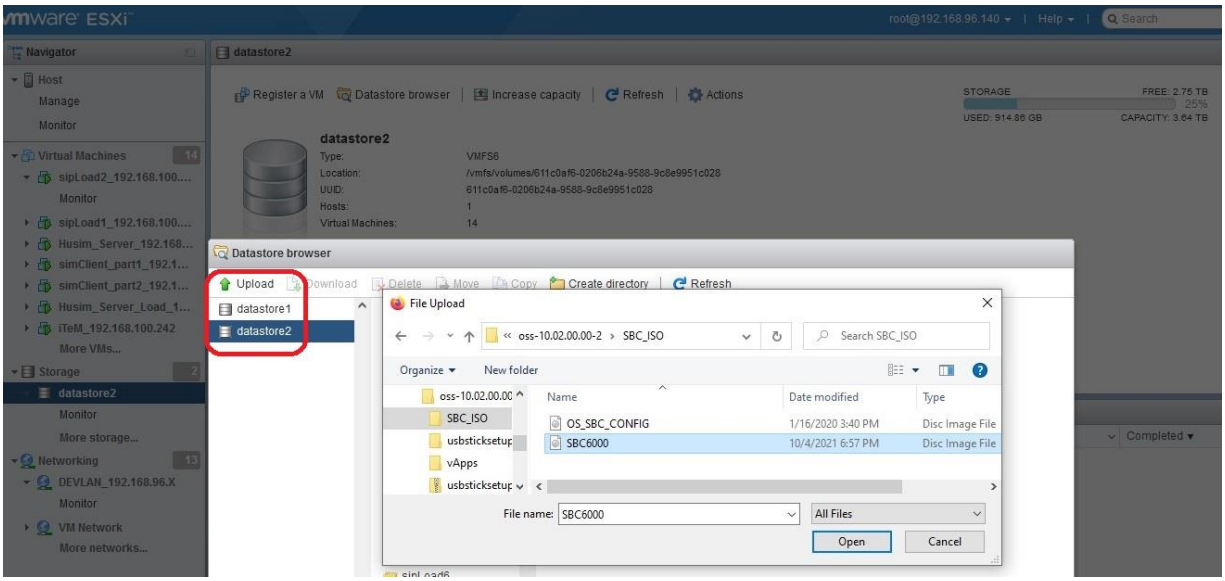


4. When creating the OS-SBC VM, assign this Network label to the appropriate interface of the OS-SBC (i.e. LAN or WAN). There is no need to modify the Hostname of the OS-SBC to append any suffix.

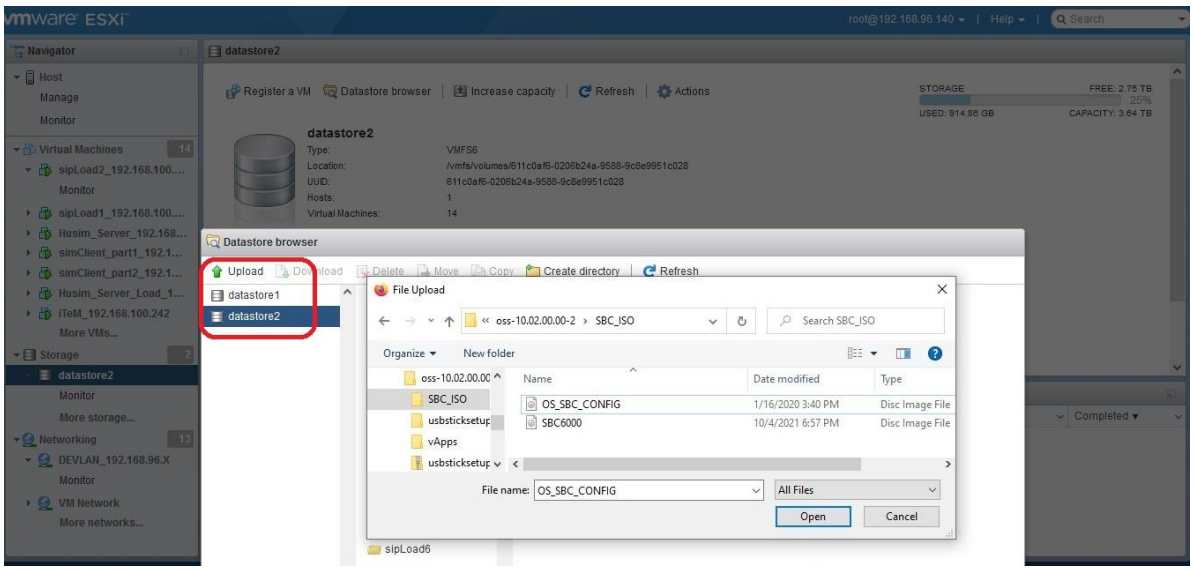
2.3.4 Detailed steps to deploy with a vApp (cont)

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

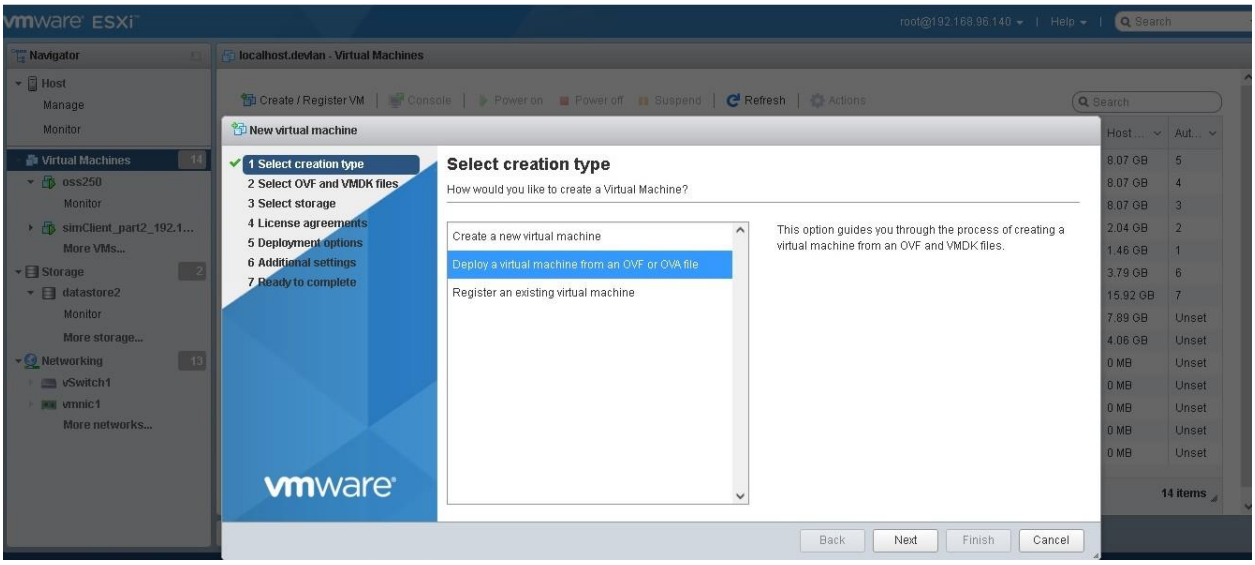
1. Upload the OS-SBC ISO image to VM Host Datastore. The ISO image generation is mentioned in **2.3.2.1 How to create the OS-SBC ISO image with the Software Load**.
2. Select the **Storage** option.
3. Right click on **datastore** and select **Datastore browse.**
4. Select the folder where you want to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



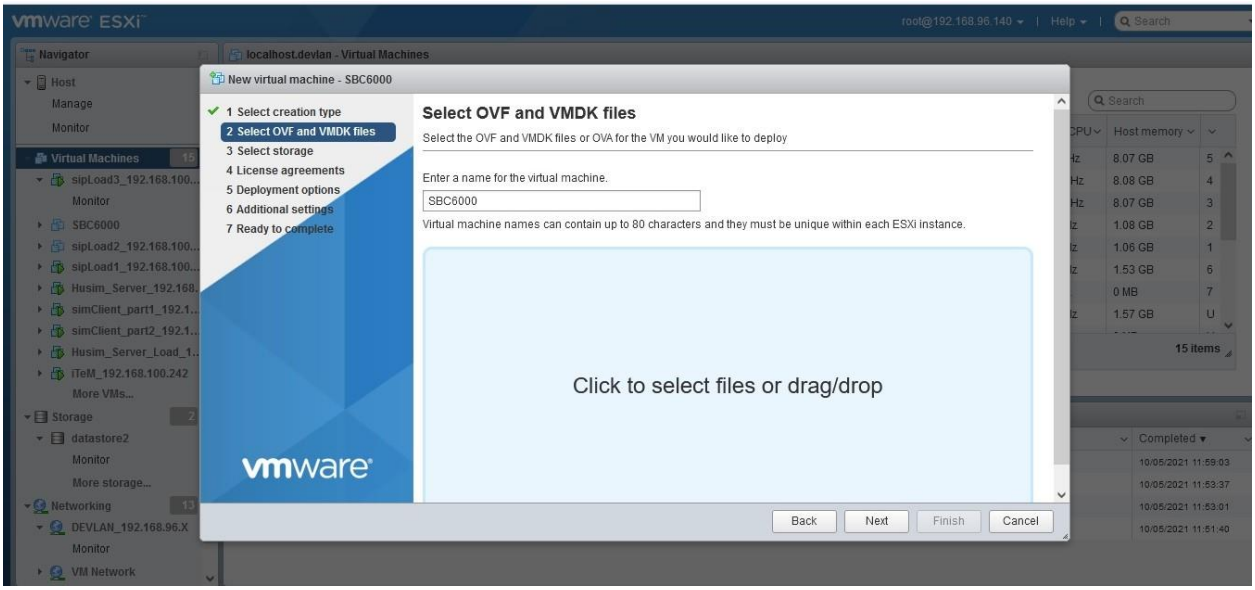
Repeat this procedure to upload the OS-SBC Configuration ISO image if it is available.



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**.

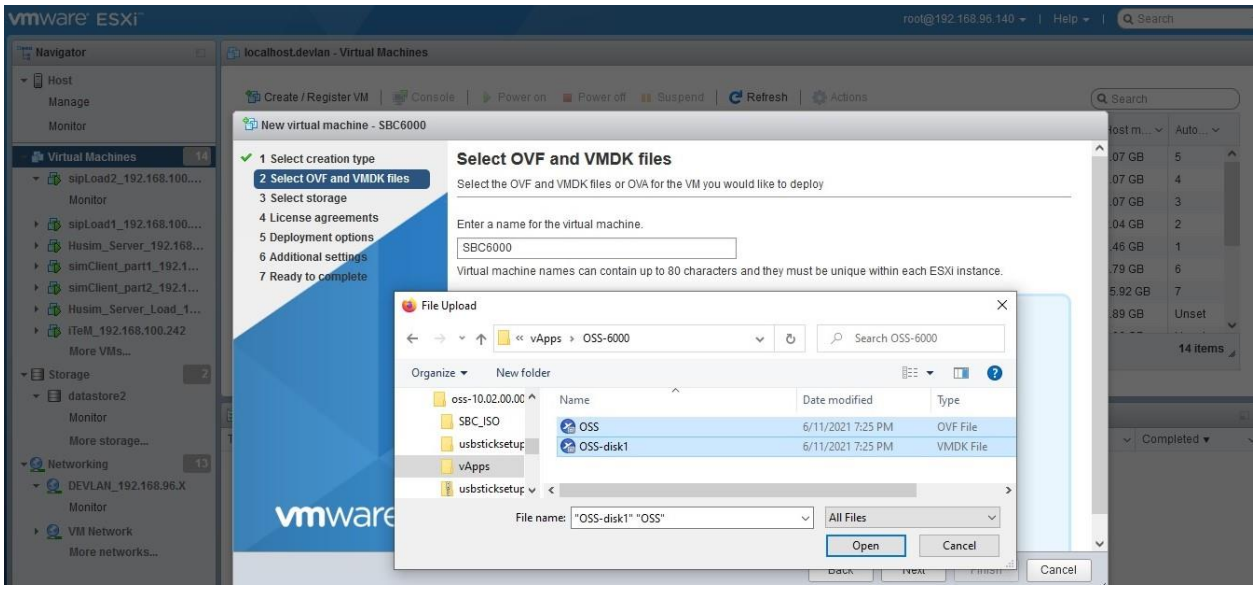


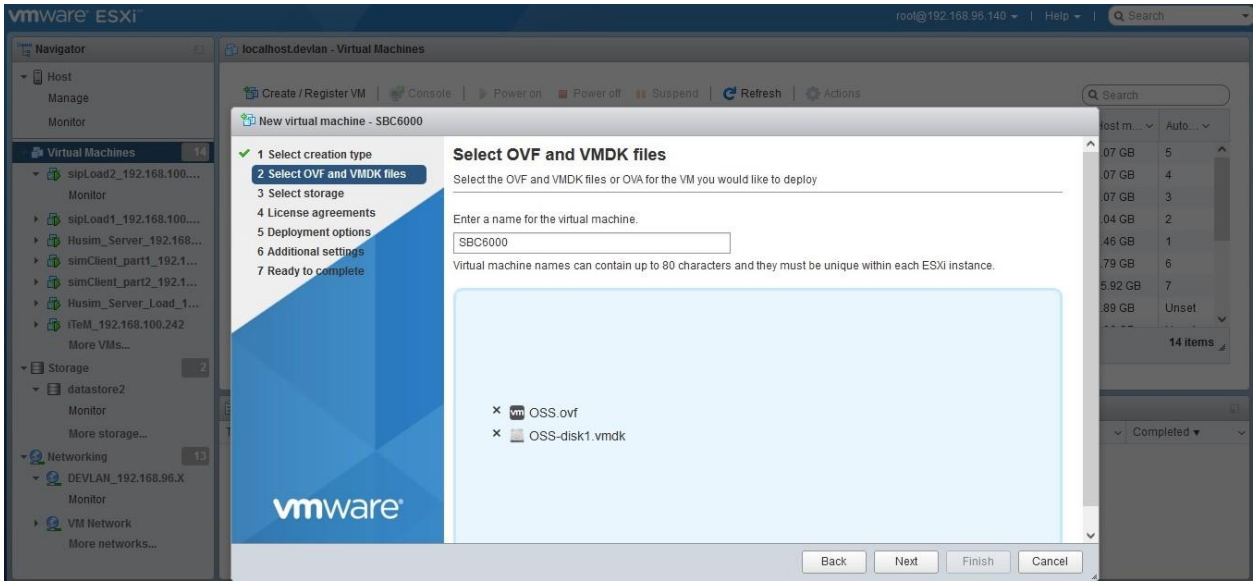
8. Enter a name for the virtual machine and click to select files.



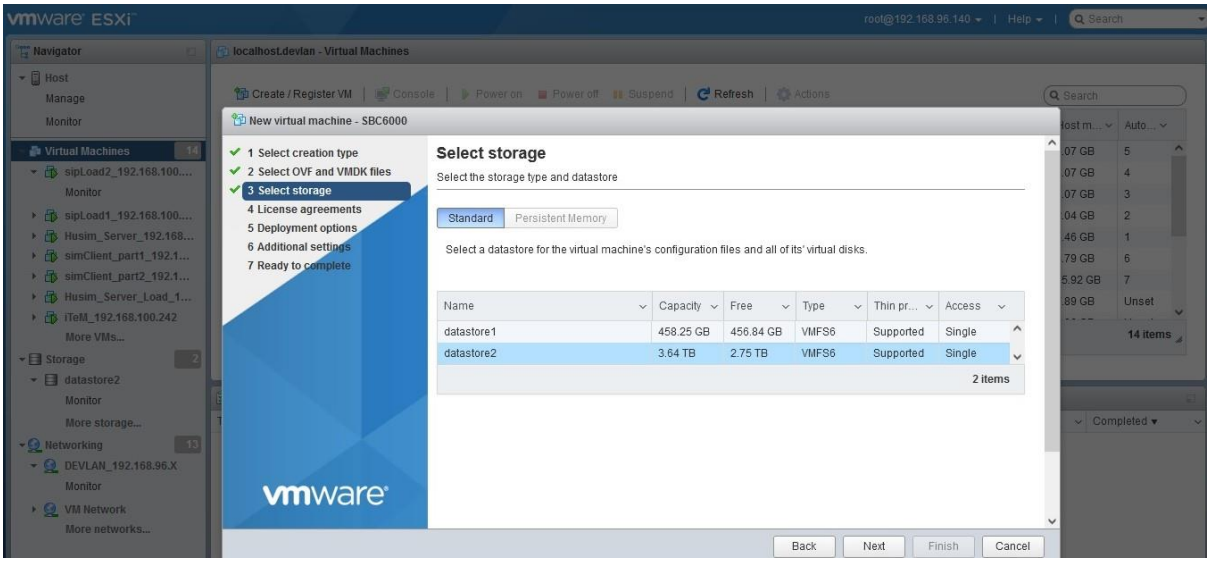
9. Select the **vApps** folder for the right OS-SBC type (OSS 250, OSS 6000 or OSS 20000).
10.Select the **OSS.ovf** and **OSS-disk1.vmdk** files and click **Next**.

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**.



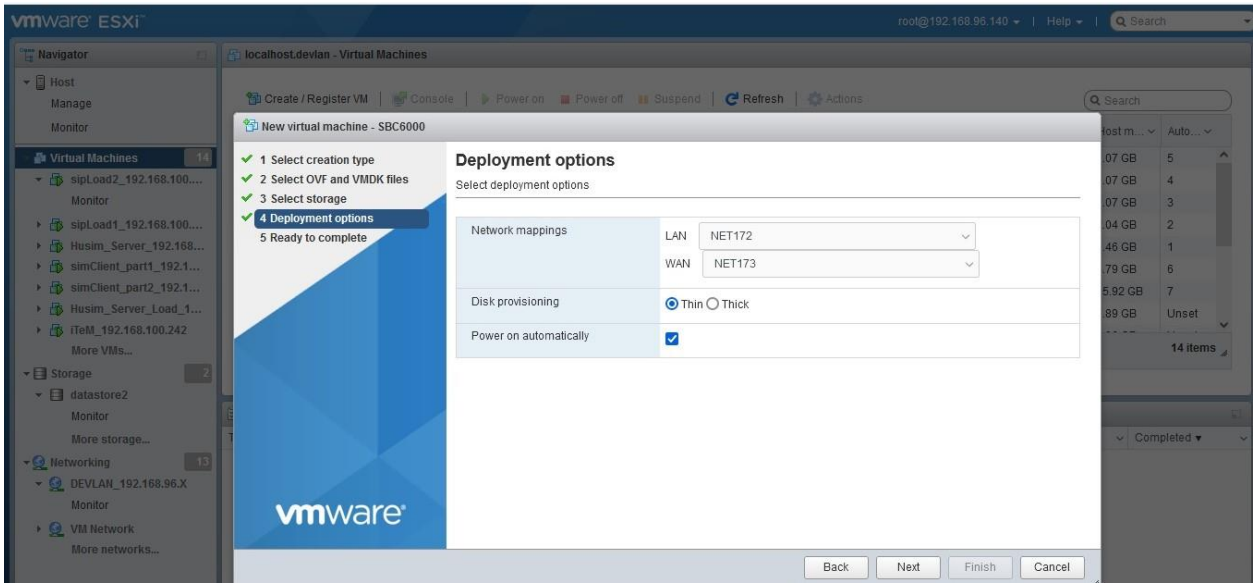
Map Network cards to ports and configure LAN and WAN options:

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.

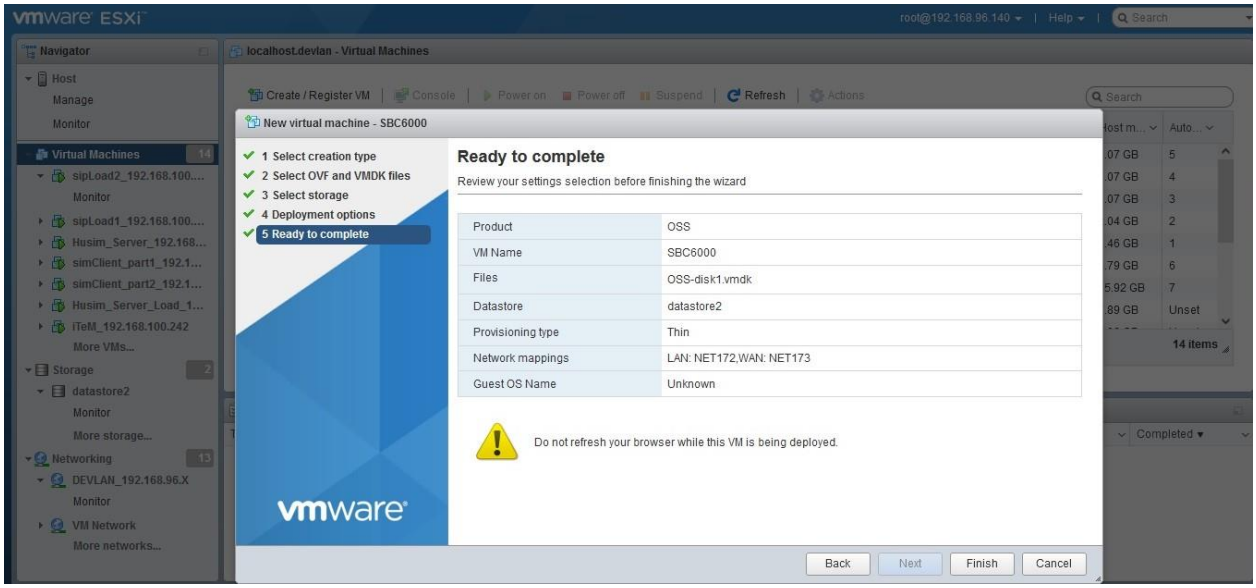
Note: Using thick eager-zeroed virtual disk reduces delays the first time that a block is written to the disk and ensures that all space is allocated and initialized at creation time.

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

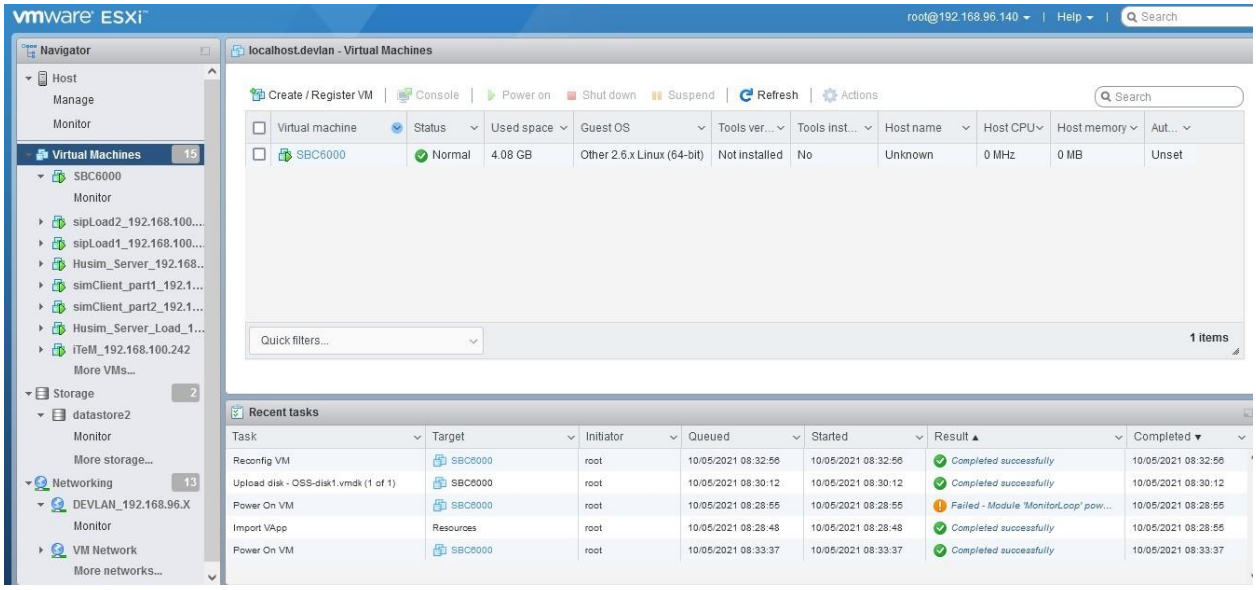


The virtual machine is ready to complete.

14.Click **Finish**.



The virtual machine has been created.



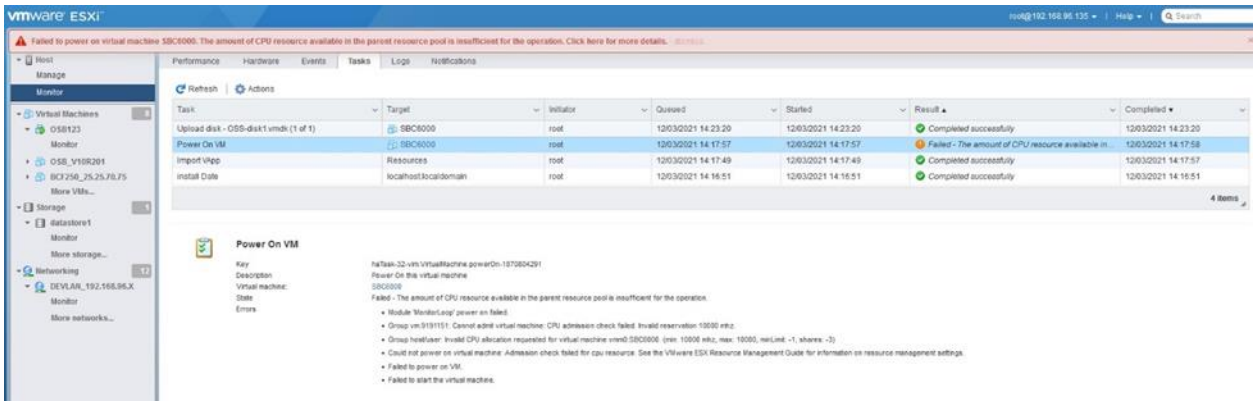
Note: When deploying vApps these values are set automatically (based on the 2.5 GHz core processor).
In OVF file in vApps, the CPU reservation is configured for Virtual OSS 250 (5000 MHz), Virtual OSS 6000 (10000 MHz) and Virtual OSS 20000 (20000 MHz).
Regardless if VM has been created manually or with 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

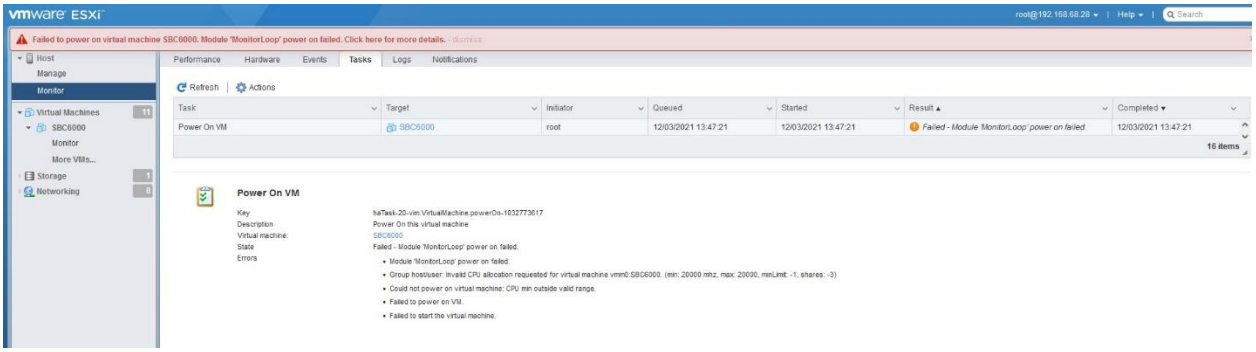
- Module 'MonitorLoop' power on failed.
- Group vm.8998268: Cannot admit virtual machine: CPU admission check failed. Invalid reservation 20000 mhz.
- Group host/user: Invalid CPU allocation requested for virtual machine vmm0:SBCConfigDemo. (min: 20000 mhz, max: 20000, minLimit: -1, shares: -3)
- Could 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:SBCConfigDemo. (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.

****

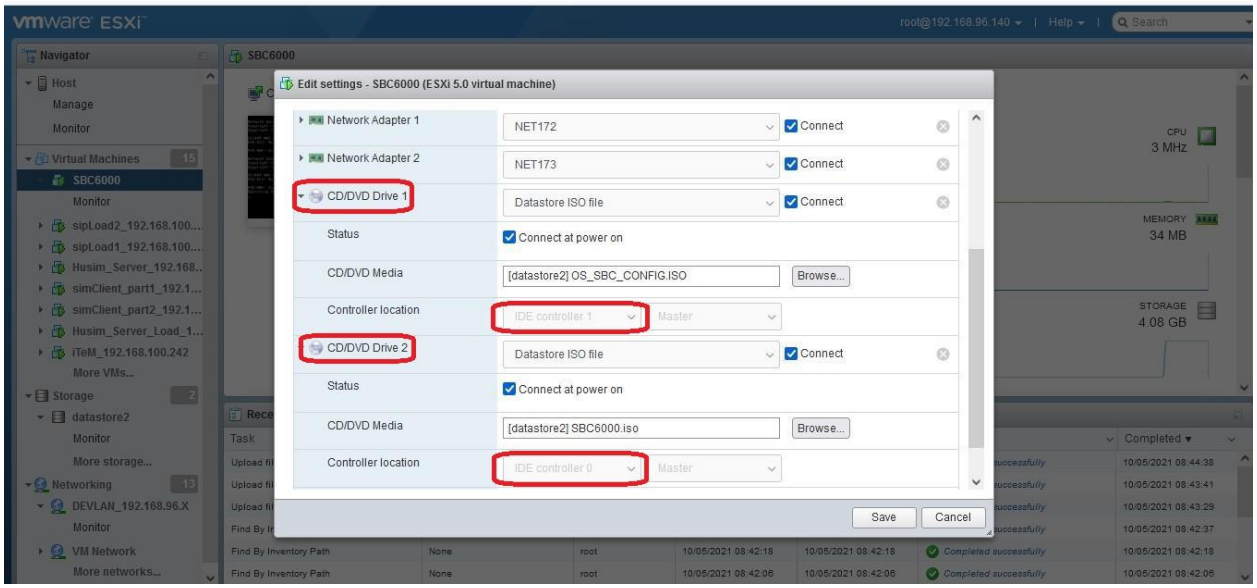
15. Click **Edit Settings** on your VM to attach the ISO image to the CD/DVD Drive.

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

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 penalty box.
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:

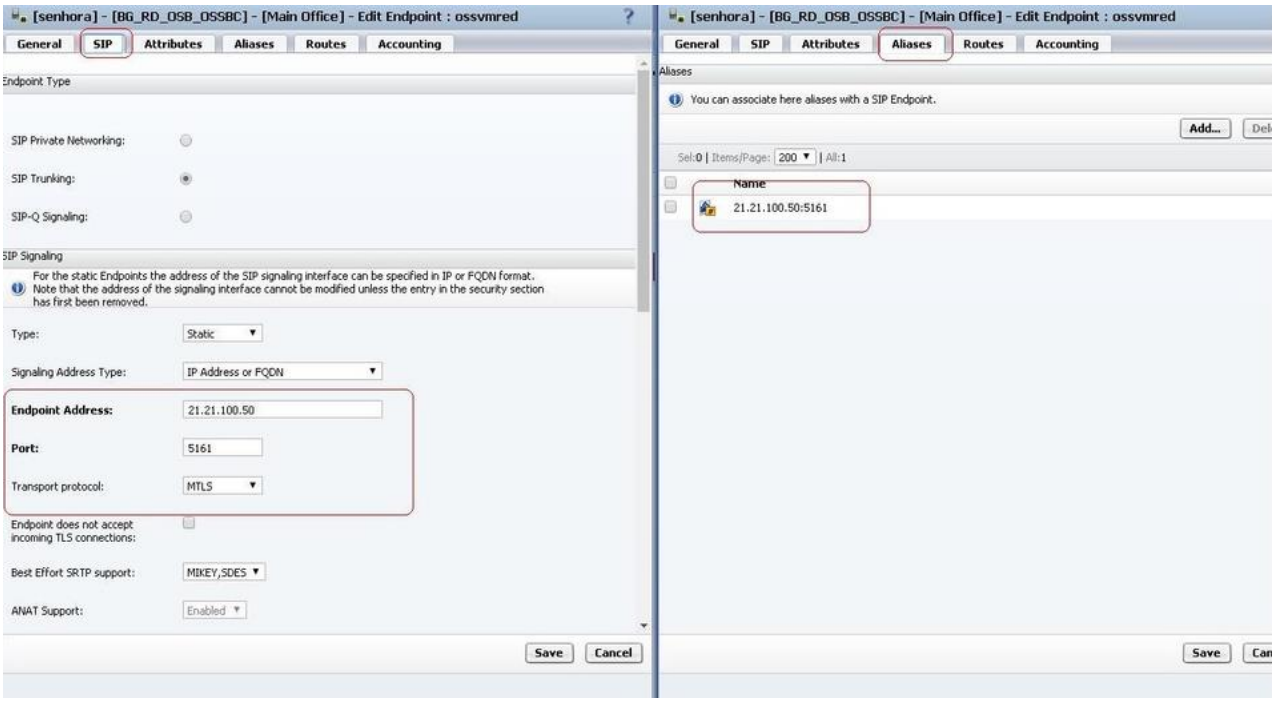
Create the OS SBC endpoint in OpenScape Voice. Configure the **Endpoint Address**.

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)".

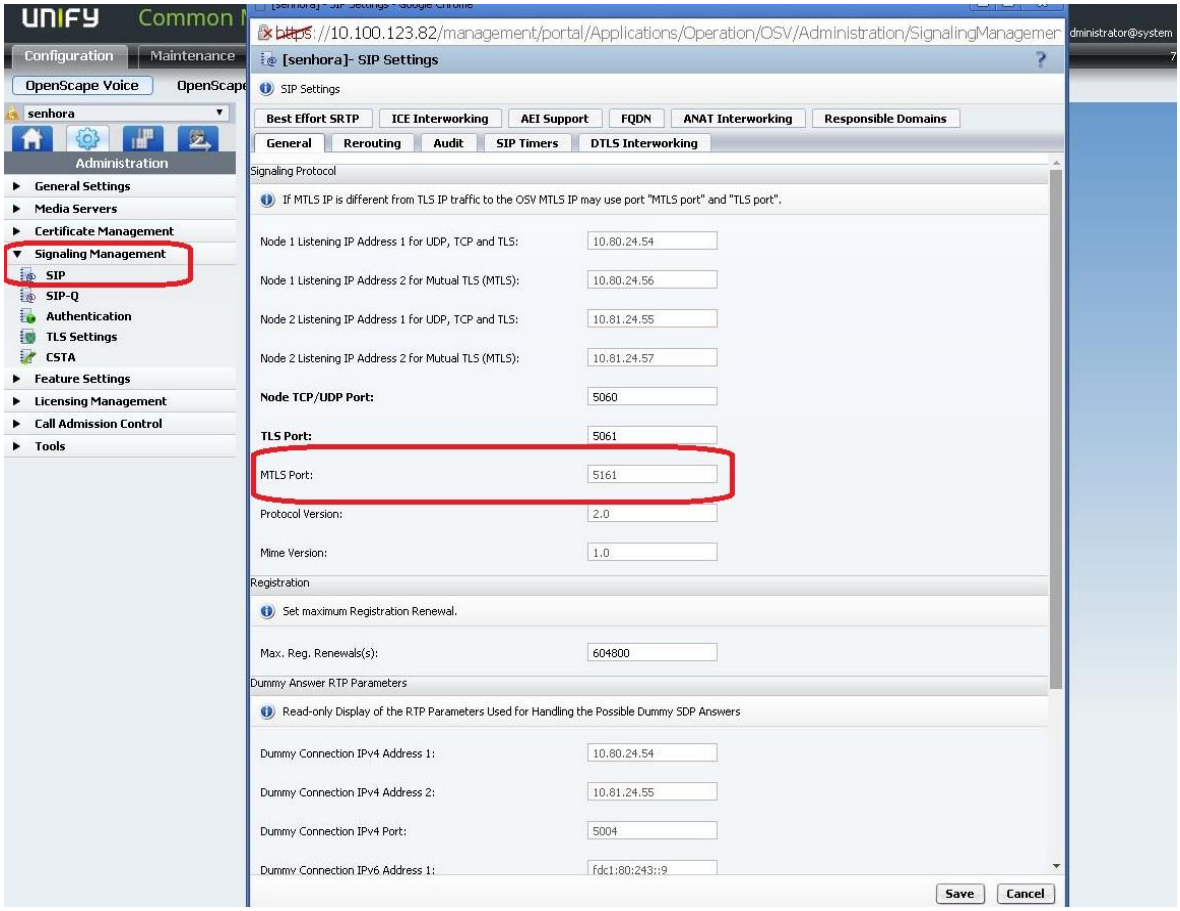
Configure the Aliases with the ip address and port.

Save the configuration.



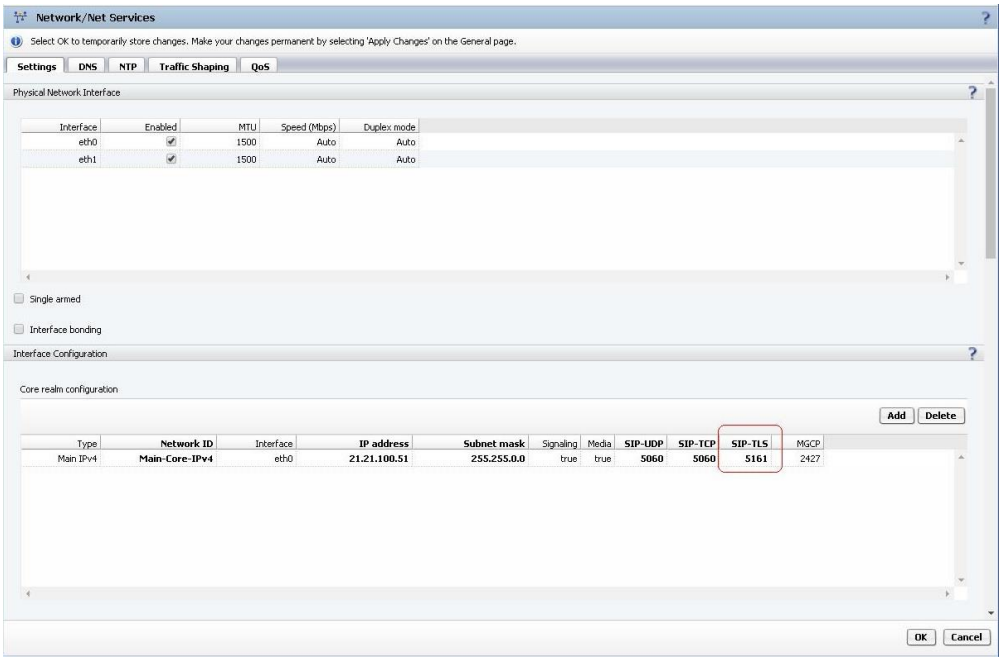
OpenScape Voice MTLS port configuration

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



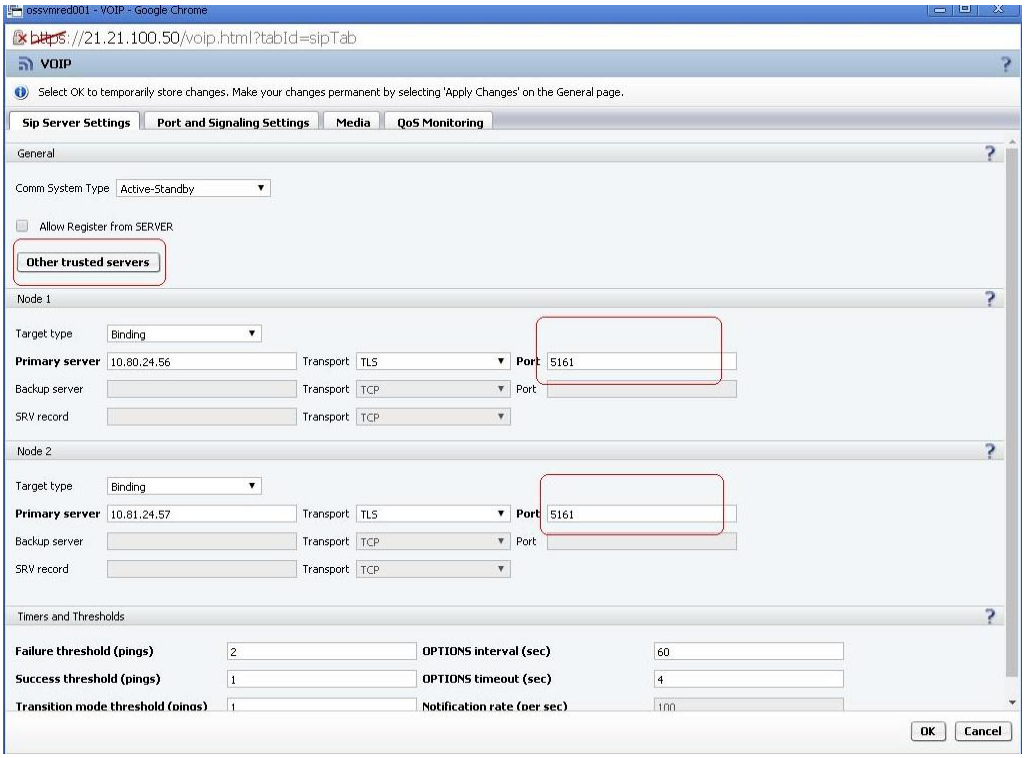
Configuration in OS SBC

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



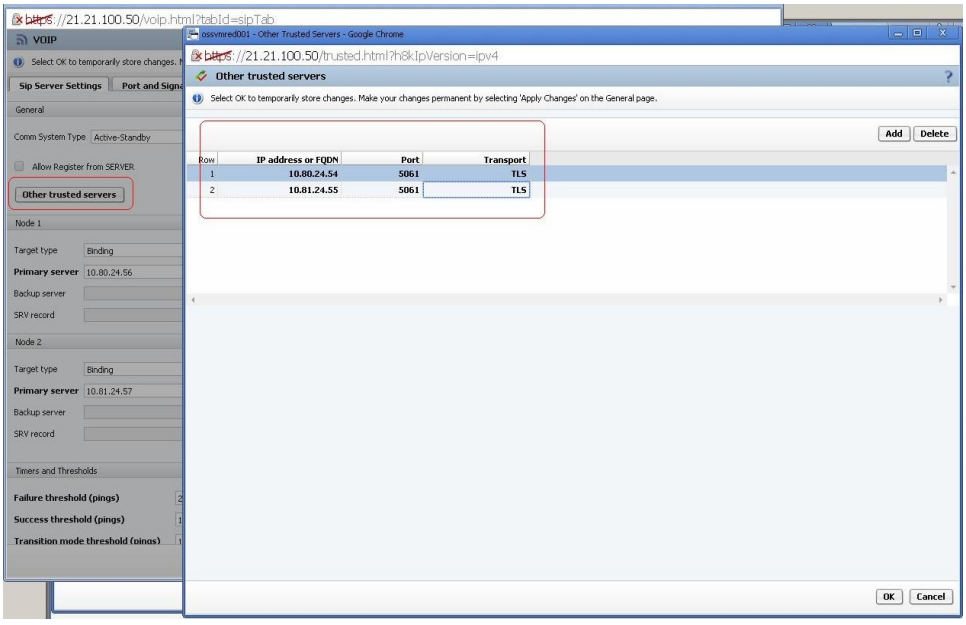
b) Under folder **VOIP/ SIP Port Settings** configure the OSV's MTLS addresses for OSV Node1 and Node2. Use the information described in the item 3.4.4.1.

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).



c) <u>Configure the other trusted servers in OS SBC</u>:

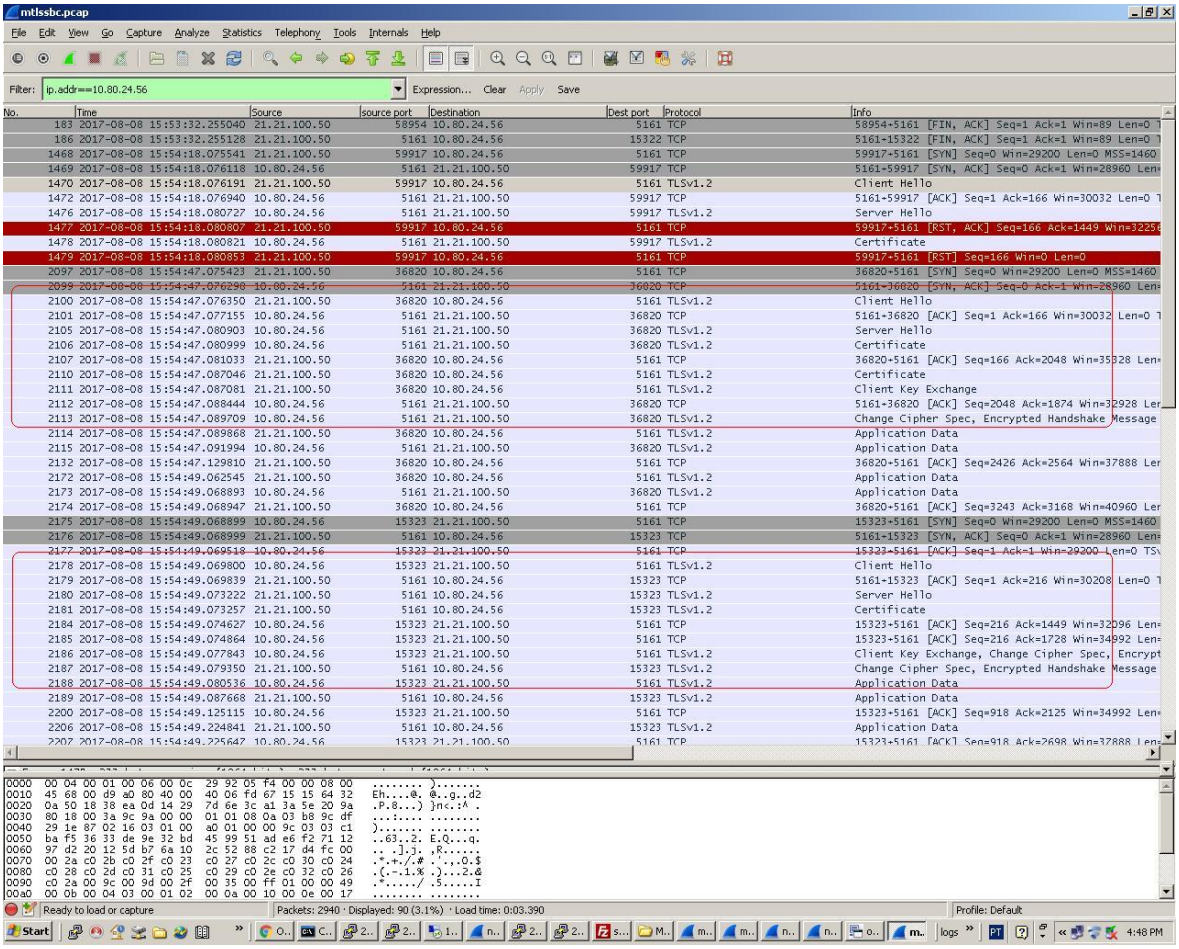
In this case it was configured **sipsm1_vip** and **sipsm2_vip** for OSV Node1 and Node2.



Wireshark example

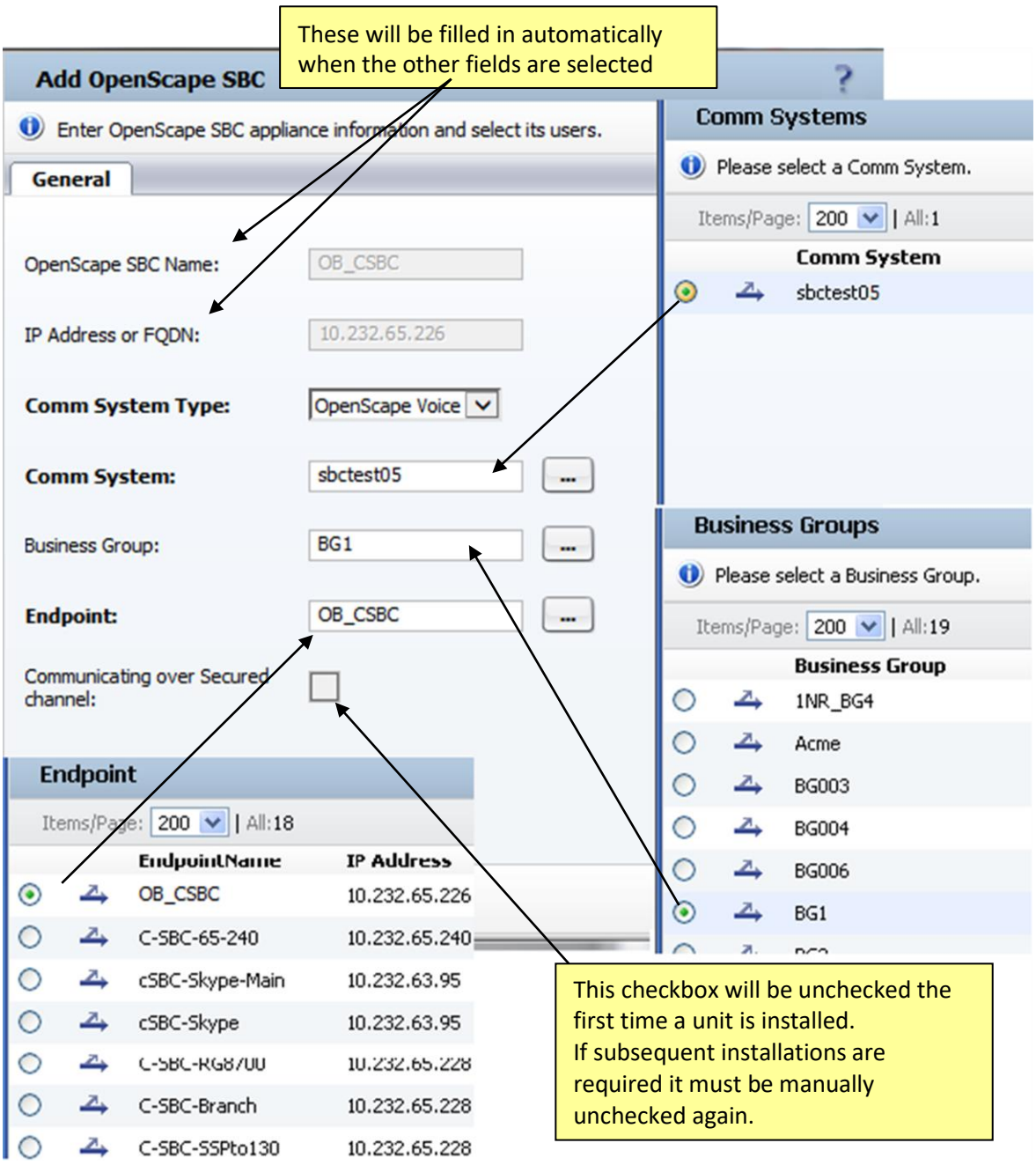
See the messages Client and Server Hello.

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

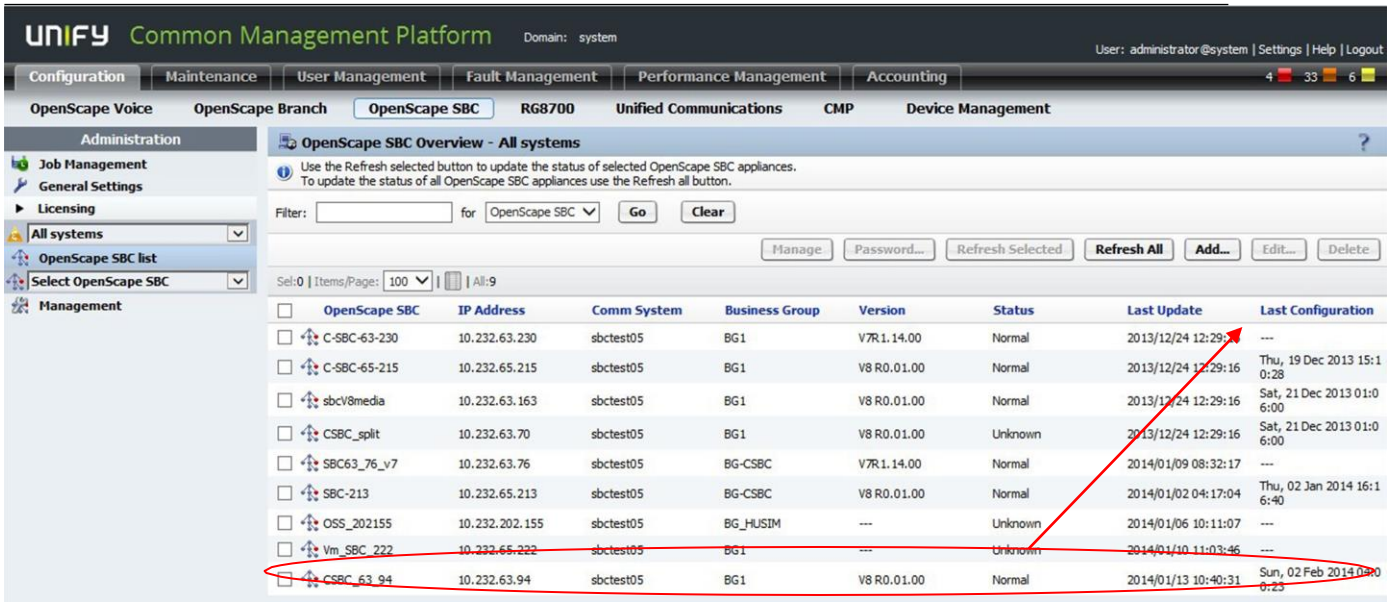


3.2.4 Add an appliance to OpenScape SBC list

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



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



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">

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:

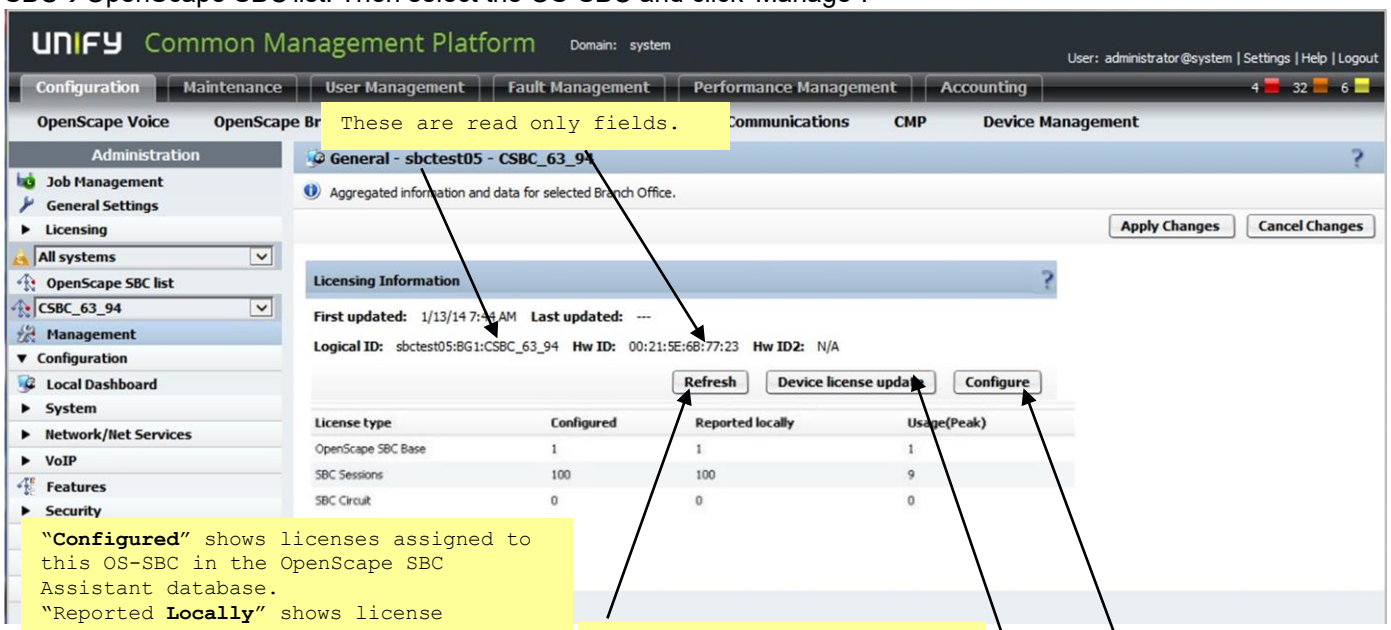
1. Exchange of authentication statements
2. Logical ID of OS-SBC, and
3. Hardware ID of OS-SBC

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”.



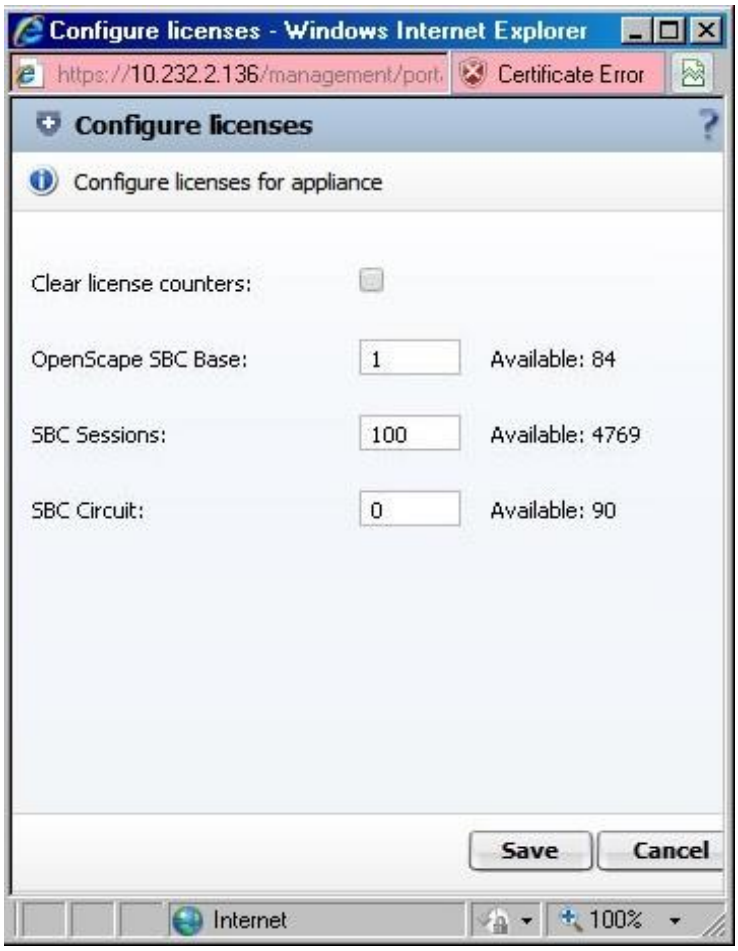
These are read only fields.

“**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.



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.

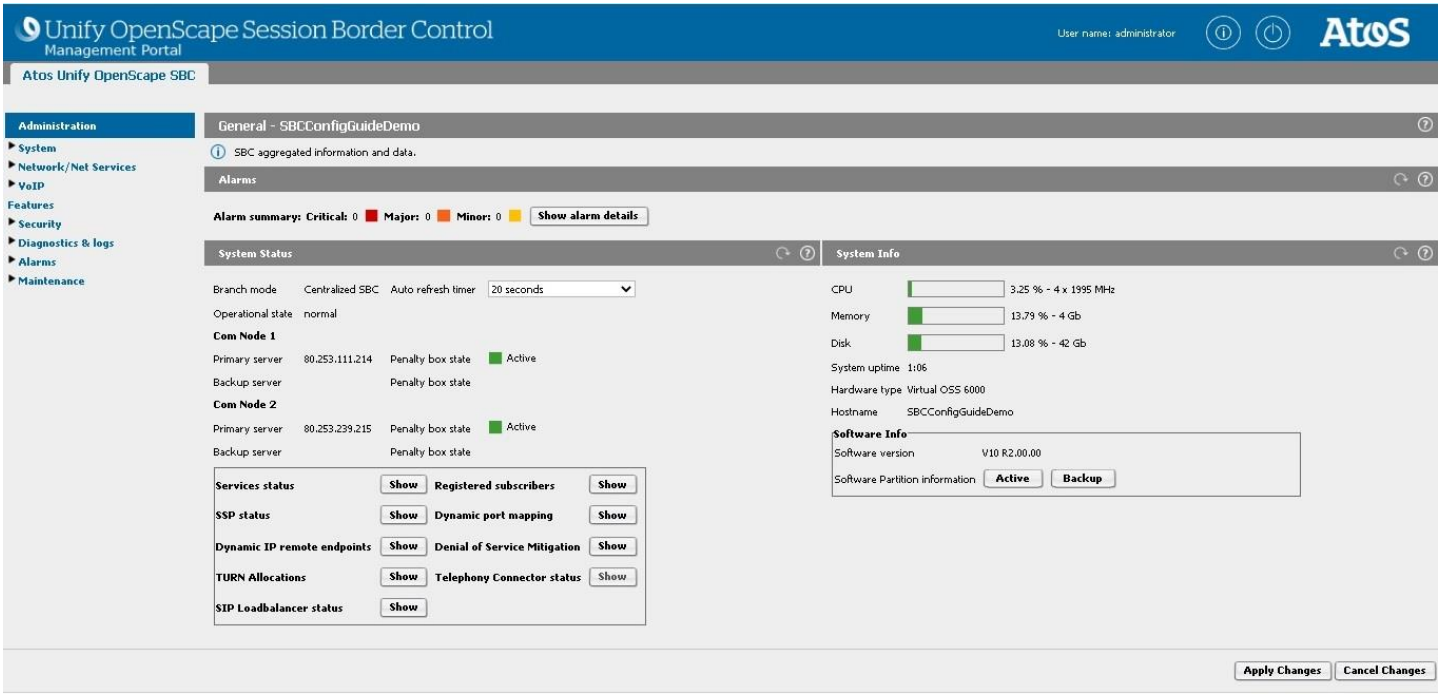
An established SBC session where no RTP packages are not exchanged for 3 min will be dropped after (15~18 min), no alarm is generated, only ssm logs in certain level will show dropped sessions.

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

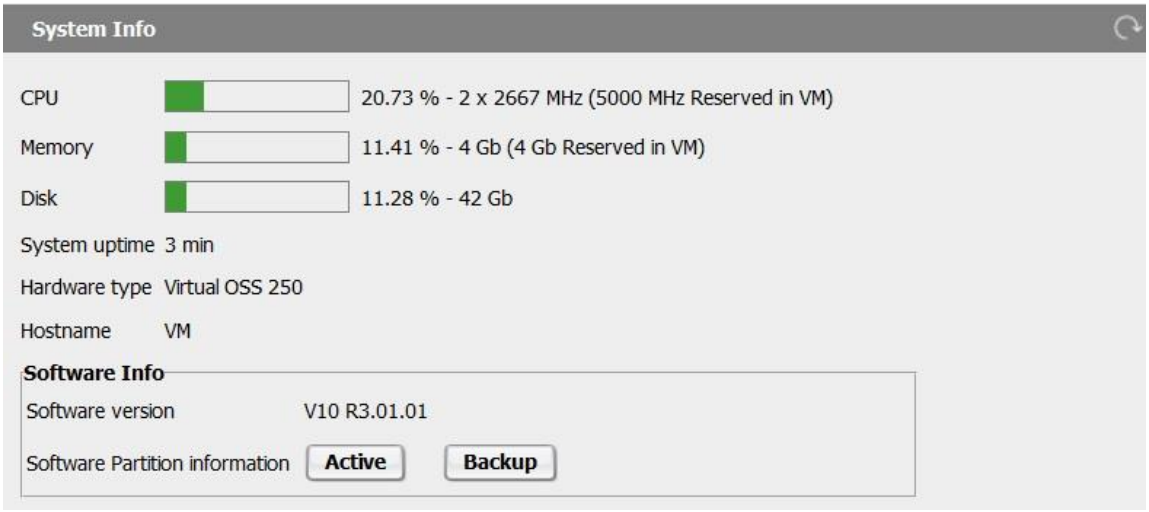
For sessions with media optimization where the RTP packages are exchanged directly there is no audit, therefore is always recommend to use session timers between parties, this will avoid hung session is case of missing BYEs. To overcome this in the Port and Signaling Settings a configurable timer to 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



3.4.1.1 System Status and info



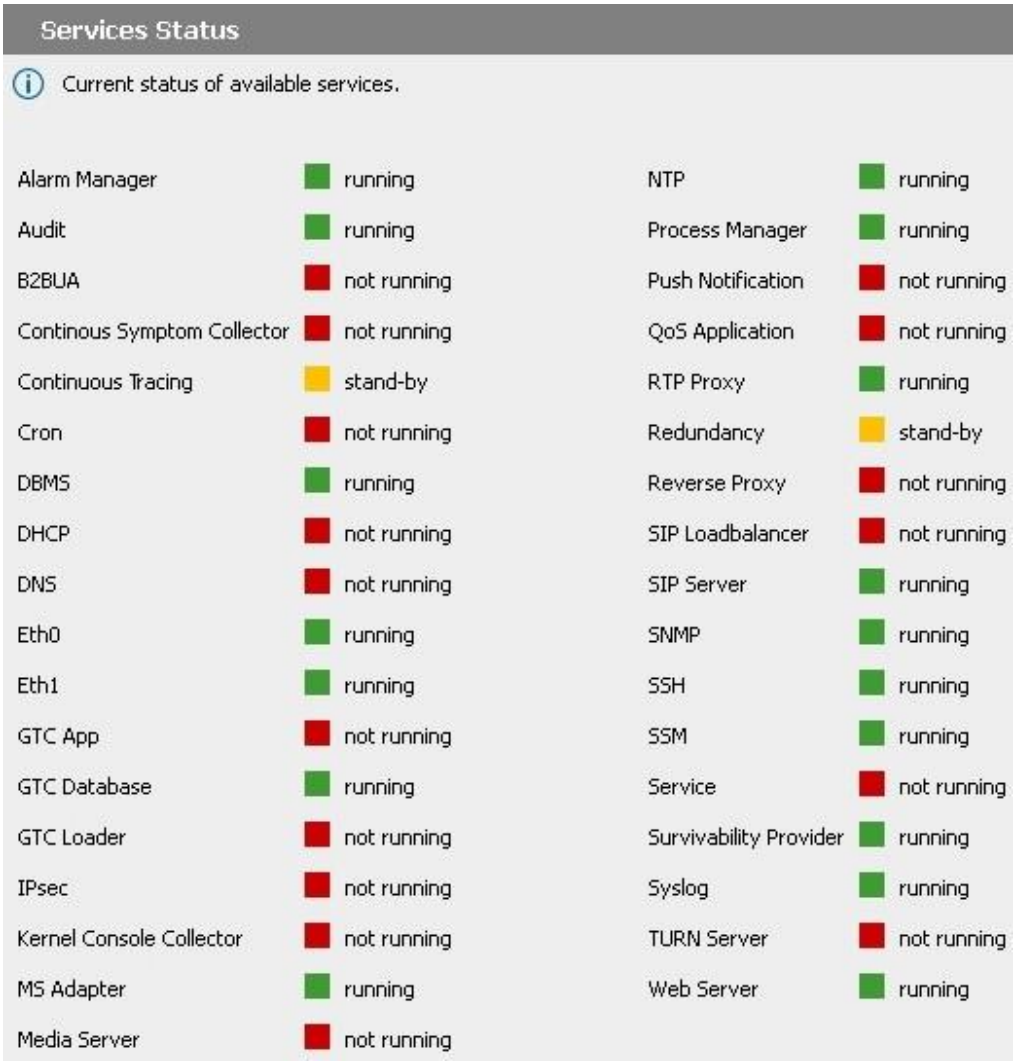
Operational state shows the system connectivity with the central SIP Server. The state "normal" indicates full connectivity to primary and/or backup server.
'Survivable' mode status is only relevant internally and transition to survivability mode (when OSV nodes become unreachable) does not initiate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

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

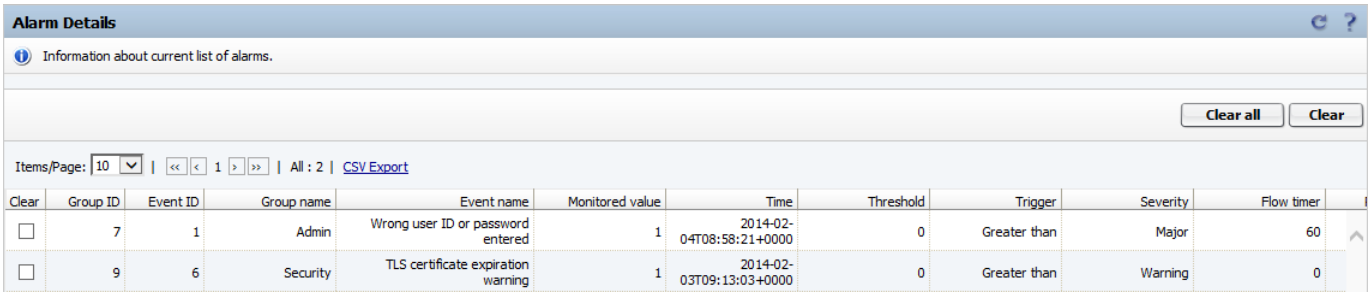


NOTE: Some services are not enabled by default

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

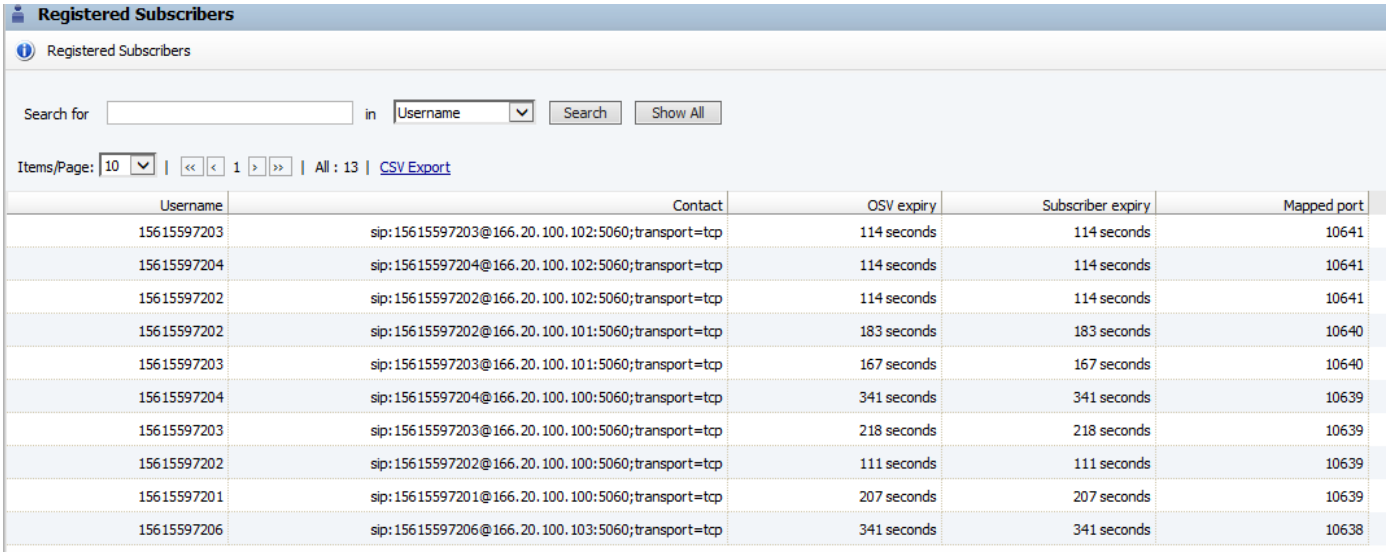
These services will **NOT** run in **Backup mode**: `ipsec, named, zooclient, kamailio, sp, bcfMonitor, push, msadapter, redis, haproxy, turnserver, gtc, siplb, gtcloader`

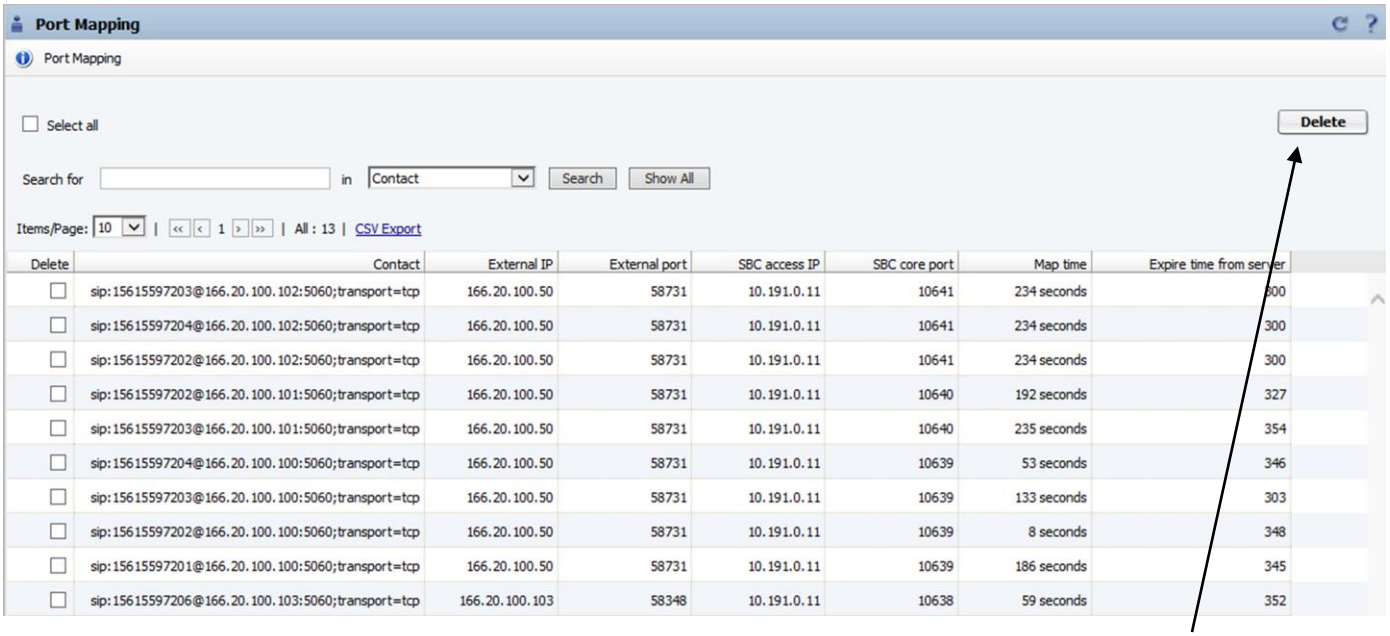
- **Peer Monitoring** - The application is responsible for monitoring peers using OPTIONS messages. It is utilized for the SBA, the endpoint connectivity checks in the "Standalone with internal SIP Stack" mode, and in OPTIONS with alias port on the core side.
  Note: This option is only available in V11R1.01.00 or higher.



Clear	Group ID	Event ID	Group name	Event name	Monitored value	Time	Threshold	Trigger	Severity	Flow timer
☐	7	1	Admin	Wrong user ID or password entered	1	2014-02-04T08:58:21+0000	0	Greater than	Major	60
☐	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





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.

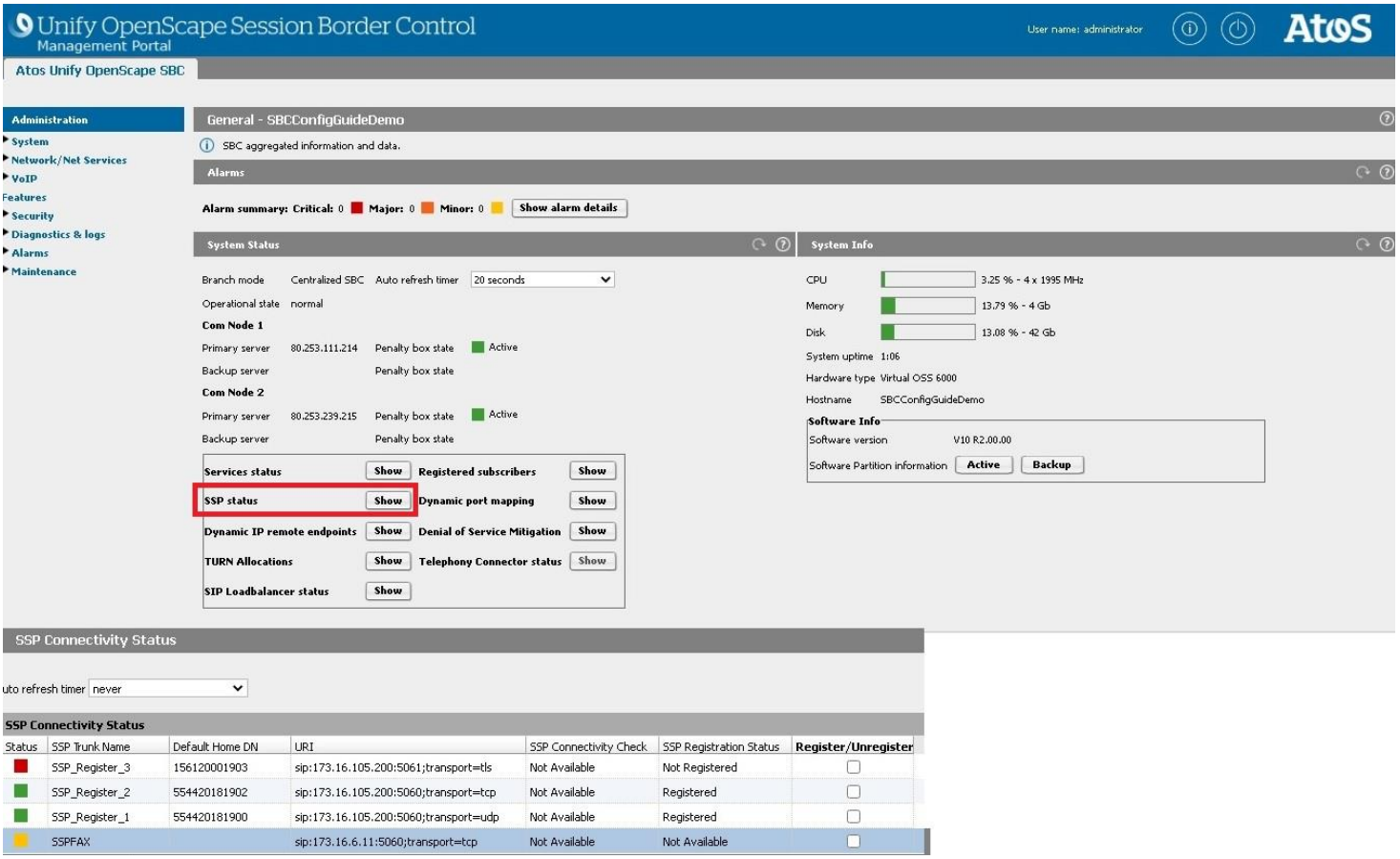
Note: Each registered key appearance counts toward the platform limit for registered subscribers.

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

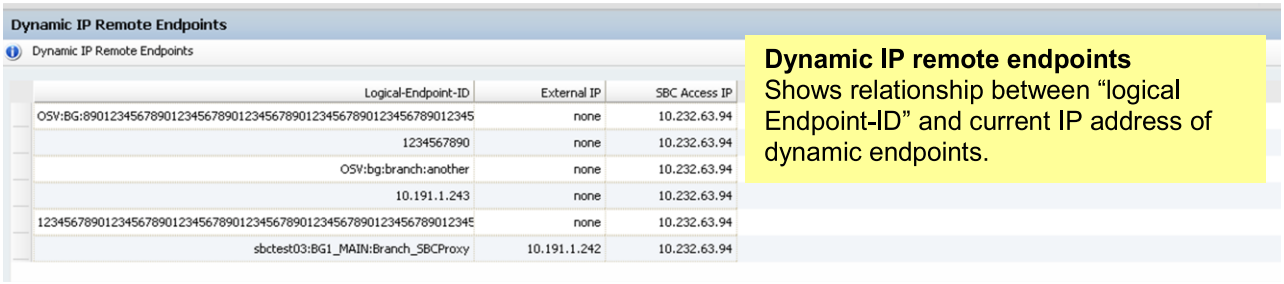
3.4.1.4 SSP Connectivity Status

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.



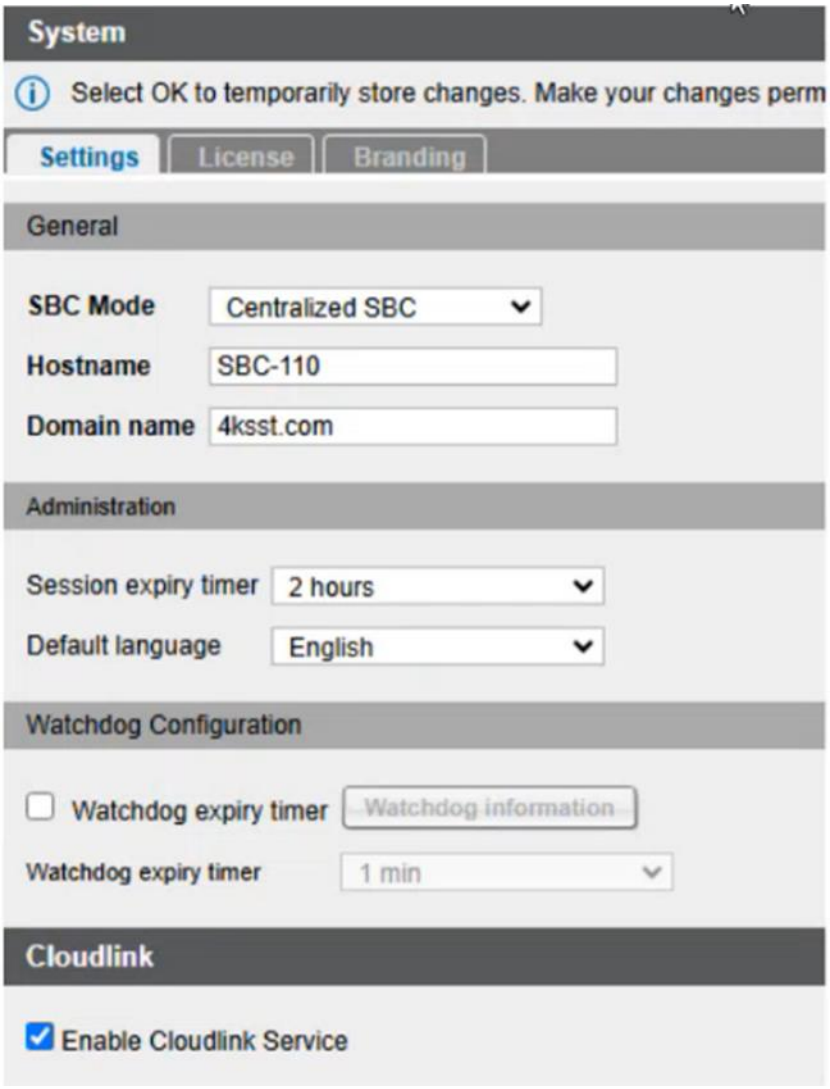
3.4.1.5 Dynamic IP Remote Endpoints



3.4.1.6 Denial of Service Mitigation display

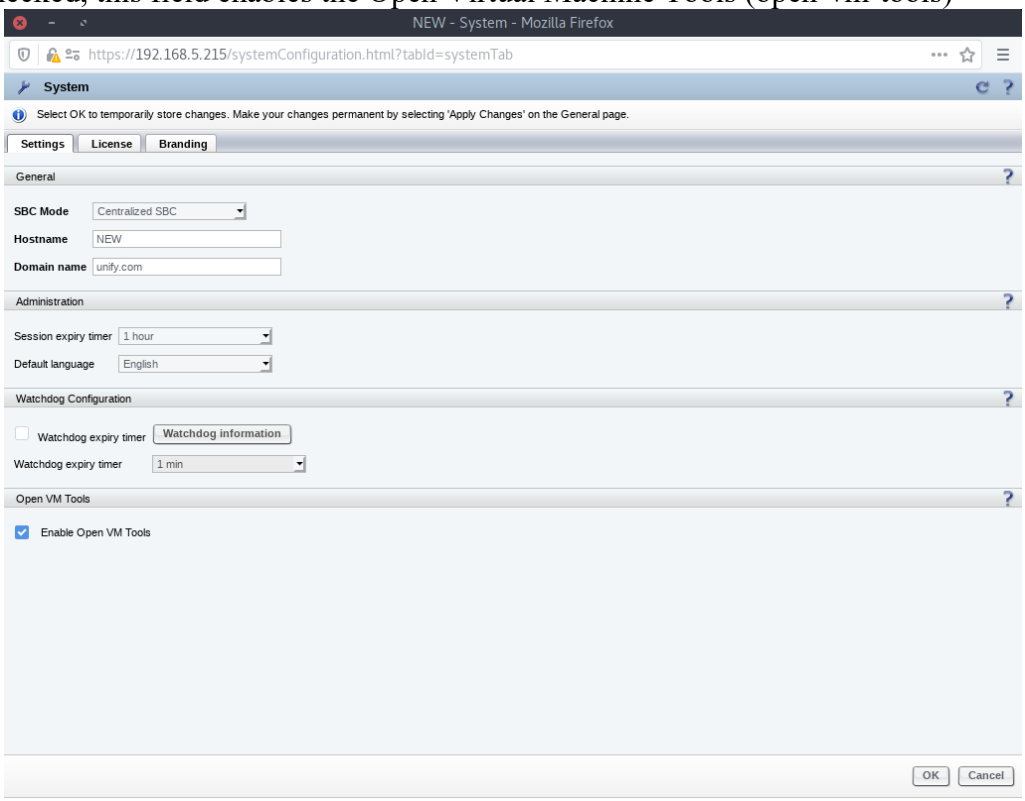
This shows the “Quarantine Grid” of Source IP addresses affected by denial of service blocking due to message rate limit violations only. The list may be searched by IP, quarantine TTL or network ID. Selected devices may be unblocked from this screen.
Refer to Denial of Service Mitigation
Quarantine Grid for Unauthorized/Unknown Users shows the IP:Port and Expire time of Unauthorized/ Unknown Users.

3.4.2 System Settings

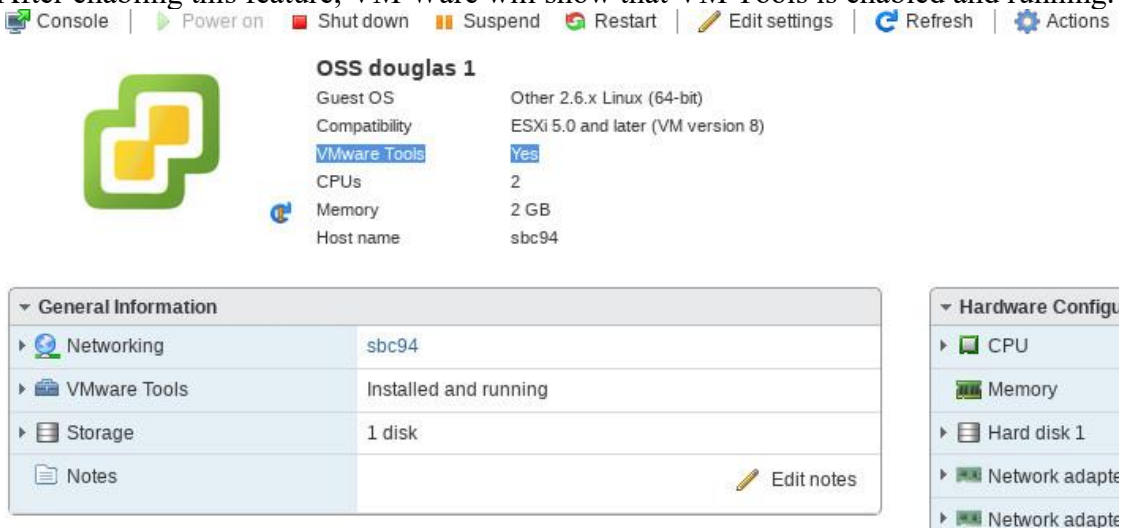


3.4.2.1 Enabling Open VM Tools

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



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



3.4.2.2 Connecting OpenScape SBC to CloudLink Daemon

If your communication system is OpenScape Voice or OpenScape 4000, the OpenScape SBC must beproperly configured to establish a connection with CloudLink. This configuration enables the routing of callsfrom the communication system to Zoom Phone.

To facilitate this connection, the OpenScape SBC administrator is required to complete specific tasks usingthe OpenScape SBC Assistant (version V10R2.4.0 or later). For OpenScape SBC, CloudLink also servesas the platform for transmitting mobile push notification requests to the Zoom Service.

Prerequisites:
1. Adequate administrative permissions.
2. The CloudLink Daemon RPM is installed. For more information, refer to the "Searching for RPMs" section, included in the Using osc-setup for handling Repositories chapter of the OpenScape UCApplication V10 Installation Guide.
3. CMP is connected to CloudLink Daemon. For more information, refer to OpenScape Common Management Platform.

To connect OpenScape SBC to CloudLink Daemon:

1. Log in to the OpenScape SBC Assistant.
2. Navigate to the **System** > **Settings** tab.
3. To enable the SBC-CloudLink connection, check the **Enable Cloudlink Service** checkbox.
4. Click **OK**.

You are redirected to the main page, where the SBC Dashboard displays the **CloudLink status**.

5. To activate the SBC-CloudLink connection information, click **Show** next to the **Cloudlink panel** item.

The CloudLink Daemon window pops up. By default, CloudLink is disconnected.

6. Click **Link to CloudLink** to connect to the CloudLink server.
7. Enter your credentials in the sign-in pop-up window and click **Next**.

The CloudLink Daemon window displays the connection details.

Note: Upon a successful connection, an inventory report is generated and refreshed approximately every 30 minutes.

8. To configure tunnels and enable the SBC UI within CloudLink:
    - In the **Tunnels** section of the CloudLink Daemon, click **Start** next to the OpenScape SBC component.
    - Click **Yes** to confirm.
    - Log in to CloudLink Daemon with the same credentials used in the previous step.

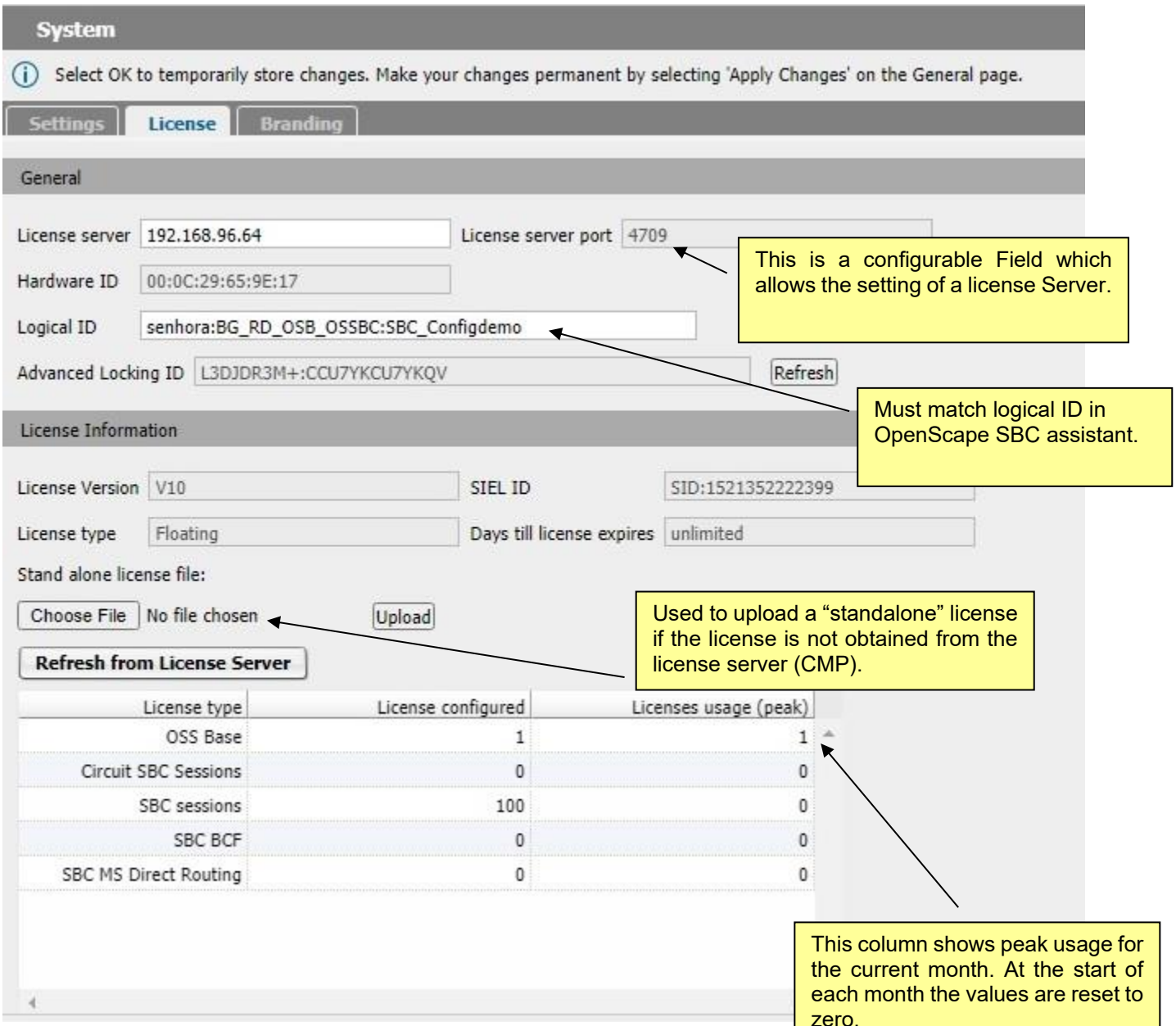
You are connected to CloudLink.

10. Optionally, you can view system information and launch a remote SBC configuration:
    a. From the left-hand menu, click the **System Inventory** drop-down to expand it.
    b.To view the SBC(s) connected to CloudLink, select **Platforms**.
    c.To perform a remote SBC server configuration, select **Applications**, then click **Launch**.

    Note: The **Launch** button becomes active only after the tunnel has been successfully established.

To disconnect from CloudLink, click **Disconnect from CloudLink** in the main CloudLink window.

3.4.2.3 Licenses



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

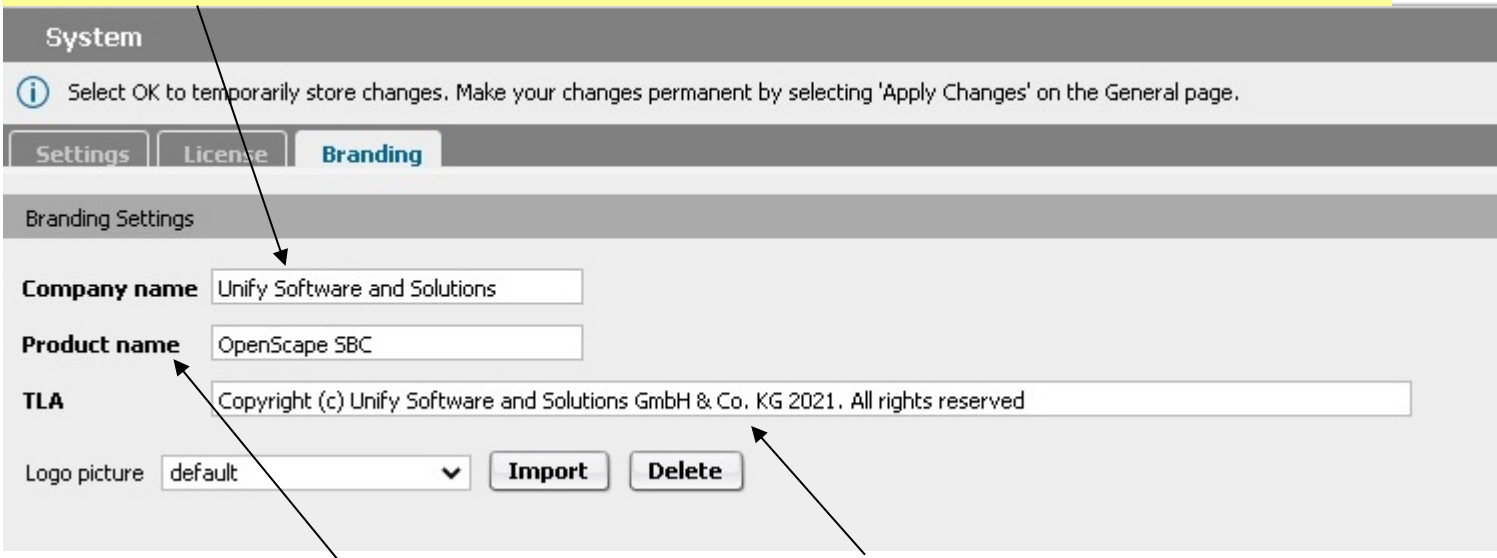
3.4.2.4 Branding

3.4.2.4.1 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.



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.

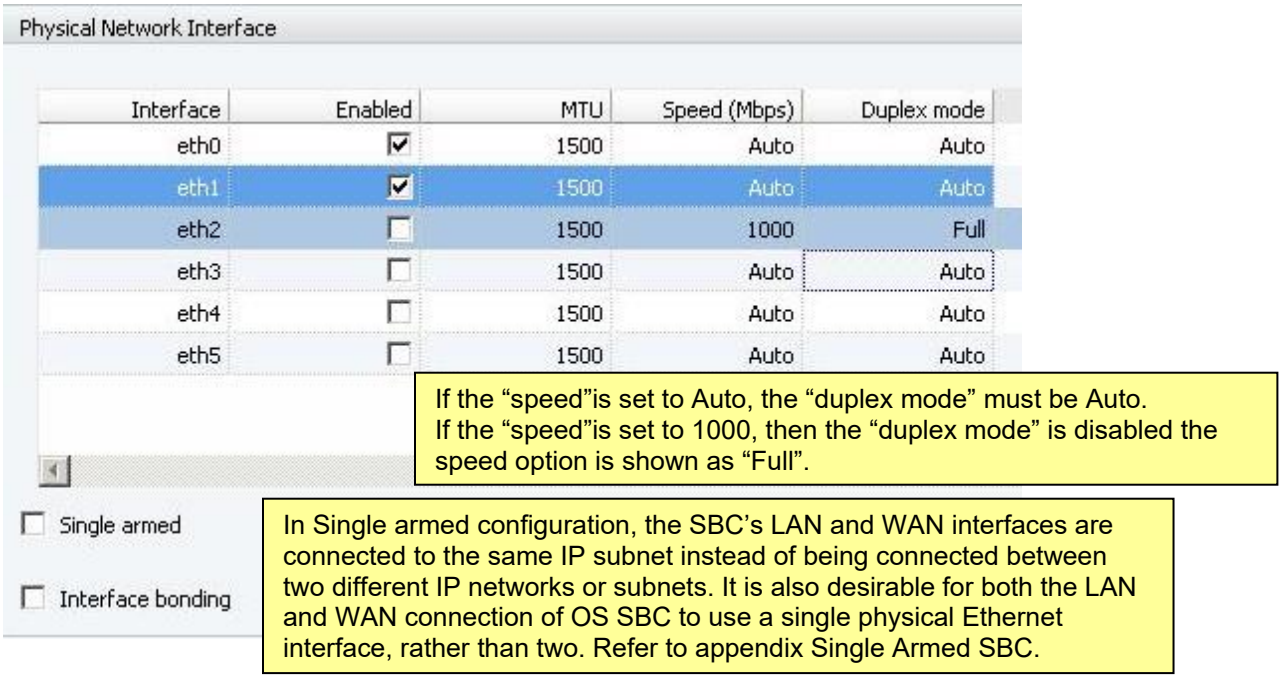
Trademark License Agreement can be entered here. This name can be made up of upper or lower case letters, digits, or special characters. Special characters can be any of the following set: !@#%&()_-+{}|:;'?/=,^$.*[]™©äÄüÜöÖ€µß and the white space.

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.

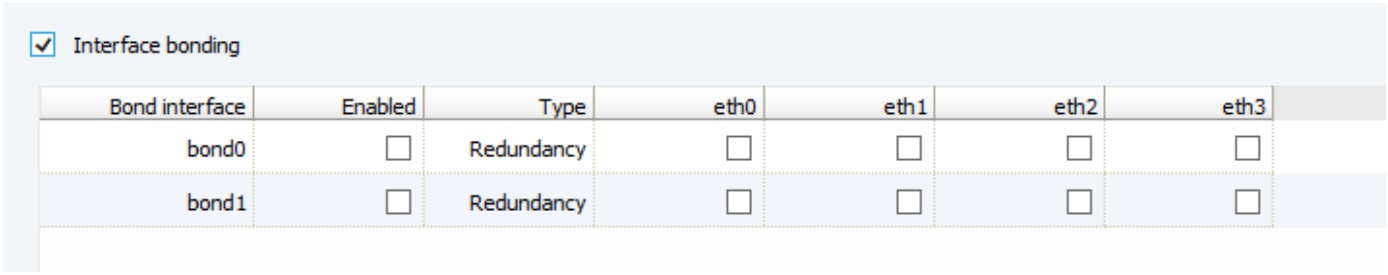
3.4.3 Network / Net Services

3.4.3.1 Physical Network Interfaces



3.4.3.2 Ethernet Bonding on LAN and/or WAN interfaces

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

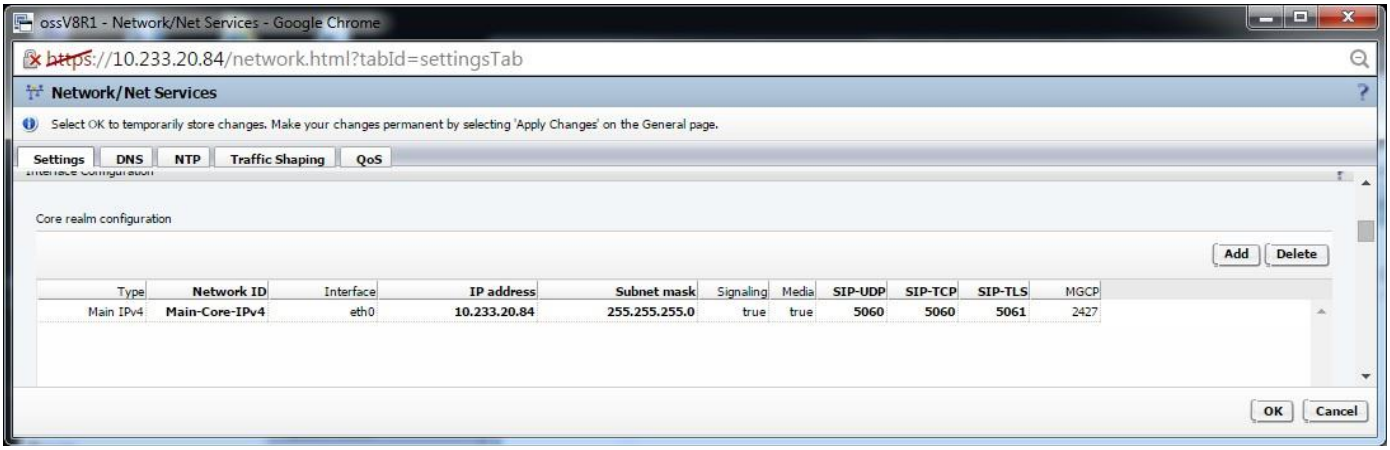


This allows the *available* Ethernet network interfaces to be bonded or teamed together to support network interface redundancy helping to prevent an SBC node Loss of Service in the event of a single EthernetNIC failure, local switching network failure.

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 Vlan IP
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

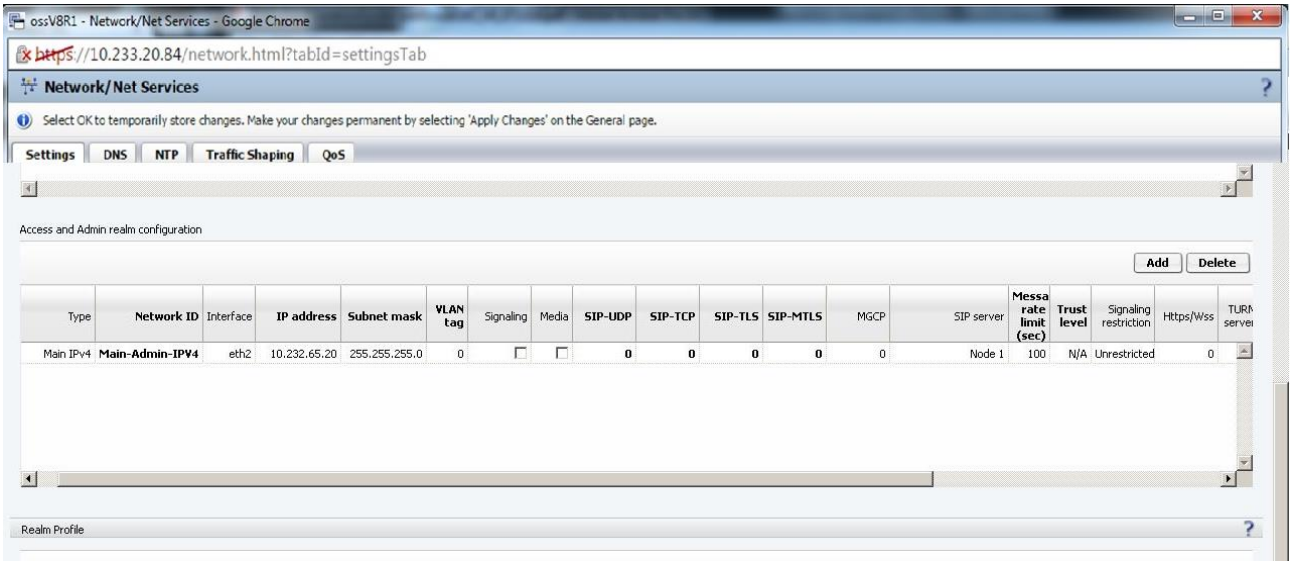
If a separate management interface is desired on the SBC and the physical hardware supports more than 2 interfaces, interface eth2 may be used. After connecting interface eth2 to the new management network, the SBC must be configured as follows to separate the management interface from the LAN interface. 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"

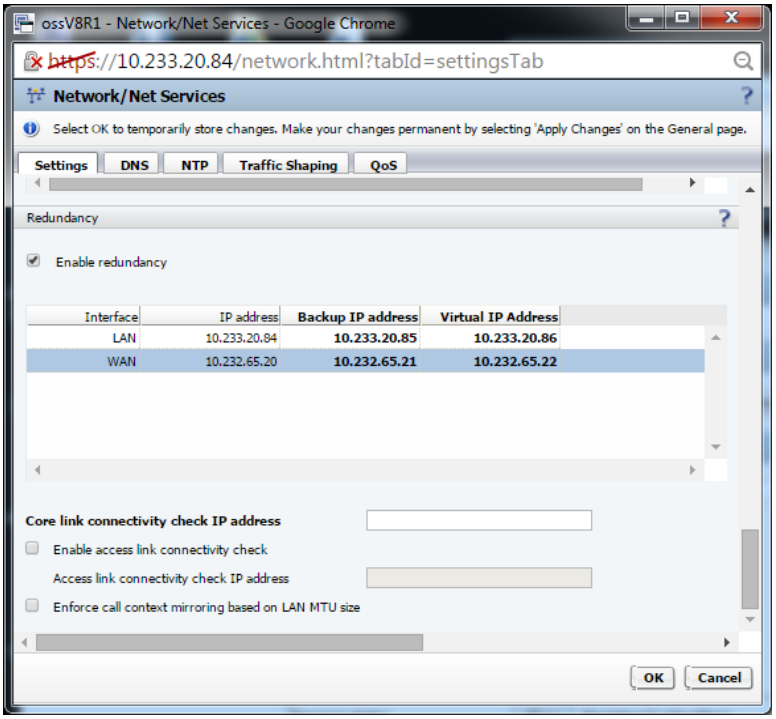
a. The fields “SIP-UDP”, “SIP-TCP”, “SIP-TLS”, “SIP-MTLS” and “MGCP” must be 0.
b. The fields “Signaling” and “Media” must be unchecked.



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”

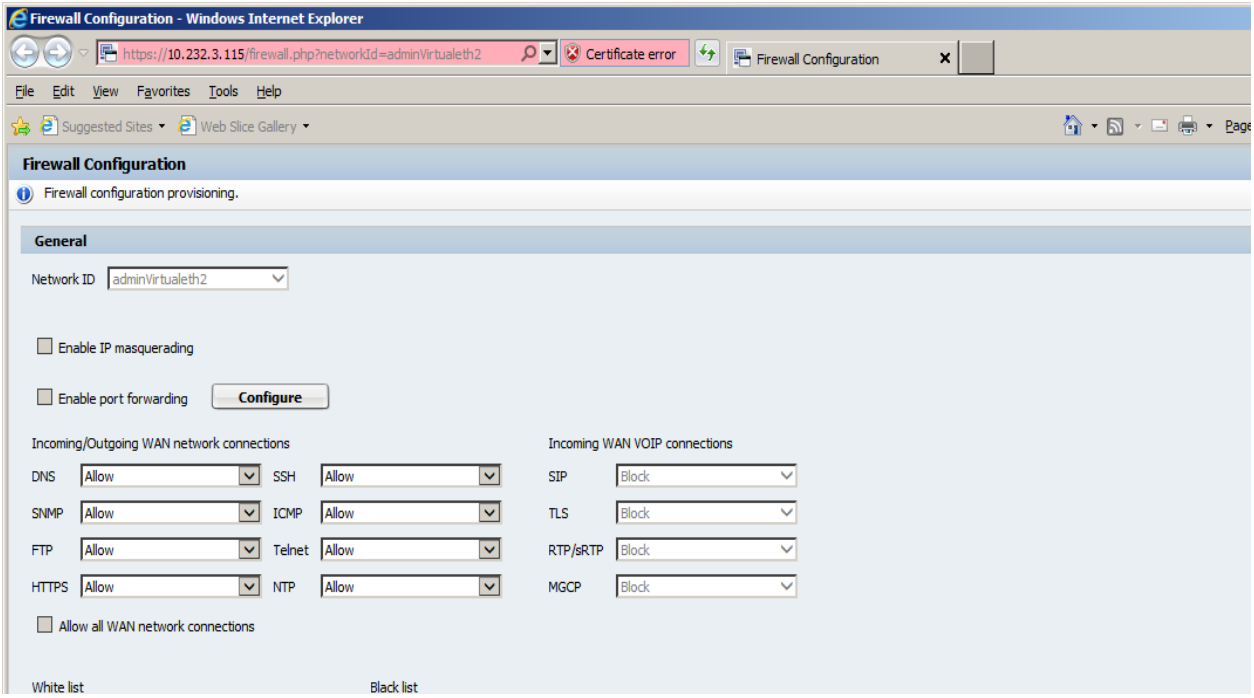
There are invalid field values: Enter a valid Backup IP address for Interface ADMIN in Redundancy list at row 3.

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 Network ID.
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.



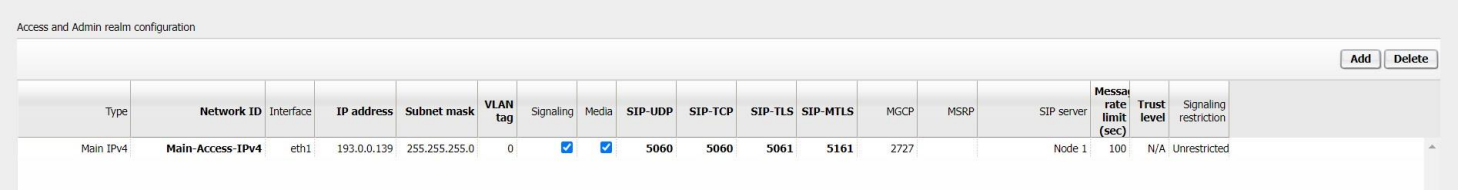
10. Once new Admin Firewall is configured then all unknown admin access on the LAN interface from outside is blocked.
11. If HTTPS access is not allowed on the new Admin firewall then it would be automatically enabled on the LAN interface in order to avoid no Admin access.
12. Since NTP or DNS servers 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



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

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 core realm

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	☑	☑	**5060**	**5060**	**5061**	**5161**	2727	
VLAN IP	**Main-Access-VLANIP**	eth1	0.0.0.0	0.0.0.0	173	☐	☐	**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**	

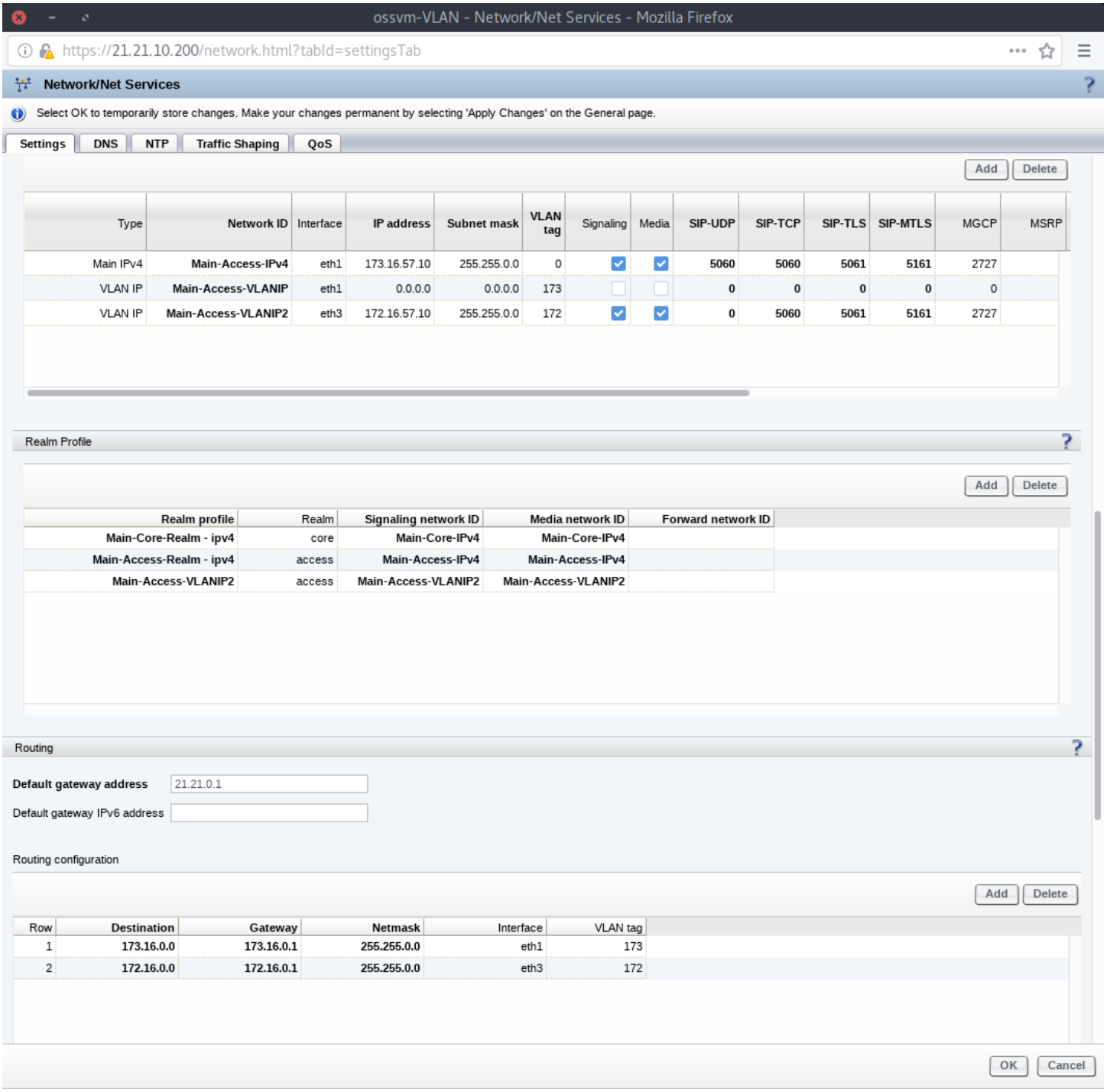
Routing configuration

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.

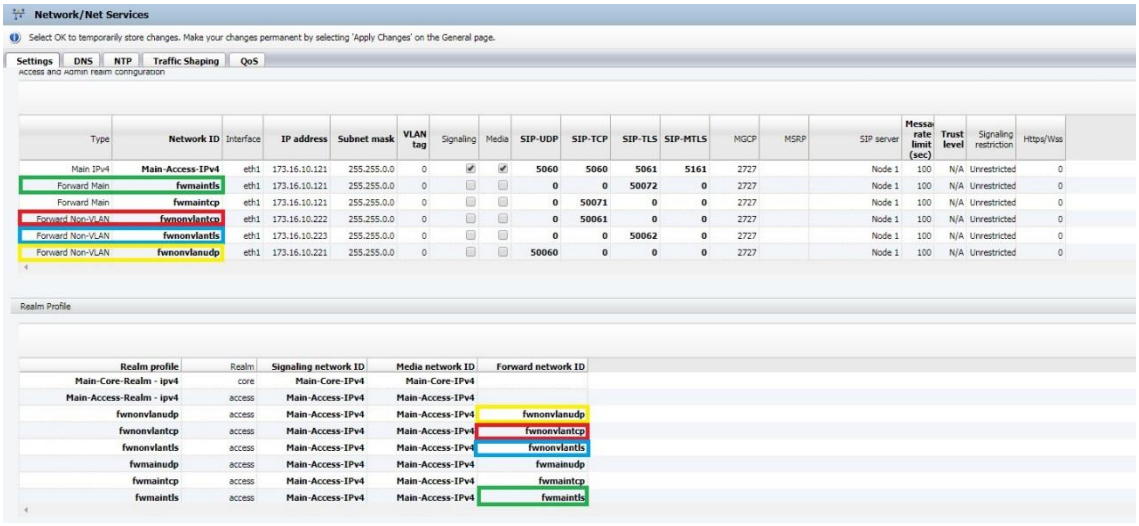
SBC can support several VLANs to the same access Ethernet interface. Each VLAN will have its own IP address tagged with the specific VLAN ID.
For each created VLAN IP there is a need to add the routing table entry, so that SBC routes the traffic to the specific VLAN.
Additional details about the configuration are given in the following picture:


ossvm-VLAN - Network/Net Services - Mozilla Firefox
https://21.21.10.200/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
Add
Delete
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
5060
5060
5061
5161
2727
VLAN IP
Main-Access-VLANIP
eth1
0.0.0.0
0.0.0.0
173
0
0
0
0
0
VLAN IP
Main-Access-VLANIP2
eth3
172.16.57.10
255.255.0.0
172
0
5060
5061
5161
2727
Realm Profile
Add
Delete
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
Main-Access-VLANIP2
access
Main-Access-VLANIP2
Main-Access-VLANIP2
Routing
Default gateway address
21.21.0.1
Default gateway IPv6 address
Routing configuration
Add
Delete
Row
Destination
Gateway
Netmask
Interface
VLAN tag
1
173.16.0.0
173.16.0.1
255.255.0.0
eth1
173
2
172.16.0.0
172.16.0.1
255.255.0.0
eth3
172
OK
Cancel

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).

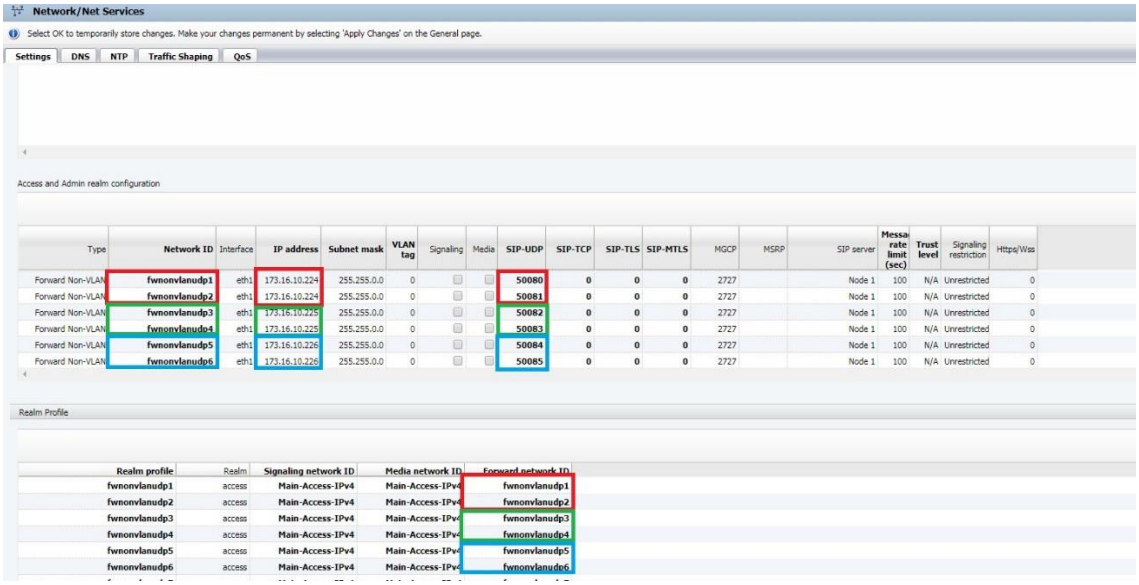
From now, the Ports configured in Access realm should not be in the range from 60000 to 62000. This range was reserved for internal system usage.
Additionally, for each Forward network, an entry in Realm Profile should be created (mandatory to associate the "**Network ID**" with new field **"Forward Network ID"** in Realm Profile)

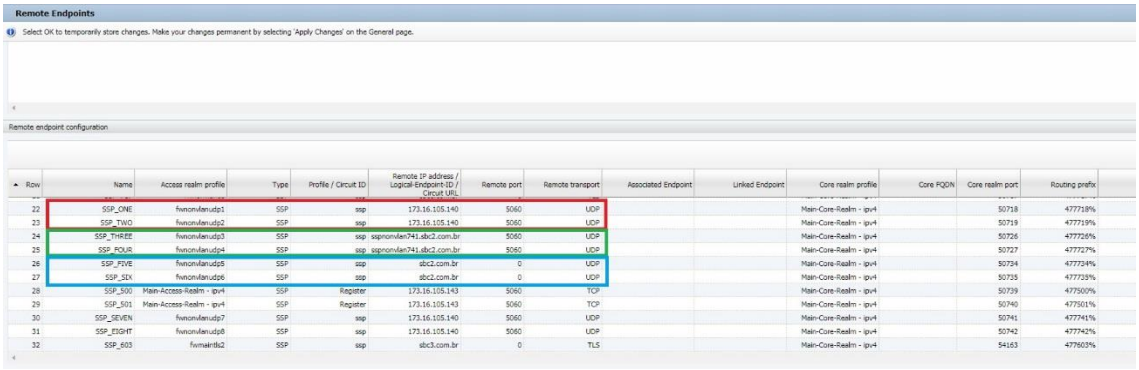


Now, it is possible to configure the Forward Main, Forward Non-VLAN and Forward VLAN using the same IP address and different ports.

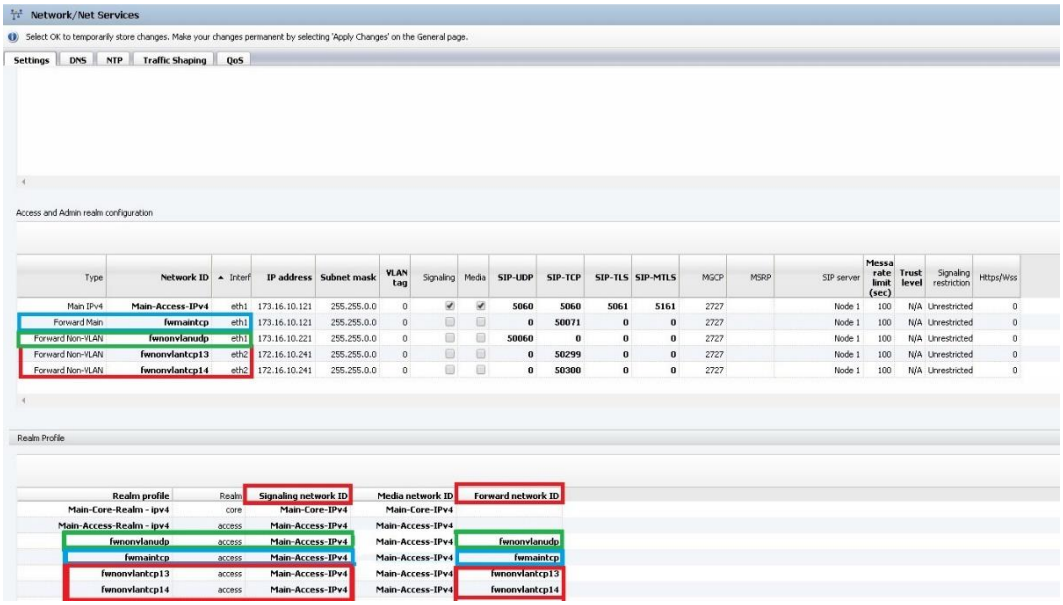
Then, it is also possible to configure the SSP using the same IP address or URL(fqdn) or SRV and different core realm ports. Associate the respective access realm profile in the remote endpoint configuration.

See the following example:





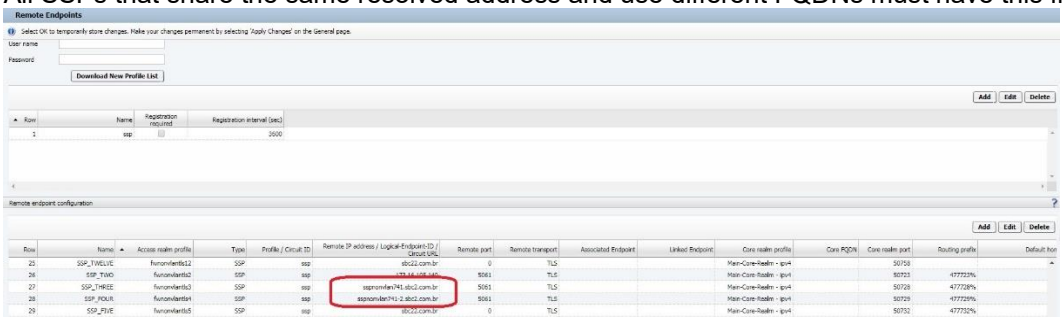
NOTICE: When creating a Realm Profile: if a forward non-vlan Network is to be used (even if different network interfaces are used) such network must be configured only as the "Forward network id" and the Signaling network ID must be "Main Access network ID"

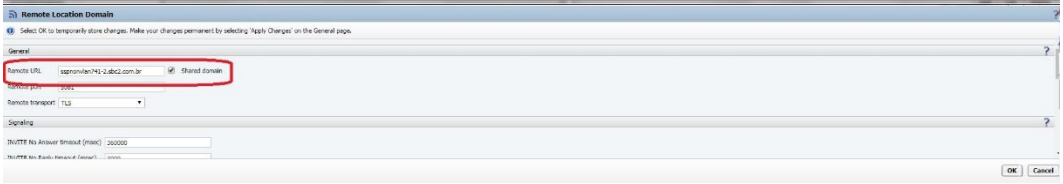


Flag Shared Domain

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.





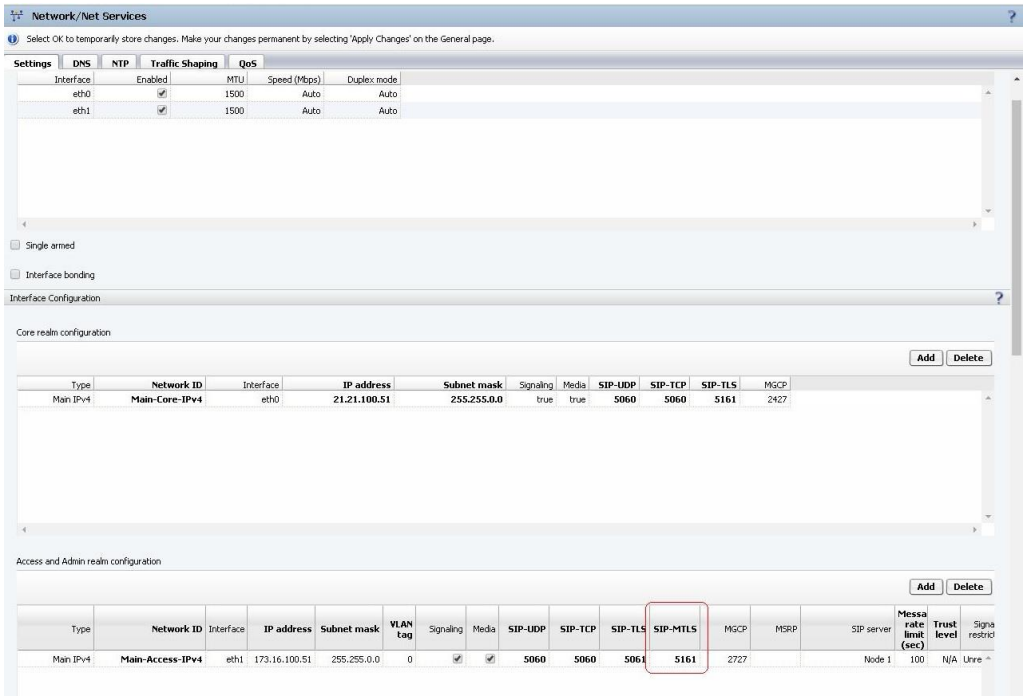
RESTRICTIONS:

- 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



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

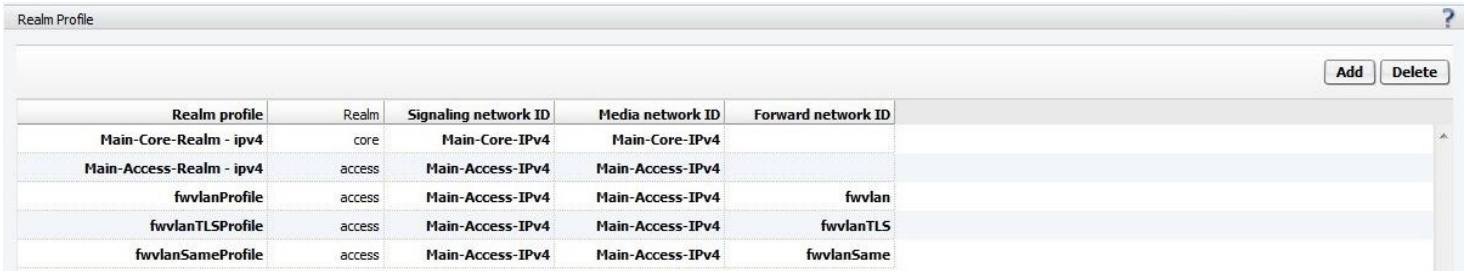
In versions prior to OSV V9, OSV challenged OPTIONS requests coming from the SIP proxy endpoint (OSB, SBC). In that case, it was recommended to configure the SBC IP address + port as trusted in the OSV.
From OSV V9, OPTIONS requests will not be contested if the 'SIP Proxy' endpoint attribute is set and **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



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.

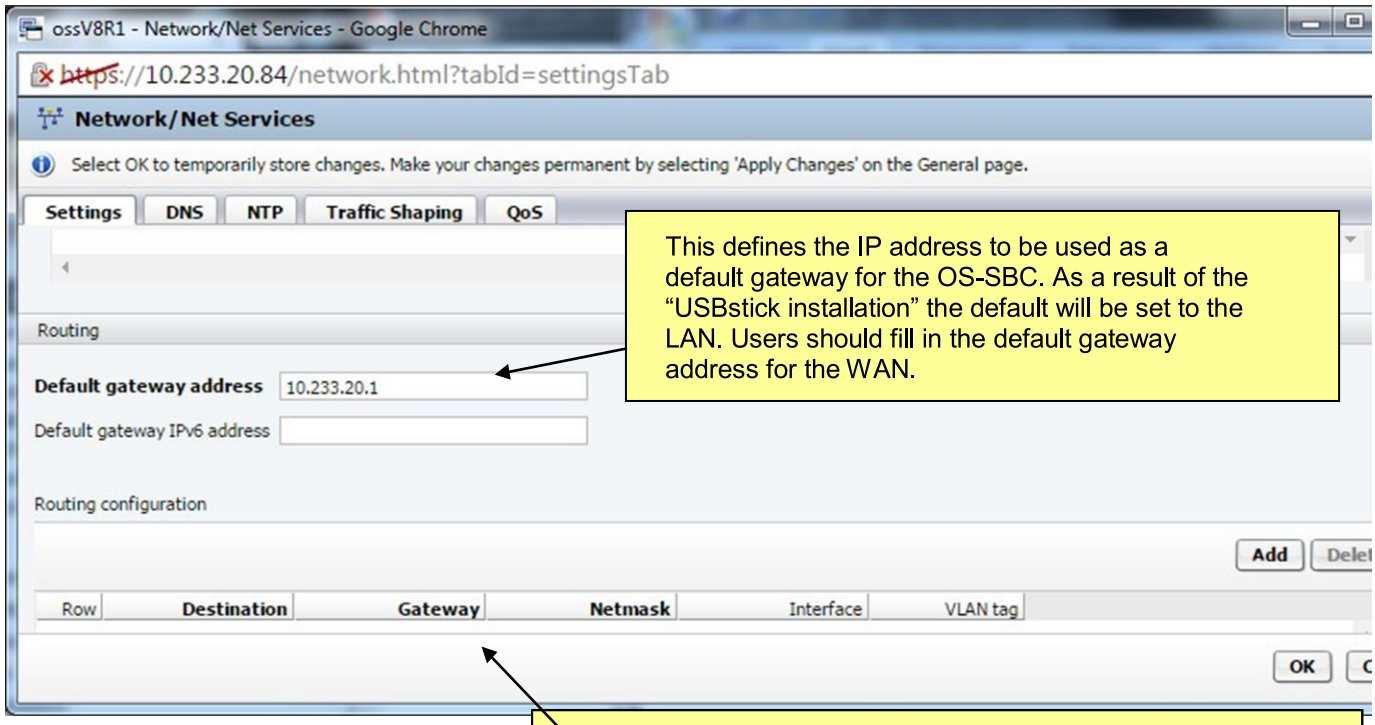
• **Signaling Network-ID** - The user is presented a list of signaling capable Network-ID's for selection. Alternatively the user may be provided a list of Network-ID's filtered by the chosen association.

• **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*



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".

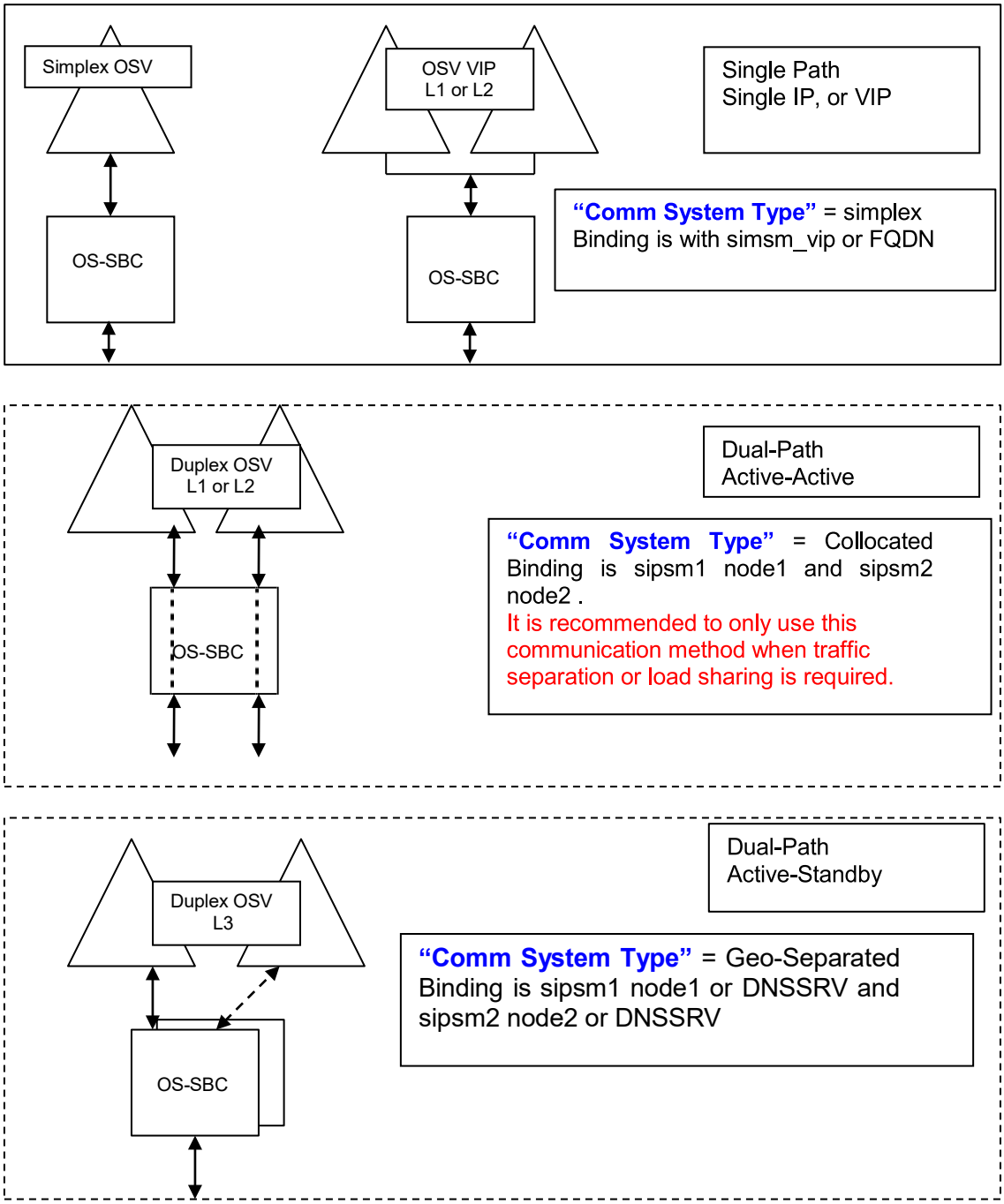
Note 2: It is recommended to only use this "Comm System Type" when traffic separation or load sharing, between two OSV nodes, is required.

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)

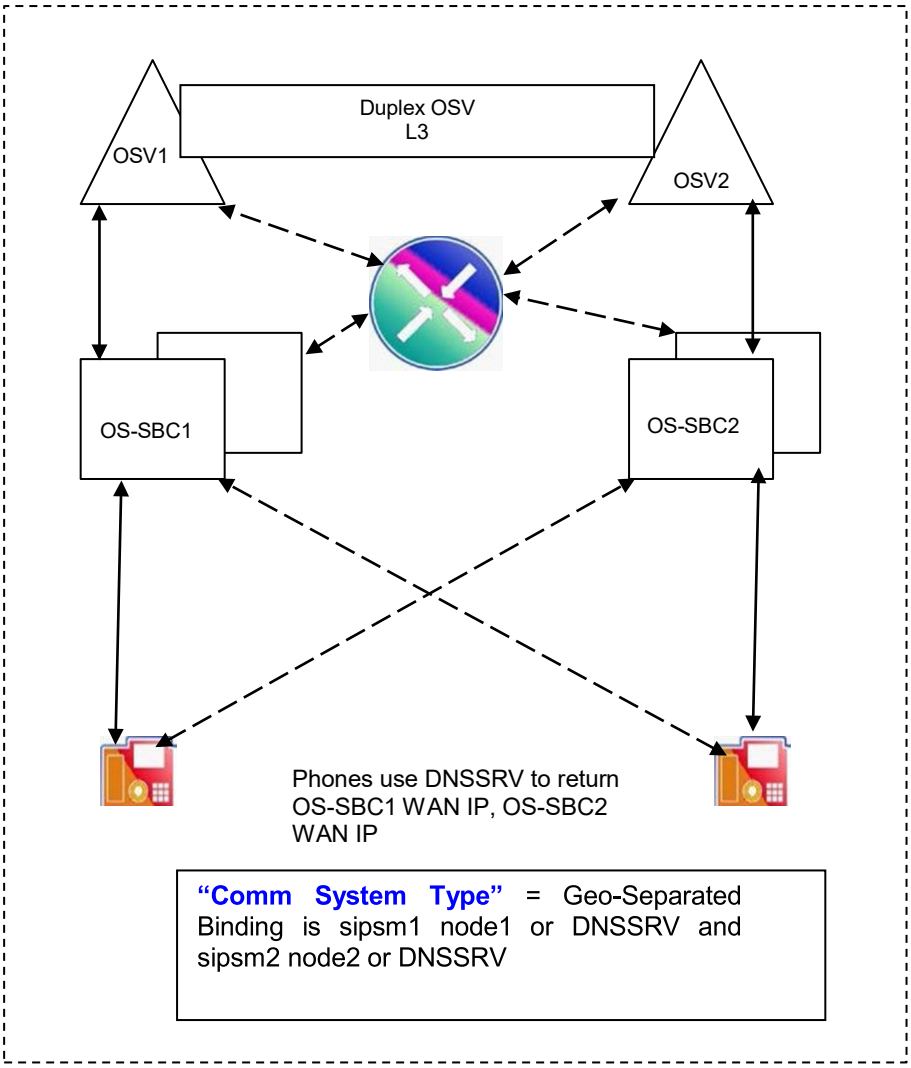
Table 1 IP Address Calculations: The above assumes using "single core" address.

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



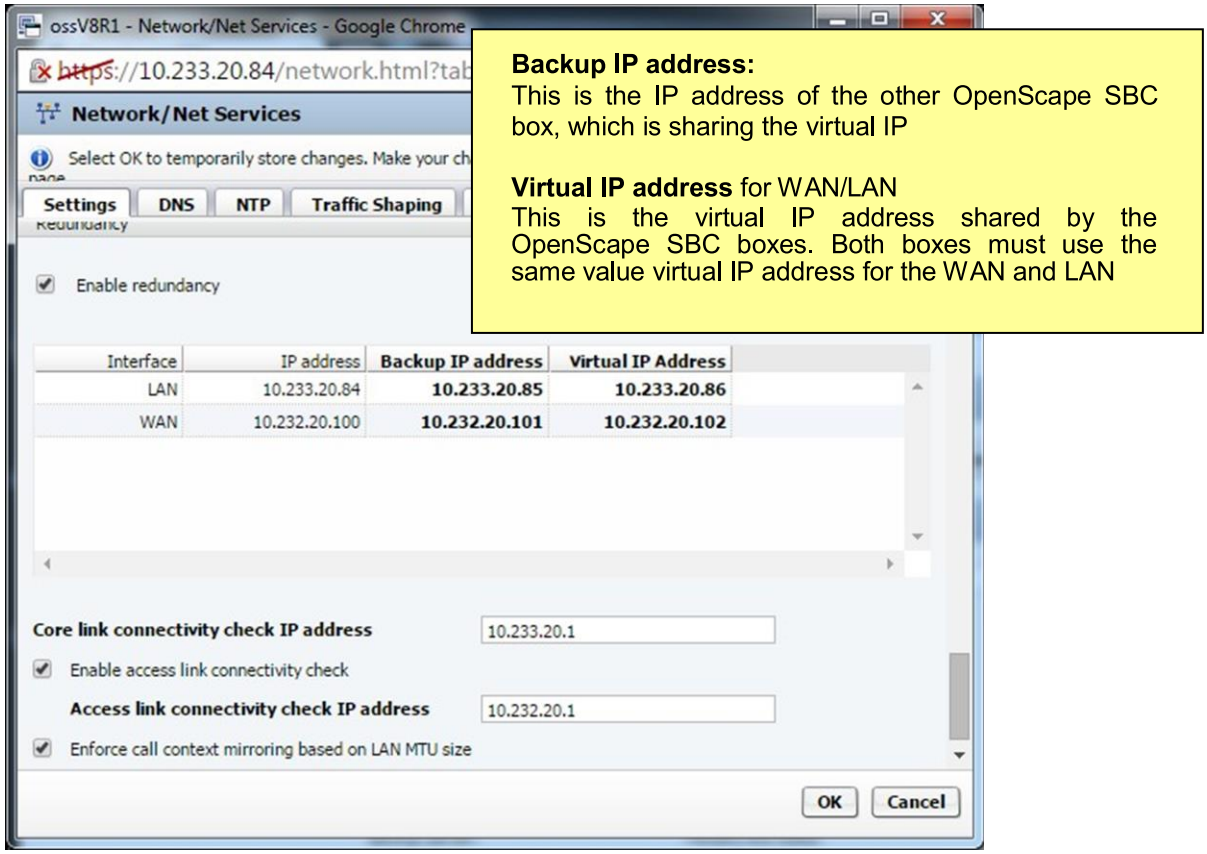
Example OSV Connections



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



Backup IP address:
This is the IP address of the other OpenScape SBC box, which is sharing the virtual IP

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 virtual IP address for the WAN and LAN

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

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 forWAN/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 Unbalanced Redundancy

In order for two nodes to be a redundant OS-OSB system, both nodes must have the same hardware configuration. However, in versions after V11R0.02.00-1, it is possible to create a new type of redundancy, called Unbalanced Redundancy. In this type of redundancy, the user can pair two different types of hardware, given it's one of the combinations that are listed below:

x3250	**sr250**
x3550	**sr530**
x3550	**sr630**
sr530	**sr630**

3.4.3.9.5 Access Link connectivity check (WAN redundancy)

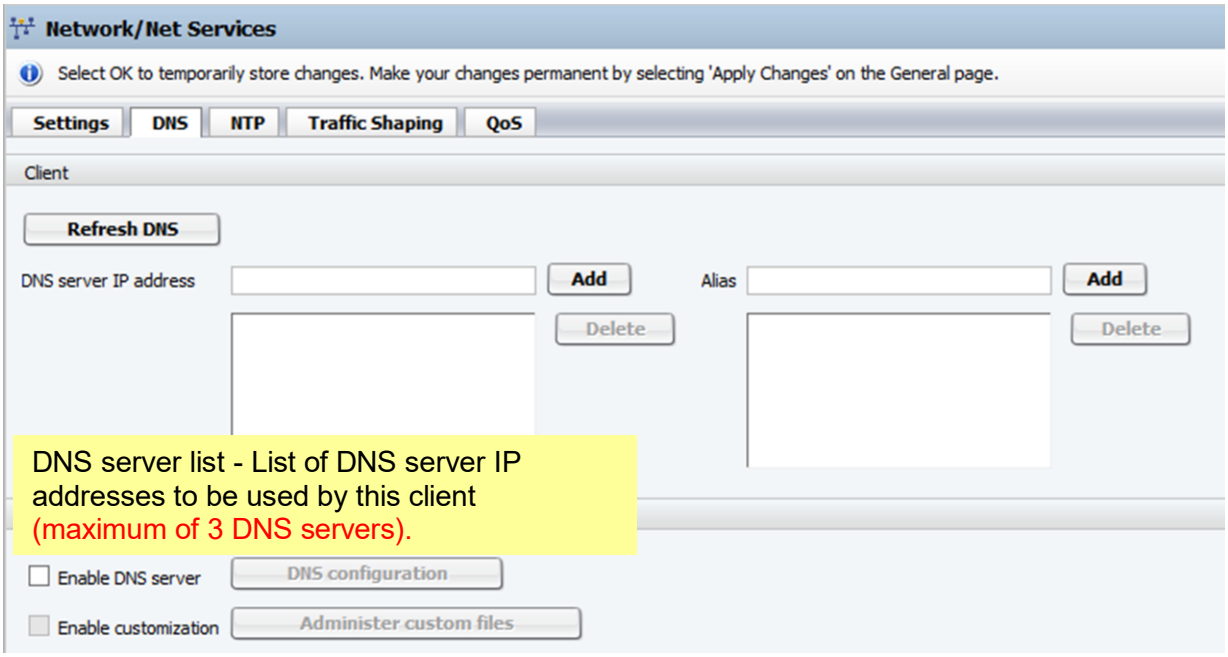
Customer Responsibilities for WAN redundancy

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.

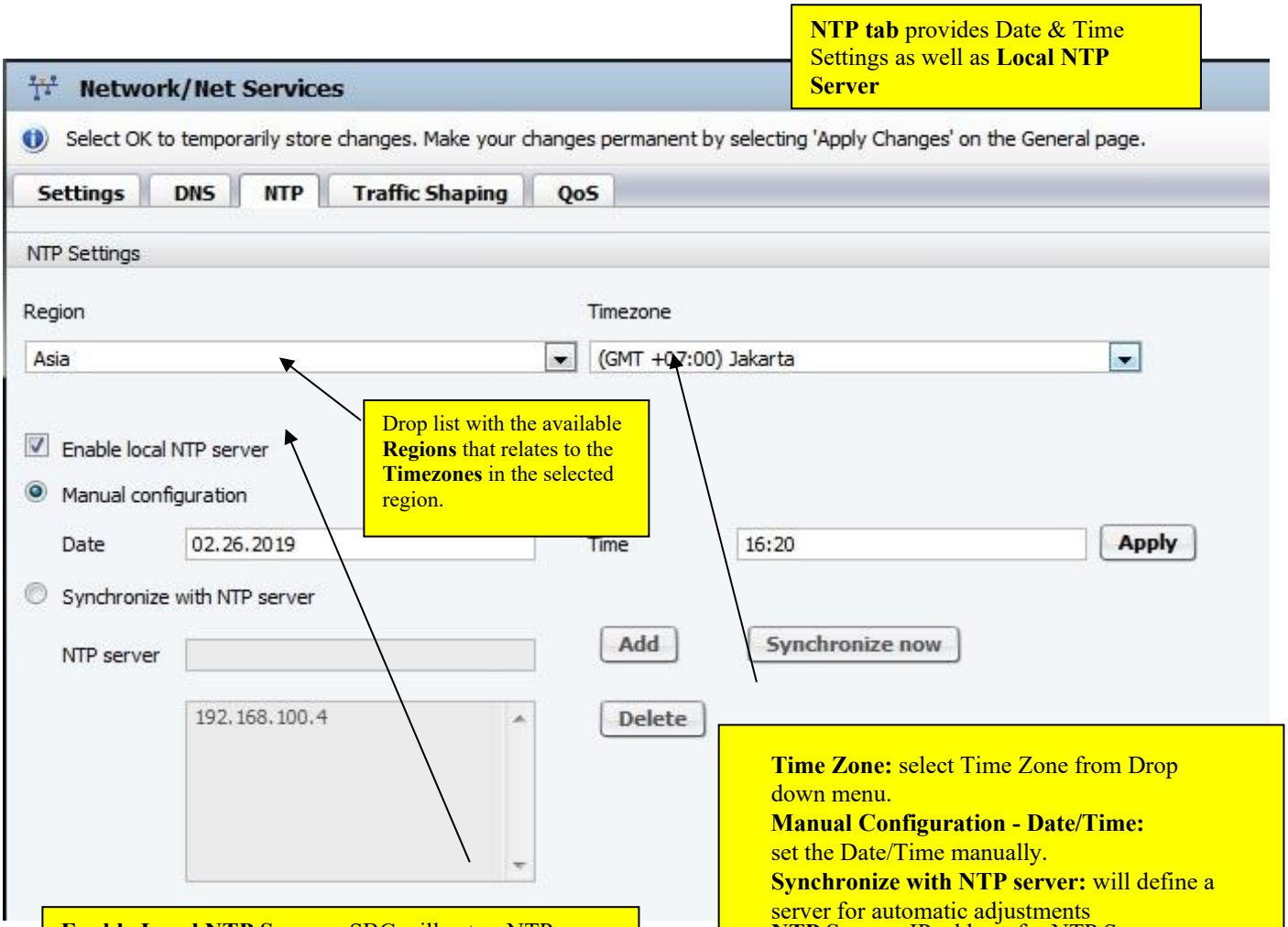
The customer SHALL be responsible for providing an OS-SBC WAN IP address for each OS-SBC server node. This means 3 addresses are required, two additional IP addresses in addition to the VIP address.

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
Delete
Alias
Add
Delete
DNS server list - List of DNS server IP addresses to be used by this client (maximum of 3 DNS servers).
Enable DNS server
DNS configuration
Enable customization
Administer custom files

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



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.

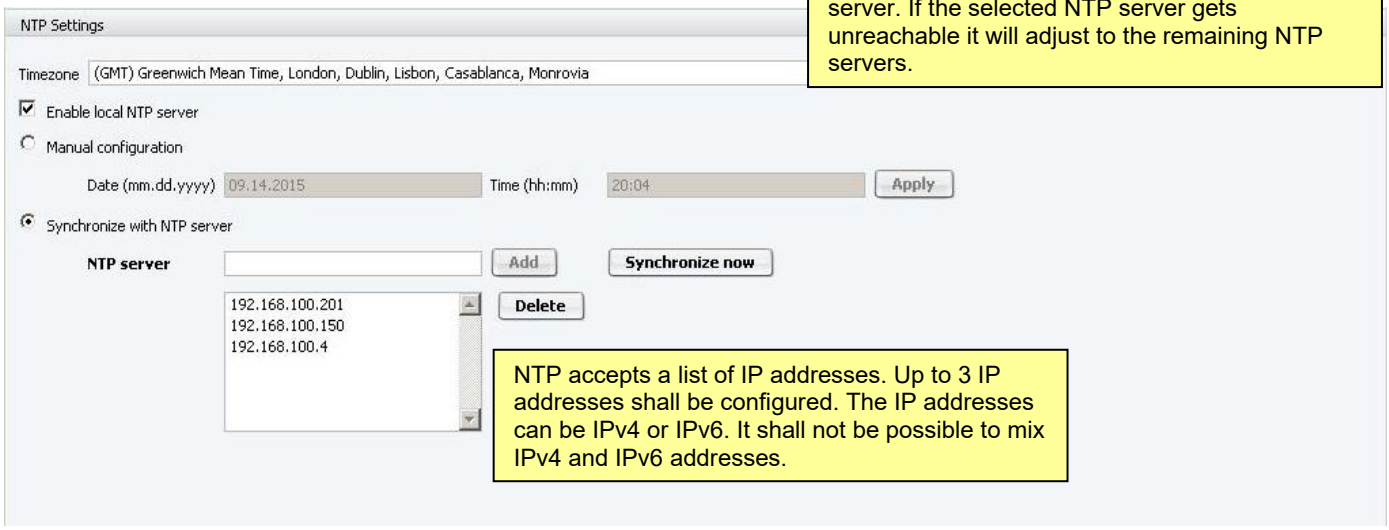
Time Zone: select Time Zone from Drop down menu.
Manual Configuration - Date/Time: set the Date/Time manually.
Synchronize with NTP server: will define a server for automatic adjustments
NTP Server: IP address for NTP Server.

Note: Some changes will require a system restart.

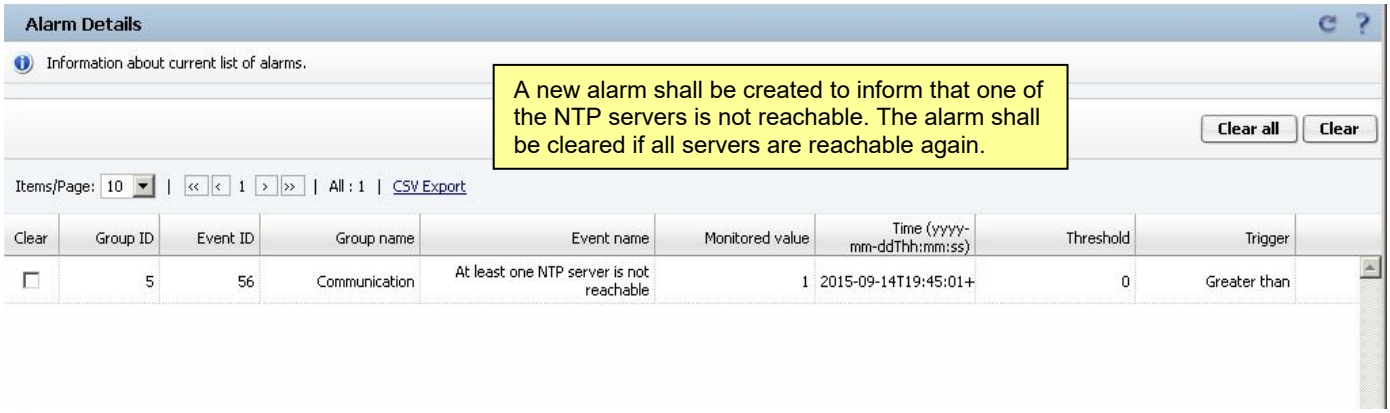
Enable Local NTP Server - SBC will act as NTP server for the Branch

3.4.3.11.1 Support_Multiple_NTP_Servers

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.

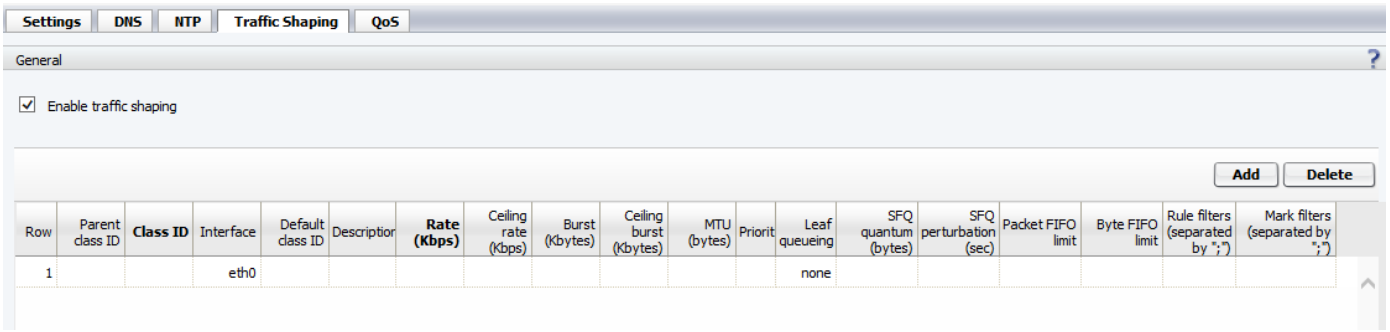


NTP accepts a list of IP addresses. Up to 3 IP addresses shall be configured. The IP addresses can be IPv4 or IPv6. It shall not be possible to mix IPv4 and IPv6 addresses.



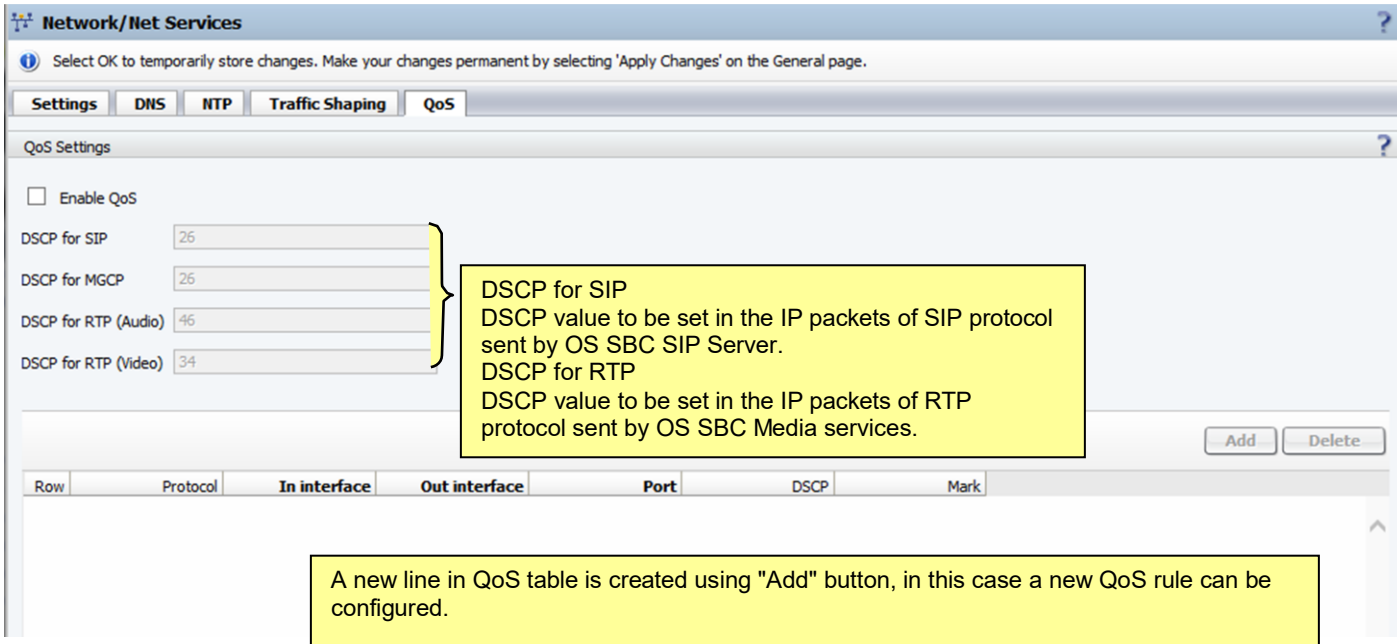
A new alarm shall be created to inform that one of the NTP servers is not reachable. The alarm shall be cleared if all servers are reachable again.

3.4.3.12 Traffic Shaping



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

3.4.3.13 QOS Settings



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.

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

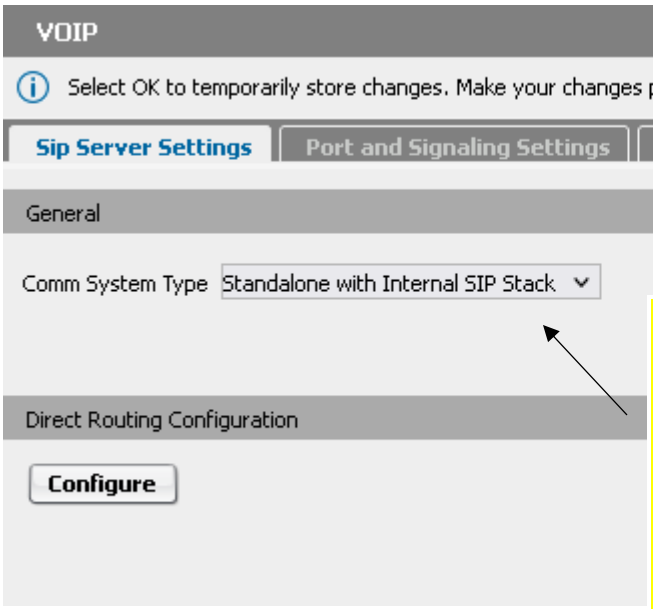
It can set the DSCP value for IP packets filtered according to the configured parameters and/or set the mark for traffic shaping. The QoS rule is deleted from table using "Delete" button.

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.

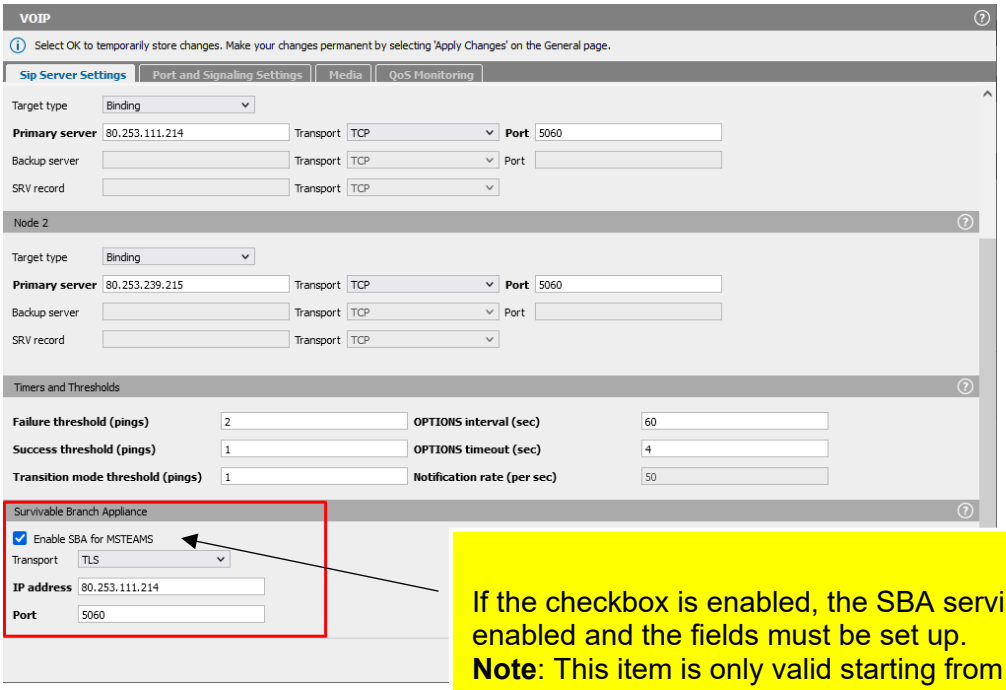
3.4.4 VOIP / SIP Server Settings

Standalone with internal SIP Stack



In this mode, the B2B-Controller can function as a B2BUA and support the BYOT (Bring Your Own Trunk) feature. BYOT enables the SBC to route and establish calls between endpoints without requiring an external SIP server. In this mode, the server configuration is disabled, and Direct Routing Configuration is enabled.

SIP Server Settings none clustered



If the checkbox is enabled, the SBA service is enabled and the fields must be set up.
Note: This item is only valid starting from V11

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.

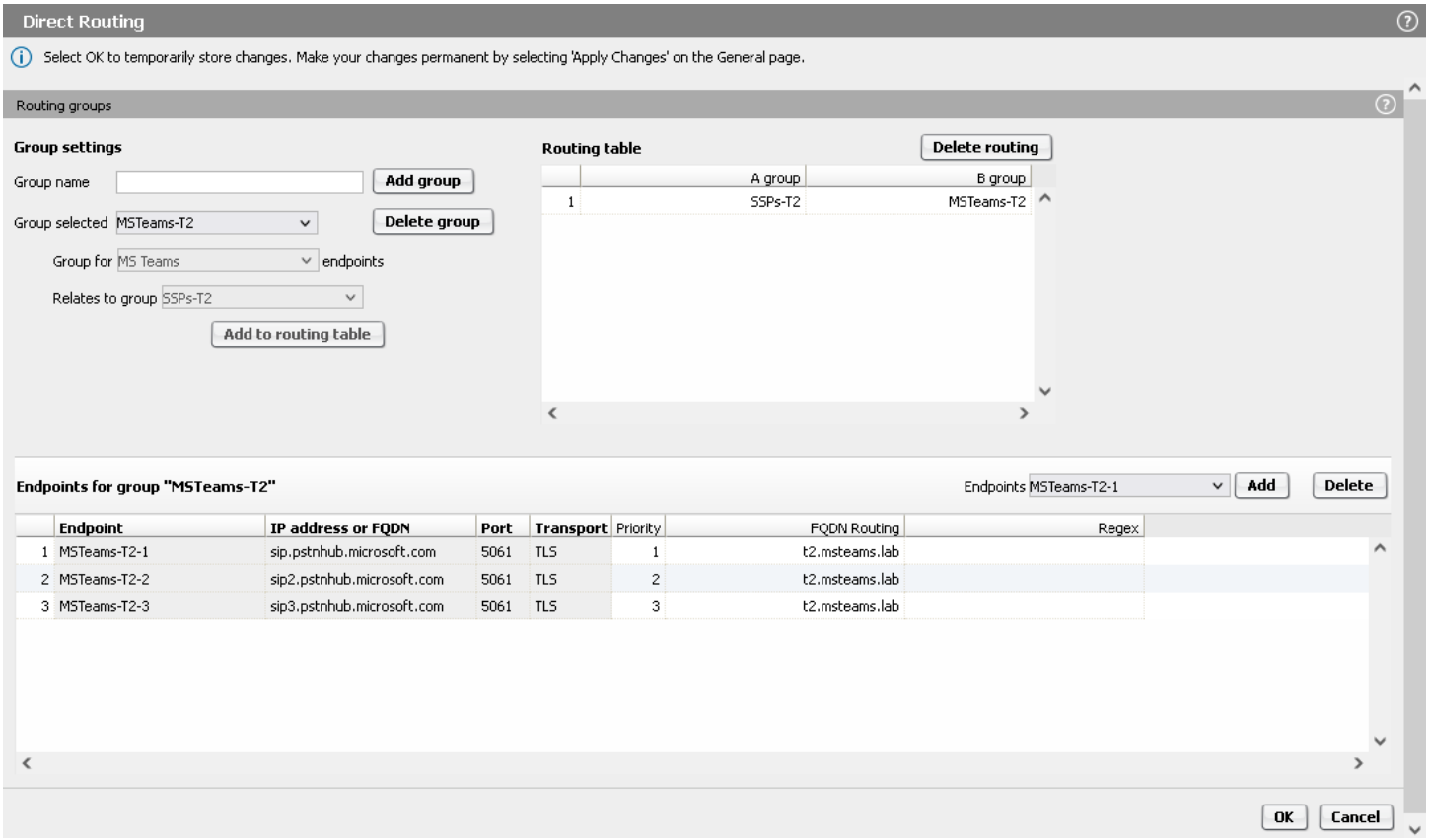
(Node 1/ Node 2)

- 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

Direct Routing Configuration



Routing groups

In this session it is possible to configure all remote endpoints groups with routing rules and link them.

- **Group settings**
- **Group name** - Configures the remote endpoints group name to be added using the "Add group" button.
- **Group selected** - Select the group to be configured or deleted. Use the "Delete group" button to delete the group.
- **Group for endpoints** - Define the endpoints group type (MS Teams, SSPs, Gateway, and Proxy) to be listed in the endpoints list. “MS Teams” refers to endpoints of type SSP and MS Teams profile. “SSPs” refer to endpoints of type SSP without the profile MS Teams profile.
- **Relates to group** - Links the group to another group. The association is added to the routing table by the "Add to routing table" button.

  NOTE: The following combination of types are allowed to associate the groups:

  - MS Teams with SSP, and vice-versa.
  - Gateway with SSP, and vice-versa.
  - Proxy with SSP, and vice versa.

- **Routing table** - Table with all remote endpoints' groups association.
  Use the "Delete routing" button to delete the selected associations from the routing table.

- **Endpoints for group** - Configure the remote endpoints for the selected group and add routing rules to the endpoints.
  The **Endpoints list** allows selecting the endpoints to be added to the group using the "Add" button. The "Delete" button removes the selected endpoints.

For each endpoint it is presented the name, address, port, and transport. The priority, FQDN Routing and Regex can be configured to reach the endpoint. The priority field defines the order of endpoints that will be selected when more than one rule matches the rule. FQDN Routing indicates the R-URI domain that should match to reach the endpoint. And Regex is the regular expression in ES6 pattern for the user part of the R-URI that should match to reach the endpoint. The FQDN Routing and Regex are optional, and empty values indicate that they will not be checked.

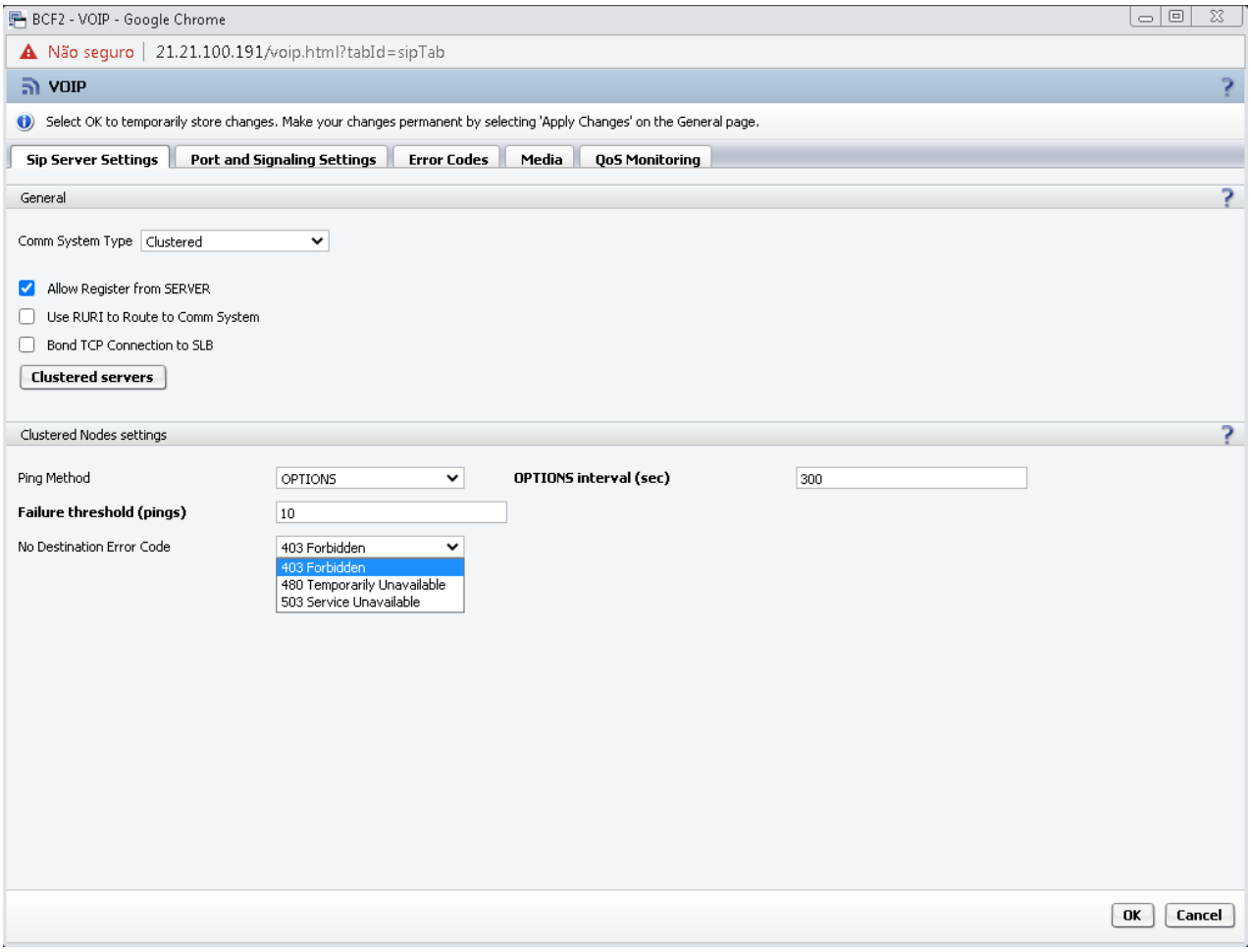
Examples:

INVITE URI is *sip:98765432@abc.msteams.com:5061;transport=tls*

1. FQDN is set to *abc.msteams.com*, and Regex is empty - Endpoint is selected because FQDN matches.
2. FQDN is set to *def.msteams.com*, and Regex is set to *^9876* - Endpoint is not selected because FQDN does not match.
3. FQDN is empty, and Regex is set to *^9876* - Endpoint is selected because Regex match
4. FQDN is empty, and Regex is set to *^4567* - Endpoint is not selected because Regex does not match.
5. FQDN is set to *abc.msteams.com*, and Regex is set to *^9876* - Endpoint is selected because FQDN and Regex match.
6. FQDN and Regex are empty - Endpoint is selected because FQDN and Regex are not checked.

More than one endpoint can be selected and, in that case, the priority will define the routing order. Lower values have higher priority. Additionally, rerouting can occur if the endpoint or endpoints with higher priority fail.
When more than one endpoint with the same priority is selected, b2b-controller will sort the endpoints by the endpoint with the longest unused time.
Unavailable endpoints (Failed by SSP OPTIONS connectivity check) are not included in the selection of endpoints for routing.

3.4.4.1 VOIP / SIP server Settings Clustered



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 FDQN.

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.

- **Success threshold (pings)**

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

- **Transition mode threshold (pings)**

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

- **OPTIONS interval (sec)**

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

- **OPTIONS timeout (sec)**

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

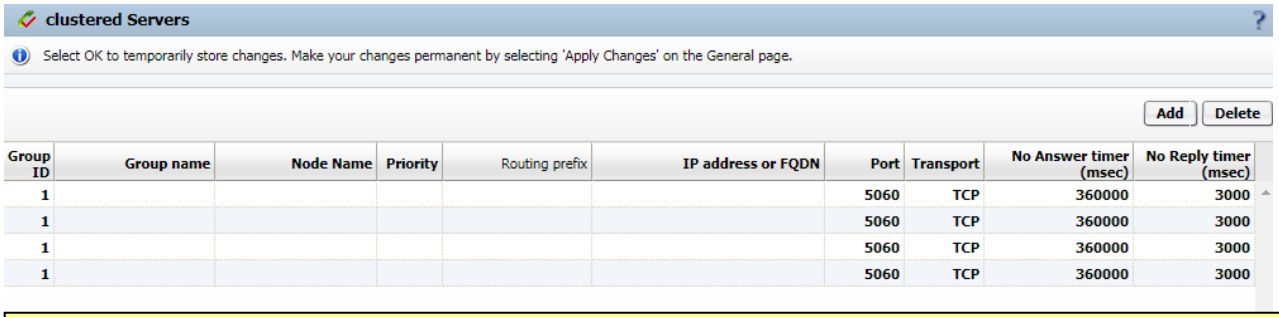
- **Notification rate (per sec)**

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

- **No Destination Error Code**

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

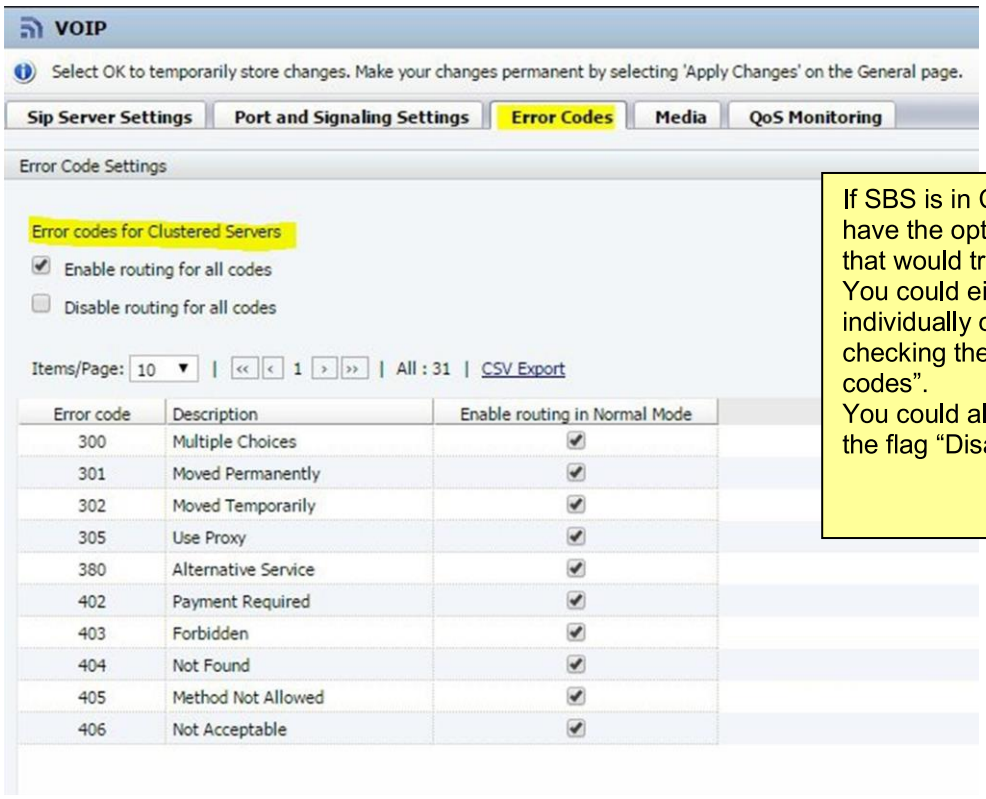
  - 403 Forbidden (Default option)
  - 480 Temporarily Unavailable
  - 503 Service Unavailable



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

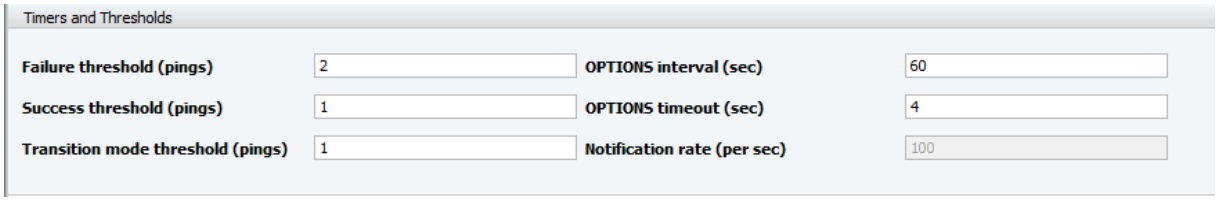
- **Group Id**: this field is set internally, i.e. not editable.
- **Group name**: name corresponds to the cluster nodes grouped together. This group name is associated with the tab “Sipserver” under “Access and Admin realm configuration”.
- **Node Name**: cluster node name.
- **Priority**: the higher number has precedence. The higher number has precedence. Accepts priority 1 up to 100.
- **Routing Prefix**: if set, then the dialed digits in RURI are checked against the provisioned “Routing Prefix”, and the destination node is selected accordingly.
- **IP address or FQDN**: IP or FQDN of the node.
- **Port**: port to be used for the cluster node.
- **Transport**: transport to be used for the cluster node.
  - **NOTE**: The transport type must be the same for all clustered servers.
- **No Answer timer and No Reply timer** may be different for each of the cluster nodes. They are both initialized to 360000 and 3000 ms respectively.
- **Stick with CommServer** This flag makes all devices that got registered in this server use this server exclusively for all communications.

3.4.4.1.1 VOIP / Error codes Clustered

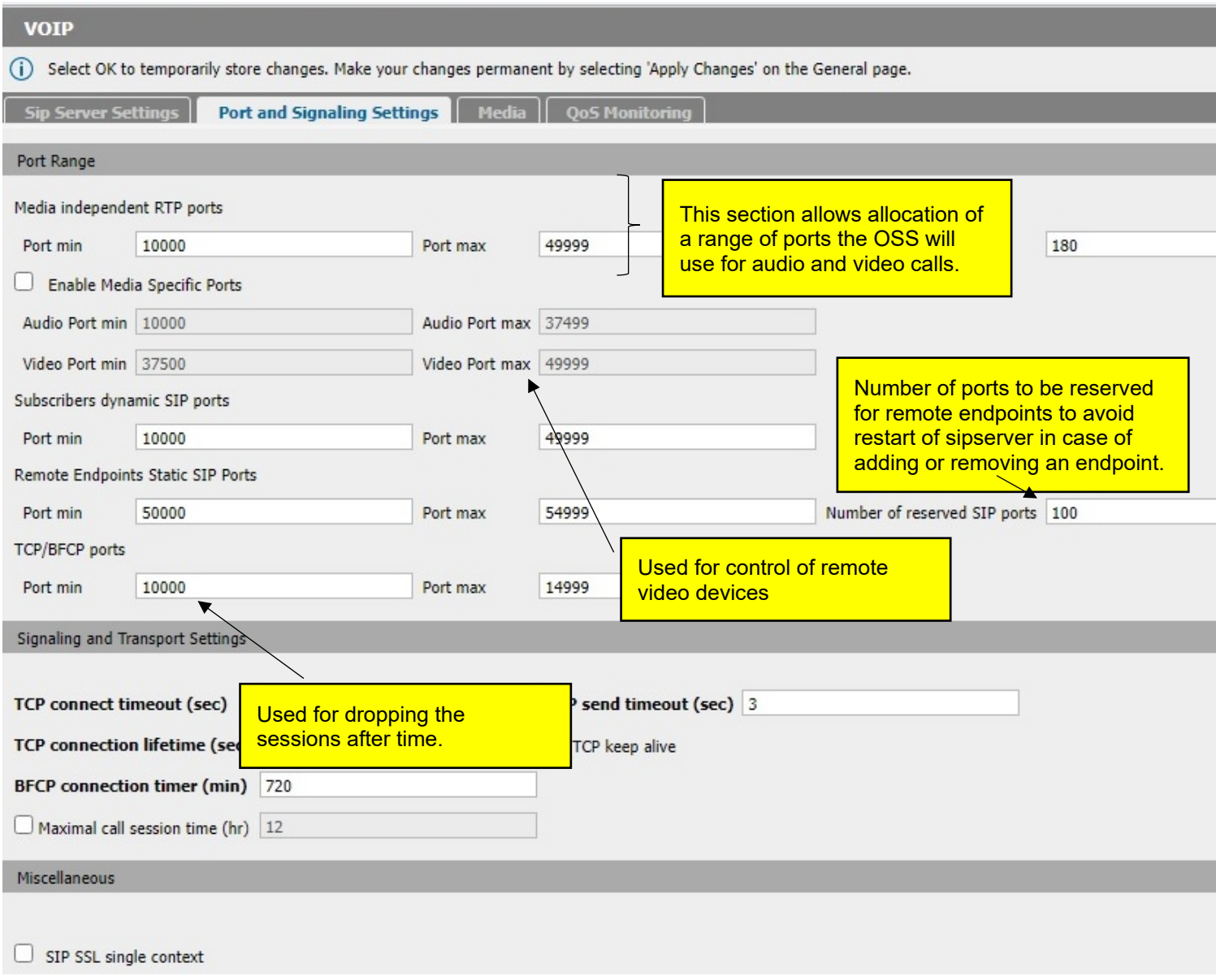


If SBS is in Cluster mode, then you have the option to choose error codes that would trigger a rerouting.
You could either set error codes individually or set them all at once by checking the “Enable routing for all codes”.
You could also disable all by checking the flag “Disable routing for all codes”

3.4.4.2 Timers and thresholds



3.4.4.3 Port and Signaling Settings



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.

3.4.4.4 Media

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.

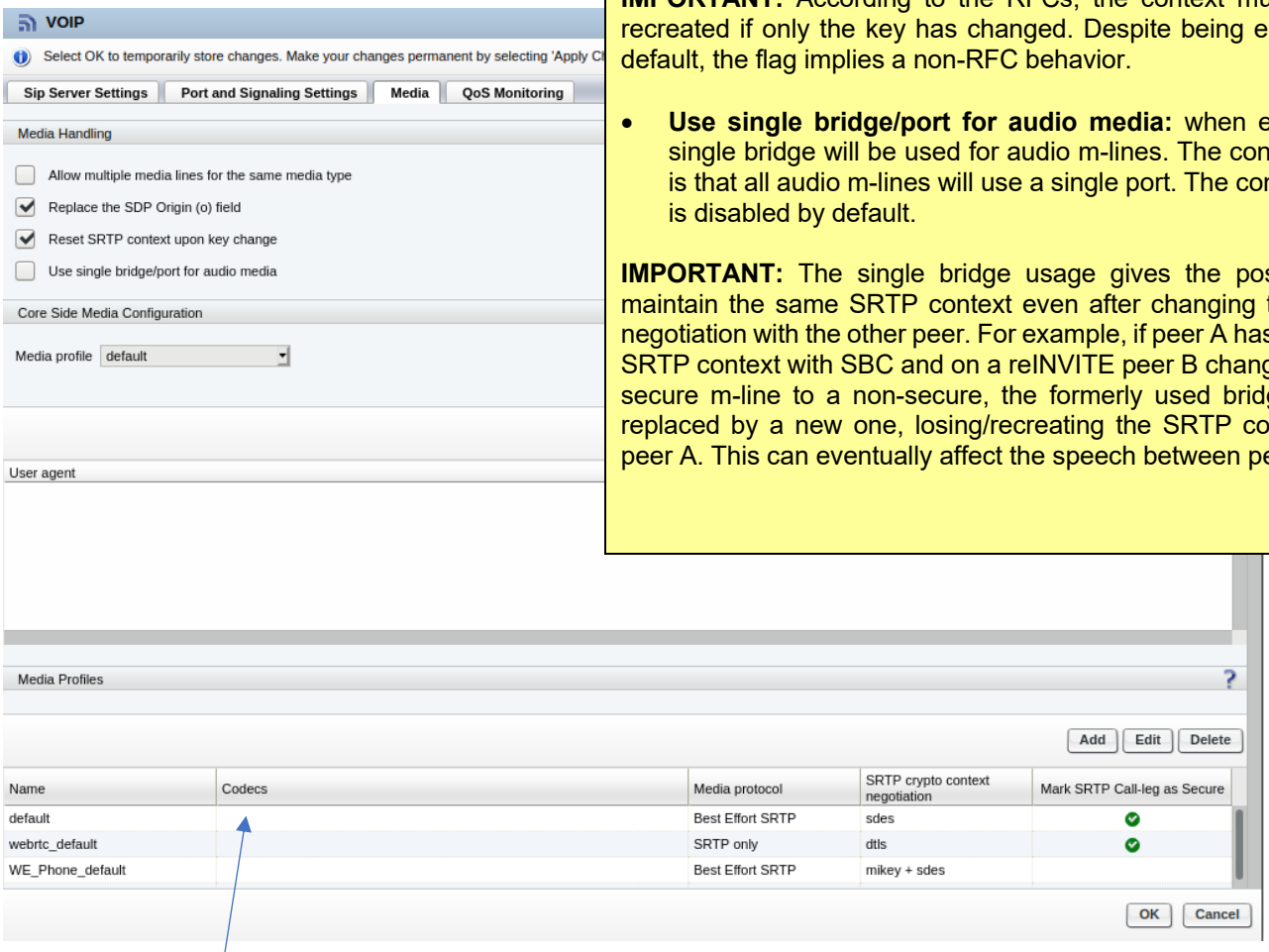
- **Replace the SDP Origin (o) field:** enable the replacement of SDP Origin (o) field with the SBC addresses and username *OSSBC.*

- **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.

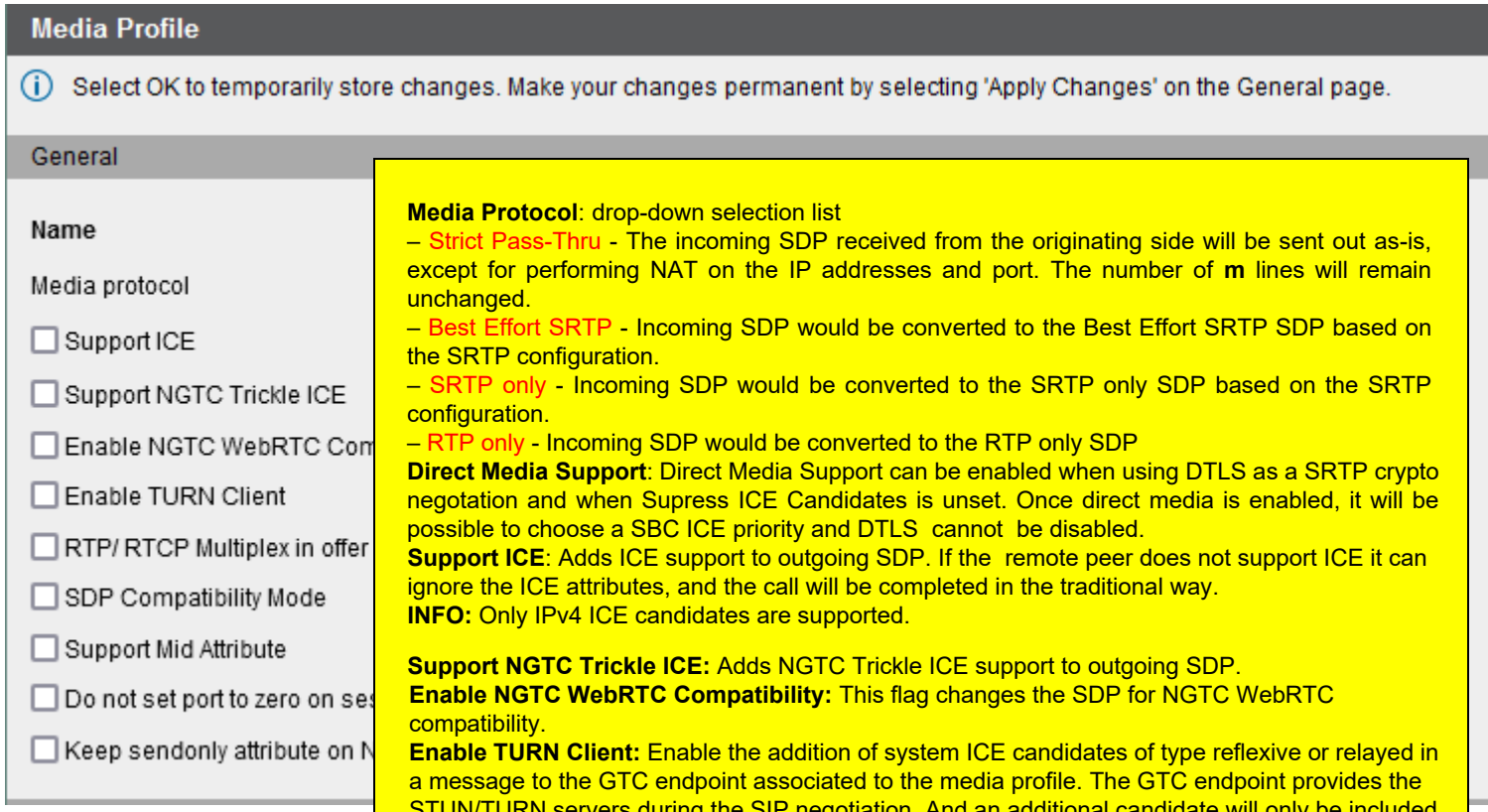


After selecting the codecs in Features Enable Codecs Support for transcoding, add the codecs in desired media profile and defiy the priority.

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



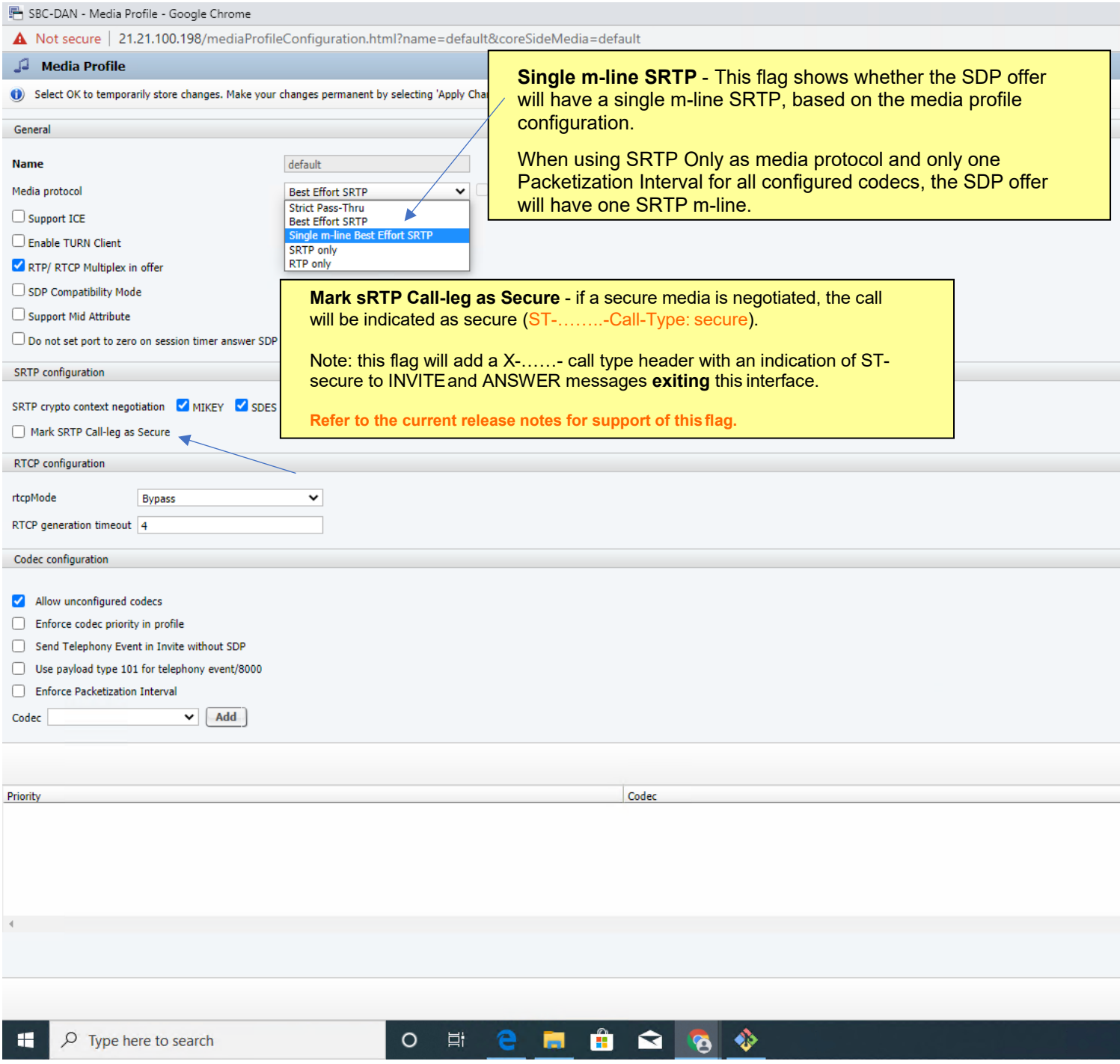
Media Protocol: drop-down selection list
– Strict Pass-Thru - The incoming SDP received from the originating side will be sent out as-is, except for performing NAT on the IP addresses and port. The number of **m** lines will remain unchanged.
– Best Effort SRTP - Incoming SDP would be converted to the 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 negotation and when Supress 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 GTC endpoint provides the STUN/TURN servers during the SIP negotiation. And an additional candidate will only be included in a message to GTC endpoint if it differs from a host address.
RTP/RTCP Multiplex in offer: Adds rtcp-mux support to outgoing SDP. If the remote peer does not support rtcp-mux it can ignore the attribute and the call will be completed in the traditional way.
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.
Do not set port to zero on session timer answer SDP - This flag will avoid setting the SDP media port to zero on SDP answer of session timer when no SDP change is verified. Although the last port is kept with a no-zero port, SBC will not listen to the respective port.
Keep sendonly attribute on NAT - This flag ensures that the received ***sendonly*** attribute is sent to the destination associated with the media profile, even if NAT is detected. Naturally, when NAT is detected, the ***sendonly*** attribute is converted to the ***sendrcv*** attribute
Important: Keep sendonly attribute on NAT is available starting from V11R2.

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. IIf 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 on endpoint do 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**.



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.

Crypto change mode: This option can be configured in any of the following ways:

- **Default:** The crypto key on media renegotiation is preserved when associated with the core side and changed when associated with the access side.
- **Steady**: This mode preserves the crypto key on media renegotiation when associated with either the core or access side.

  Note: The behavior described is also influenced by the SSP profile— for the MS Teams default profile, the behavior of Steady mode operates independently of the configured crypto change mode.

RTCP Configuration

Some peers may need to receive RTCP packets. This configuration allows the application handling media to generate RTCP when not being sent to it.

- **RTCP Mode**
  - **Bypass**: This is the default behavior. The media application does not generate any RTCP, it forwards them. When the QoS is disabled, the packets are transparently forwarded
  - **Generate Always**: The media application generates RTCP packets, regardless if the media (RTP) is active (for example, call on hold).

    - **Generate only When RTP is active**: The media application generates RTCP packets only when the media (RTP) is active.

- **RTCP generation timeout**: The time (in seconds) that the media application must wait for an RTCP on the same direction before it starts generating them.

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.

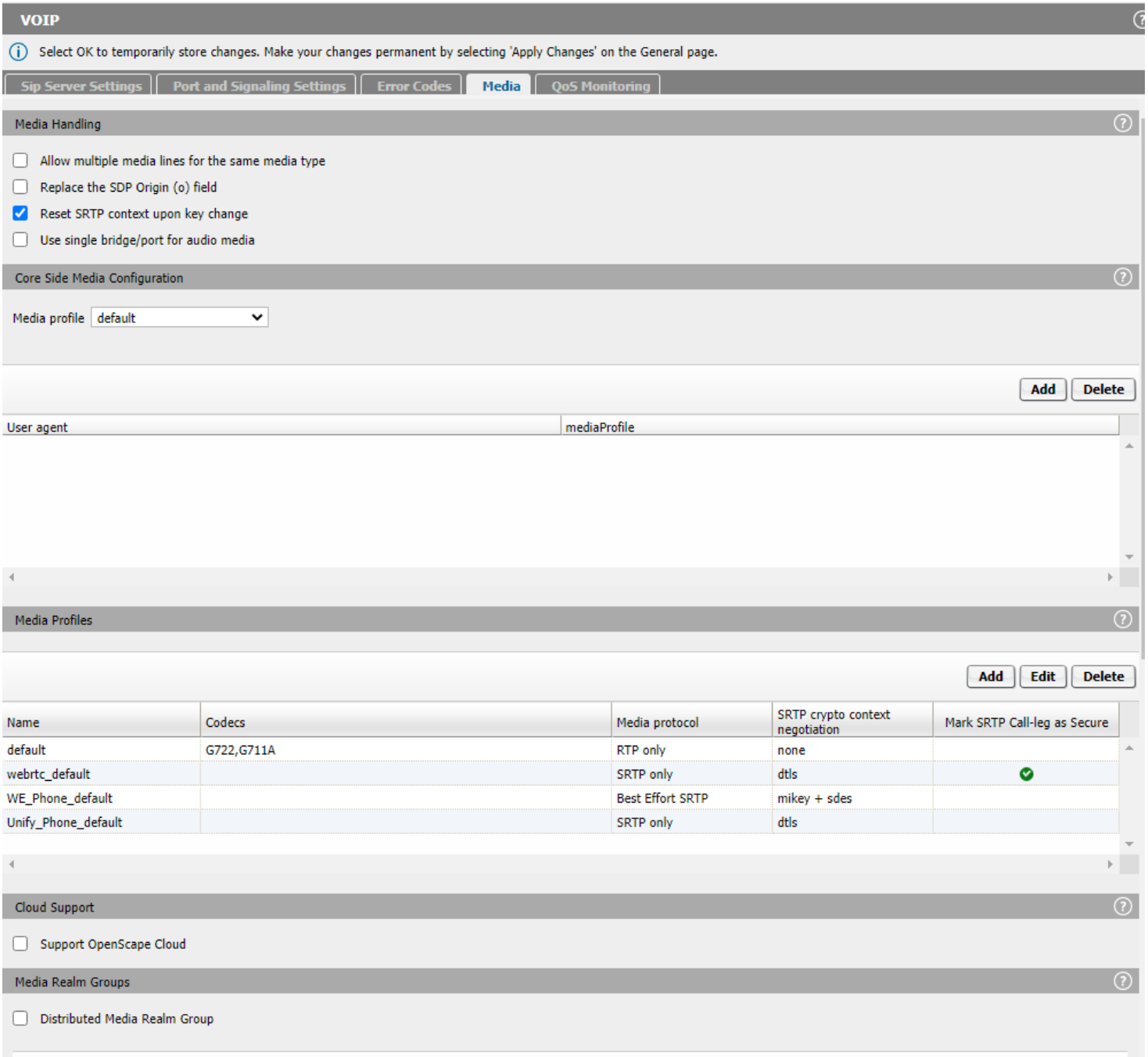
Codec: The user shall be able to select a codec from a drop-down list and click **Add** to add it to the bottom of the list of codecs for this media profile.If a codec is already in the list of codecs for this media profile then it shall not appear in the drop-down list for adding codecs. The user shall 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.

3.4.4.5 Core Side Media Configuration



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 Pro		
Best Effort		
Strict Pass		
SRTP Onl		
RTP	none	none(grayed out)

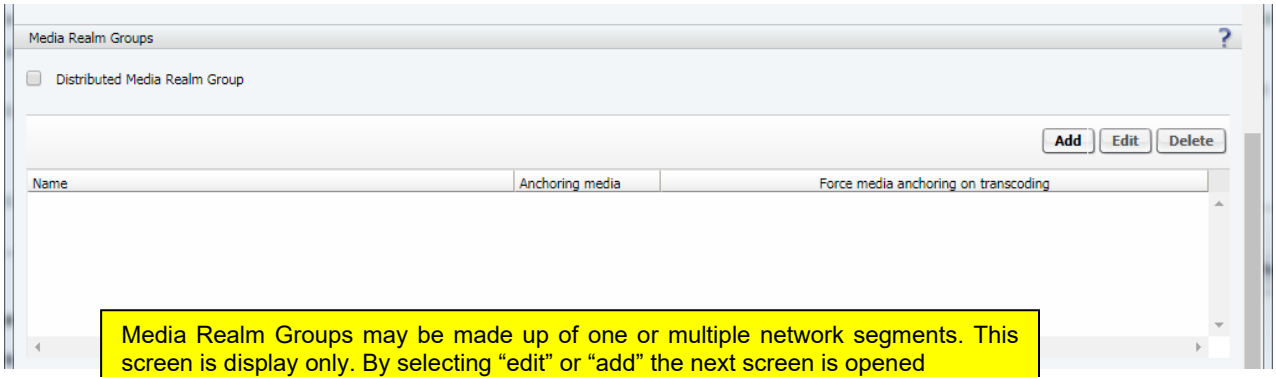
3.4.4.6 Media Realm Groups

GUI → VOIP → Media

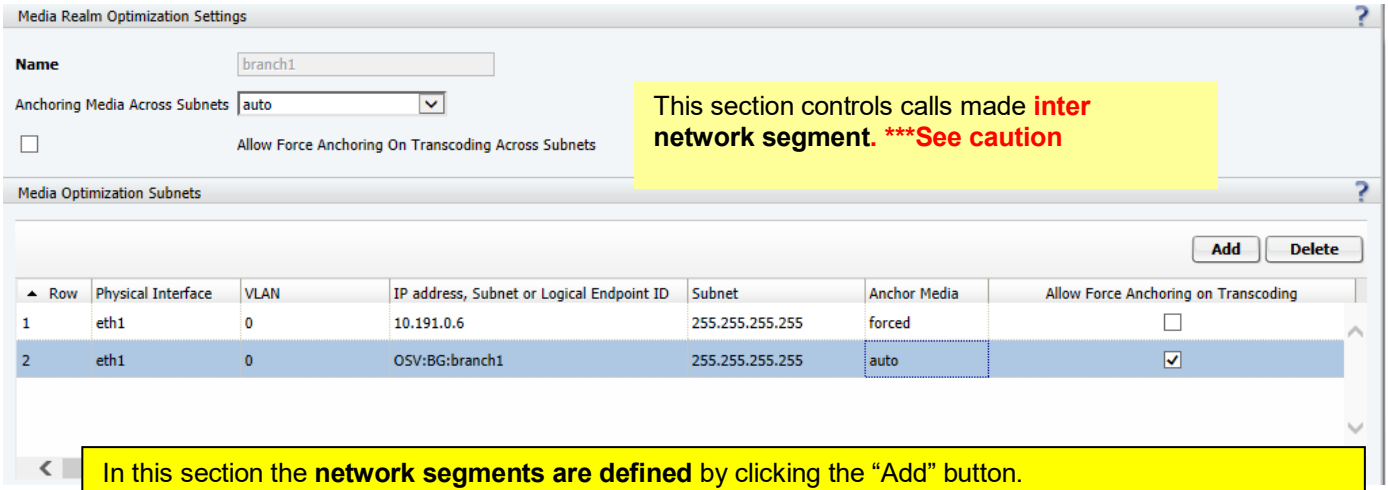
The Media Realm Groups allow the customer to have some control over media connectivity between network media domains (or network segments) without L3 NAT.
To support the needed flexibility, the customer is required to identify network segments (media realms) in a group (Media Realm Groups), identifying 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 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



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

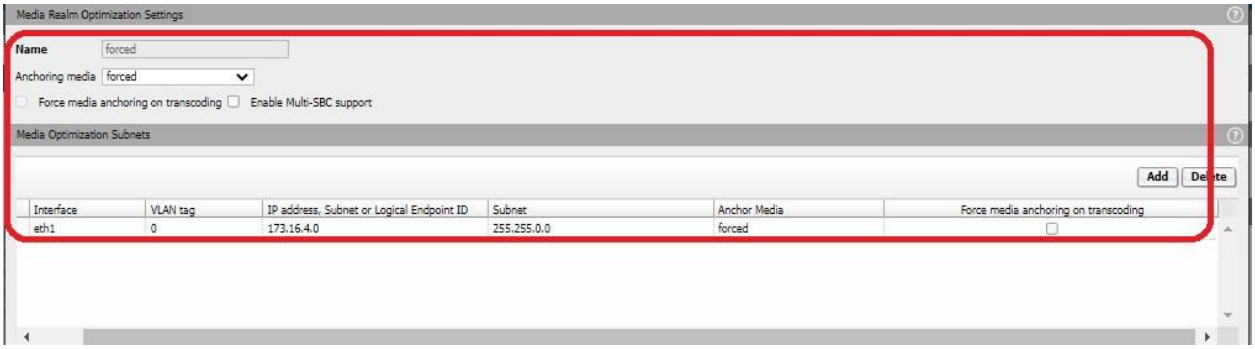
When there is a need to anchor media for a specific subnet, it is necessary to create separate Media Realm Groups.

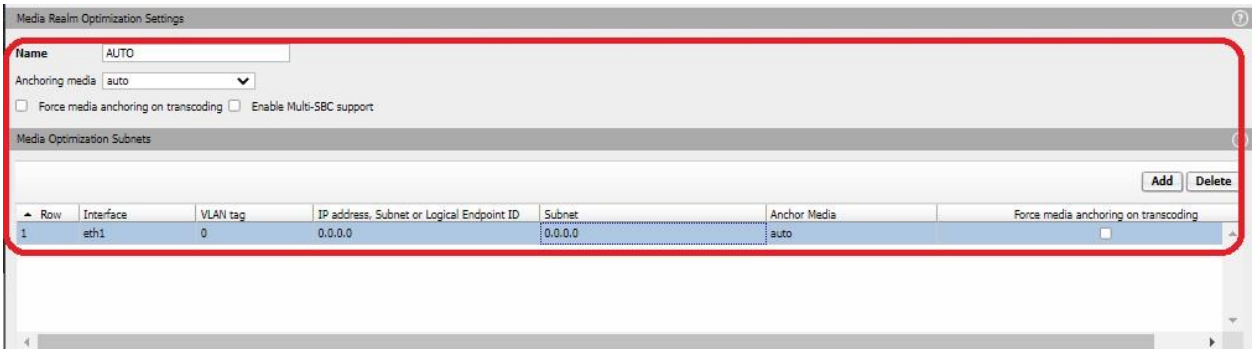
- One Realm Group to Anchor media

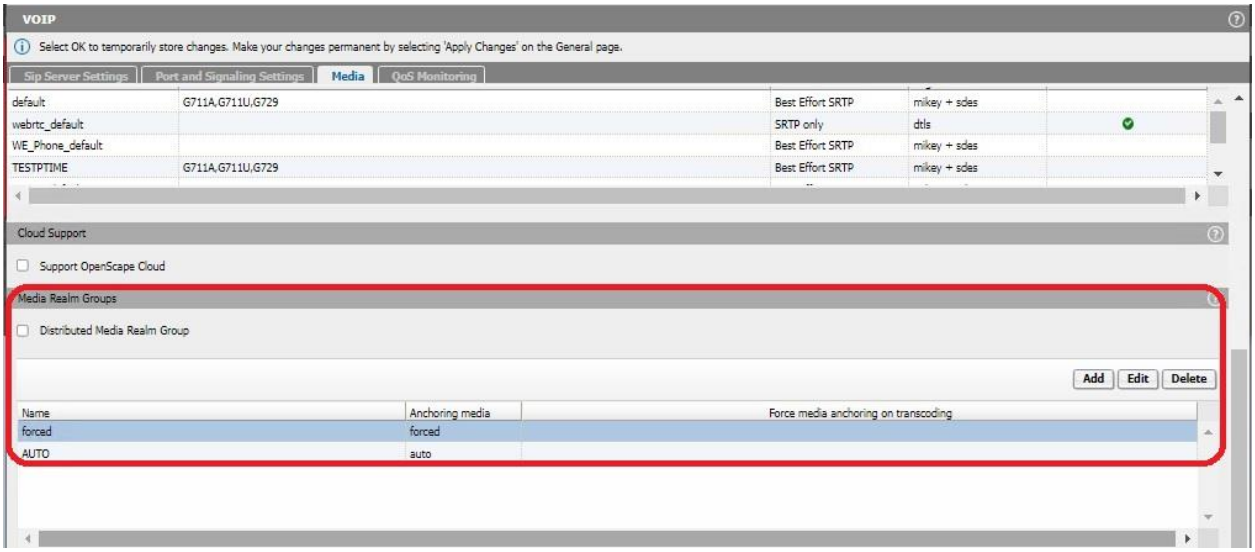
Select the subnet (example 173.16.4.0) with the option Anchor Media set to forced

- The second Realm Group to not Anchor media

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







3.4.4.7 Media Optimization

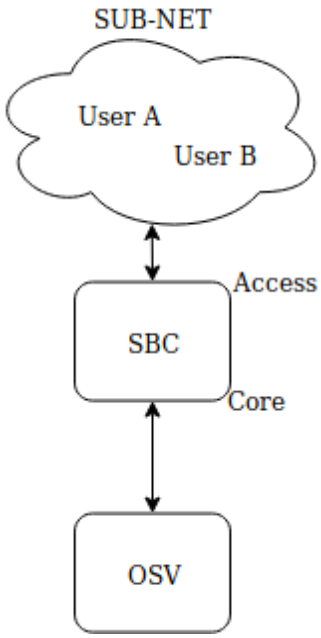
The purpose of this chapter is to give a better explanation of all media optimization possibilities in a way that the user has the full knowledge to properly configure the SBC. SBC provides two main possibilities to optimize the media path, the Media Realm Groups and Direct Media. These features are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



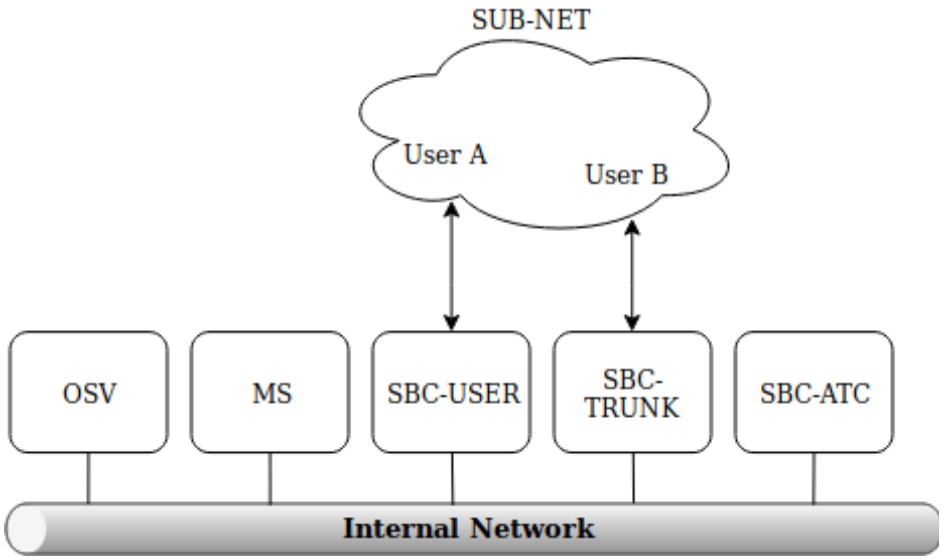
A Sub-net is configured to identify each group. The ‘auto’ option for ‘Anchoring Media’ must be chosen in order to optimize the media path. In that way, if both legs of the call are in the configured sub-net, SBC will try to establish the media directly between the endpoints.

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.

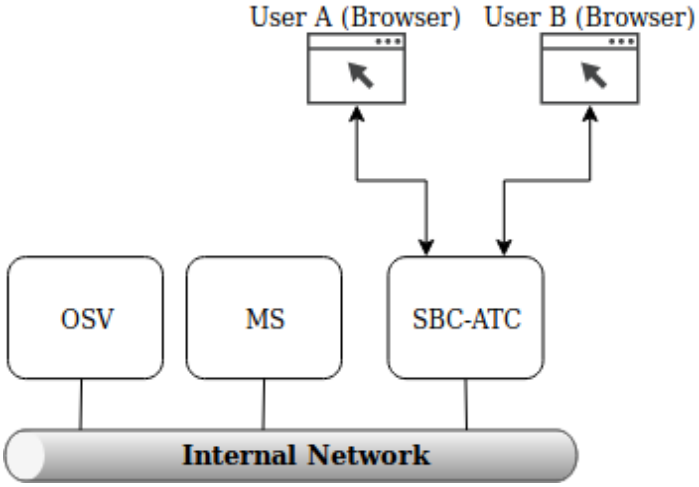
Take the example bellow, where both users A and B are in the same sub-net but connected to different SBCs, User A connected to SBC-USER and User B connected to SBC-TRUNK.



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.

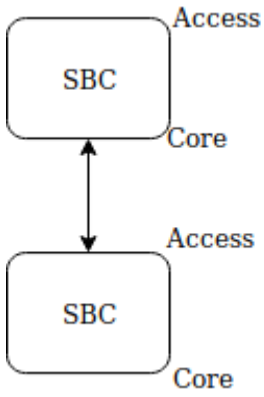


When enabled for both peers, SBC will forward the ICE and rtcp attributes from one peer to another. The rest is handled by ICE itself, which will establish the media with the pair candidates with the highest priority that can reach each other.

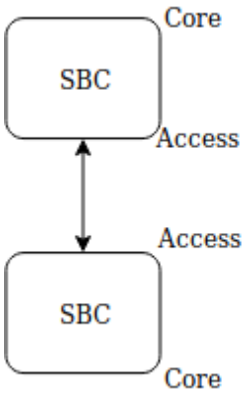
CASCADED SBCs

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

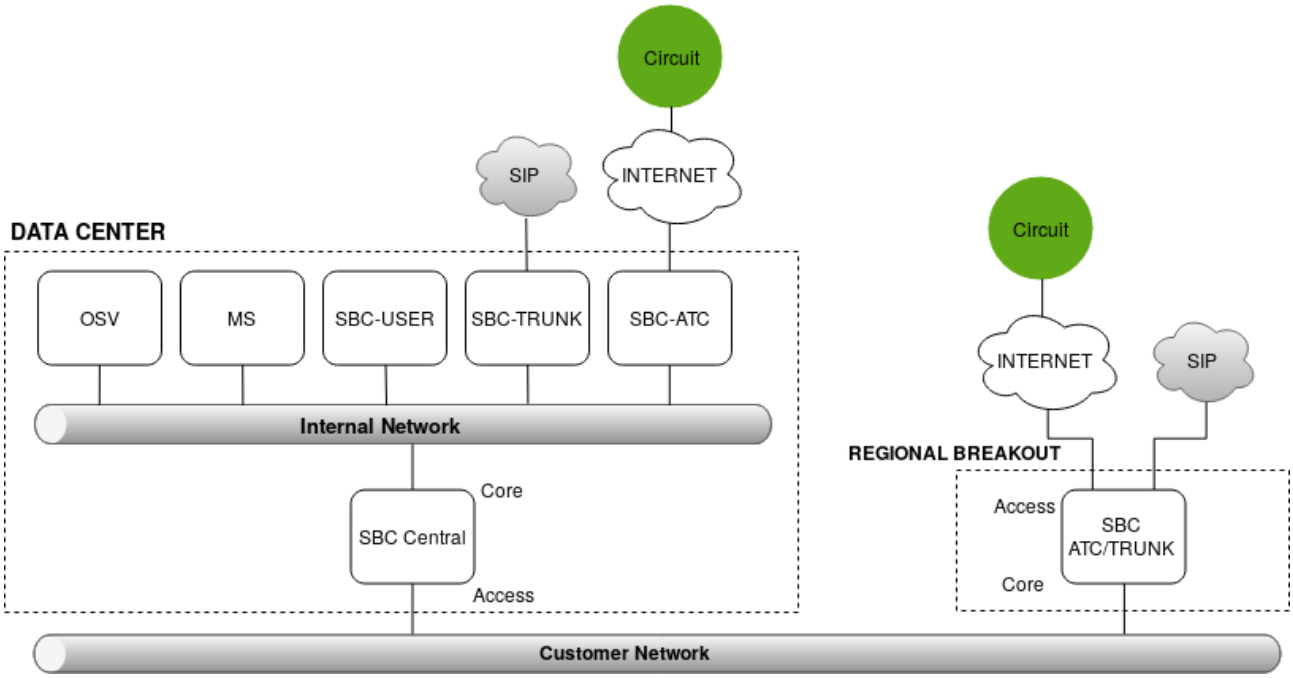
particularity regarding the media optimization because more than two components may interfere on the call negotiation (SDP).
There are two possible designs:
1 - **Core-Access** interaction



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:

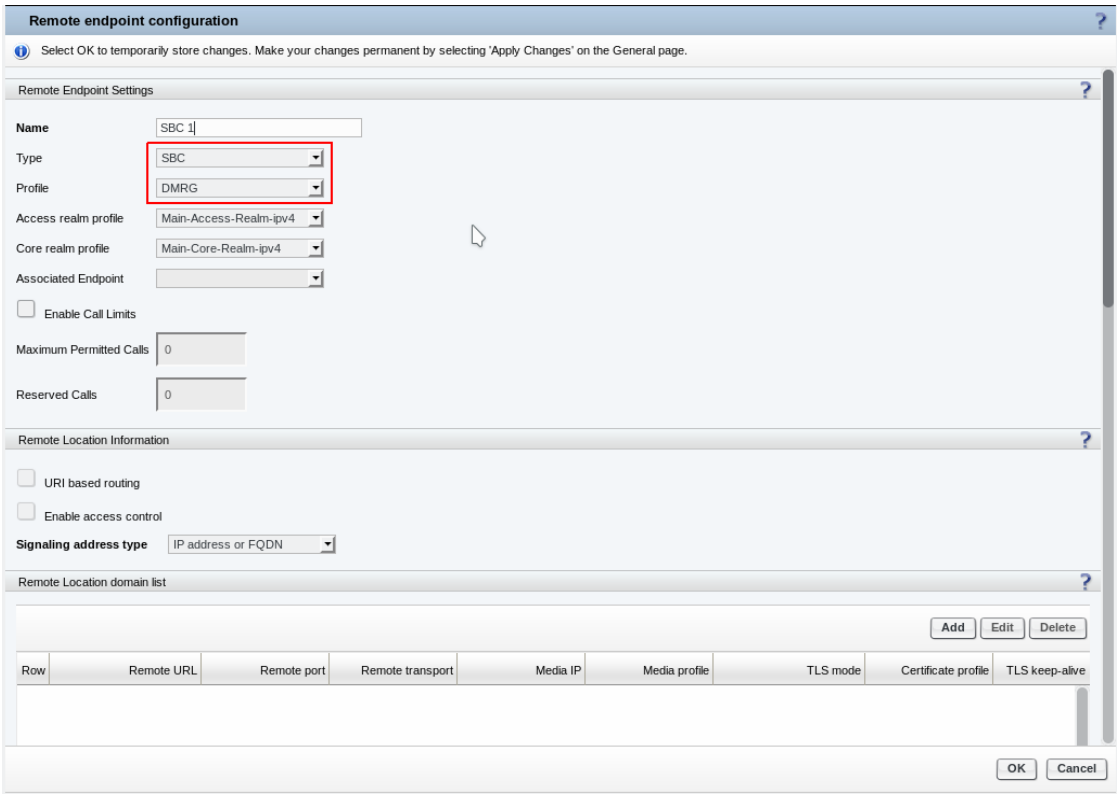
Sip Client A -> SBC on Regional Breakout -> SBC Central -> OSV -> SBC-TRUNK (DataCenter) -> Sip Client B

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



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.

3.4.4.8 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/qnMqzxKDb647ISyJ2c42rmGKLcdKvcri/zmSi
a=key-mgmt:mikey

AQAVgNCfGY4CAAAAAAAAAAAAAABElEGcAAAAAAUBAAVtaWtleQsA20XazwAA
AA
AKFETL/
+S5pSctgaHaThAq3Hmg3Gm0AQAAADYCAQEDBAAAAKAEBAAAAHALBAAAAFAAA
Q
EBBAAAAIAJAQAGAQAFAQAIAQEKAQEHAQEMBAAAAAAAAAAkABAAEOCNHUuw
zR5eU2YxgqSrhN4ADsBXllJ6WxBZvu0Pwl3ZAA==
```

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/qnMqzxKDb647ISyJ2c42rmGKLcdKvcri/zmSi
a=key-mgmt:mikey
AQAVgNCfGY4CAAAAAAAAAAAAAABElEGcAAAAAAUBAAVtaWtleQsA20Xazw
AAAA
AKFETL/
+S5pSctgaHaThAq3Hmg3Gm0AQAAADYCAQEDBAAAAKAEBAAAAHALBAAAAFA
AAQ
EBBAAAAIAJAQAGAQAFAQAIAQEKAQEHAQEMBAAAAAAAAAAkABAAEOCNHUuw
zR5eU2YxgqSrhN4ADsBXllJ6WxBZvu0Pwl3ZAA==
```

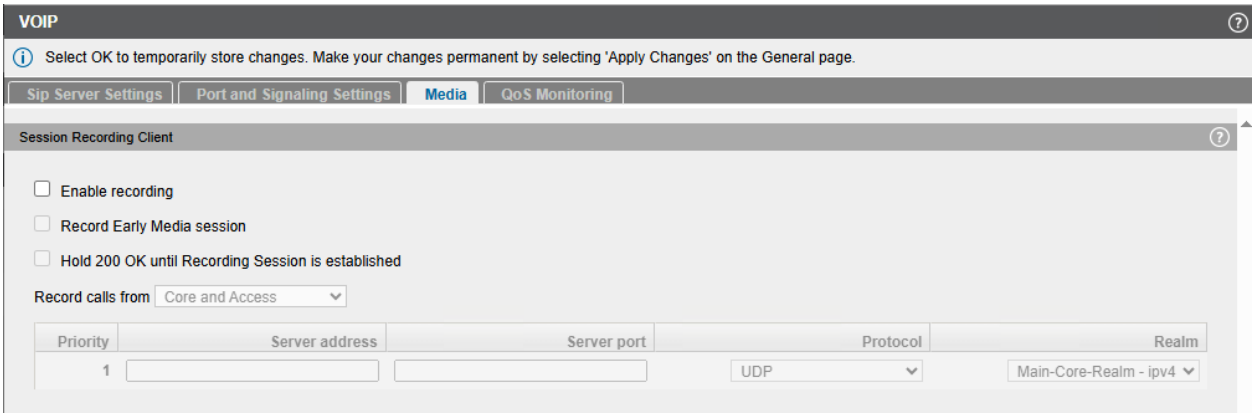
4.Now SBC2 can check the m-lines with the attribute “partnerfsm” verifying if media optimization is possible and if it is SBC rebuilds the original SDP and send it to the destination:

```
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).

3.4.4.9 Session Recording Client (SRC)

Starting from V11R2.2.0, the **Session Recording Client** (SRC) tab allows the configuration of SIP Recording Server, which records RTP streams using the SipRec protocol.



NOTICE: SipRec restrictions: Only audio will be recorded.

• **Enable recording**
This flag enables the Session Recording Server

• **Record Early Media Session**
If enabled, the SBC will start the Recording Session on receive provisional responses (180 or 183 with SDP) from call taker. The default value is Disabled.

• **Hold 200 OK until Recording Session is established**
When enabled, the SBC will delay sending the 200 OK response to the caller until the recording session is established. If disabled, the SBC will forward the response as soon as possible, which may result in media loss in the recording. The default is disabled.

• **Record calls from**
Specifies the call direction from which the SBC will record calls. The available options are:

- **Access interface**
- **Core interface**
- **All calls (Core and Access interface)**

The default is All calls (Core and Access interface).

• **Priority**
Defines the recorder's priority.

NOTICE: This setting does not affect the SBC, as it supports only one recorder.

• **Server address**
The IP address or FQDN of the recording server.

• **Server port**
The port on which the recorder listens for SIP messages.

• **Protocol**
The protocol used to communicate with the recording server. Options: **UDP**,

TCP, or **TLS**.

• **Realm**
The SIP realm associated with the recording server.

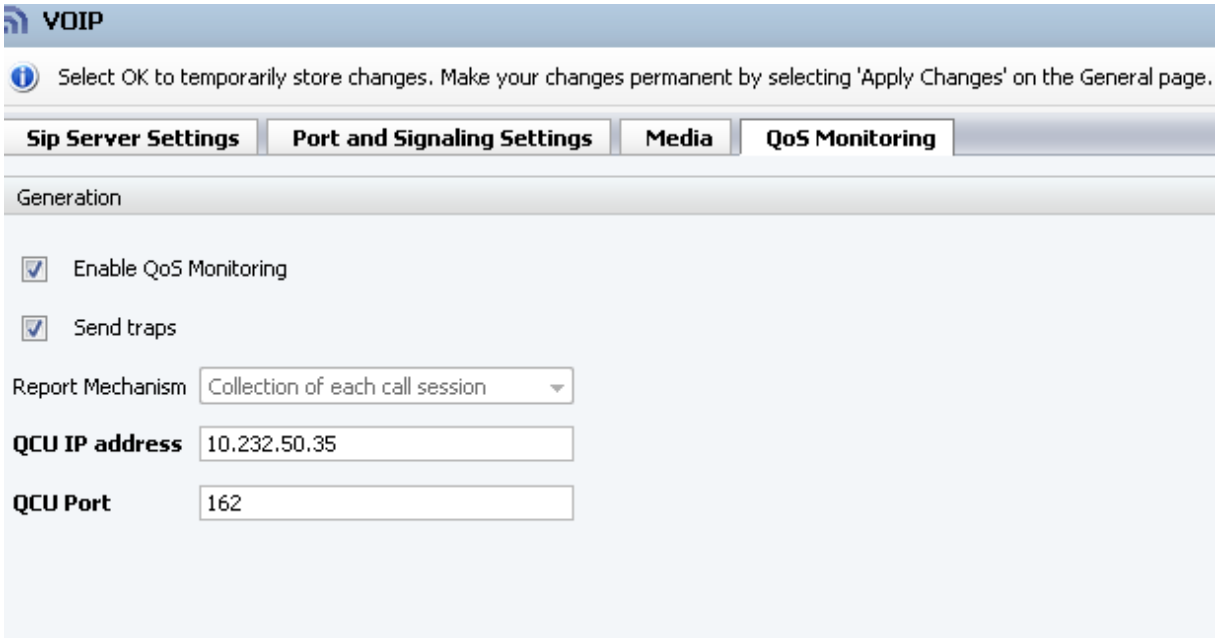
3.4.4.10 QoS Monitoring

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

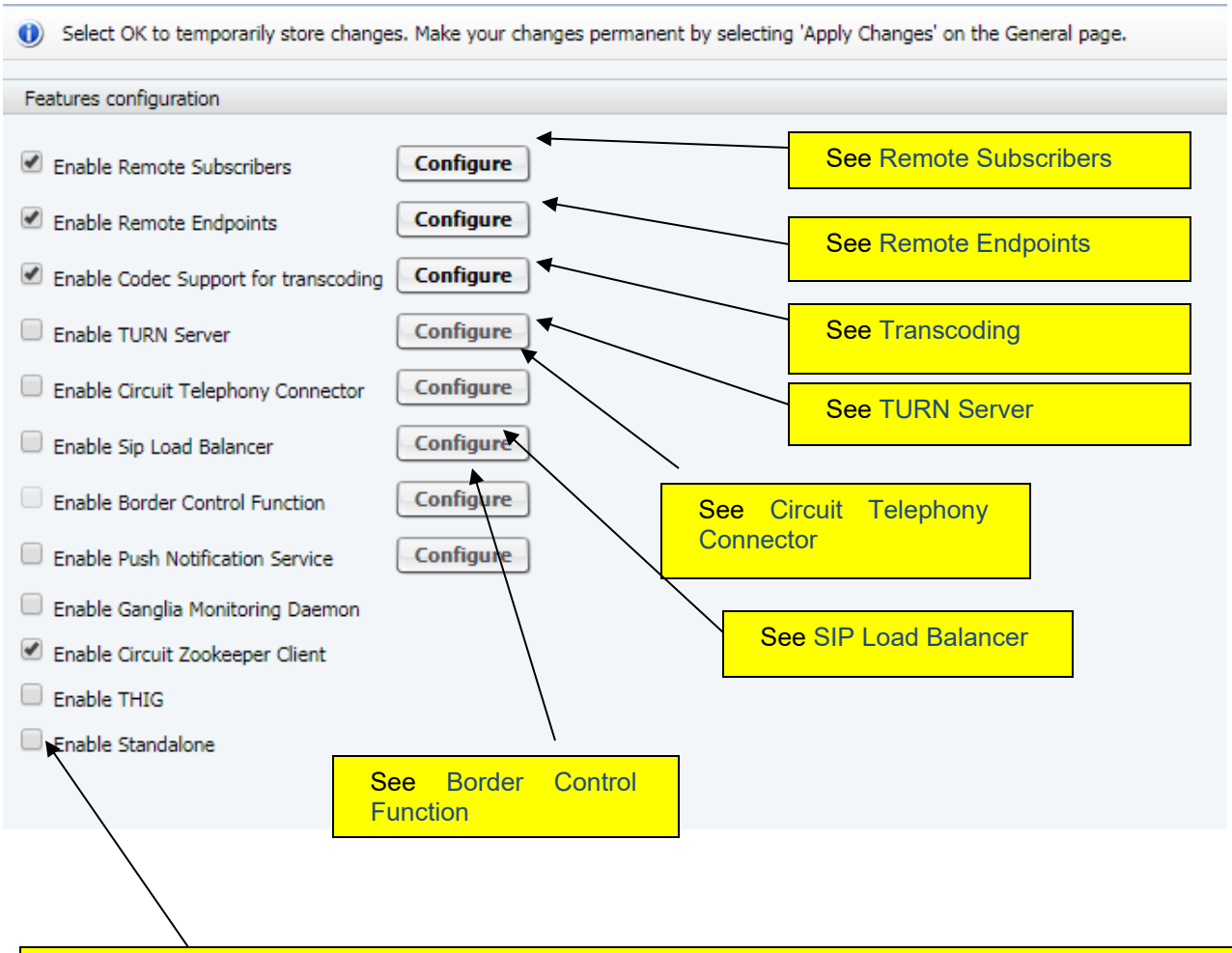
Send traps flag enables / disables the generation of traps to the QDC server. The QDC trap is generated at the end of the media session with QoS statistics report for the Access Side, the Core Side and the Remote Endpoint. The default status of this flag is unchecked.

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.



3.4.5 Features



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.

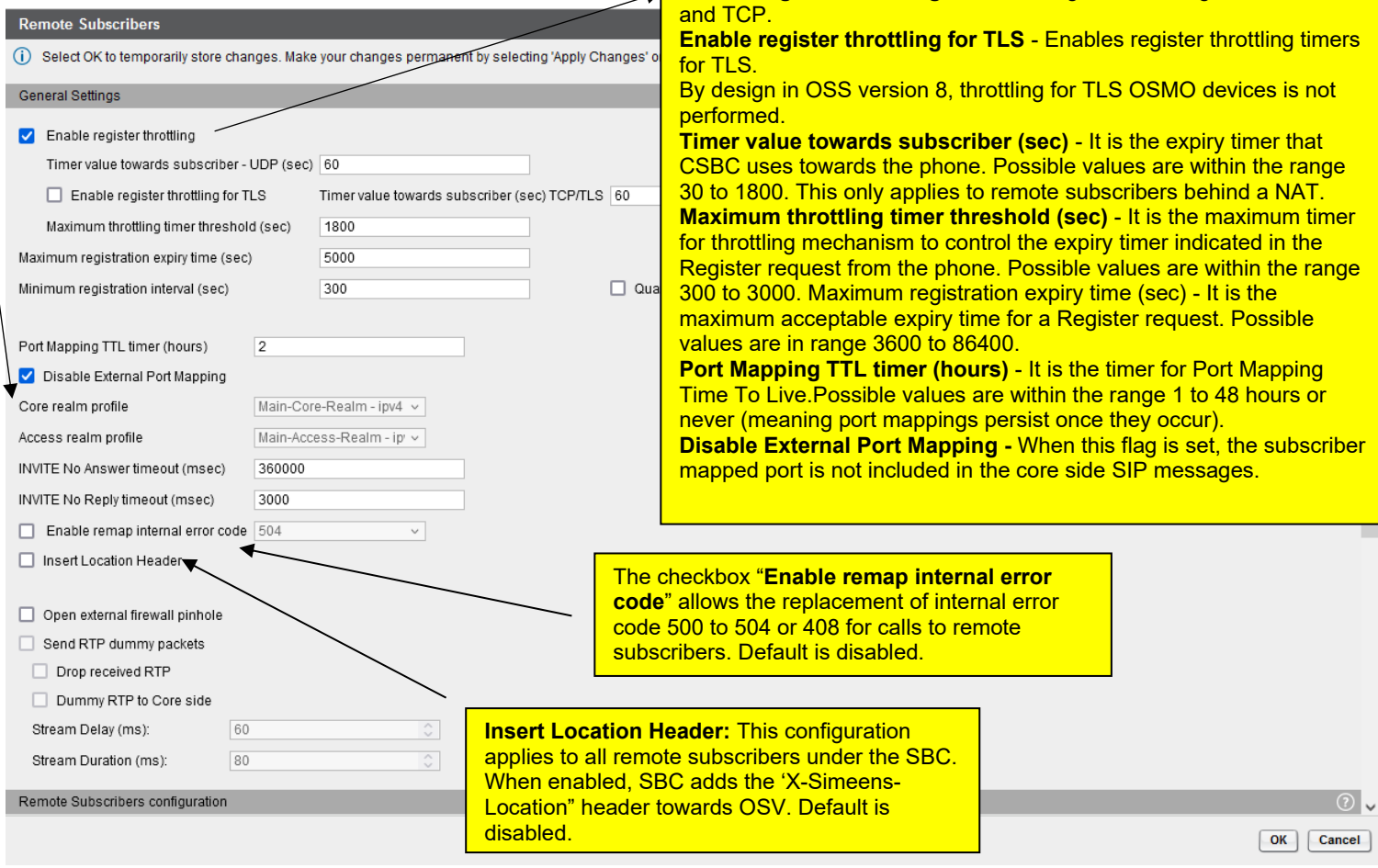
3.4.5.1 Remote Subscribers

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.

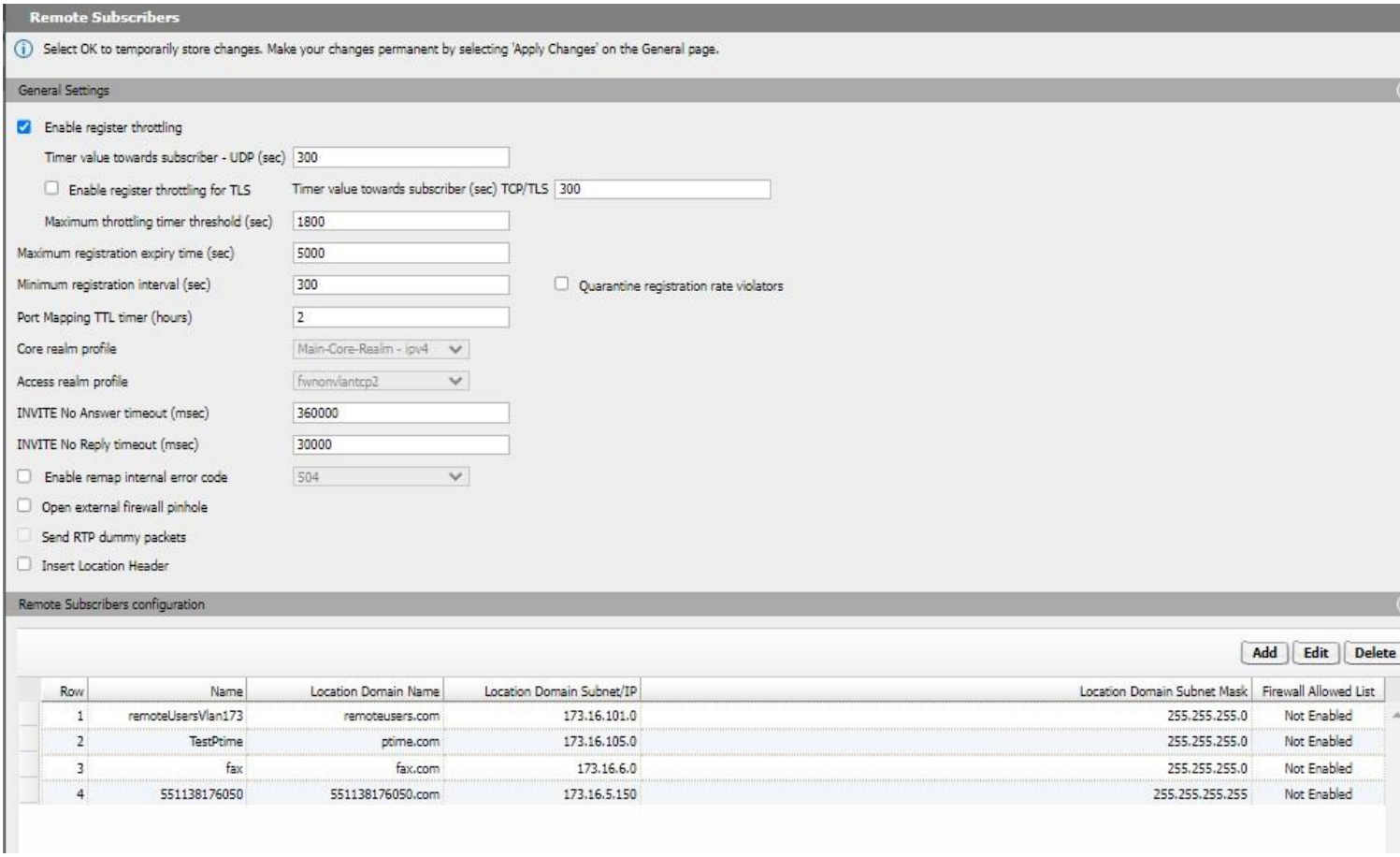
Core realm profile - For the core realm, the “Main-Core-Realm” profile is always selected by the system and cannot be modified by the user (grayed out).
Access realm profile - For the access realm, the “Main-Access-Realm” profile is always selected by the system and cannot be modified by the user (grayed 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).
Disable External Port Mapping - When this flag is set, the subscriber mapped port is not included in the core side SIP messages.

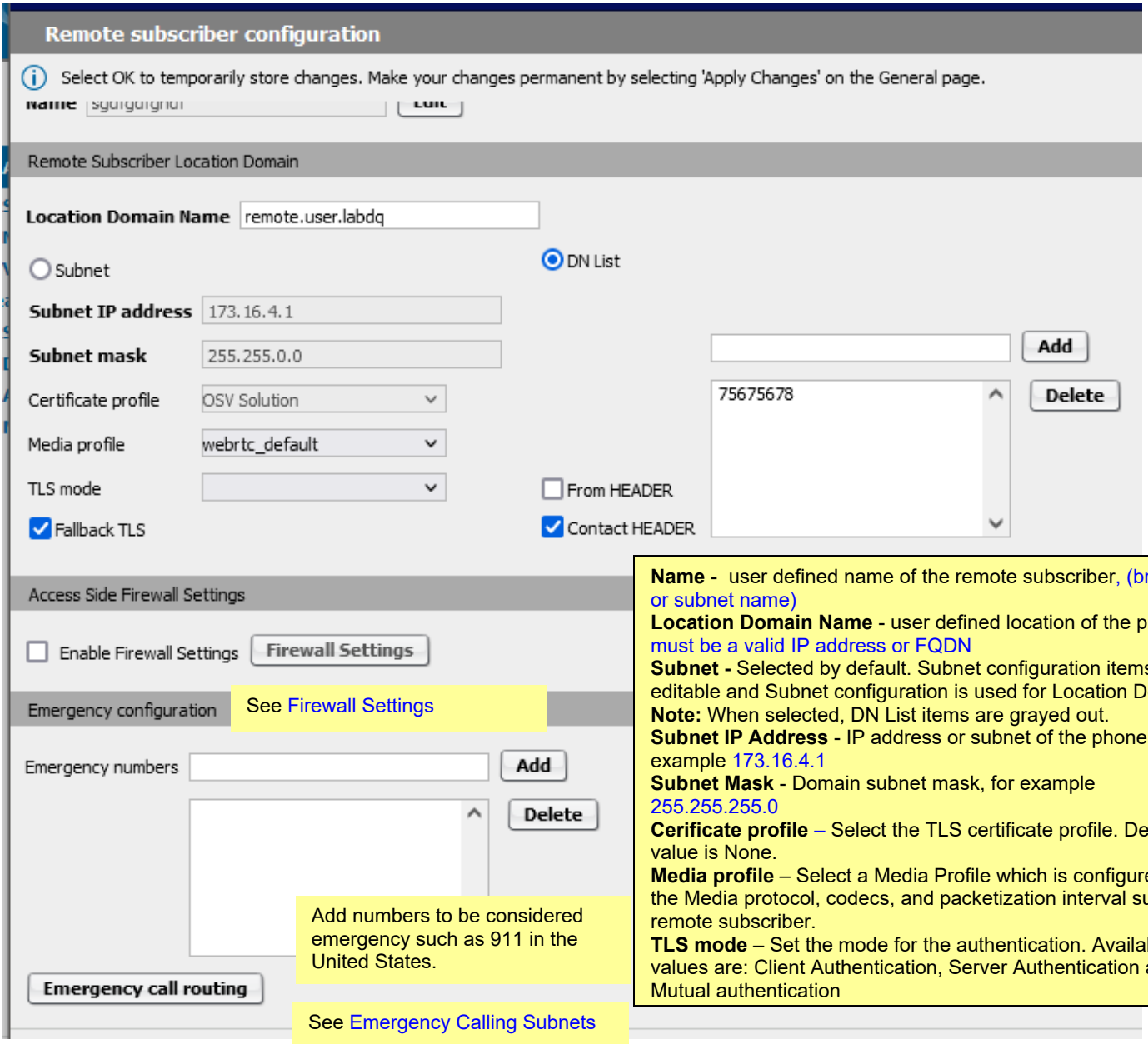
The checkbox “**Enable remap internal error code**” allows the replacement of internal error code 500 to 504 or 408 for calls to remote subscribers. Default is disabled.

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.

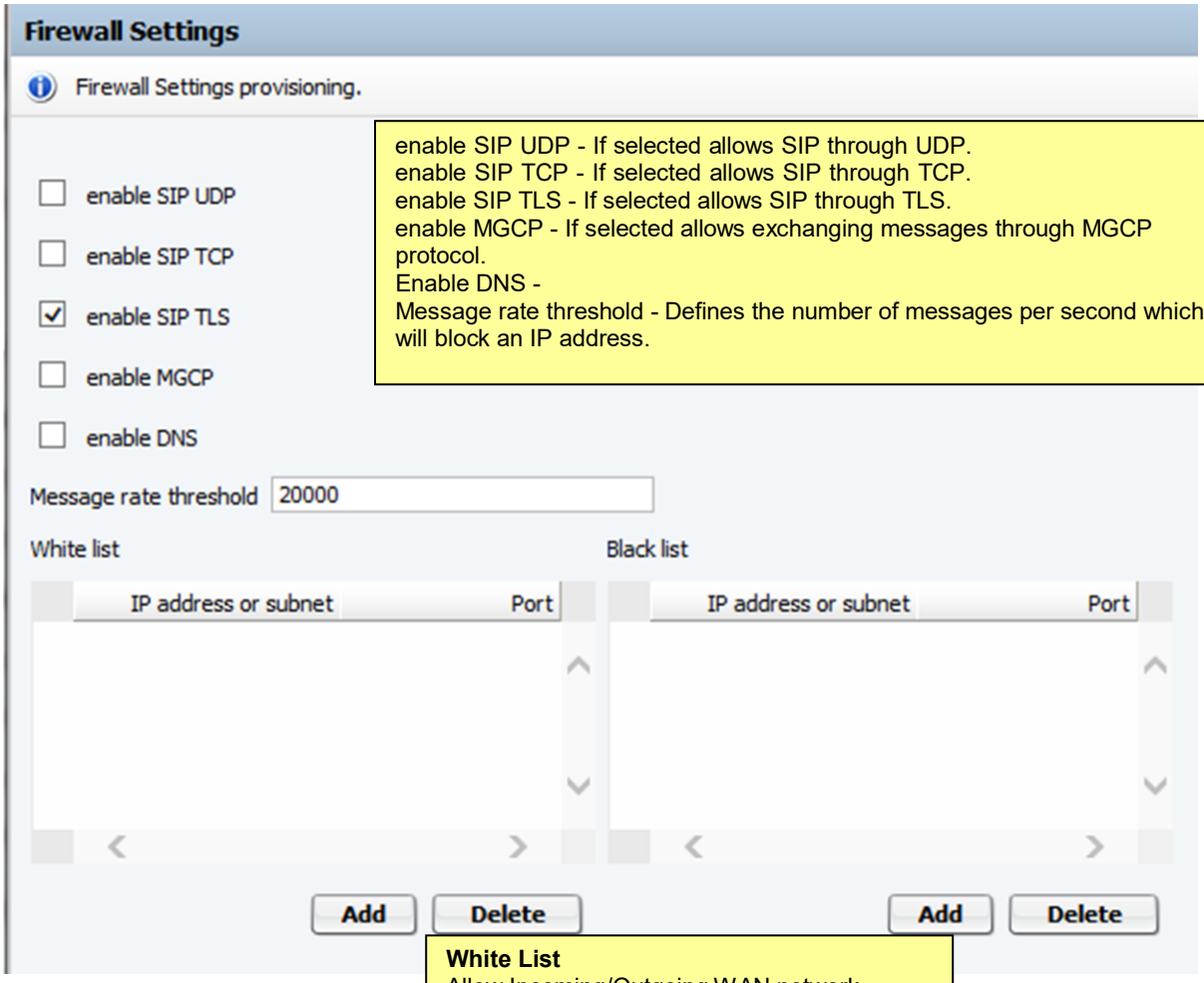


Note: By design, throttling of Registrations for TLS OSMO devices is not performed.

3.4.5.1.1 Remote Subscriber Settings



3.4.5.1.2 Firewall Settings

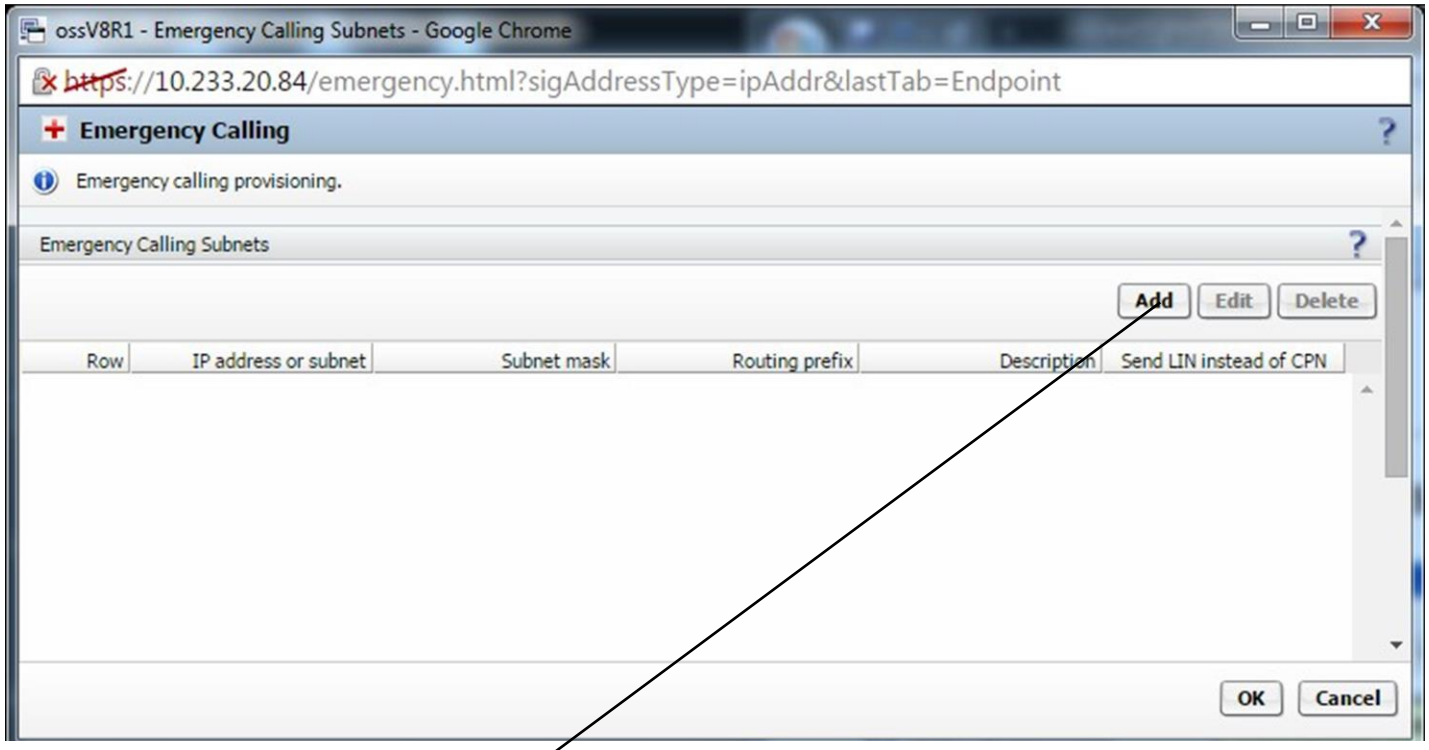


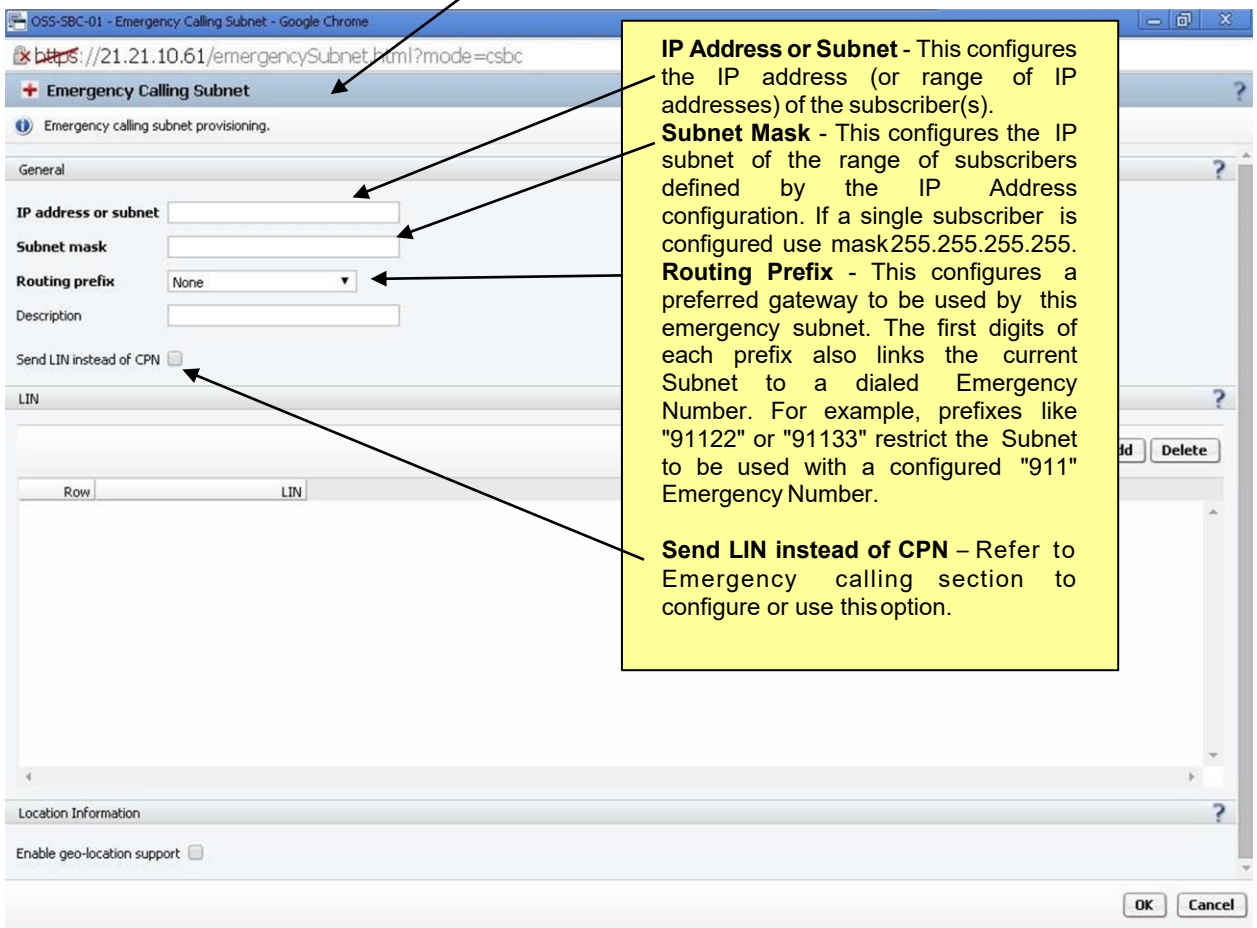
enable SIP UDP - If selected allows SIP through UDP.
enable SIP TCP - If selected allows SIP through TCP.
enable SIP TLS - If selected allows SIP through TLS.
enable MGCP - If selected allows exchanging messages through MGCP protocol.
Enable DNS -
Message rate threshold - Defines the number of messages per second which will block an IP address.

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





IP Address or Subnet - This configures the IP address (or range of IP addresses) 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" Emergency Number.

Send LIN instead of CPN – Refer to Emergency calling section to configure or use this option.

3.4.5.2 Remote Endpoints

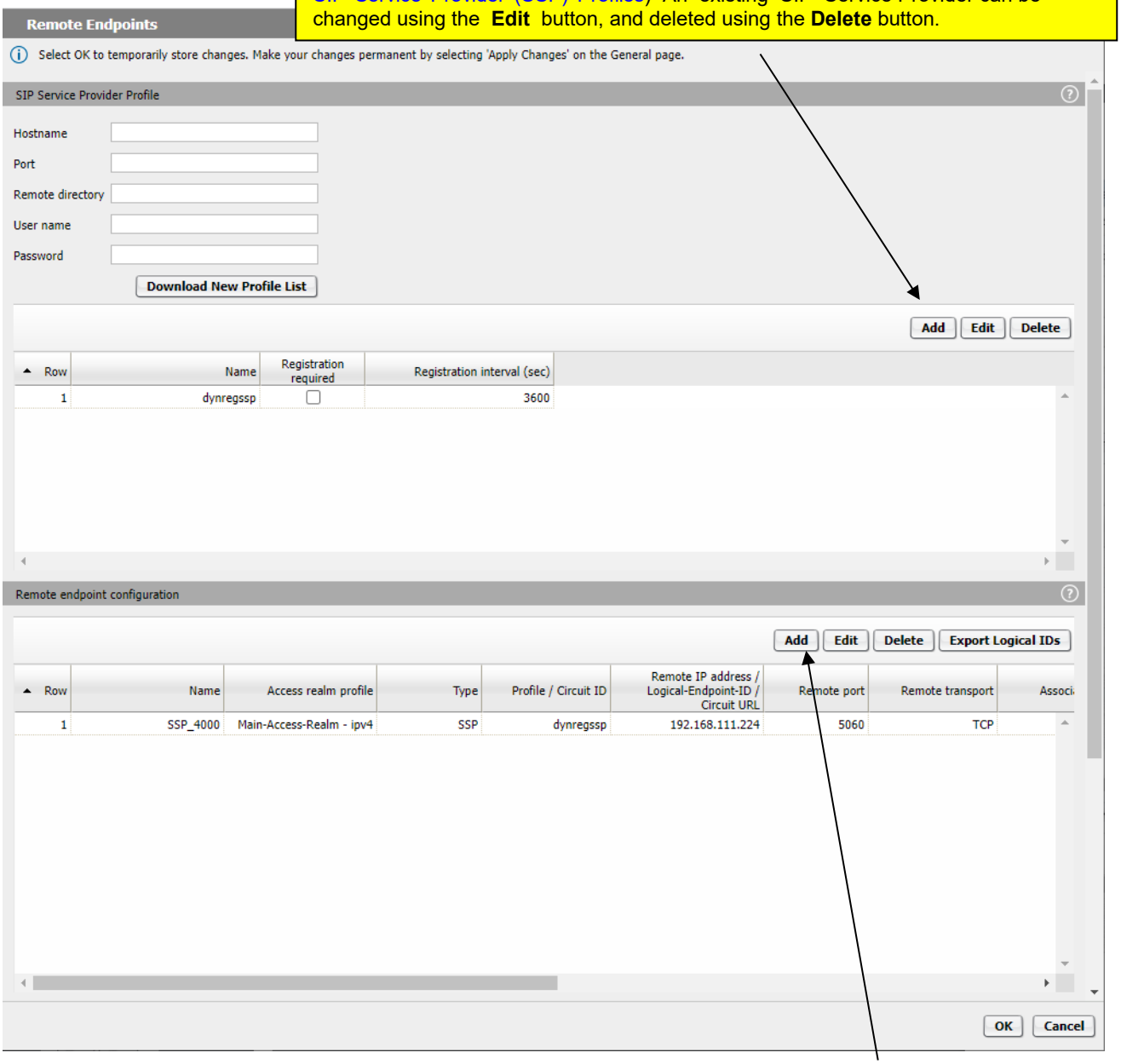
There are there different options in order to configure successful OSB iGW behind an SBC

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.

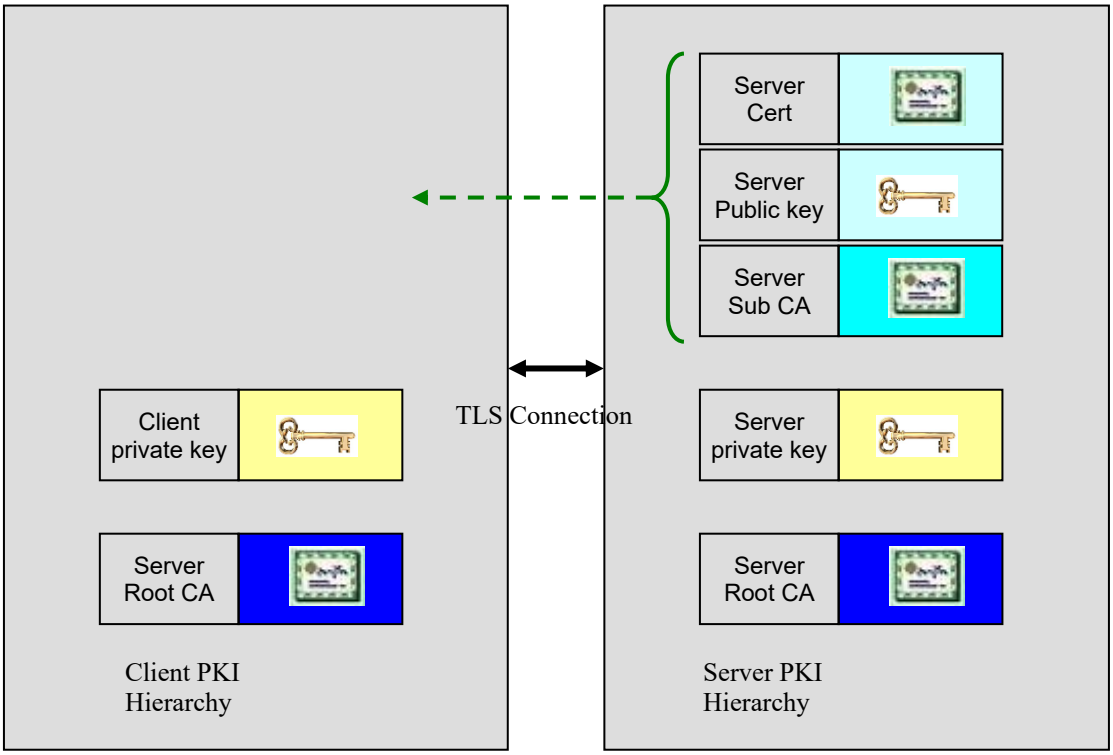


A new Remote Endpoint is configured using the **Add** button (see Remote Endpoint Configuration). An existing Remote Endpoint can be changed using the **Edit** button and deleted using the **Delete** button. Notice the "ID" in the "remote IP address/Logical endpoint ID" column indicates a dynamic IP 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:
  - The server Certificate;
  - The server intermediate CA Certificates;
  - 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.

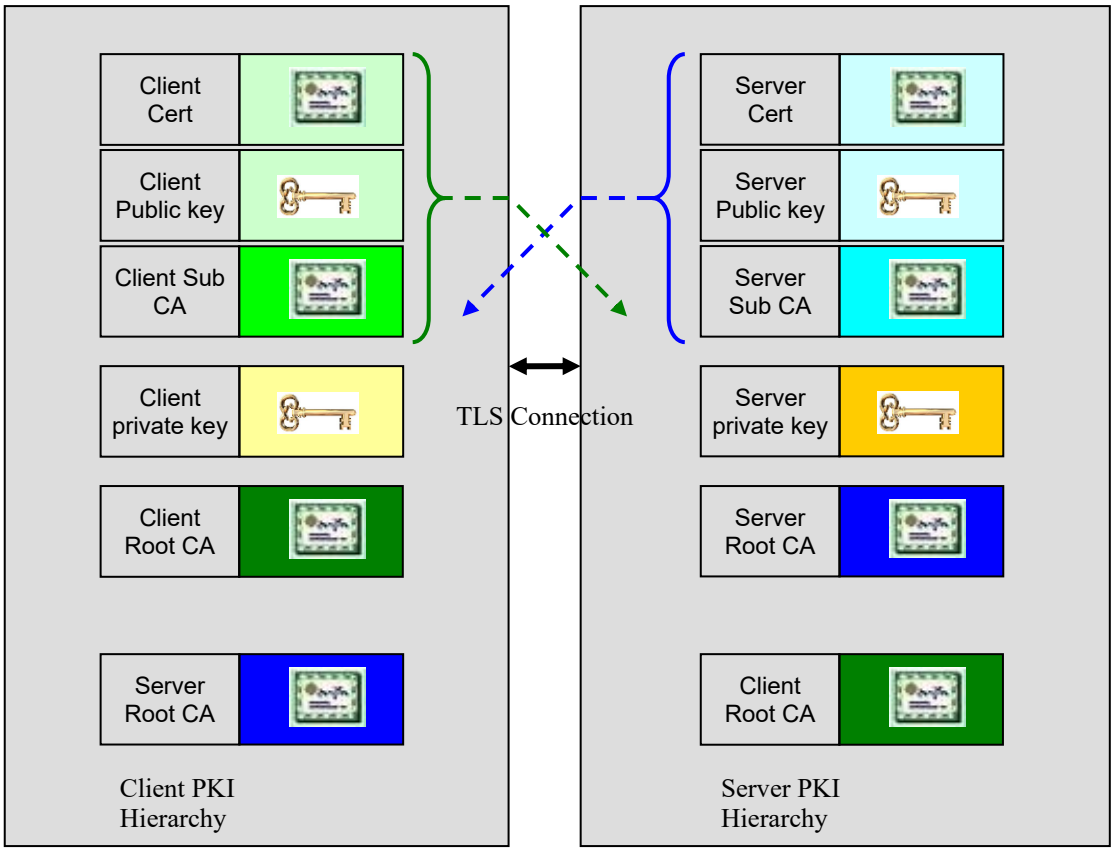


In the case of an MTLS connection in which both the TLS client and the TLS server provide their certificates, the following certificates must be stored in the client and in the server:
In the TLS Server:
- The following information shall be sent to the client during the establishment of the TLS connection:
  - The server Certificate;
  - The server intermediate CA Certificates, if any;
  - 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:
  - The client Certificate;
  - The client intermediate CA Certificates, if any;
  - 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

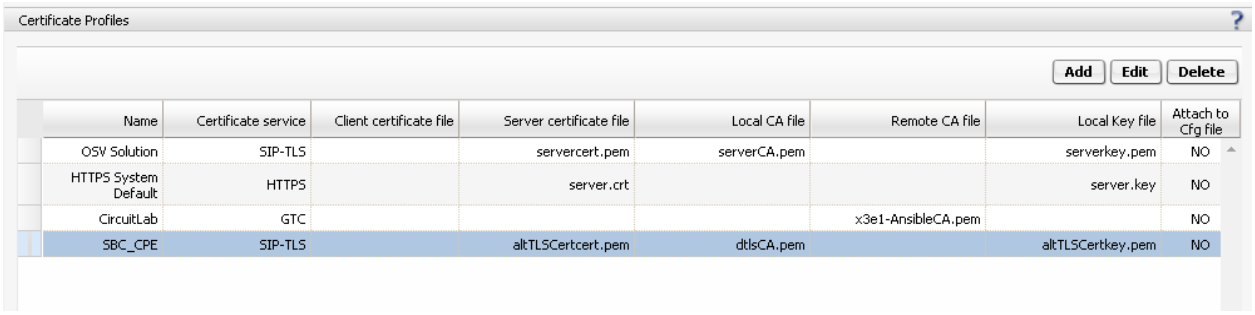
During the establishment of TLS / MTLS, certificates are exchanged between the endpoints. The certificates carry the public key, the sender identification, information about the validity period of the certificate and extensions.

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.

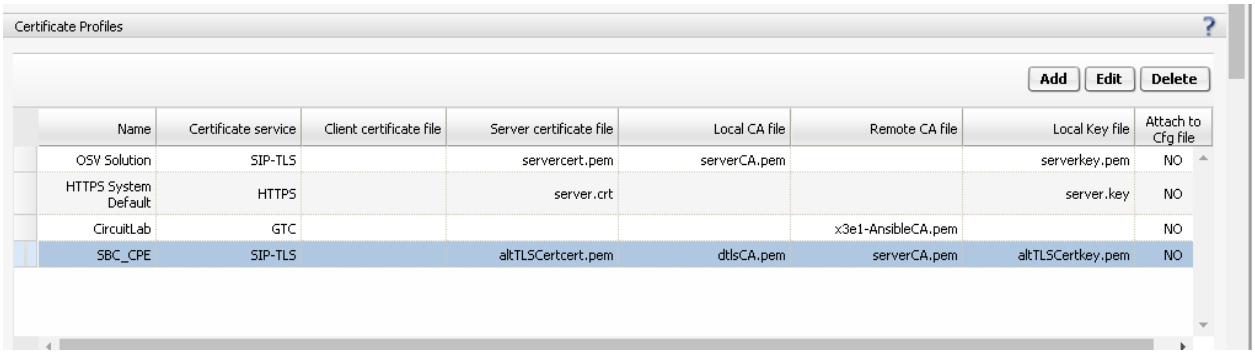
Certificate profile Setup

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:



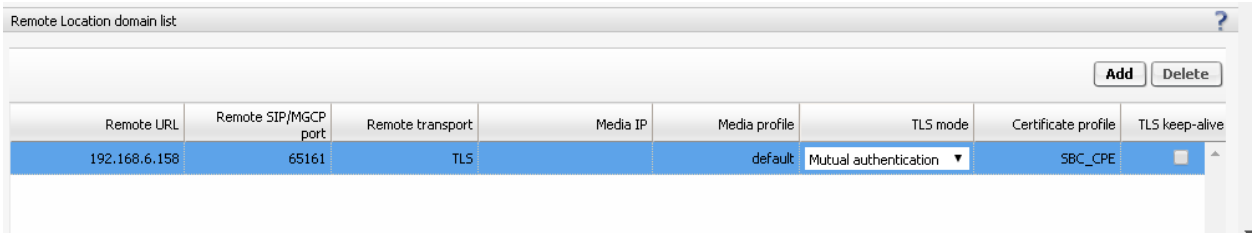
Name	Certificate service	Client certificate file	Server certificate file	Local CA file	Remote CA file	Local Key file	Attach to Cfg file
OSV Solution	SIP-TLS		servercert.pem	serverCA.pem		serverkey.pem	NO
HTTPS System Default	HTTPS		server.crt			server.key	NO
CircuitLab	GTC				x3e1-AnsibleCA.pem		NO
SBC_CPE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

And here with different CA file:



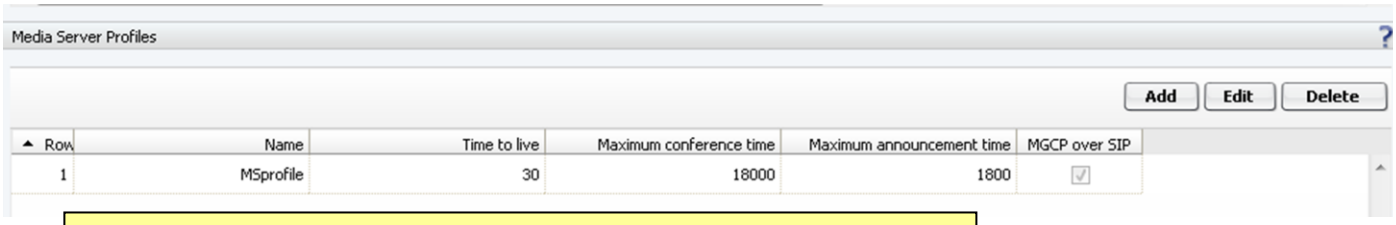
Remote endpoint TLS/MTLS configuration

On the Remote endpoint configuration the TLS mode and Certificate profile must be configured on both remote endpoints (in case of cascaded SBC).



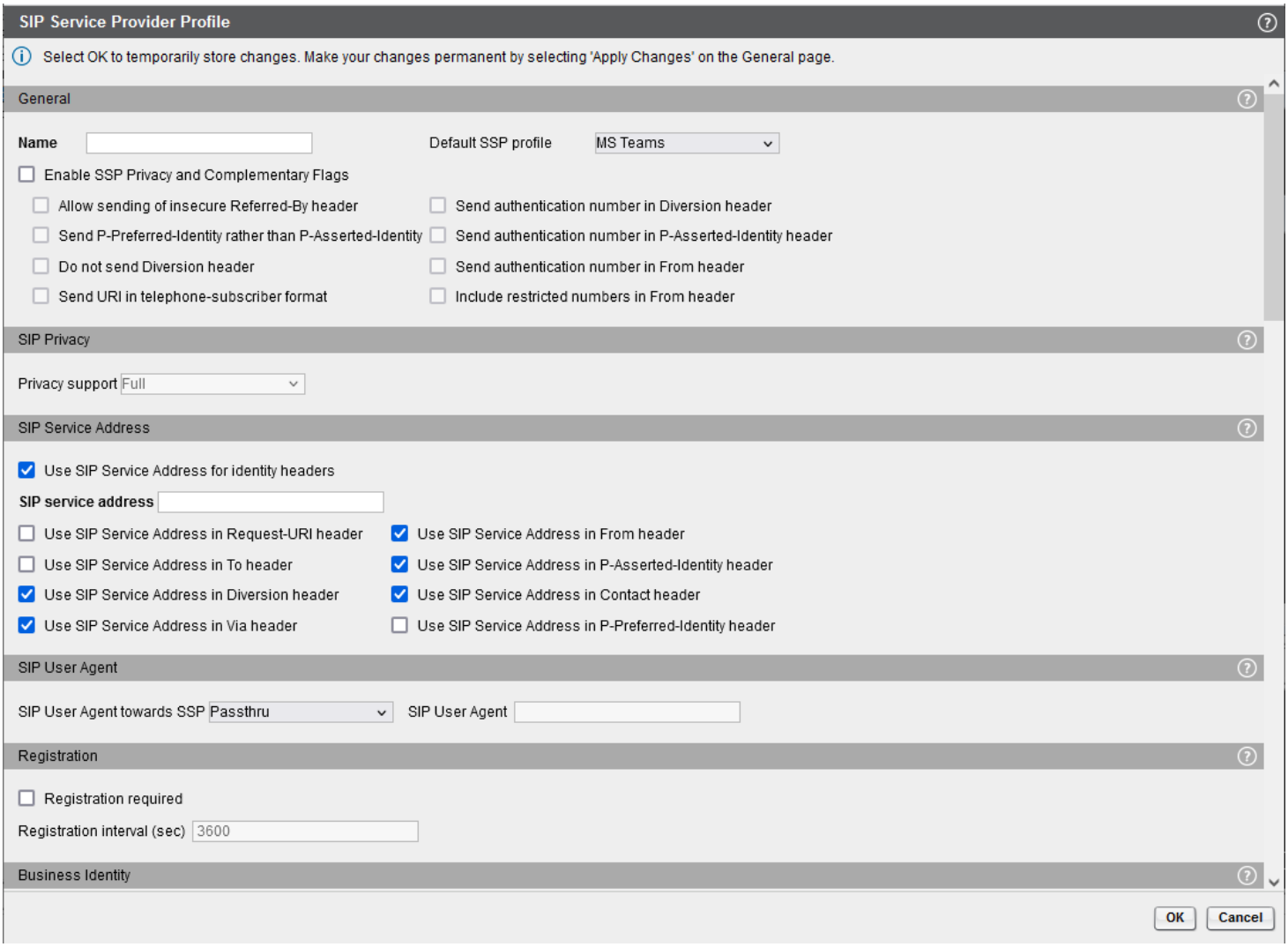
The certificate profile must be set accord to profile created in steps before.
For the TSL mode the options are: Server Authentication, Mutual Authentication and Client Only mode.
If the TLS Mode is set as Client only mode the TLS Client Request from Remote Endpoint will not be accepted.

3.4.5.3 Media Server profiles



The “MGCP over SIP” checkmark allows MGCP messages to be encapsulated inside SIP NOTIFY messages that are sent from the OSS towards hosted branch media servers. Used when creating a endpoint which is of type media server.

3.4.5.4 SIP Service Provider (SSP) Profiles



General

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

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/SDES, 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

- **Enable SSP Privacy and Complementary Flags** - This flag enables configuration and behavior of the general flags below it, and the SIP Privacy – Privacy Support field. If disabled, the behavior will be the same as previous releases (V10).
- **Allow sending of insecure Referred-By header** - When enabled, a Referred-By header field will be sent for calls transferred to the SIP Service Provider. Otherwise, the header will be removed from messages sent to SSP. The Referred-By header field is only sent for Blind Transfer scenarios. For these scenarios, the initial SIP INVITE request sent to the endpoint contains the transferred party identity as the calling party (From and P-Asserted-Identity header fields). The transferring party identity is in the Referred-By header field.
- **Send P-Preferred-Identity rather than P-Asserted-Identity** - When enabled, a P-Preferred-Identity header field will be sent whenever a P-Asserted-Identity header field would be normally sent. This attribute is primarily intended for use when connecting to a SIP Service Provider that does not accept a P-Asserted-Identity SIP header field.
- **Do not send Diversion header** - When enabled, a SIP Diversion header field will not be sent to the SSP. This attribute is primarily intended for use when connecting to a SIP Service Provider that does not understand the Diversion header field.
- **Send URI in telephone-subscriber format** - When enabled, "+" is inserted only in front of the 'R-URI' and 'TO' headers (not the FROM, PAI, or Diversion headers).
- **Send authentication number in Diversion header** - When enabled, the authentication DN will be included in the Diversion header. The authentication number can be the Authentication user ID, Default Home DN or Business Identity DN, depending on the SSP profile configuration. For calls that are redirected to the SSP, the calling party number may not be a subscriber that belongs in that SSP. In this case, the SSP needs to authenticate the call based on the number of the redirecting subscriber, i.e., the number contained in the Diversion header.
- **Send authentication number in P-Asserted-Identity header** - When enabled, the authentication DN will be included in the PAI or PPI header. The authentication number can be the Authentication user ID, Default Home DN or Business Identity DN, depending on the SSP profile configuration. Most SSPs authenticate all incoming calls to assert that the call has been originated by a subscriber (DID Number) that belongs to that provider. For some SSPs the authentication is done with the calling party number provided in the P-Asserted-Identity header field.
- **Send authentication number in From header** - When enabled, the authentication DN will be included in the From header. The authentication number can be the Authentication user ID, Default Home DN or Business Identity DN, depending on the SSP profile. Most SSPs authenticate all incoming calls to assert that the call has been originated by a subscriber (DID Number) that belongs to that SSP. For some SSPs the authentication is done with the calling party number provided in the From header field.
- **Include restricted numbers in From header** - When enabled, the authentication number present in PAI, PPI or Diversion headers will be present in From header in situations where it should be restricted (i.e., in the presence of "Privacy:id" header).

SIP Privacy

Define Session Border Control behavior in respect to receiving/sending/ignoring PAI (or PPI) header.

If Privacy Support is set to **Basic**, the OpenScape Session Border Control SHALL NOT send a P-Asserted-Identity header field in the messages (requests or responses) to the endpoint. The Unify

OpenScape Session Border Control SHALL also ignore any received P-Asserted-Identity header fields.

If Privacy Support is set to **Full**, the OpenScape Session Border Control SHALL send a P-Asserted-Identity (or a P-Preferred-Identity) header field in the messages (requests and responses) to the endpoint. The Unify OpenScape Session Border Control SHALL also accept any received P-Asserted-Identity header fields. If the caller ID is restricted, the "Privacy: id" header will be sent to the SSP.

If Privacy Support is set to **Full-Send**, the OpenScape Session Border Control SHALL send a P-Asserted-Identity (or a P-Preferred-Identity) header field in the messages to the endpoint. However, the OpenScape Session Border Control SHALL ignore any received P-Asserted-Identity header fields. If the caller Id is restricted, the "Privacy: id" header will be sent to the SSP.

If Privacy Support is set to **Full-Receive**, the OpenScape Session Border Control SHALL NOT send a P-Asserted-Identity header field in the messages (requests and responses) to the endpoint. However, the Unify OpenScape Session Border Control SHALL accept any received P-Asserted-Identity header fields.

SIP Service Address

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

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.

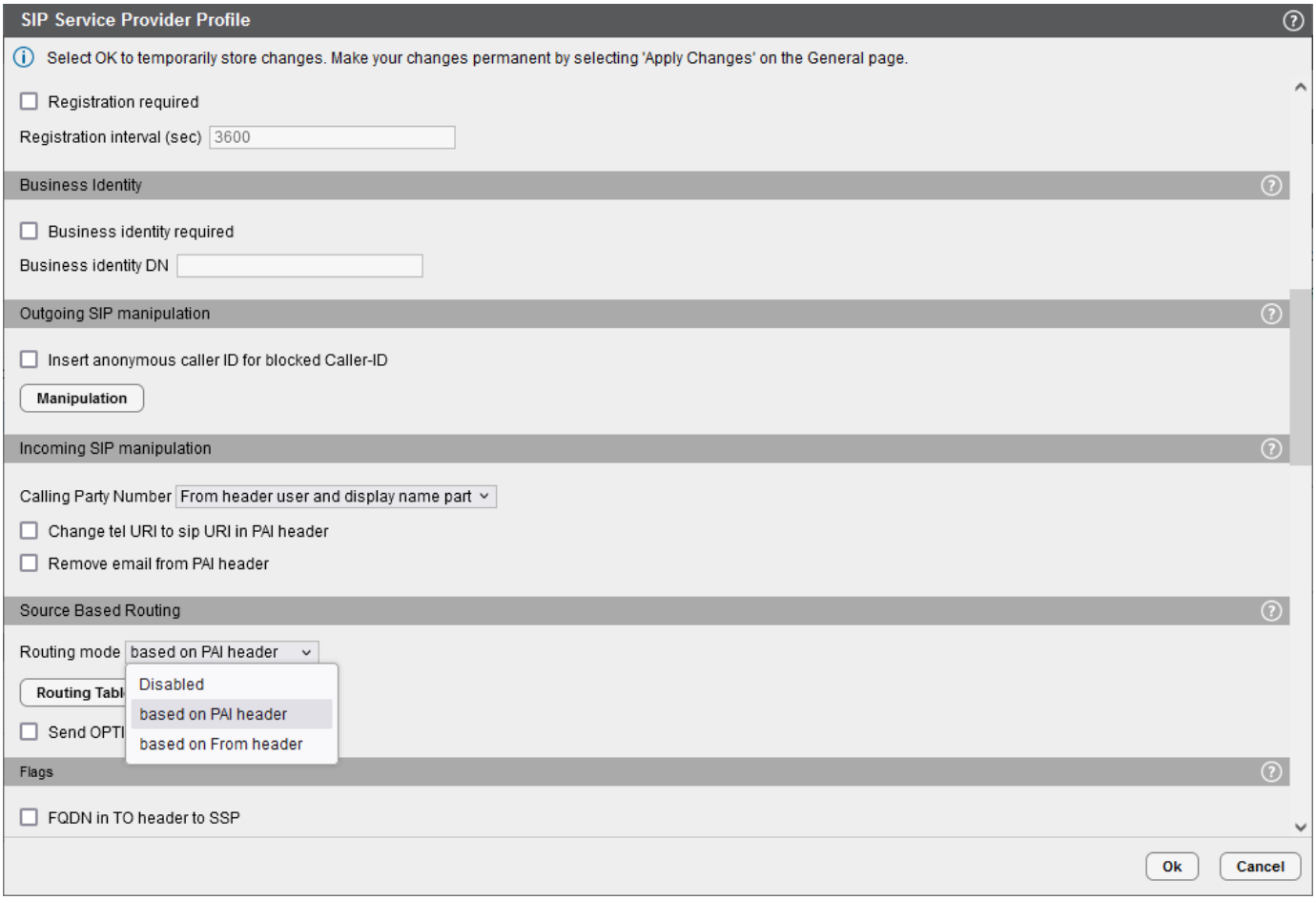
IMPORTANT: If no User Agent is received from the LAN side, the configured User Agent will be added.

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''

Registration

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

- **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

Outgoing SIP manipulation

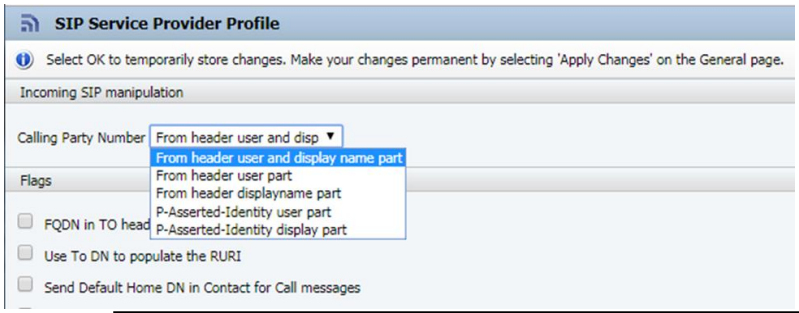
- **Insert anonymous caller ID for blocked Caller-ID** - If enabled, blocked Caller-ID's will be updated by adding Anonymous to message headers.
- **Manipulation** - Opens the Outgoing SIP Manipulation configuration window allowing creation/modification/deletion of specific SIP manipulation rules.

Incoming SIP manipulation

- **Change tel URI to sip URI in PAI header** - If enabled, the incoming call converts a PAI header with TEL URI to a PAI header with SIP URI. In that case, the parameter "user=phone" is included in the SIP URI.
- **Remove e-mail from PAI header** - If enabled, the incoming call with e-mail (alphanumeric user and domain) in the PAI header is removed.

Most of SSPs send the calling party number only in the user party of From or P-Asserted-Identity headers. However, some provides send the user and display name parts of those headers as described in RFC2161. This configuration item allows to configuration which information shall be used.

The possible options are:



From header user and display name part: Preserves the user and display name parts of From header. **Default value.**
From header user part: Uses the From user part as the Calling Party Number. If present, the display name is removed from this header.
From header display name part: Uses the display name part of the From header as the Calling Party Number. If present, the display name replaces the user part in From header. Otherwise, no manipulation is done.
P-Asserted-Identity user part: Uses the P-Asserted-Identity user part as the Calling Party Number. If present, the display name is removed from this header.
P-Asserted-Identity display name part: Uses the display name part of the P-Asserted-Identity header as the Calling Party Number. If present, the display name replaces the user part in P-Asserted-Identity header. Otherwise, no manipulation is done.

SIP User Info header and Regex

Available only for SIP Service Provider Profile with "MS Teams" as the Default SSP profile. It allows the manipulation of the user part of incoming From or/and P-Asserted-Identity headers using a regular expression.

It is possible to select the following options:

1. None
2. From header
3. P-Asserted-Identity header
4. From and P-Asserted-Identity headers

The first item disables the feature and is the default value. The other options modify the respective header and require the configuration of Regex, which is a regular expression based on POSIX regex substitutions.

Regex format

The regex format is the following: /{ME}/{RE}/{F}

See below the description for each item:

- {ME}: Match expression (Posix regular expression)
- {RE}: Replacement expression is substitution expression with back references to matched tokes: \1, \2, ..., \9
- {F}: flags (optional):
  - i - match ignore case
  - s - match within multi-lines strings
  - g - replace all matches

Some characters are not allowed by configuration ("|", "@", "<", and ">") and the limit is 64 characters in length.

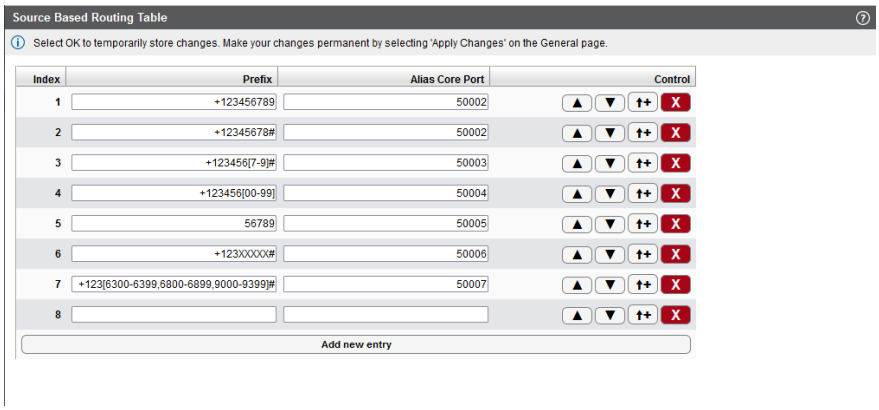
If the match expression has no match, the replacement is not performed. The same occurs if the regular expression does not result in a valid URI user part.

Example:

Received From header URI:
sip:+441291222222;ext=6963333@sip.pstnhub.microsoft.com:5061;user=phone
Received User part of From header URI: +441291222222;ext=6963333
Regular expression configured for From header: /^.*;ext=(.*)$/\1/
New user part of From header URI: 6963333

Source Based Routing

Note: This configuration is only available in V11R1.01.00 or higher.



- **Source Based Routing table** - In the table it is possible to add a prefix and alias core port. The prefix can have up to 20 characters and can contain digits and the characters "[", "]", ",", "+", "-", "X", and "#".

The character "+" can be used in the initial prefix. The character "X" means any digit that can be included in any position. The character "#" can be used in the last position to indicate that no more digit is expected after a prefix.

Ranges of digits can be configured as in the following example:

- "[23-34,55-58]" means two ranges: one from 23 to 34 and another from 55 to 58.

A list of numbers can be also configured using brackets:

- For example, the list of numbers 234, 345, and 678 can be configured as "[234,345,678]".

When multiple prefixes match the configured header for source base routing, the following priority sequence will be used:

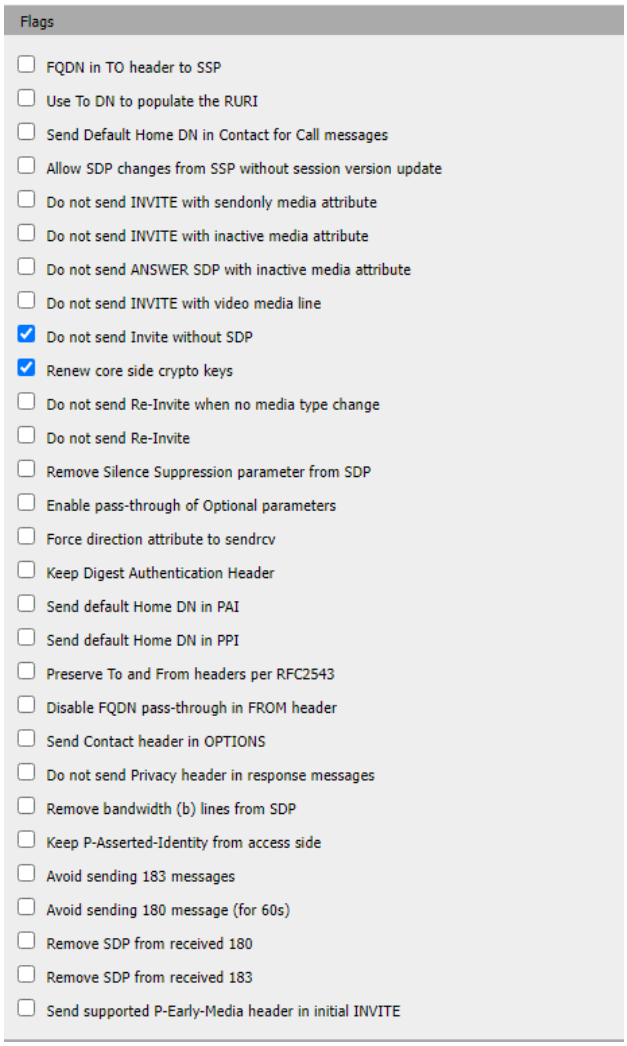
1. The Specific Prefix (complete digits)
2. Prefix with wildcards "X"
3. Ranges of digits in multiple prefixes

The Alias core port column should contain one alias core port in the range of remote endpoint core ports and this port can be duplicated in one or more rows in the table and can be included in other profiles tables. But, it should not be configured as a core port of a remote endpoint.

- **Routing mode** - This item allows enabling the source base routing using the user part of PAI or From header. The options are:
  - **Disabled** - Disable the source base routing.
  - **Based on PAI header user part** - Use the PAI header user part to match a prefix for an alias port.
  - **Based on From header user part** - Use the From header user part to match a prefix for an alias port.

- **Send OPTIONS to Alias ports** - This flag allows sending SIP OPTIONS messages periodically with 60s intervals to all configured alias ports from the profile prefix table.

Flags



- **FQDN in TO header to SSP** - If selected (enabled), To header is modified for the in-dialog SIP Requests sent to SSP with FQDN configured for SSP.
- **Use To DN to populate the R-URI** - Enable if the SIP Service Provider is sending the Account information in the Request URI and the destination information in the To header. Disabled by default.
- **Send Default Home DN in Contact for Call messages** - If enabled, the configured default home DN is used to set the Contact header only for call messages.
  It is not applicable for REGISTER message. Disabled by default.
- **Allow SDP changes from SSP without session version update** - Flag to take care of SSP which are incorrectly keeping the same session id and session version but changing the contents of the SDP.
- **Do not send INVITE with sendonly media attribute** - Do not send INVITE with sendonly media attribute to SSP.
- **Do not send INVITE with inactive media attribute** – Change ‘inactive’ media attribute to ‘sendrecv’ in the OFFER SDP.
- **Do not send ANSWER SDP with inactive media attribute** - Change ‘inactive’ media attribute to ‘sendrecv’ in the ANSWER SDP
- **Do not send INVITE with video media line** - Do not send INVITE with video media line to SSP.
- **Do not send Invite without SDP** - Do not send INVITE without SDP to SSP. When enabled, the SBC interworks an INVITE without SDP to an INVITE with SDP towards the SSP, which does not

support INVITE requests without SDP. All re-invites originating from the core side that include SDP, will be delivered to the access side using normal processing procedures such as transcoding and m-line type modifications. However, if a re-invite without SDP is sent from the core side to the access side, SSM will retrieve the most recent SDP sent to the access side, remove the media attribute (sendrecv, inactive, sendonly, or recvonly) and send the re-invite to the access side.

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.

INFO: To use the flags, LAN-WAN or LAN-SSP interworking must be enabled.

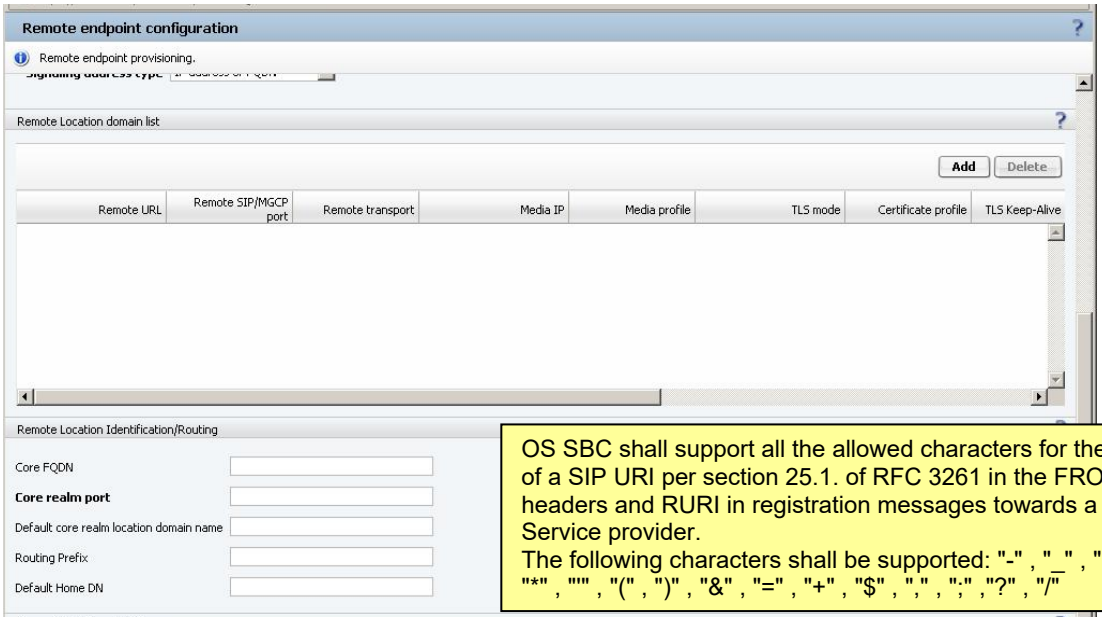
- **Remove Silence Supression parameter from SDP** - Remove the attribute for silence suppression in the SDP towards the SIP Service Provider. Disabled by default.
- **Enable pass-through of Optional parameters**- When enabled, you may configure up to 10 optional SIP - Header parameters pass-through 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.

Note: 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.



- **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.
- **Remove SDP from received 180** - If set, the SBC will remove the SDP from received 180 Ringing messages
- **Remove SDP from received 183** - If set, the SBC will remove the SDP from received 183 Session Progress messages
- **Send supported P-Early-Media header in initial INVITE** - If set, the SBC adds the "P-Early-Media: supported" header in the initial INVITE

  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 adresses.

TLS

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

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

transport=tls - Uses parameter "transport=tls" in SIP messages and does notaccept 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 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-rtcpx
- **Bulk registration required** - When checked, then the Registration AOR must also be configured. In this case the OSB/SBC shall use the configured Registration AOR in the FROM and TO headers of the REGISTER request towards the SSP.
- **Registration AOR** - The SIP-PBX must be capable of provisioning any format of SIP-URI as the Registration AOR, in order to accommodate SP-SSE requirements

Survivable Branch Appliance

This session configures the MS Teams Survivable Branch Appliance (SBA) for Direct Routing. When the SBA is activated, the SBC will fork Public Switched Telephone Network (PSTN) calls to the Microsoft Phone System and the SBA. This configuration ensures that Microsoft Clients can sustain the ability to initiate and receive PSTN calls even when communication with the Microsoft Cloud is disrupted.

- Enable SBA for MSTEAMS - If the checkbox is enabled, the SBA service is enabled and the fields must be set up.
- Certificate profile - The certificate must be the same as the one added on the SBA Server. It is recommended to use a specific certificate for the SBA.
- FQDN - The SBA Server FQDN.
- Port - By default, SBA uses port 5061.

Emergency Call Configuration

In the SSP profile, a new flag enables the PSAP capabilities, identifying the emergency call by the Priority header on the origin endpoint. Once this flag is set, new configuration options become available:

- Location header forward: this flag enables the RFC-6442 (geolocation header forward to be sent to the next hop). Default is enabled.

- Map ELIN to PAI header: this flag is used to move the ELIN string to PAI header. Default is disabled.
- Enable callback based on ELIN: a flag to allow callback calls from the original B-side to be forwarded to the original caller.
    - Callback binding timeout: it defines the maximal time for a callback after the end of the emergency call, which is identified by the ELIN association to the caller. After this time the biding/association is removed. It is configurable from 30 to 300 minutes. Default is 30 minutes.

New emergency calls with the same ELIN will overwrite the previous callback binding. This means that callbacks to that ELIN will connect to the most recent caller from an emergency call if it takes place during the callback binding period.

Other emergency parameters i.e. ELIN as part of the From/PAI header will be automatically bypassed when the flag “Enable PSAP capabilities” is set.

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→OpenScape 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 Incomming 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.

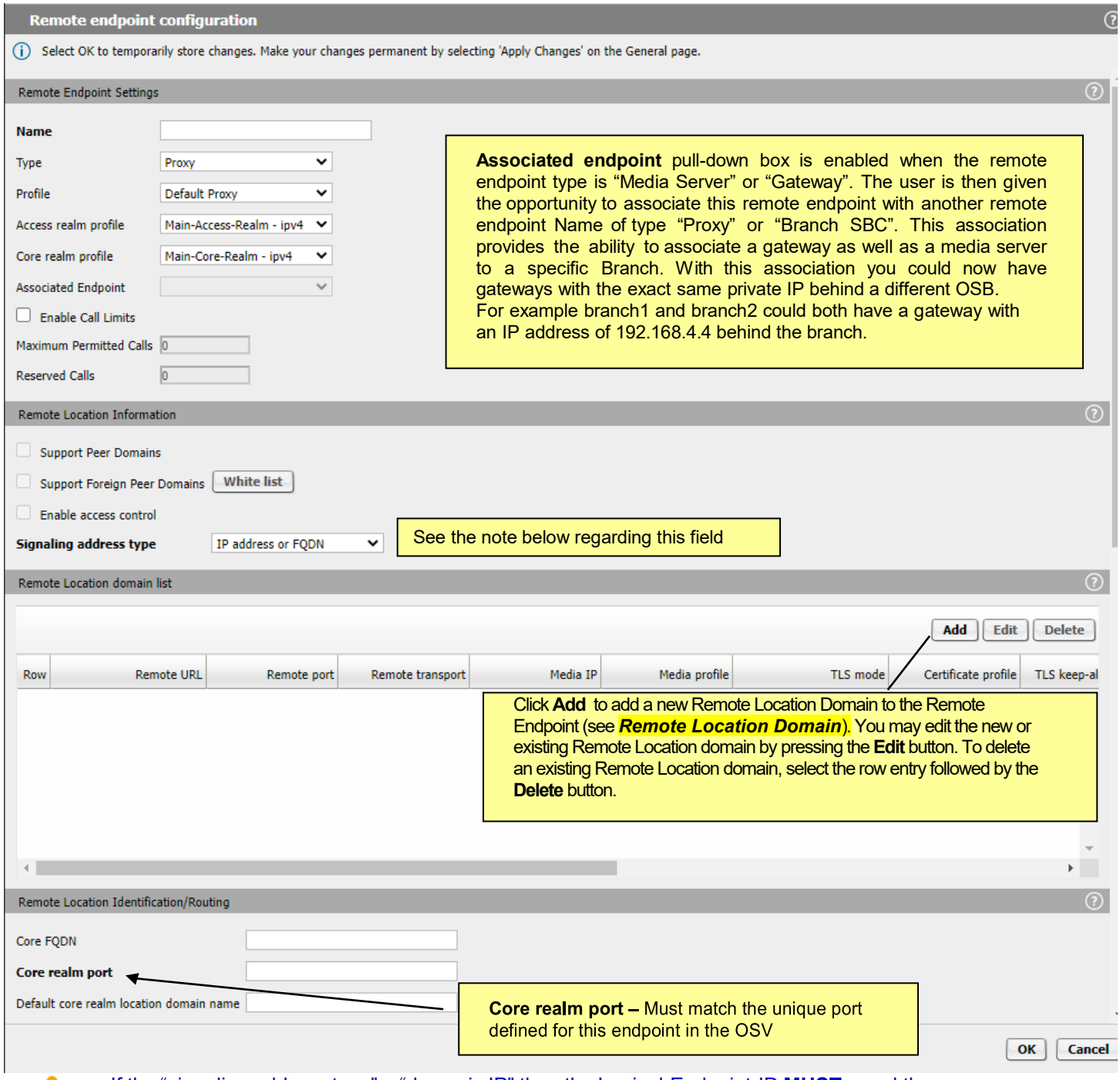
WARNING: The "Do not send re-Invite" flag precedes the "Do not send Invite without SDP" flag. When using the "Do not send Re-Invite" flag, it is recommended not to use the endpoint attribute "Enable Session Timer" in the corresponding endpoint (OSV).

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



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 → OpenScape 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`.

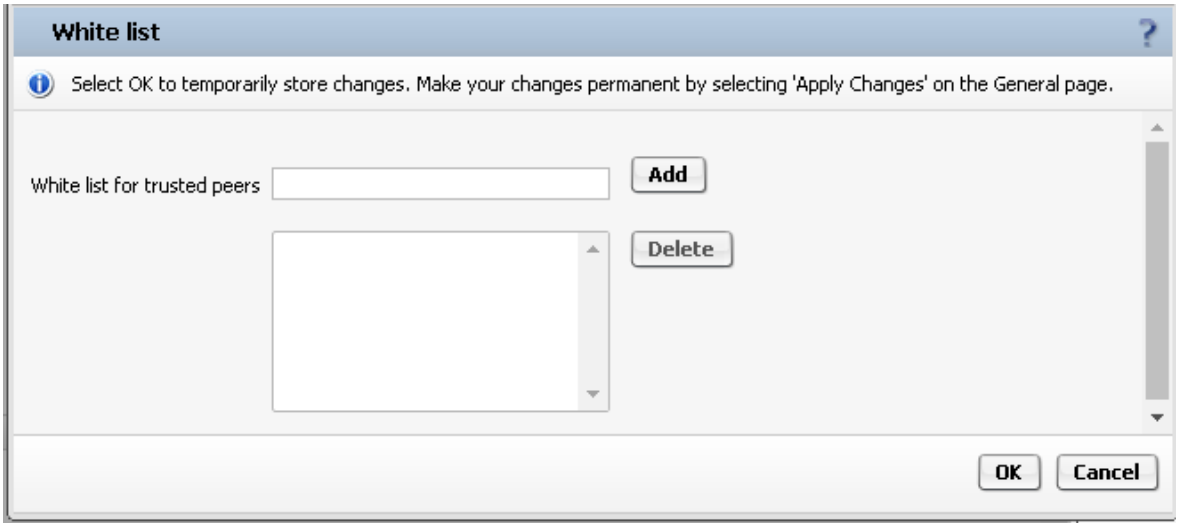
Note: Foreign Peers Domains will use the Default media profile

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.

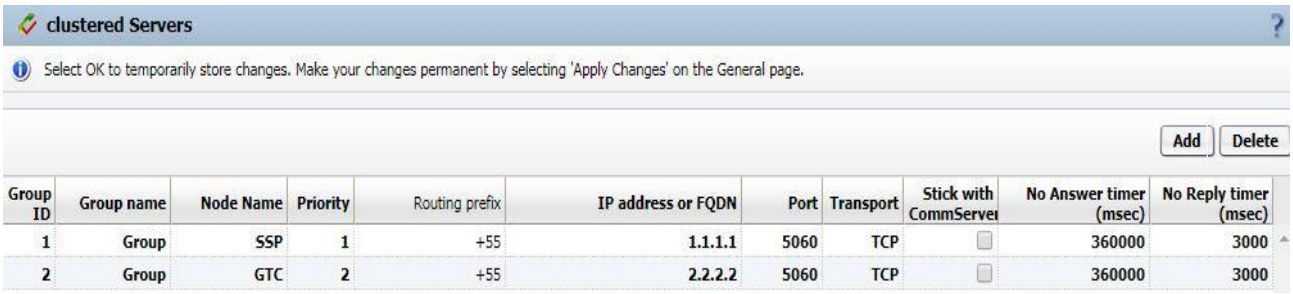
Whitelist: Enables the configuration of allowed URLs in the destination R-URI for the incoming calls, when the attribute Support Foreign Peer Domains is enabled.
The possible items added to the whitelist to match the destination are :

- 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)]

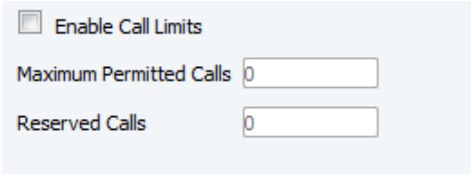


Enable Access Control: You can activate this check box only when the Support Peers Domains check box is checked. Otherwise, this field is deactivated. When you check this box is, the access control functionality is enabled by allowing multiple entries in the Remote Location Domain list. Calls are only 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.

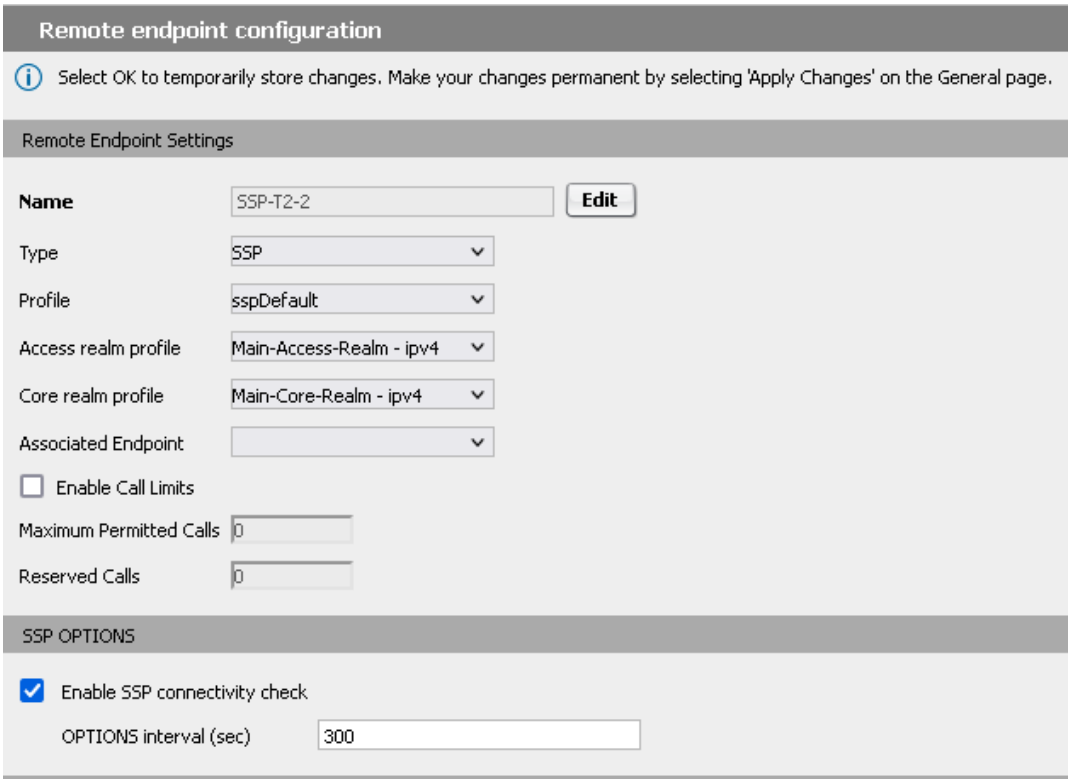


Endpoint on clustered mode works following the configuration presented on the clustered servers screen, exception for the endpoint type GTC. In the scenario that GTC range number and SSP range number are in the same routing prefix and cant be changed, the following configuration can be used, changing 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 : 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.

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



SSP OPTIONS

This session is available only for endpoints of type SSP when the Comm System type is configured with "Standalone with internal SIP Stack" or when the feature standalone is enabled.

The SSP connectivity check can be enabled for the endpoint. It is also possible to configure the OPTIONS interval (sec) for the mode "Standalone with internal SIP Stack" .

When enabled, the flag will affect the SSP connectivity status in the field SSP Connectivity check, and in the routing selection in “Standalone with internal SIP Stack” mode.

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 then 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).

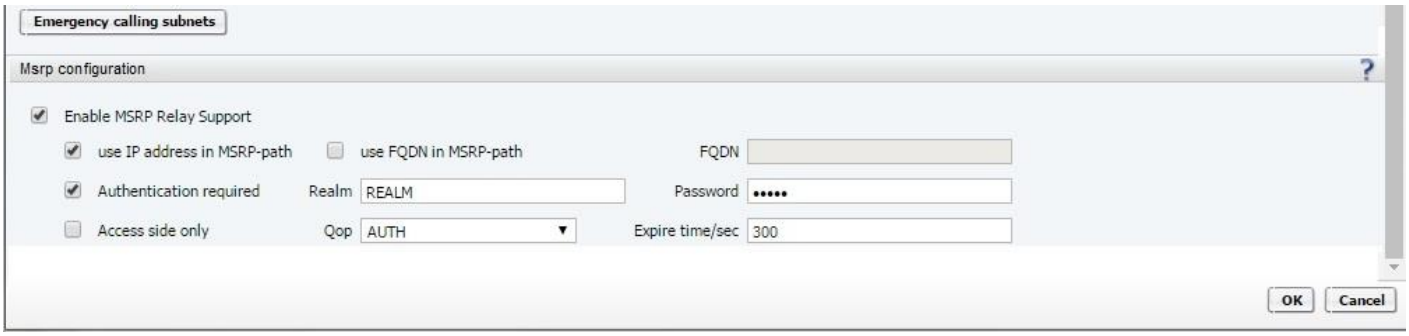
Subnet mask - This configures the IP subnet of the range of subscribers defined by the IP Address configuration. If a single subscriber is configured use mask 255.255.255.255.

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" Emergency Number.

"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.



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.

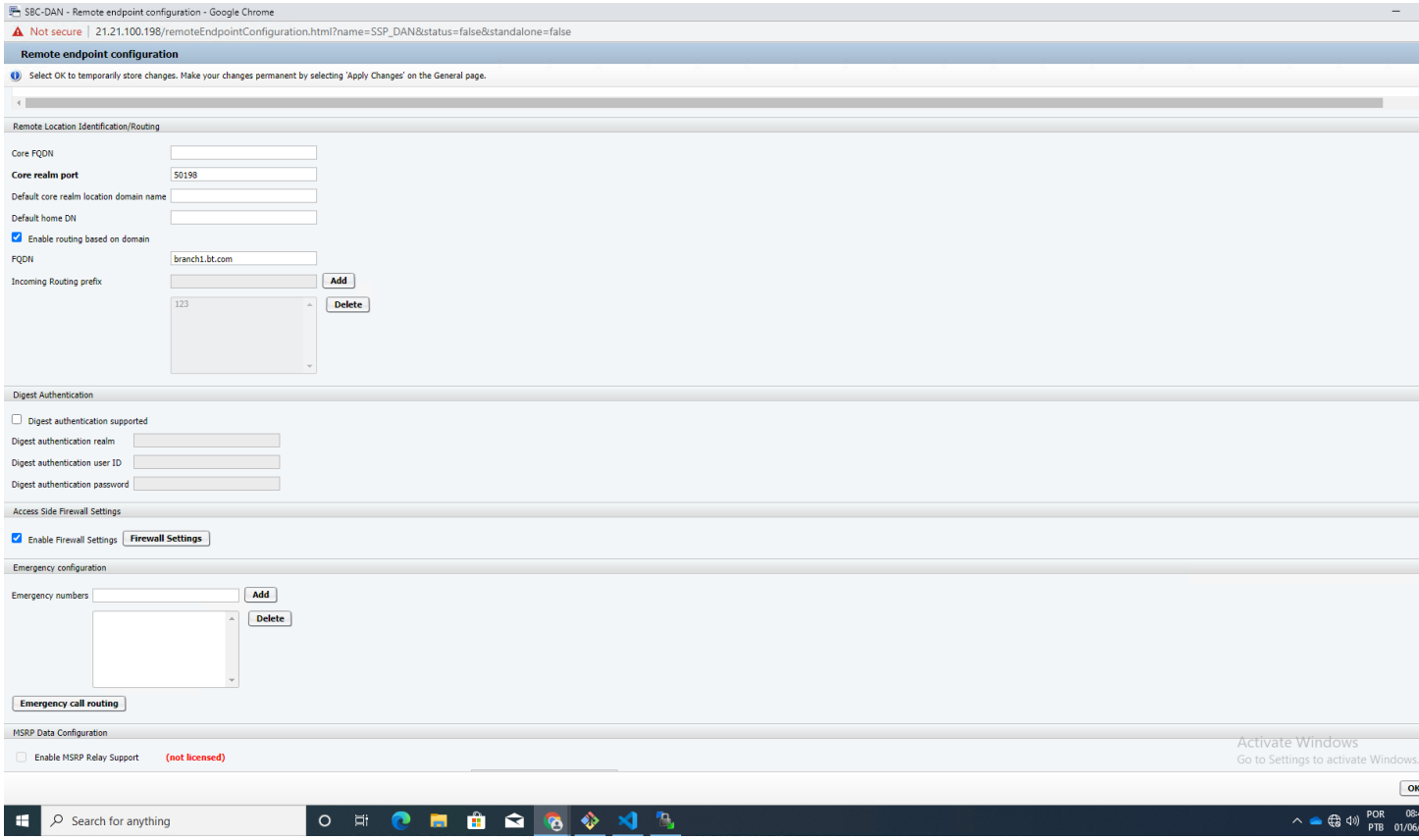
Password: Password to be used on both sides of the path through the OSS.

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

Qop: Select the Quality of protection.

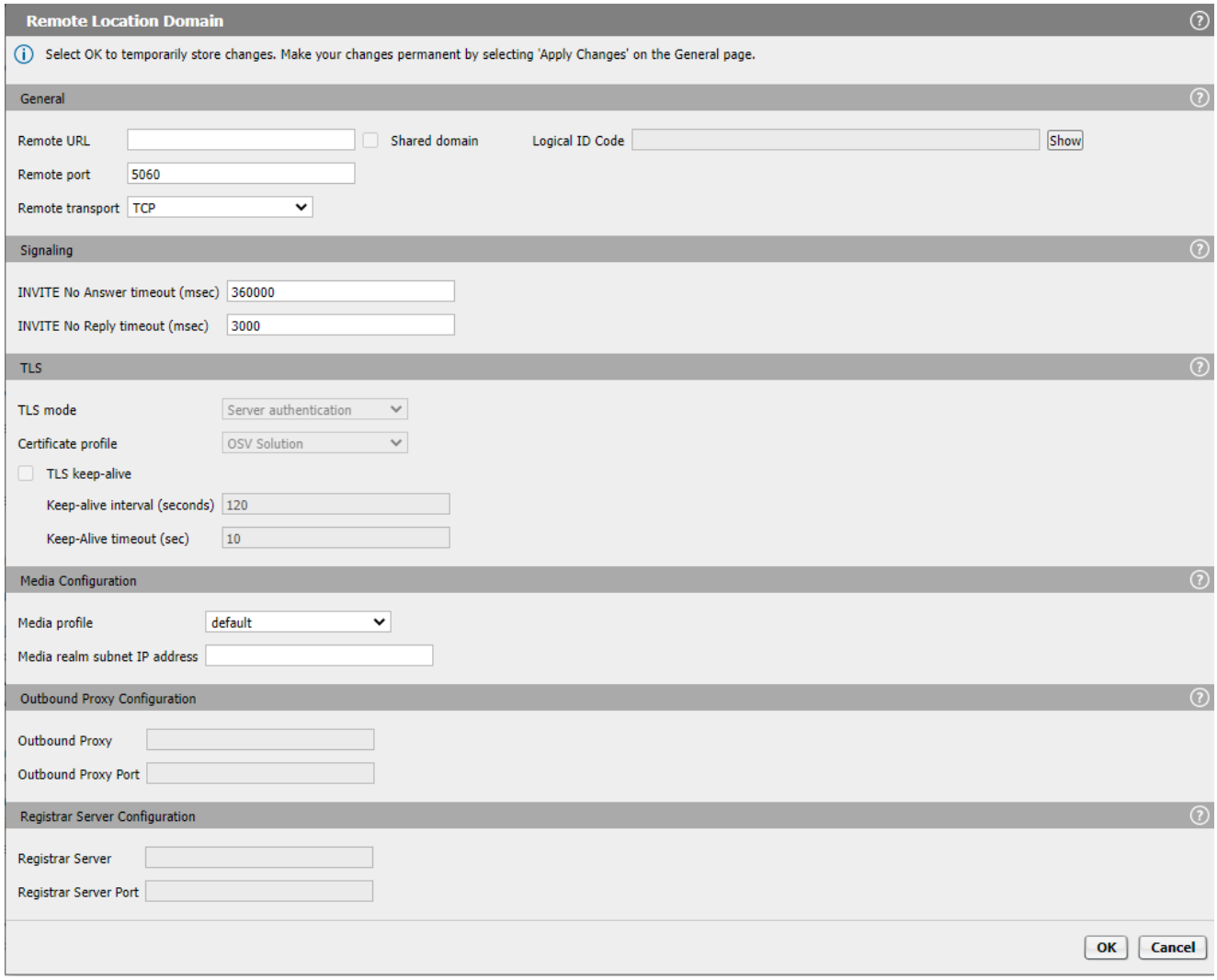
Expire time/sec: Expire default maximum and minimum values**.** Min: 60, Max: 3600

Enable routing based on domain



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 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.

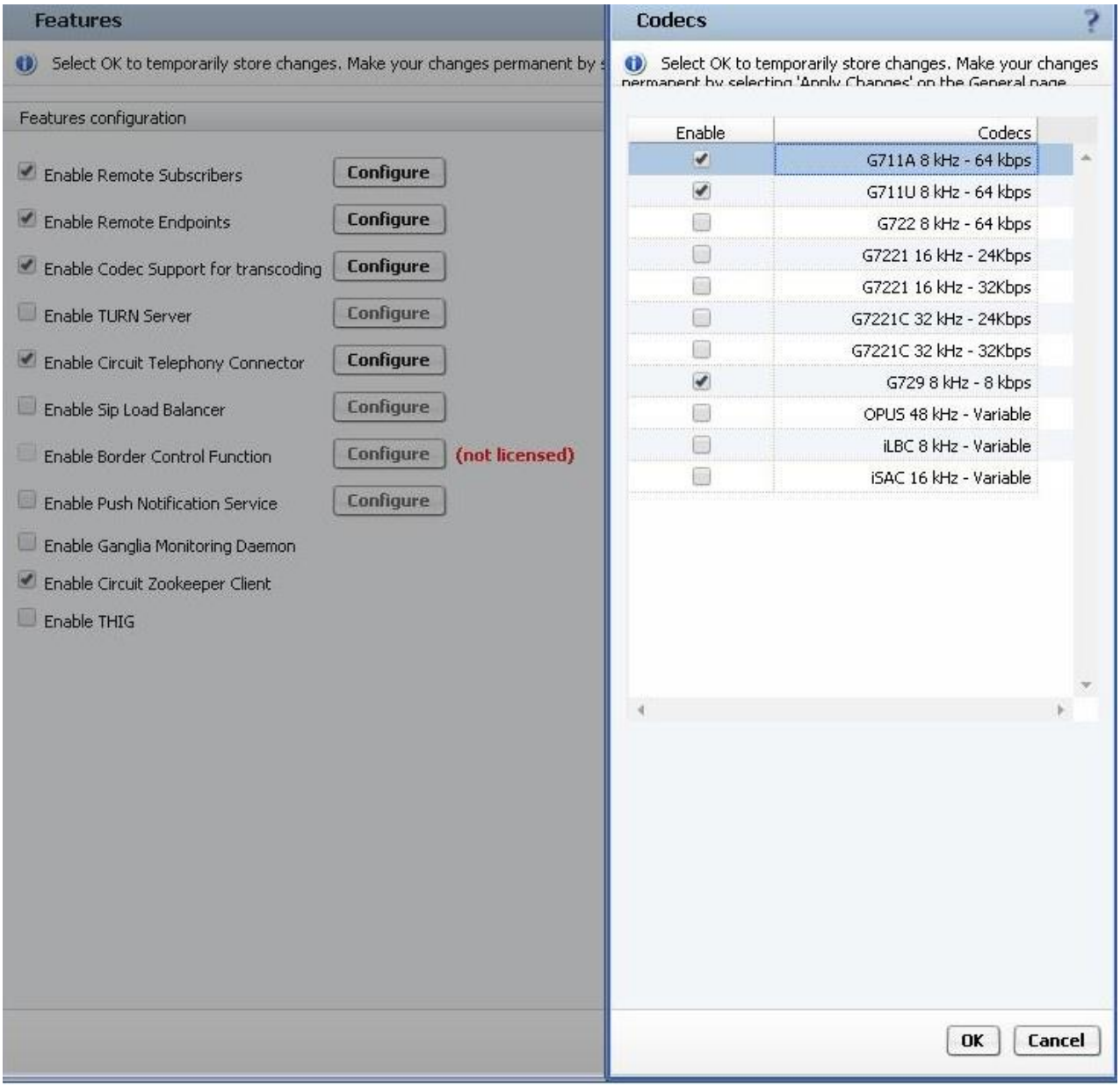
Outbound Proxy Port - Defines the port to be used in communication with the outbound proxy.

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)



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 HidingInterworking Gateway) feature in 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

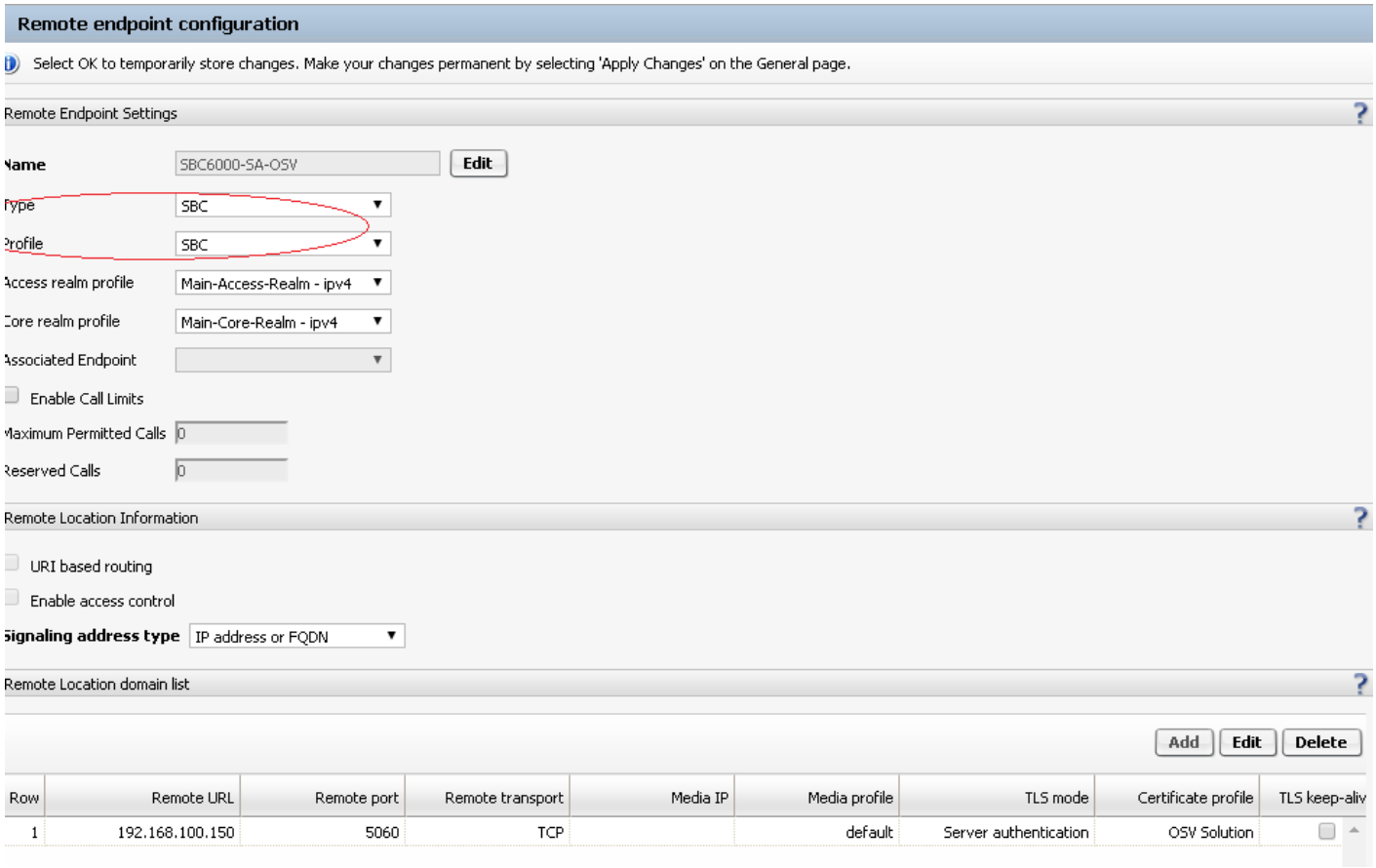
When THIG is enabled, the way that SBC handles the NAT is changed to provide the THIG functionality.So instead of changing the source IP as its own IP, THIG will bypass the IP and just change the port according to port forwarding rules.That way network elements will point to SBC WAN address as destination 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

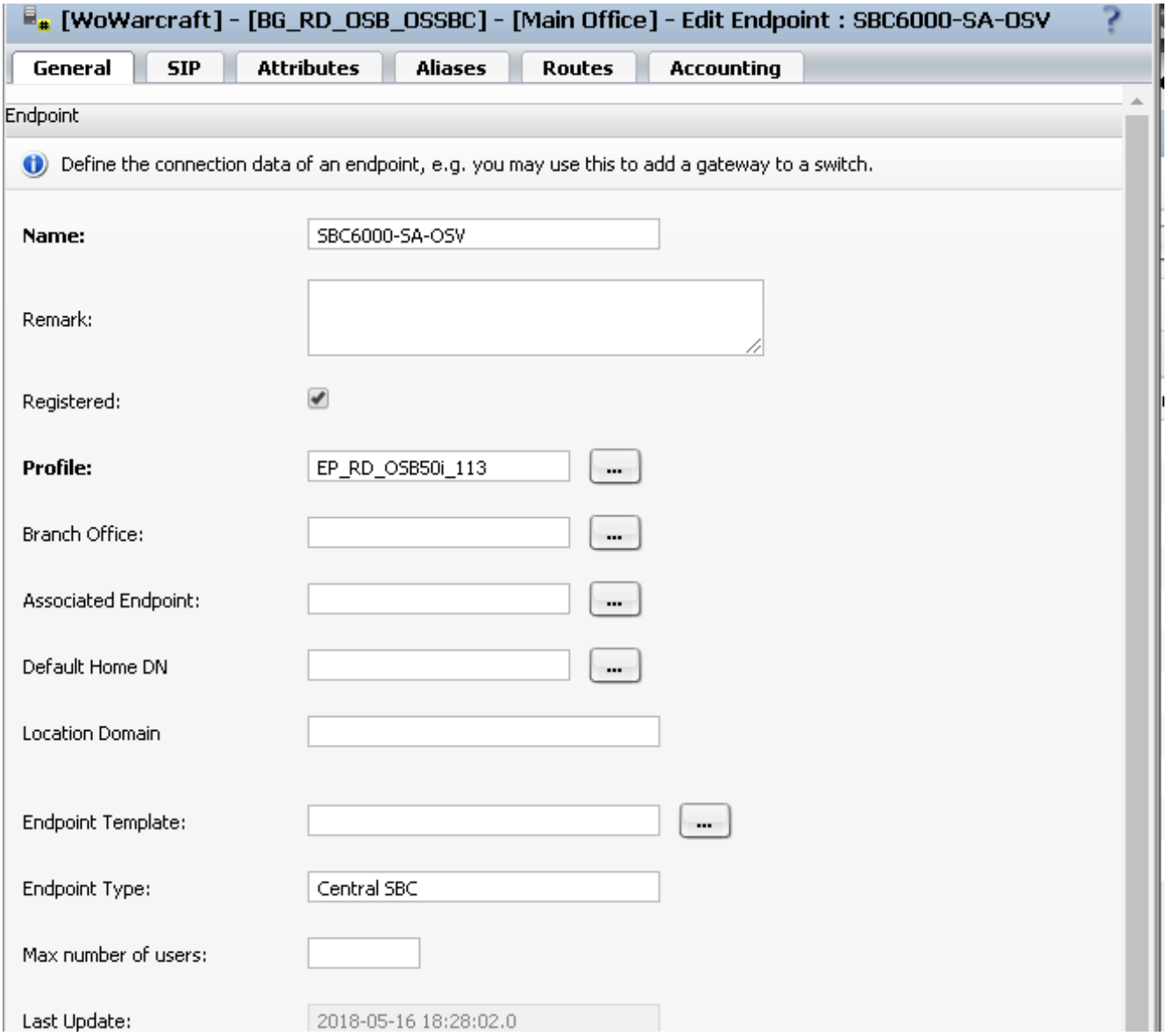
The port forwarding rules along with the rest of the THIG configuration are provided by WebCDC during the initial staging.

3.4.5.8 Enable Standalone

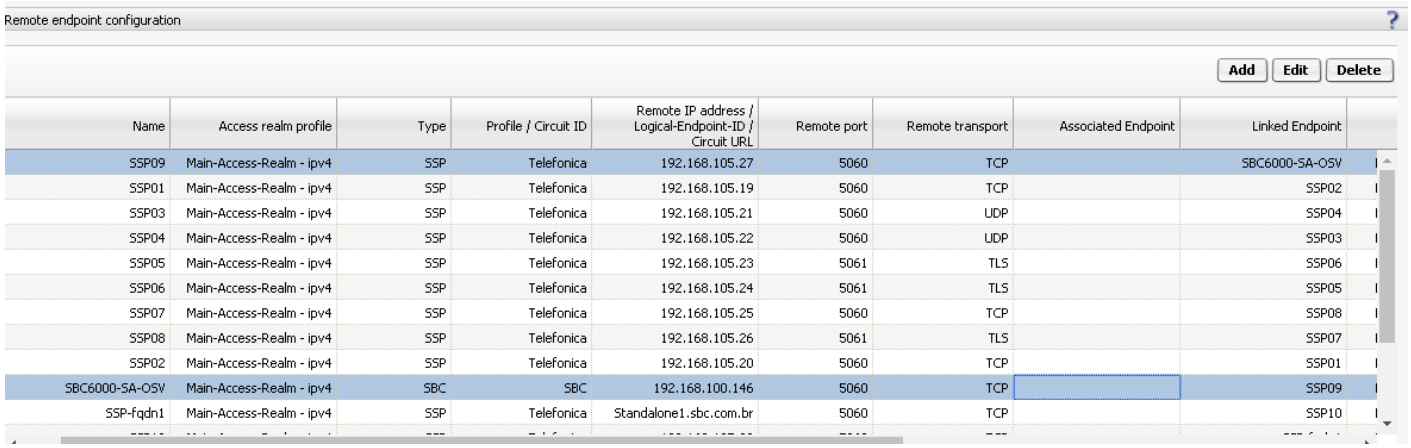
For Openscape Cloud the standalone SBC is a remote endpoint of type and profile as SBC configured at TRUNK-SBC as in the example below.



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.

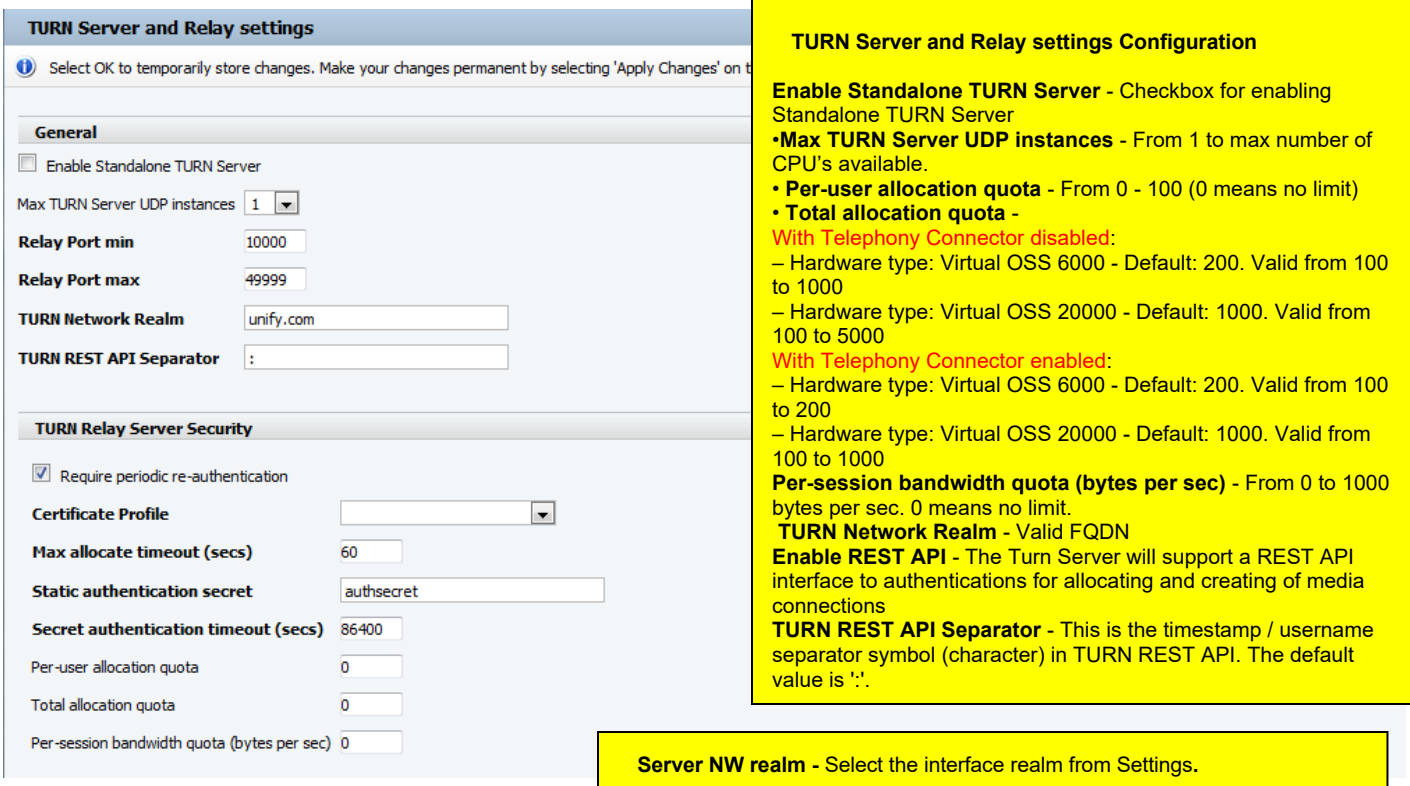


In the Stand Alone SBC itself we have at least one endpoint that should point to the TRUNK-SBC endpont as explained above, and a second endpoint that is used to connect to SSP or Gateway/Proxy, both endpoint as linked together as can be seeing in the picture below (see endpoints blue colored). In a practical 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.



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 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 ':'.

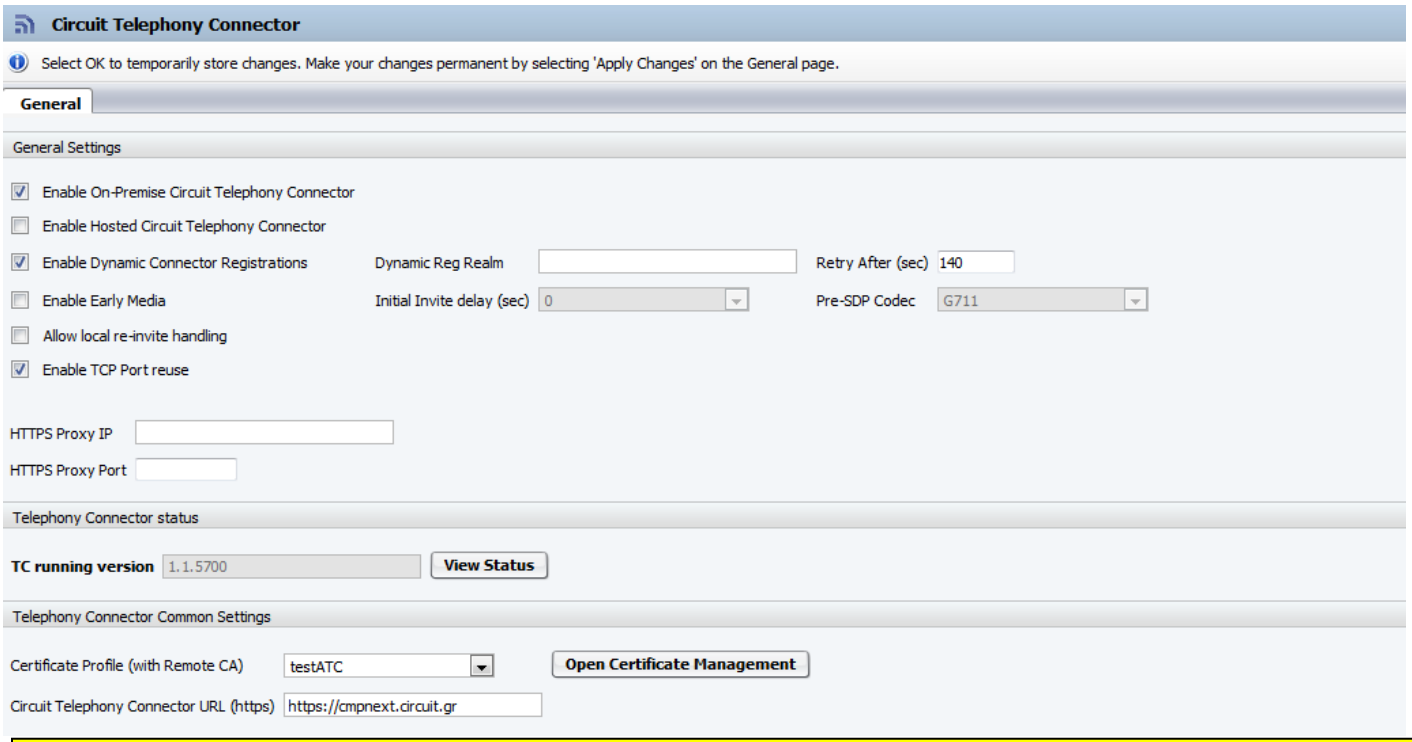
Server NW realm - Select the interface realm from Settings.

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 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

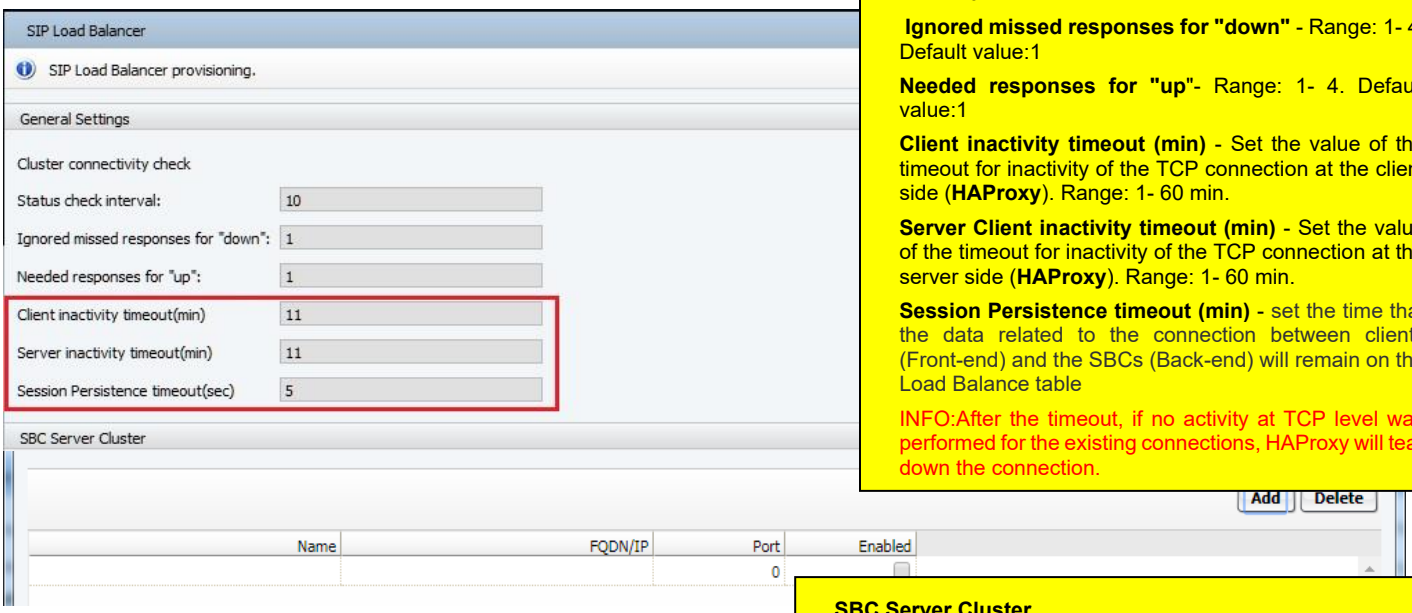
The SIP Load Balancer (SIP-LB) distributes the SIP traffic among a set of SBCs based on establishing a TCP / TLS connection (Round-Robin mechanism).TheSIP-Load Balancer is used in Circuit deployments as well as Cloud Telephony (OSV based) deployments. Once the Load Balancer is activated, the other SBC 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.

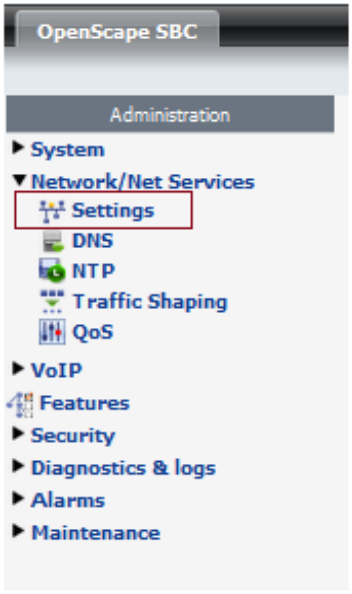
- LAN IP for management access of SBC-LB and the SBCs
- NAT IP address of the SBC-LB and the SBCs
- Public IP address of the SBC-LB and the SBCs ("External firewall IP")

- 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.

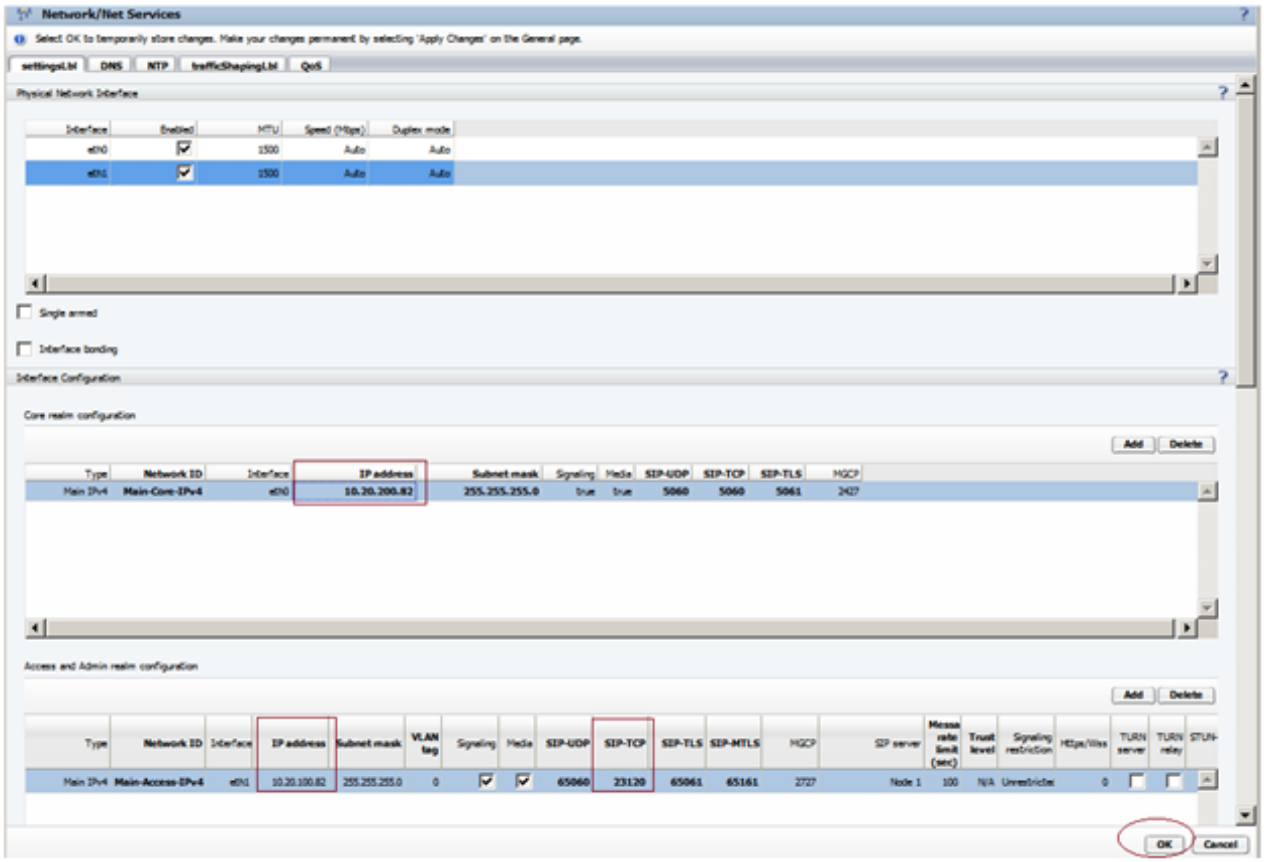
	LAN(Core)-IP	WAN(Access) NAT IP	WAN(Access) External firewall IP	WAN signaling TCP port	VOIP port range settings for RTP	External IP Signalling	External IP Media
SBC-LB	10.20.200.82	10.20.100.82	80.157.193.193	23120	11000-49999	80.157.193.193	N/A
SBC-1	10.20.200.86	10.20.100.86	80.157.193.125	23120	11000-49999	80.157.193.193	80.157.193.125
SBC-2	10.20.200.87	10.20.100.87	80.157.193.196	23120	11000-49999	80.157.193.193	80.157.193.125

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.

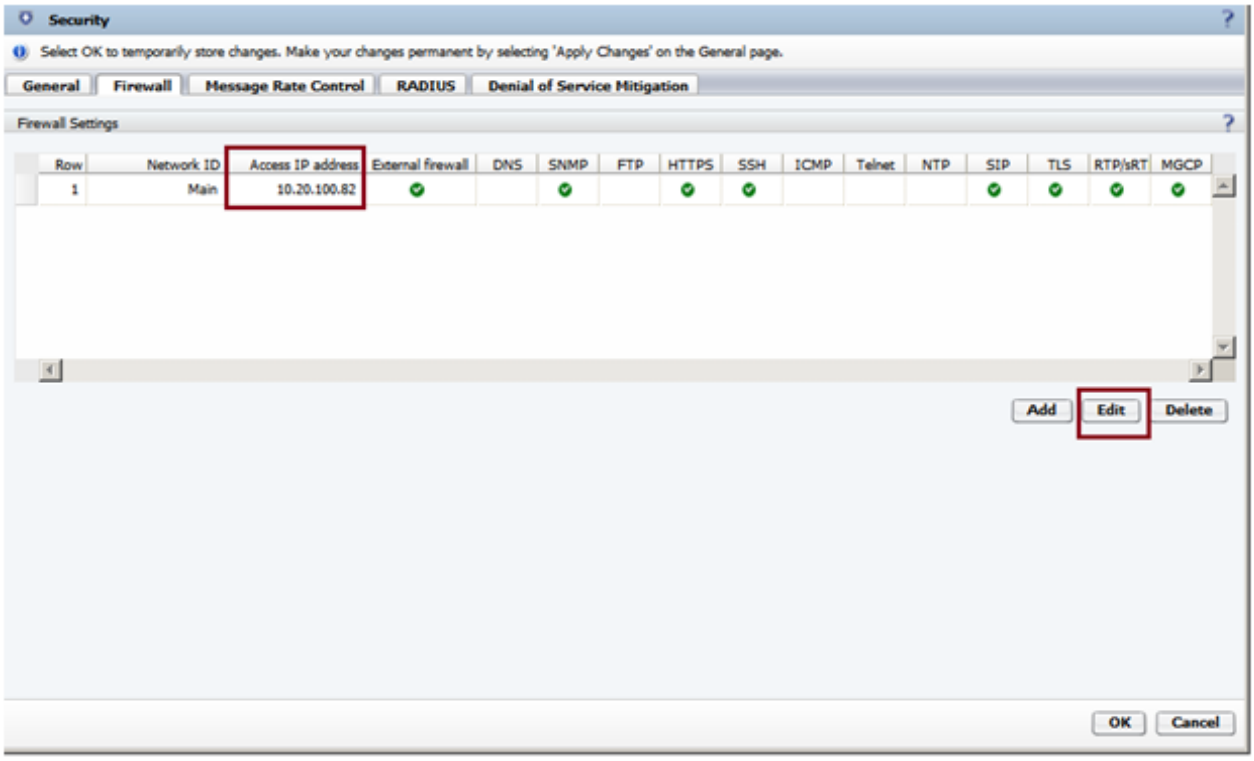


5. The above step will take you to the Network Services Window. Here, configure the Core and Access realm configuration as shown below. Click "OK". In the main window click "Apply Changes"

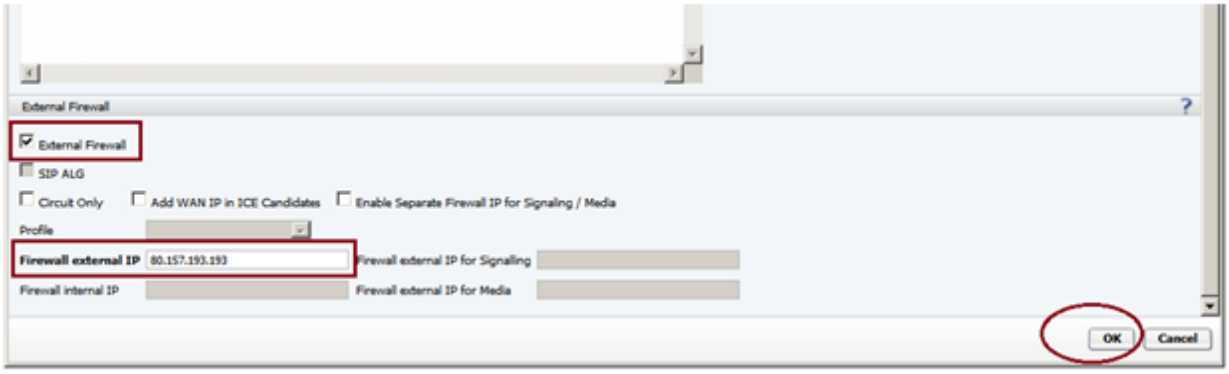


6. When the Management interface has successfully applied the network settings. Click on the Security->Firewall configuration.

7. This will open the “Firewall” tab of the security settings. Select the first and *only* item in the list and click “Edit”.



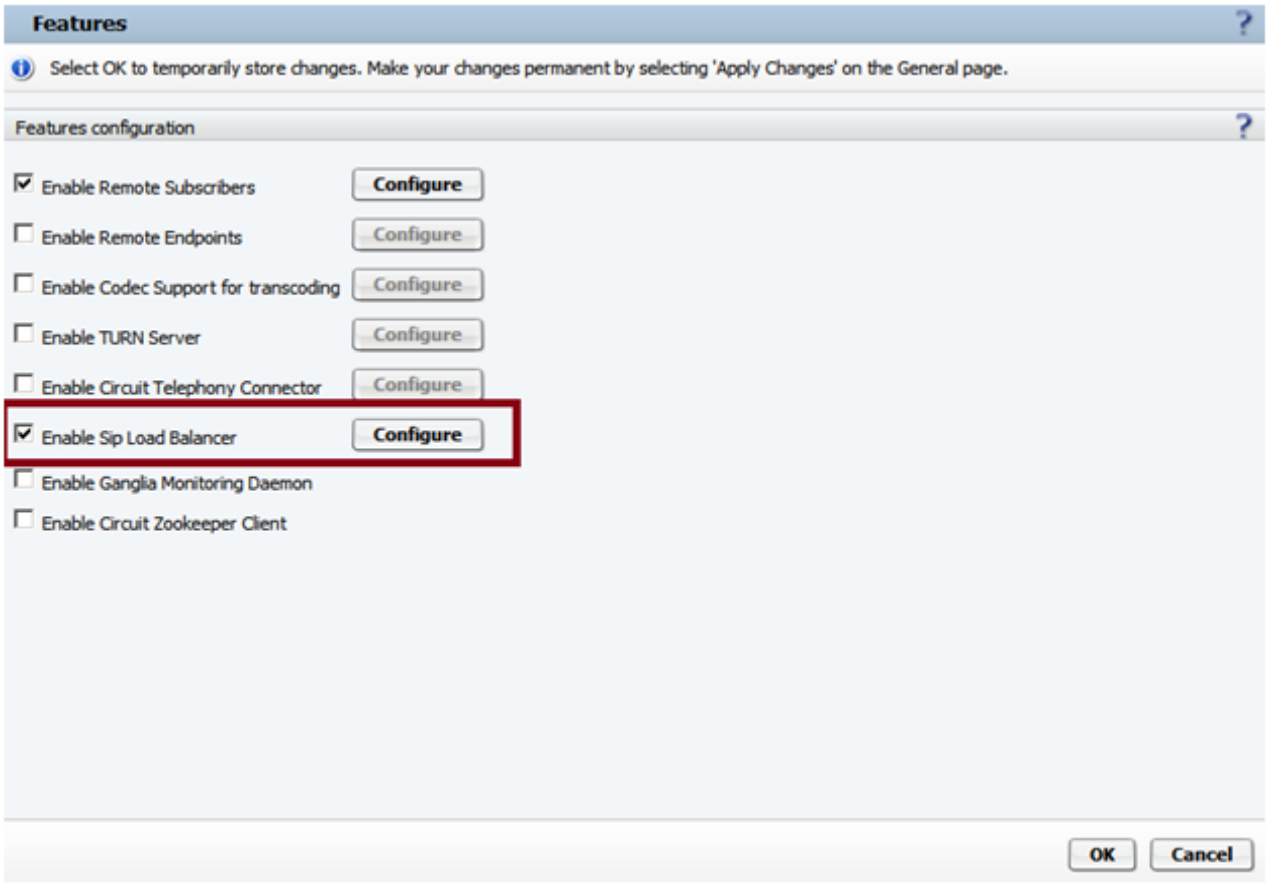
8. Scroll down to the section “External Firewall” . Check the box “External Firewall” . Add your public IP to “Firewall external IP” and click OK



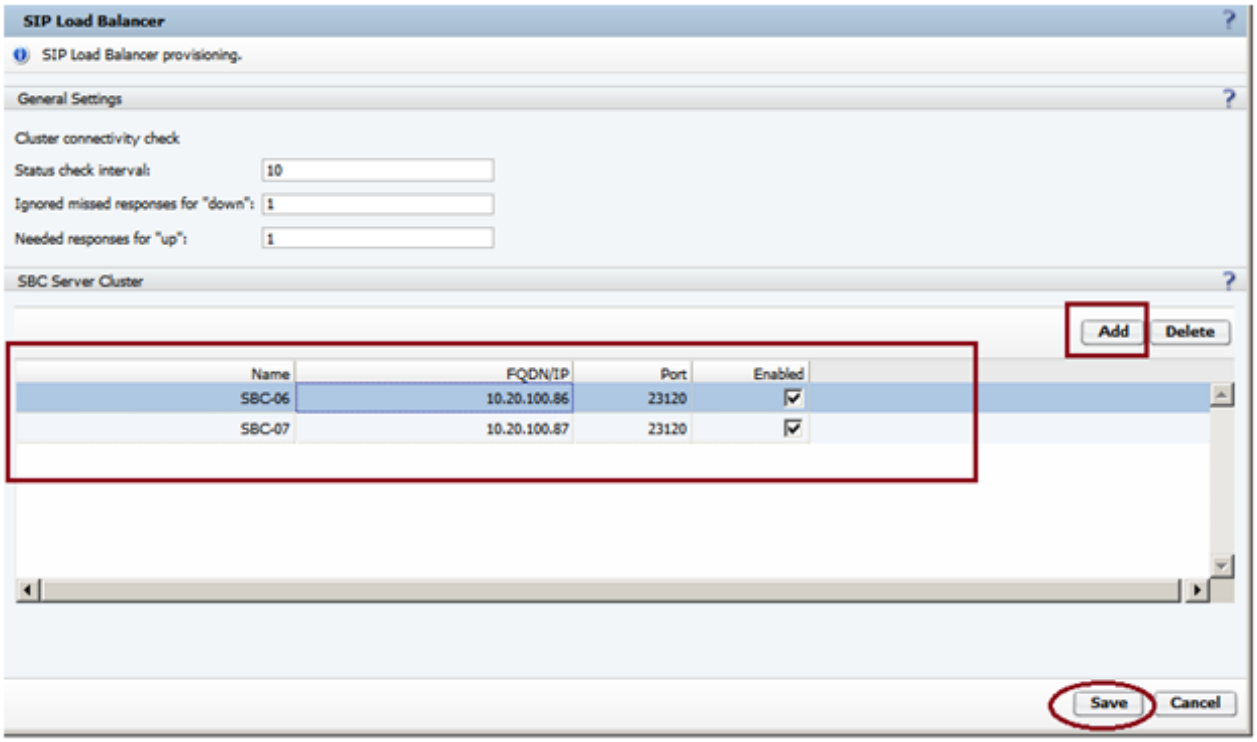
9. This will take you back to the Security window. Click OK. In the main window click “Apply Changes”

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…”



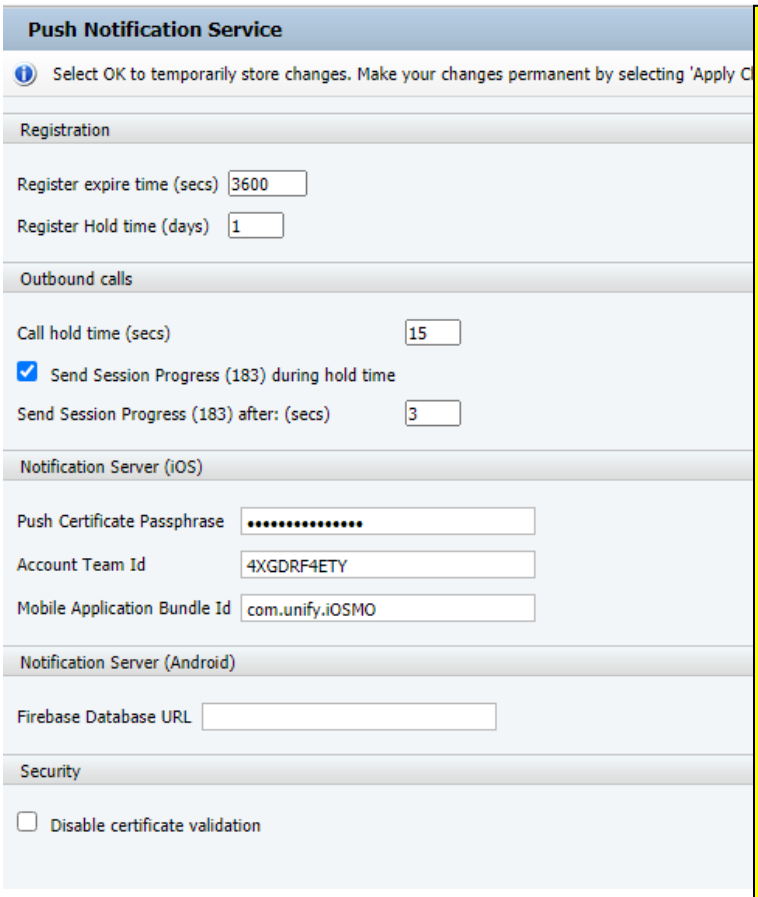
12. Within the load-balancer configuration window, add the IP address of the SBCs and make sure the WAN ports are entered correctly. Click “Save



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 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 clientDefault 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

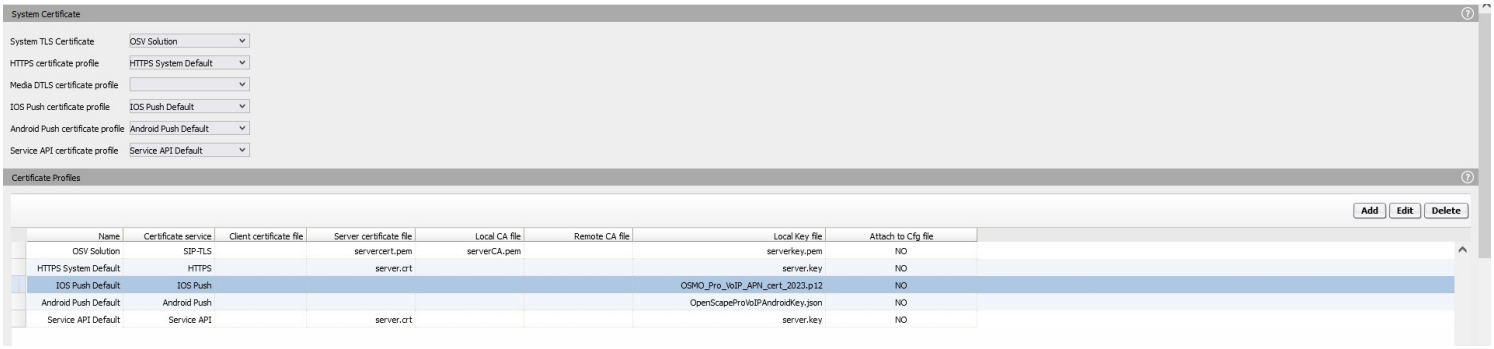
Note: For OSMO the default client credentials are configured in IOS Push certificate profile and Android Push certificate profile.

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”.

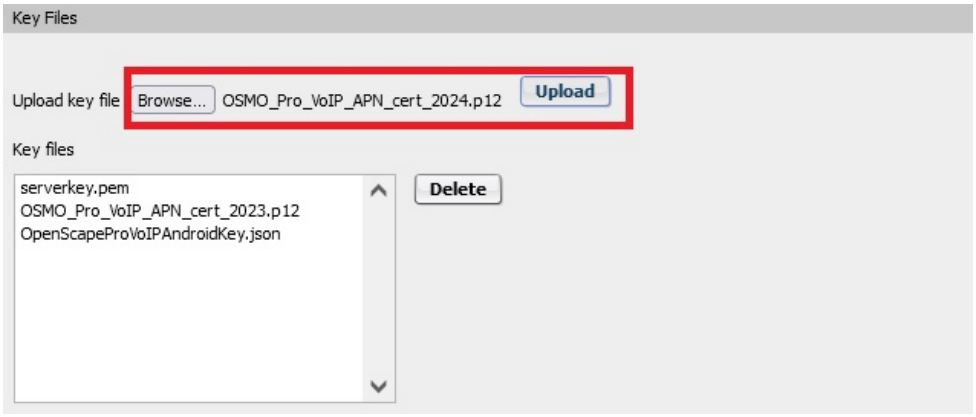
For example: If the current certificate used on the profile "IOS Push Default" is OSMO_Pro_VoIP_APN_cert_2023.p12, after upgrading to V10R3.2.0, it will be automatically replaced by the OSMO_Pro_VoIP_APN_cert_2024.p12 certificate.

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**.

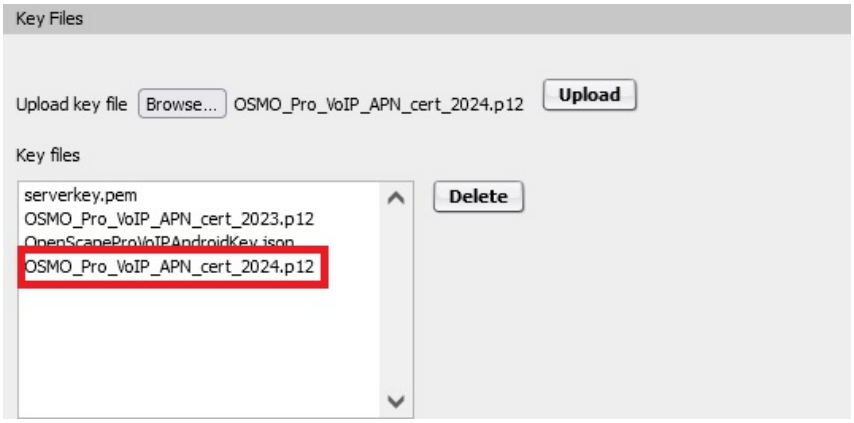
If you need to upload a new certificate, navigate to the **Security->General->Certificate Management** page. There you will find the default profile and certificate of the feature. For example the new IOS Push certificate:



Scroll down to the **Key Files** section.
Click **Browse** to select the new file.
Click **Upload** to upload the new **Local Key** file.

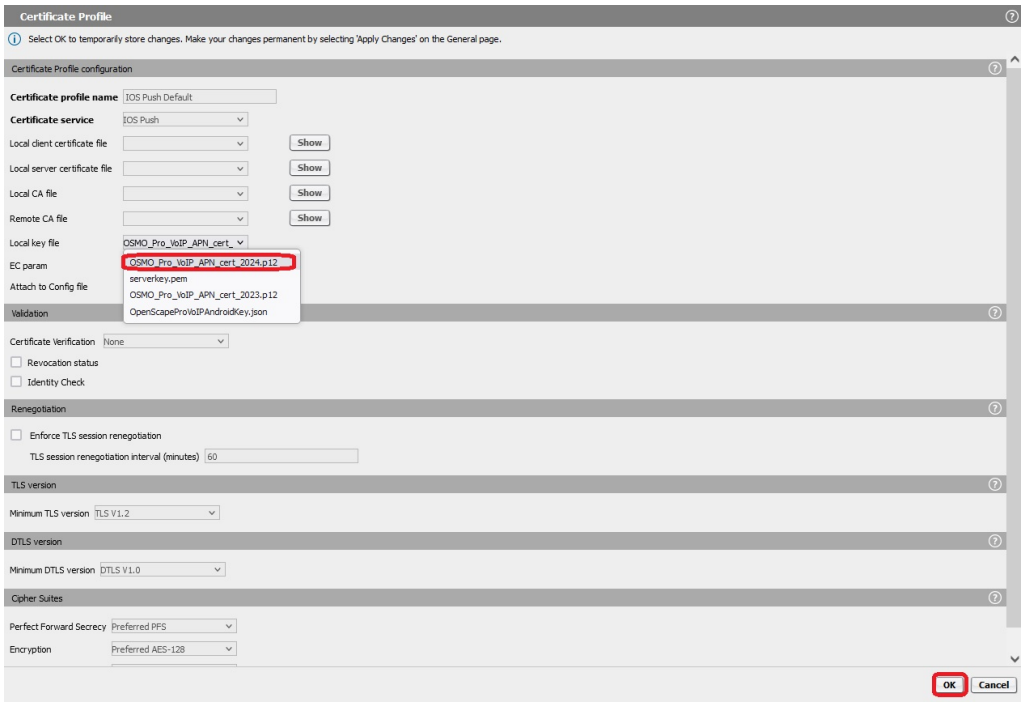


If the upload is completed successfully, the new certificate will be listed in the **Key files** section.



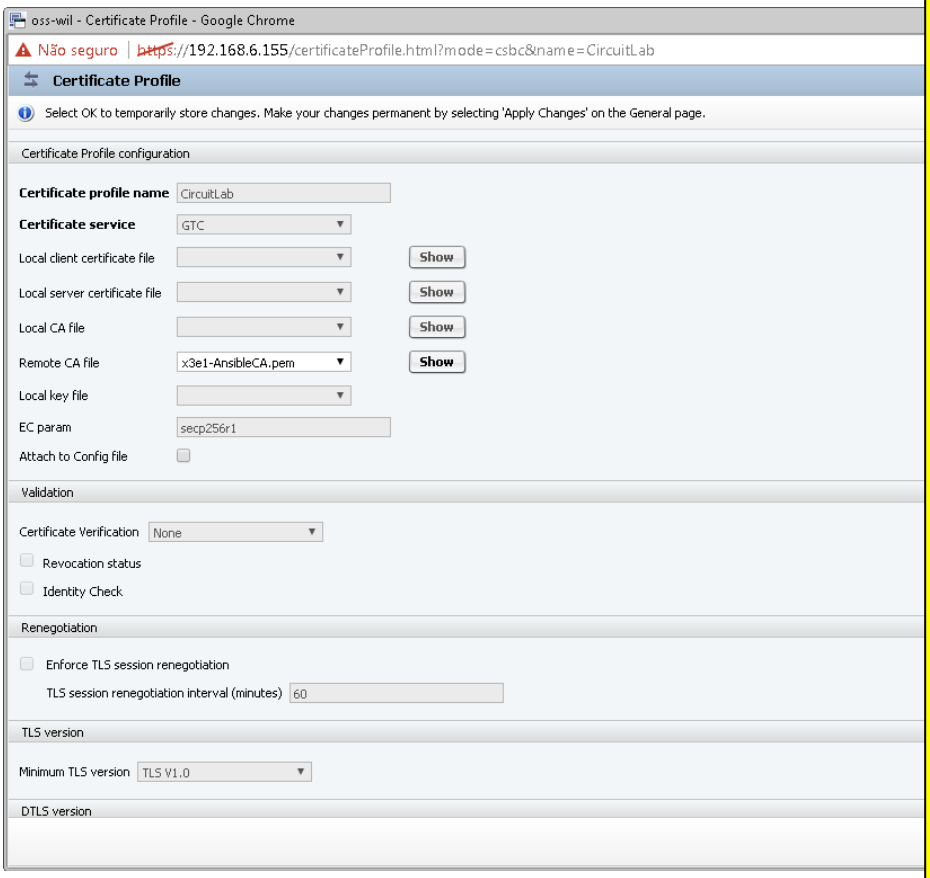
In the **Certificate Profiles** section, select the profile you want to edit, and then click **Edit**.

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 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.

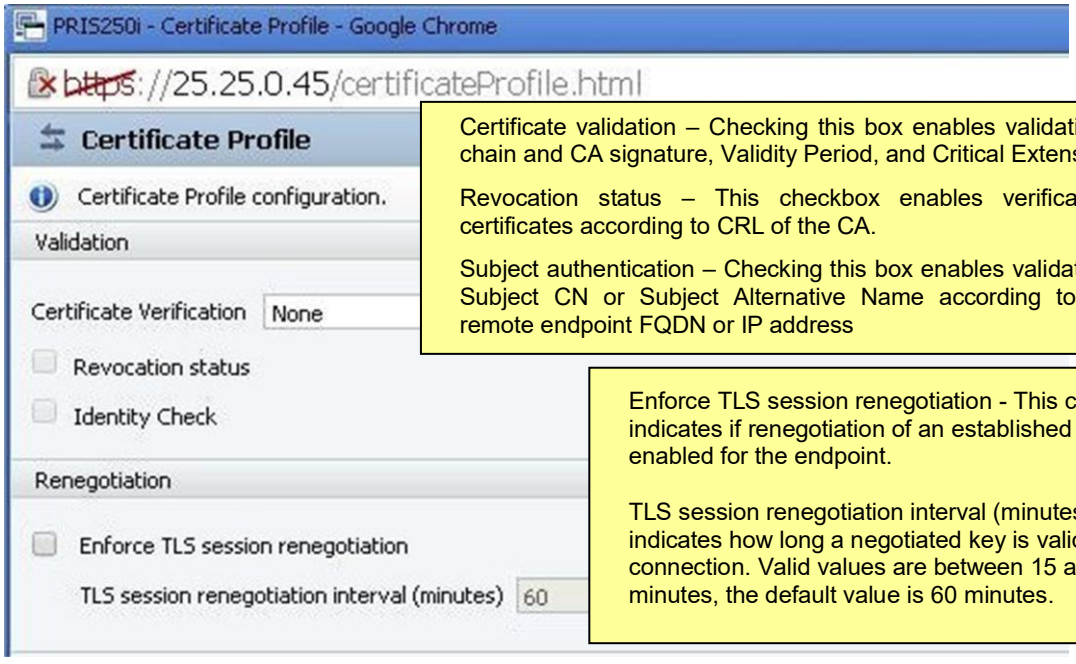
Local CA file – This is the CA file with the root CA certificate which signed the local certificates.

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.



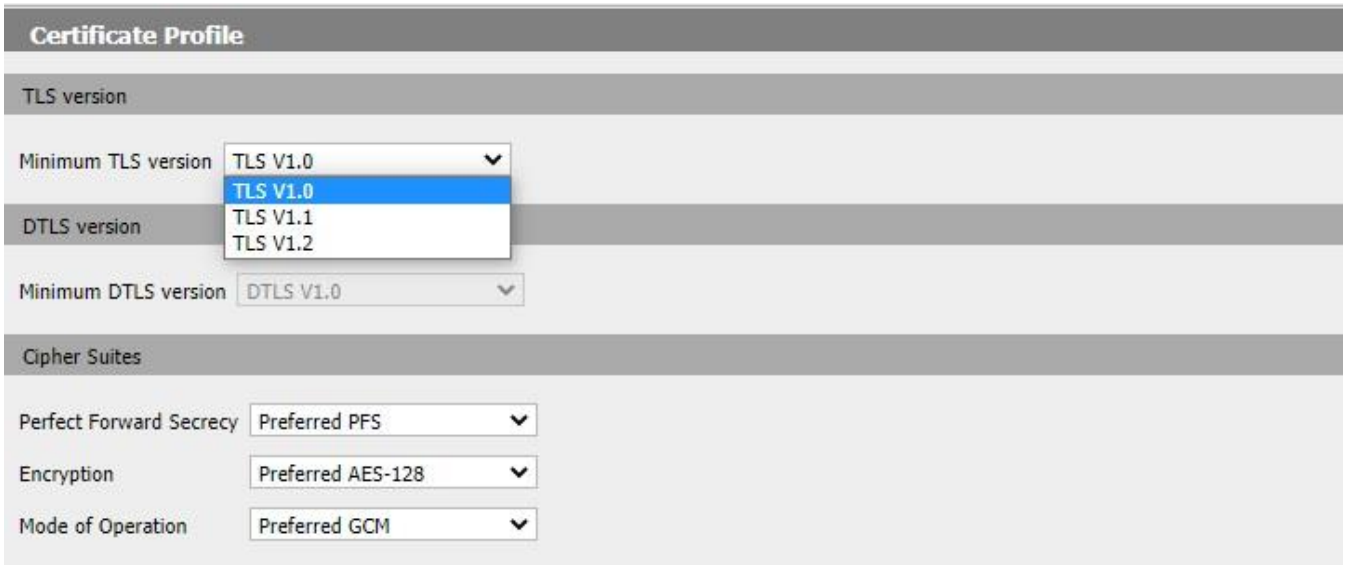
Certificate validation – Checking this box enables validation of the CA chain and CA signature, Validity Period, and Critical Extensions.

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.



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.

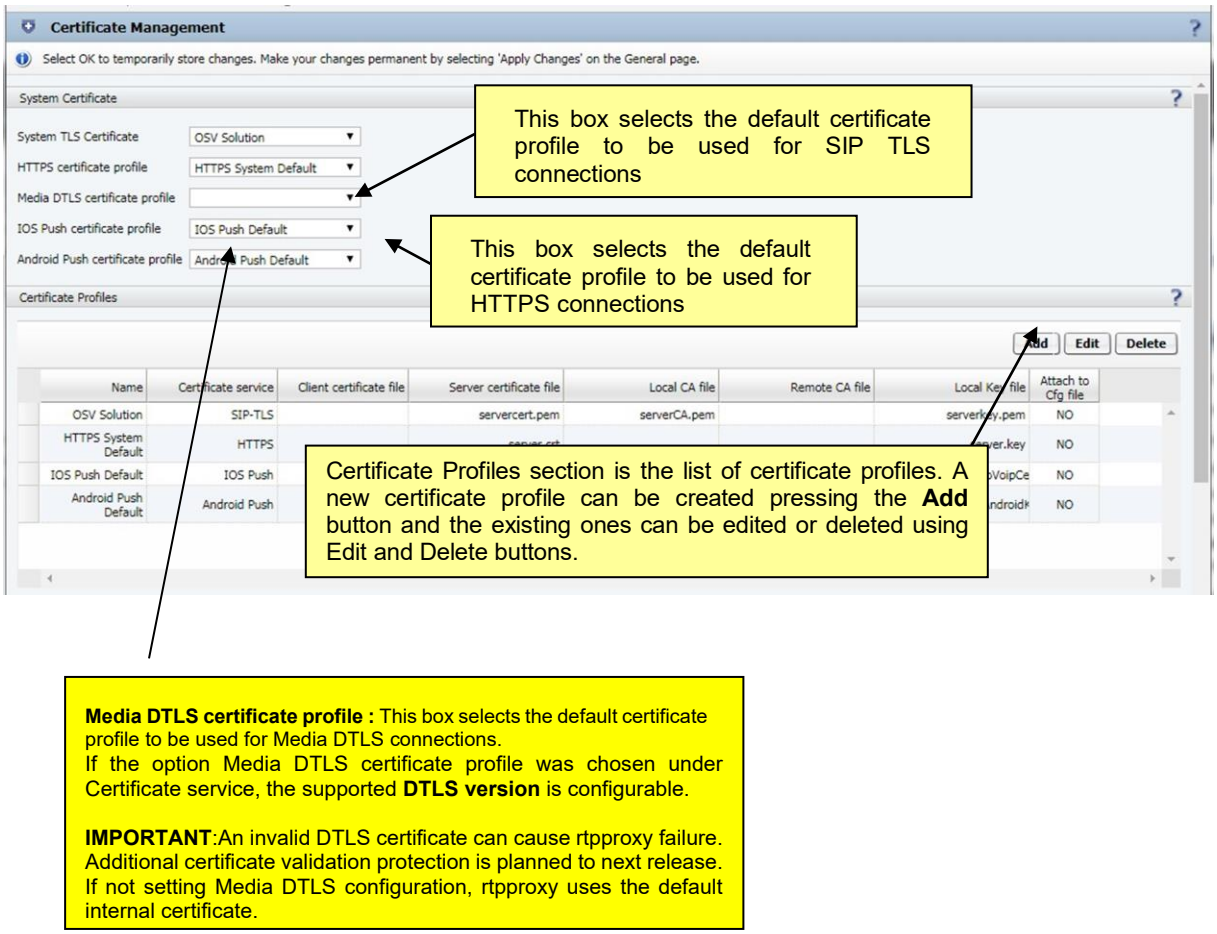
Minimum TLS Version Configured in SBC/OSB	TLS Version in Remote Endpoint as Client	SBC as TLS Server	SBC as TLS Client. TLS Version offered to TLS server
TLSv1.0	TLSv1.2	Accept	**TLSv1.2**
	TLSv1.1	Accept	
	TLSv1.0	Accept	
	SSLv23/SSLv3	Reject	
TLSv1.1	TLSv1.2	Accept	**TLSv1.2**
	TLSv1.1	Accept	
	TLSv1.0	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 pem format.

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.

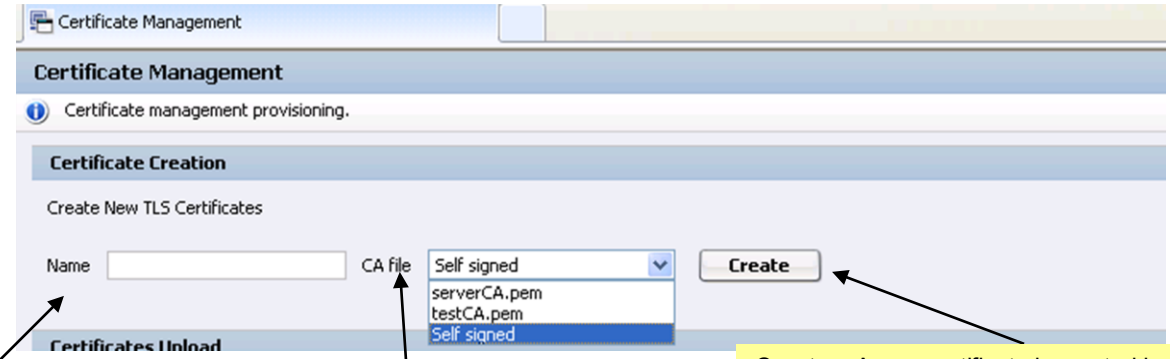
The saving of the xml will save the certificate profiles but not the files they refer to, so the user should save/restore these files using the following procedure.

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.

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.

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.

Certificates generated using GUI will be created with default parameters of Openscape SBC.

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.

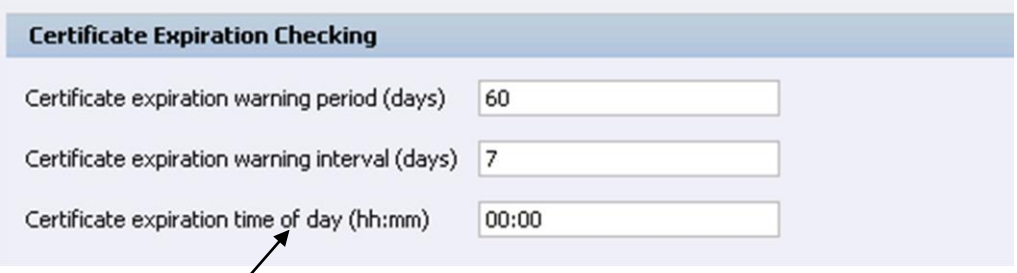
If extra parameters for certificate creation are required, please refer to Create/Upload TLS Certificates for OpenScapeSBC (Using openssl).

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 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.



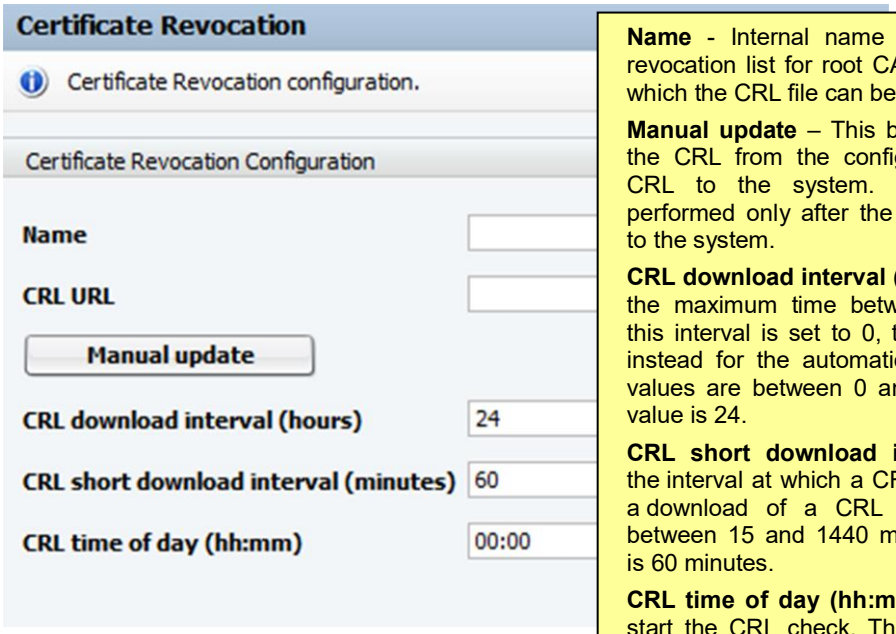
Certificate expiration warning period (days) - The number of days before a certificate expires at which an alarm is generated to warn the administrator about the impending expiration of the certificate. The valid values are between 0 and 300 days, and the default value is 60 days.

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:
OpenScape 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



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.

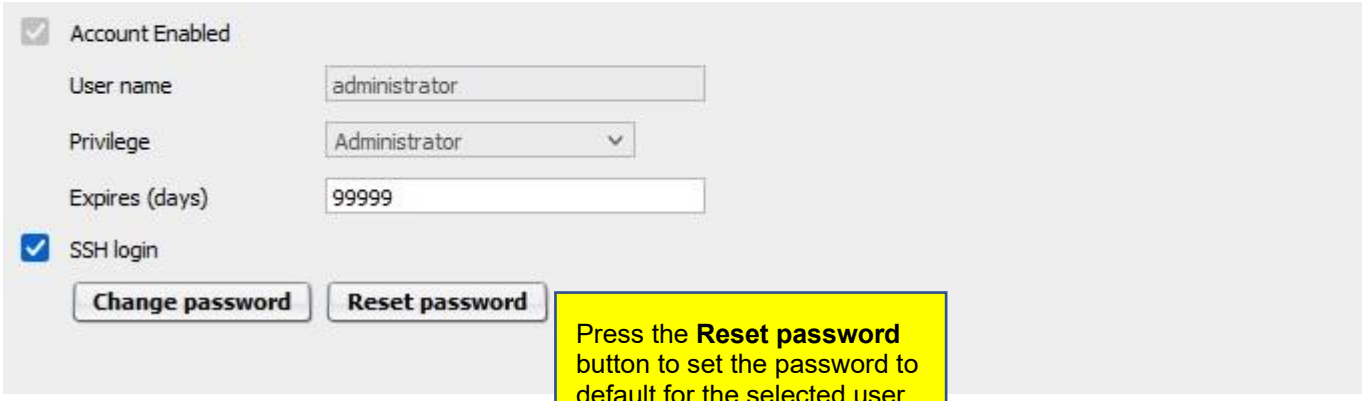
CRL download interval (hours) – This interval defines the maximum time between two CRL downloads. If this interval is set to 0, the Next Update field is used instead for the automatic CRL downloads. The valid values are between 0 and168 hours, and the default value is 24.

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



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: 1clENtk=
User : redundancy, Password Asd!.123

For security purposes it is recommended to change **ALL** passwords from their defaults as delivered with a new system.

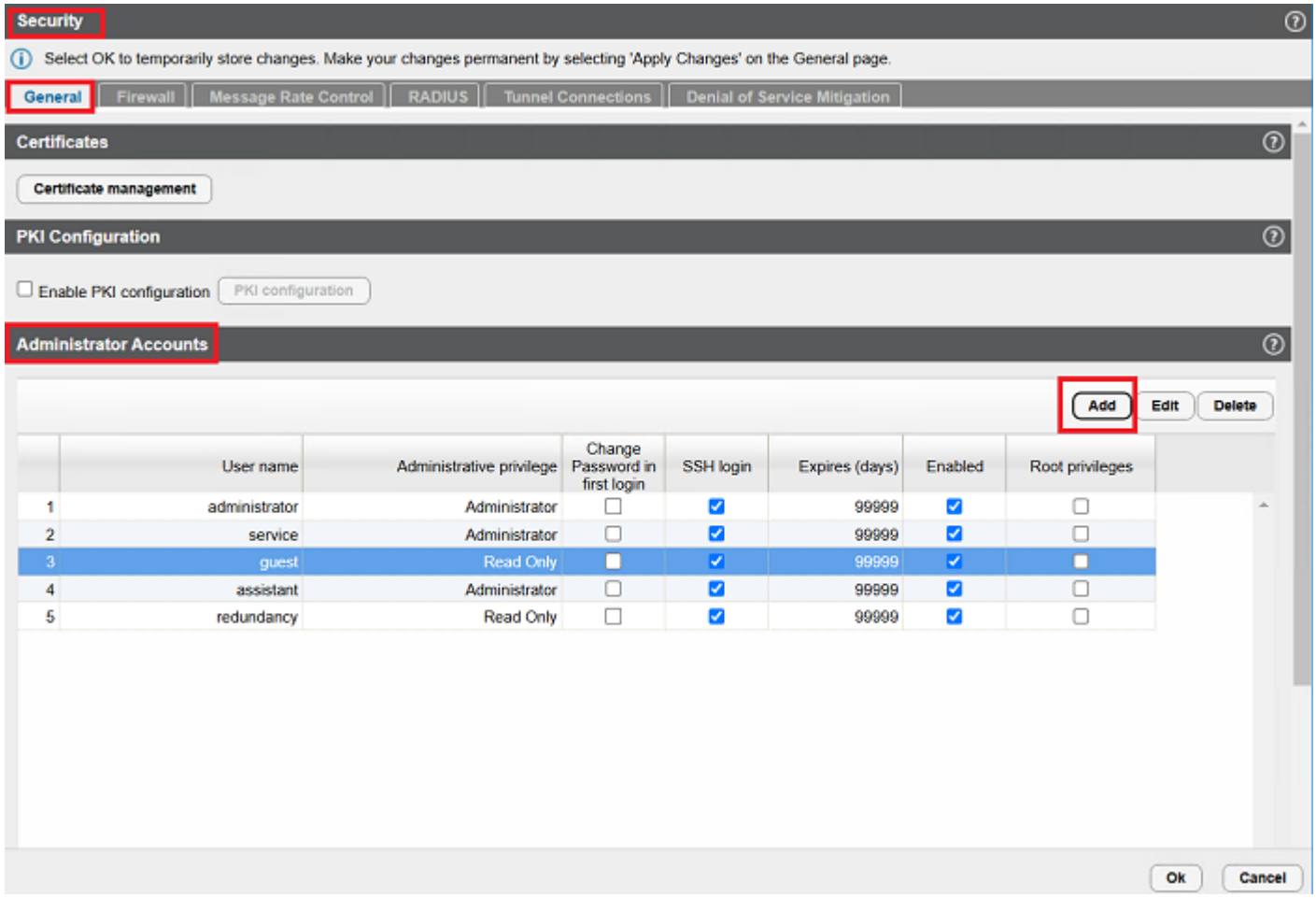
Warning: In case you change the redundancy password on the master node and have a collocated redundant OSS system, the information gets updated after data synchronization. No change is necessary in the backup node.

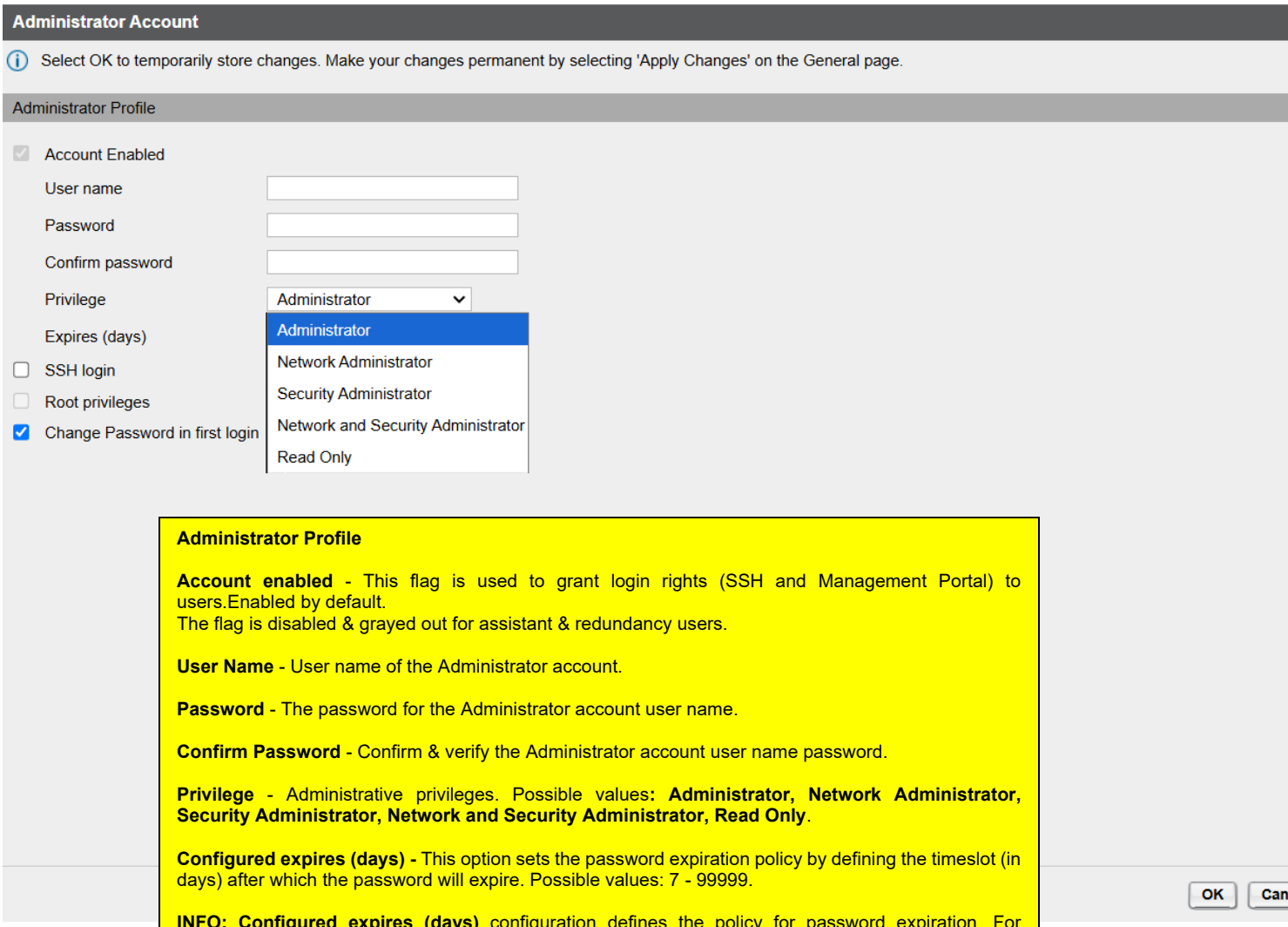
3.4.6.3 Administration Accounts

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

Important: Starting from V11R2, **Administrator Accounts** are presented as **User Accounts**. The only settings that can be modified for default users (e.g., administrator, guest, assistant, service, redundancy) are **Password** and **Configured expires**. All other settings are restricted.

Administrator 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.





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**.

Configured expires (days) - This option sets the password expiration policy by defining the timeslot (in days) after which the password will expire. Possible values: 7 - 99999.

INFO: Configured expires (days) configuration defines the policy for password expiration. For example, if set to 30 days, the password will expire after a 30-day timeslot from the last password change.
This option does not reset or alter the days that have already passed since the last password change; it only sets the expiration timeslot moving forward.
It is intended to define the password expiration policy and should not be used to extend a user's expiration time. If the password has already expired, the administrator can only modify this option after the user has changed their password.

SSH login - Login to the Linux open source application that allows data to be exchanged using a secure channel between two networked devices. Disabled by default.

Root privileges: Starting from V11R2**,** root access via GUI is blocked by default. To enable it, you must create the file "rootAccess" using the following command:
`./sbin/usercontrol --enable`

To perform all user-related functions, typically available to the root user, run the following script:
`/sbin/usercontrol --exec`

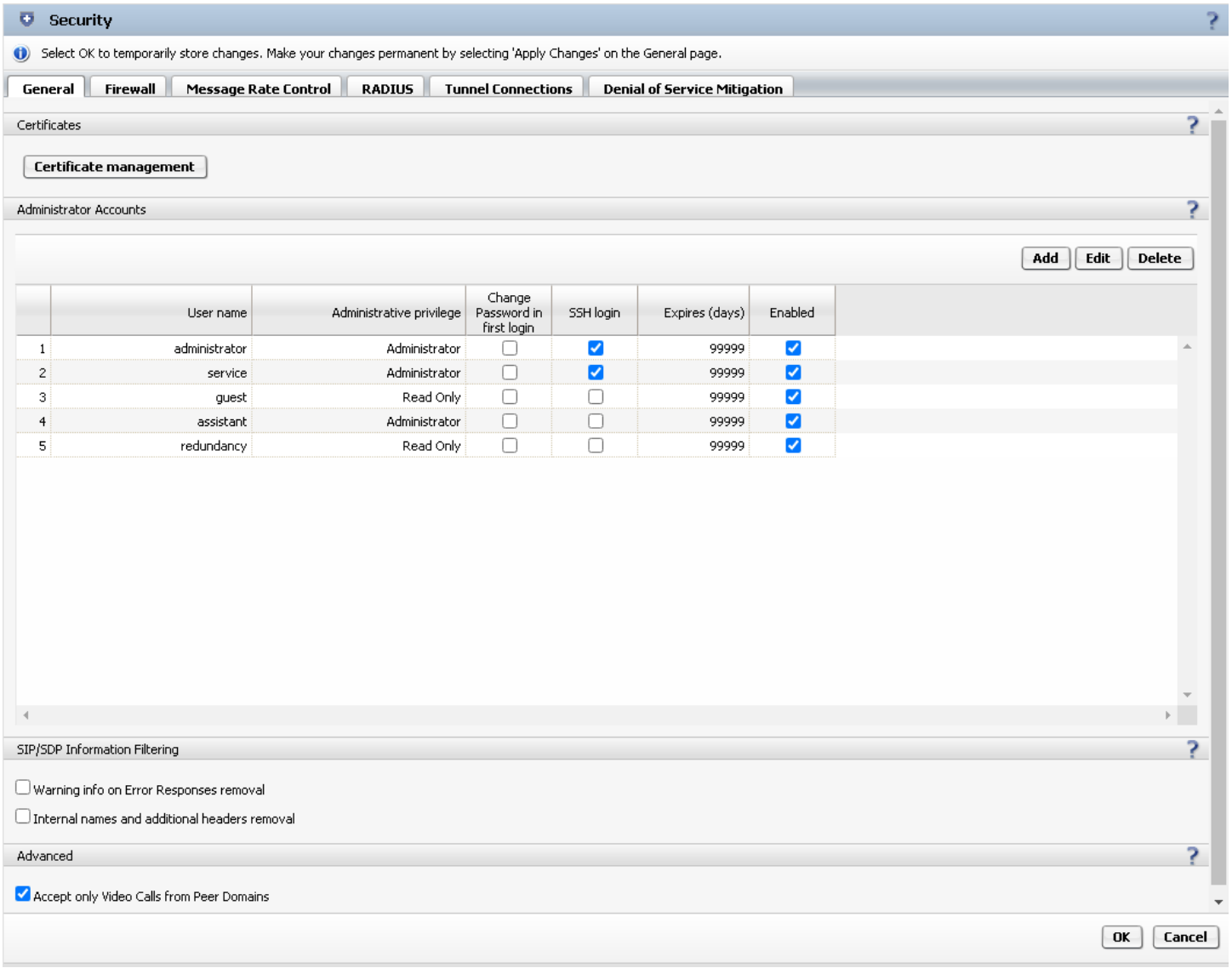
This script allows you to reset passwords, change passwords, change expiration time, enable/disable SSH login and enable or disable root privileges.

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 Warings 399 and 488 Header from SIP messages
- **"Internal names and additional headers removal"** - will remove the UA names, server names and X-Siemens headers from SIP messages



3.4.6.5 Advanced

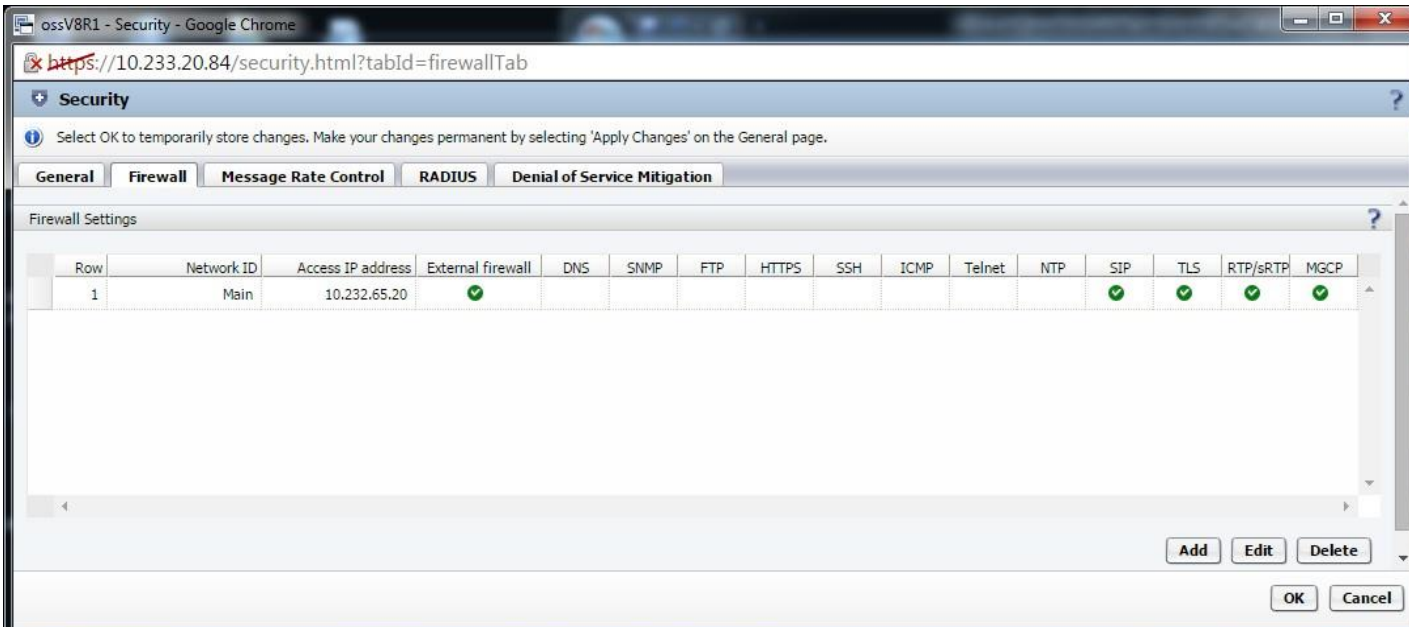
Accept only Video Calls from Peer Domains: When this flag is enabled, only INVITE messages containing a video m-line in the SDP is accepted from calls coming from the Access side (WAN) if Support Peer Domains or Support Foreign Peer Domains is the endpoint to be used. When no video m-line is received 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

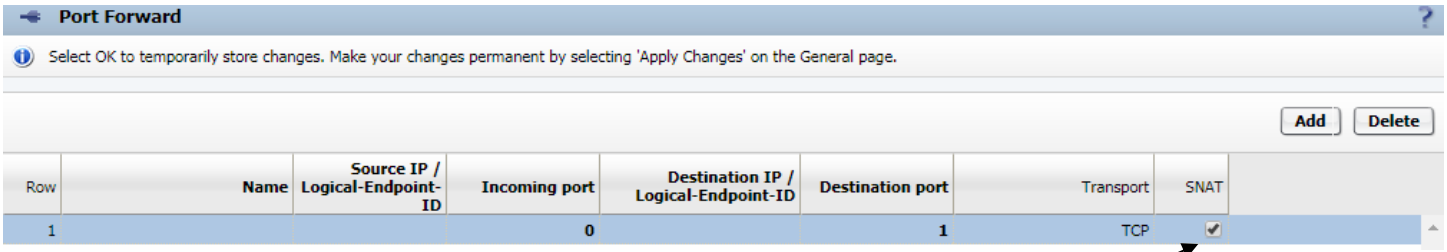
Each “Network Id” may have individual firewall

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.

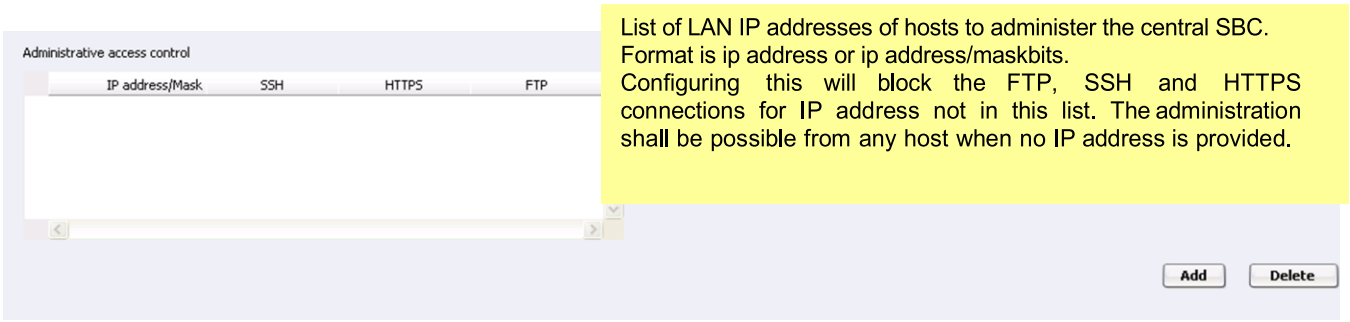
If port forwarding is administered for a TCP connection it will not take affect till the TCP connection is reestablished.

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 OpenScape desk top client using port 8443 to communicate with the CMP via the OS-SBC. OpenScape desktop functions.

3.4.6.6.3 Administrative Access Control

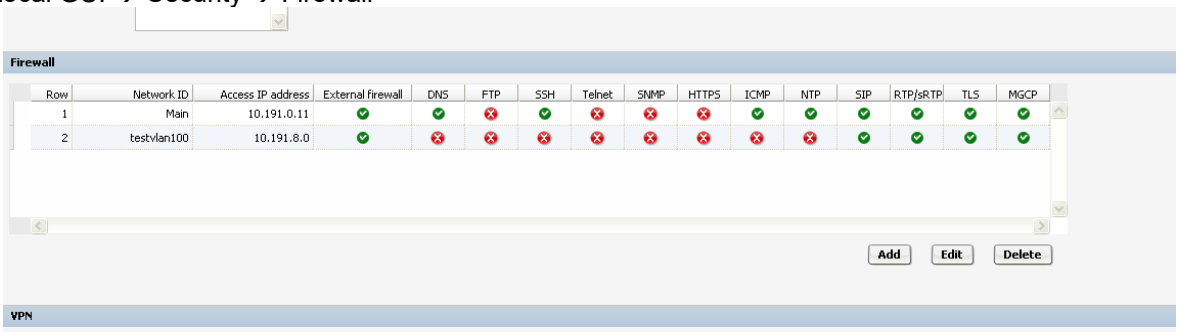
Local GUI → Security → Firewall → Select the network and Edit → Administrative Access Control → Add



List of LAN IP addresses of hosts to administer the central SBC. Format is ip address or ip address/maskbits. Configuring this will block the FTP, SSH and HTTPS connections for IP address not in this list. The administration shall be possible from any host when no IP address is provided.

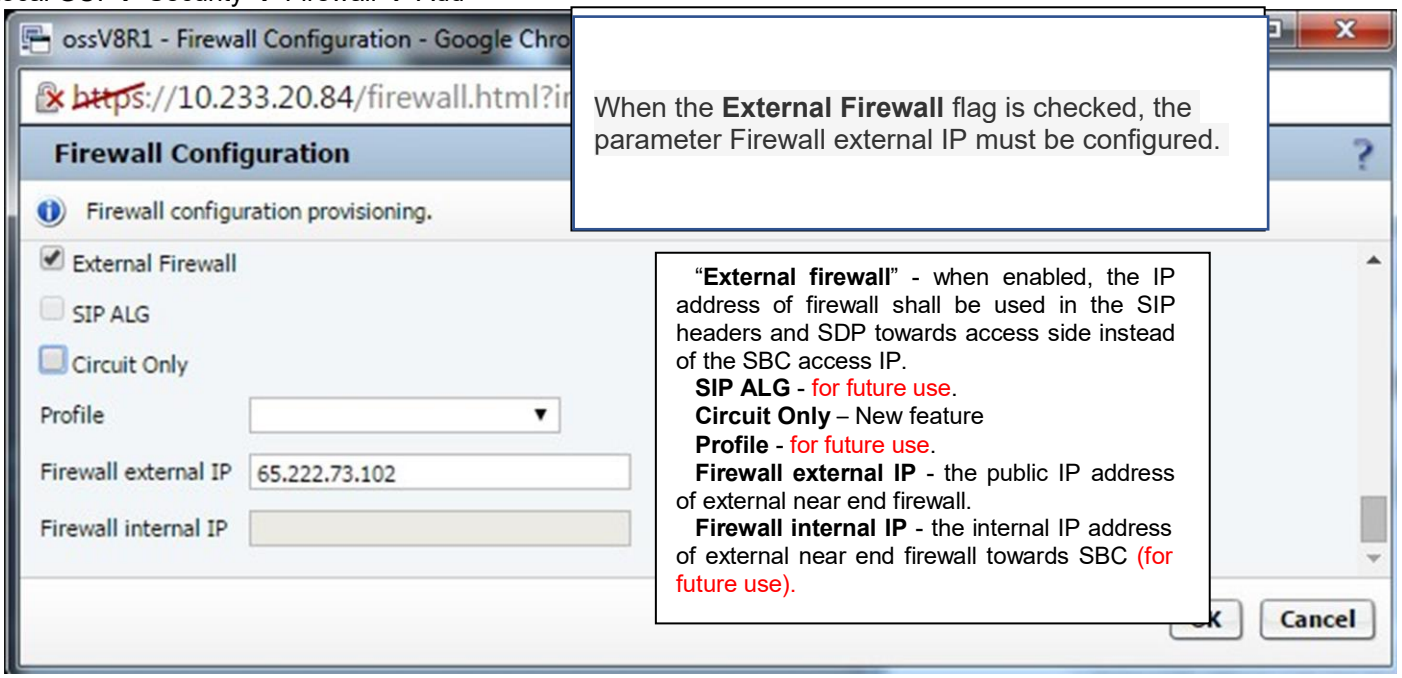
3.4.6.6.4 WAN Interface External firewalls TCP non TLS

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



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: number of sessions x 5 gives the number of required ports to be opened. 100 x 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.

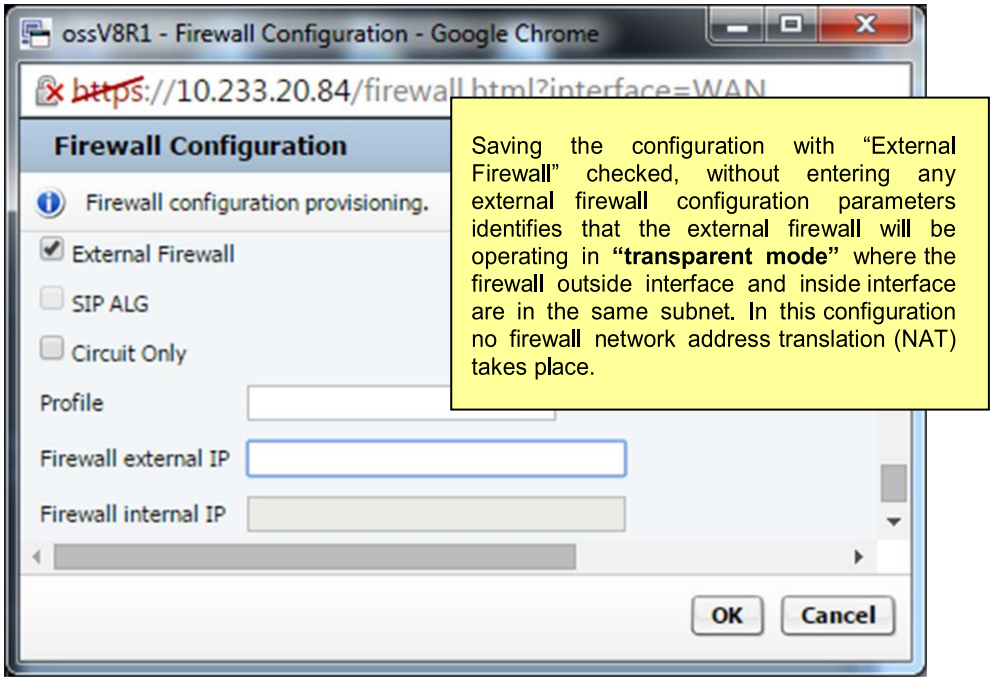
Using a firewall within the internal network.

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

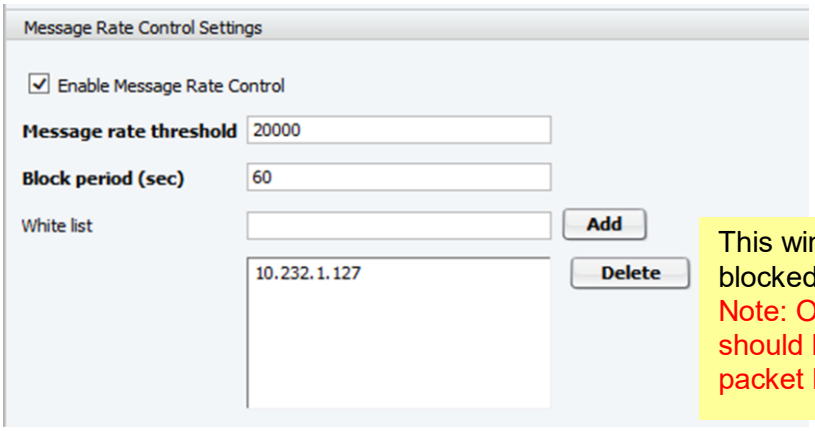
When Message Rate Control is enabled and Message Rate Threshold is reached, Message Rate Control will configure a Firewall rule to block the IP that generated such traffic. This IP will be monitored, if no more traffic comes from this IP the Firewall rule will be removed when "block period" expires. 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 belowered to the VoIP PPS threshold (recommended value of 300).

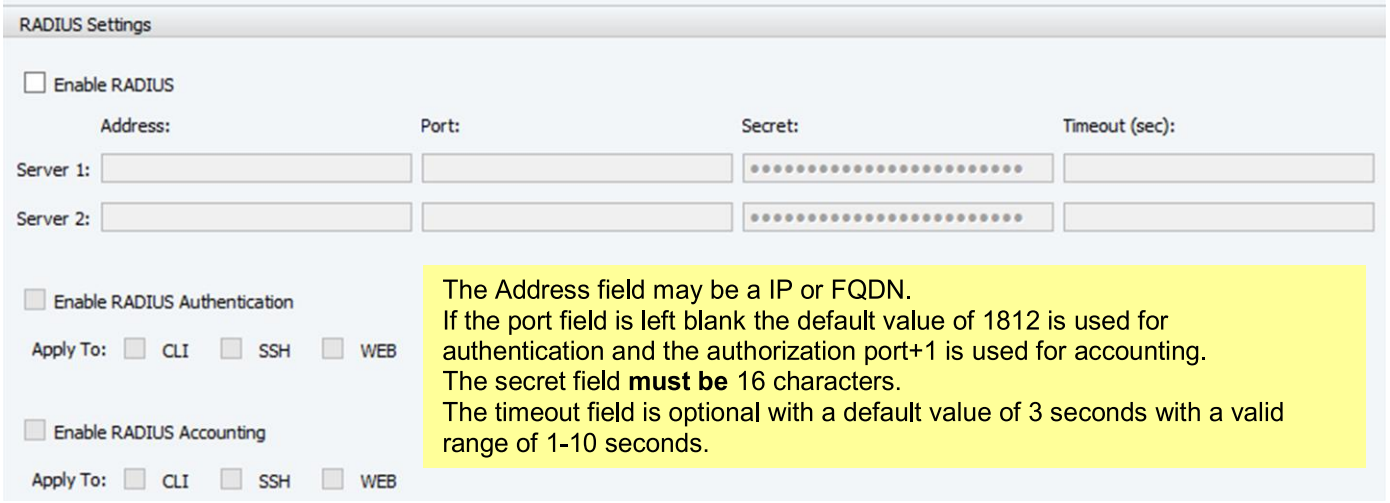
2. The Message Rate Control threshold is configured to the VoIP PPS threshold (recommended value of 300) and all network interface(s) used for the system upgrade file upload are configured in the Message Rate Control white-list. By placing these network interface address(es) into the white-list, they 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.



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

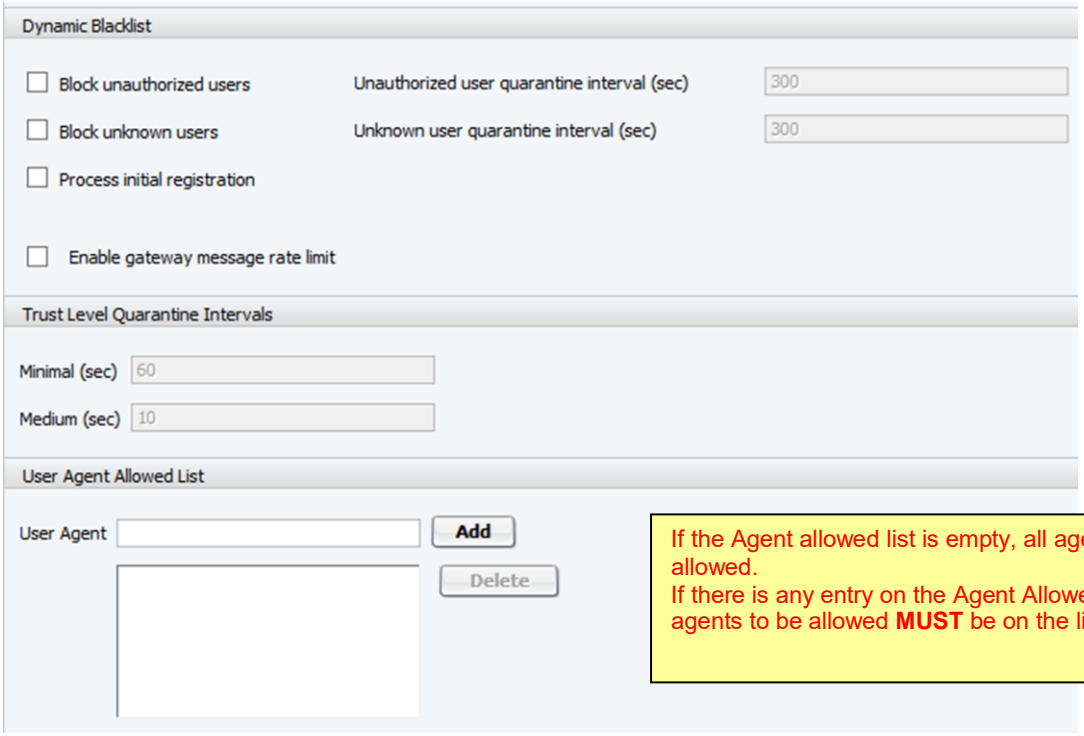
3.4.6.8 RADIUS



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**

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: 300 sec.)

- **Unknown user quarantine interval**

Quarantine interval for unknown users.
Valid range: 60 to 90,000 seconds (default: 300 sec.)

- **Enable gateway message rate limit**

By default the checkbox is unchecked. When checked (feature enabled) the system applies message rate limiting and quarantining according to the configuration of the OS-SBC Access SIP listening IP:Port address.

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 not present.

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 prefix name.
For Example
Polycom - This will match the user agent name PolyCom-V1 and PolyCom-V2

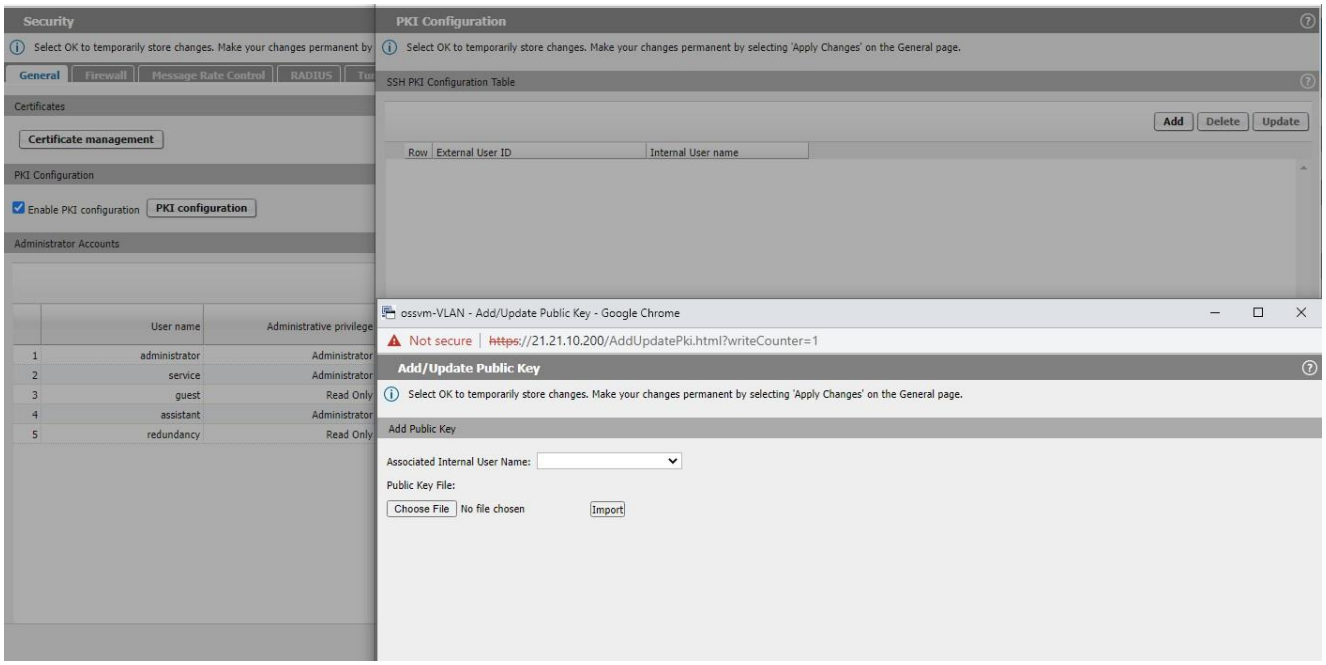
Note: The Denial of Service mitigation can be overridden by Firewall White List or Message Rate Control White List.

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 OpenScape SBC without having to explicitly log into the OpenScape SBC using a password. This is achieved by storing the external user's public key on the OpenScape SBC.

In order to configure a PKI for SSH follow the steps below:

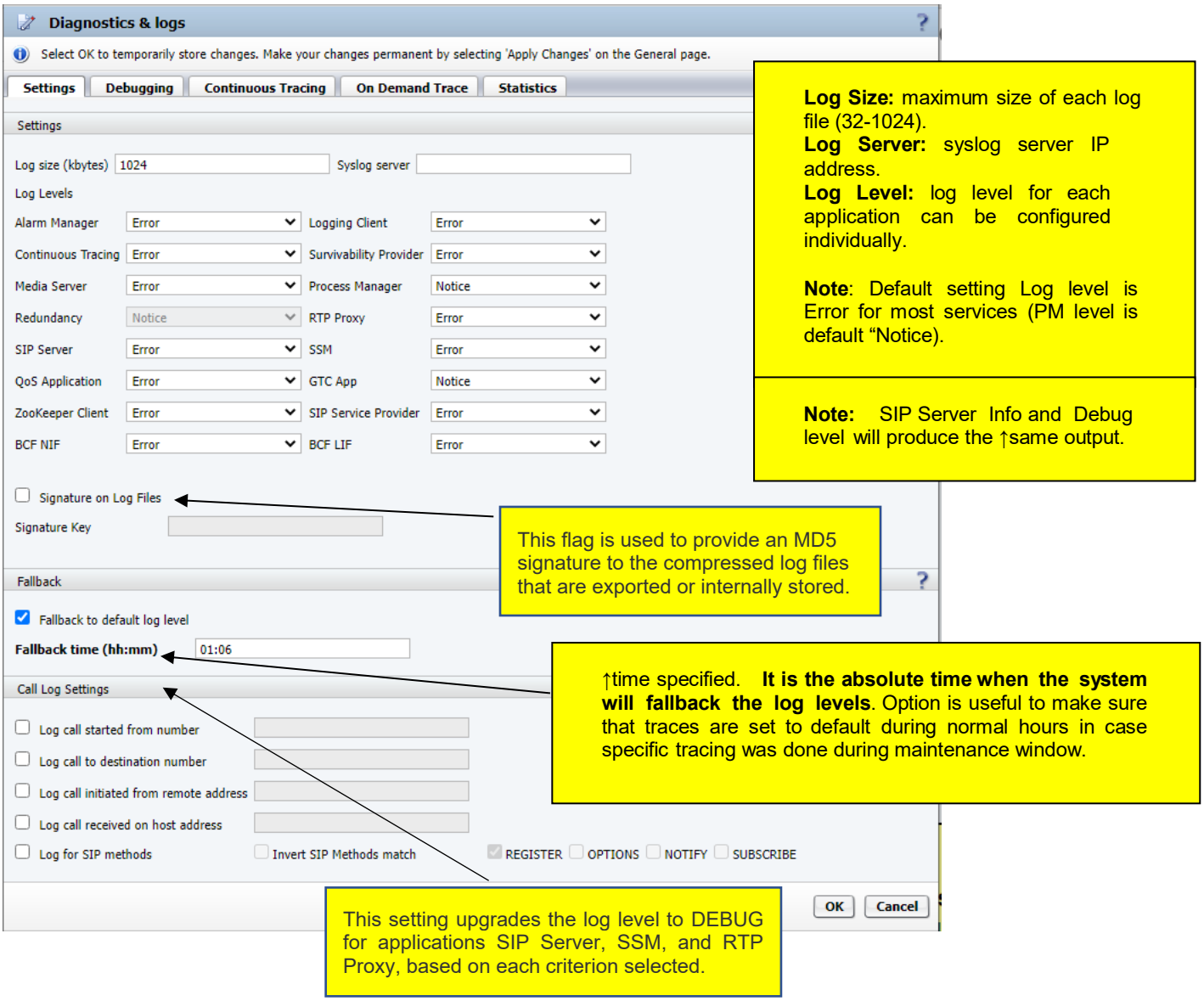
1. Check the checkbox **Enable PKI Configuration**.
2. Click **PKI Configuration**.
   ➔ A new PKI Configuration screen is displayed.
3. Click on the **Add** button.
   ➔ A new **Add/Update Public Key** screen is displayed.
4. Select from the **Associated Internal User Name** dropdown list the internal 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 inthe 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 than 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.

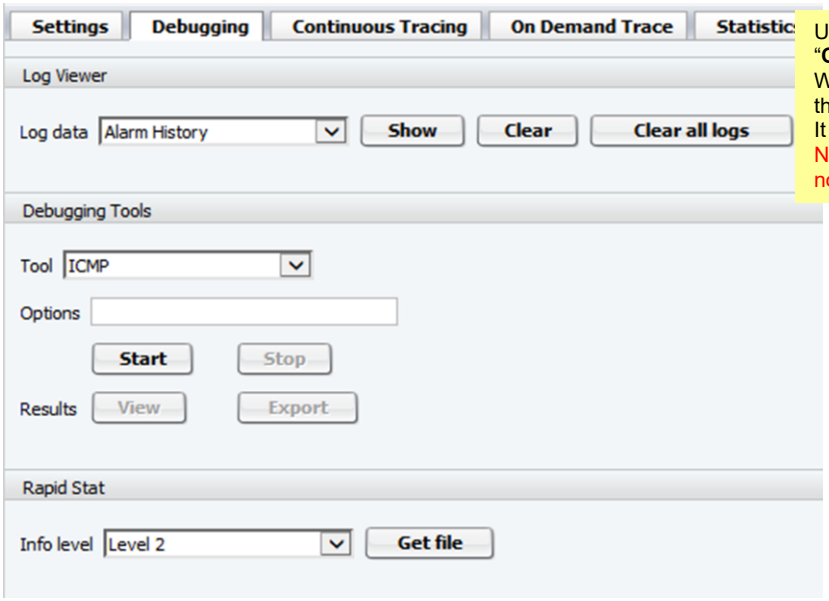


Log Data	Description
Alarm History	Alarm history shows details about alarms triggered in the system. These details include information of date, time and, threshold when the alarm was activated or cleared.
Alarm Manager	Log of the Alarm manager application. Useful when an alarm is not being triggered, 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.
Peer Monitoring	Log of the Peer Monitoring application, which monitors some peers using OPTIONS messages.
	Note: This configuration is only available in V11R1.01.00 or higher.

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"

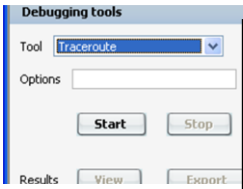
3.4.7.2 Debugging



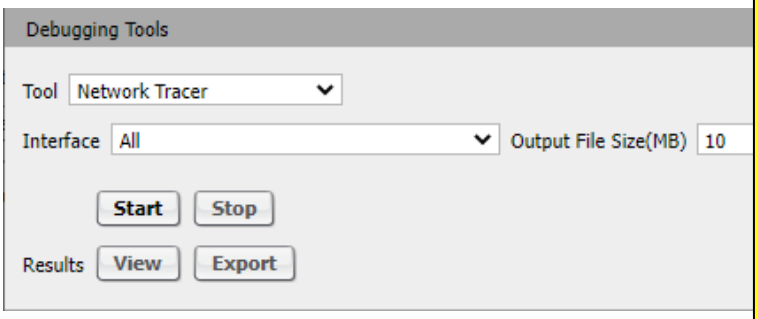
User can select a logfile and "**Show**" it, or "**Clear**" the selected logfile.
While "showing" a file, the user may export the data to a save file.
It is also possible to "**Clear All**" logfiles.
Note: certain logfiles are read only and can not be cleared (ex. Alarm History, Boot log)

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 thisoption.

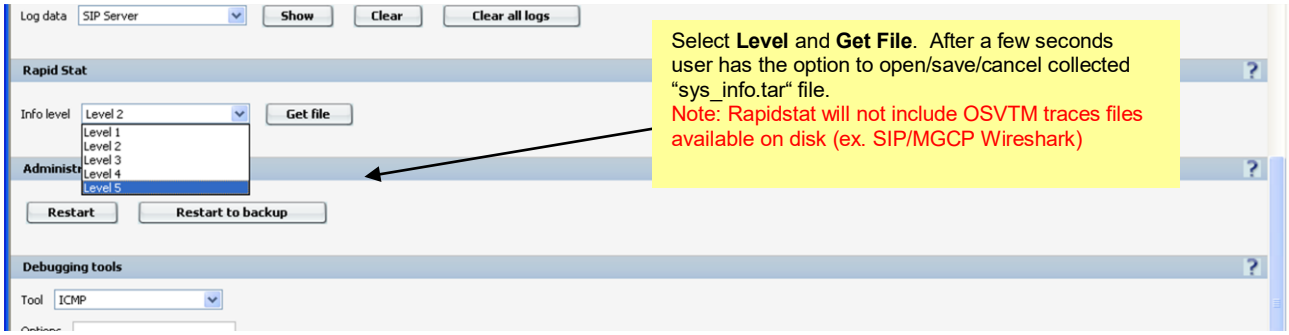
The SIP/MGCP trace option is used to capture network trace in the application level. (SIP and MGCP protocols are shown as UDP messages. Q931 is shown as TCP and is only applicable for Integrated Gateway.)
Use the SIP/MGCP/RTP trace option to capture RTP for debug of speech problems.

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.

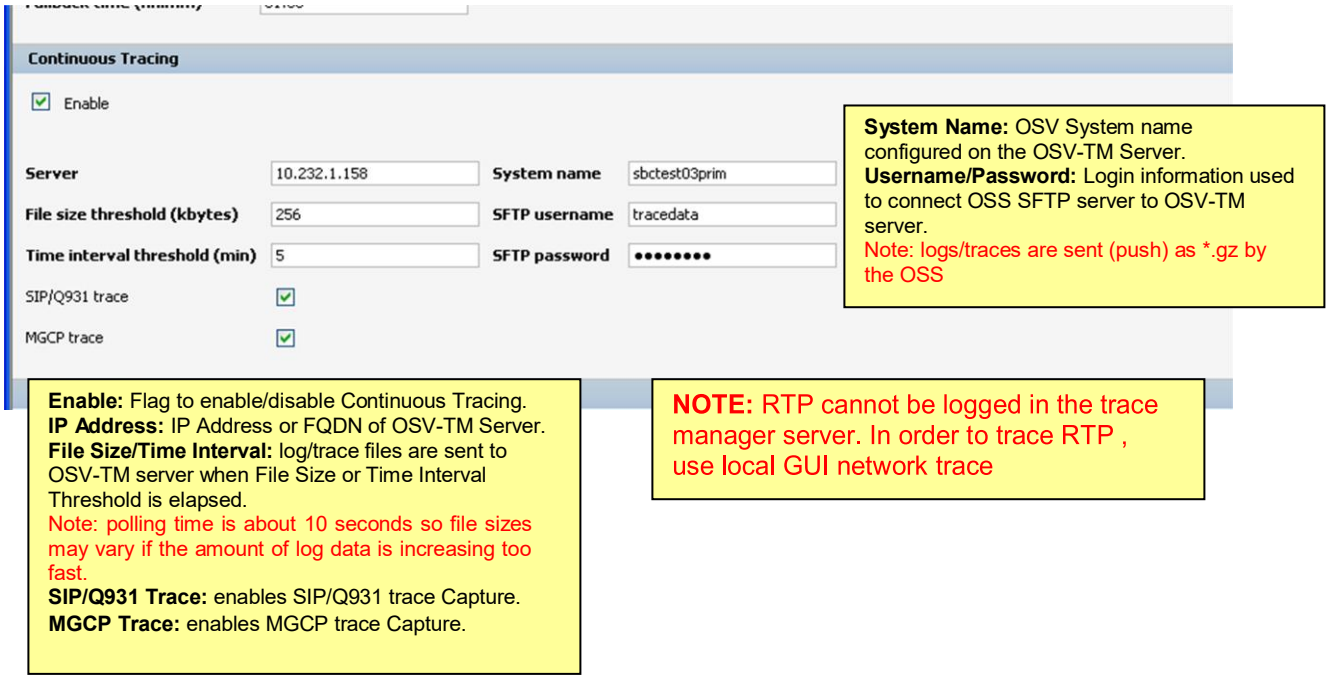
According to the level the following information will be stored in the compressed file:

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



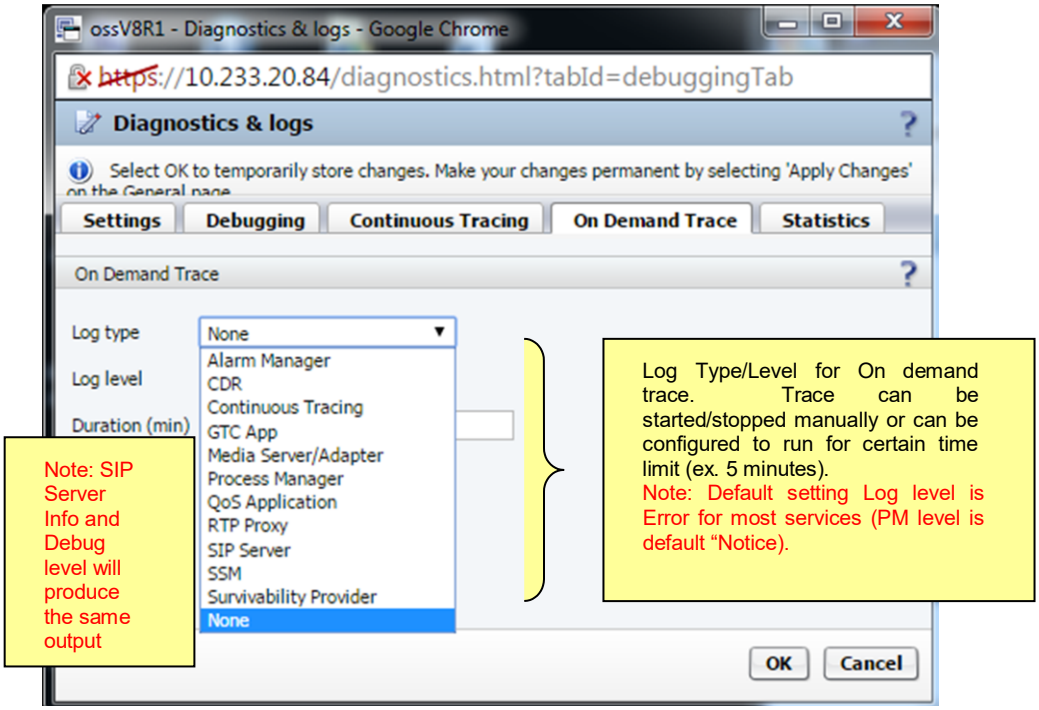
3.4.7.3 Continuous tracing

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 than 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



3.4.7.4 On Demand Trace

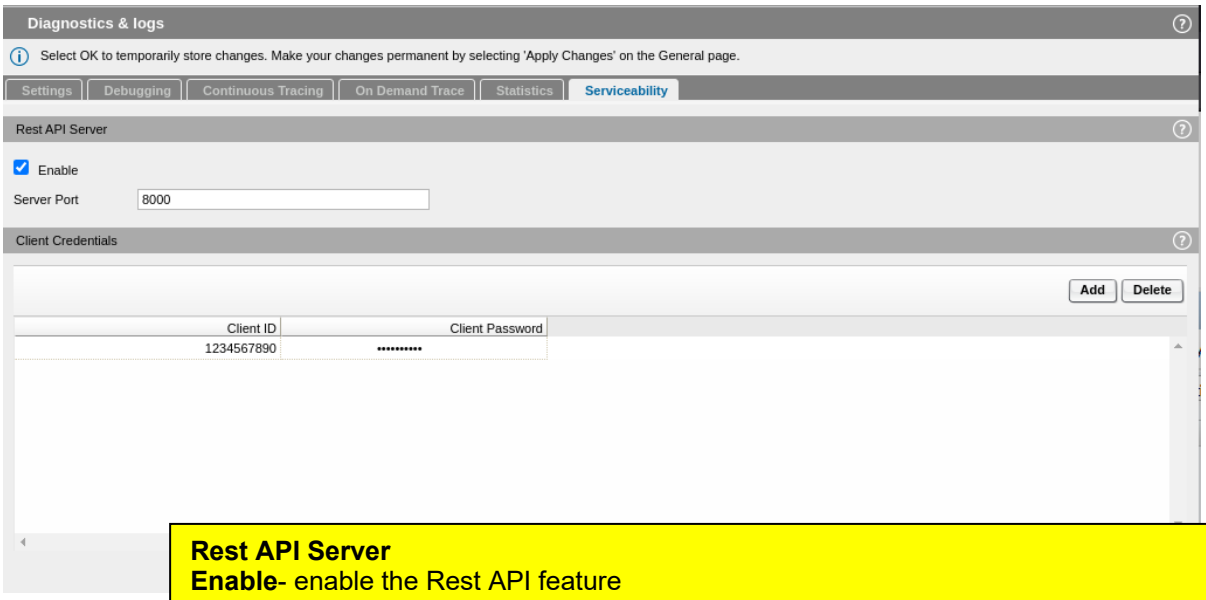
On Demand Trace allows selecting a log type and log level manually or for a specific time period. The "on demand trace" overwrites the log level configuration for a specified interval of time. After that the log level configuration goes back to the configured one. The Continuous Tracing file size and 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



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.

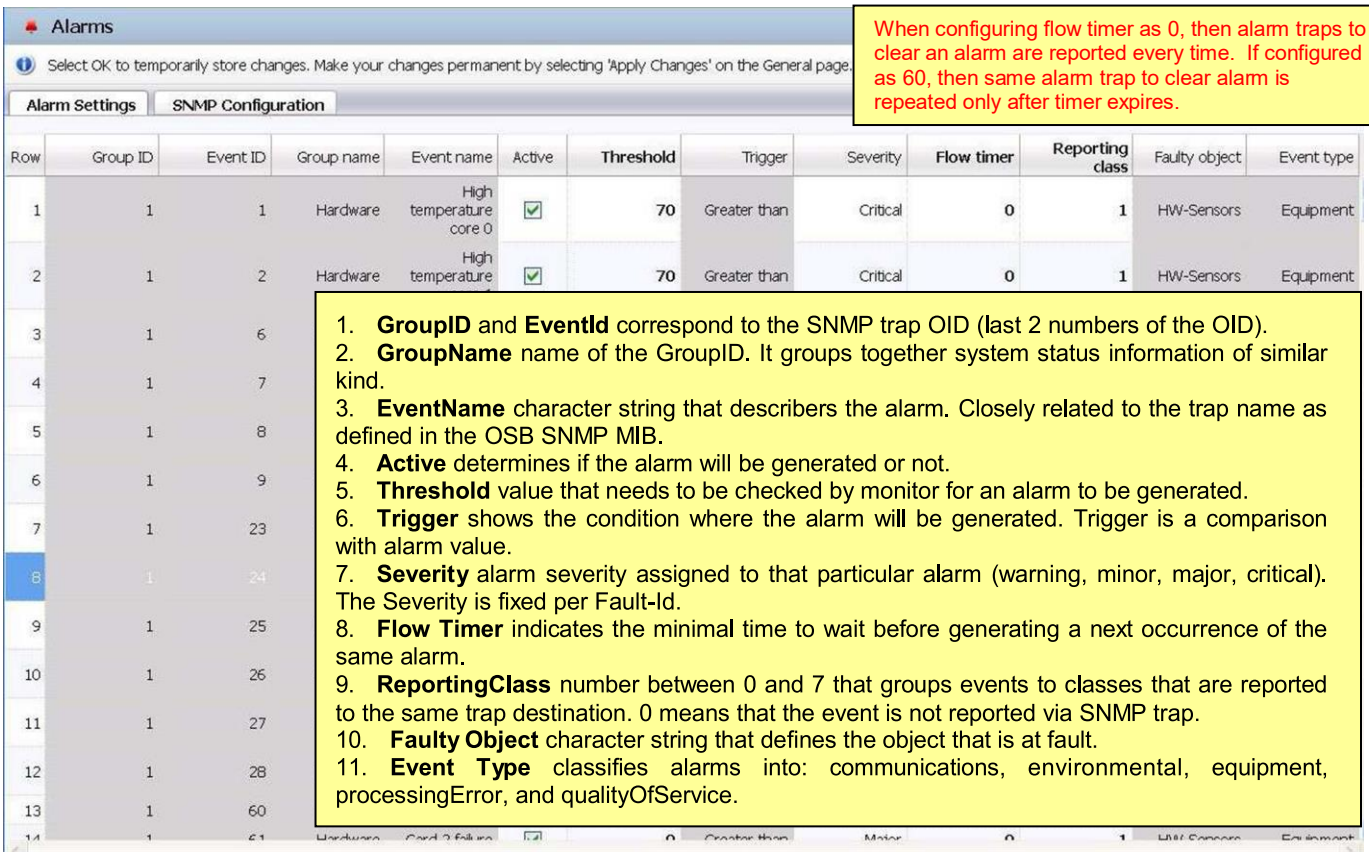
Client ID - Unique ID with at least 10 characters.
Client Password - Password with at least 10 characters.

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

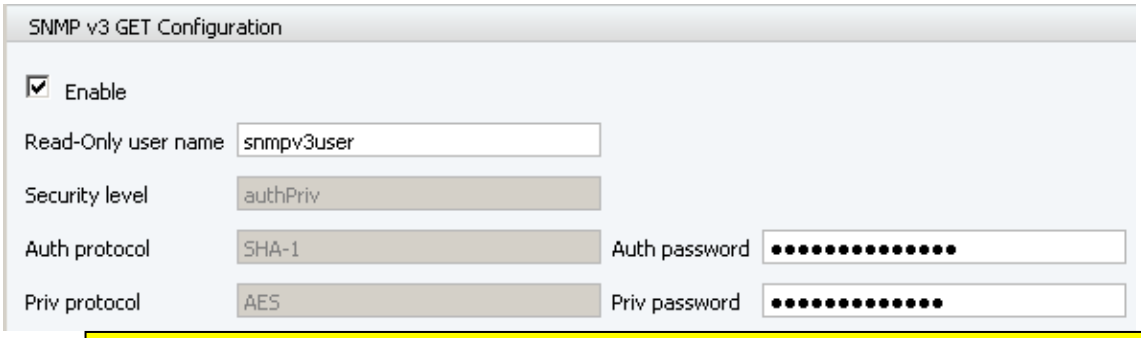
This allows configuration of alarm thresholds, severity level, flow timer, reporting class and if the reporting of the alarm is activated.



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.



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.

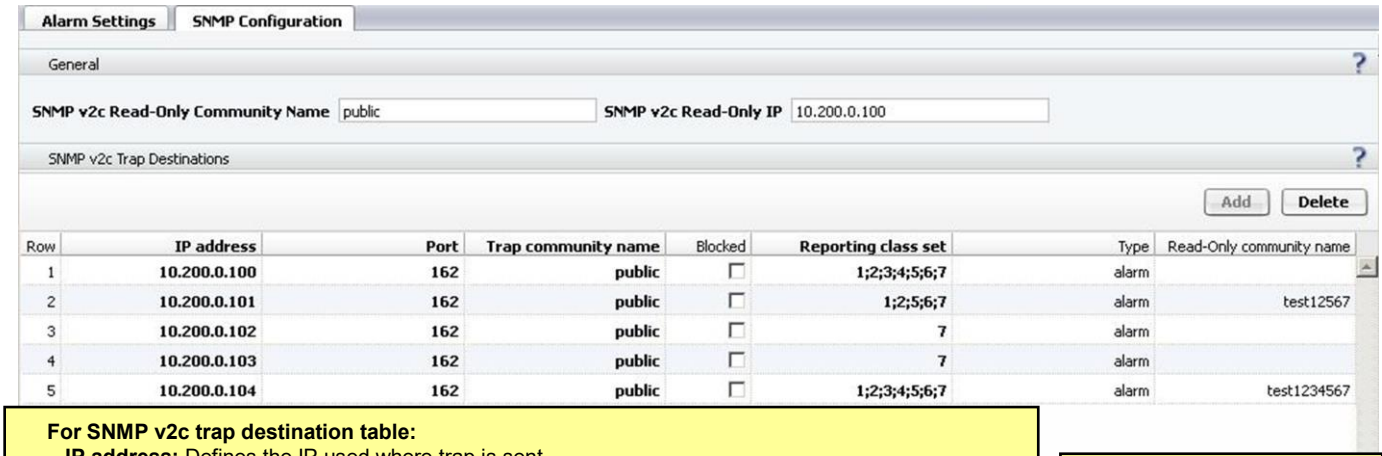
The following format should be used in the file:
alarm_trap[index]_community = "[newSnmpCommunityString]"

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.

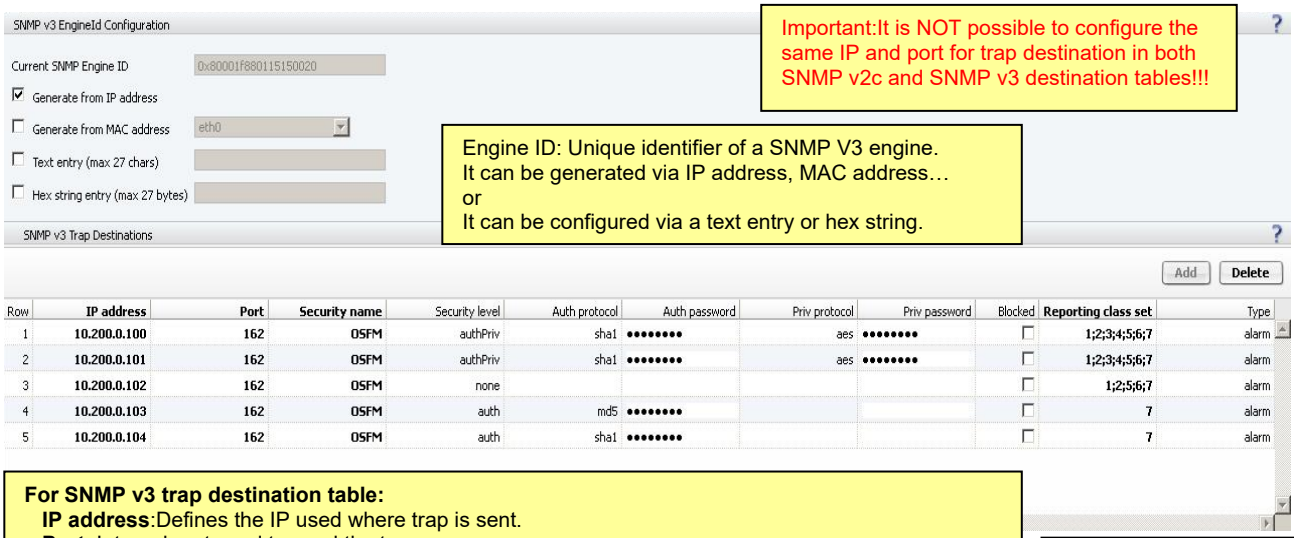
Alarms can be routed to a remote device using SNMP v2c or SNMP v3.

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.



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.



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

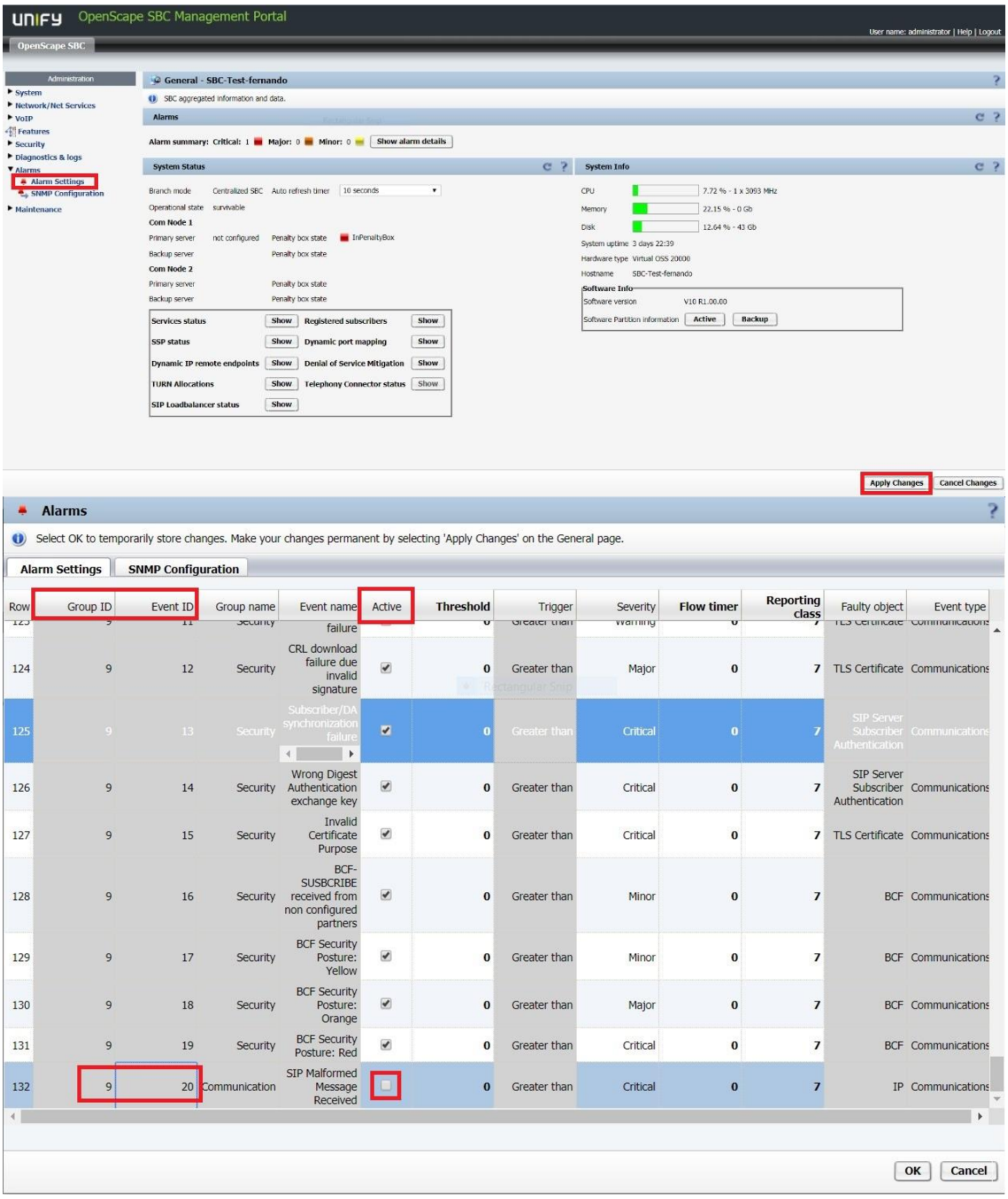
Engine ID: Unique identifier of a SNMP V3 engine.
It can be generated via IP address, MAC address…
or
It can be configured via a text entry or hex string.

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 opassword.
Blocked: Trap will not be sent (if checked).
Reporting class set: list of Alarm Reporting Classes that will be reported via SNMP TRAP.

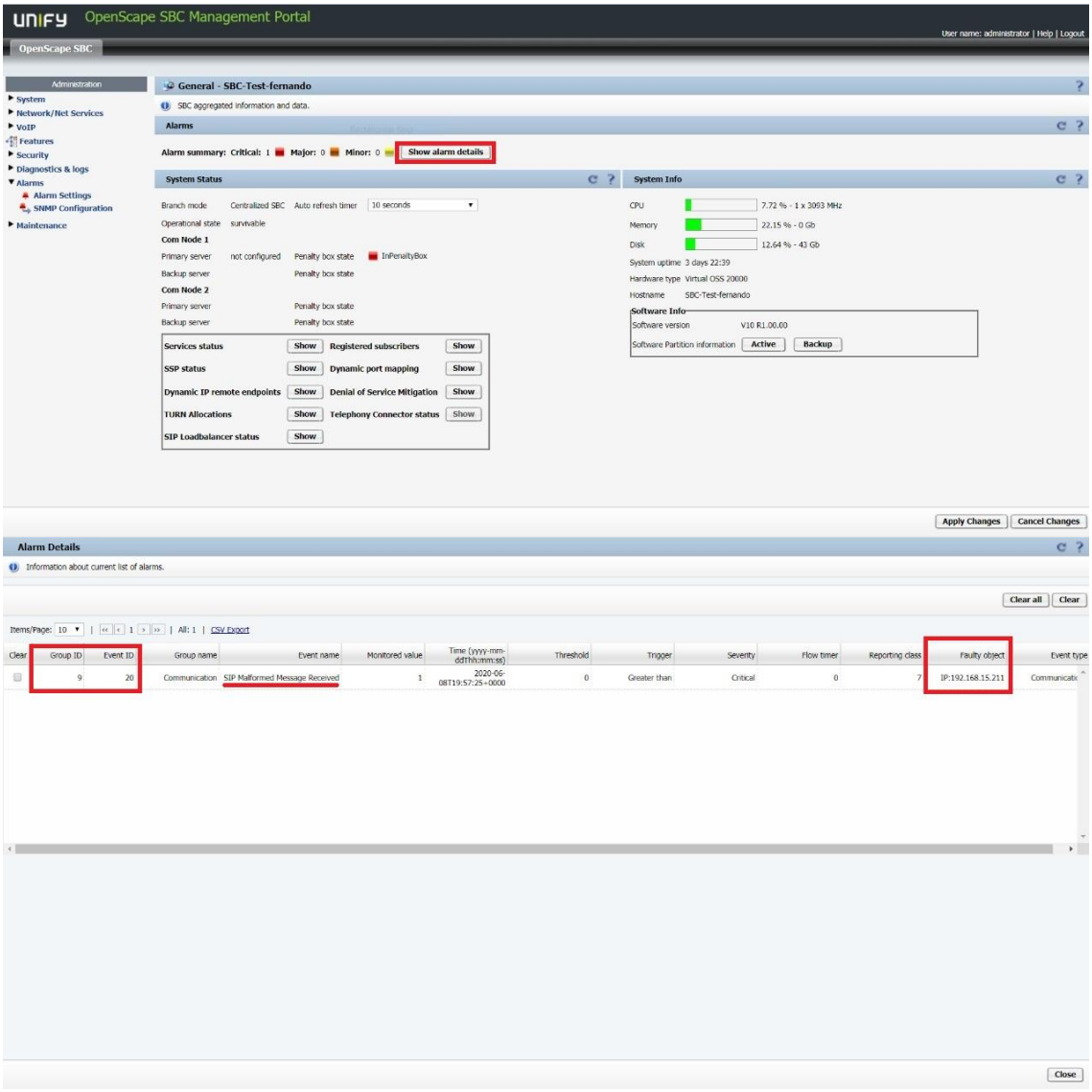
Note:up to 5 trap destinations can be configured.

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.



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.

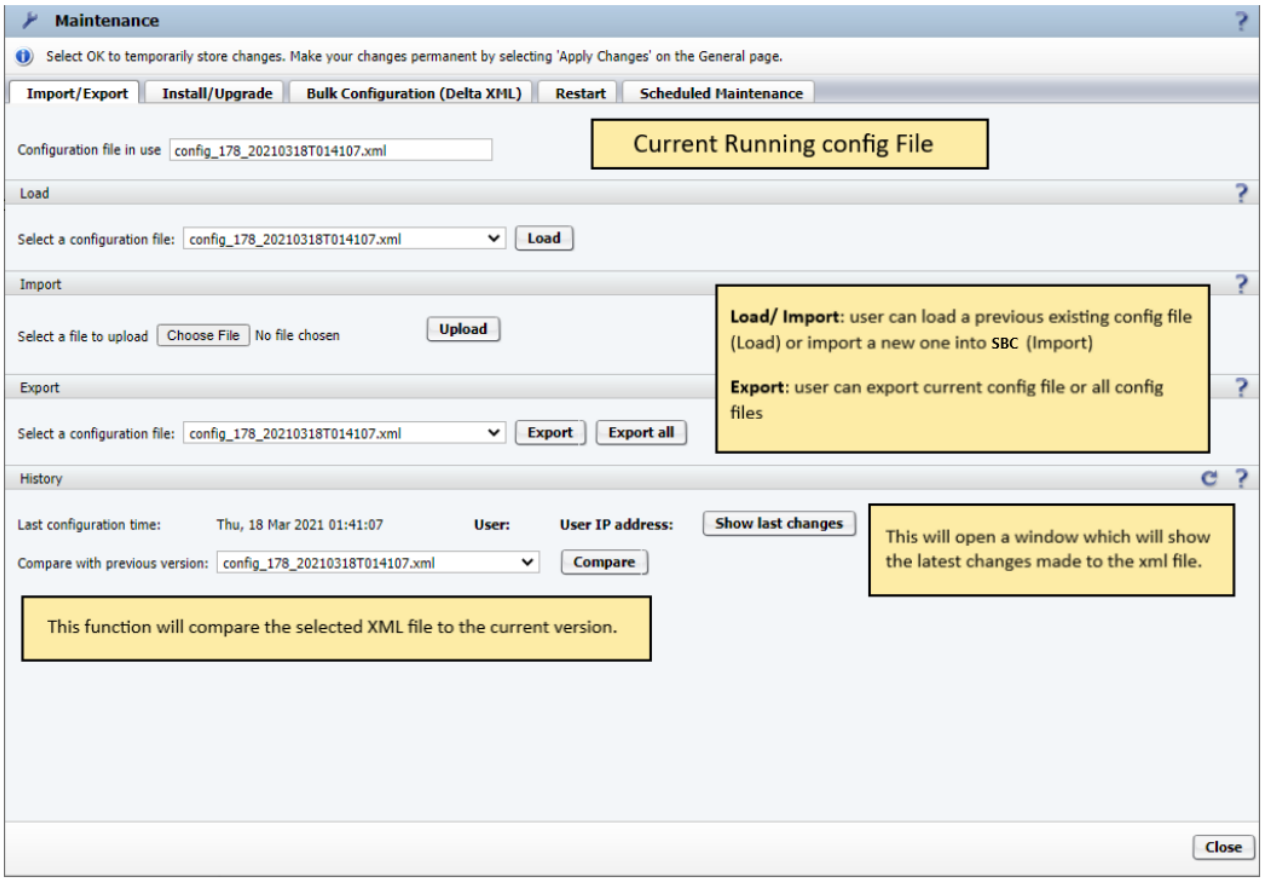


3 – This alarm also can generate Trap messages (SNMP). Please refer SNMP configuration section in this guide.

3.4.9 Maintenance

3.4.9.1 How to import / export a file

Import / Export Tab under Maintenance includes the following fields:



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

Installation erases both backup and active partitions and overwrites the existent software version in USB. The database can be preserved if previously stored in USB stick.

Starting from V10R2, **the UEFI bootloader flag is available in the installation option. "UEFI Bios detected" or "UEFI Bios NOT detected" message is also shown, depending on the boot mode configured in the server.**

For Legacy Mode, this flag should be deactivated and for UEFI Mode this flag should be activated.

The UEFI bootloader flag could be also activated in the USBsticksetup.

Please, attention to choose this option. The System Boot Mode must be configured correctly, otherwise the Server will not boot from the Hard Drive.

INFO: For virtual machines, it is recommended to use Legacy Mode, then this flag should be not used.

INFO:
Using physical hardware, this option is available only if the USB stick is plugged and the system is booting from the USB stick. For virtual machines, this option is also available in full installation.

- **Partitioning**

By default, the system disk has 2 partitions:

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”

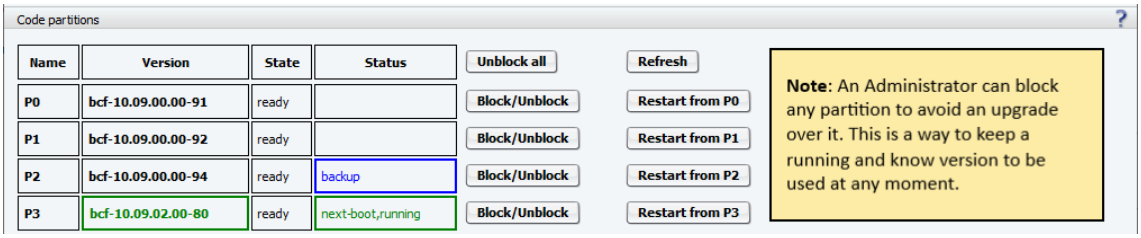
As shown, the partition 2 becomes the new “Active” partition and the Partition 0 is the new “Backup” of “Active” partition. If a new upgrade is done, then the result is:

- 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”**

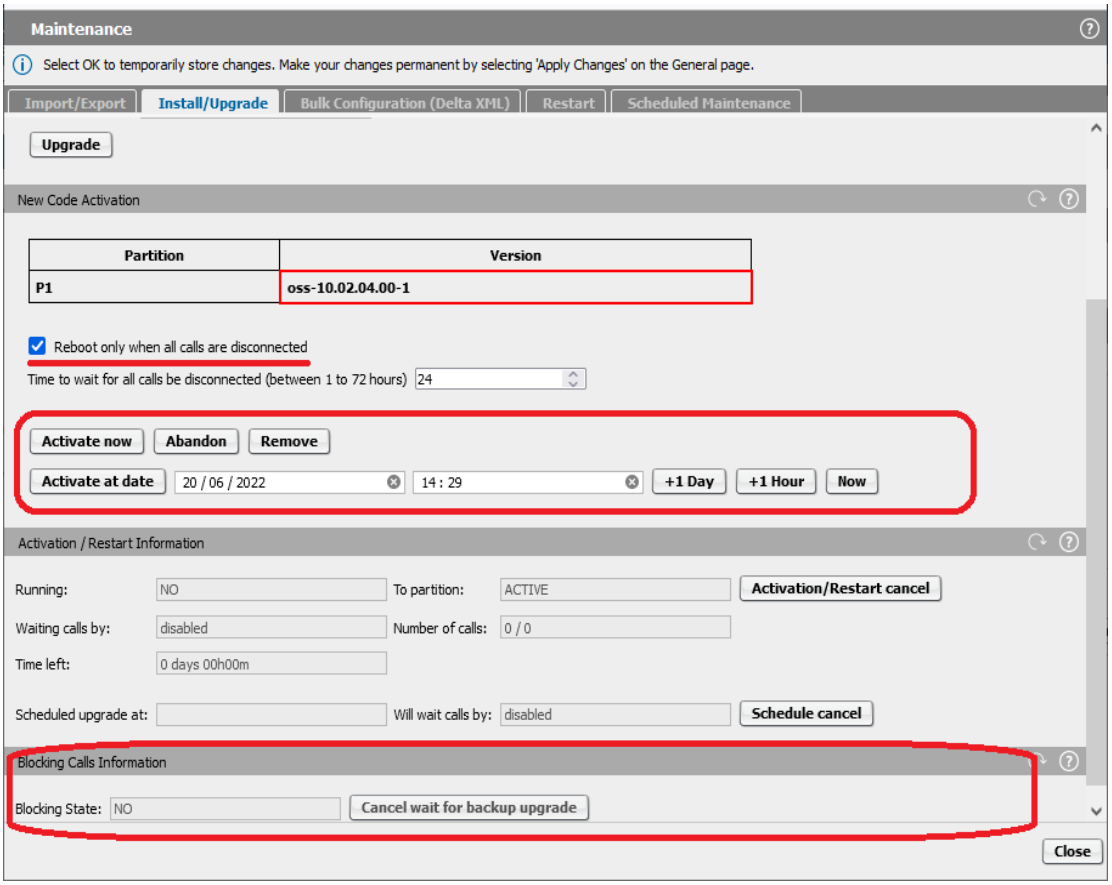
The process continues as described. An administrator can change the “Active” partition to any valid software partition and its backup partition is automatically selected if it is still available. This is done at code partitions under the restart tab.



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:



- **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.

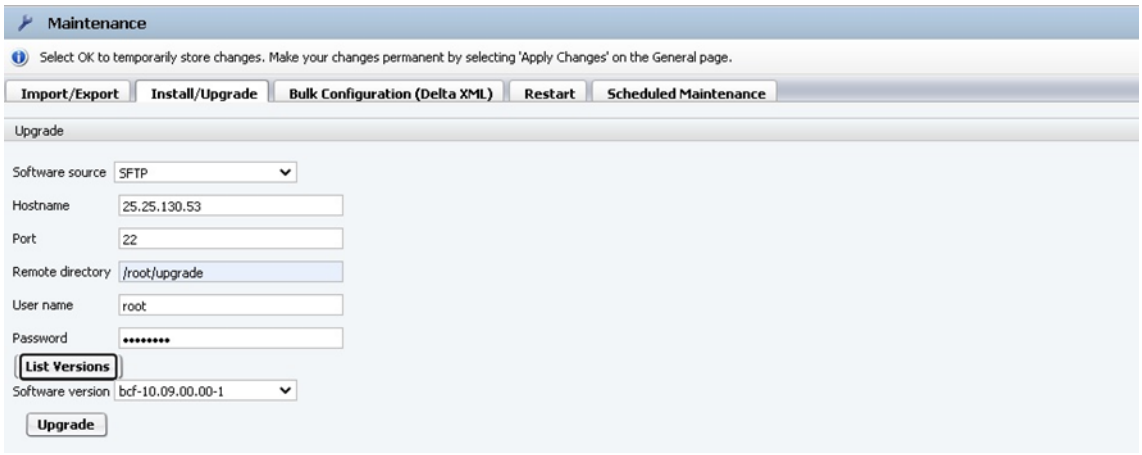
a) Browse to select the "tar" file to be used for the update.
b) Click **Upgrade**.
c) When files are copied confirm restart.

Note: In case of a redundant system both nodes are upgraded. Master node first and after that the backup node.

3. HTTPS

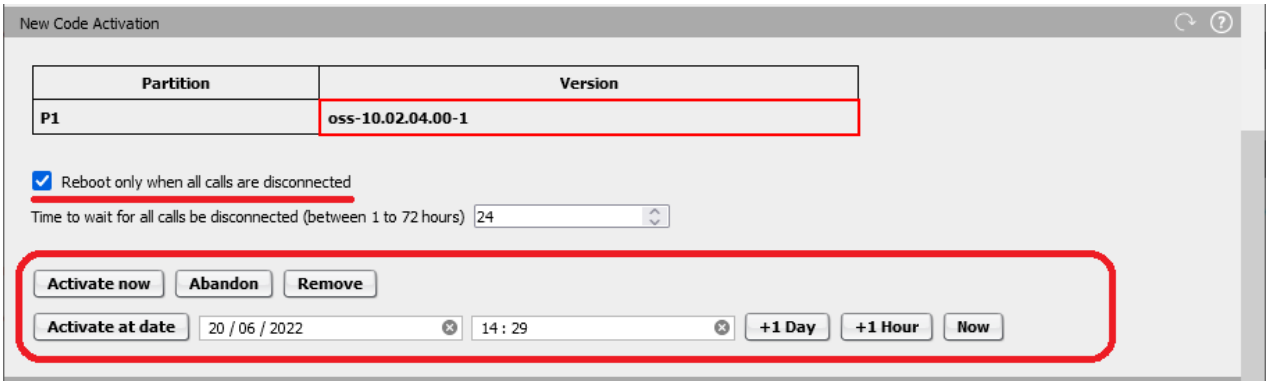
a) Provide the hostname (IP address) and remote directory of a https server which contains the software image.
b) Add the *.tar and *.spa files in this directory. The file named "**list**" must be added in the same directory. This file should contain the name related to the software image, e.g. image_SBC-10.09.00.00-1.tar.
c) Click **List Versions** and select the available software version to upgrade.

4. SFTP



a) Provide the hostname (IP address), port and remote directory of SFTP server which contains the software image.
b) Supply a username and password to login to the server.
c) 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.
d) Click **List Versions** and select the available software version to upgrade.

- **New code activation** field



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.

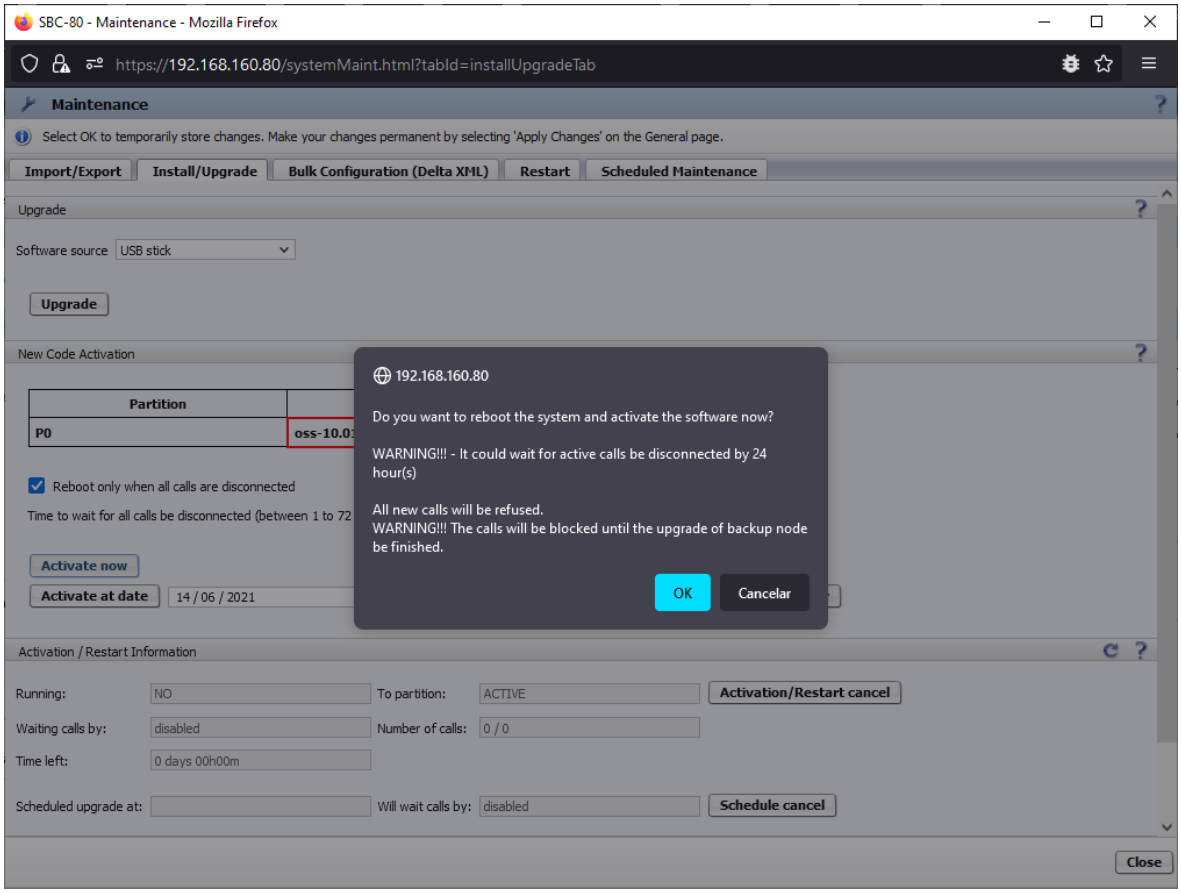
It is also possible to request the system to wait for running calls before reboot to activate the new code. For redundant system, when the flag **Reboot only when all calls are disconnected** is selected and upgrade is activated, the calls will be blocked until the end of upgrade process in both nodes (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.



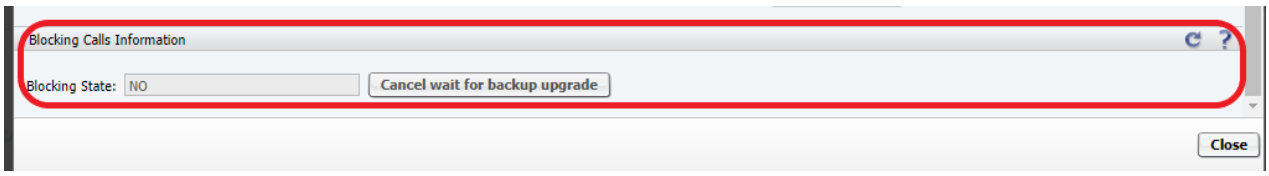
- **Activation / Restart Information** field

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.

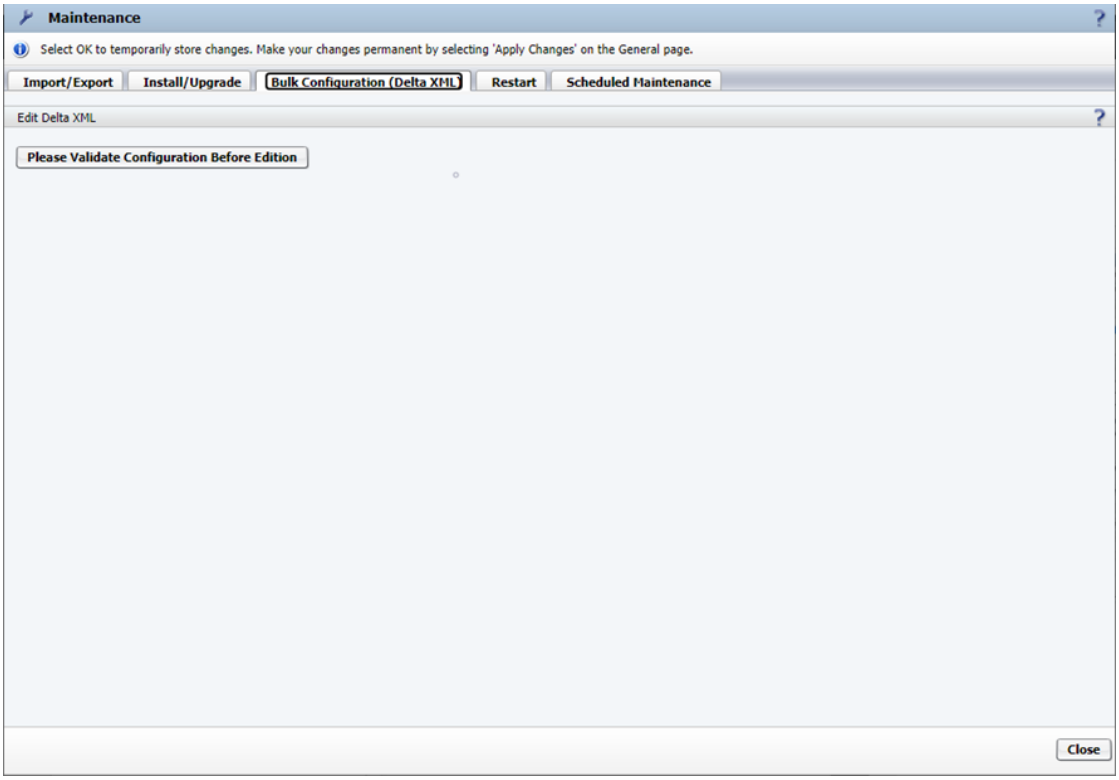
However, it is possible to unlock the calls when the master node has already performed the upgrade and the backup node is not finished yet. For this, it is necessary to use the **Cancel wait for backup upgrade** button.

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.

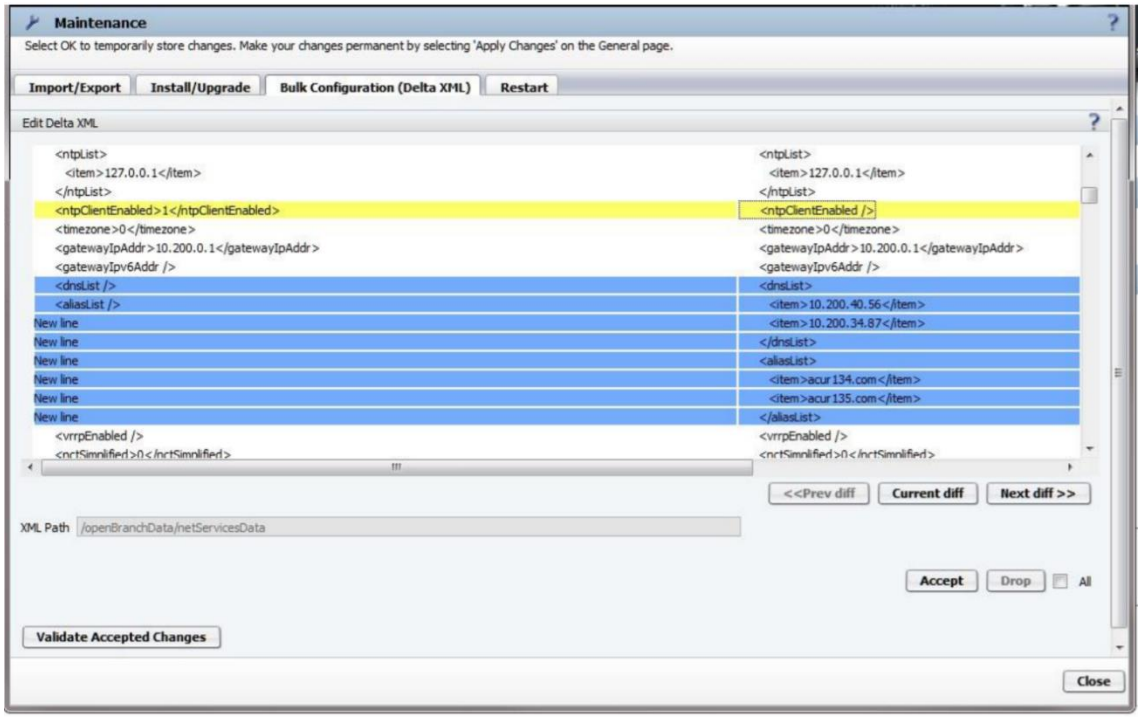
Note: Changes done on configuration after this step are detected only when reloading the "Bulk Configuration (Delta XML)" tab.

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).

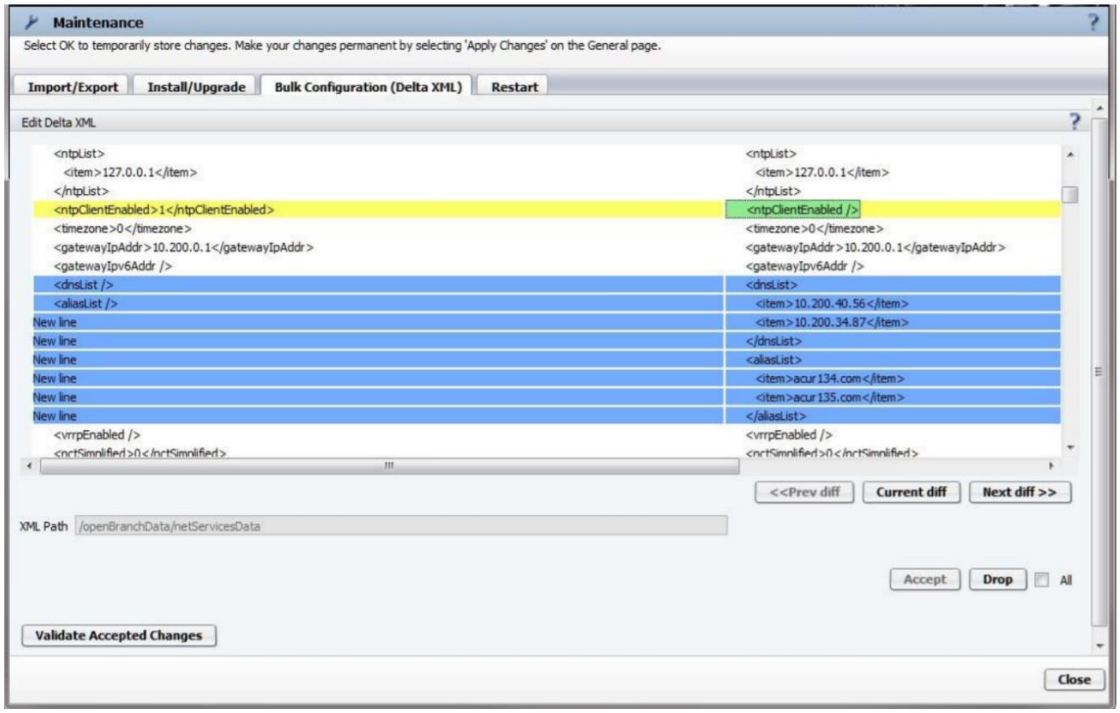
Note: In normal configuration task this feature can be used to have a preview of modifications on xml before the **Apply Changes**.



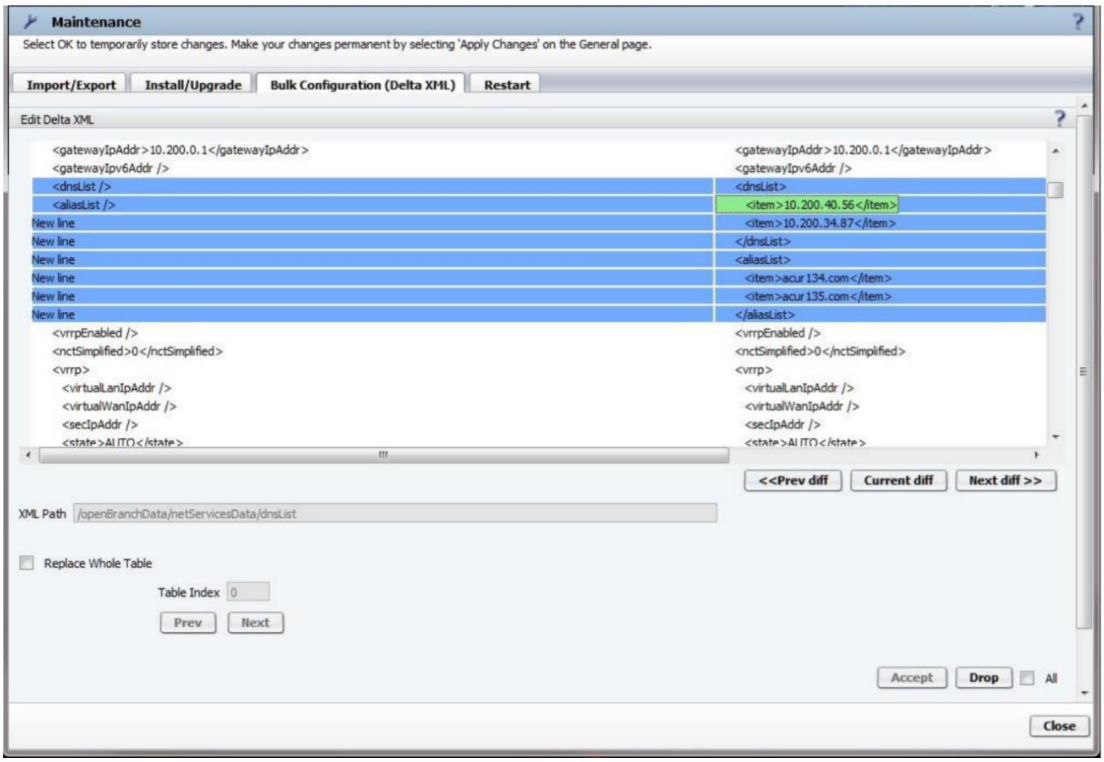
Only "accepted" changes are included on Delta XML files. It is possible to include/exclude changes on Delta XML file individually or in groups ("item" elements (lists or tables).

Accept and **Drop** acts over currently selected change (checkbox **All** unchecked).

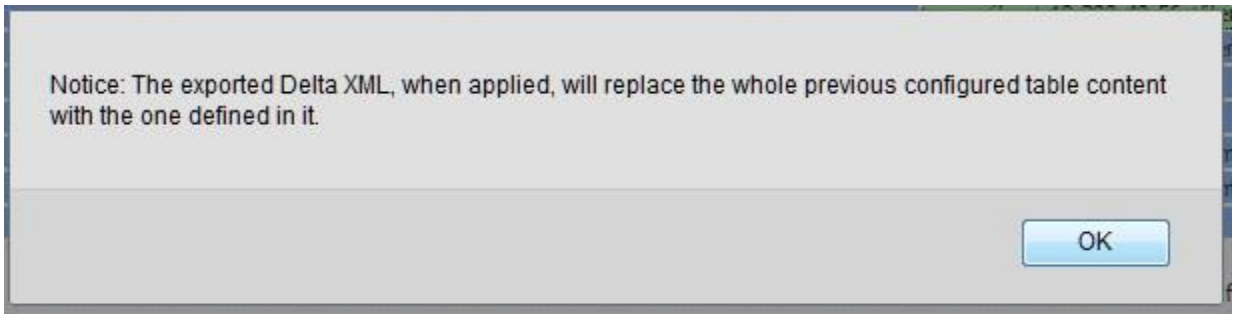
Accepted changes are marked with a green background. Dropping an accepted change returns its background to the original color. Original background colors are the same ones used on the **Compare** on **Import / Export** tab.



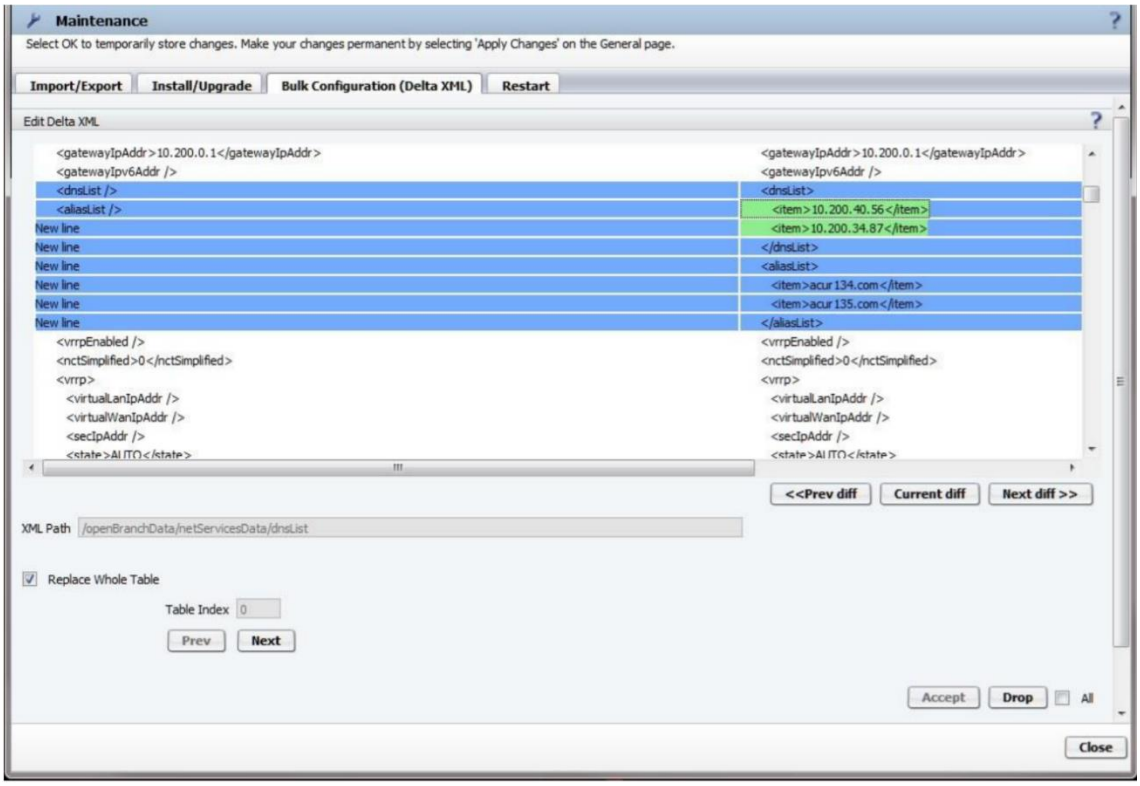
For lists and tables ("item" elements) there are additional operations shown at the left area below the "XML Path".



This Notice is presented the first time **Replace Whole Table** is checked:

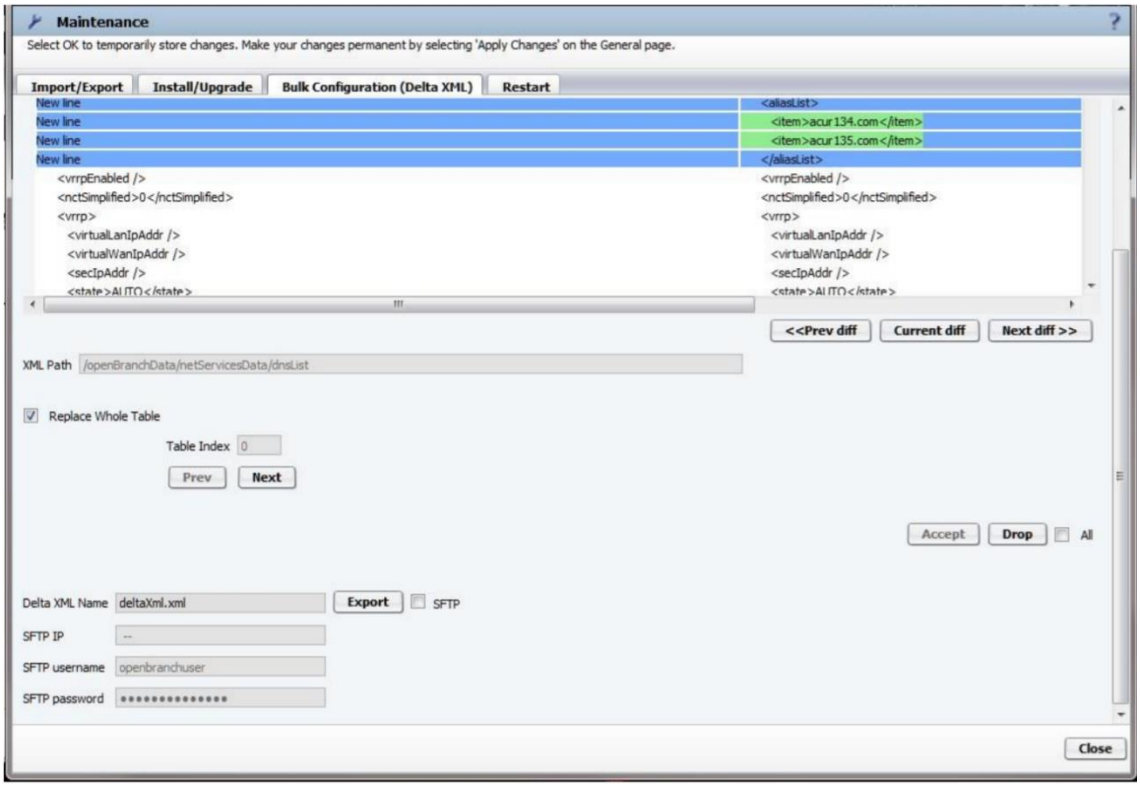


If the **Replace Whole Table** is checked, all "item" elements in the same level are colored in green. The exported Delta XML, when applied, replaces the whole previous configured table content by the one in green. **Table Index** informs the position of the "item" element (starts with 0).
Prev and **Next** 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.

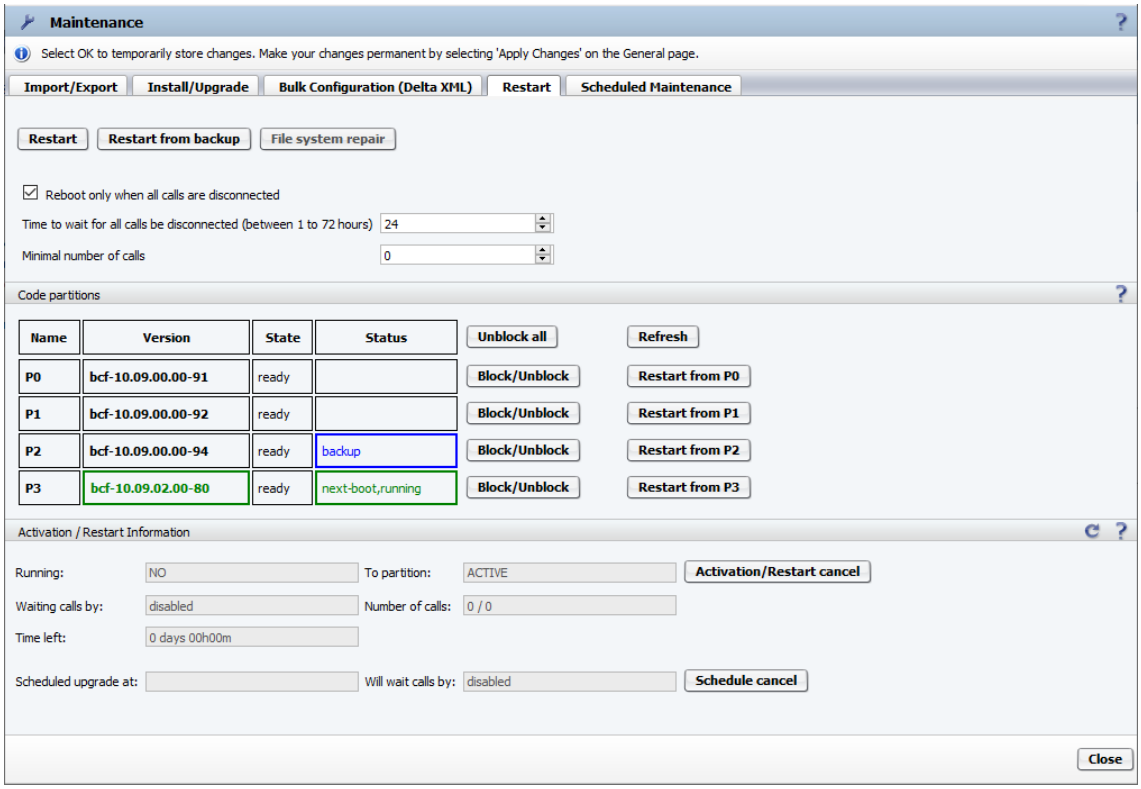
All xml tags inside the following xml tags are ignored for the purpose of generating Delta XML file:

- alarmList
- saveUser
- saveRUser
- saveTime
- clientIpAddr
- swVersion
- hwType
- product
- hostname

- logicalBranchOfficeId
- hwId
- saveCounter
- openBranchNetwork
- mode
- voipData.

3.4.9.4 How to Restart

Restart Tab under Maintenance includes the following areas:



- **Restart** button

This button is used to reboot the system and use the active partition.

The user is prompted to confirm the system's restart.

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

Note: When the node that is restarted is acting as Master the other node might take over the Master function.

- **Restart from backup** button

This button is used to reboot the system and use the software stored in backup partition of the current partition. If the backup partition is not available (code was removed or overwritten), this button is disabled.

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

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

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

- **File system repair** button

This button calls the check and repair tool for all Branch disks. All problems found are automatically fixed.

Note: This option is only available if the USB stick is plugged and the system is booting from the USB stick.

- **Code partitions** field

The available code partitions are listed in a table with buttons to control them.

The State column will inform the states:

- Blocked – the partition cannot be used by an upgrade process.
- Ready – the partition is available for an upgrade and has a valid software.
- Empty - the partition is avail but has no valid software.

The Status column will inform the status:

- Next-boot – the partition that runs in case of restart.
- Running – Is the partition currently being executed.
- Backup – this is the backup partition of the running partition.
- New – this partition is changed by an upgrade (it will keep this status until it is validated, checked against problems).

The buttons **Block / Unblock** and **Unblock all** are used to block the partitions against upgrades. It does not block the partition that is selected to run. Using the buttons **Restart from X**, all valid partitions can be selected to run.

Read more about the behavior of partitions in Partitioning under How to Install / Upgrade a file.

- **Activation / Restart information** field

This area shows if a reboot process is running. If the process has not been completed yet, it is possible to cancel it using the buttons **Activation / Restart** cancel and **Schedule Cancel**.

Note: This information is also available on the install / upgrade tab.

It is also possible to request the system to wait for running calls before reboot to a partition. The use of the option to wait calls also rejects new calls. If the calls rejected by this process cannot be diverted to other servers, they get lost.

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.

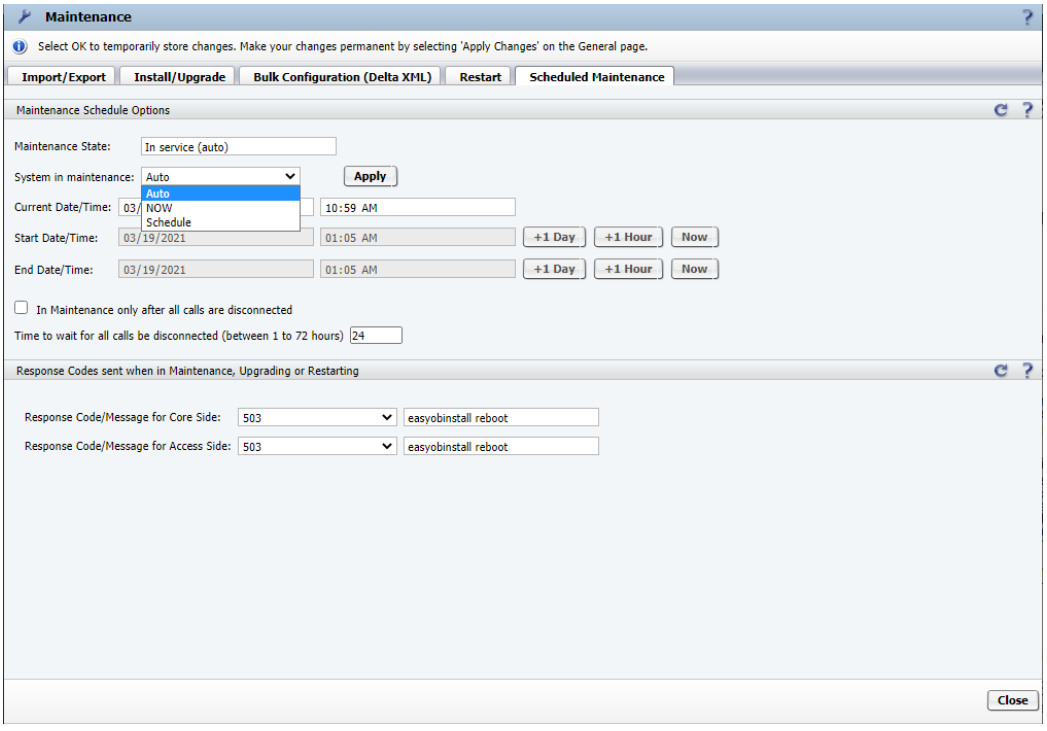
Note: The server can enter in maintenance state even before the date and time defined if the server thinks that is the right decision.

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.



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.

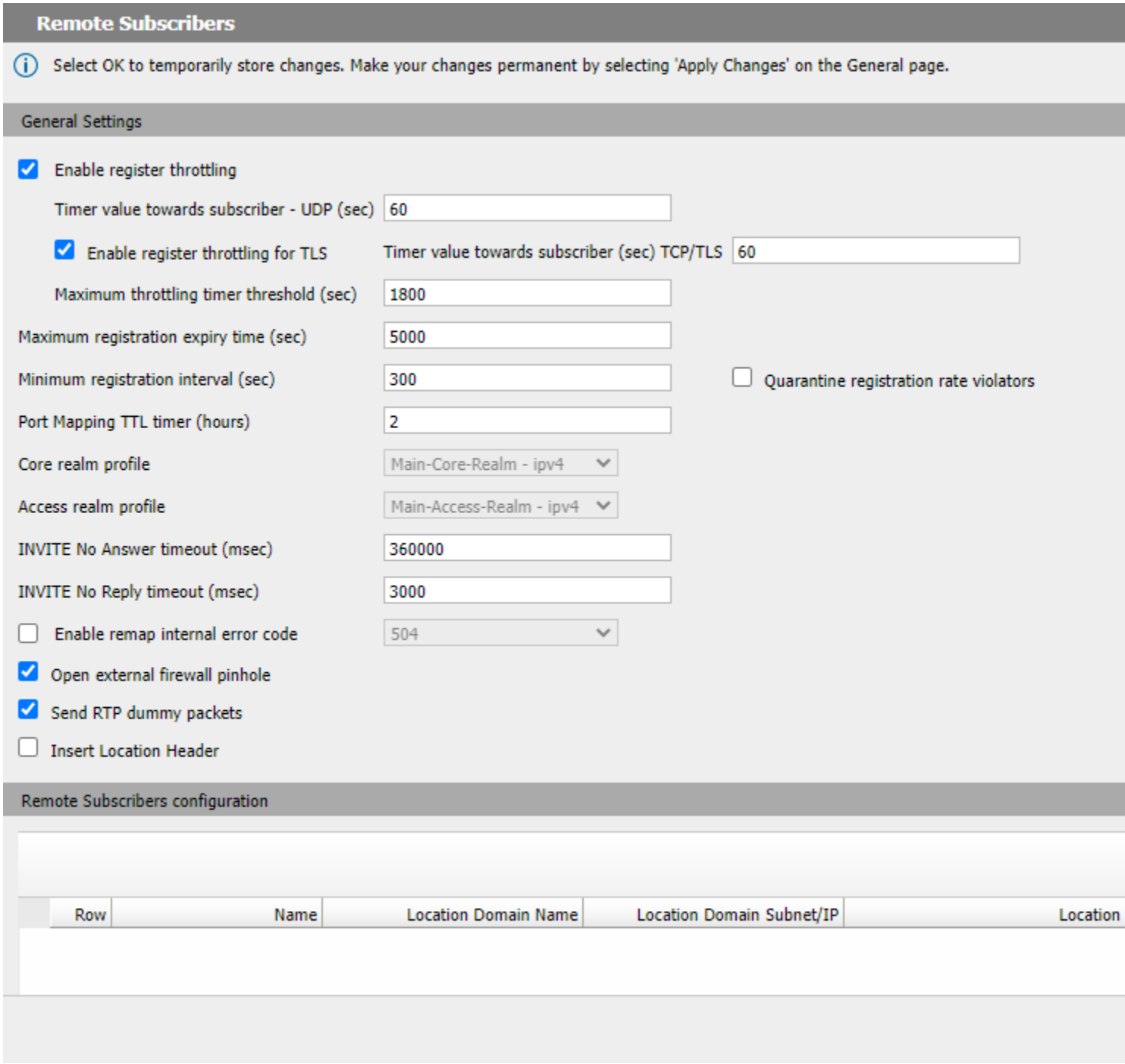
NOTE: This feature only applies for the addresses and ports used for the media streaming. It is not applicable to the SIP or MGCP protocols.

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**

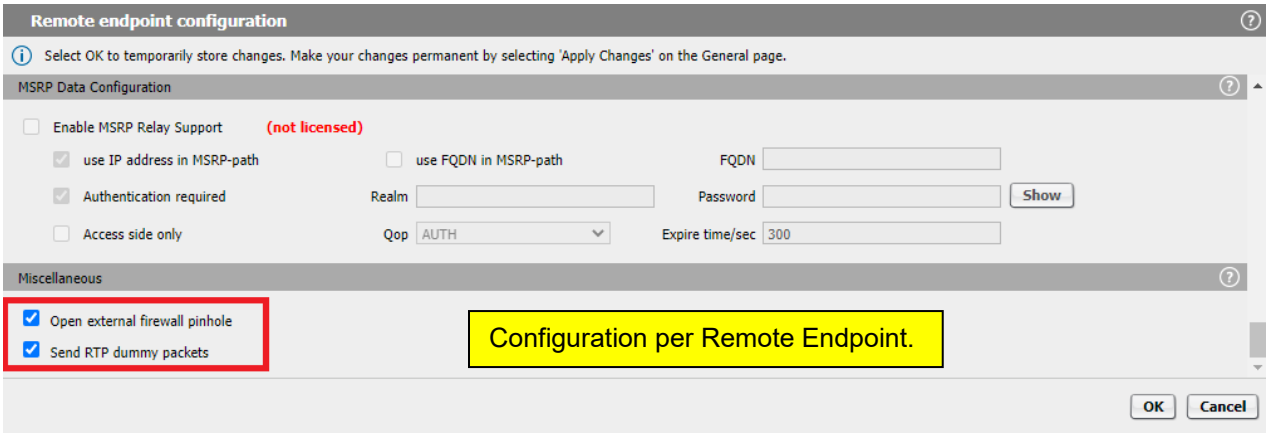
This feature can be configured/enabled under:

Remote Subscribers (Administration → Features → Enable Remote Subscribers → Configure)



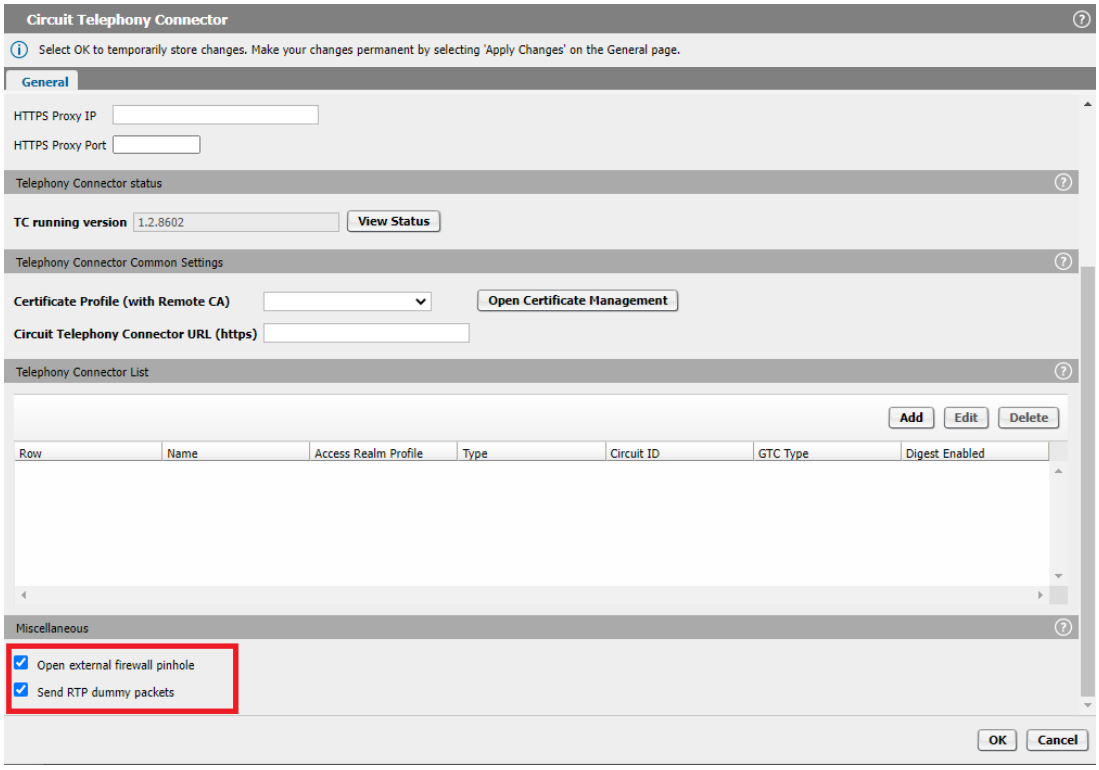
Remote Endpoint

Administration→ Features→ Enable Remote Endpoints→ Configure→ Remote Endpoint Configuration→ Miscellaneous

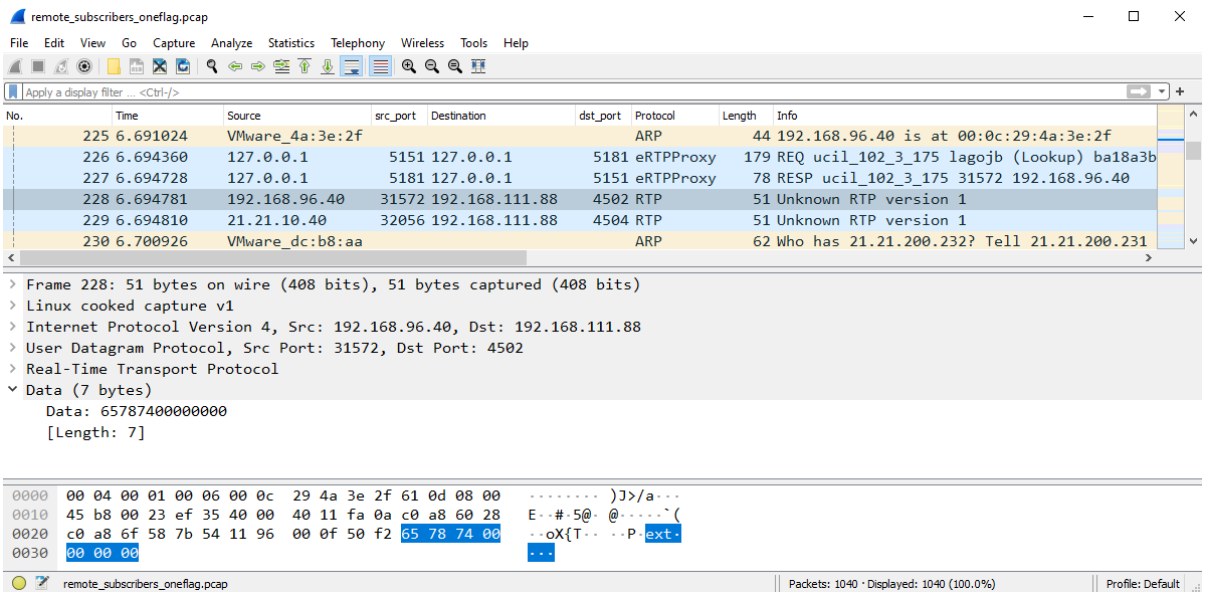


Telephony Connector

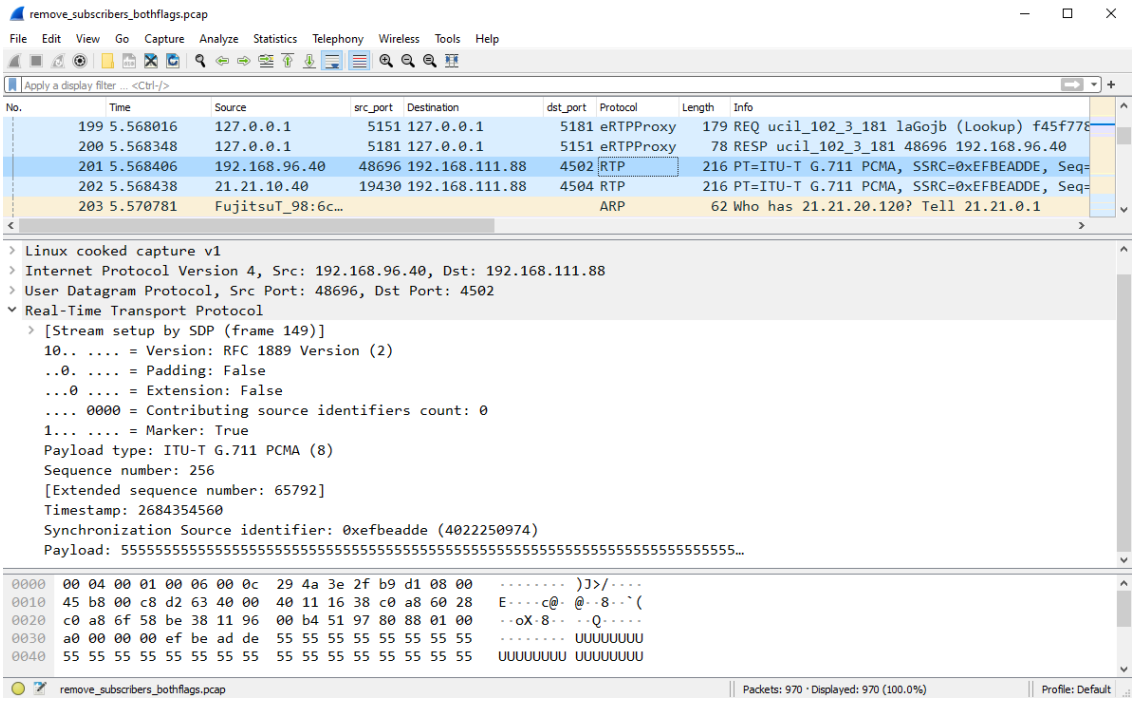
Administration → Features → Enable Circuit Telephony Connector → Configure → Miscellaneous



Example of UDP packet (pinhole) that is sent when only **Open external firewall pinhole** is enabled:



Example of RTP packet (pinhole) that is sent when **Send RTP dummy packets** is enabled:



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 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.

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 whilethe LAN interface is used for subscribers and gateways

On the Branch Phones
The checkmark for Outbound Proxy should beset.
The SIP server address should be the WAN address of the OS-SBC. The SIP registrar address should be the WAN address of theOS-SBC.
The SIP gateway address should be the LAN address of the OpenScape Branch. (not the LAN gatewayIP)

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 theOS-SBC.

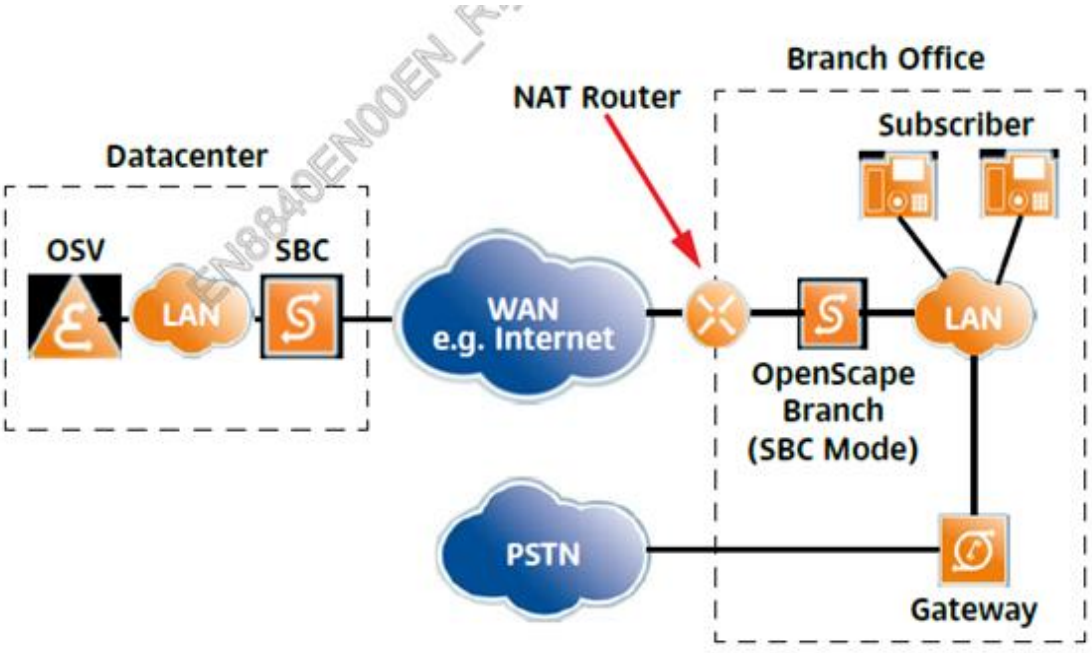
Note 8:
This is the address of the address of the branch not the address of the NAT
Local GUI→VOIP→ "Enable Remote Endpoints" →click on "Remote Endpoints configuration". Under "Remote Endpoints Configuration" click Add.
Under "Remote Endpoint Settings" enter the Name, Type and Profile.
Under "Remote 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 OpenScape Branch

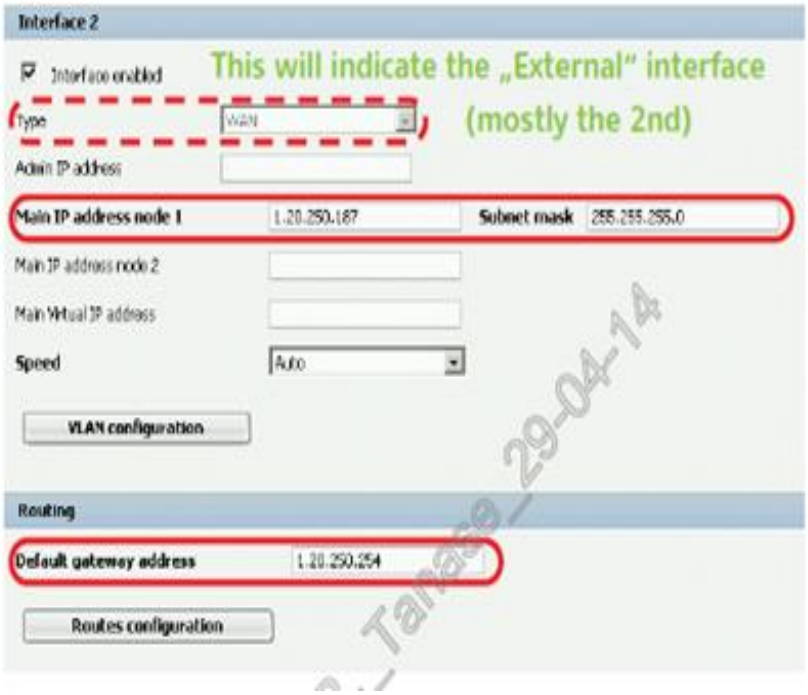
Local GUI->VOIP-> Node 1 primary server-> set the address, transport and port of the WAN interface of theOS-SBC. https://www.g-dms.com/livelink/llisapi.dll/view/inf-13-000221

Add in Bold provisioning of Branch Office behind NAT and with Gateways.

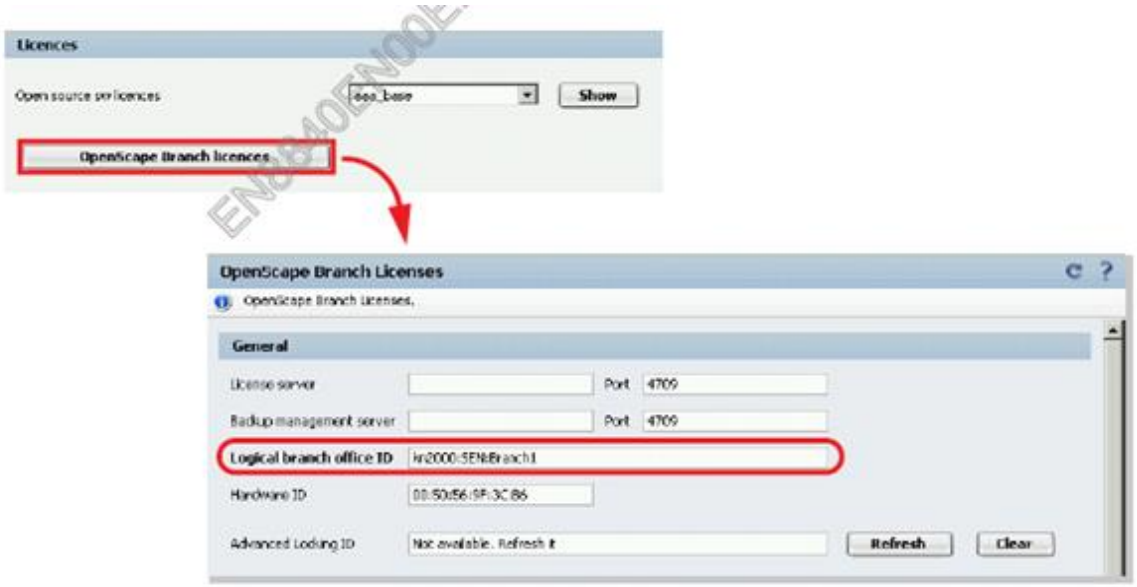
The following diagram provides an overview of the scenario which will be configured on the following pages :



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:



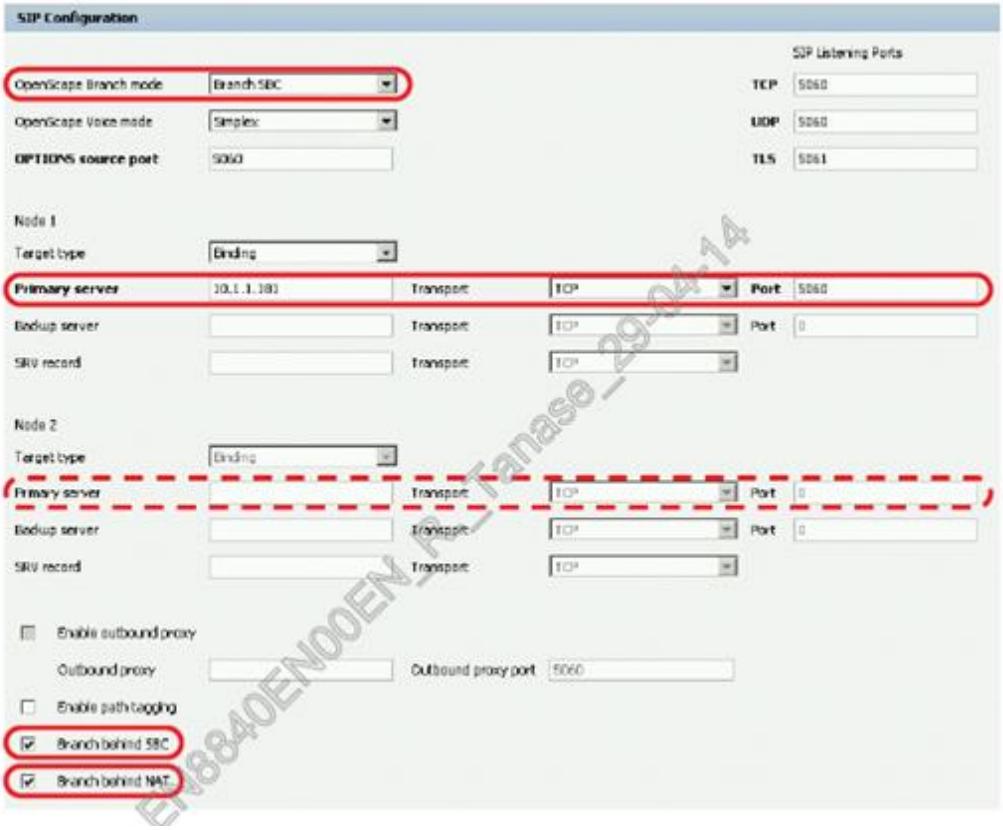
Next,under the **Licenses** tab of the **System** menu,verify that the Logical branch office ID is configured:



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 OpenScape SBC's WAN IP or FQDN must be configured:

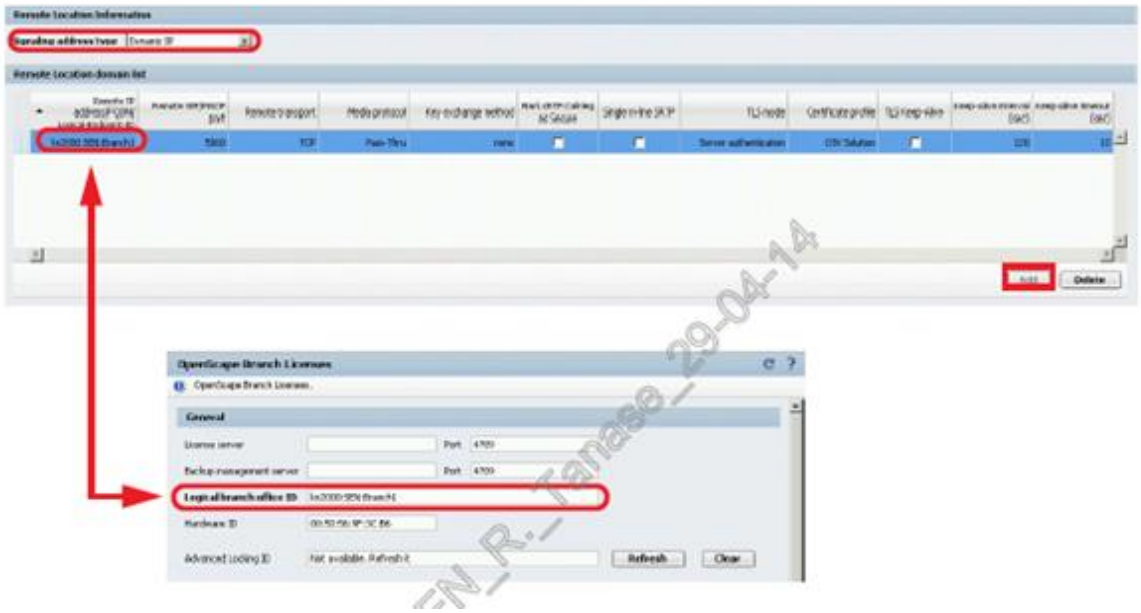


Click on **Apply Changes** to activate the new configuration.
Now,on the SBC,the OpenScape Branch device must be configured under **Remote Endpoints**

configuration.Click on **Add** under **Remote Endpoints configuration** in order to create a new endpoint mapping entry:

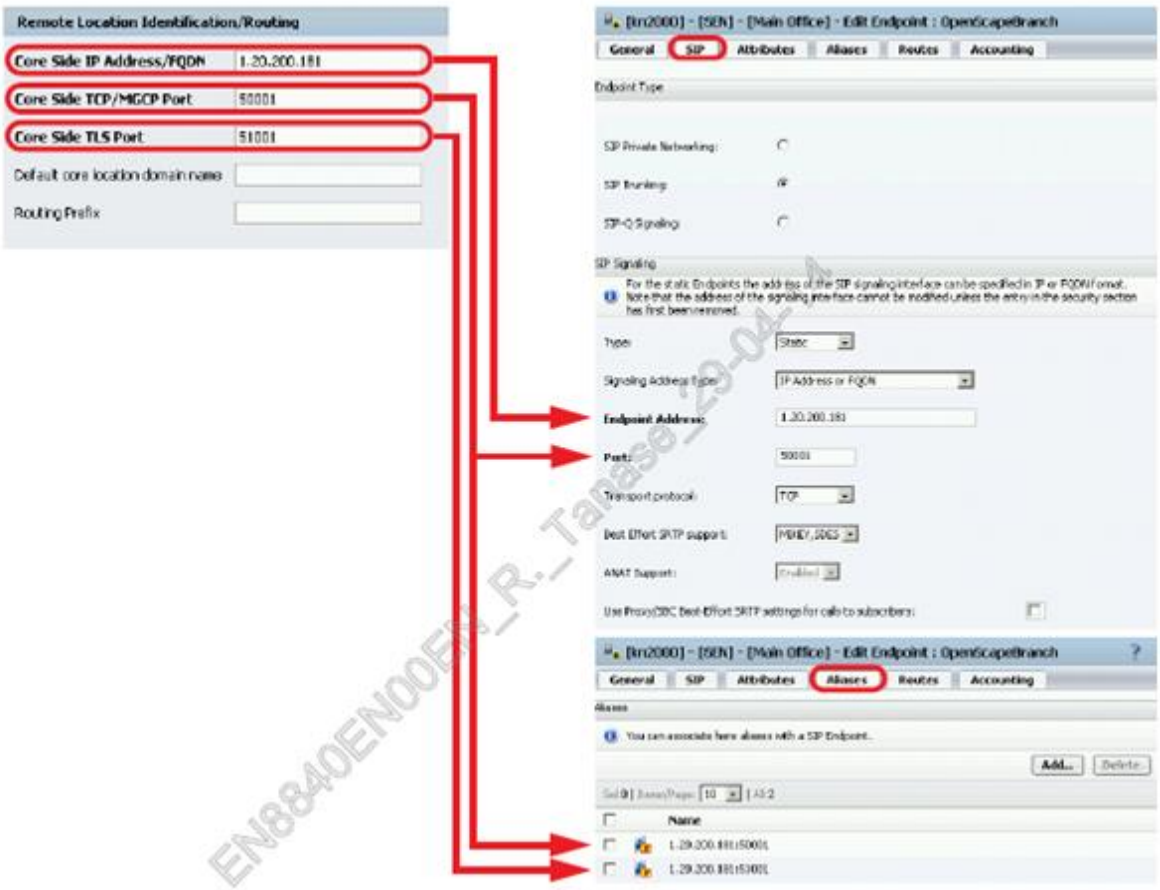
Enter a name for the entry and select the new type **Branch SBC** (this will automatically select the profile **Default SBC**).Optionally, select the VLAN under which the OSB can be reached:

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:

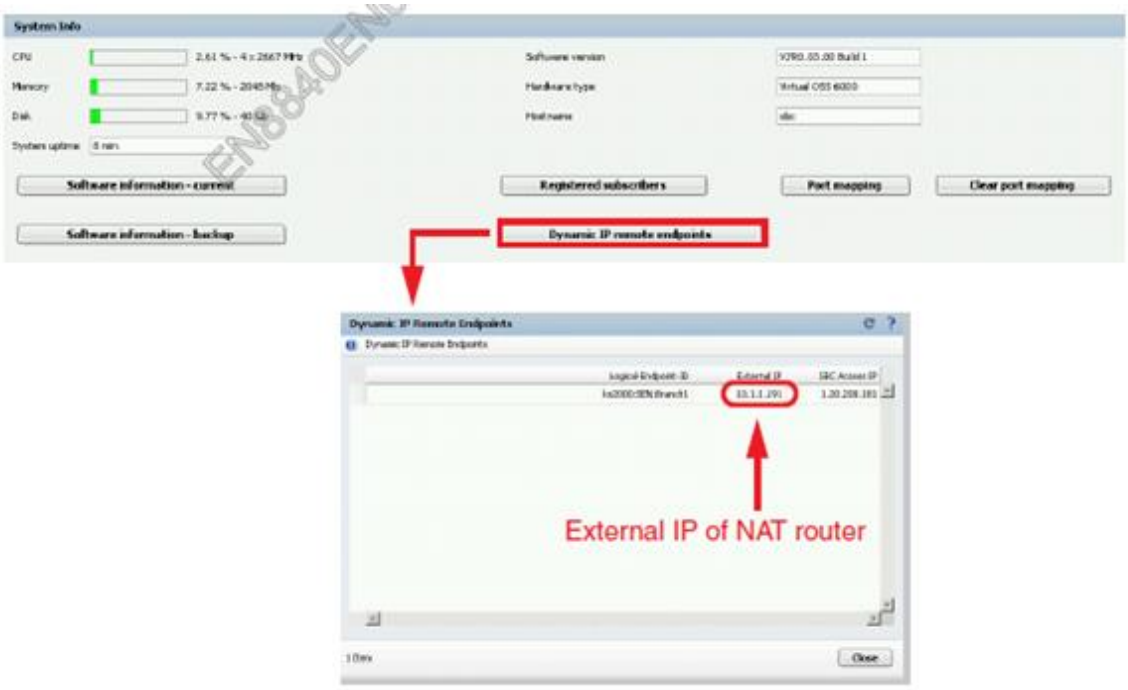


Save all configurations and click on **Apply Changes** to activate the new configuration.The OSB should switch to **Normal Mode** shortly:

The SBC can reach the branch office, the OSB will send a SIP OPTIONS message with it's 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=z9hG4bKe8ce3f2c
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=403737563
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/llisapi.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.

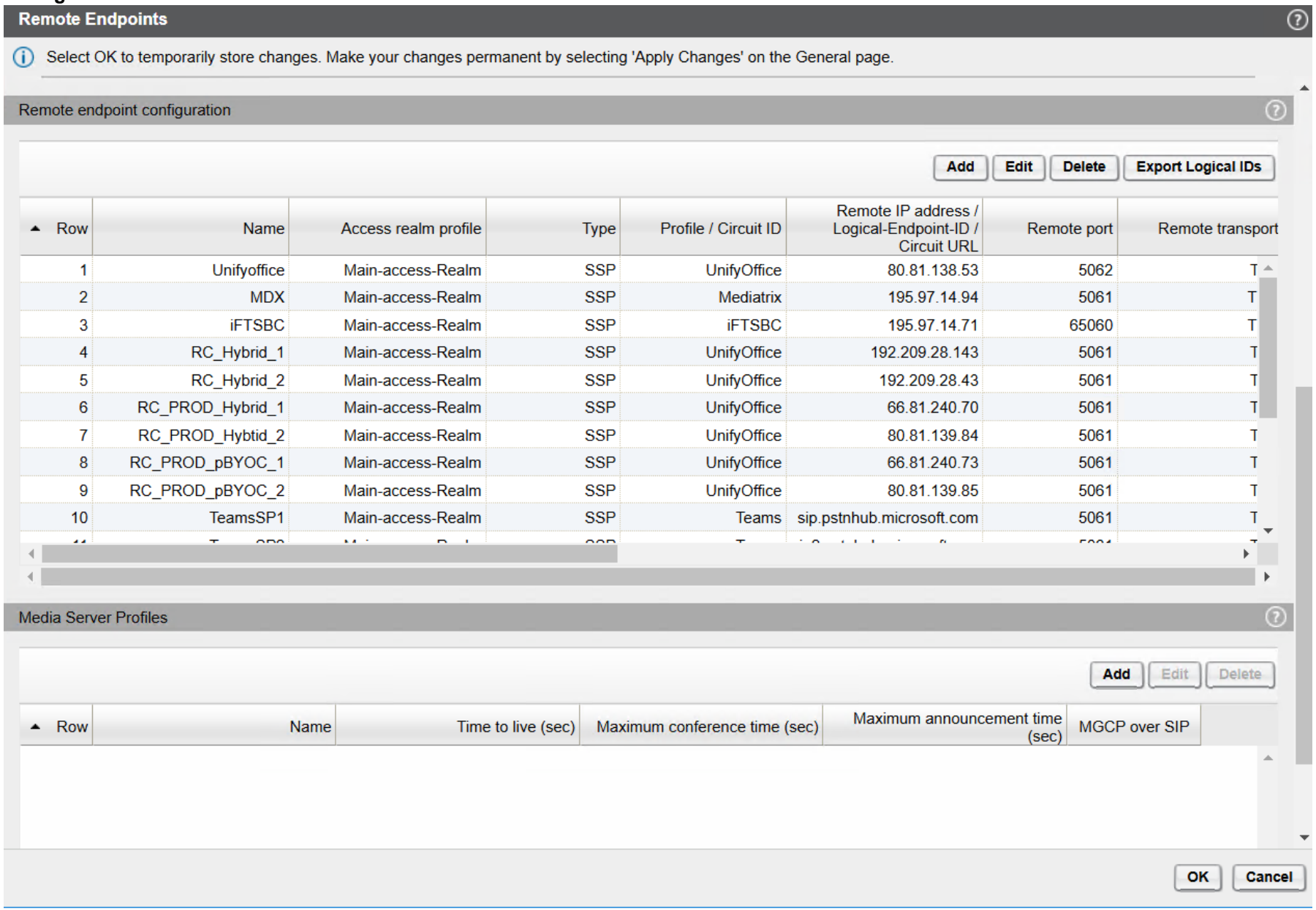
Dynamic IP remote endpoints on the OS-SBC
Local GUI-> Maintenance & Diagnostics-> Port Mapping.
This should show the current relationship between the "Logical-endpoint-ID" and the current IP address of the NAT.

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*

The remote endpoints can be configured using Local GUI or CMP under **Features → Enable Remote Endpoints → Remote Endpoints Configuration**.



To add a new remote endpoint, click **Add**.
Under Remote Endpoint Settings:

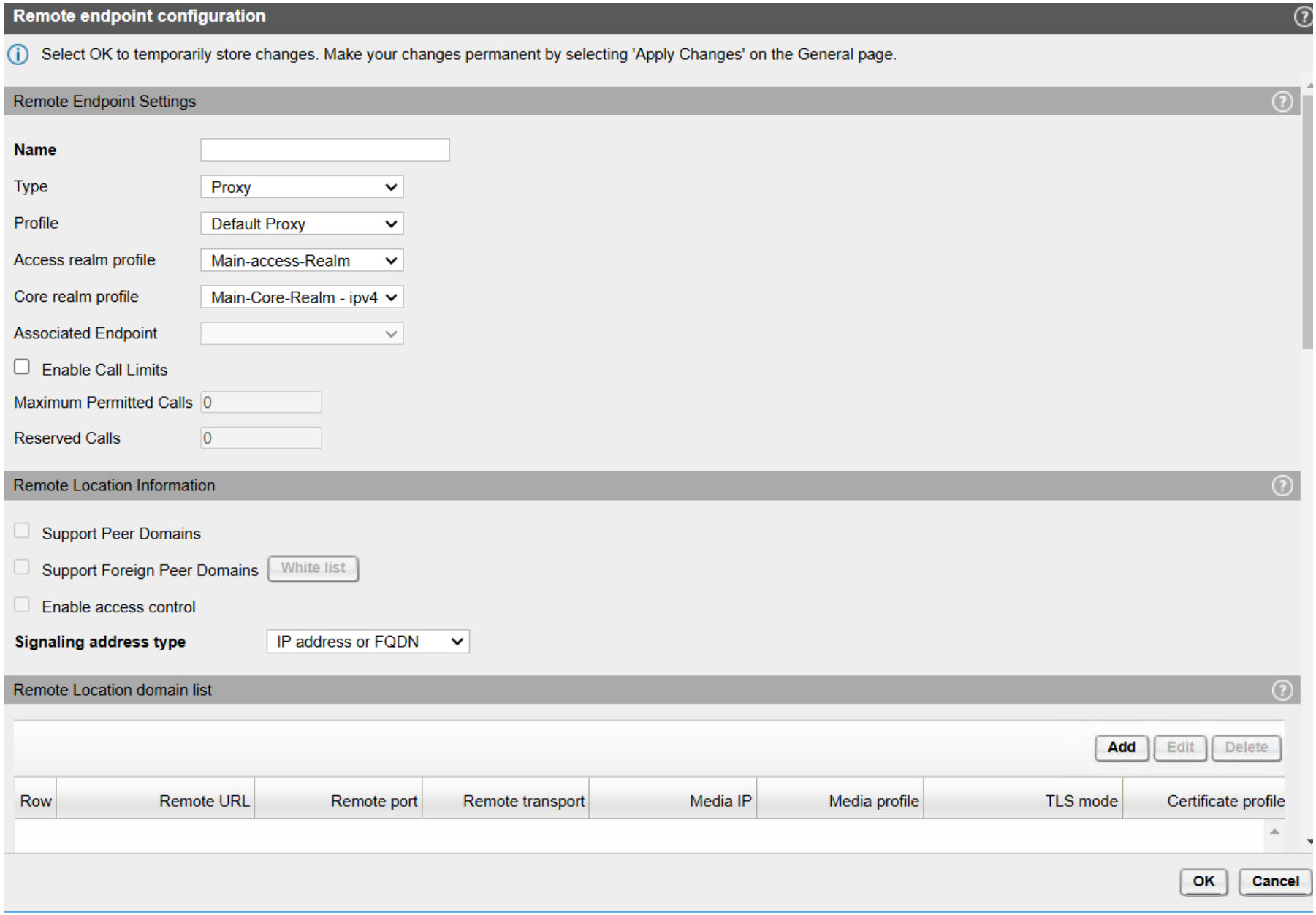
- Enter the **Name**
- **Type**: This box defines the remote endpoint type.
  Available options: **Gateway,Proxy, Branch SBC, Media Server, SSP,SBC, OSBIZ**.

- **Profile** – Select 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 the **Remote Location domain list** area**,** 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 Endpoints* for details.
Under **Remote Location Identification/Routing** enter the core Realm port. This is not required if the OS SBC's default IP address is to be used.

To edit or delete a remote endpoint, click **Edit** to modify it or **Delete** to remove it. To export the logical IDs along with the hashes in a csv format, click **Export Logical IDs.**


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
Proxy
Profile
Default Proxy
Access realm profile
Main-access-Realm
Core realm profile
Main-Core-Realm - ipv4
Associated Endpoint
Enable Call Limits
Maximum Permitted Calls
0
Reserved Calls
0
Remote Location Information
Support Peer Domains
Support Foreign Peer Domains
White list
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
OK
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 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, 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 toconnect to the OSS whilethe 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.g-dms.com/livelink/llisapi.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.

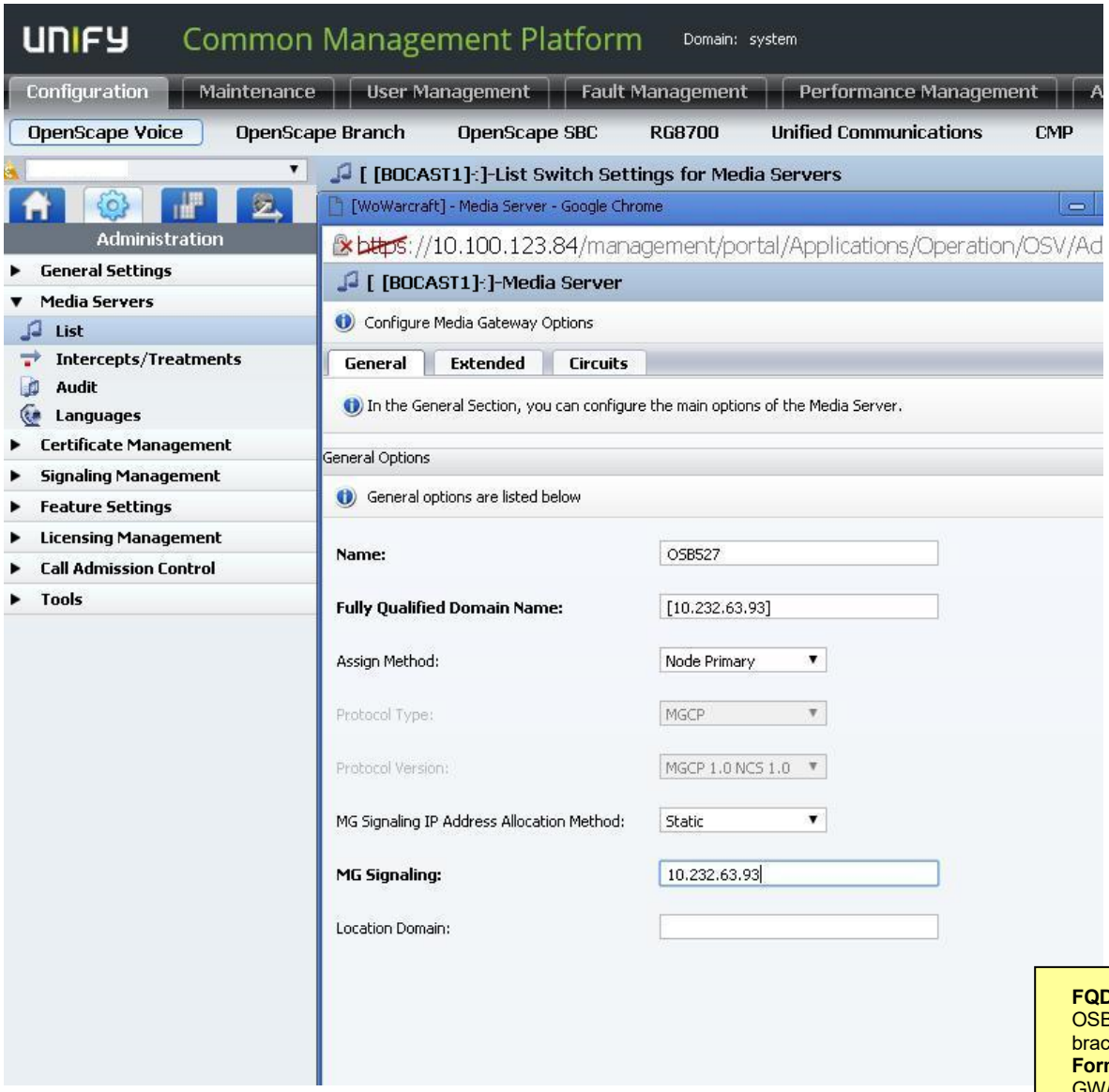
3.5.13.1 Configuring OSB as main Media Server in OSV

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**”.

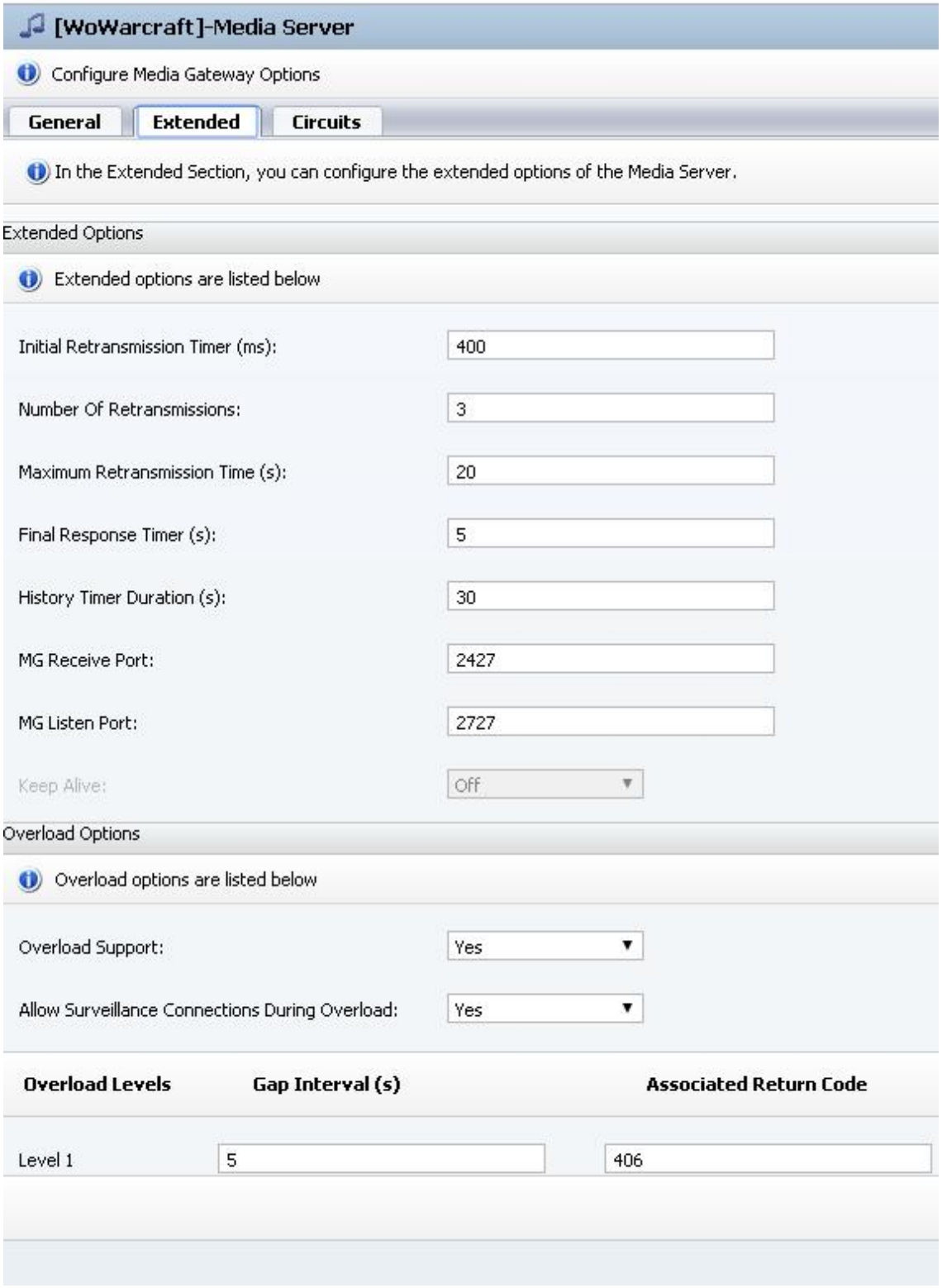
It is possible to have OpenScape Branch as the Main Media Server for the OSV. These steps also assume a distributed deployment where an OpenScape Branch provides MS service at the main location.

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.

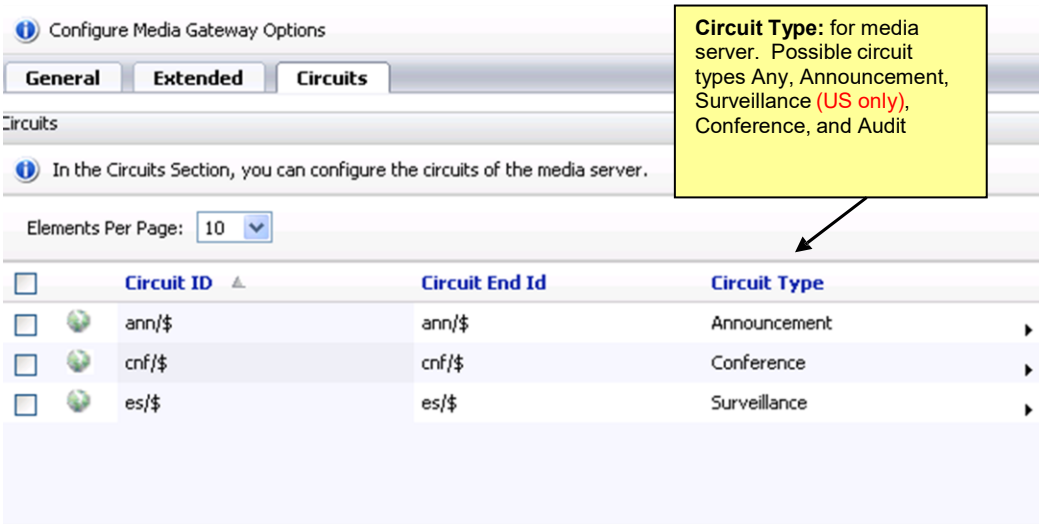
1. Under **Configuration > OpenScape Voice > Administration > Media Servers**, select **List** and Press **Add**:



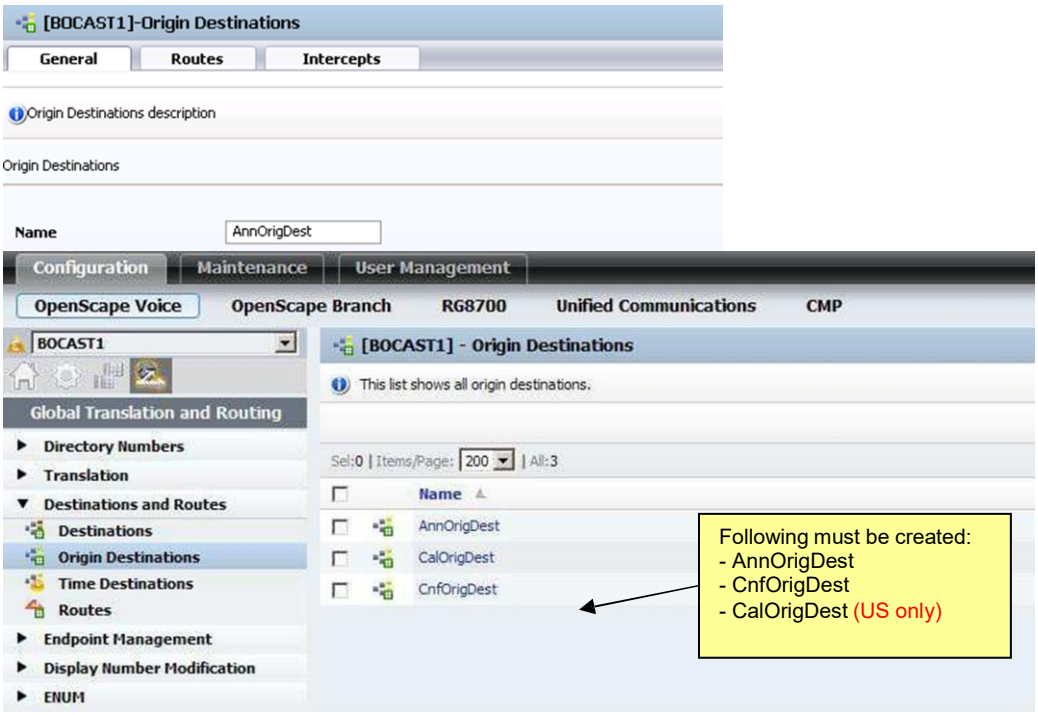
FQDN: IP address for OSB. Please note the brackets "[]" **Circuit Format:** ID for the GW/Server. $ serves as Wildcard. Media Server will select free Endpoints as needed.
MG Signaling: IP address for OSB


[WoWarcraft]-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):
400
Number Of Retransmissions:
3
Maximum Retransmission Time (s):
20
Final Response Timer (s):
5
History Timer Duration (s):
30
MG Receive Port:
2427
MG Listen Port:
2727
Keep Alive:
Off
Overload Options
Overload options are listed below
Overload Support:
Yes
Allow Surveillance Connections During Overload:
Yes
Overload Levels
Gap Interval (s)
Associated Return Code
Level 1
5
406

2. Depending on the traffic type being served the corresponding circuits must be created.

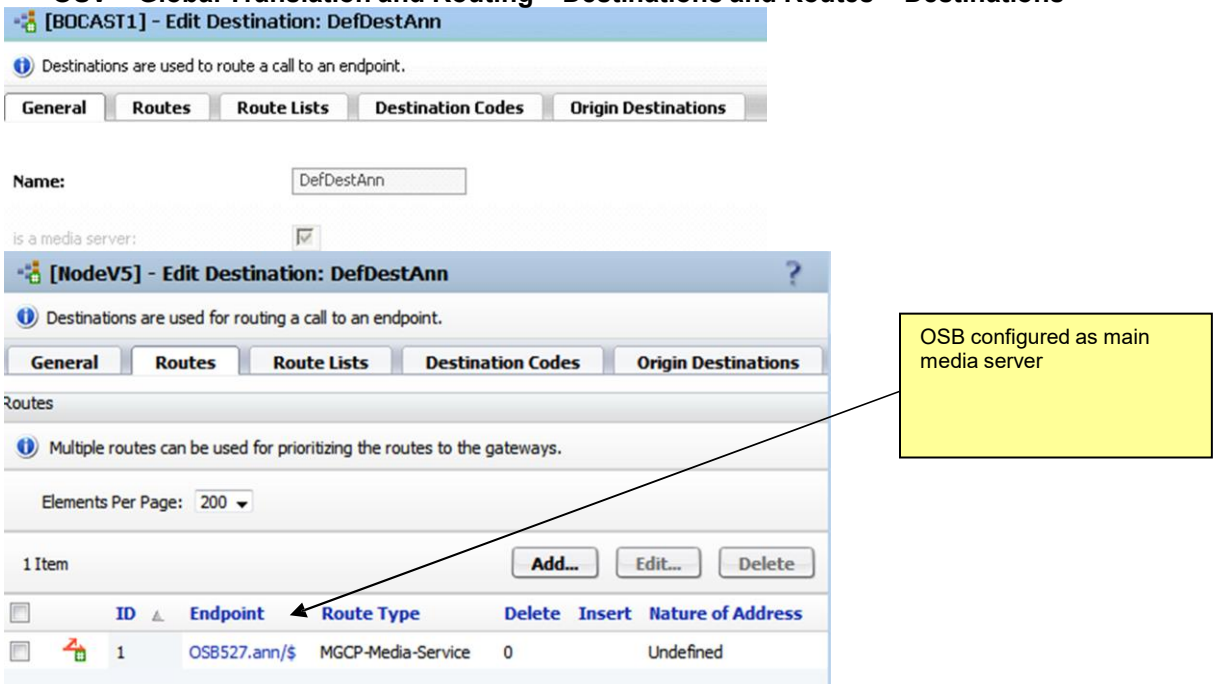


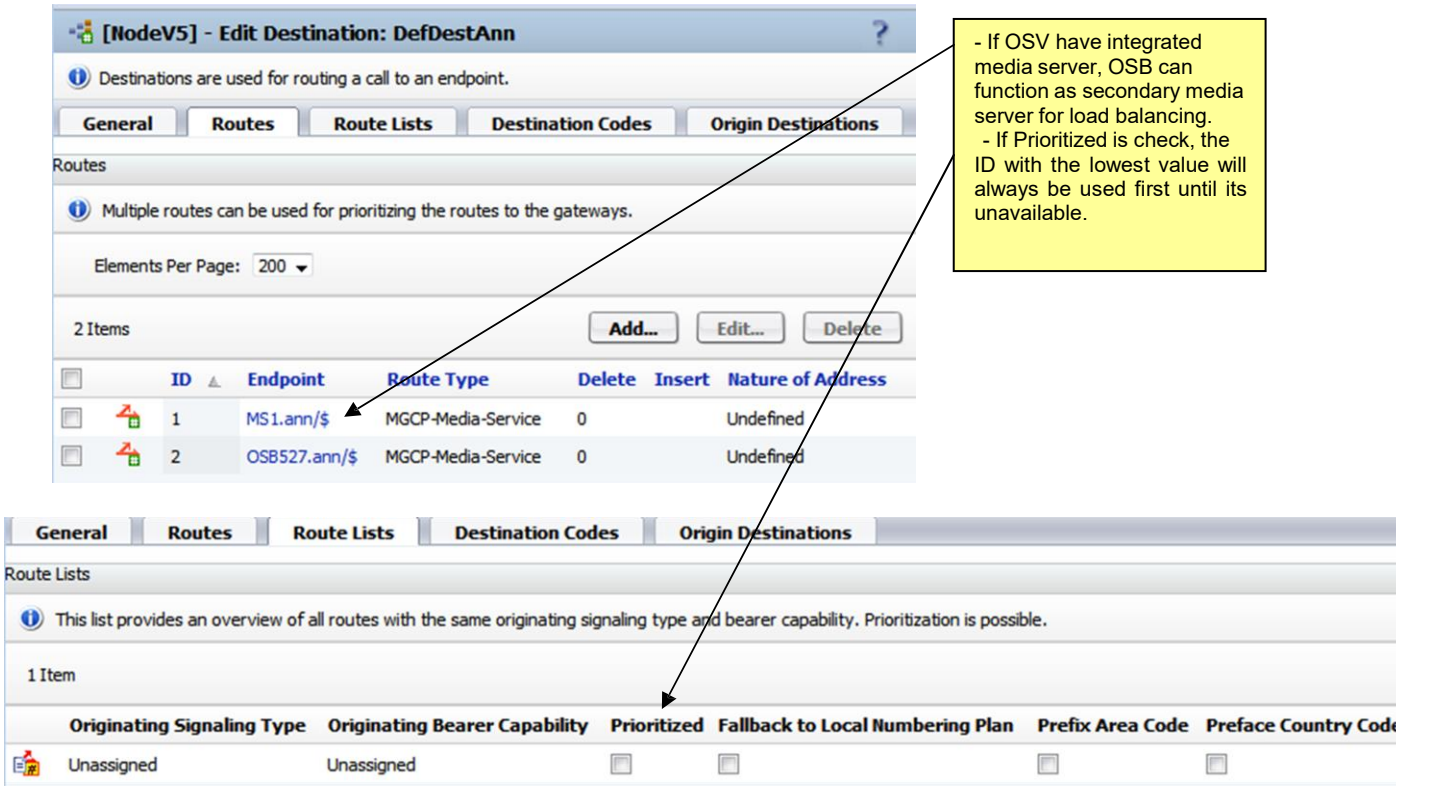
3. Create an **Origin** Destination for each traffic type: Announcements, Conference and Electronic Surveillance. OSV -> Global Translation and Routing -> Destinations and Routes -> Origin Destinations.



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

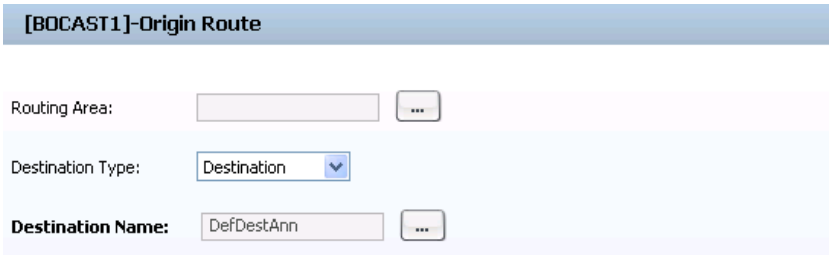


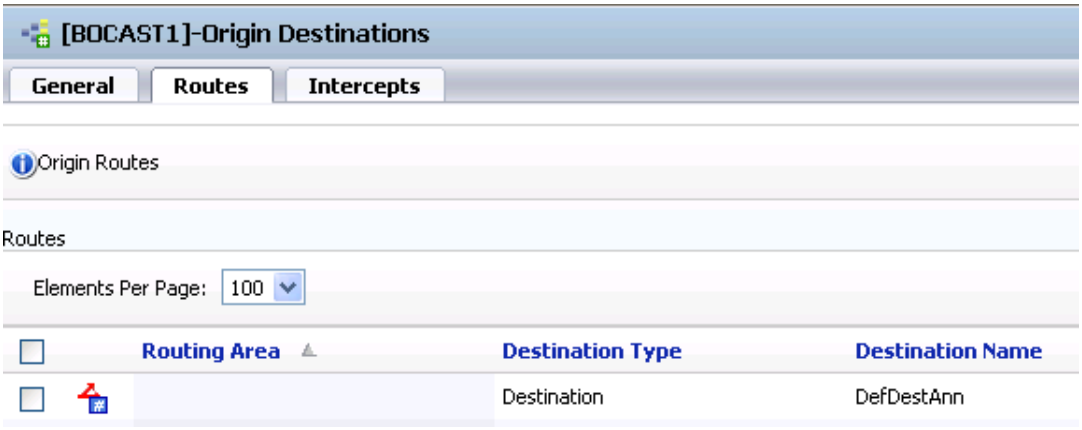


5. Do the same for default destination for conference and surveillance (DefDestCnf and DefDestCal).

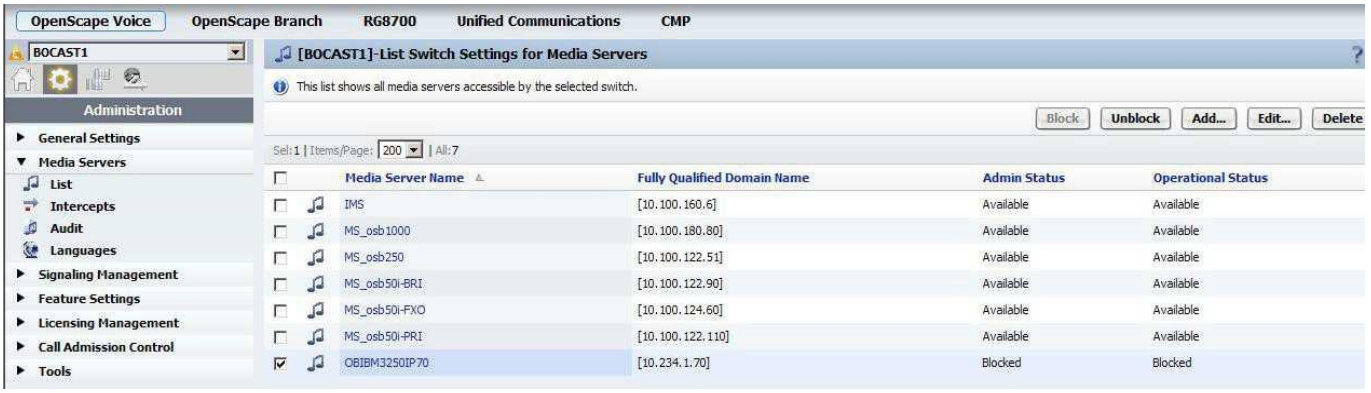
6. Add the **Default** Destination to the **Origin** Destinations as a Route
   OSV -> Global Translation and Routing -> Destinations and Routes -> Origin Destinations -> Edit and go to the Routes Tab and press Add

   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.





7. Unblock the Media server



Announcements for the Main Office (default) are now provided by OpenScapeBranch.

8. Provision the treatments. OSV provides media server script to add the treatments for the Media Server. NOTE: The following instructions may change depending on the OpenScape Voice patch set level. For updated script information refer to the OSV Media Server Configuration Instructions or OSV "***OpenScape Voice V5, Configuration, Administrator Documentation***" or "**OpenScape Voice V5, Installation and Upgrades, Installation Guide**".

   The script is located at:
   /unisphere/srx3000/srx/ms_scripts
   Execute the script in the OSV by entering the following command(run as user "srx"):
   sh msconf.sh
   Select the following options:
   - 11 to Assign the default treatments
   - 3 to select Distributed Media Server Deployment
   - Press "Enter" to assign treatments to the default Origin Destinations created or type the Origin Destination name(e.g. AnnOrigDest) and press "Enter", for value different than Default, type the name and press "Enter"
   - Press "y" to backup the current configuration of the treatments
   - Press "y" to effect the selected modifications
   Note: add the PAC codes in the respective numbering plan. The script provided with the system does not add PAC codes for you.

9. 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:

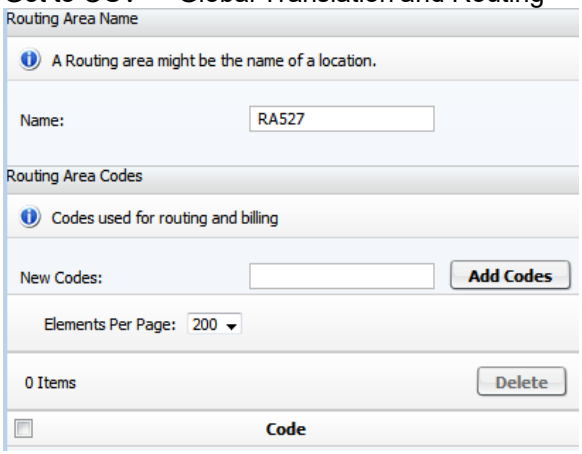
These steps are a continuation from the previous section.

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**".

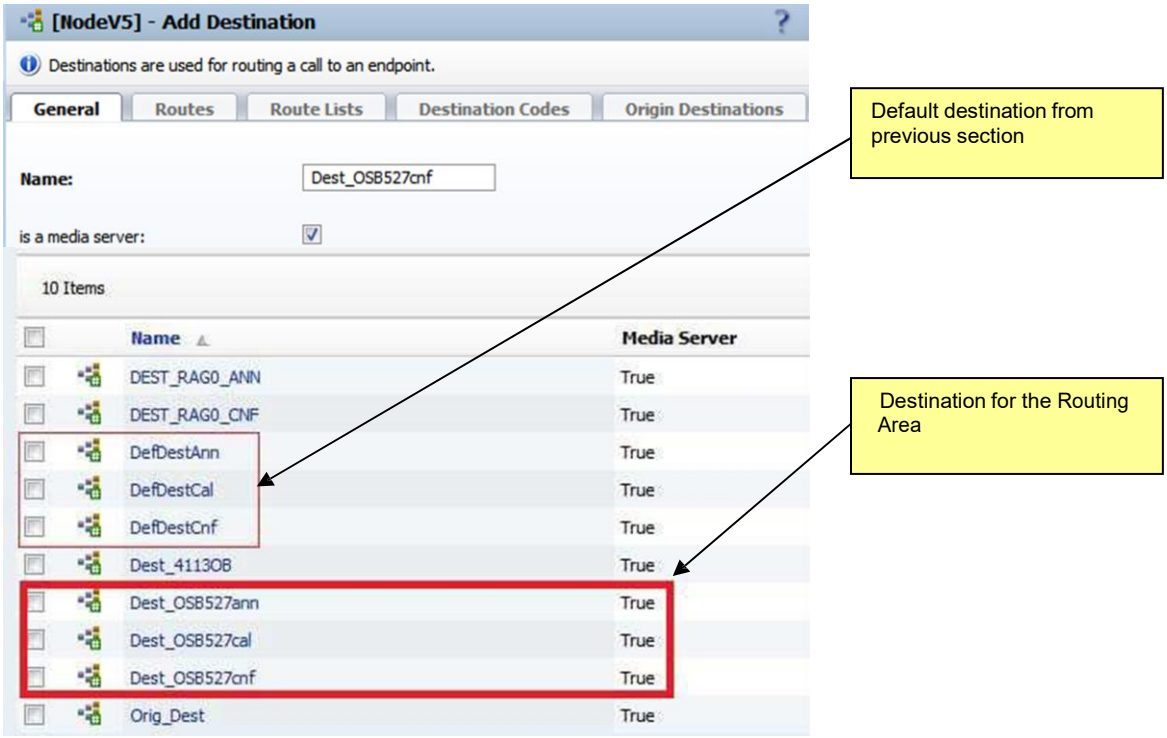
The following steps will show how to configure an OpenScape Branch server as the Media Server for a Branch.

1. Add and Configure OpenScape Branch as a Media server following Steps from previous section.

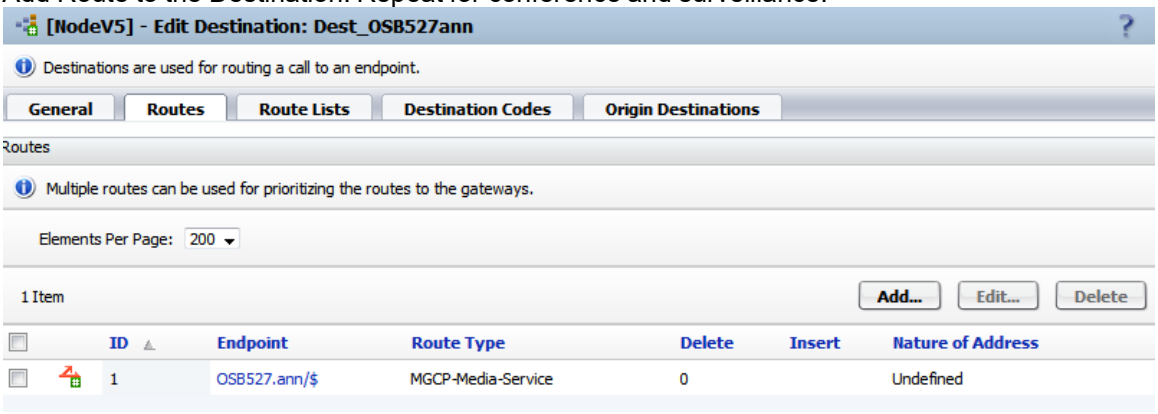
2. Create a Routing Area for the branch.
   Got to OSV -> Global Translation and Routing -> Translation



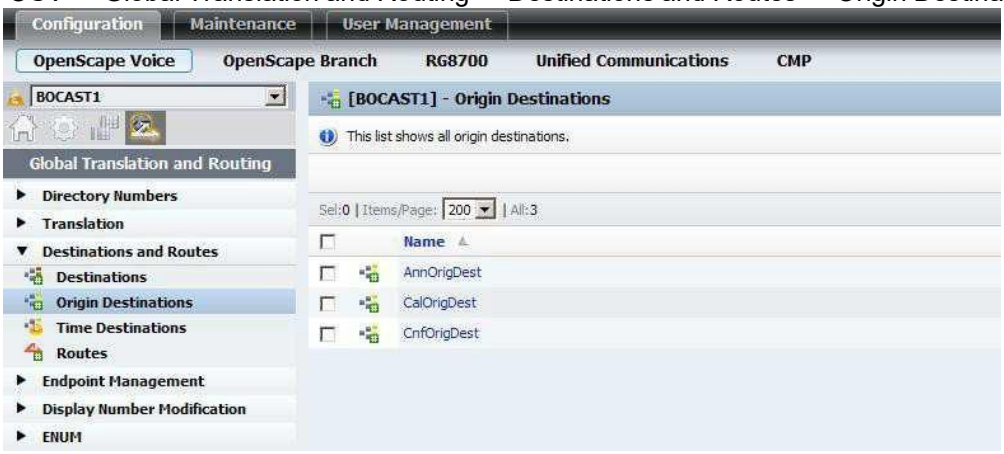
3. Destination for newly created Routing Area (announcement, conference and surveillance). Declare that it is a media server.



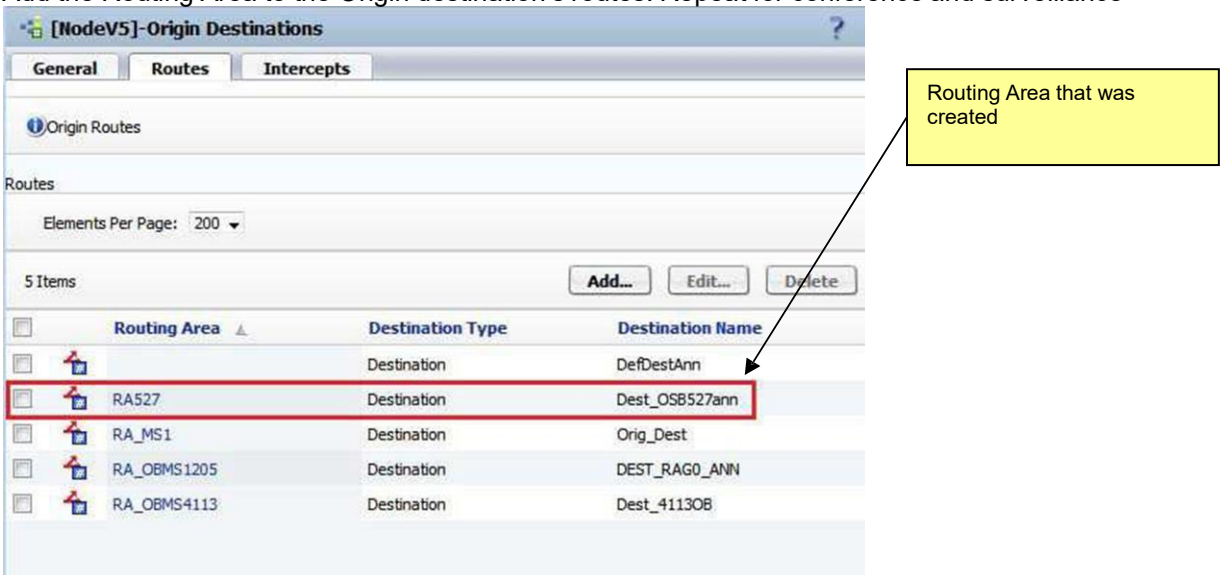
4. Add Route to the Destination. Repeat for conference and surveillance.



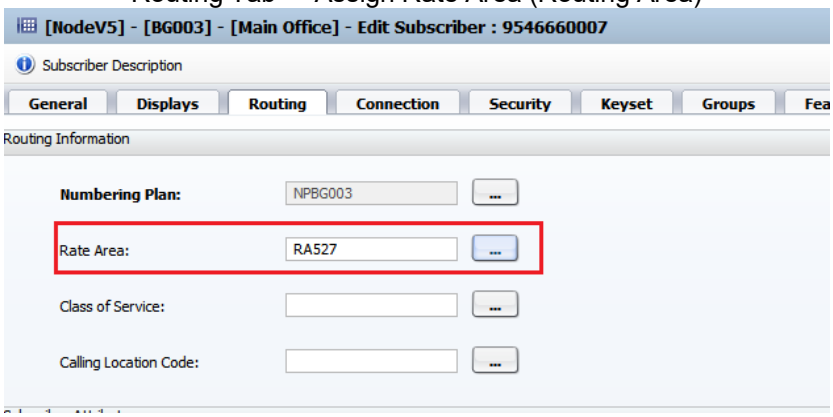
5. Origin Destinations for each traffic type must have been created for the main Media Server (See previous section).
OSV -> Global Translation and Routing -> Destinations and Routes -> Origin Destinations.



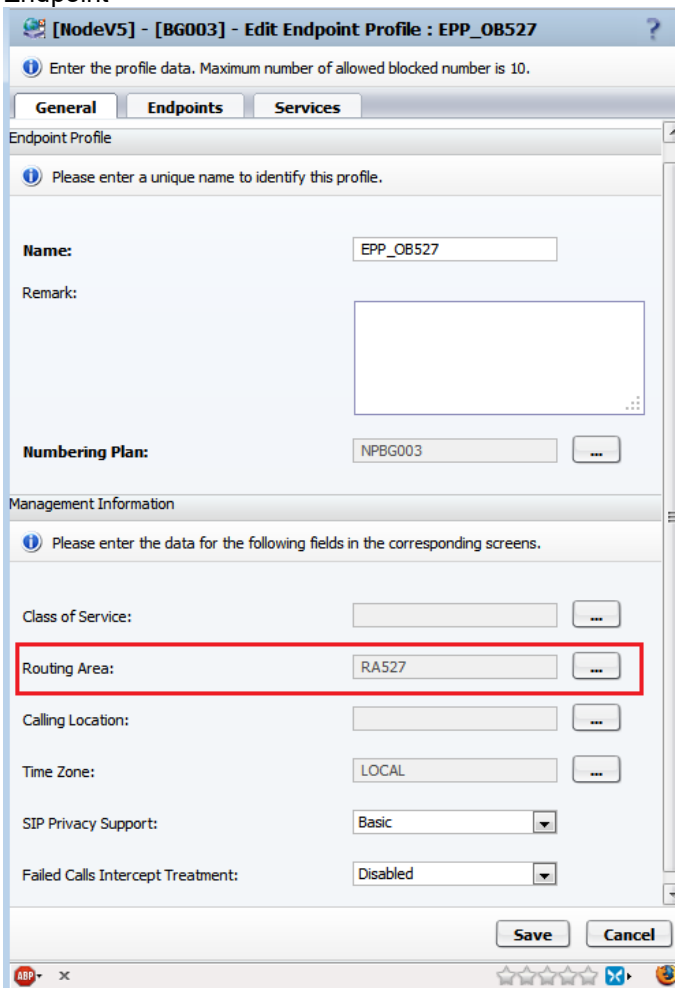
6. Add the Routing Area to the Origin destination's routes. Repeat for conference and surveillance



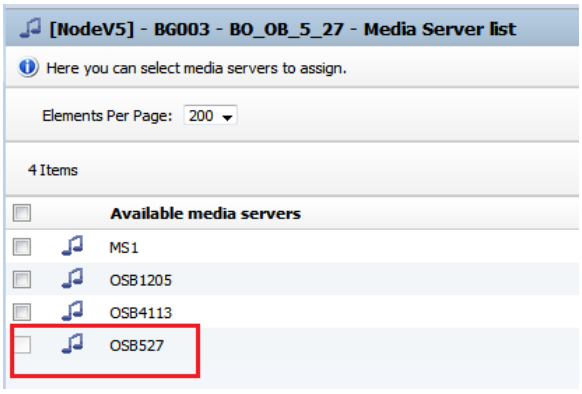
7. There are two ways to assign the OSB media server as a media server for a subscriber. The first is to assign the RA directly to the subscriber: Openscape Voice -> Business group -> Members -> Subscribers -> edit Sub -> Routing Tab -> Assign Rate Area (Routing Area)



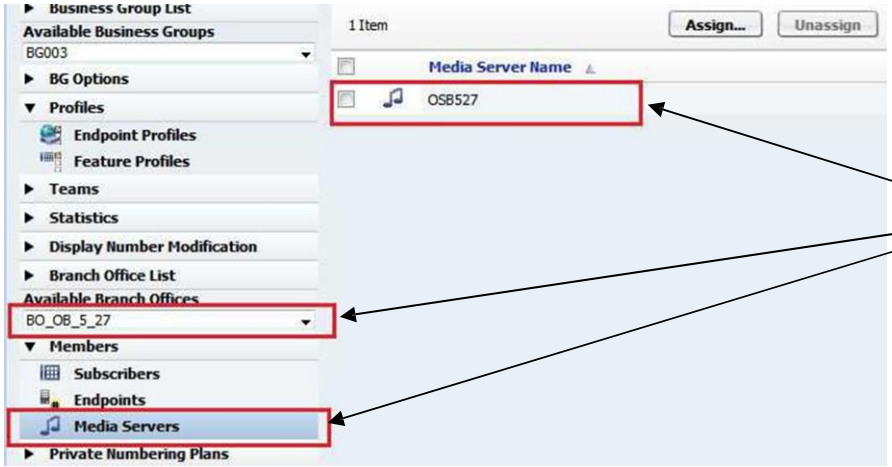
8. The second way is to assign the Rate Area for the entire Branch: Assign the newly added Routing Area to the Endpoint Profile of the Proxy serving the Branch Office. OSV -> Business Group -> BG(x) -> Profiles -> Endpoint



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)



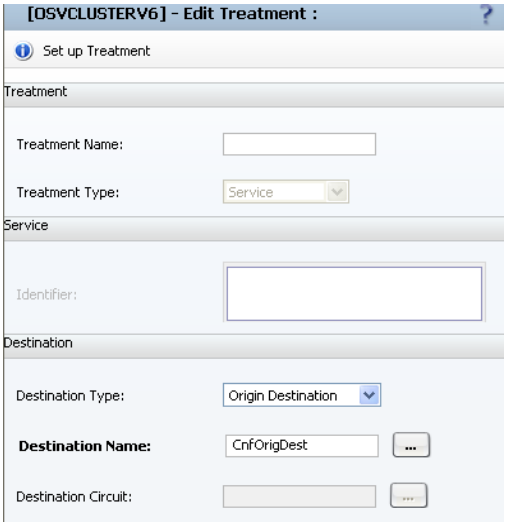
OpenScapeBranch is now configured to server the Branch Office as Media Server.



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)

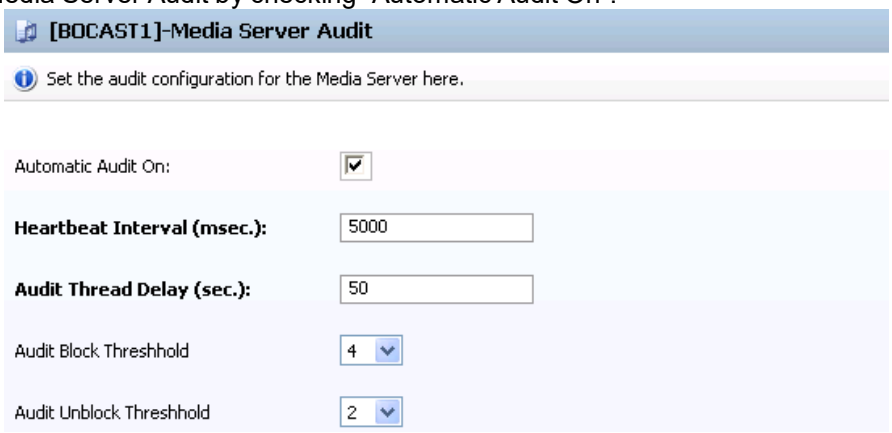
3.5.13.3 Configuring the main Media Server as a backup of the Branch MS:

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:

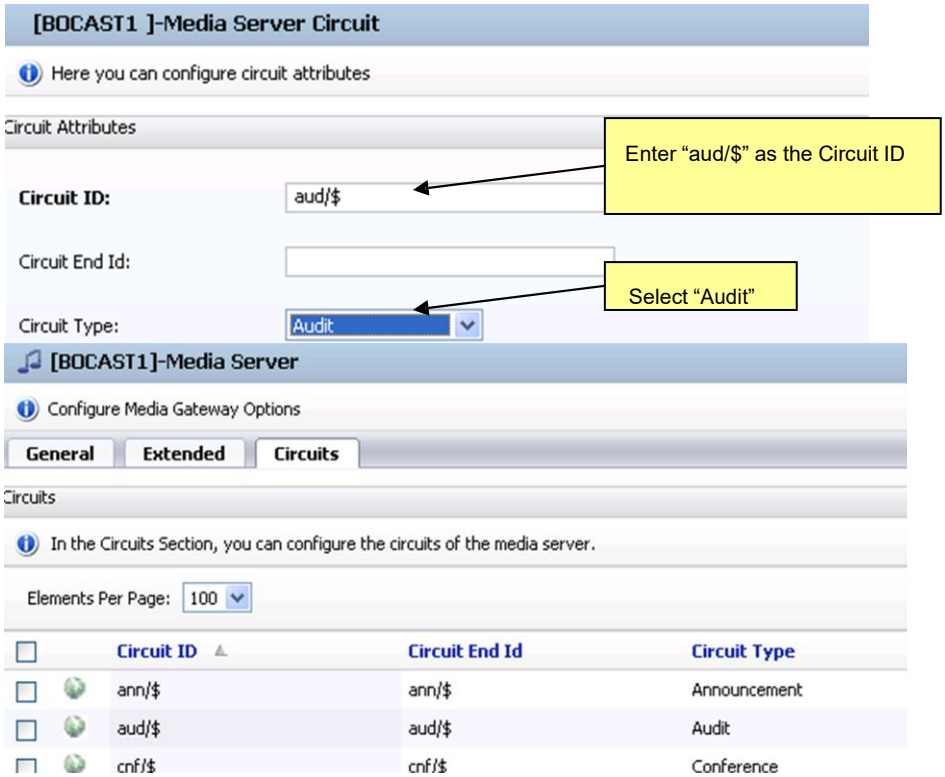
Via CMP go to **OSV -> Administration -> Media Servers > Audit**

1. Enable the Media Server Audit by checking "Automatic Audit On":



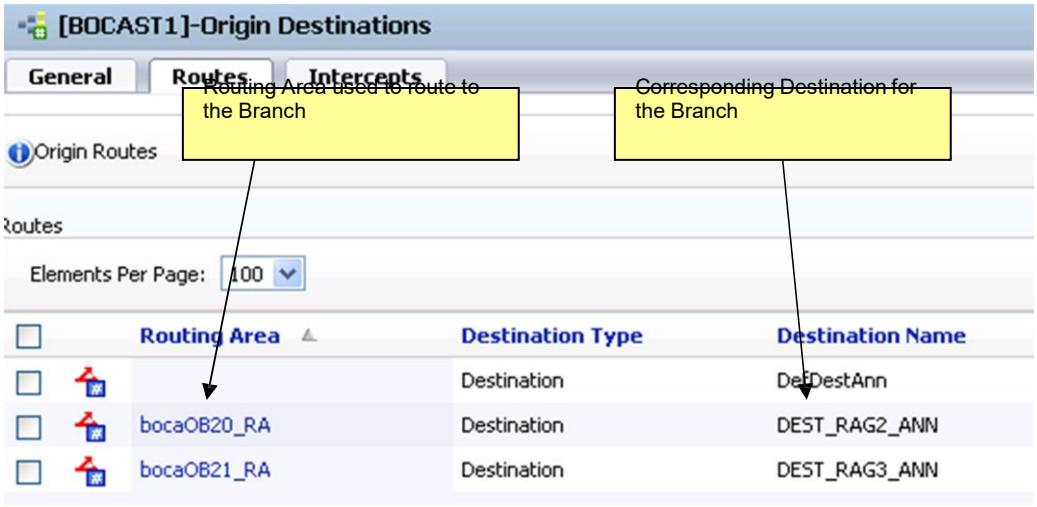
2. Create the Audit circuit in the Branch Media Server.
Go to **OSV -> Administration -> Media Servers -> List** and click on the desired Branch Media Server.

3. Go to the **Circuits** tab and add the new circuit



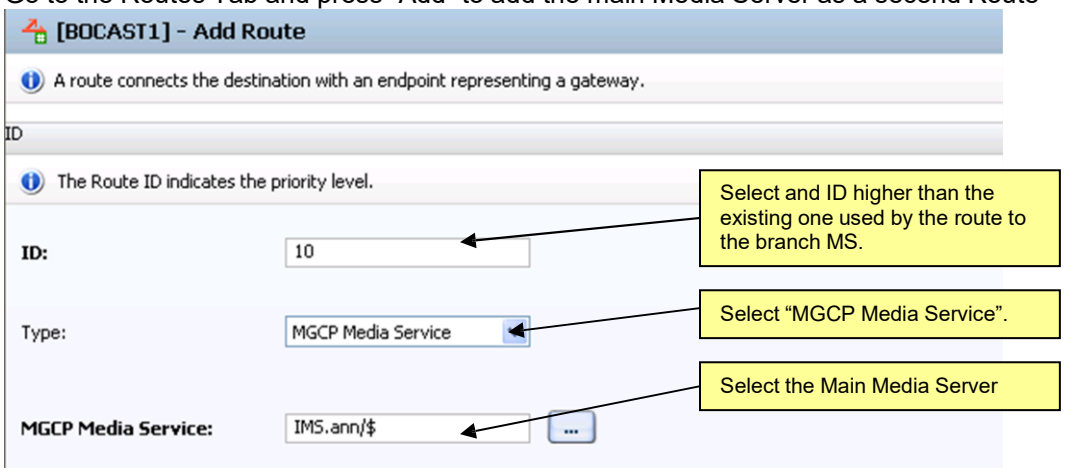
Add Main Media Server as a second Route to the Branch Media Server:

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”.

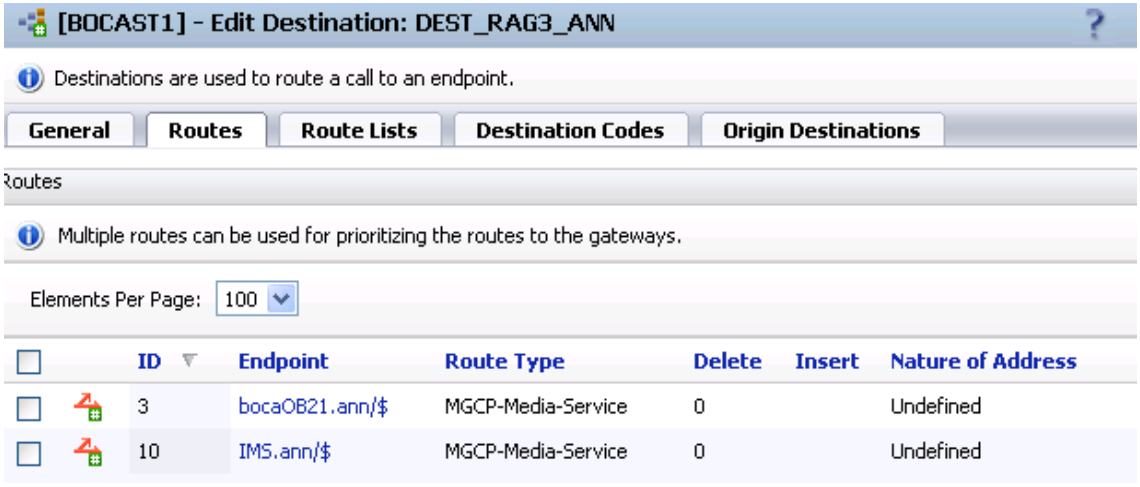


Open the Destination from the above step.
Got to OSV -> Global Translation and Routing -> Destinations and Routes -> Destinations

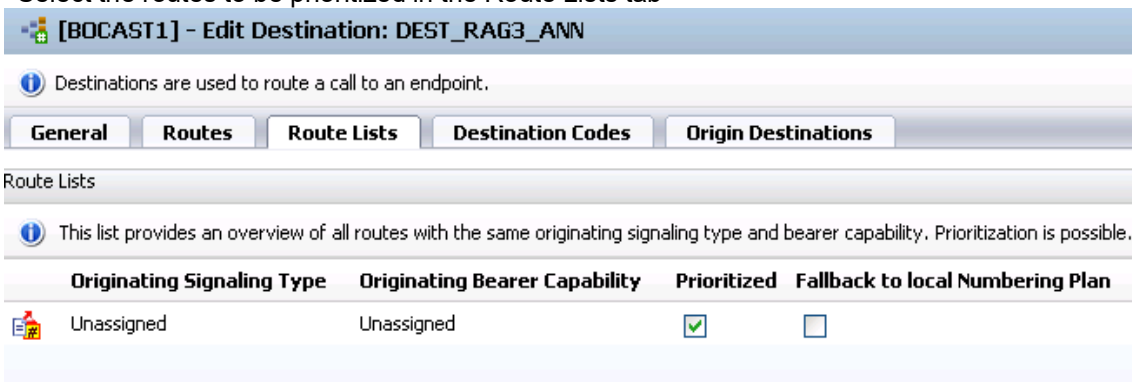
Go to the Routes Tab and press “Add” to add the main Media Server as a second Route



The destination should have now 2 routes. One to the branch media server and the second (backup) to the main media server.



Select the routes to be prioritized in the Route Lists tab



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

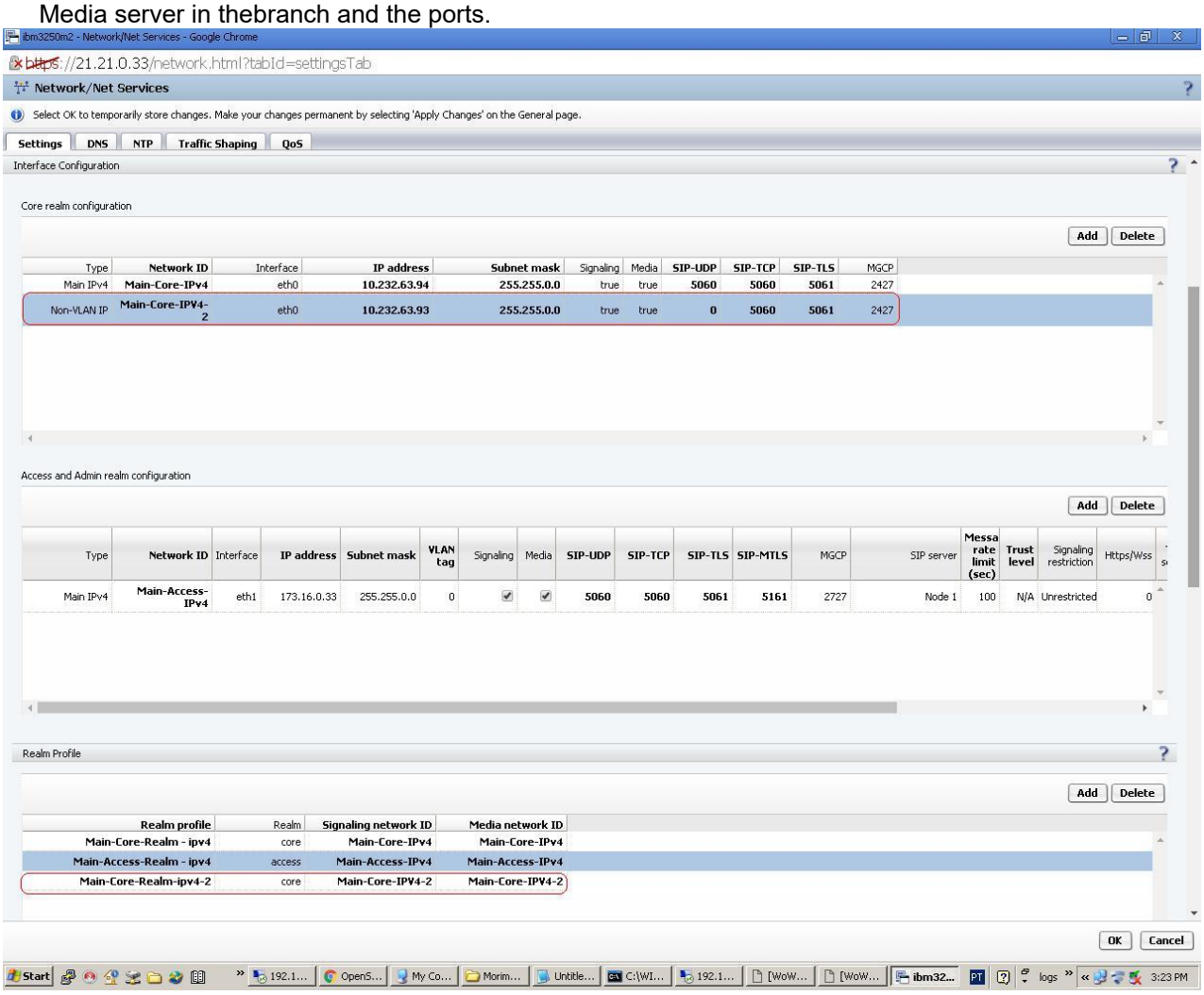
1. Create the Media Server profile

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 thebranch 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

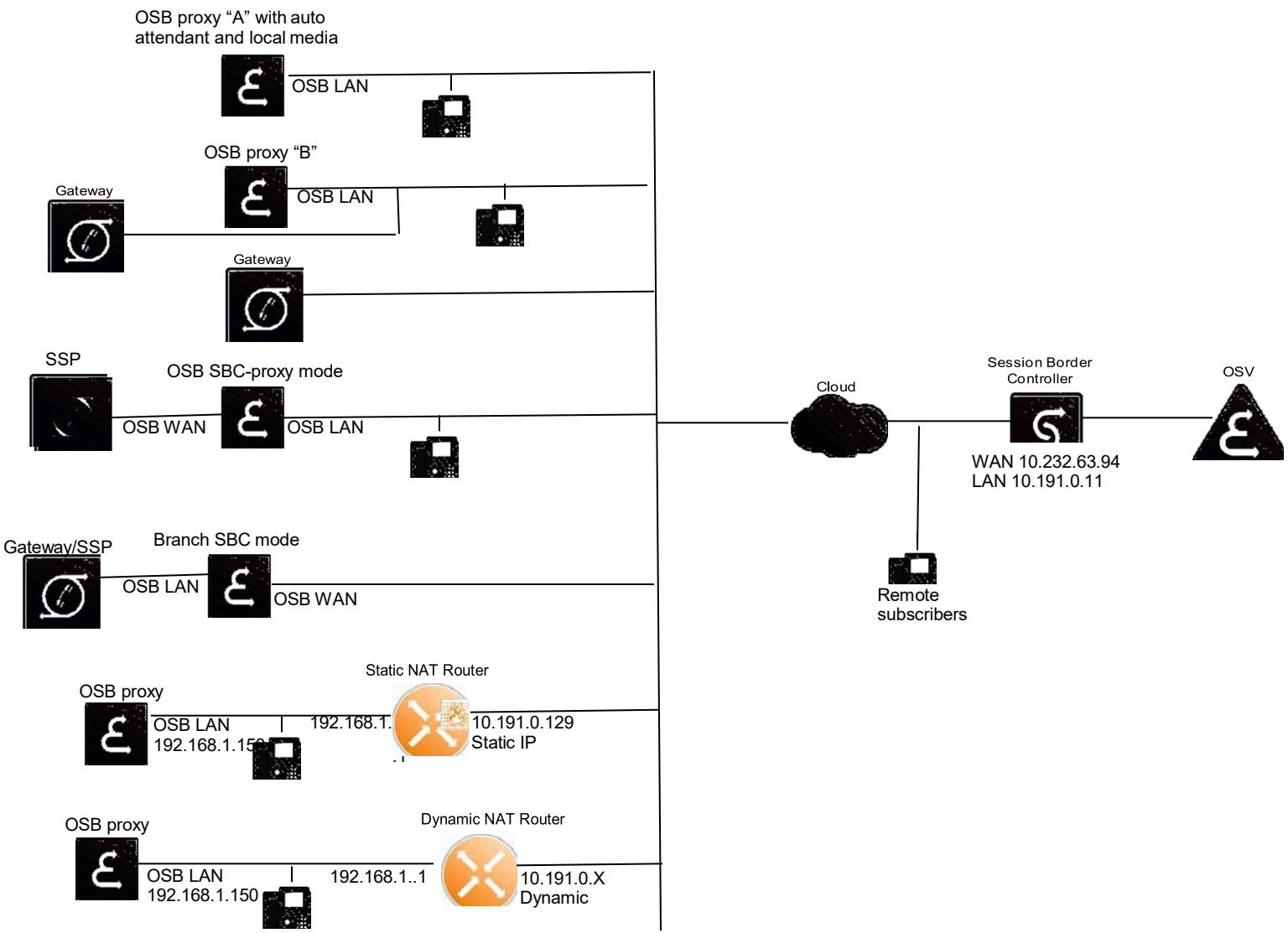
Under Remote endpoint Settings: Set the name, type = Media Server, Profile = the profile created in step 1, select theAccess realm profile, select Core realm profile = from step 2.

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 media server.

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.


OSB proxy “A” with auto attendant and local media
OSB LAN
OSB proxy “B”
Gateway
OSB LAN
Gateway
SSP
OSB SBC-proxy mode
OSB WAN
OSB LAN
Cloud
Session Border Controller
OSV
WAN 10.232.63.94
LAN 10.191.0.11
Remote subscribers
Gateway/SSP
Branch SBC mode
OSB LAN
OSB WAN
Static NAT Router
OSB proxy
OSB LAN
192.168.1.150
192.168.1.
10.191.0.129
Static IP
OSB proxy
Dynamic NAT Router
OSB LAN
192.168.1.150
192.168.1..1
10.191.0.X
Dynamic

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

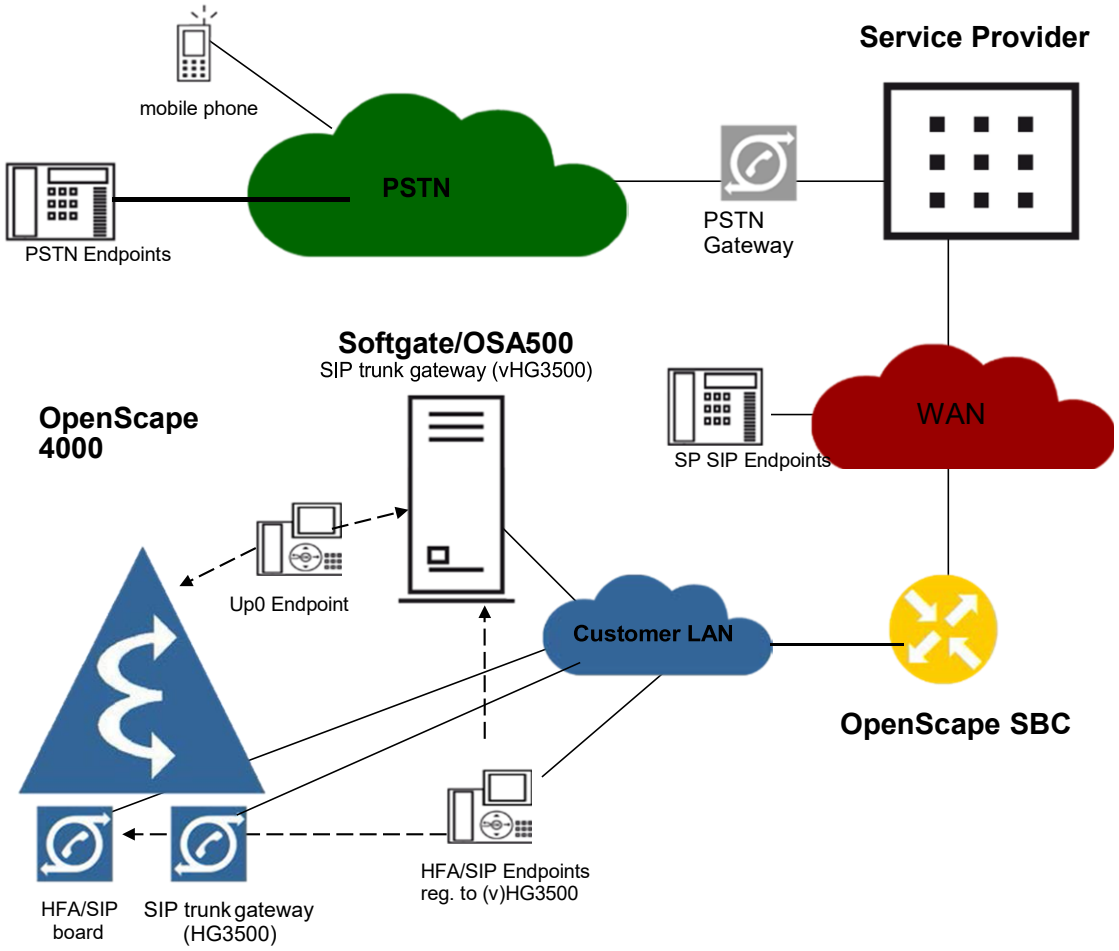
3.6.9 *Installation*

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 specificprofile.
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.

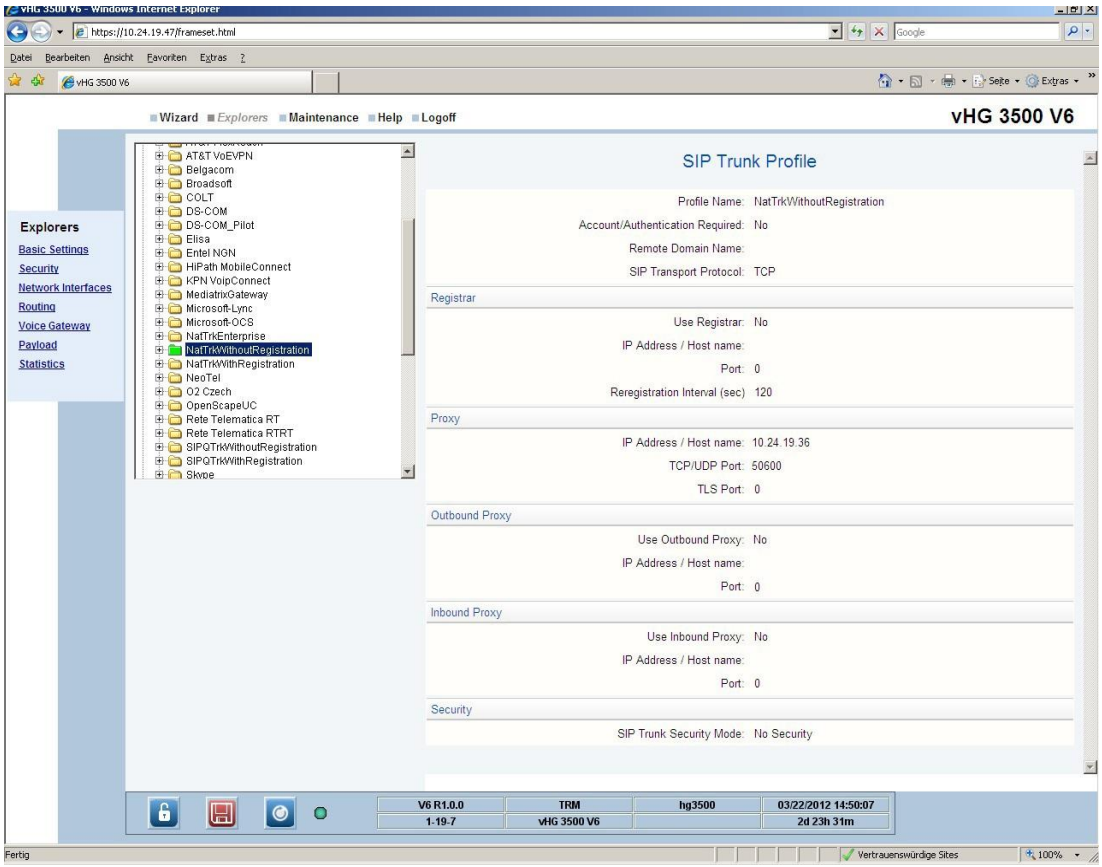


3.6.10 *Configuration change at OpenScape 4000/HG3500 w/ OpenScape SBC*

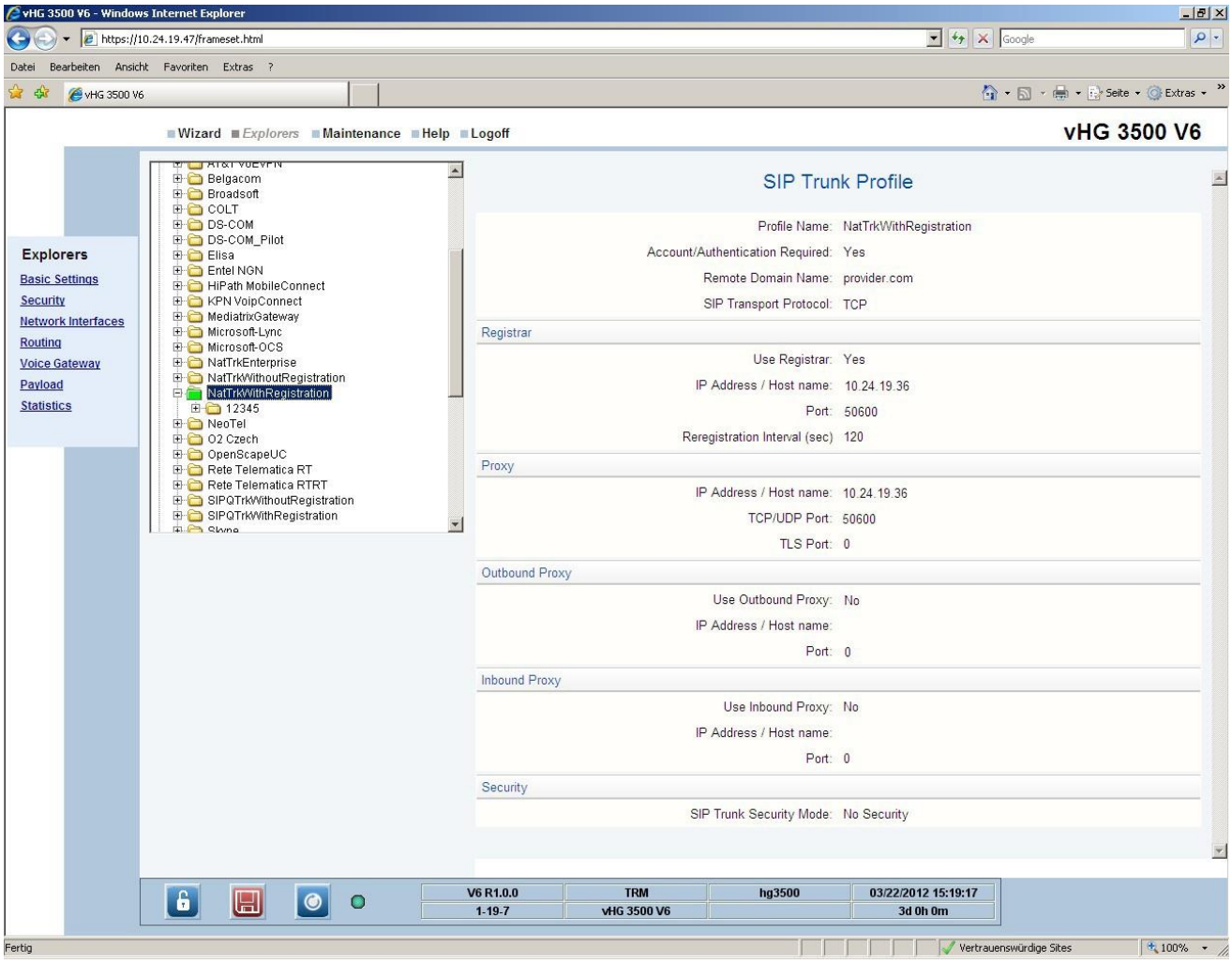
The configuration change at OpenScape 4000/HG3500 with OpenScape SBC has to be done within (v)HG3500.

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 listen port.



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

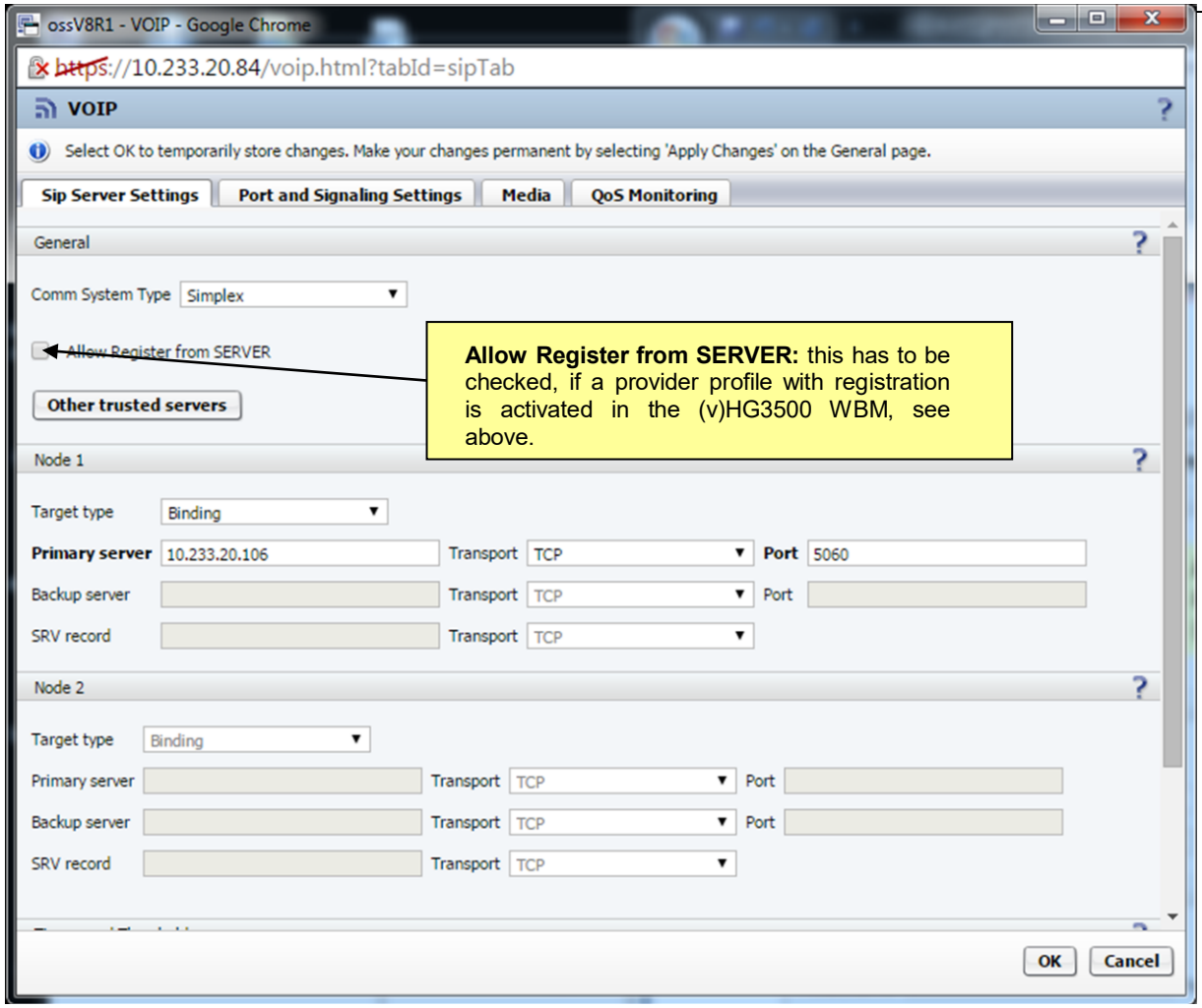
The OpenScape 4000 connection can either be configured with Simplex or Clustered mode:

- 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.

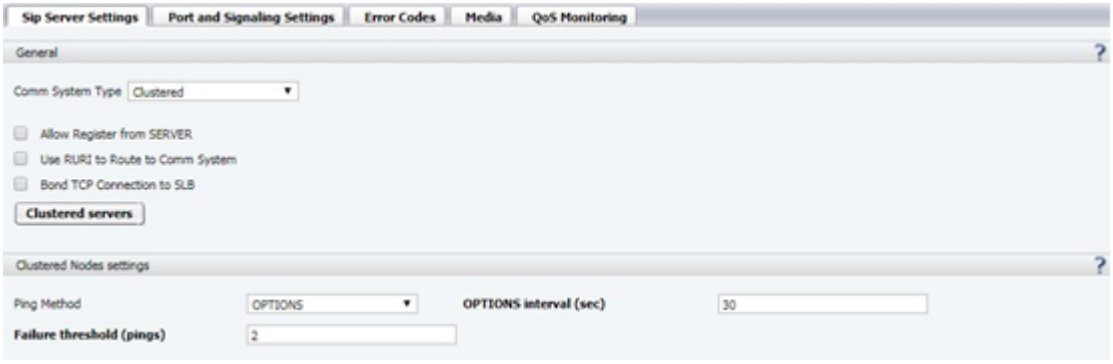
1) Simplex

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.



2) Clustered

Choose 'Clustered' as 'Comm System Type' and switch to 'Clustered servers' configuration dialog. In this dialog the needed clusters may be configured.



Each rule is treated as own node, therefore, Group Name, Priority, Routing Prefix, Ip/FQDN, Port must be

configured individually for each gateway rule.

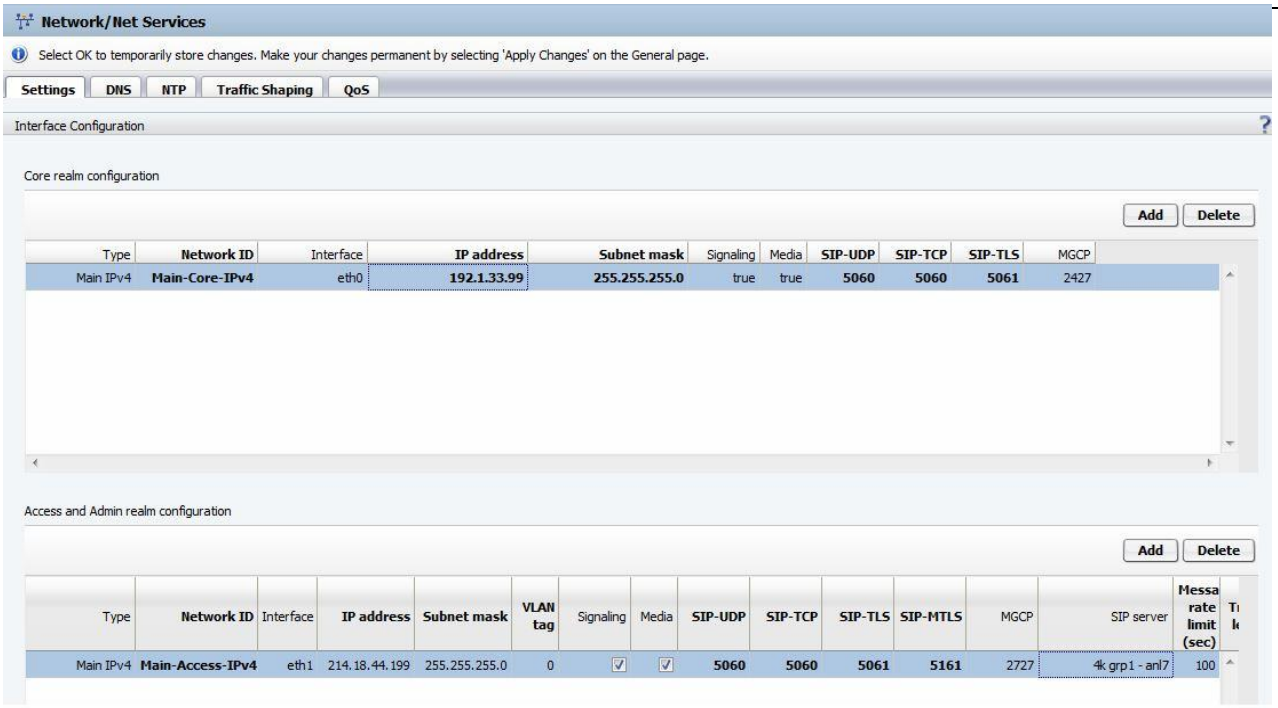
clustered Servers

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	☐	360000	3000
2	4g_grp1_anl7	sg33_vhG1	1	970	192.1.33.76	5060	TCP	☑	360000	3000
3	4g_grp1_anl7	sg33_vhG1	1	970	192.1.50.79	5061	TLS	☐	360000	3000

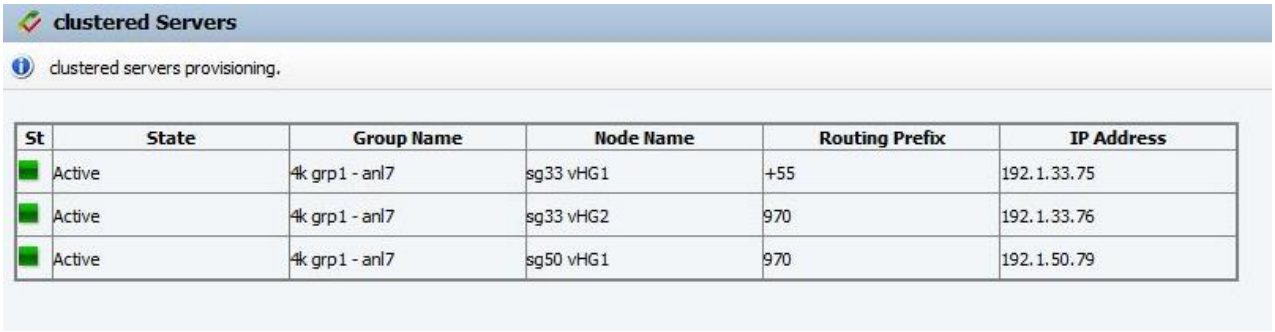
Subsequent to the cluster configuration the 'SIP server' in the 'Access and Admin realm configuration can be configured accordingly, for each interface rule a specific group can be configured or "Any" to allow all groups to be used by the interface



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.



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

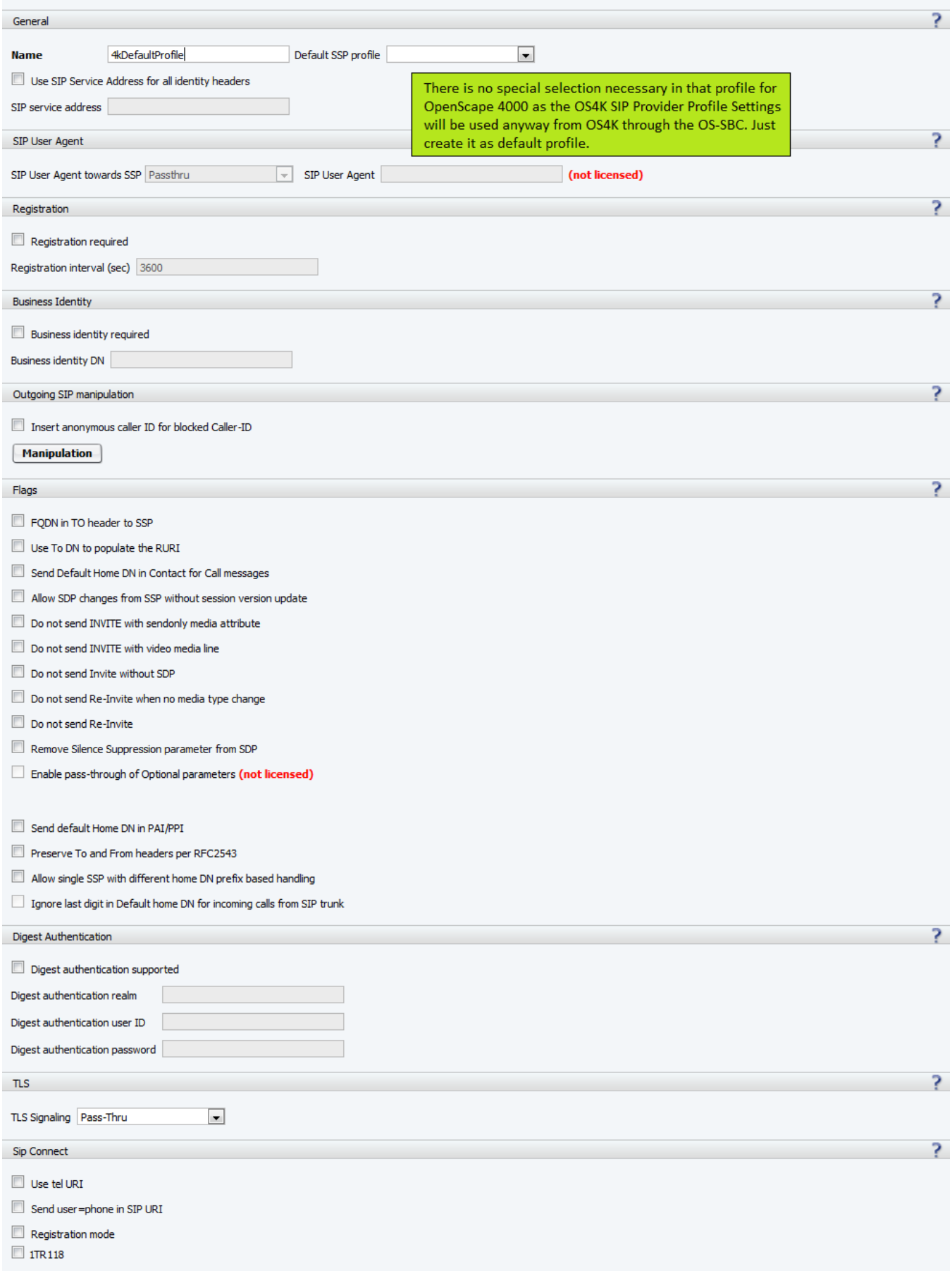
Group ID	Group name	Node Name	Priority	Routing prefix	IP address or FQDN	Port	Transport	Stick with CommServer	No Answer timer (msec)	No Reply timer (msec)
1	Group_1	Default	1		1.1.1.1	5060	TCP	☐	360000	3000
2	Group_2	General_1	1	+22	2.2.2.1	5061	TLS	☑	360000	3000
3	Group_2	General_2	2	+22	2.2.2.2	5060	TCP	☑	360000	3000
4	Group_2	General_2	3	+22	2.2.2.3	5060	TCP	☑	360000	3000
5	Group_3	Gw_1	1	+33	3.3.3.1	5060	TCP	☐	360000	3000
6	Group_3	Gw_2	1	+33	3.3.3.2	5060	TCP	☐	360000	3000
7	Group_4	Specific_1	1	+44	4.4.4.1	5060	TCP	☐	360000	3000
8	Group_5	GTC	1	+55	5.5.5.1	5060	TCP	☐	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 Remote Endpoints.

SIP Service Profile:
At first, create a service provider profile, that is generally used for SIP provider connectivity with OpenScape 4000;


General
Name
4kDefaultProfile
Default SSP profile
Use SIP Service Address for all identity headers
SIP service address
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.
SIP User Agent
SIP User Agent towards SSP
Passthru
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 Signaling
Pass-Thru
Sip Connect
Use tel URI
Send user=phone in SIP URI
Registration mode
1TR118

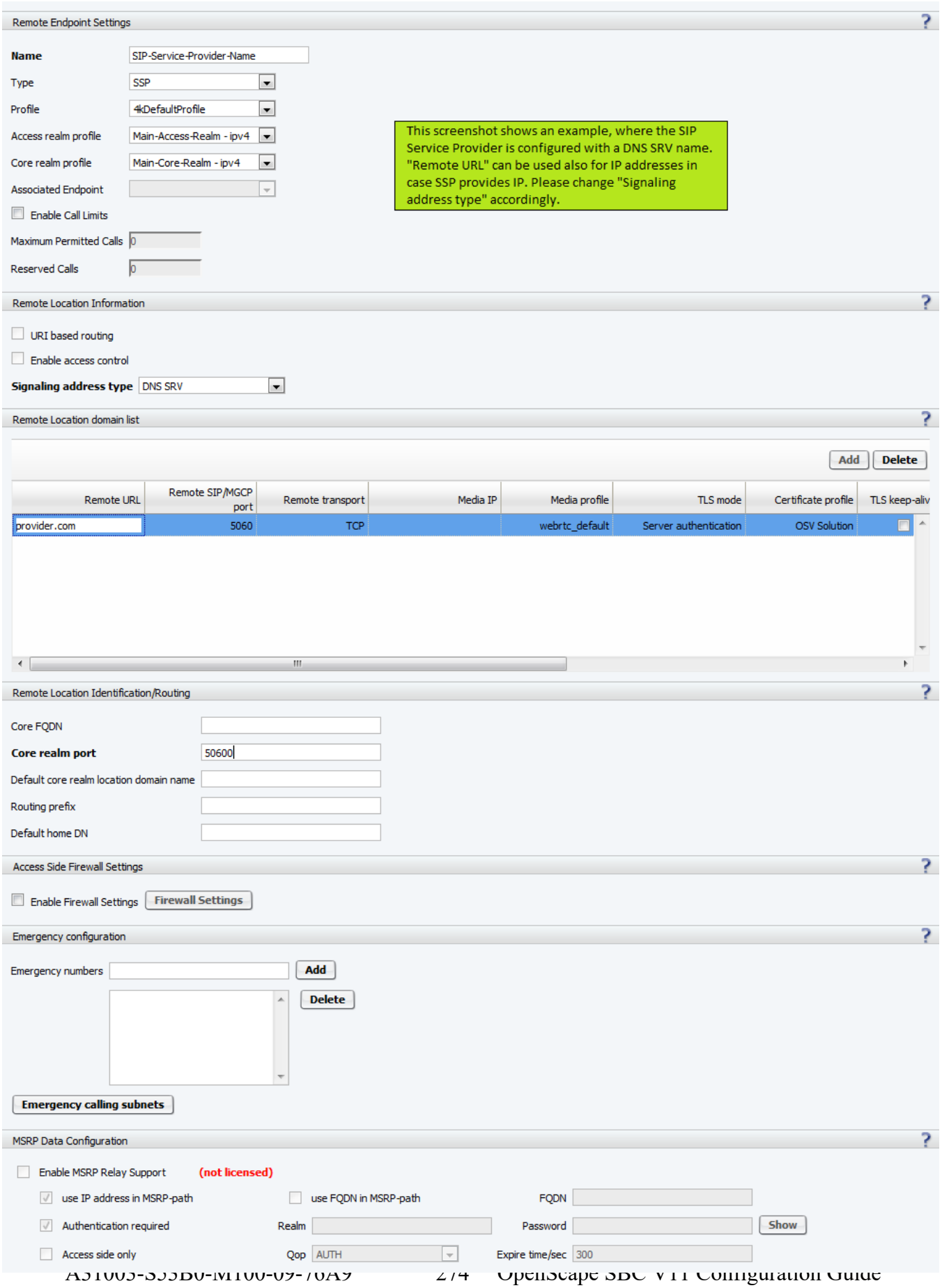
Remote Endpoints Configuration:

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
4kDefaultProfile
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

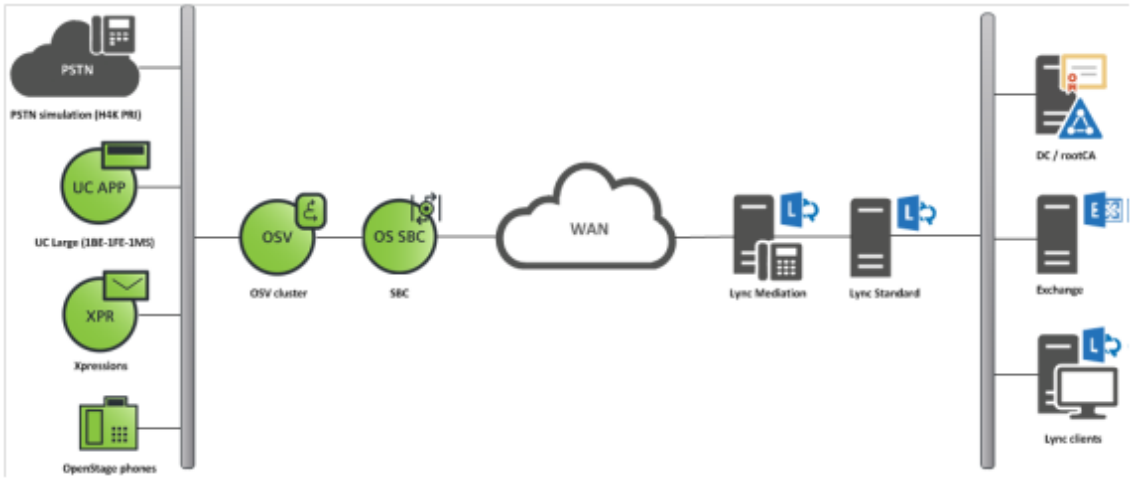
The configuration of remote endpoints to work with OpenScape 4000 as SIP server is no different from remote subscriber configuration as described in 3.4.5.1. The only exception is, if OpenScape 4000 is used in cluster mode, in this case the routing prefix is used to send the request to a specific OpenScape 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 OpenScape SBC;

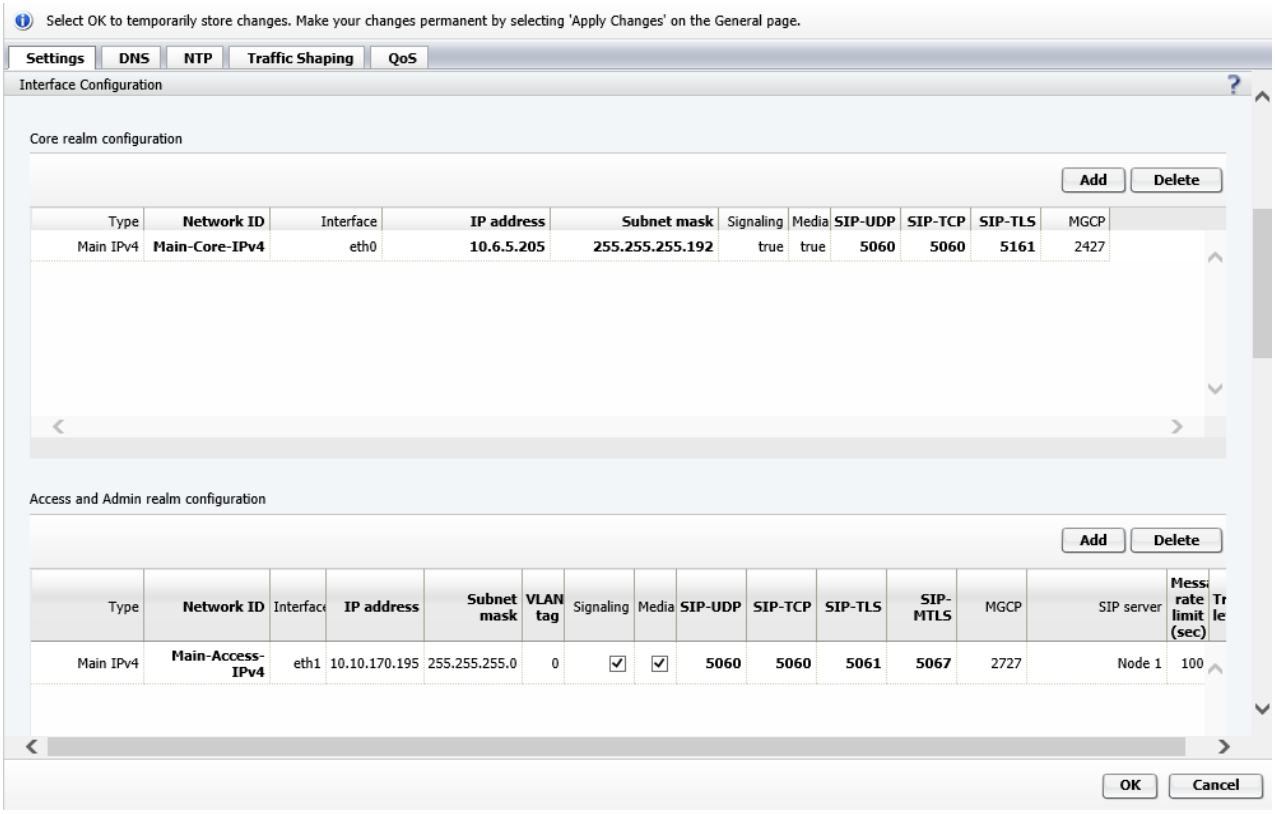
- DMC has to be disabled (AMO TDCSU: DMCALLWD=N) for the SIP trunk, UPDATE w/ SDP is not sent by OpenScape 4000/(v)HG3500.
- UPDATE is offered in the Allow header, a provider might send UPDATE w/ SDP; in this case a special profile has to be provided by OpenScape 4000 as workaround (CR created for OpenScape 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**:



   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

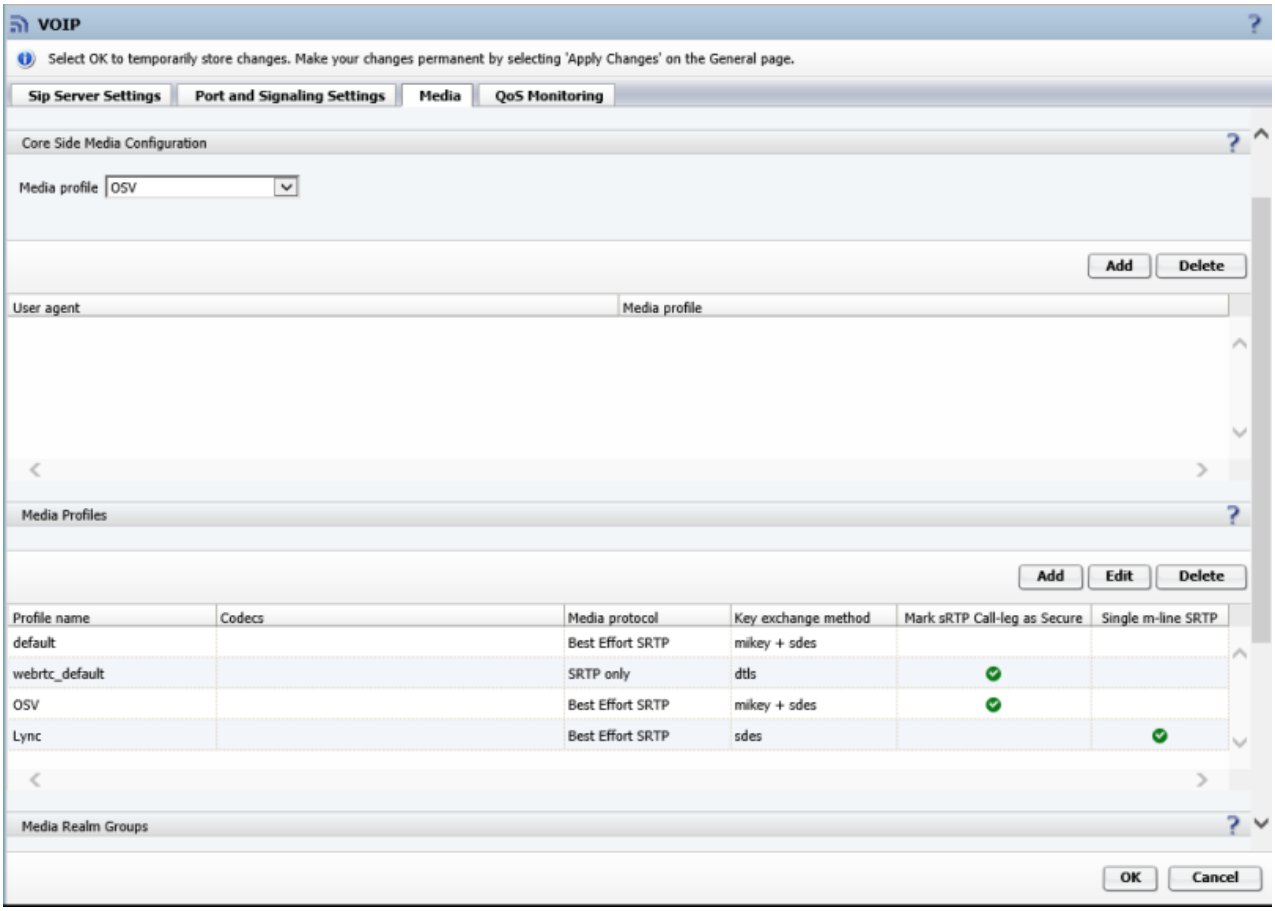
2. From SBC Management portal, go to **VOIP** >**Sip Server Settings**:

   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

SBC-Lync Mediation (e.g. Lync).



a. Under **Core Side Media Configuration**, select the value e.g. “OSV” (custom).

b. Under **Media Profiles** for the “OSV” profile, select:

The **Media Protocol** should be “Best Effort SRTP”.

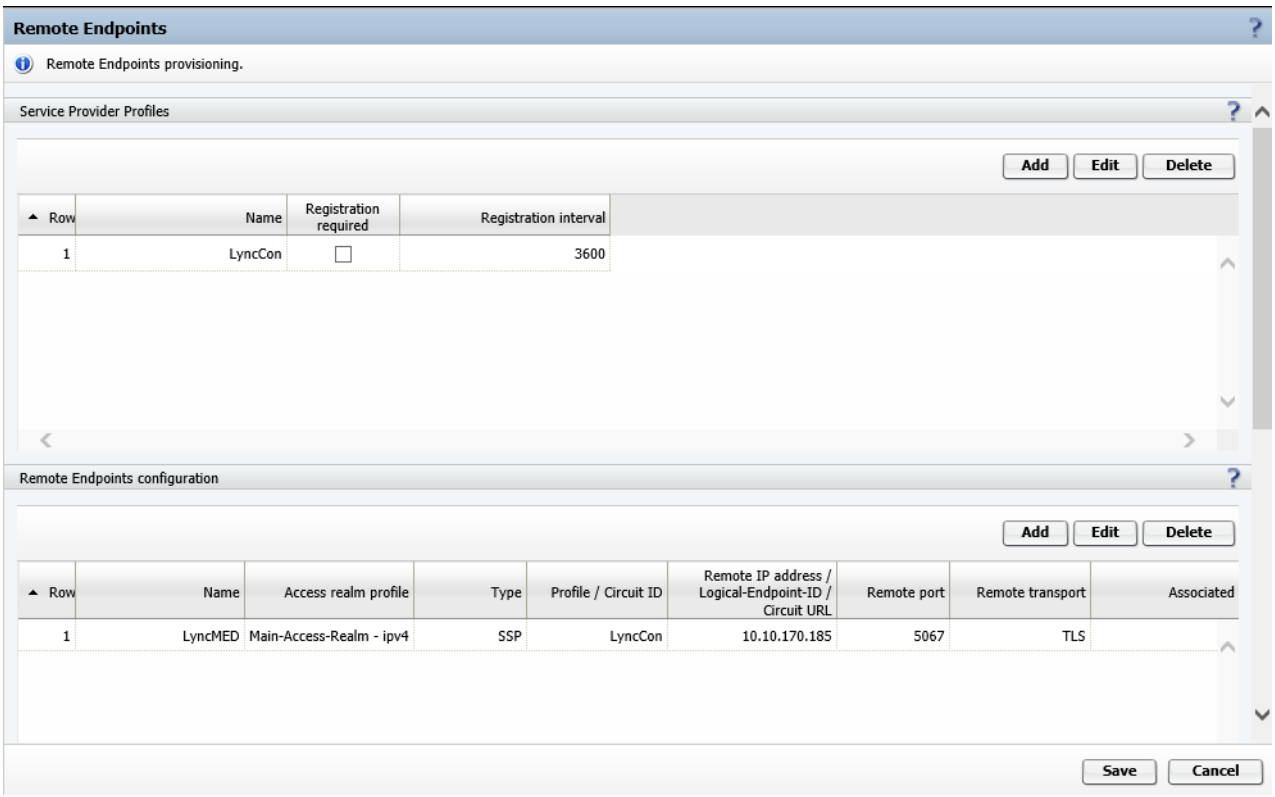
The **Key exchange method** should be “mikey + sdes” (set based on OSV domain equipment preference).

The **Mark SRTP Call-leg as Secure** should be “enabled/checked”.

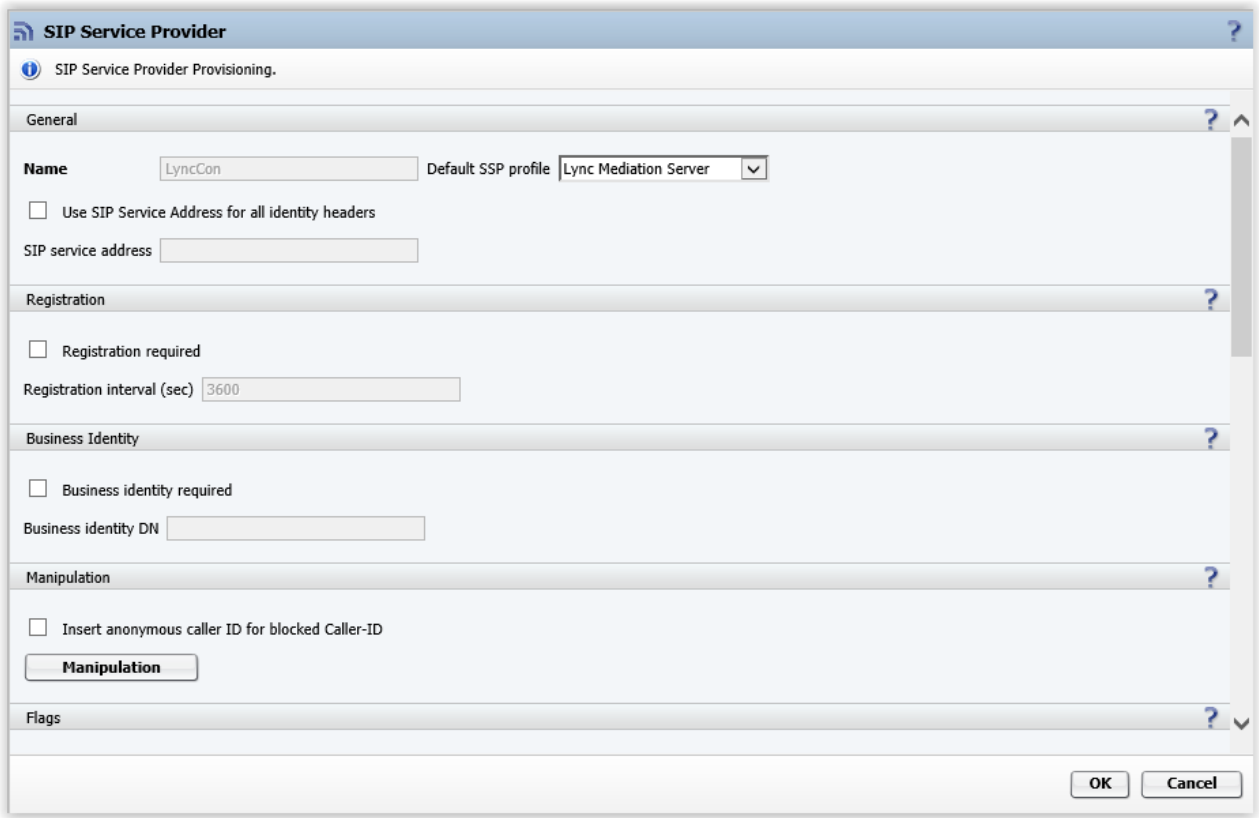
c. Under **Media Profiles** for the “Lync” profile, select:

- 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”.

4. 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:

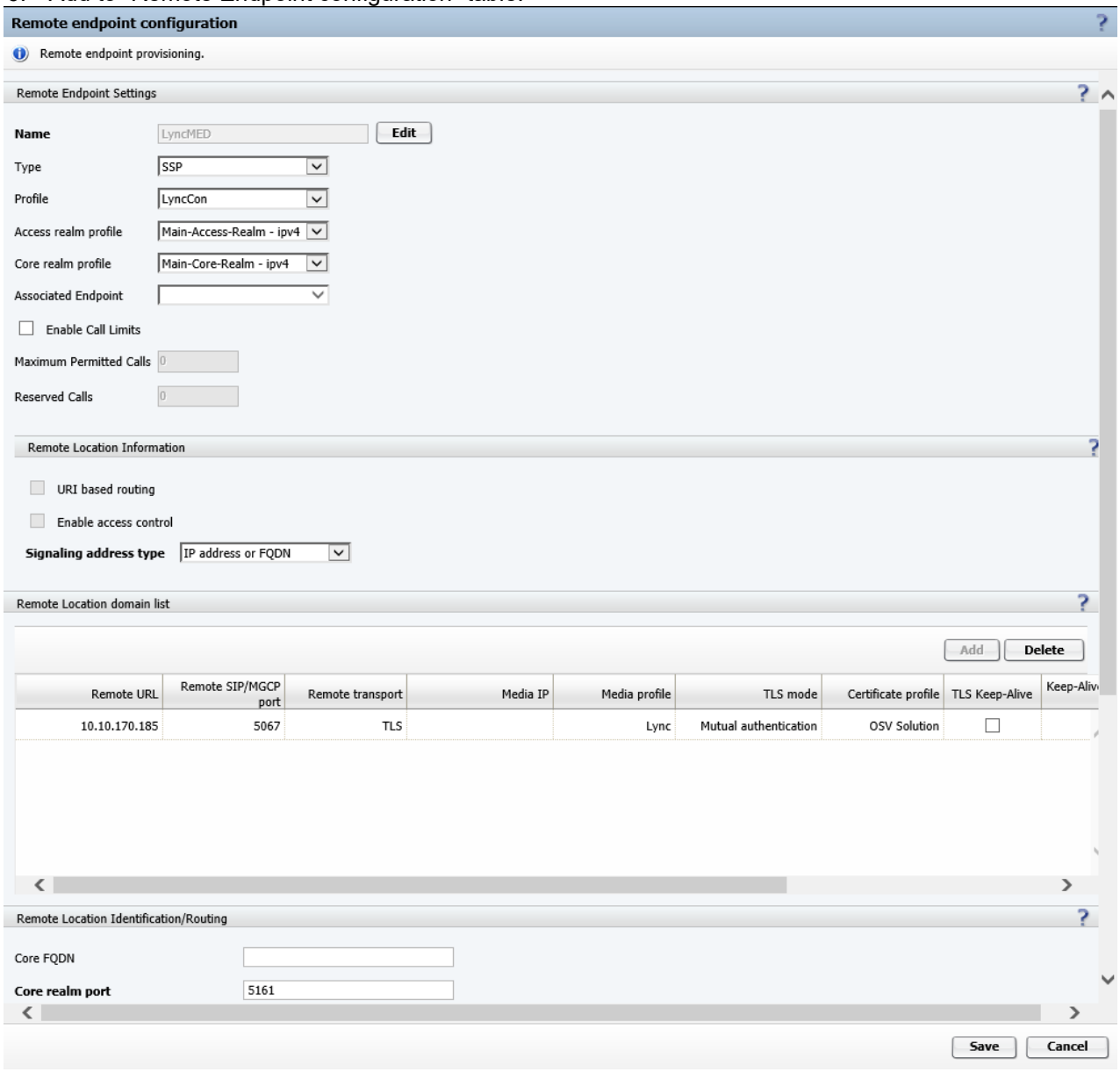


5. A new Service Provider Profile is required:



a. Select for “**Default SSP Profile**” the option “Lync Mediation Server”.

6. Add to “Remote Endpoint configuration” table:



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.

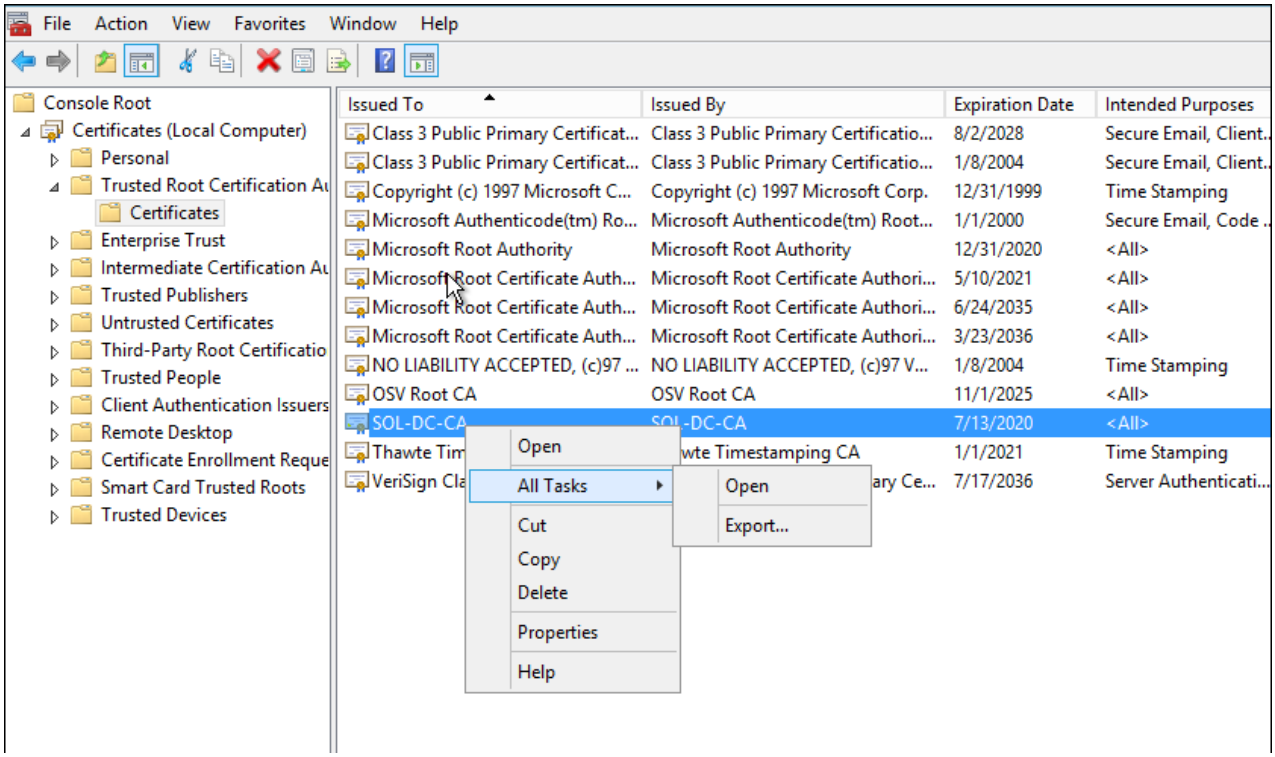
1. The OSV rootCA certificate file need to be imported in the trusted CA store of Lync Mediation server in order to trust the SBC server certificate during MTLS handshake.

    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”.

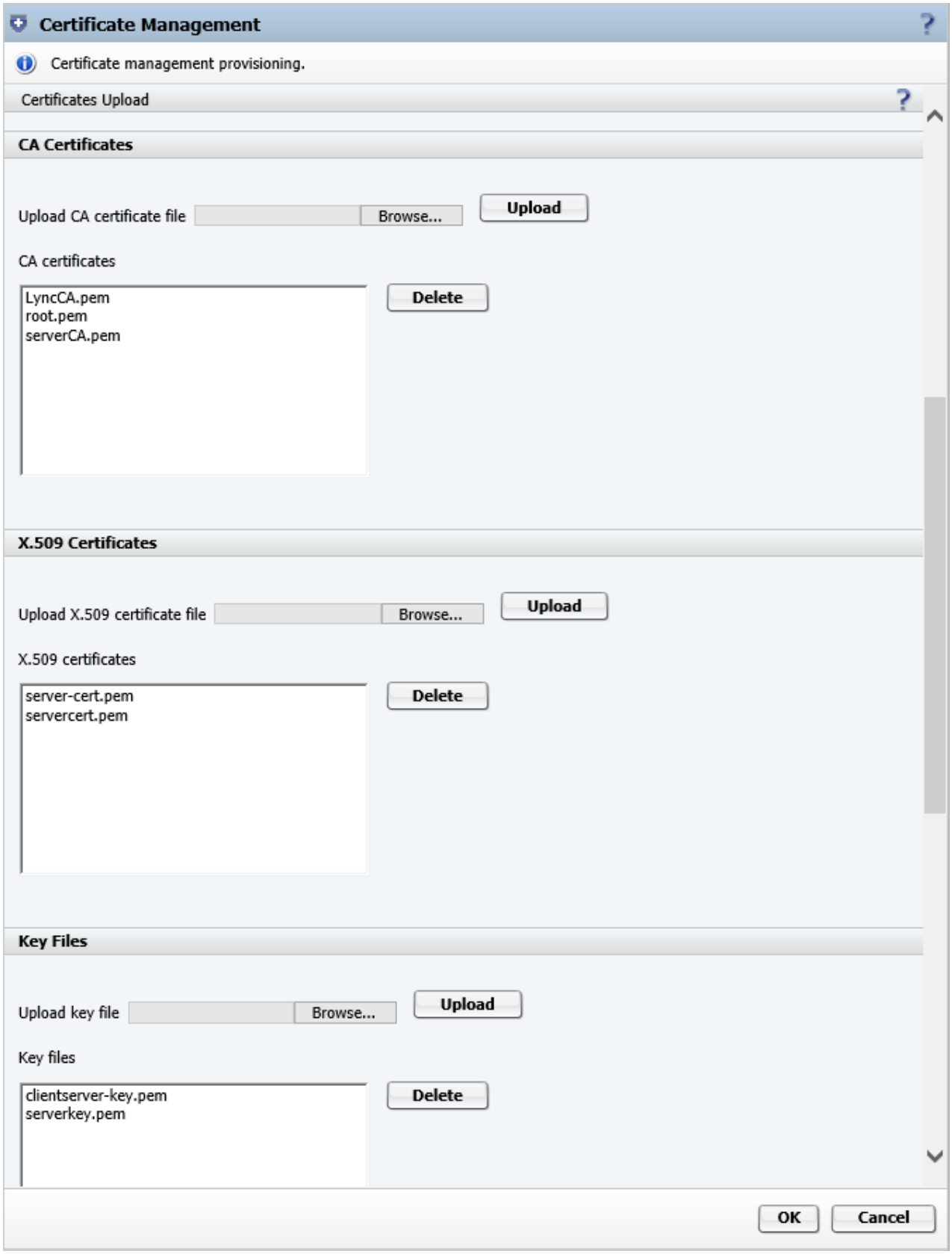
The “X509v3 Extended Key Usage”.

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:



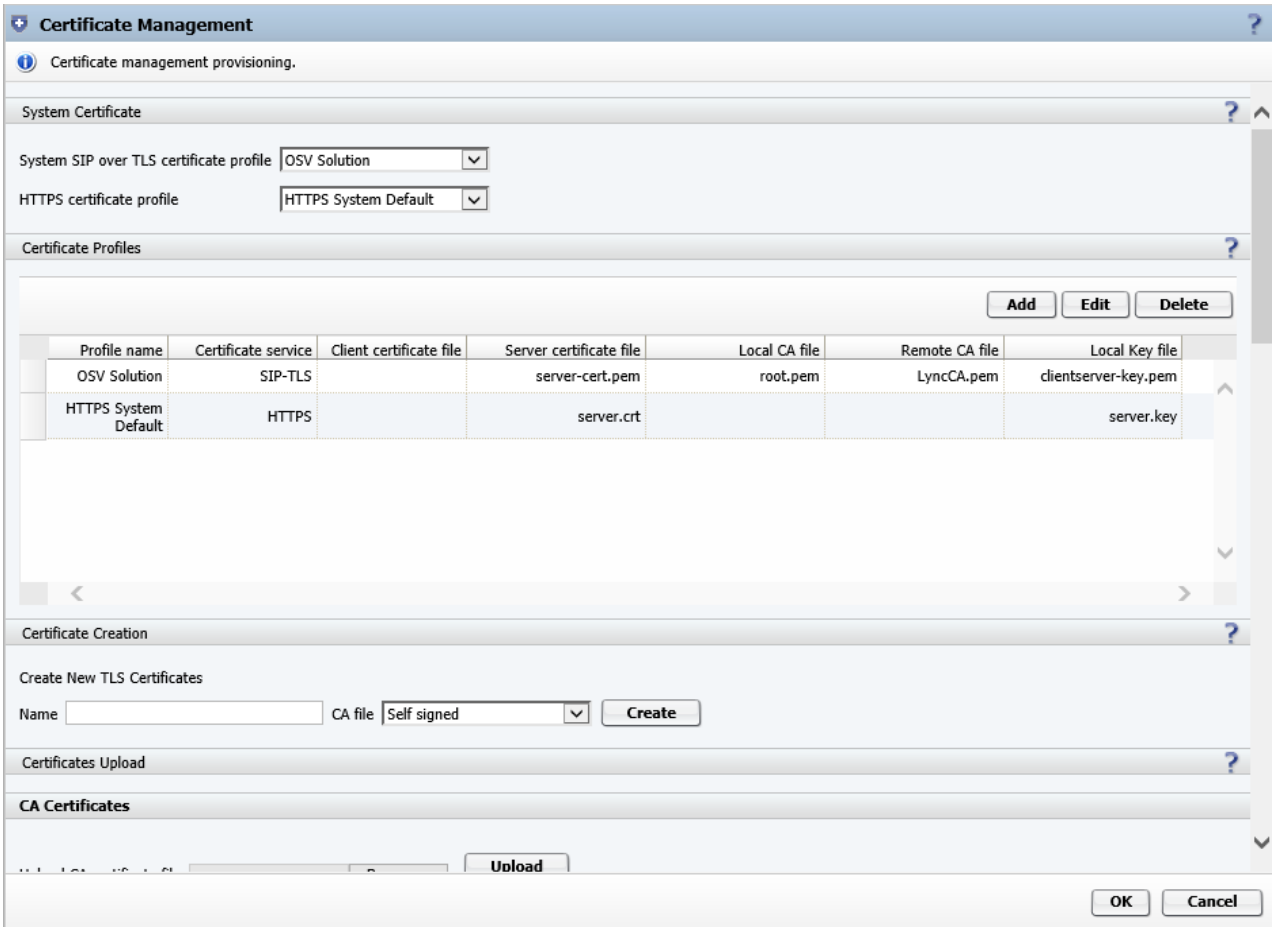
a. The **CA certificates** contain:

- 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.



At **Server certificate file** use e.g., "`server-cert.pem`"

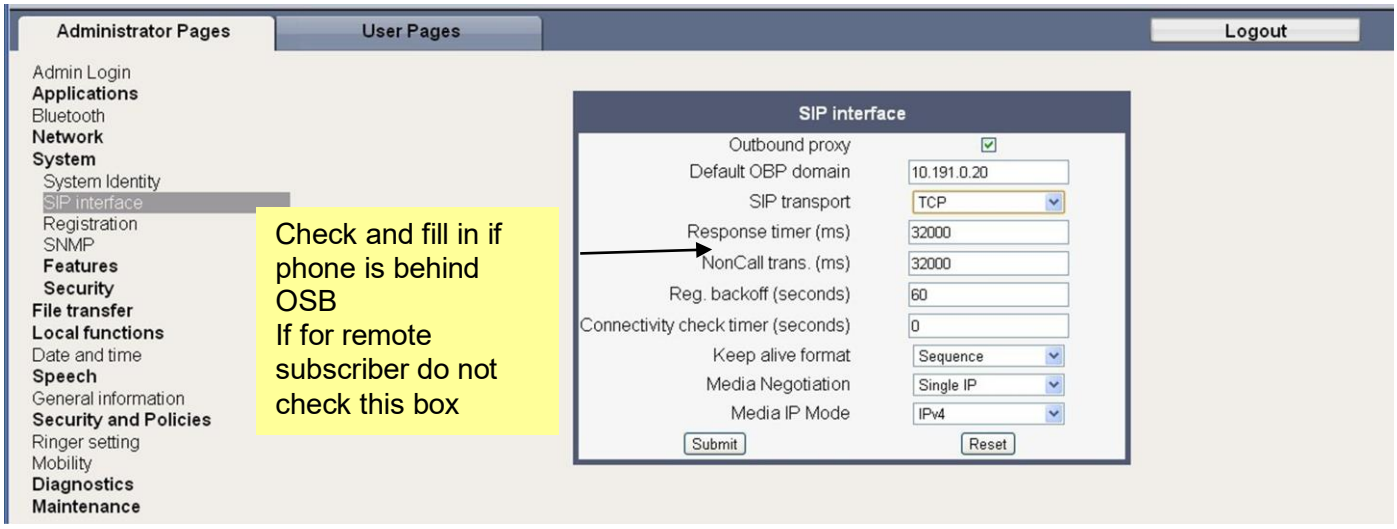
At **Local CA file** use e.g., "`root.pem`"

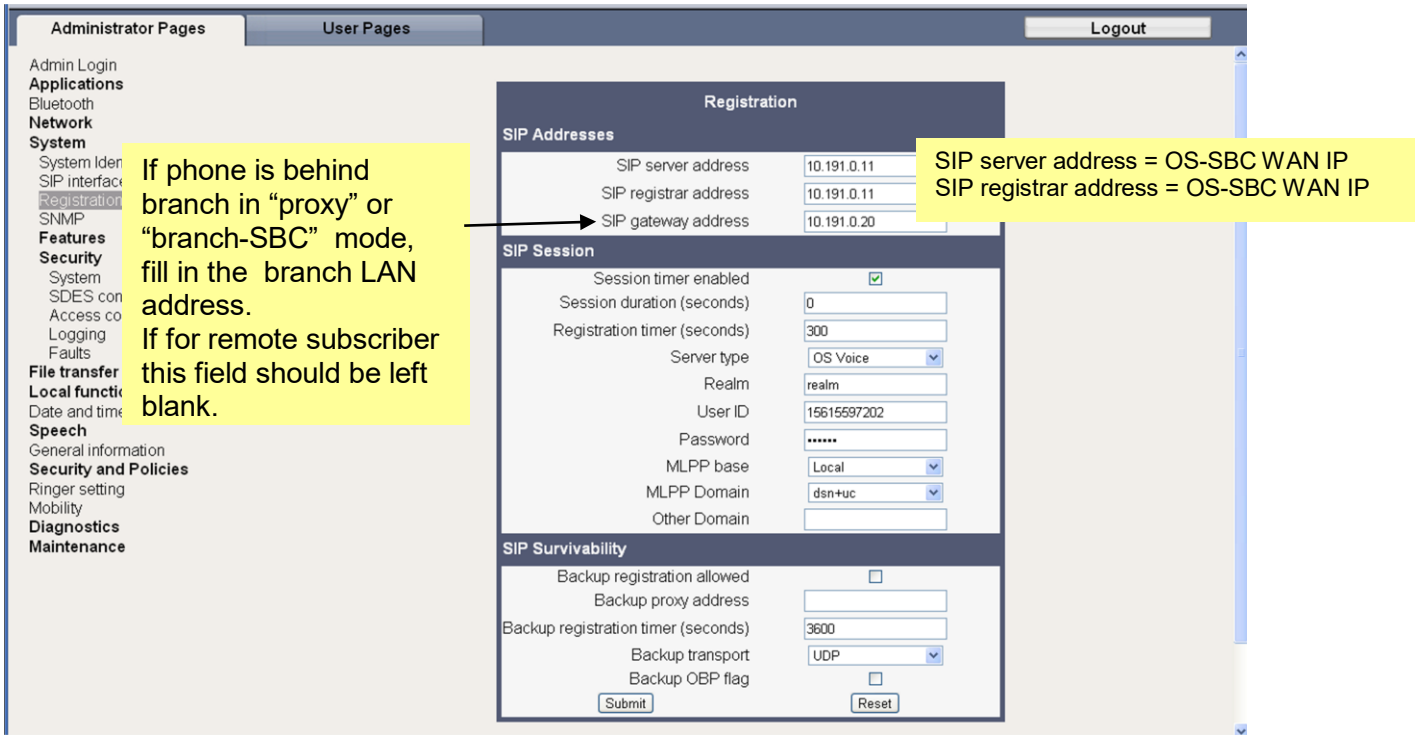
At **Remote CA file** use e.g., "`LyncCA.pem`"

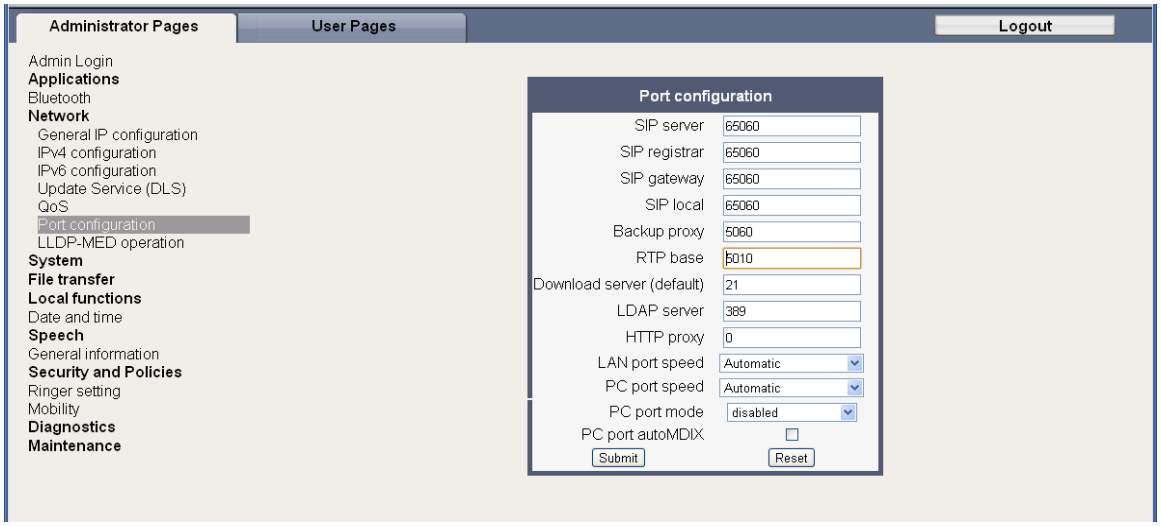
At **Key files** use e.g., "`clientserver-key.pem`"

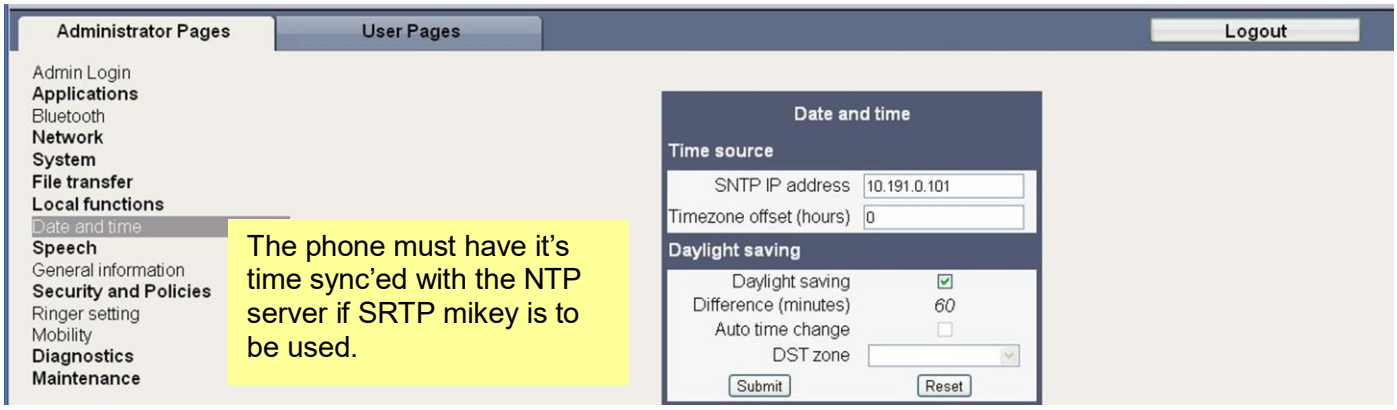
3.8 Phone Configuration as Remote user

The following configuration is used for all versions of OpenStage phones.






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 server 65060
SIP registrar 65060
SIP gateway 65060
SIP local 65060
Backup proxy 5060
RTP base 5010
Download server (default) 21
LDAP server 389
HTTP proxy 0
LAN port speed Automatic
PC port speed Automatic
PC port mode disabled
PC port autoMDIX
Submit
Reset


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
The phone must have it's time sync'ed with the NTP server if SRTP mikey is to be used.
Date and time
Time source
SNTP IP address 10.191.0.101
Timezone offset (hours) 0
Daylight saving
Daylight saving
Difference (minutes) 60
Auto time change
DST zone
Submit
Reset

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 thatcodec.

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, afterthe 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 IBM x3550.

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 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 OpenScape SBC

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)	5096
	ISAKMP (Key management)	500
	Syslog Server (used for system logging)	514
	Ipsec Nat-Transversal (RFC 3947)	4500
	Secure HTTPS (used by Fusion)	8443
Configurable / dynamic Default values shown	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: number of sessions x 5 gives the number of required ports to be opened. 100 x 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

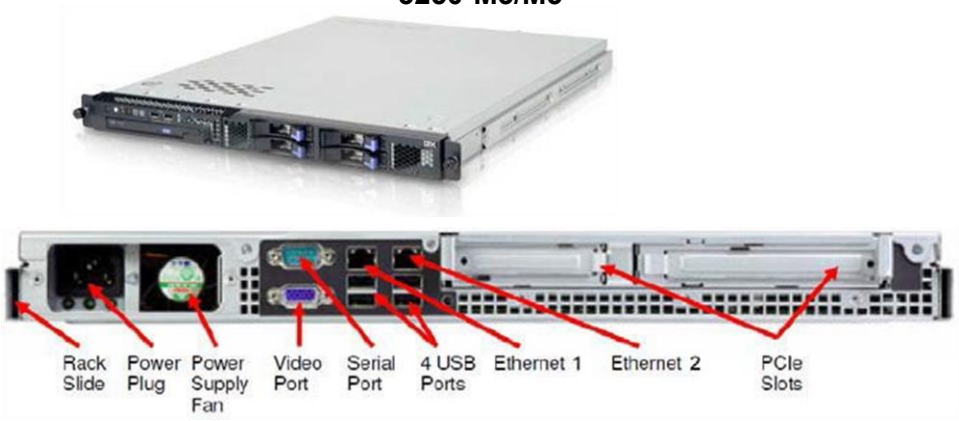
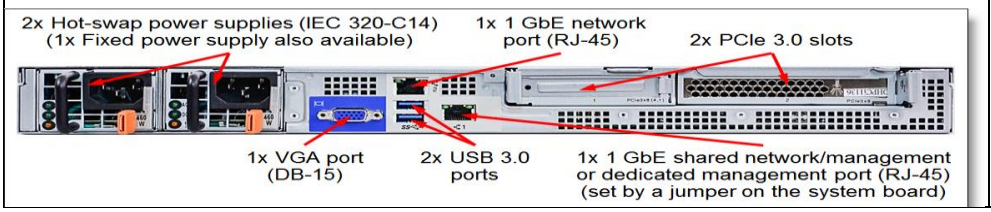
From build 09.04.12.02, new configurable sipserver parameters are available to control message rate. These parameters are maxRegisterRate, maxCallRate, maxNotifyRate, and maxSubscribeRate. And, they are configurable only via XML file. The value “0” indicates that the parameter is disabled, and the default 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:

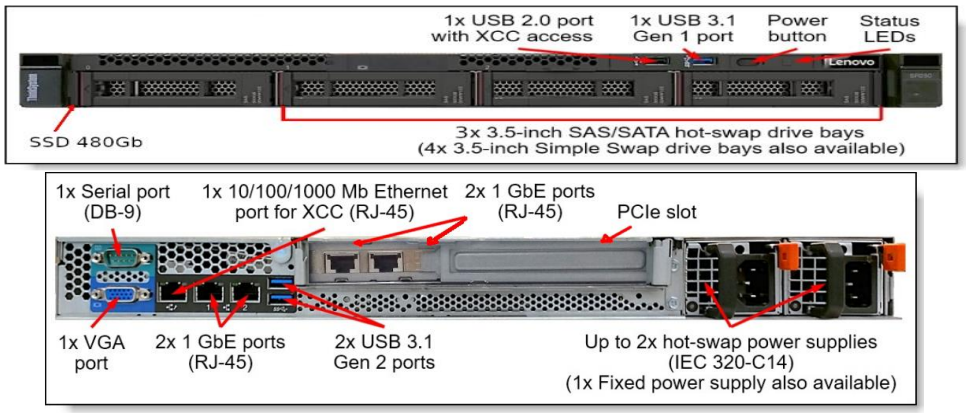
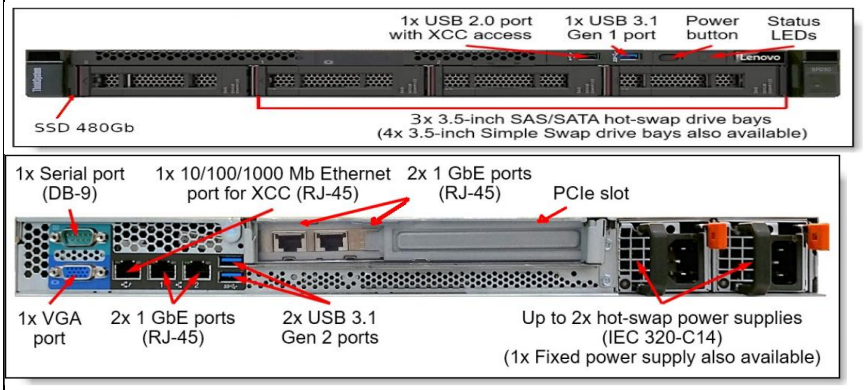
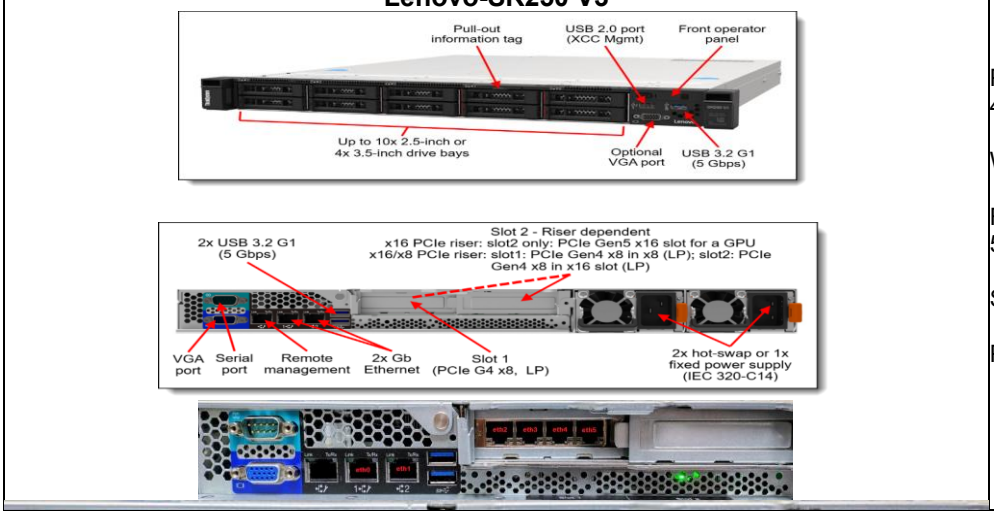
1)Update from a different release (for instance V9R3 to V9R4);

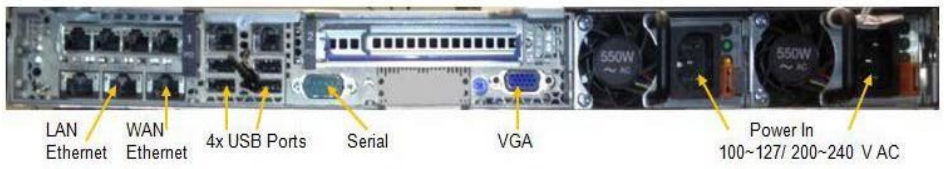
2)Any change is made to the current database.

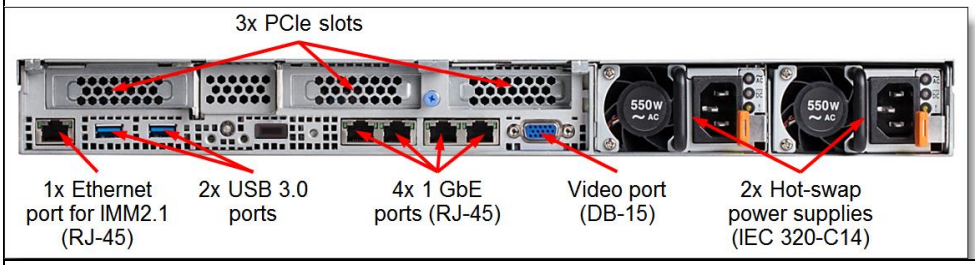
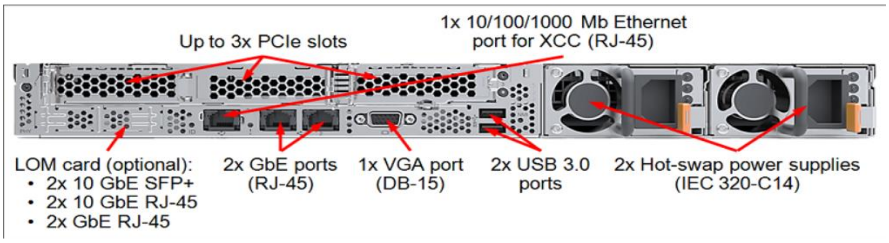
Once you have an xml file with the fields available, edit it to modify the parameters as desired and then import it.

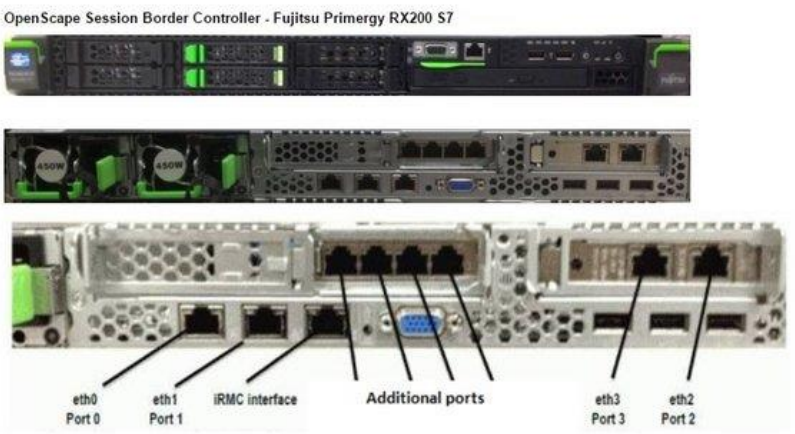
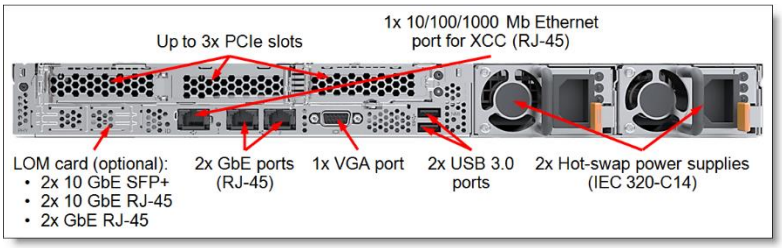
7 Table B: Hardware Types Table

OpenScape SBC Model	Details
3250-M3/M5 	**IBM x3250 M3/M5 server** 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
3250-M6  	**IBM x3250 M6 server** Physical Dimension (W x H x D): 435 x 43 x 576 For **x3250 M5**, only 2 ethernet interfaces are available. 3633AC1

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
Lenovo-SR250 V3 	**Lenovo-SR250 V3 (Replacement for Lenovo-SR250 V2)** Physical Dimension (W x H x D): 435 x 43 x 561 mm (17.1" x 1.7" x 22.1") Weight: up to 12.3 kg (27.1 lb) Rated Power: 100-127 / 200-240 V AC, 50-60 Hz SATA: SSD 480Gb 03KH094 Part Number: S30122-X8000-X136

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

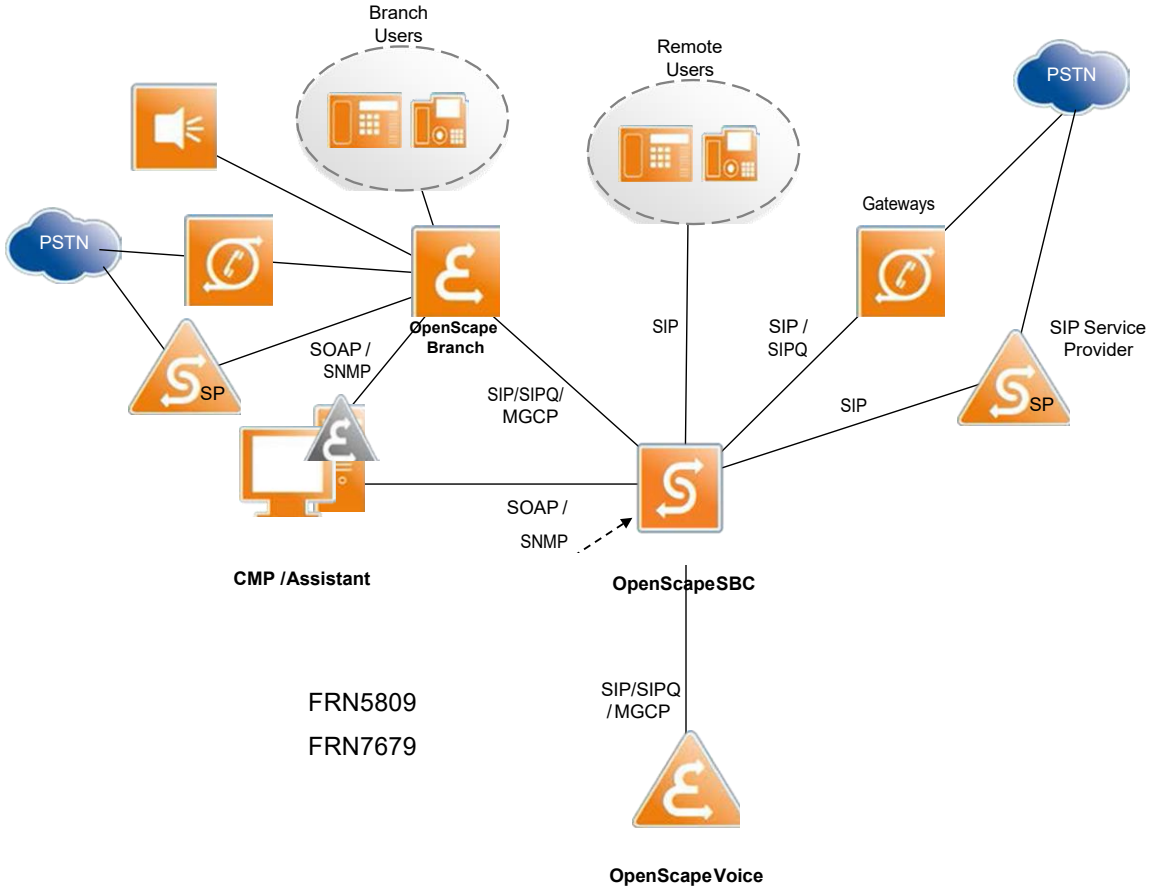
3550-M5  	**IBM x3550 M5** Physical Dimension (W x H x D): 434 x 43 x 734 mm (17.1” x 1.69” x 28.9”) Weight: up to 19.3 kg (42.5 lb) Rated Power: 100-127 / 200-240 V AC , 50-60 Hz, 351 W Operating Temperature: 5-40°C (41-104°F) Part Number :to be supplied
 	**Lenovo SR530 (Replacement for IBM x3550 M5)** 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 	**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 V3   	**Lenovo-SR630 V3** **(Replacement for Lenovo-SR630 V2)** 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 SATA: SSD 480Gb 03KH094 Part Number: S30122-X8000-X135

Lenovo-SR630 V2	**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

3x Low Profile PCIe slots (no rear drives)

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 Commmon 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 (netscapeCertficateType) 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
MCgGA1UEChMhU2llbWVucy1FbnRlcnByaXNlIENvbW11bmljYXRpb25zMRgwFgYD
-----END CERTIFICATE-----

Or, it could be a concatenation of the certificate together with the signing CAs certificate:

-----BEGIN CERTIFICATE-----
MIIESzCCA7SgAwIBAgIJAIXewvQNWUL/MA0GCSqGSIb3DQEBBQUAMIHKMQswC
QYD
VQQGEwJVUzEQMA4GA1UECBMHRmxvcmlkYTETMBEGA1UEBxMKQm9jYSBSY
XRvbjEq
MCgGA1UEChMhU2llbWVucy1FbnRlcnByaXNlIENvbW11bmljYXRpb25zMRgwFgYD
...
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
MIIESTCCA7KgAwIBAgIJAOPiOzYWpgITMA0GCSqGSIb3DQEBBQUAMIHKMQswC
QYD
VQQGEwJVUzEQMA4GA1UECBMHRmxvcmlkYTETMBEGA1UEBxMKQm9jYSBSYXRvbjEq
MCgGA1UEChMhU2llbWVucy1FbnRlcnByaXNlIENvbW11bmljYXRpb25zMRgwFgYD
...
-----END CERTIFICATE-----

For OpenScape Branch it is necessary to have separate CA and server certificate. For example as below

CA.pem
osbservercert.pe
m
osbserverkey.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 osbservercert.pem |

openssl md5 openssl rsa -noout -modulus -in

osbserverkey.pem | openssl md5 openssl req -noout -

modulus -in osbserver.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 extentions 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
ossserverkey.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 configurationfile, 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 -outossserver.csr

Note: Keep the private key (eg: ossserverkey.pem) in secure place as it will be required to install the certificates for OpenScapeSBC.

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 asossservercert.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 osbservercert.pem

One should observe the PEM formatted certificate received as follows:

-----BEGIN CERTIFICATE-----
MIIDejCCAuOgAwIBAgIJANRO4Lwz1cO6MA0GCSqGSIb3DQEBBQUAMIHMMQswC
QYD

VQQGEwJVUzEQMA4GA1UECBMHRmxvcmlkYTETMBEGA1UEBxMKQm9jYSBSYXRvbjEq
MCgGA1UEChMhU2llbWVucy1FbnRlcnByaXNlIENvbW11bmljYXRpb25zMRgwFgYD
-----END CERTIFICATE-----

Or, it could be a concatenation of the certificate together with the signing CAs certificate:

-----BEGIN CERTIFICATE-----
MIIESzCCA7SgAwIBAgIJAIXewvQNWUL/MA0GCSqGSIb3DQEBBQUAMIHKMQswC
QYD
VQQGEwJVUzEQMA4GA1UECBMHRmxvcmlkYTETMBEGA1UEBxMKQm9jYSBSY
XRvbjEq
MCgGA1UEChMhU2llbWVucy1FbnRlcnByaXNlIENvbW11bmljYXRpb25zMRgwFgYD
...
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
MIIESTCCA7KgAwIBAgIJAOPiOzYWpgITMA0GCSqGSIb3DQEBBQUAMIHKMQswC
QYD
VQQGEwJVUzEQMA4GA1UECBMHRmxvcmlkYTETMBEGA1UEBxMKQm9jYSBSYXRvbjEq
MCgGA1UEChMhU2llbWVucy1FbnRlcnByaXNlIENvbW11bmljYXRpb25zMRgwFgYD
...
-----END CERTIFICATE-----

For OpenScape Branch it is necessary to have separate CA and server certificate. For example as below

CA.pem
osbservercert.pe
m
osbserverkey.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 osbservercert.pem | openssl

md5 openssl rsa -noout -modulus -in osbserverkey.pem | openssl

md5 openssl req -noout -modulus -in osbserver.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 temp directory.

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
   ossserver.csr - noout -
   text o
```

Certificate Sign Request (DER format):

```
openssl req -inform DER –in ossserver.csr -noout
   -text o
```

Certificate (PEM format):

```
openssl x509 -in
   certficate.pem - noout -text
```

- Certificate (DER format):

```
openssl x509 -inform DER -in certficate.der -noout –text
```

9.7.10 *Converting certificate format*

Convert DER to PEM

```
openssl x509 -inform der -in
   certificate.cer -out certificate.pem o
```

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 extentions 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:

- Remote Subscribers which support dynamic registration as IPv4-only or IPv6-only:
  - Remote Subscribers may be in a private or public network without a NAT.
  - Remote Subscribers in a private network behind a NAT. Only private networks of the same IP version as the public NAT interface are supported.
- Remote Subscribers which are statically configured as IPv4-only or IPv6-only
- Remote Gateways (e.g., OpenScape 4000) which are statically configured as IPv4-only or IPv6-only
- Session establishment between IPv4-only or IPv6-only Remote Subscribers with other SIP interfaces using the same or different IP version.
- Session establishment between IPv4-only or IPv6-only Remote Gateways with other SIP interfaces using the same or different IP version
- SRTP/RTP Media bridging between media endpoints using different IP versions
- SRTP/RTP Media session optimization between media endpoints within the same subnet
- OS-SBC V1 and V2 network scenarios for the OS-SBC Access network continue

to be supported as IPv4-only:

- OpenScape Branch Proxy / Proxy (SBC) users are supported as IPv4-only or IPv6-only.
- OpenScape Branch Proxy / Proxy (SBC) external or integrated Media Gateways
- 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.
- SIP Service Providers with IPv6 is supported.

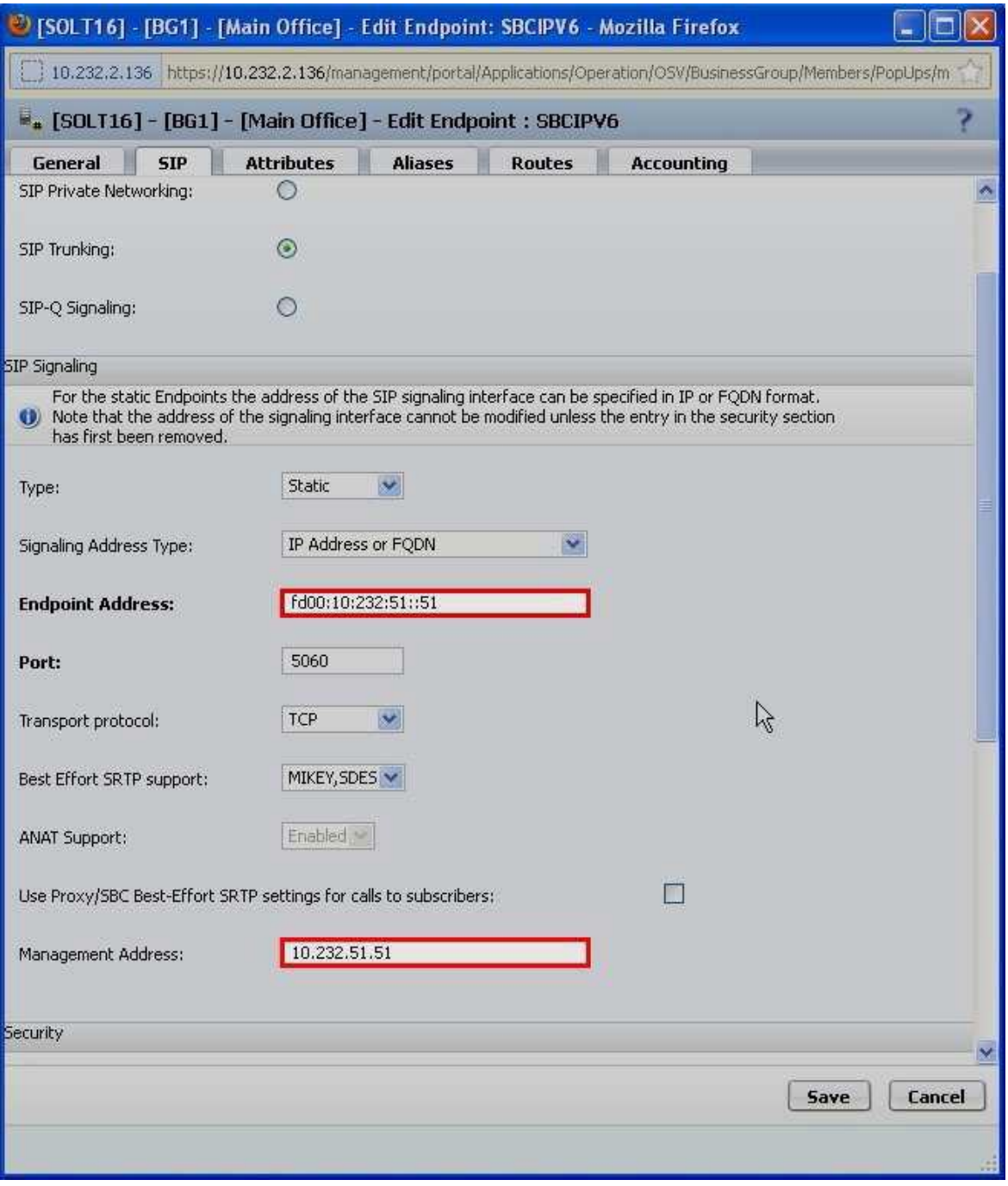
OS-SBC Core or Inside Network Interface

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.

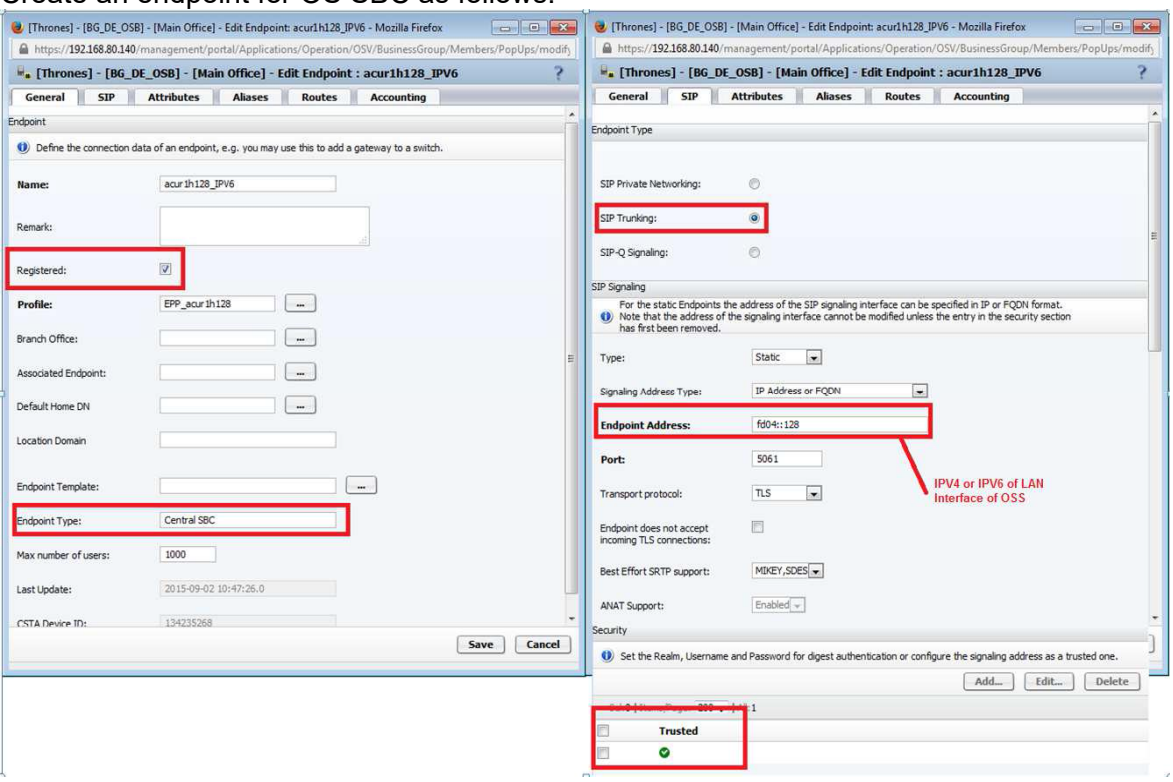
If OS-SBC core side uses 1Pv6 network then in the OSV you create your endpoint using 1Pv6 address. This requires you add management 1Pv4 address in order to manage OS-SBC from CMP.

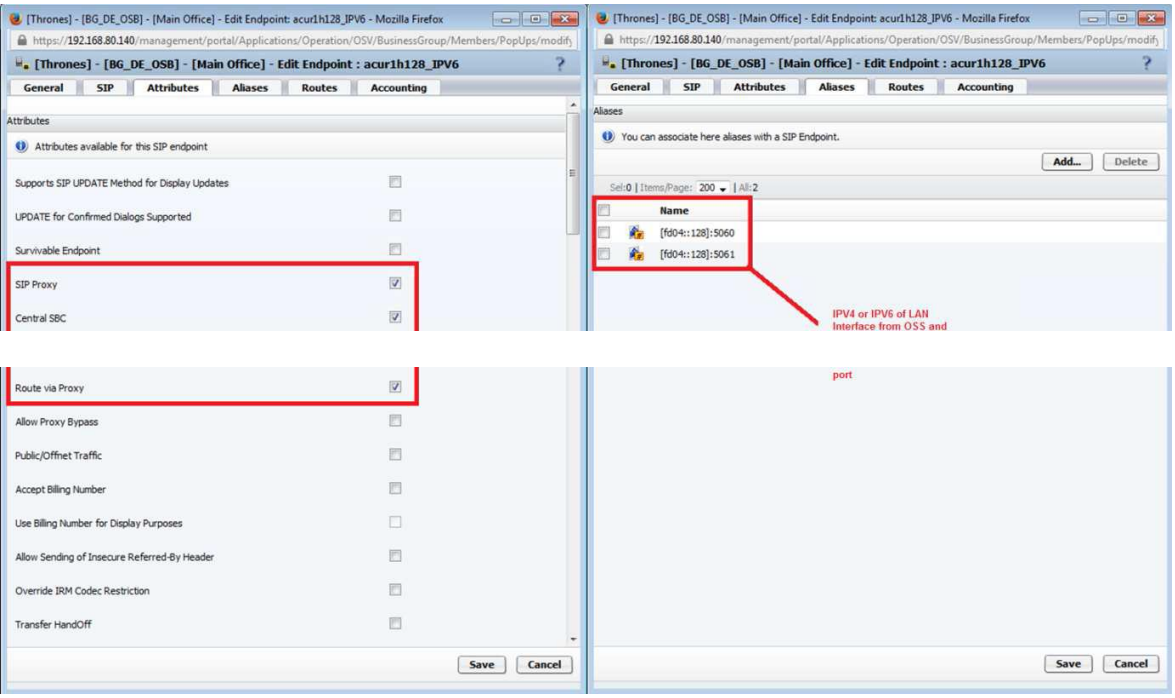


OS-SBC IPv6 Support for hosted branch offices configuration

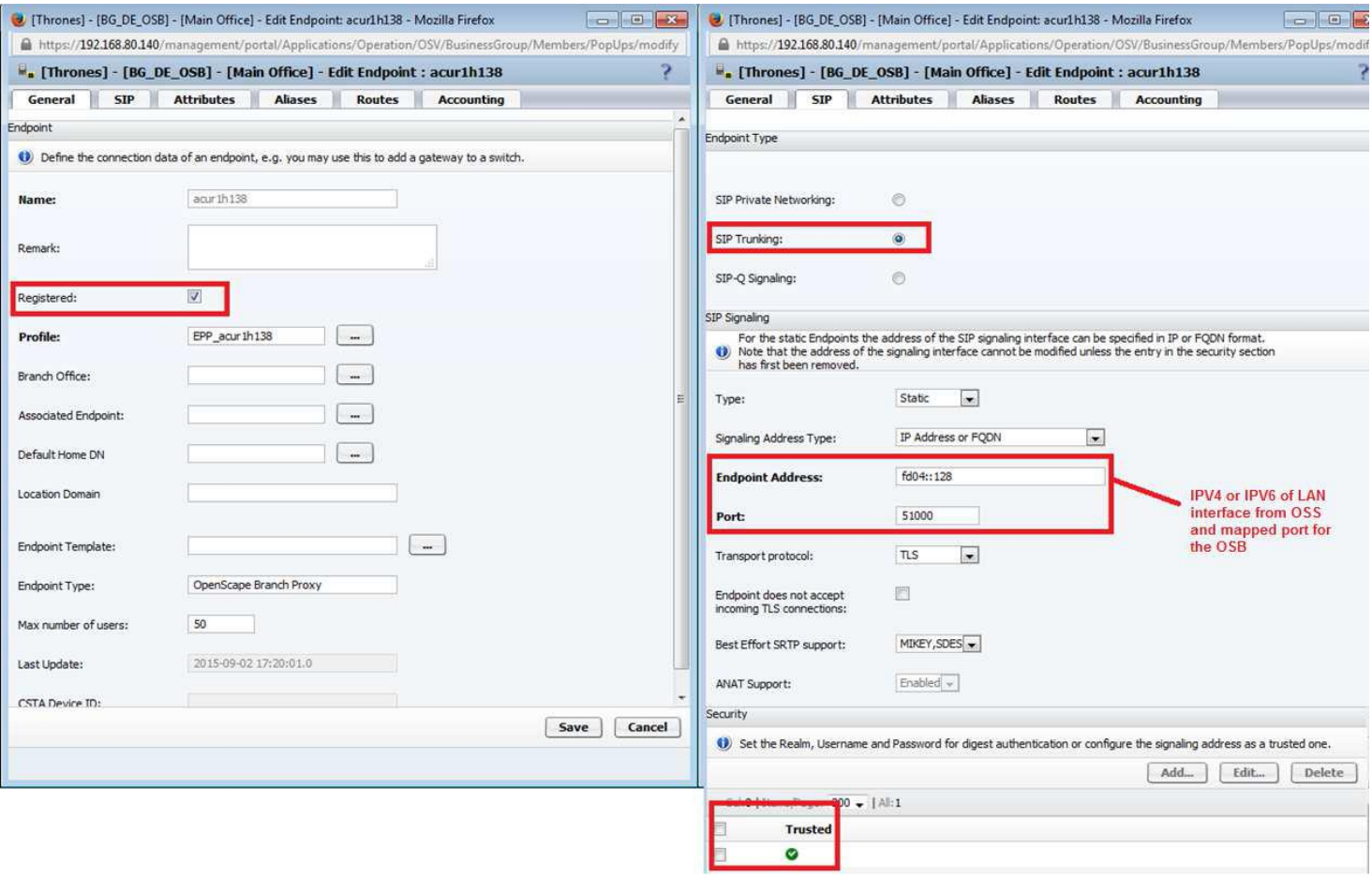
OSV configuration

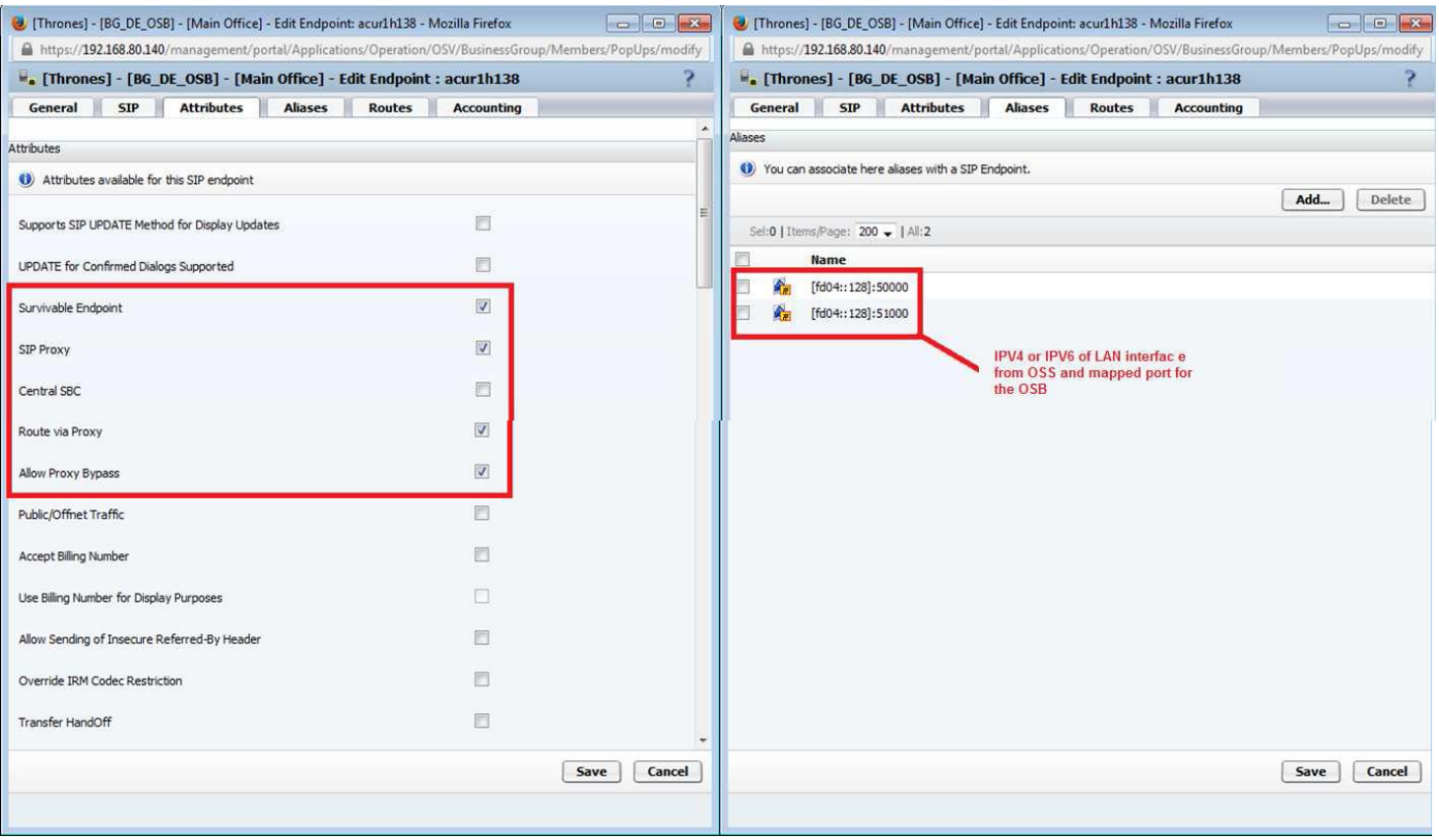
Create an endpoint for OS SBC as follows:



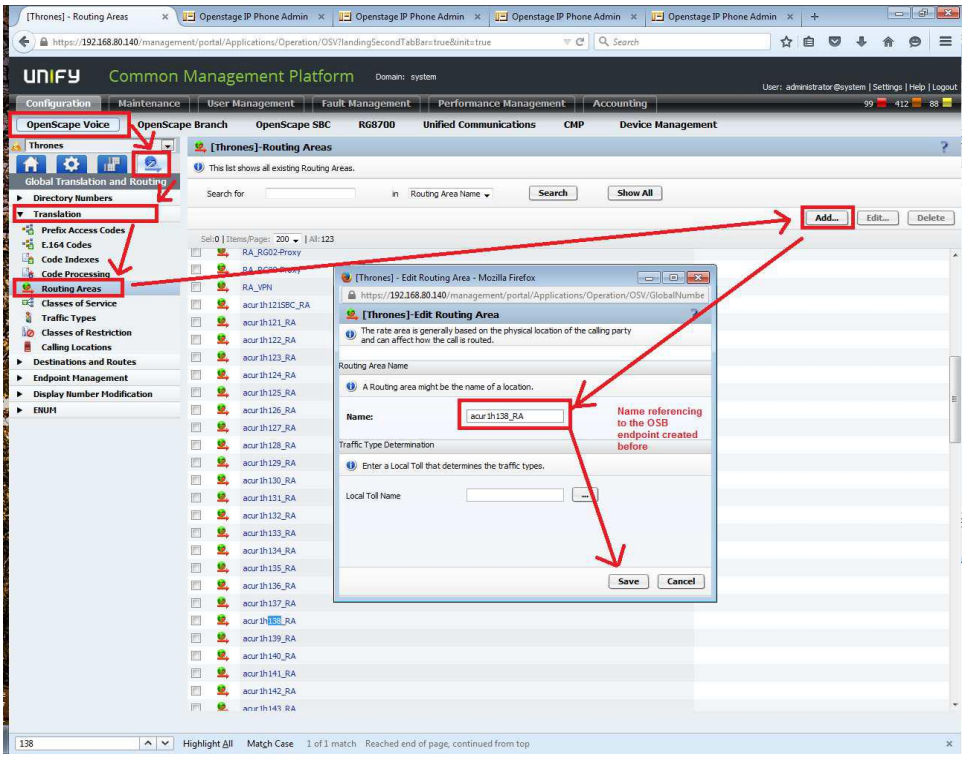


Create an endpoint for OSB as follows:

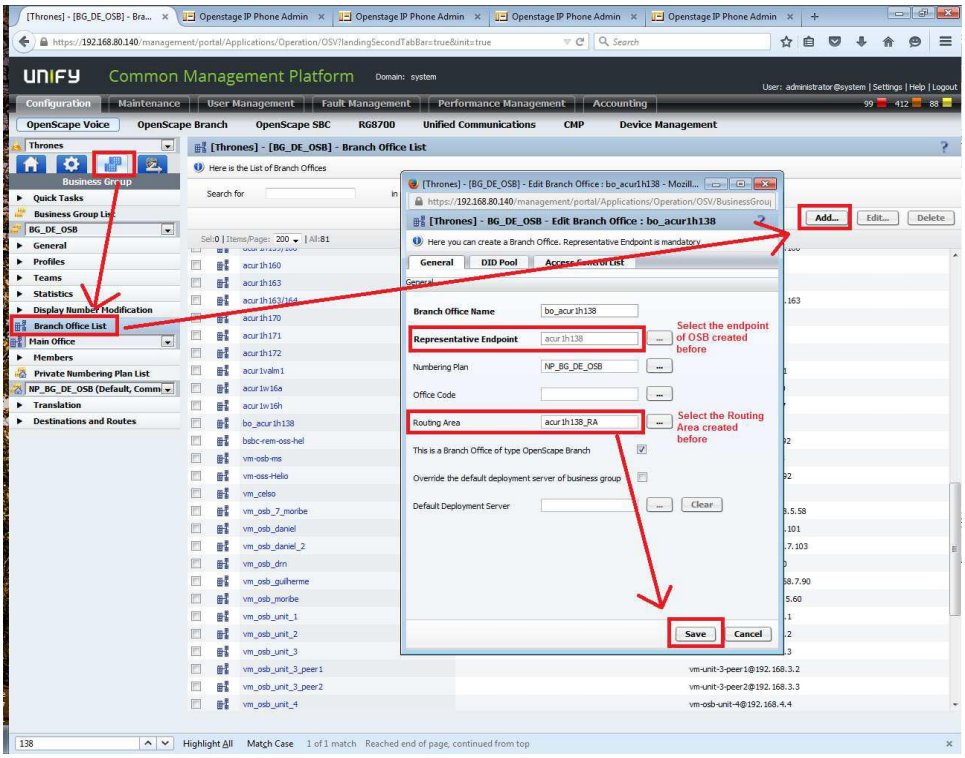



[Thrones] - [BG_DE_OSB] - [Main Office] - Edit Endpoint: acur1h138 - Mozilla Firefox
https://192.168.80.140/management/portal/Applications/Operation/OSV/BusinessGroup/Members/PopUps/modify
[Thrones] - [BG_DE_OSB] - [Main Office] - Edit Endpoint : acur1h138
General
SIP
Attributes
Aliases
Routes
Accounting
Attributes
Attributes available for this SIP endpoint
Supports SIP UPDATE Method for Display Updates
UPDATE for Confirmed Dialogs Supported
Survivable Endpoint
SIP Proxy
Central SBC
Route via Proxy
Allow Proxy Bypass
Public/Offnet Traffic
Accept Billing Number
Use Billing Number for Display Purposes
Allow Sending of Insecure Referred-By Header
Override IRM Codec Restriction
Transfer HandOff
Save
Cancel
[Thrones] - [BG_DE_OSB] - [Main Office] - Edit Endpoint: acur1h138 - Mozilla Firefox
https://192.168.80.140/management/portal/Applications/Operation/OSV/BusinessGroup/Members/PopUps/modify
[Thrones] - [BG_DE_OSB] - [Main Office] - Edit Endpoint : acur1h138
General
SIP
Attributes
Aliases
Routes
Accounting
Aliases
You can associate here aliases with a SIP Endpoint.
Add...
Delete
Sel:0 | Items/Page: 200 | All:2
Name
[fd04::128]:50000
[fd04::128]:51000
IPV4 or IPV6 of LAN interfac e from OSS and mapped port for the OSB
Save
Cancel

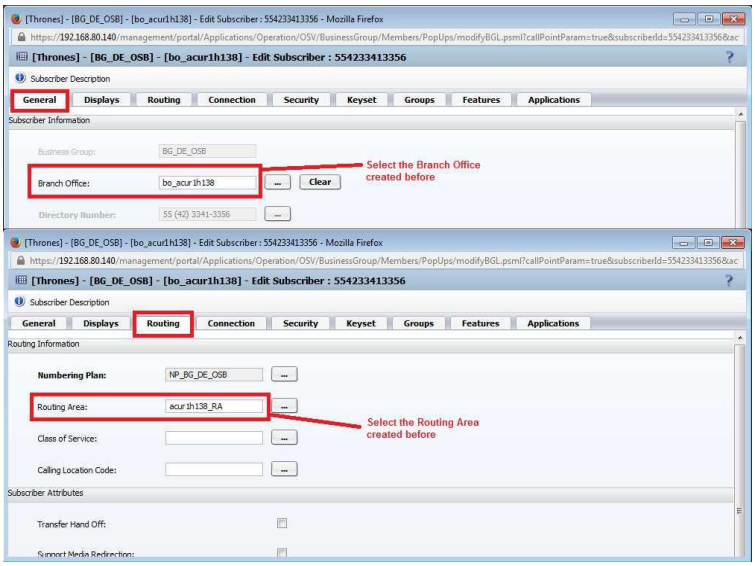
Create a Routing Area for the OSB endpoint



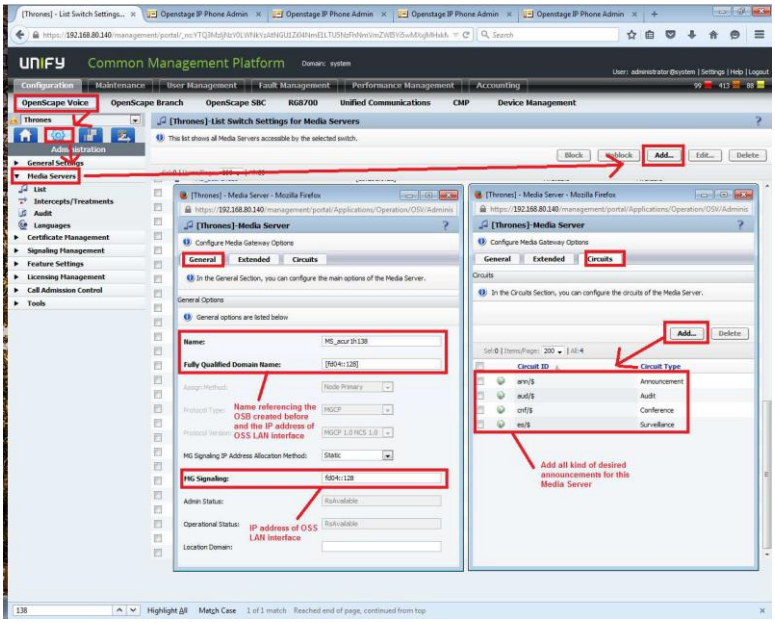
Create a Branch Office for the OSB



Create the subscribers

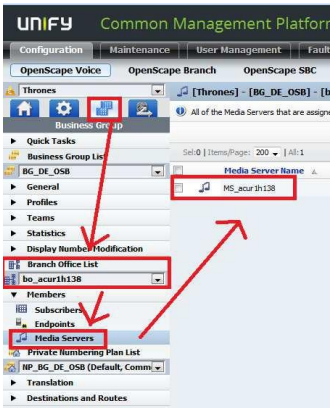


Create the Media Server for the Branch



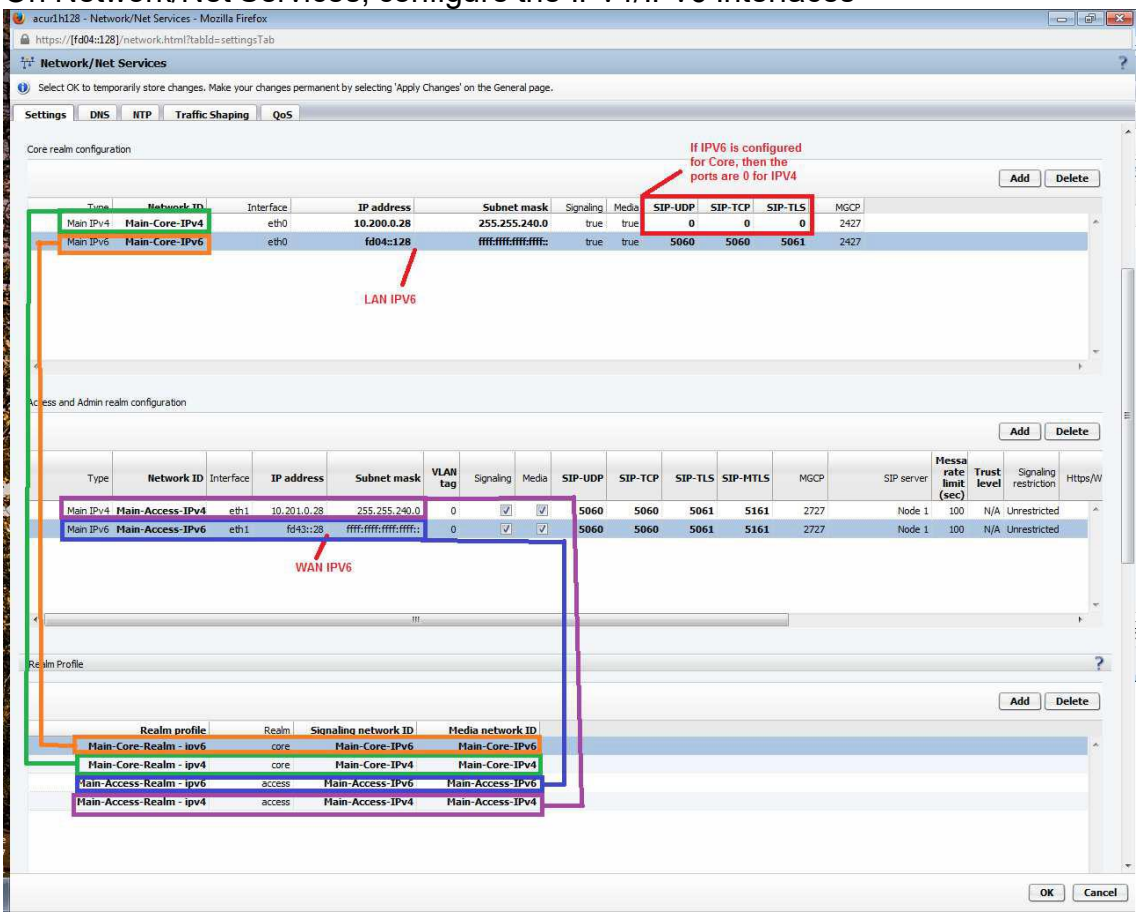
Don’t forget to unblock the Media Server

The Media Server will be assigned to the Branch Office created before



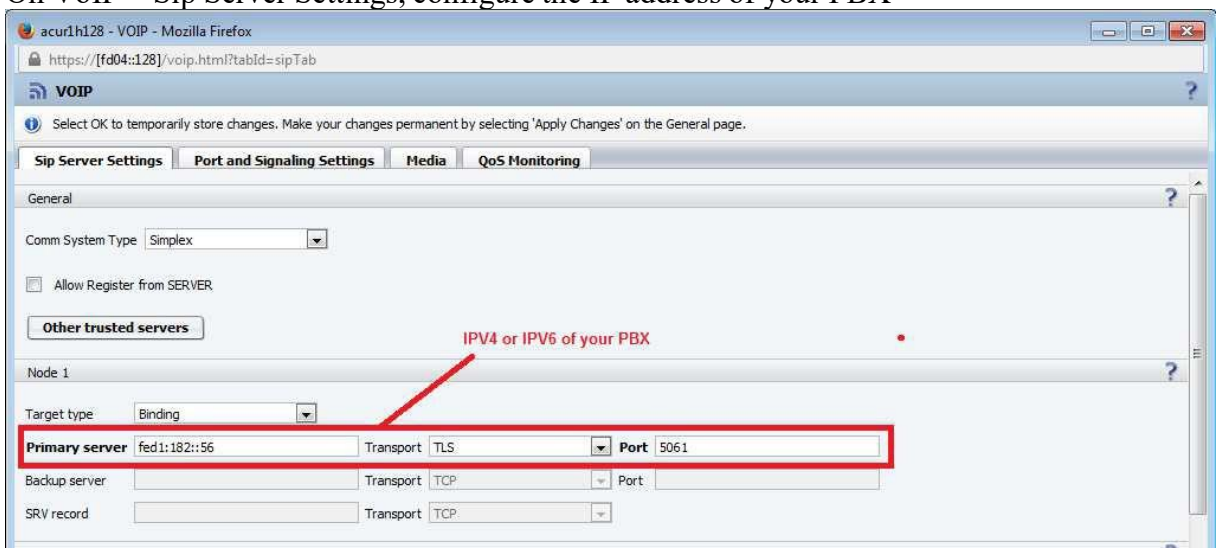
OS SBC Configuration

On Network/Net Services, configure the IPv4/IPv6 Interfaces

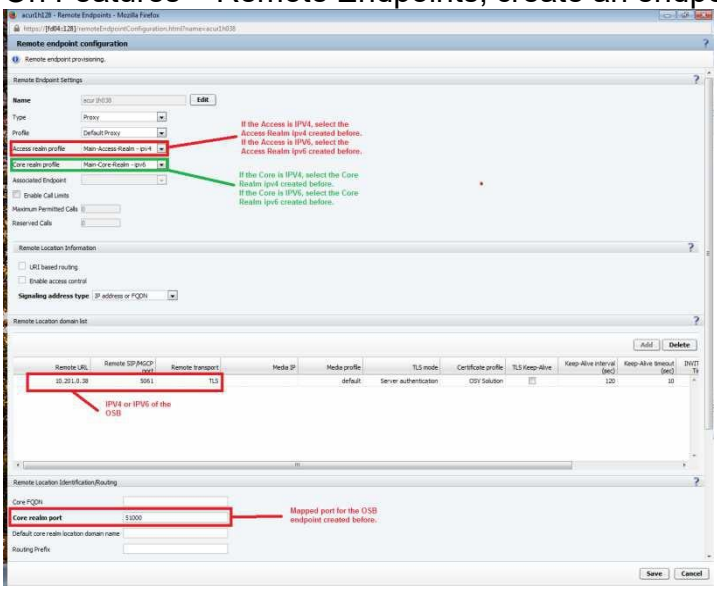


Don’t forget to set the Default Gateway IPV4/IPV6

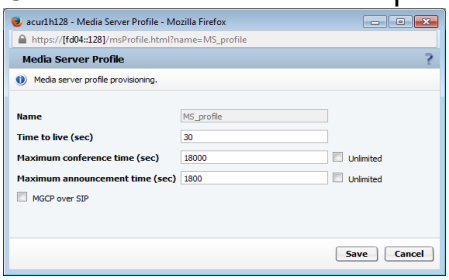
On VoIP > Sip Server Settings, configure the IP address of your PBX



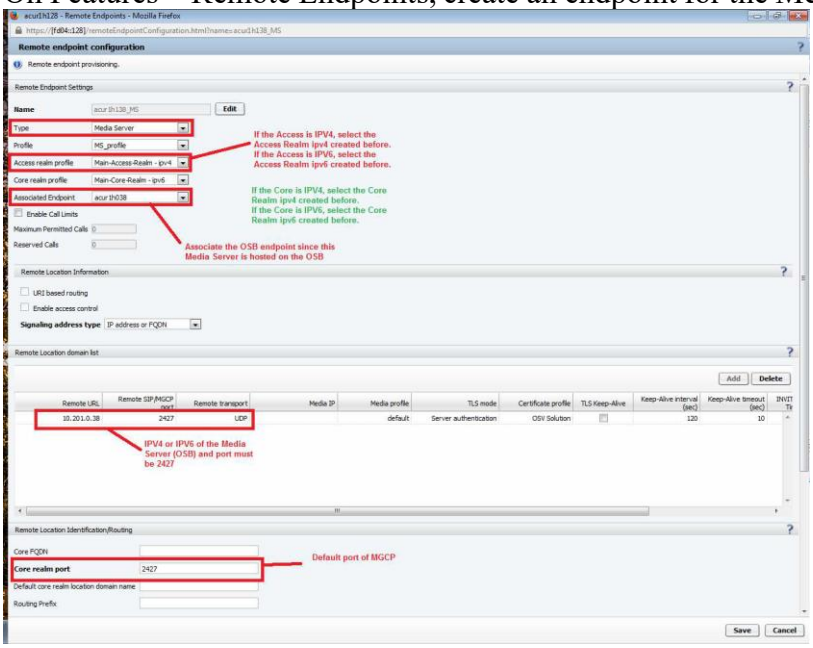
On Features > Remote Endpoints, create an endpoint for the OSB



On Features > Remote Endpoints, create a Media Server profile



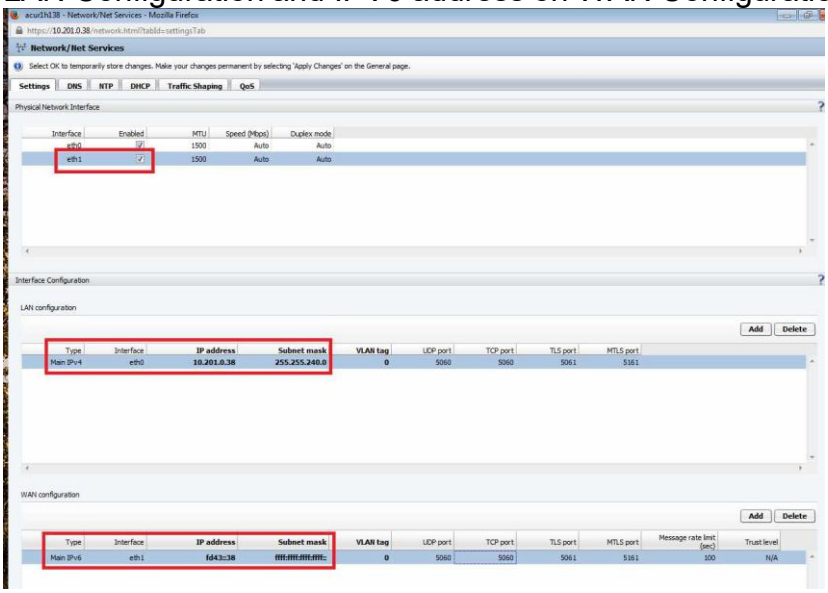
On Features > Remote Endpoints, create an endpoint for the Media Server



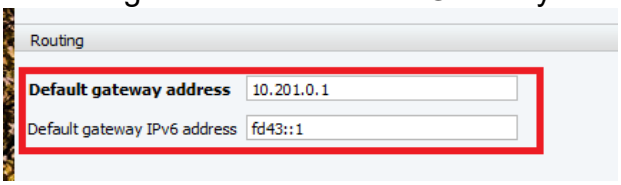
Apply the configuration, a reboot may be required.

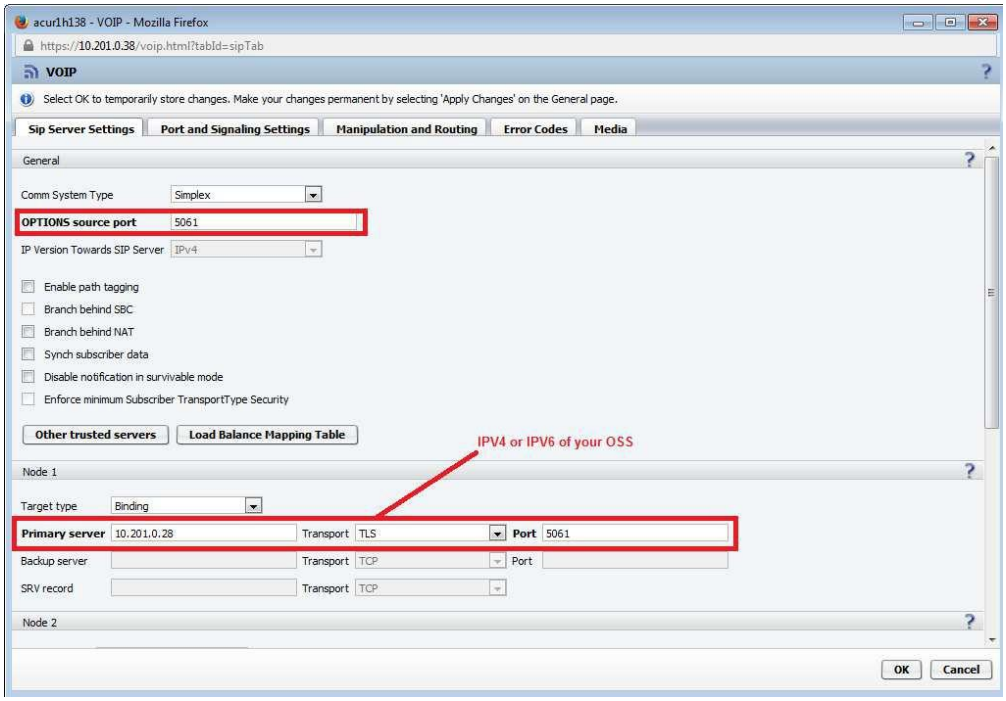
1.1.3.3 OSB Configuration

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



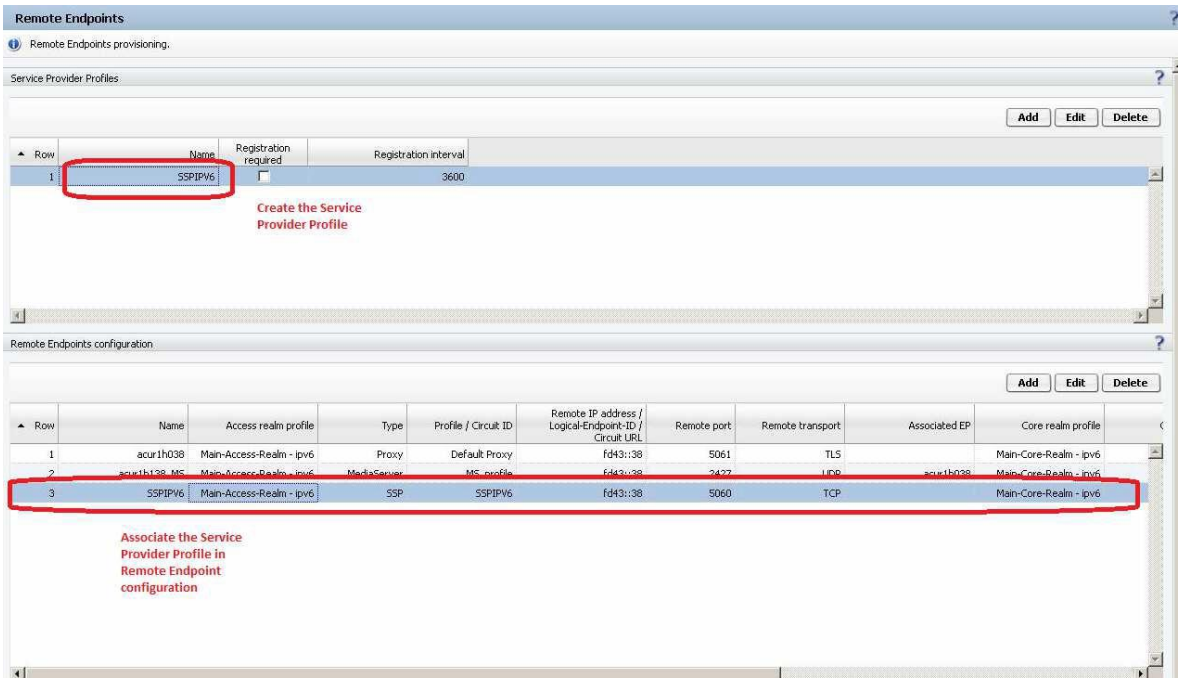


On Features, check the flag Enable Media Server.

Apply the configuration, a reboot may be required.

1.1.4. OS SBC with SIP Server Provider using IPv6

The OpenScape 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 propogated 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	OpenScape 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	r Name	Selectio n	Endpoint LAN IP	LAN Netmask	LAN Default GW
13145441010			10.232.65.212	255.255.255.0	10.232.65.1

M (SBC)	M (SBC)	M (SBC)				
			SBC relevant only			
	WAN	WAN	SIP Service	(SSP)	SSP IP	SSP SIP

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	Provider Name	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)					
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.

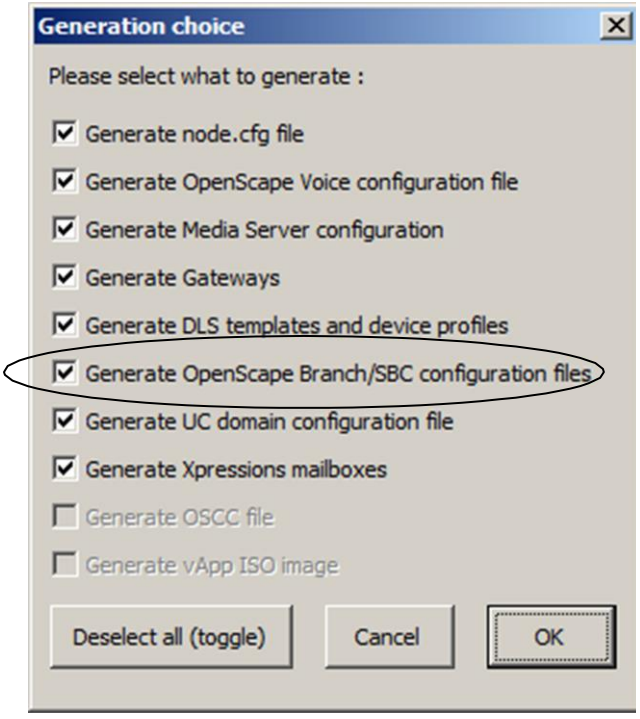
For remote subscribers, the phone must be configured with the WAN IP address of the SBC for the phones SIP Server Address and the SIP Registrar Address. The CDC Tool will provide the necessary DLS profiles with the preconfigured address information.

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.

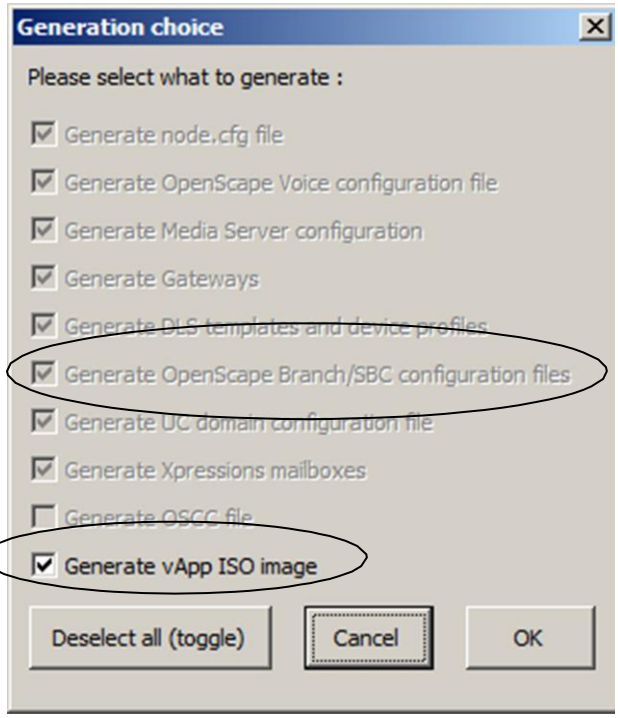
To generate all the configuration files, including the OSV data, DLS profiles, and SBC Configuration file, select the Std Site sheet and select the "Generate All Configuration Files". The following box appears (if Std Solution deployment architecture is used):



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 a 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 ae 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 unit 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.

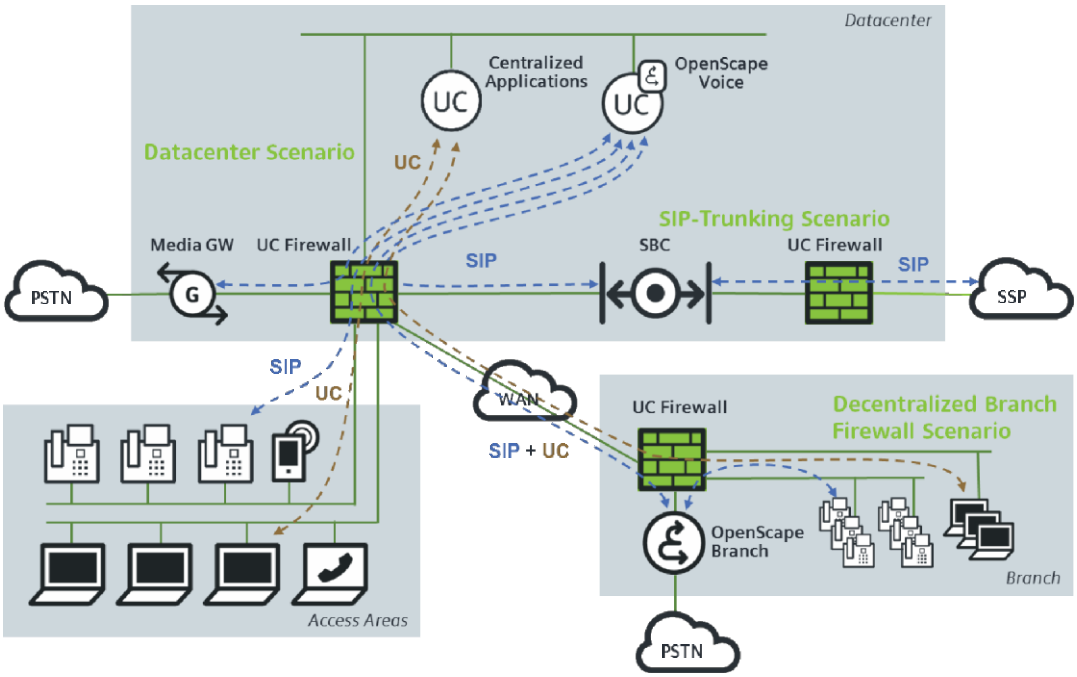


Figure 1: General overview

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 notes[1]

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 Firewall[3].

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-VoIP-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 ine
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.

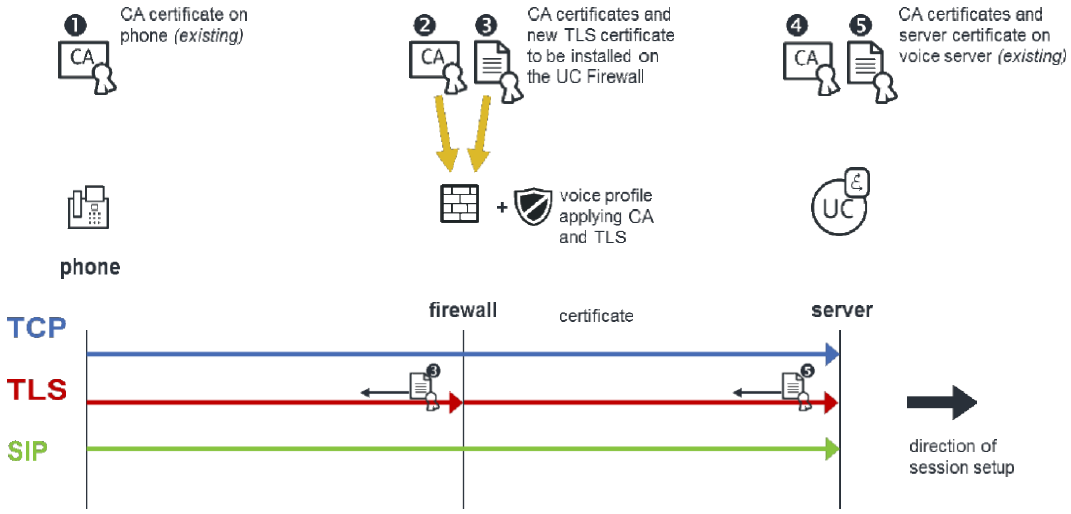


Figure 2: Firewall integration for TLS with certificates

Certificate assignment and usage within the TLS connection:

- CA certificate to verify presented server certificate .
- CA certificates to verify presented server certificate and to be included into the certificate chain of on presenting to client. All CA certificates of the chain need to be imported into the FortiGate.
- 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.

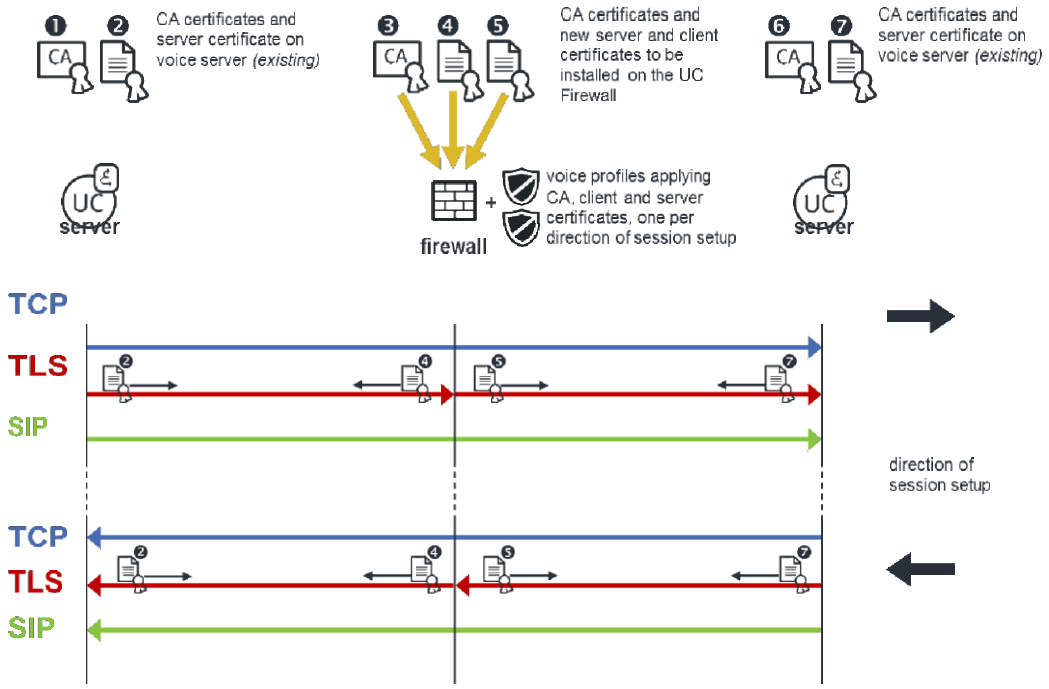


Figure 3: Firewall integration for TLS with certificates

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 manual[4].

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 reestablished[5].

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 FD31530[6].

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
```

```
            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” extents 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
```

```
                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
```

```
            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 been 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 manual[8]. 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 constrains 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*

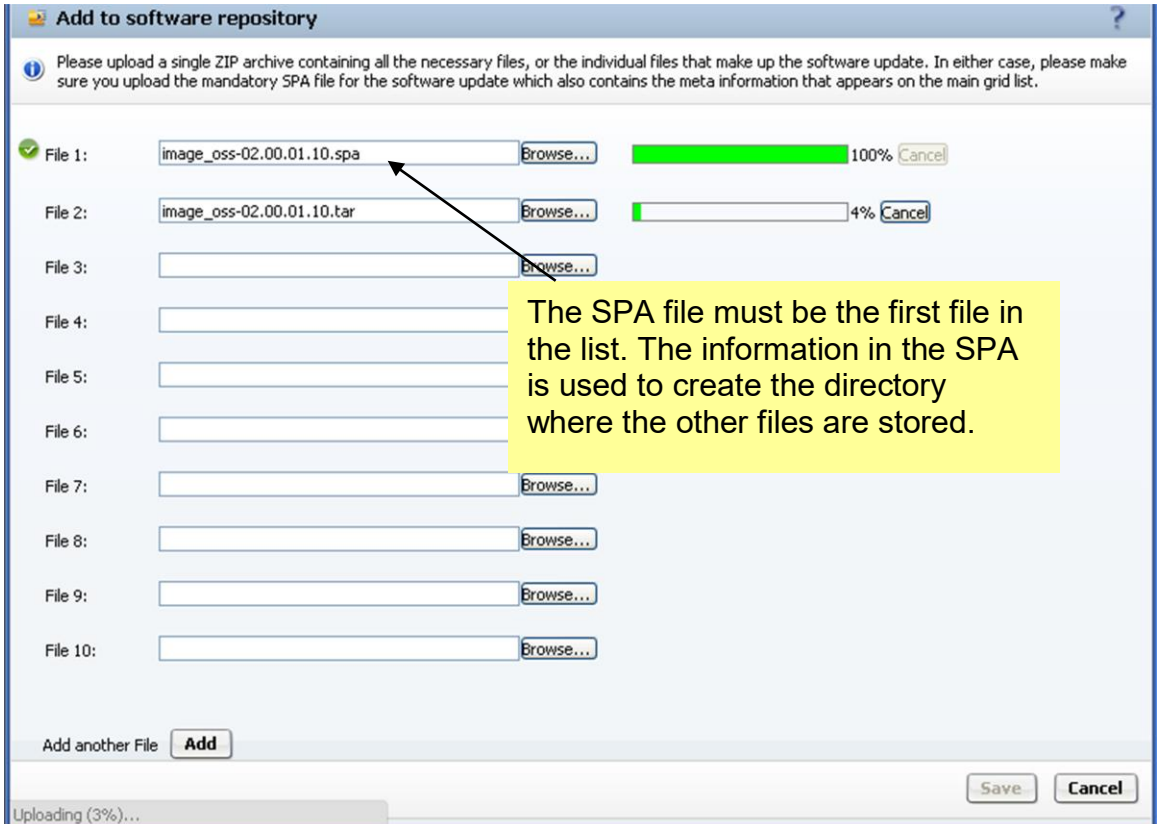
ALG	Application Layer Gateway
ASIC	Application Specific Integrated Circuit
CLI	Command Line Interface CorNet
	“Corporate Network” protocol DLS
	Deployment Service
DSCP	Differentiated Services Code Point
FGCP	FortiGate Cluster protocol
HA	High-Availability
HTTP	Hypertext Transfer Protocol
HTTPS	TLS secured 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

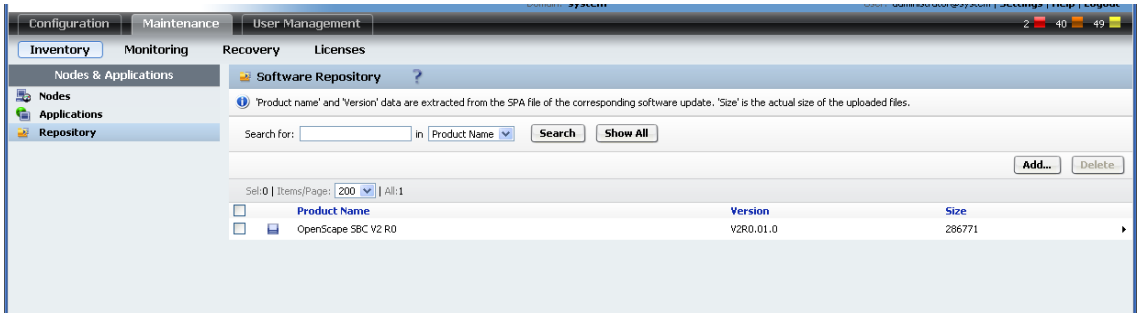
Simplified Installation

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.



When all selected files are uploaded, the “save” button will become active. Click on “save” to complete the upload process.



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)	• Generic sw used to perform loading, may not be final sw load on the appliance	• 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)

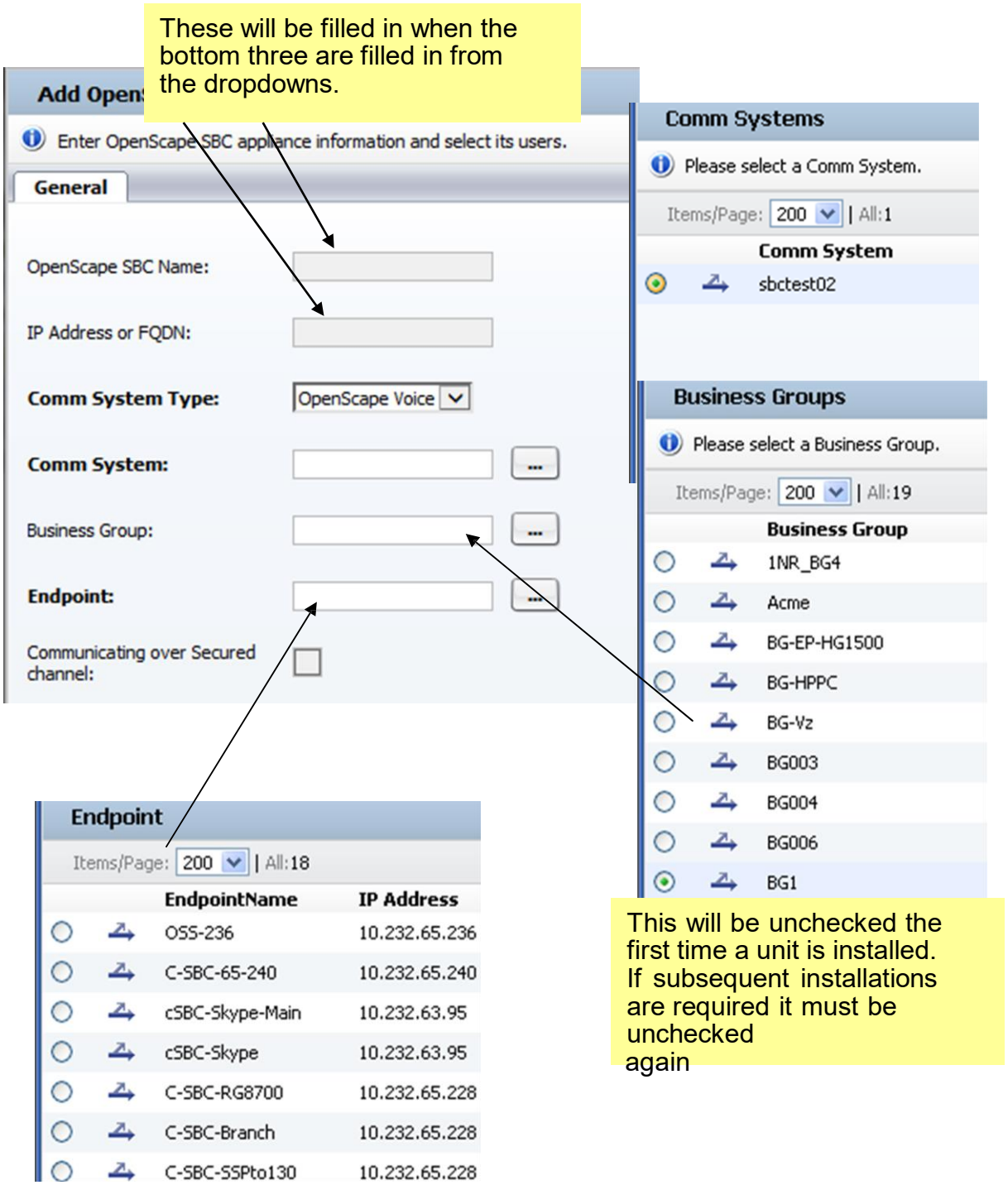
Create the EndPoint for the OS-SBC.
CMP-> Configuration->OpenScape Voice-><business group>-><main Office>->Endpoints->Add

Data is required on the General, SIP, Attributes and Aliases tabs.

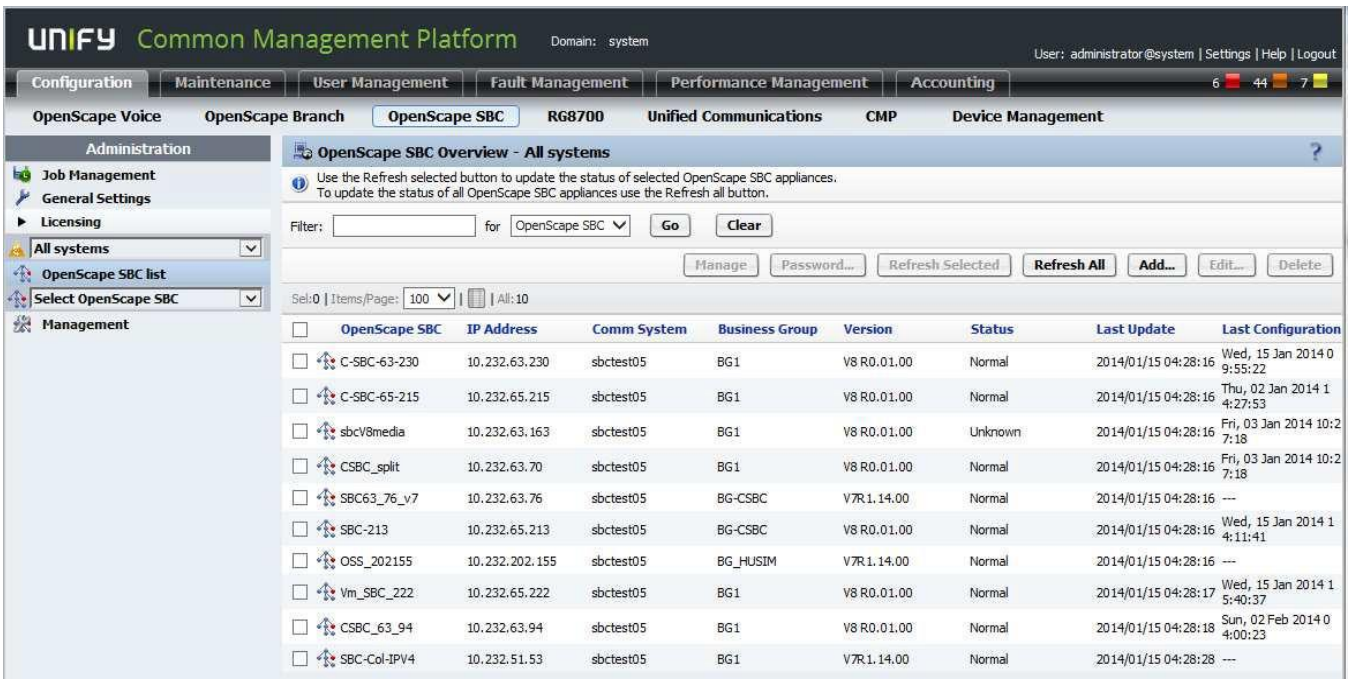
It is necessary that the “Endpoint Template” of “Central SBC” be selected. This will cause the “Endpoint
Type” to be set to “Central SBC”.

Add the OS-SBC to the OpenScape SBC list

CMP->Configuration->OpenScape SBC->OpenScape SBC list->Add



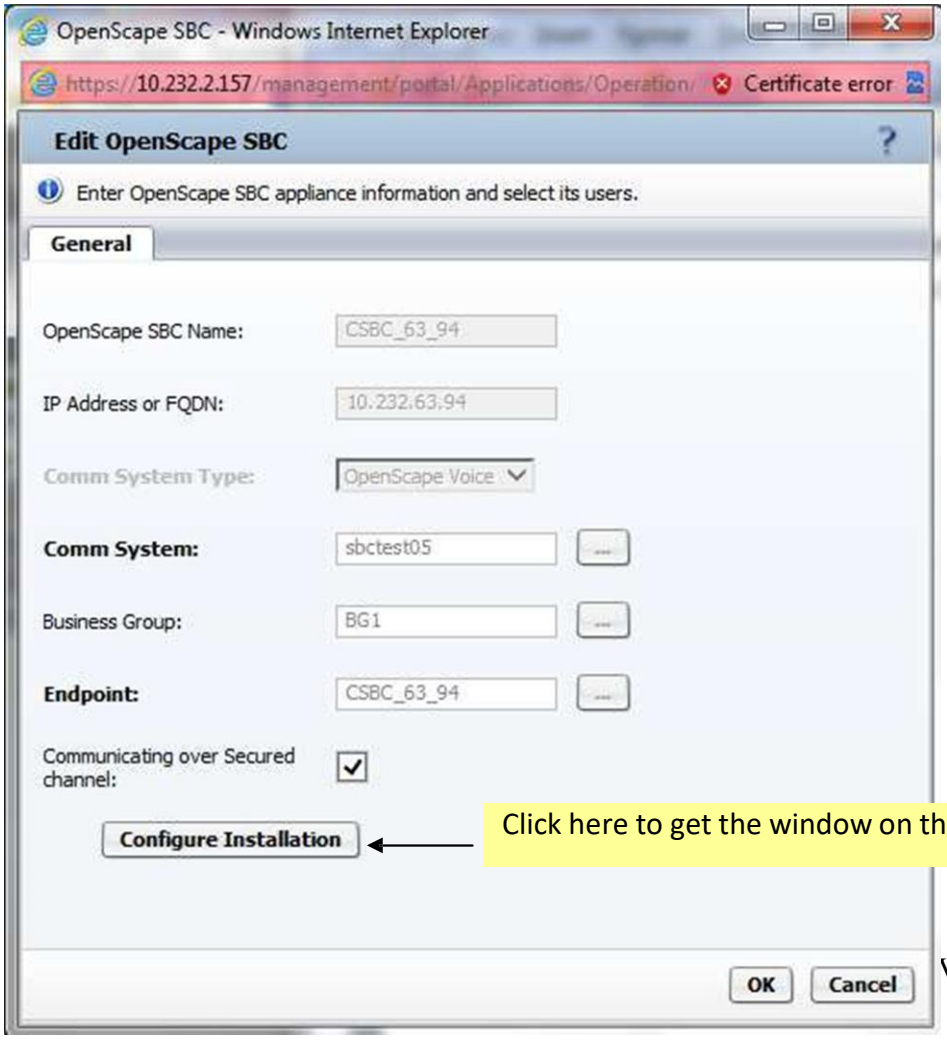
When you click “OK” the OS-SBC will then be added to the “OpenScape SBC list” as shown on the next page.

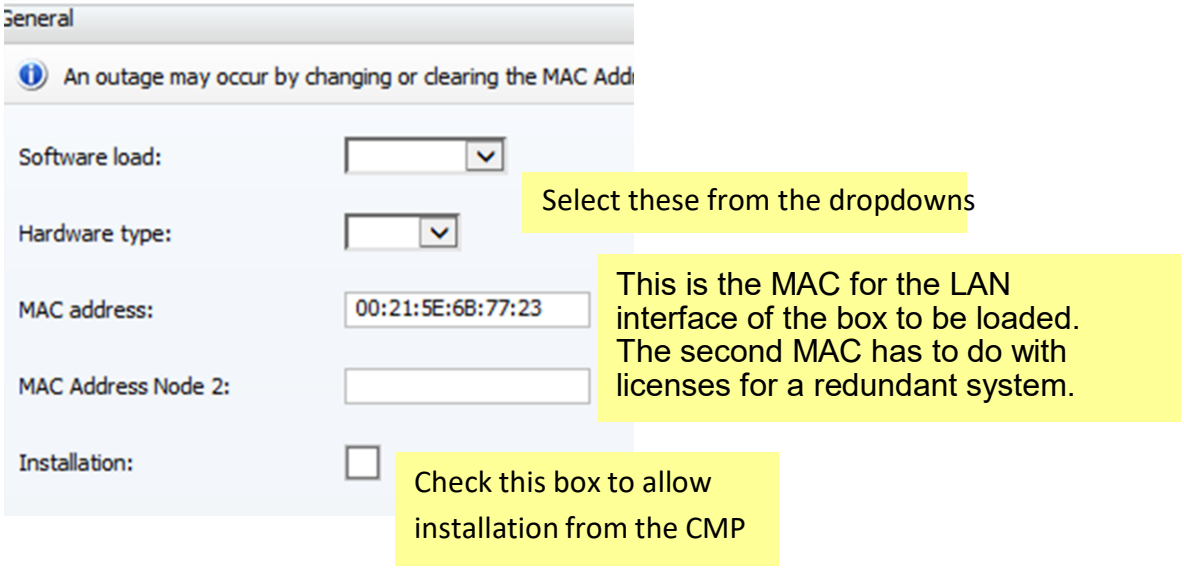


Select the checkbox to the left of the OS-SBC and click on “Edit” to open the next window.

Edit the configuration data for the OS-SBC

CMP->OpenScape SBC->OpenScapeSBC list-> select the OS-SBC and Click Edit





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 Bracnh 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)	• Generic sw • Branch/OS-SBC Logical ID	• Logical ID pre-configured in CMP • Use temporary dynamic IP from DHCP for OSB • Fetch 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

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-\I\/Orking unit, while keeping the same logicaiiD, 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)	• Generic sw • Branch/OS-SBC Logical ID • CMP URL	• 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/V3 the “Partitioned USB” flag must be marked, otherwise Lenovo SR250/SR250 V2 will noot 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	• Generic sw • Xml config file	• 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.

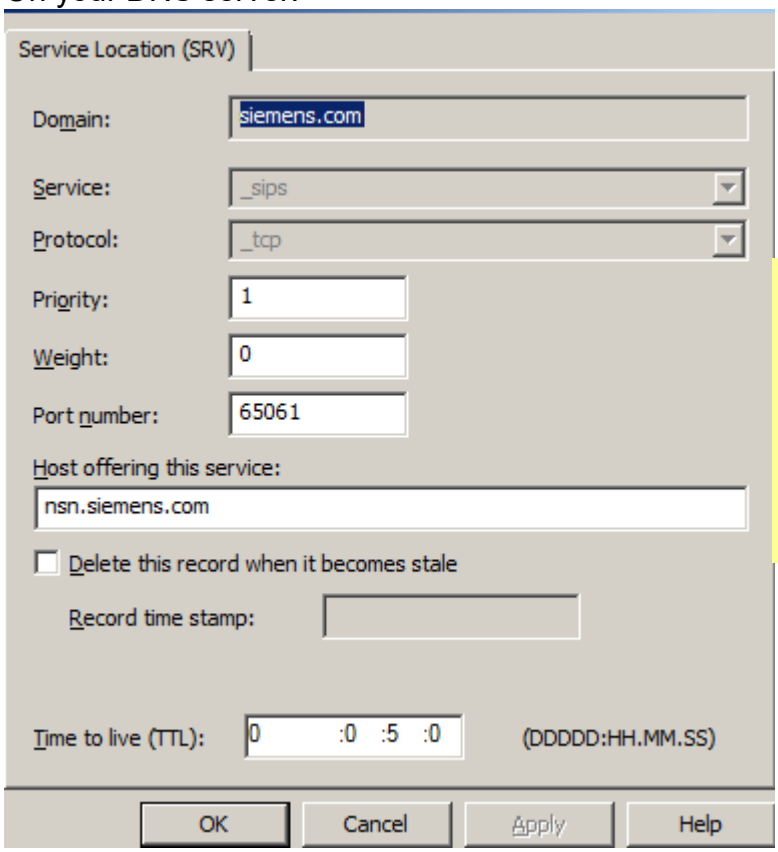
10. Delete node 1 from the OpenScape SBC assistant
11. Delete node 2 from the OpenScape SBC assistant
12. Delete node 1 from the OSV (prevent OSV from sending options to this IP address)
13. Delete node 2 from the OSV (prevent OSV from sending options to this IP address)
14. Create endpoint for the redundant 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.

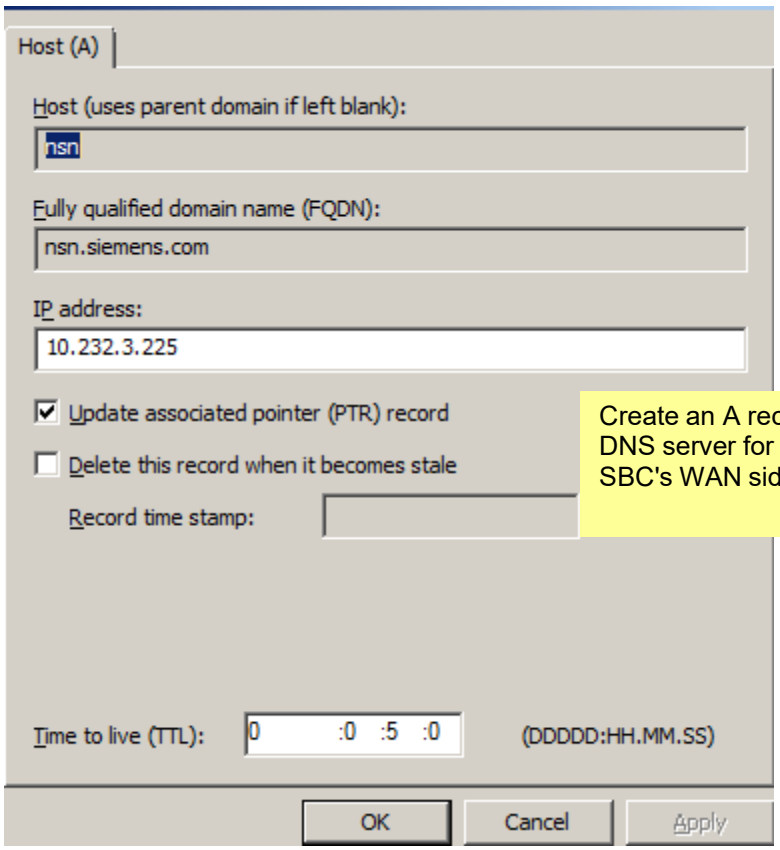
16 Configuring DNS SRV for TLS phones

Refer to the following configurations to set up DNS SRV with PHONES using TLS.

On your DNS server:

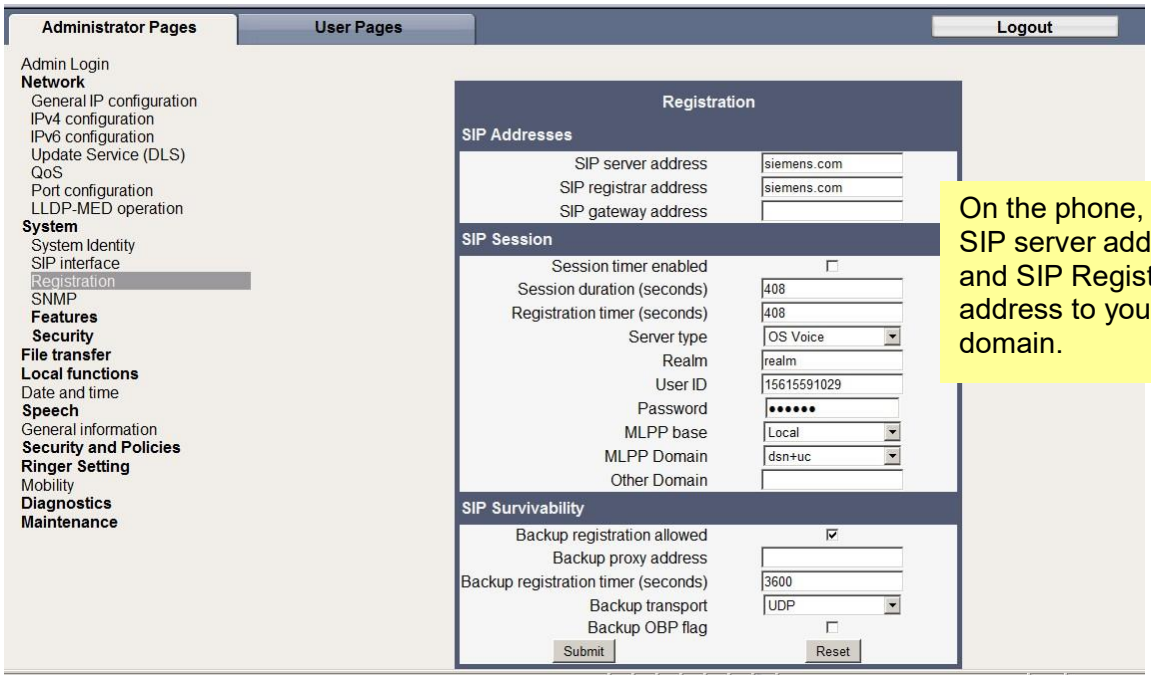


Create DNS SRV Record in your zone (siemens.com) for Service "_sips" using Protocol "_tcp" and provide a FQDN for the WAN side of your SBC (nsn.siemens.com) and the SBC WAN side Listening port (65061).

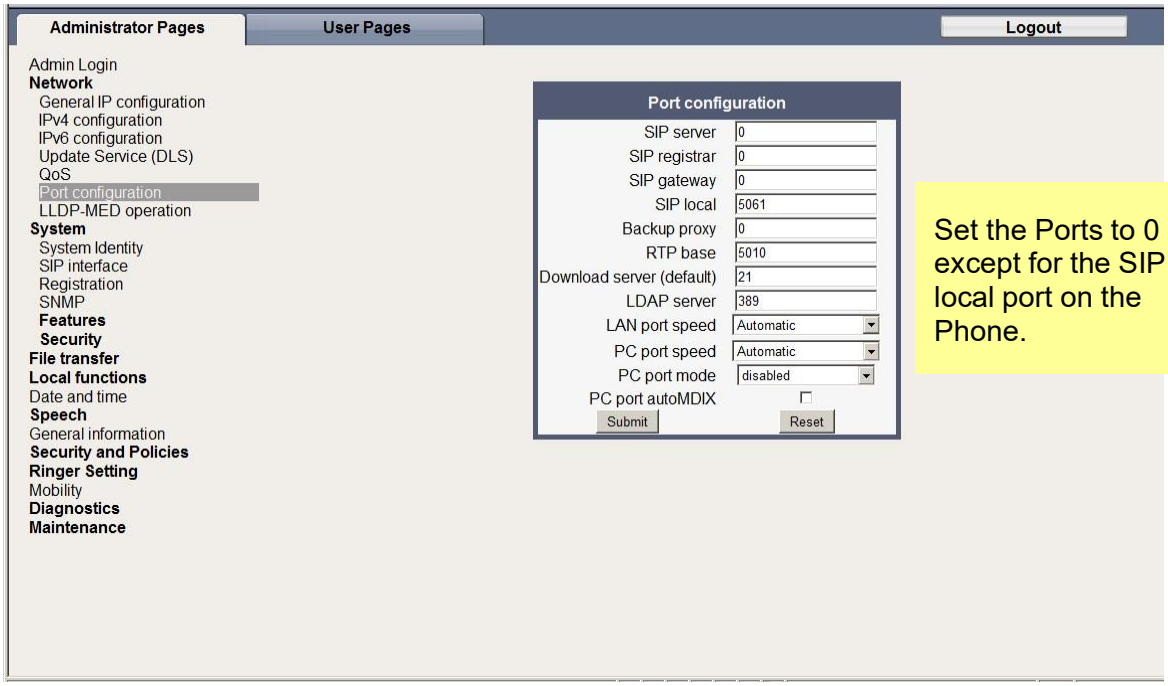


Create an A record entry in the DNS server for the FQDN of your SBC's WAN side.

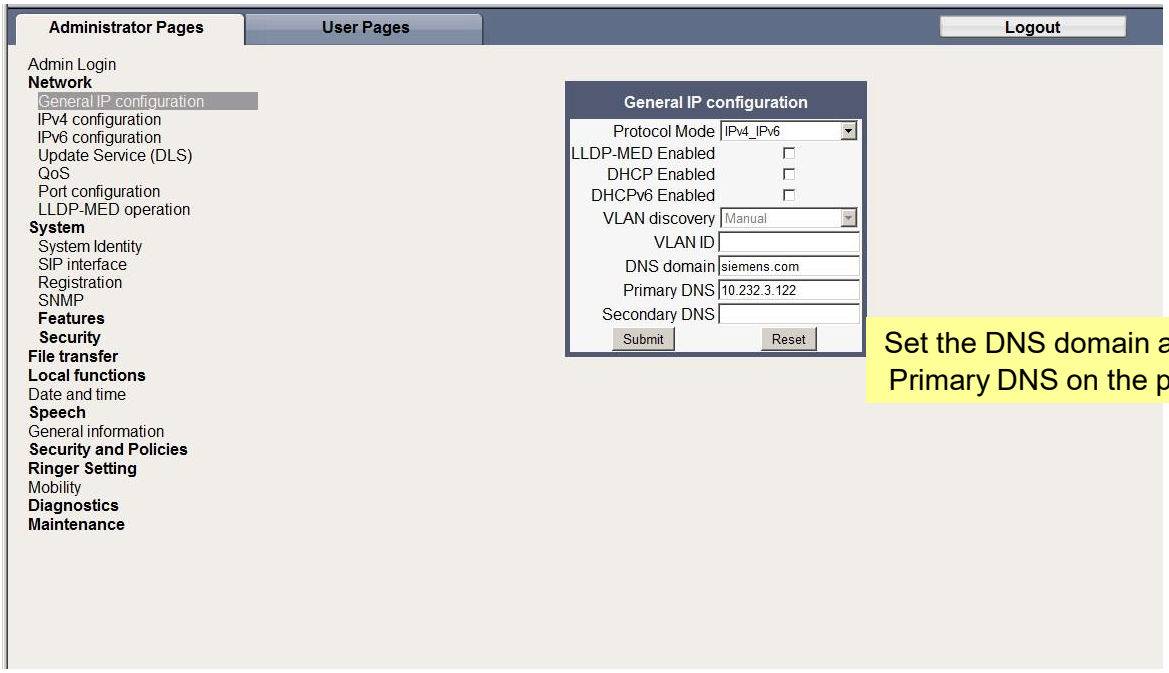
On each phone using administrator privileges:



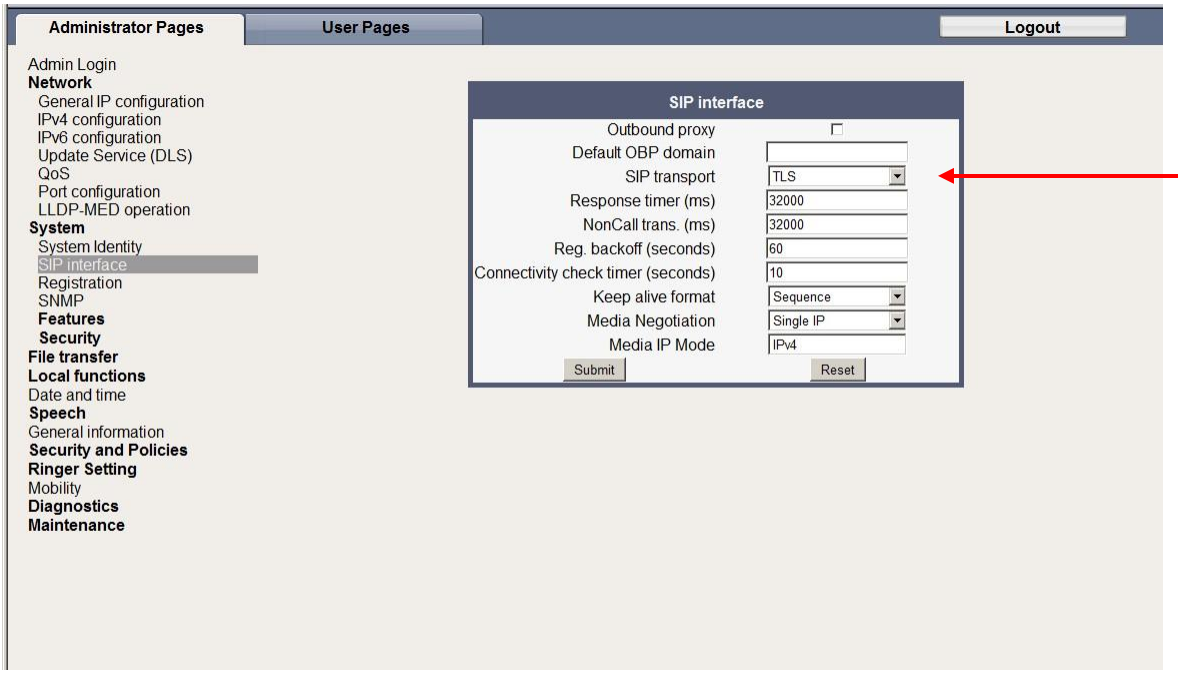
On the phone, set the SIP server address and SIP Registrar address to your domain.



Set the Ports to 0 except for the SIP local port on the Phone.



Set the DNS domain and Primary DNS on the phone.



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 Configuring DNS NAPTR

NAPTR records include fields such as Order, Preference, Flags, Service, Regexp etc. These fields guide the client in modifying the domain name and determining the next DNS record type to query, typically an SRV record.

> **Important**: **DNS NAPTR** is available starting from V11R2.

To create a new NAPTR record, go to your DNS server page, right-click, select **Other New Records**, choose **NAPTR**, and click **Create Record**.

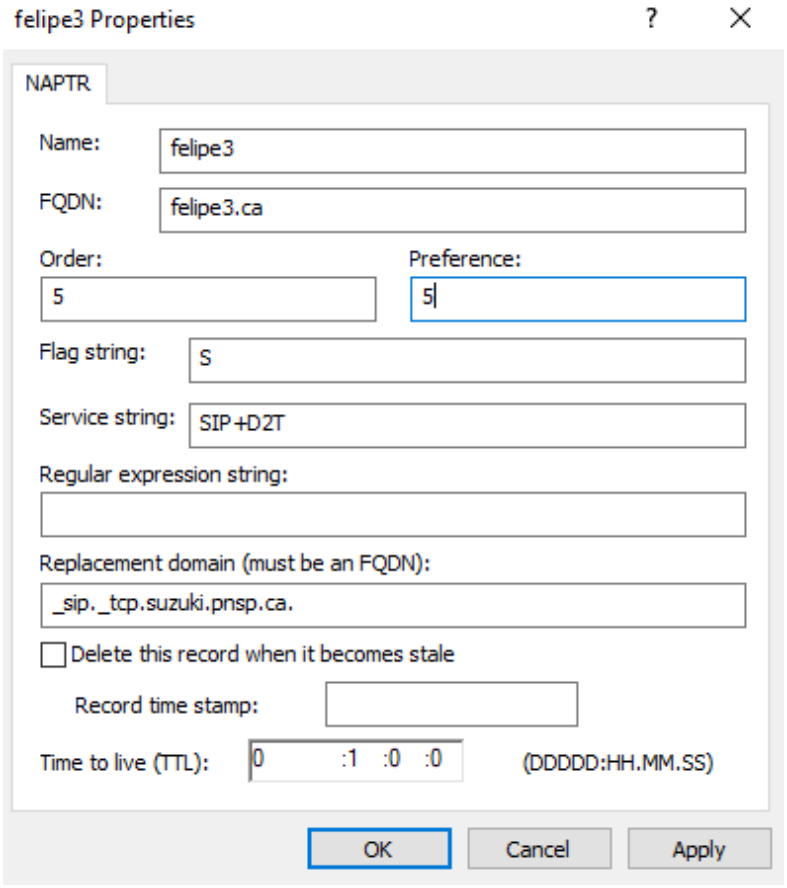
> **Prerequisite**: DNS NAPTR is enabled (Go to **Remote endpoint** > **Remote location information**: from the **Signaling Address Type** dropdown menu, select **DNS NAPTR**).

Configuring the **Order** field determines the sequence in which NAPTR records will be processed. Lower values have higher priority. If multiple records have the same order, the **Preference** field determines which should be selected by prioritizing the record with the lowest value.

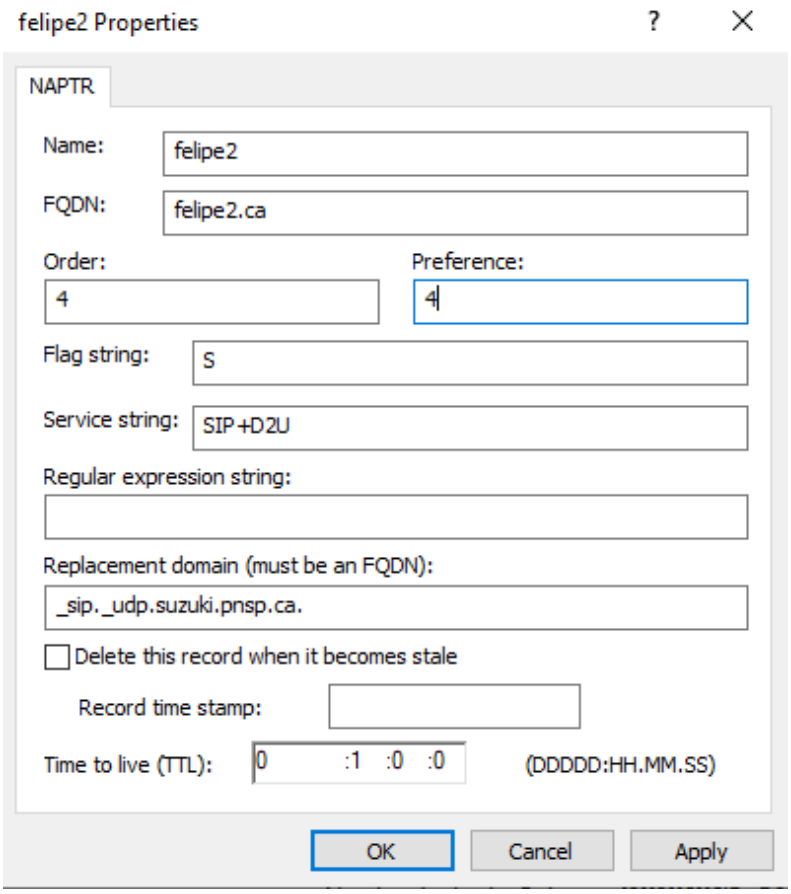
The **S Flag string** indicates that the next action should be to look up SRV records. The **Services** string specifies the service of the protocol (for example, SIP+D2T).

The **Regular Expression string** is mutually exclusive with the **Replacement Domain** field; you can choose only one, and the other must be empty to allow the **Replacement Domain** to be used.

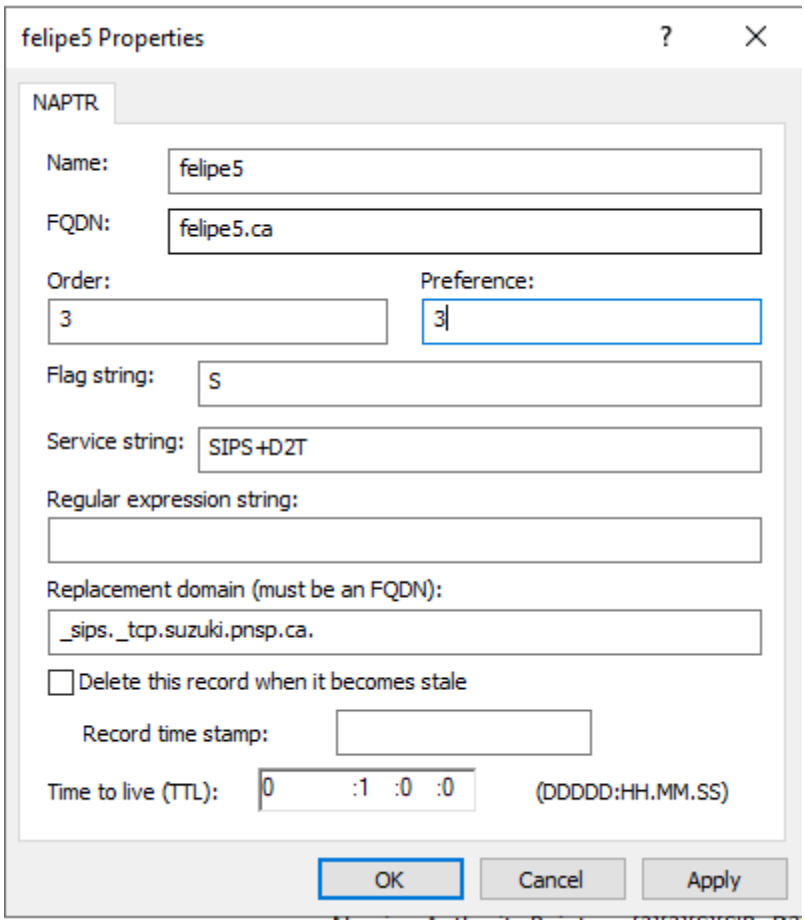
To configure a TCP NATPR record on DNS Server, refer to the example image below:



To configure a UDP NATPR record on DNS Server, refer to the example image below:



To configure a TLS NATPR record on DNS Server, refer to the example image below:



After configuring DNS NAPTR, create a new DNS domain name and add it to the DNS. Then, create a new SRV record pointing to the newly added domain.

17.1 Checking the NAPTR record works with SBC

Verify that the new NAPTR can be accessed by using the example command below:

```
kamcmd dns.lookup NAPTR <naptr_name>
```

The command returns the configured NAPTR values.

Check if the remote endpoint is stable:
`kamcmd osb_memdb.show remote_ep`

If the check is successful, you should be able to establish a call with NAPTR as the caller or the callee.

Note: Execute the tests in **all SBC modes**: OSV Mode, BYOT Mode, Cluster Mode, etc. Also, ensure you have created NAPTR records that resolve to all protocols (TCP, UDP and TLS).

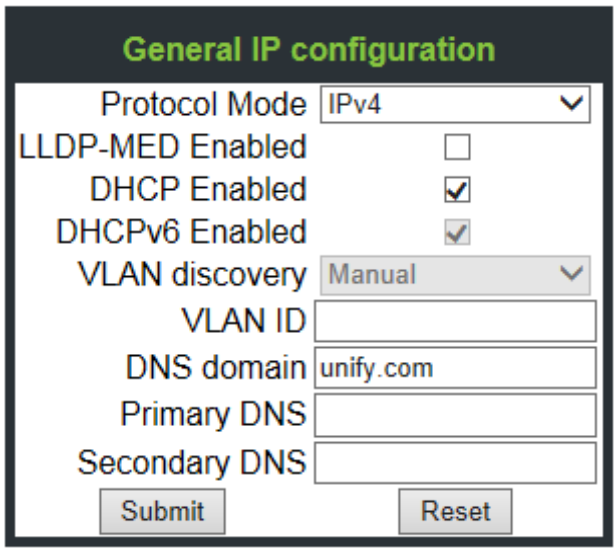
18 Configuration of location for emergency calls

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



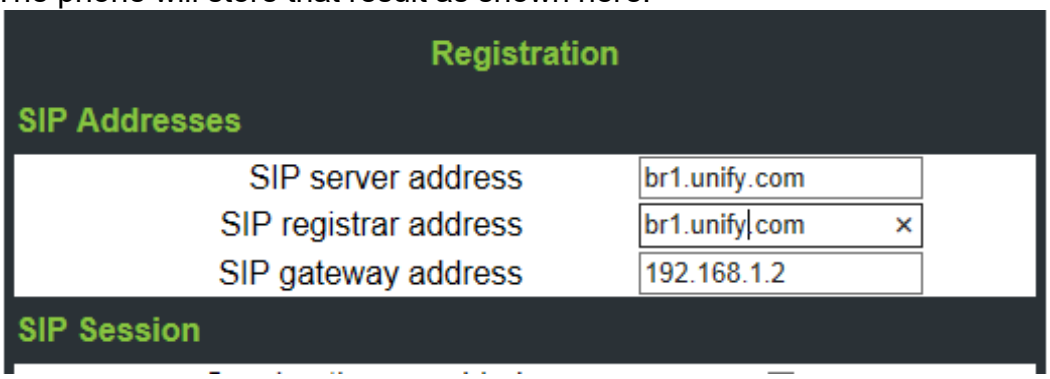
2. The DHCP server must support DHCP option 120
The DHCP server returns something like building1.unify.com per RFC 3361.

00 = the encoding for FQDN
03 = length of br1
627131 = br1
05 = length of unify
7563696679
03 = length of com

636F6

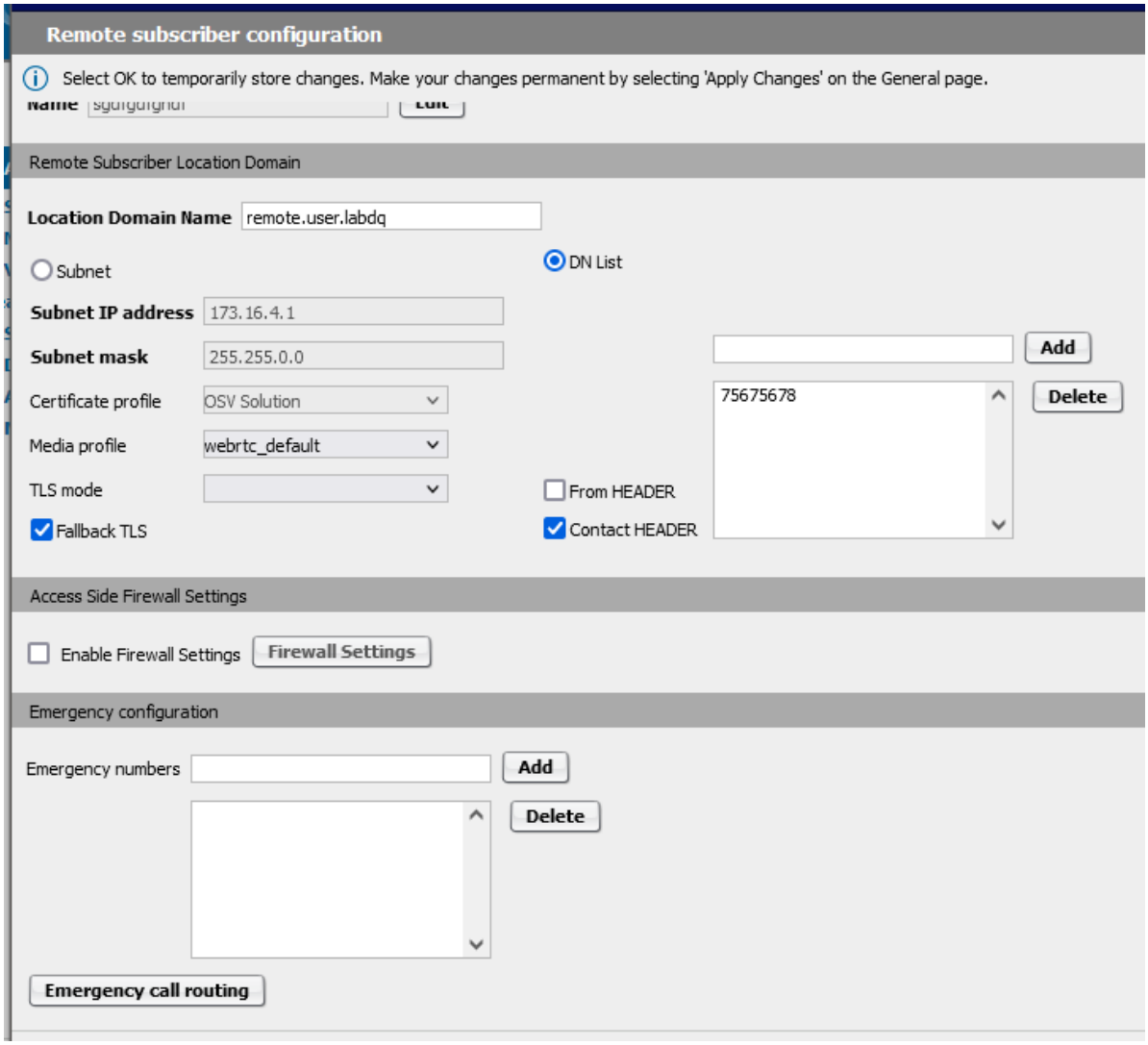
00 end of string

The phone will store that result as shown here.

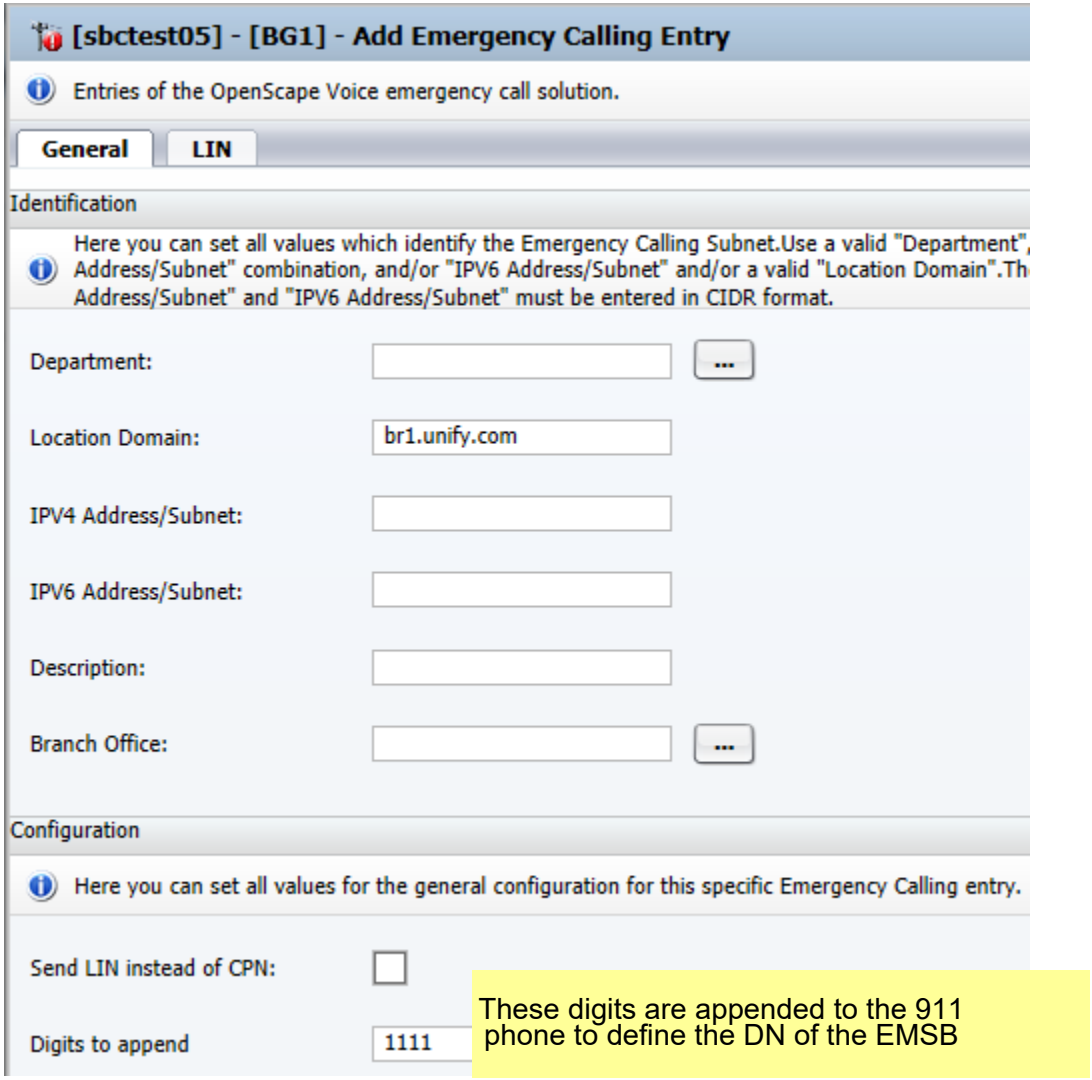


3. The DNS server must be set to return the WAN address of the SBC in response to the
DNS query from the phone.

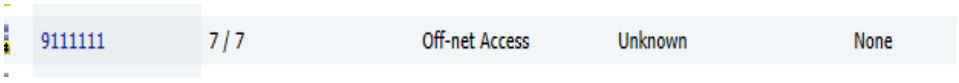
4. The SBC must be set to recognize the dialed digits as emergency (in the US this is
911).
Local GUI□□Features □□Remote Subscribers configuration □□add/edit.



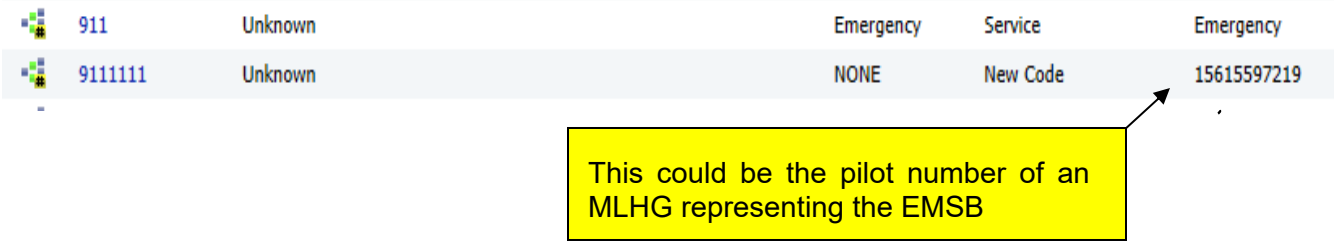
5. The OSV must be configured to resolve the location to the DN of the emergency services.
CMPconfiguration → OpenScape Voice → select OSV → select business group →
emergency calling → add



6. The OSV must be able to translate the new DN from the previous step 5 (above). Prefix access code



7. Destination code

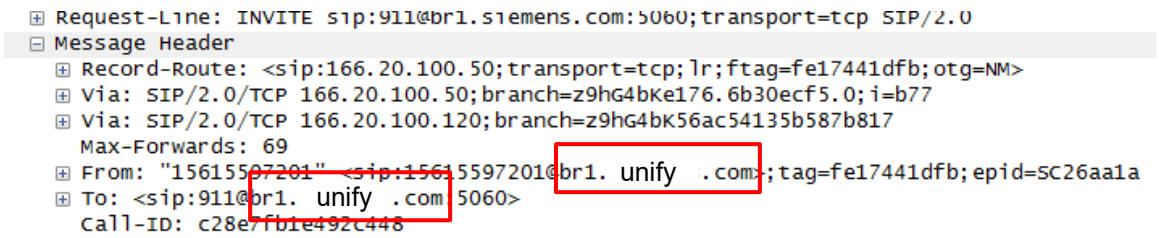


7. /etc/hosts in OSV must be configured to resolve the location to the SIPSM for the
OSV.

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
```

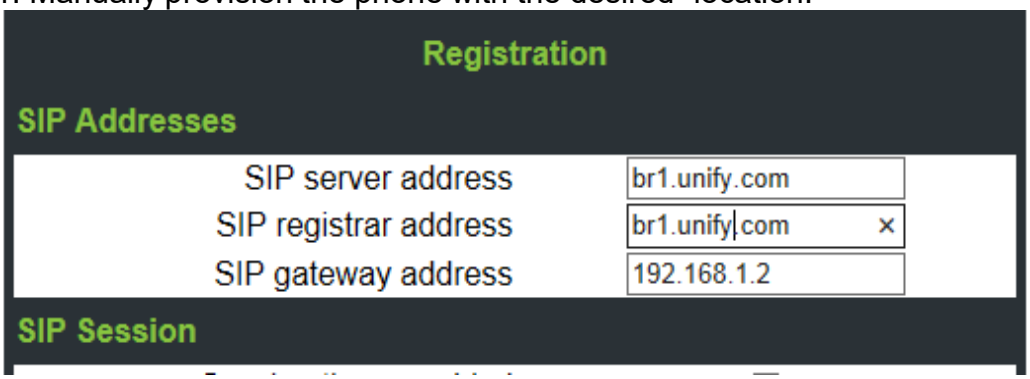
7. When the phone dials 911 the location information is passed in the INVITE to the OSS
and on to the OSV.



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.

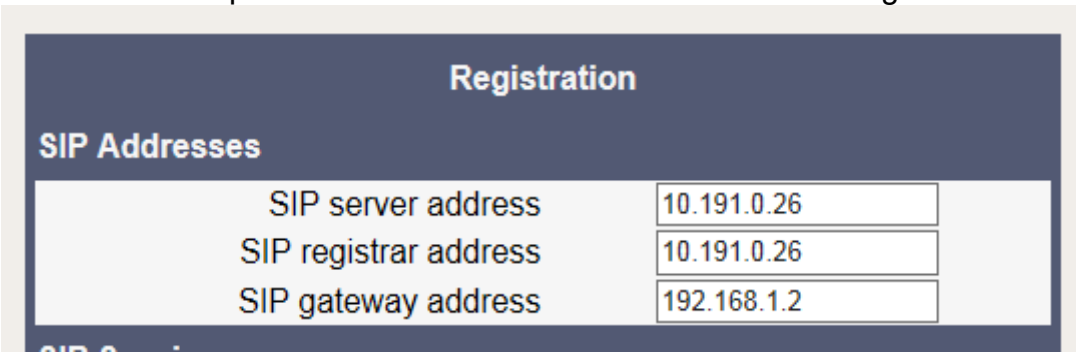


2. Continue with step 3 of Phone method #1: DHCP option 120

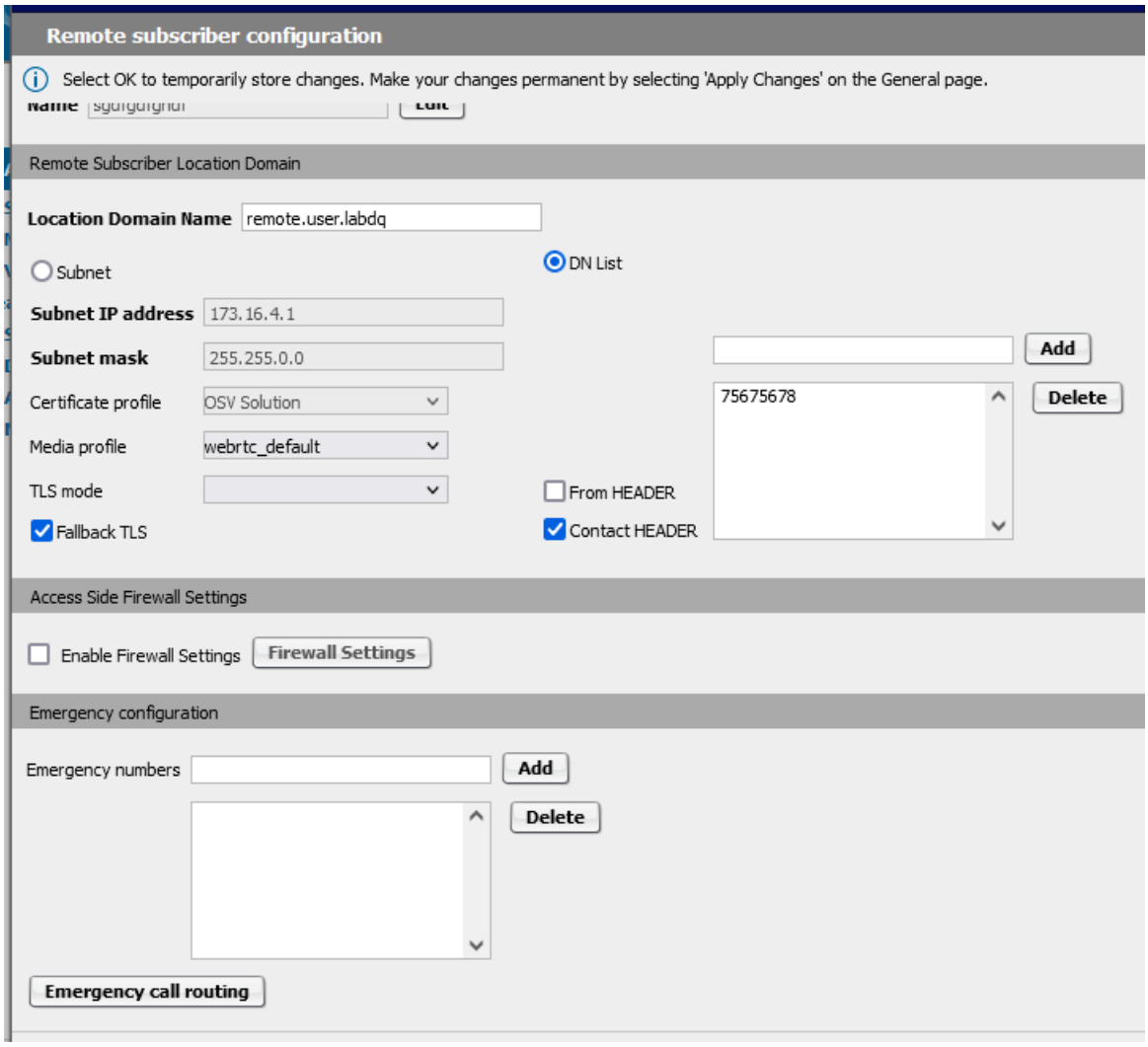
Provision location in the OSS

In the case the finest granularity is the determined by the provisioning of the subnet in step 2.

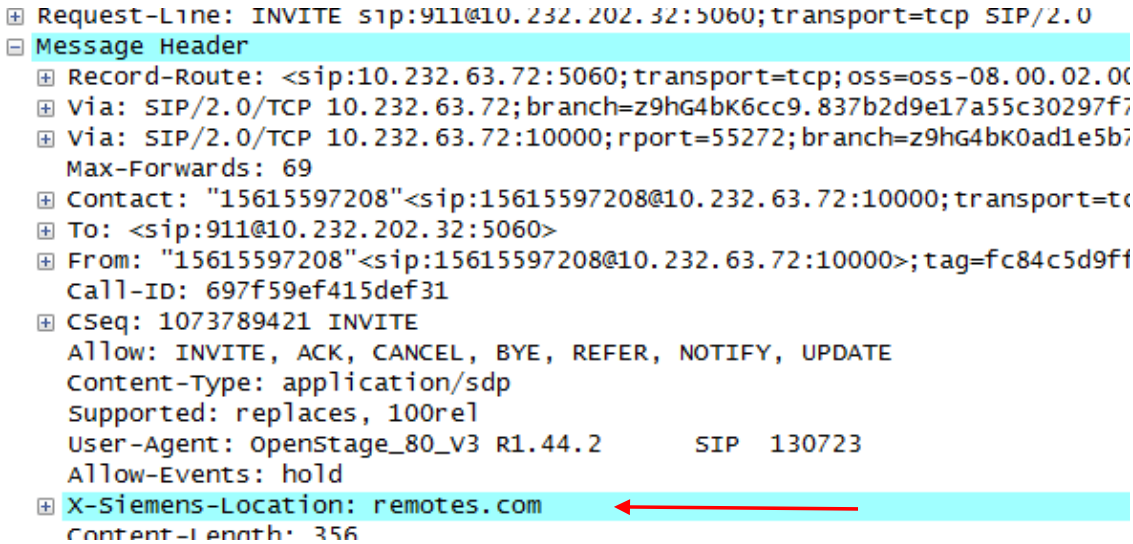
1. Provision the phone with the IP address of the OSS not using a FQDN.



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.



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.

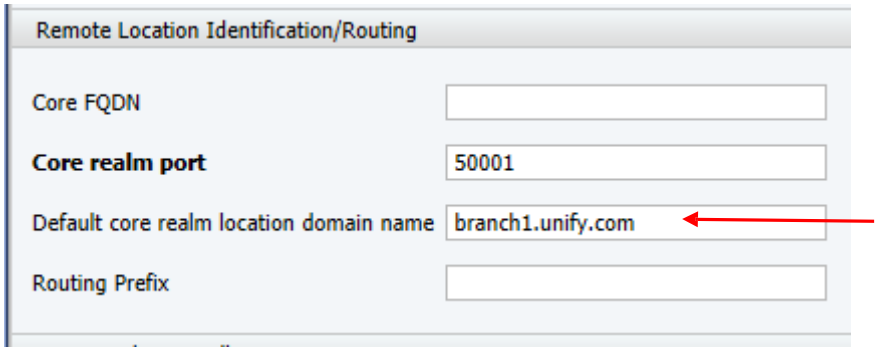


4. Continue with step 4 of Using DHCP option 120

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

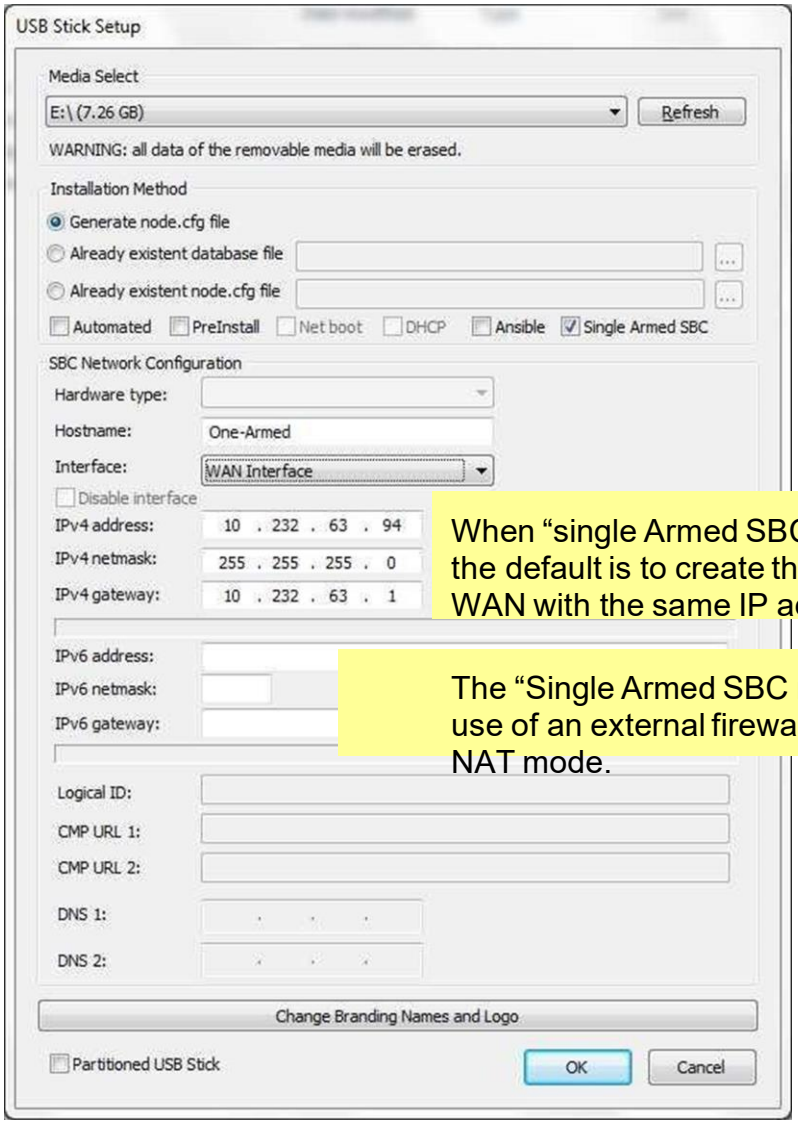
GUI> Features> Remote Endpoints configuration> add/edit> Default core realm location domain name



With this configured, it works much like Provision location in the OSS for these branch subscribers

19 Single-Armed-OS SBC

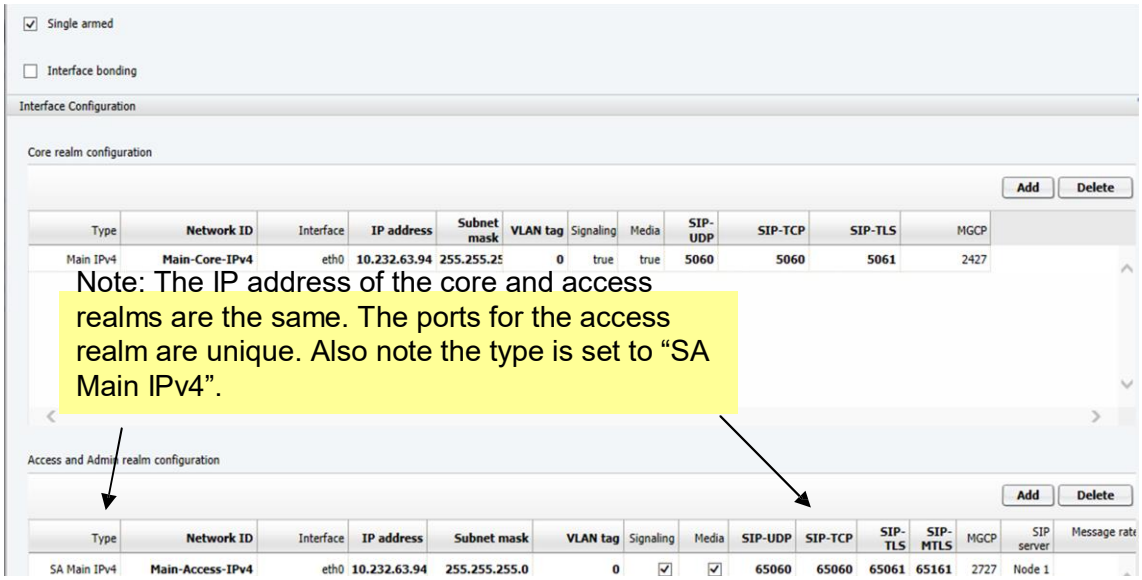
In Single armed configuration, the OS SBC's LAN and WAN interfaces are connected to the same IP subnet instead of being connected between two different IP networks or subnets. It is also desirable for both the LAN and WAN connection of OS SBC to use a single physical Ethernet interface, rather than two.



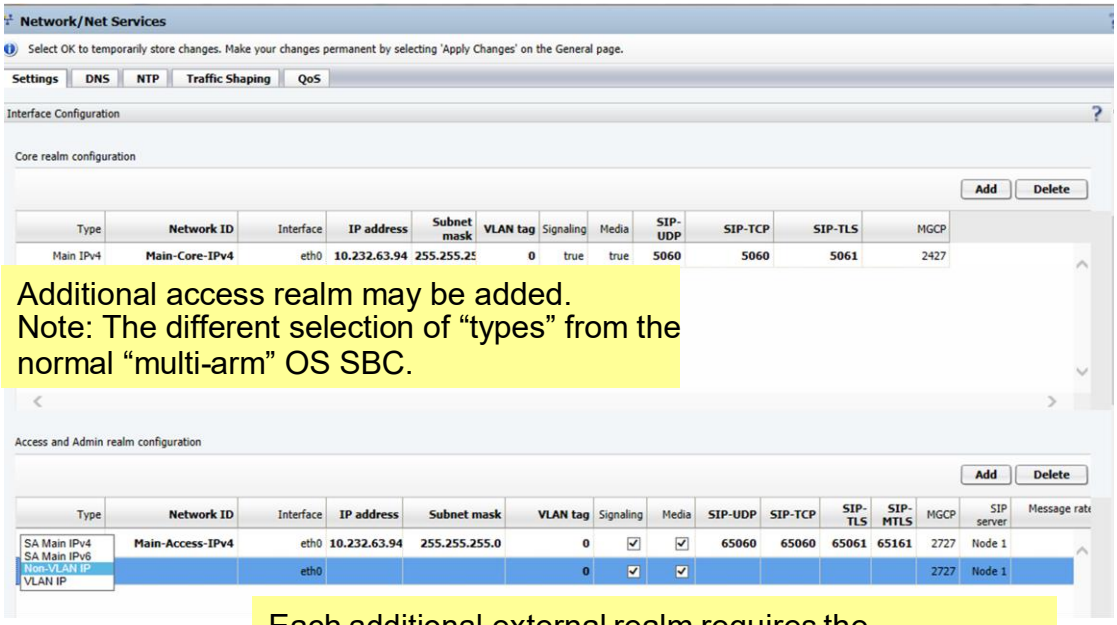
When "single Armed SBC" is selected the default is to create the LAN and WAN with the same IP address.

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”



Note: devices communicating with the access realm must use the correct port.



Normal configuration, using realm profiles, may continue from here.

20 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.

20.1 Registration Mode

Under **Remote Endpoints/Configure** add the **Service Provider Profiles**.
Select in **Default SSP Profile** the option **DTAG/NGN Registation 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 foolowing flags are activated:**Send user=phone in SIP URI**, **Registration mode**, **1TR118**.

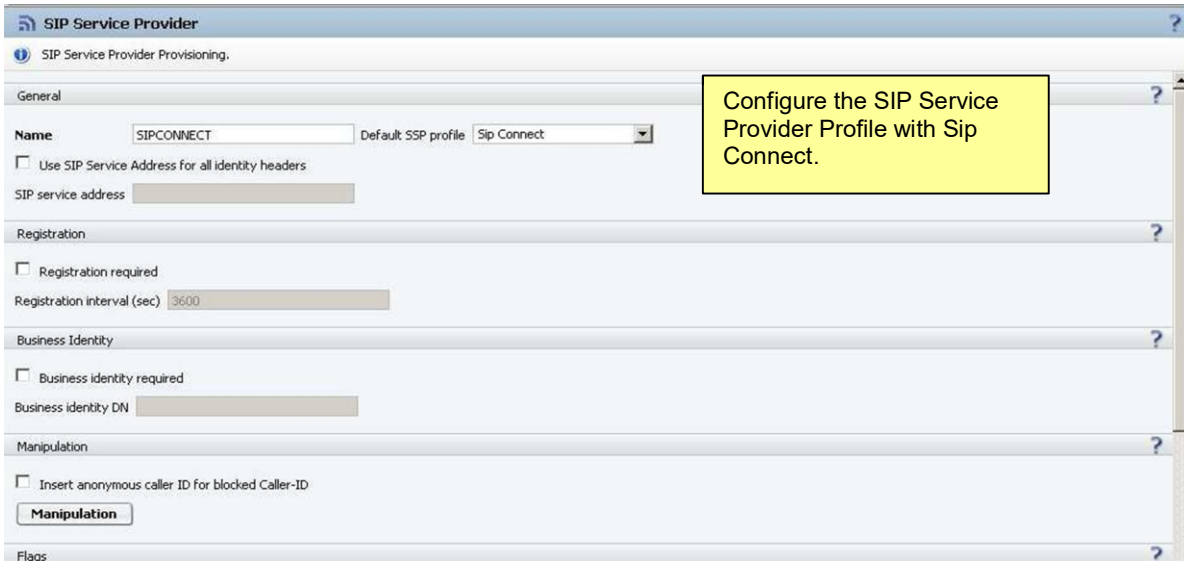
20.2 Static Mode

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.

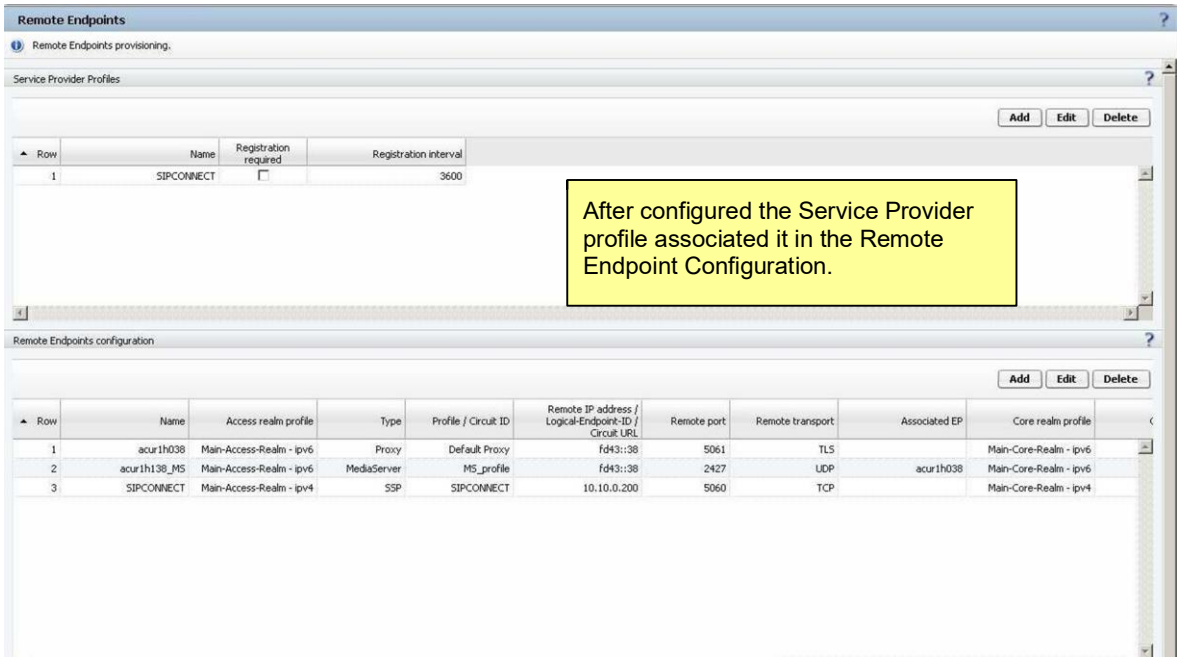
SIP Connect Configuration



Selects the flags in Sip Connect option in SIP Service Provider profile

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.



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:

21 UCaas Functionality

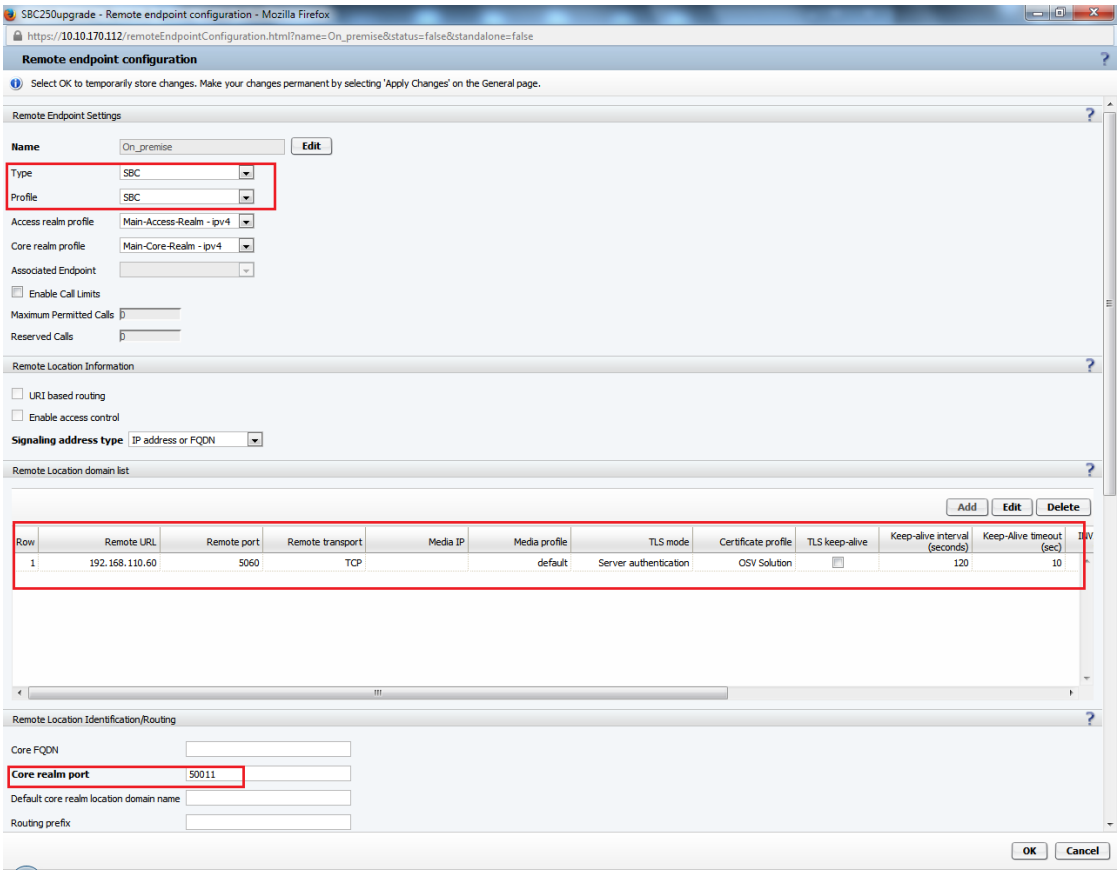
UCaaS, which stands for **Unified Communications as a Service**, integrates this communication through a cloud model, as well as integrating with cloud-based software applications.

21.1 Support Cascaded SBC configuration

21.1.1 Standalone mode

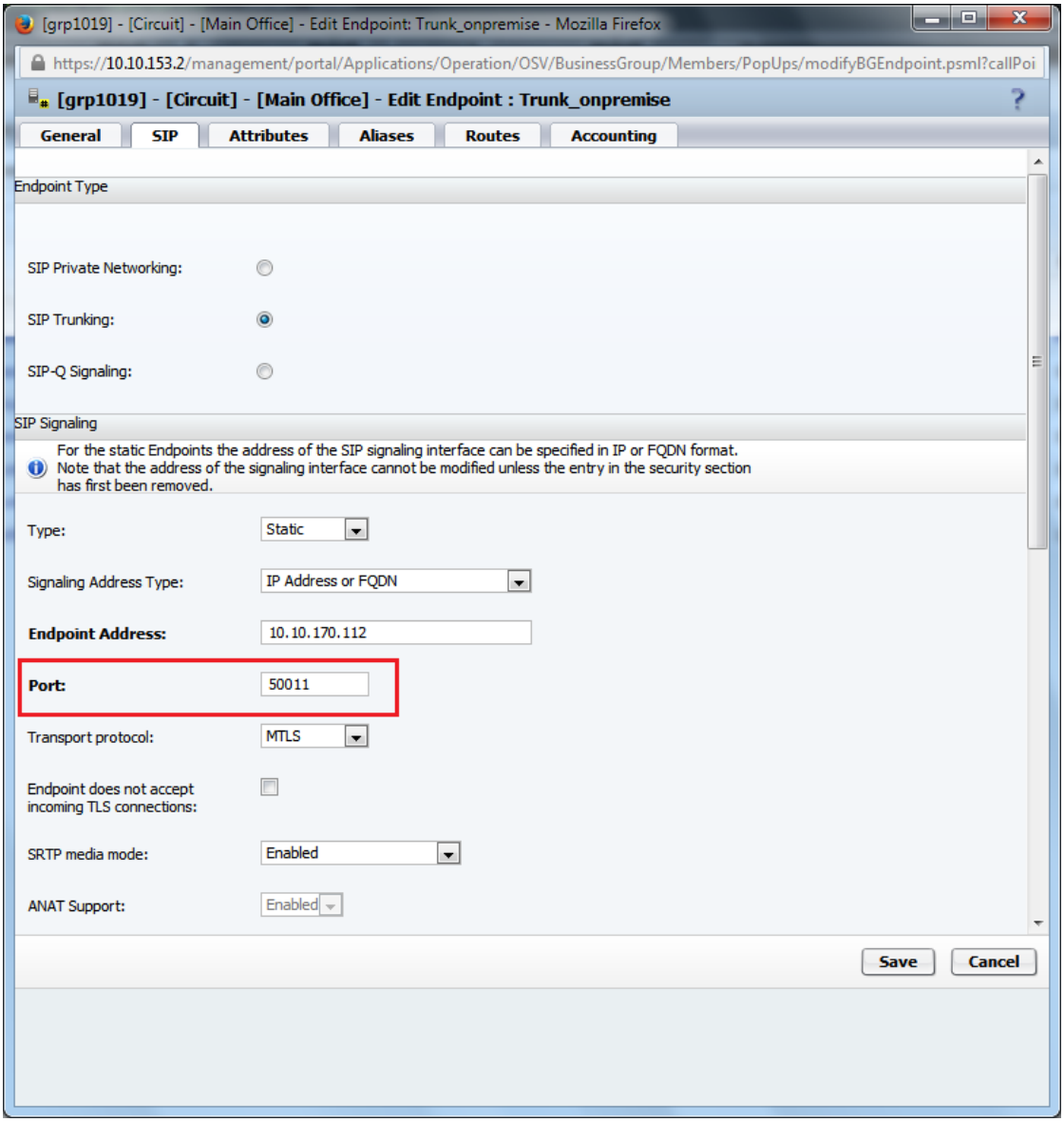
21.1.1.1 OSCloud Trunk SBC configuration

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.



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.

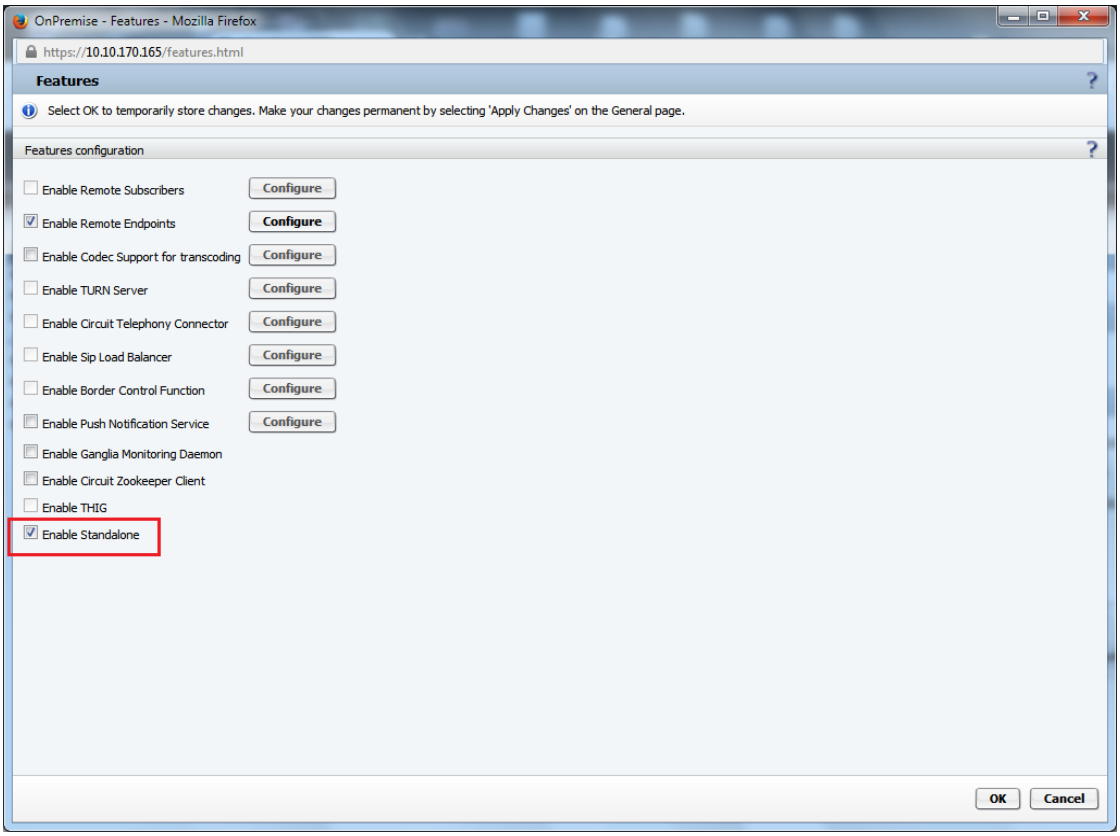


Endpoint configuration of the OSV

21.1.2 Standalone SBC Configuration

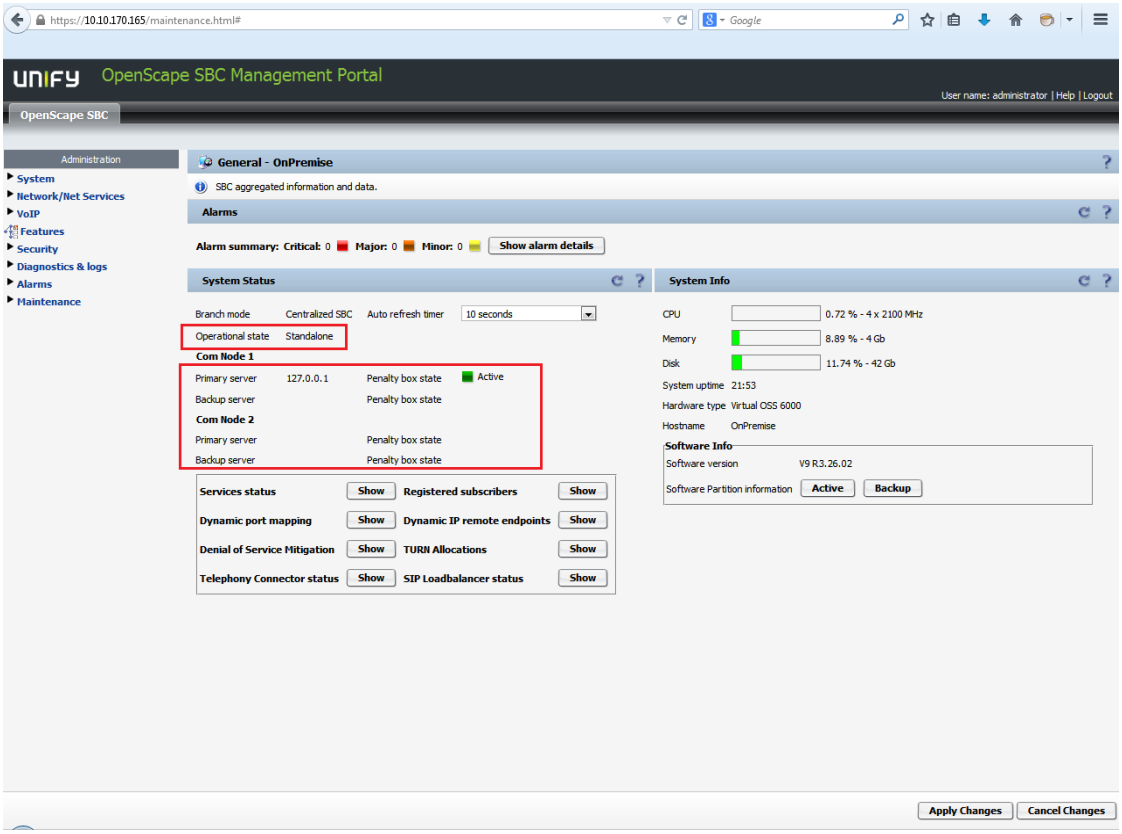
The SBC standalone mode is configurable in the "Features" windows as indicated below. Once the flag is set the following buttons became grayed out: Enable Remote Subscribers, Enable Turn Server, or Enable Sip Load Balancer and Enabled Border control function. In the same way the

Standalone Flag is grayed out if one of the previous mentioned flags is enabled.



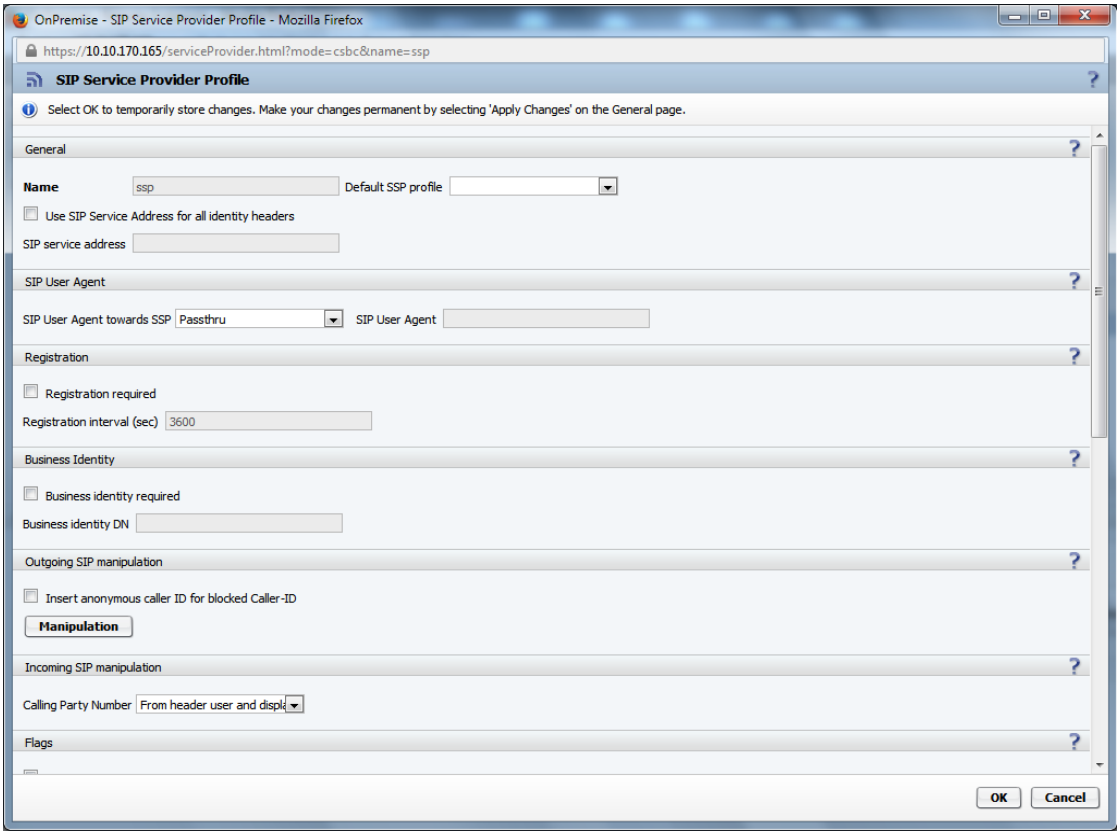
Enable Standalone functionality of SBC

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.



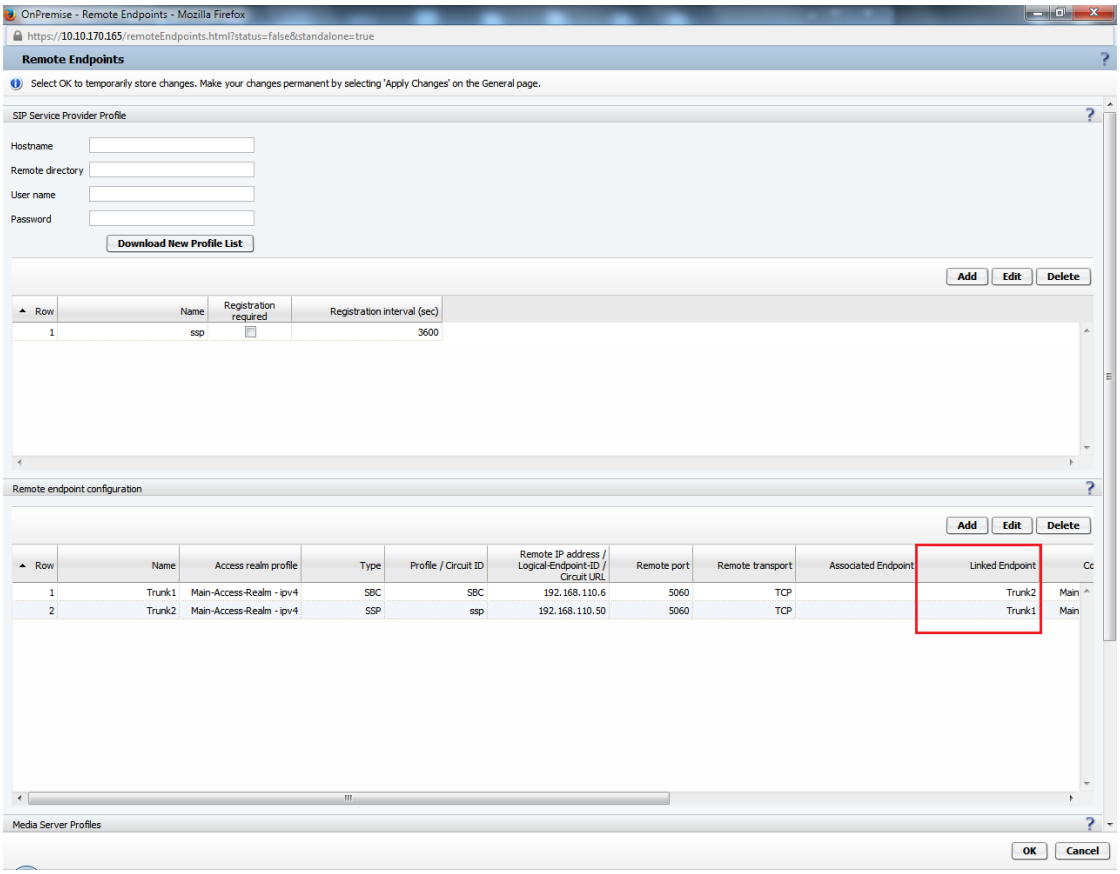
Standalone SBC dashboard

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.



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.

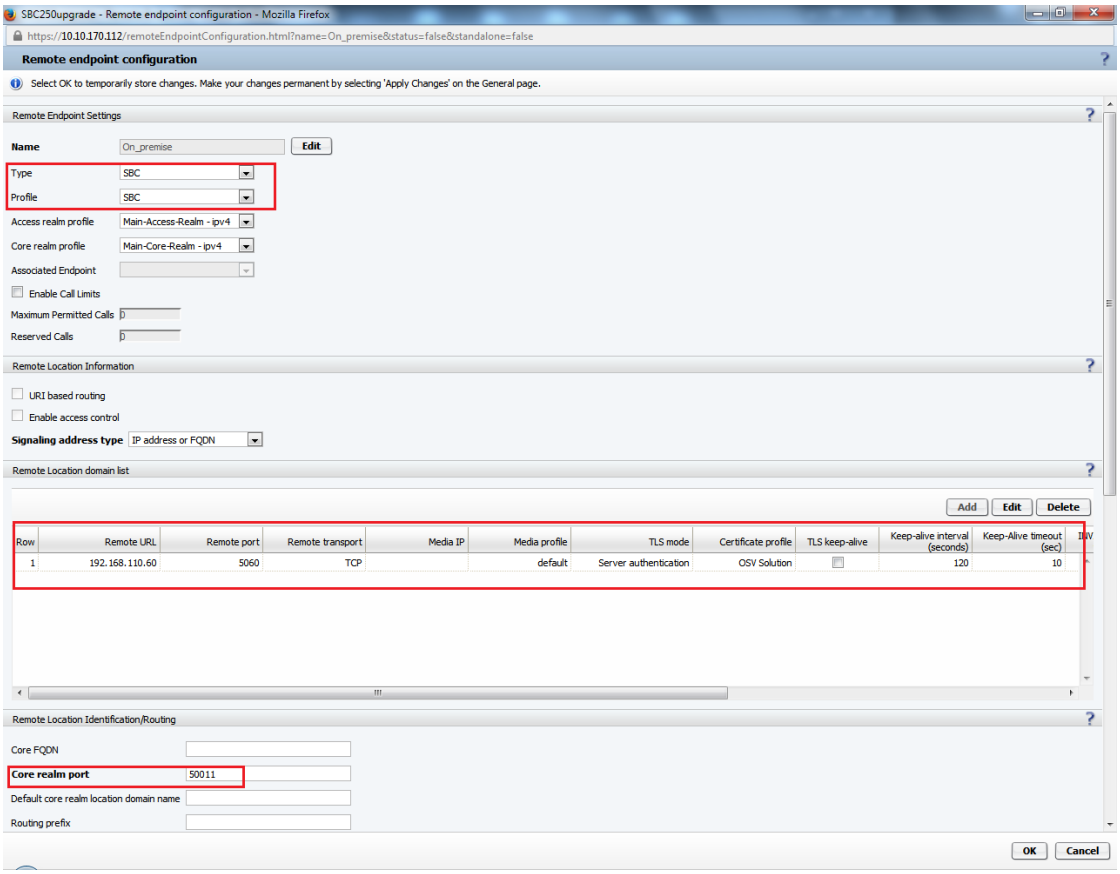


Please note that the above configuration applies when standalone on premise SBC is connected to SSP through a SBC.
If branch or gateway is used, SSP linked to a gateway behind a branch will have the branch as associated endpoint and the gateway as linked endpoint.

21.1.3 Cascaded SBC mode

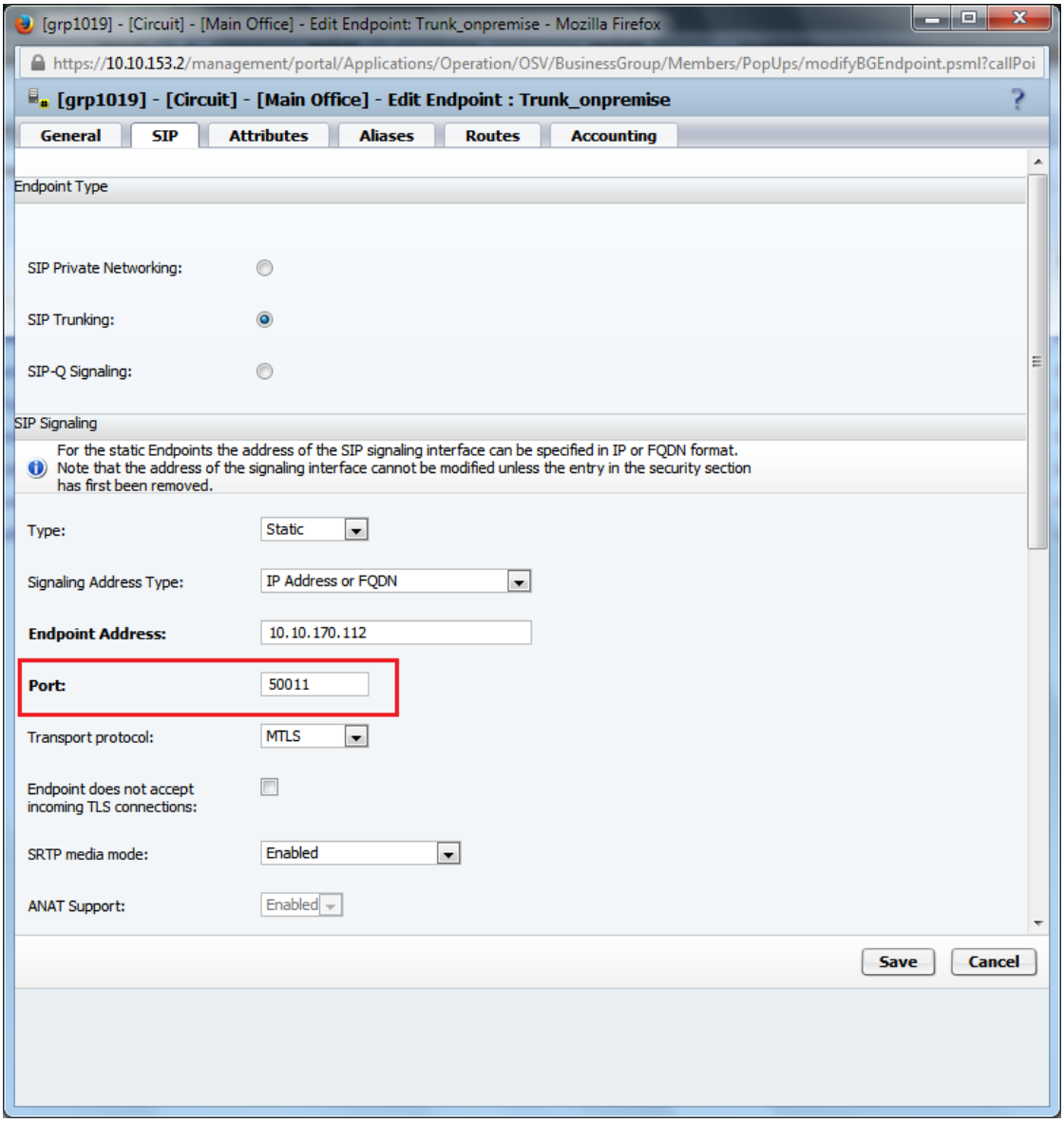
21.1.4 OSCloud Trunk SBC configuration

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.



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.

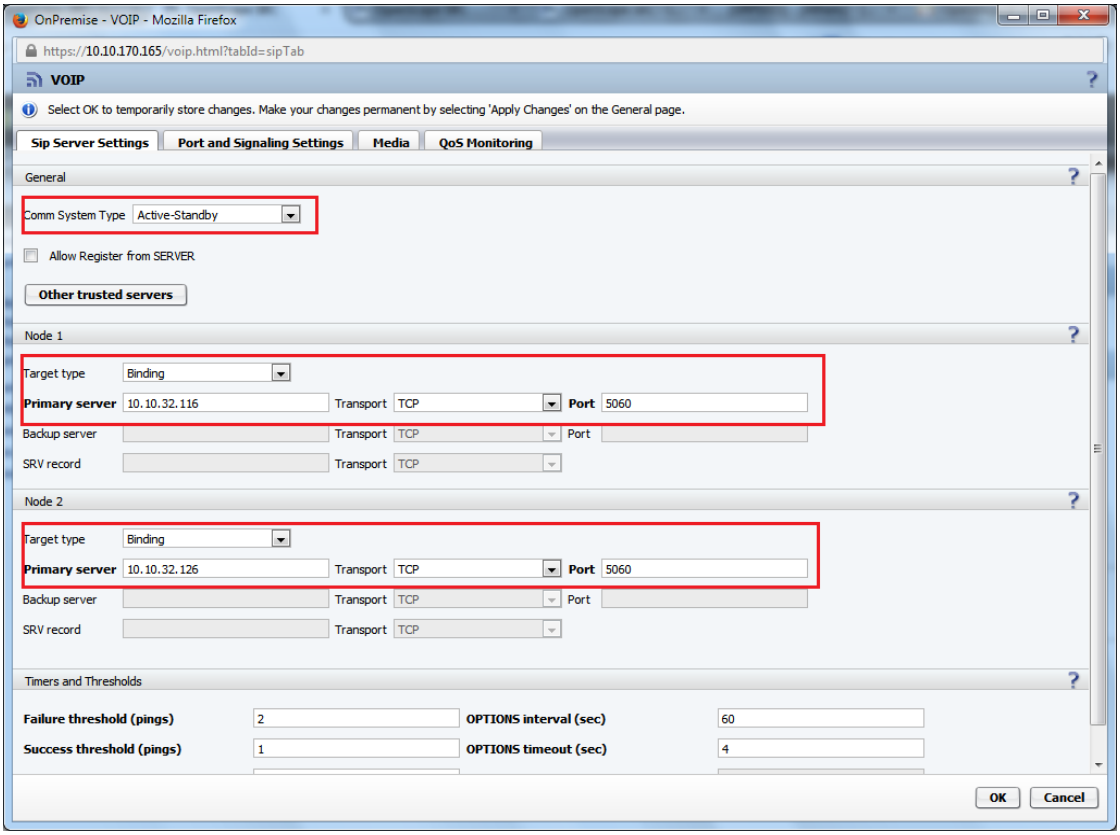


Endpoint configuration of the OSV

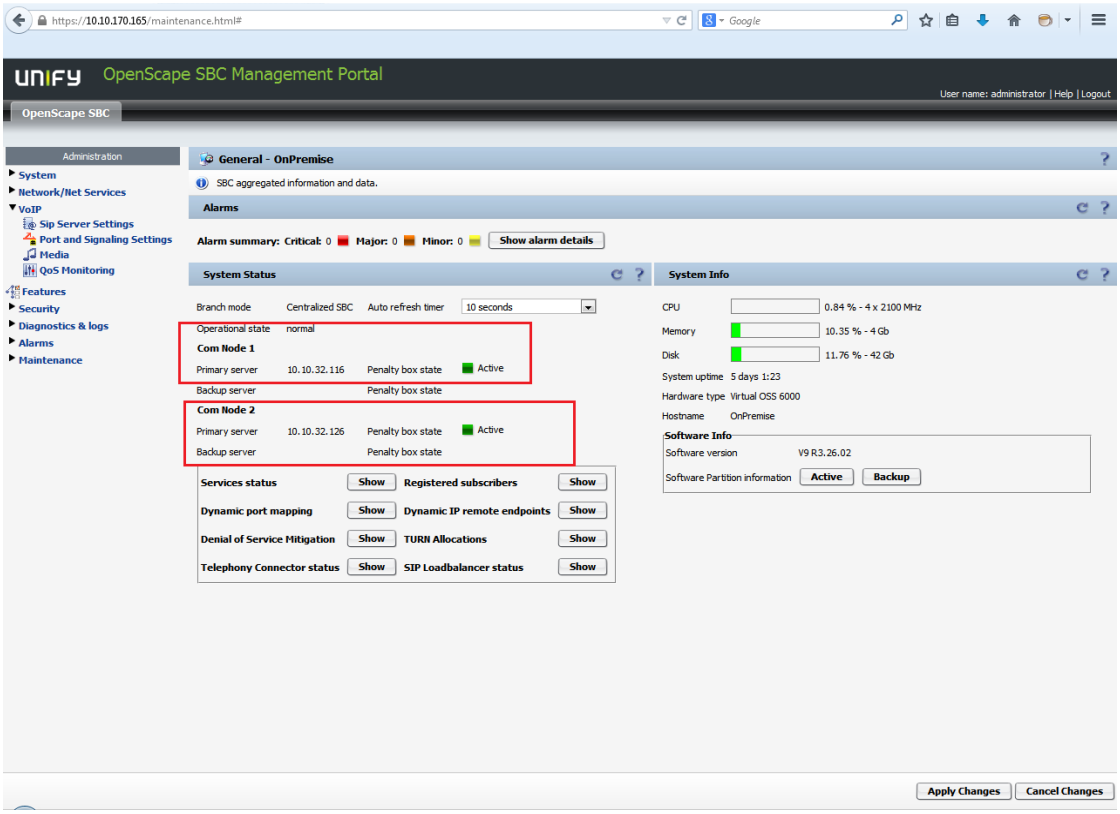
21.1.5 Cascaded SBC configuration

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.

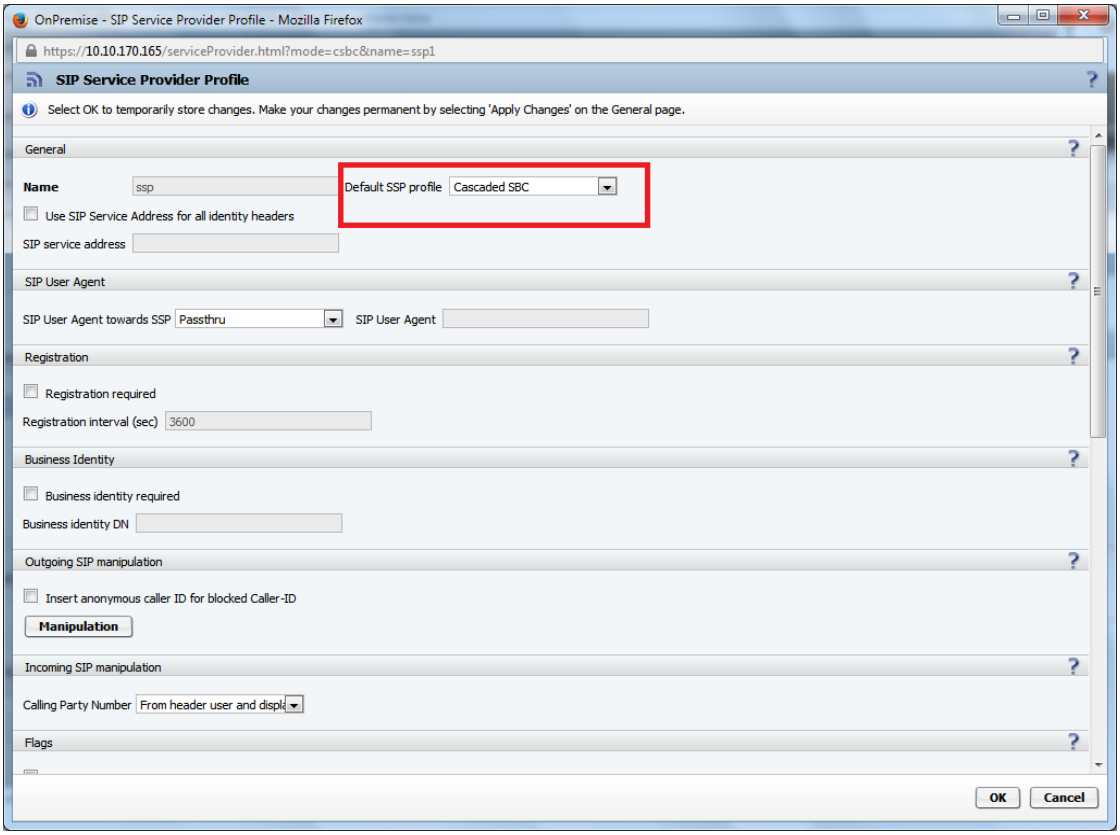


Primary server is set to customer sipsms active and standby, and the state should be green.

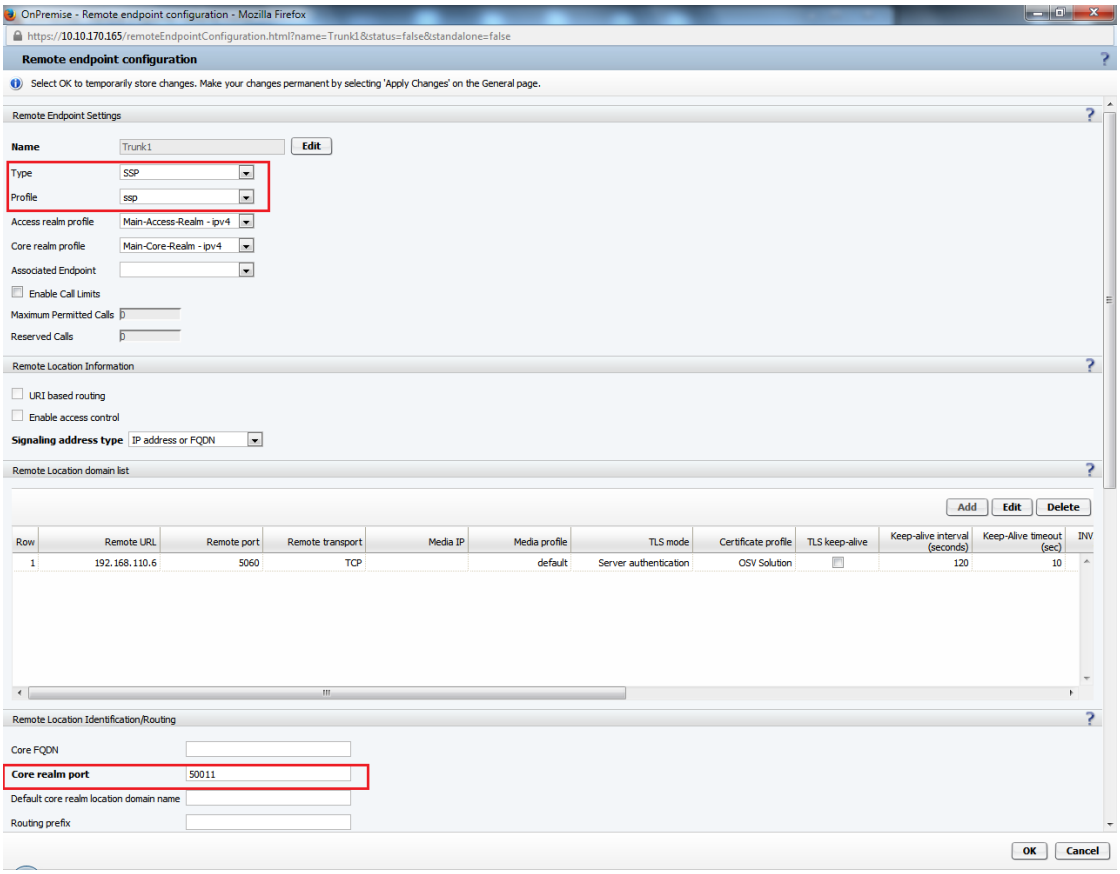


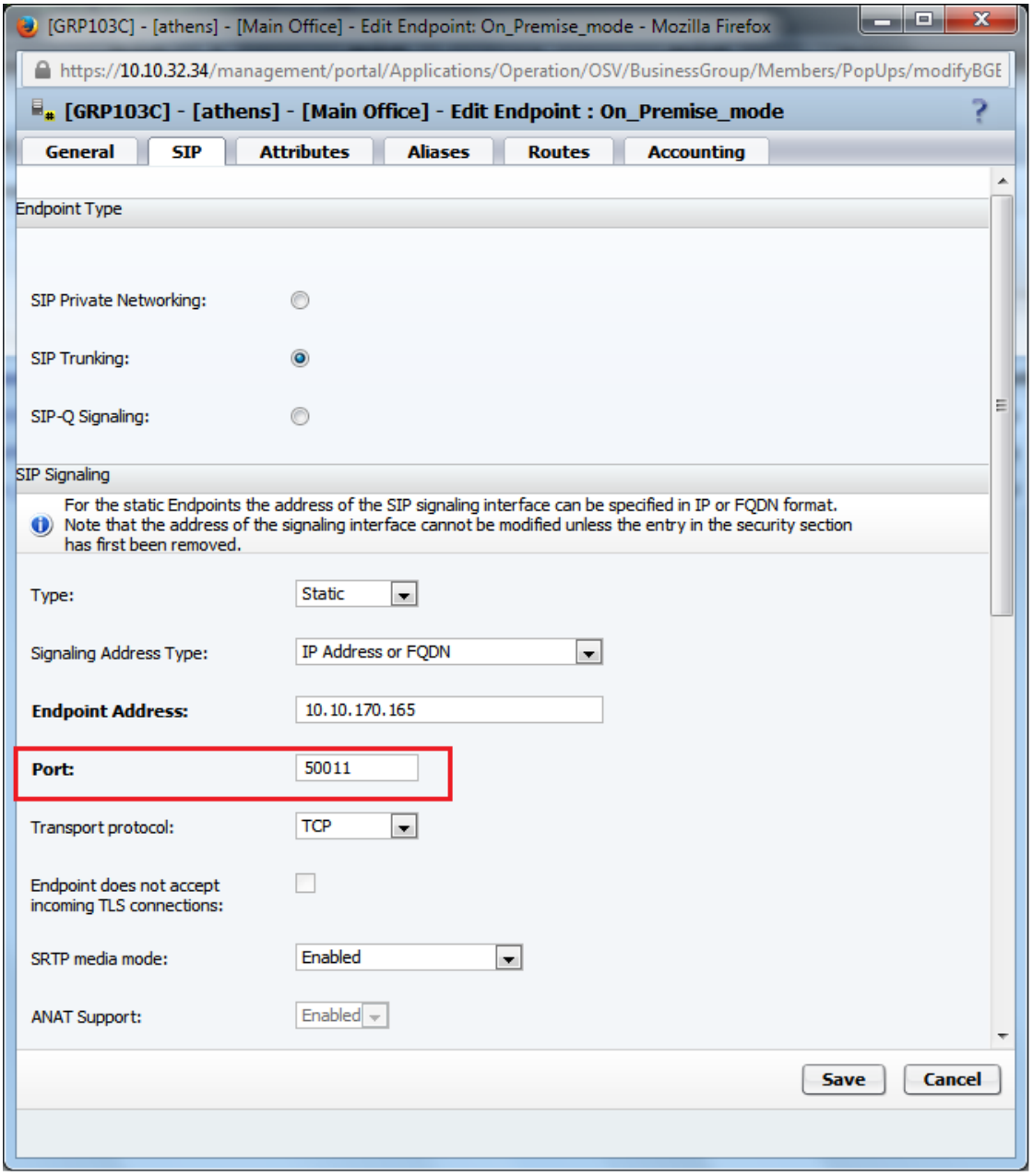
The remote endpoint configuration is changed to allow a remote endpoint of SSP type by connected to endpoint of TRUNK-SBC.

Create default SSP profile and select “Cascaded SBC” from drop down menu. This profile will set as default outbound proxy port and registrar server port to 5060 in remote endpoint.



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/remoteEndpointConfiguration.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
120
10
Remote Location Identification/Routing
Core FQDN
Core realm port
50011
Default core realm location domain name
Routing prefix
OK
Cancel



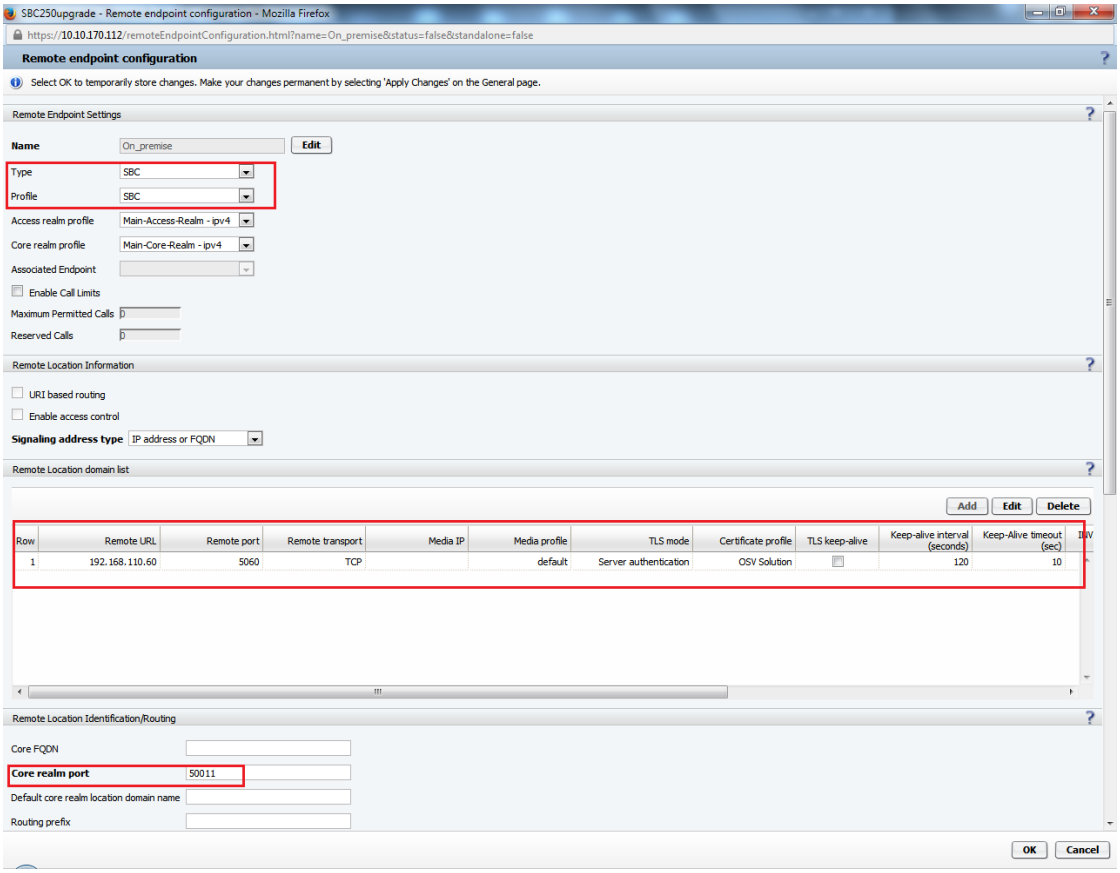
Please note that the above configuration applies when Cascaded SBC is connected to SSP through a SBC and the customer's PBX is an OSV.

21.2 Support SBC on Premise configuration

21.2.1 Standalone mode

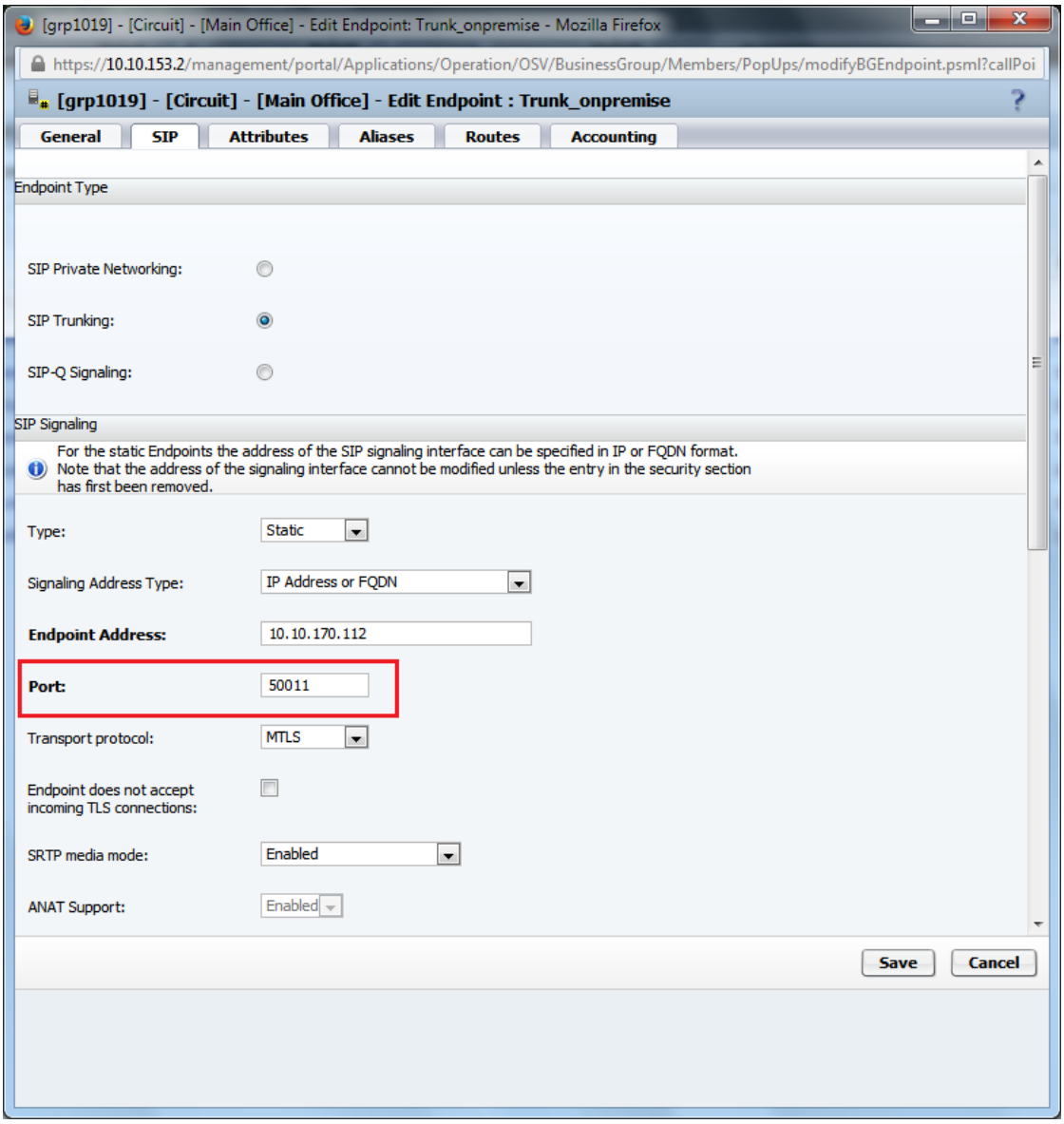
21.2.1.1 OSCloud Trunk SBC configuration

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.



Trunk SBC of OSCloud

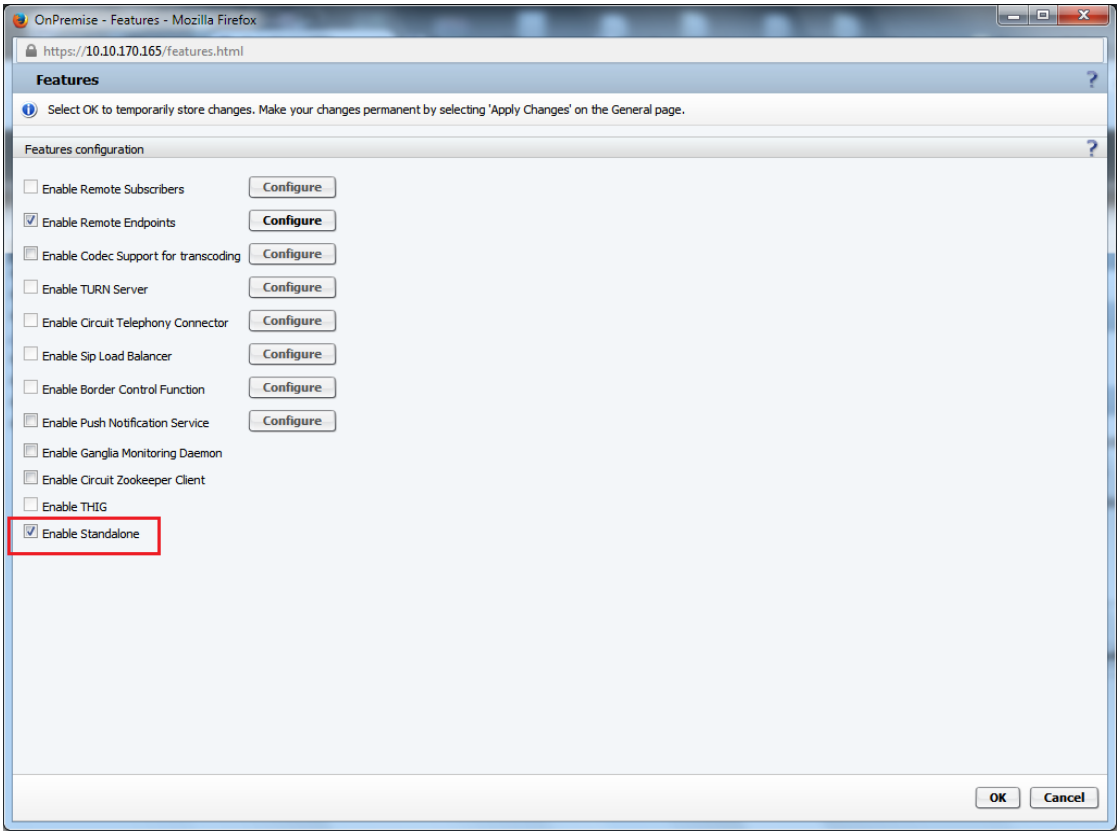
In OSV the configuration is as any other regular SBC the SIP port just have to match the core port of remote endpoint configured in the TRUNK-SBC corresponding to the Stand Alone SBC.



Endpoint configuration of the OSV

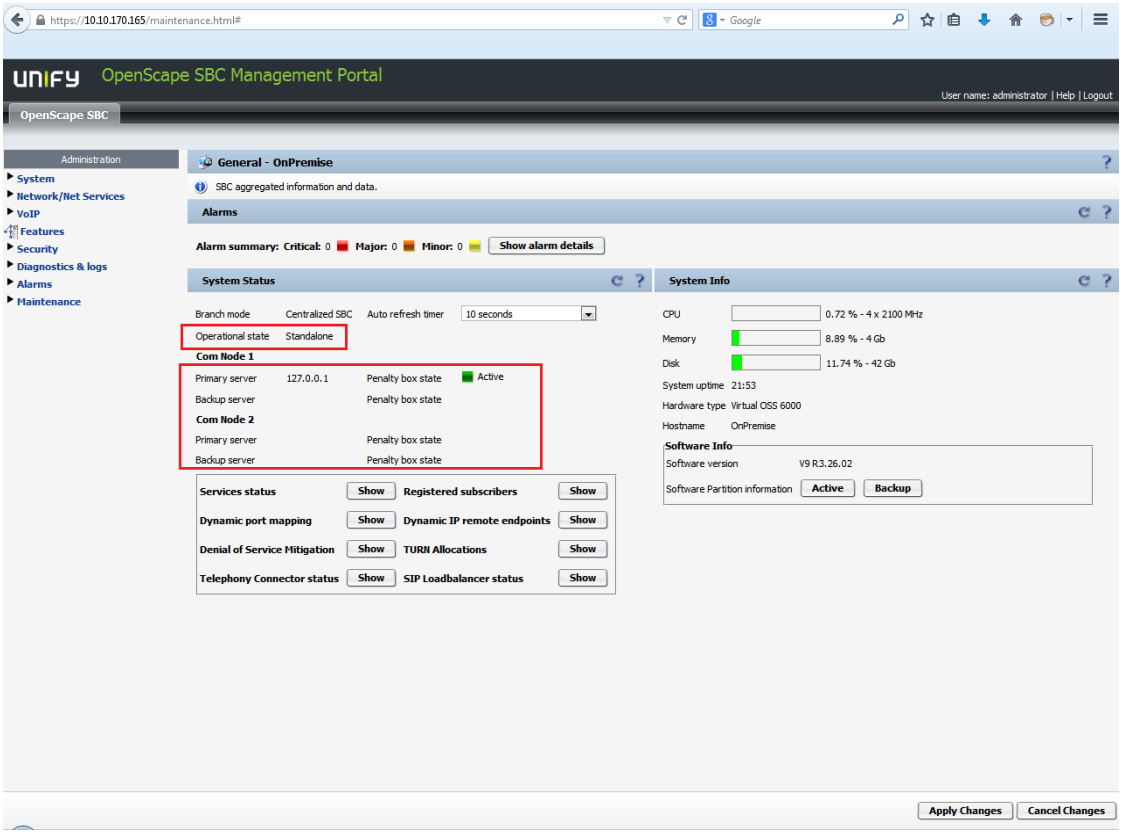
21.2.1.2 Standalone SBC Configuration

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

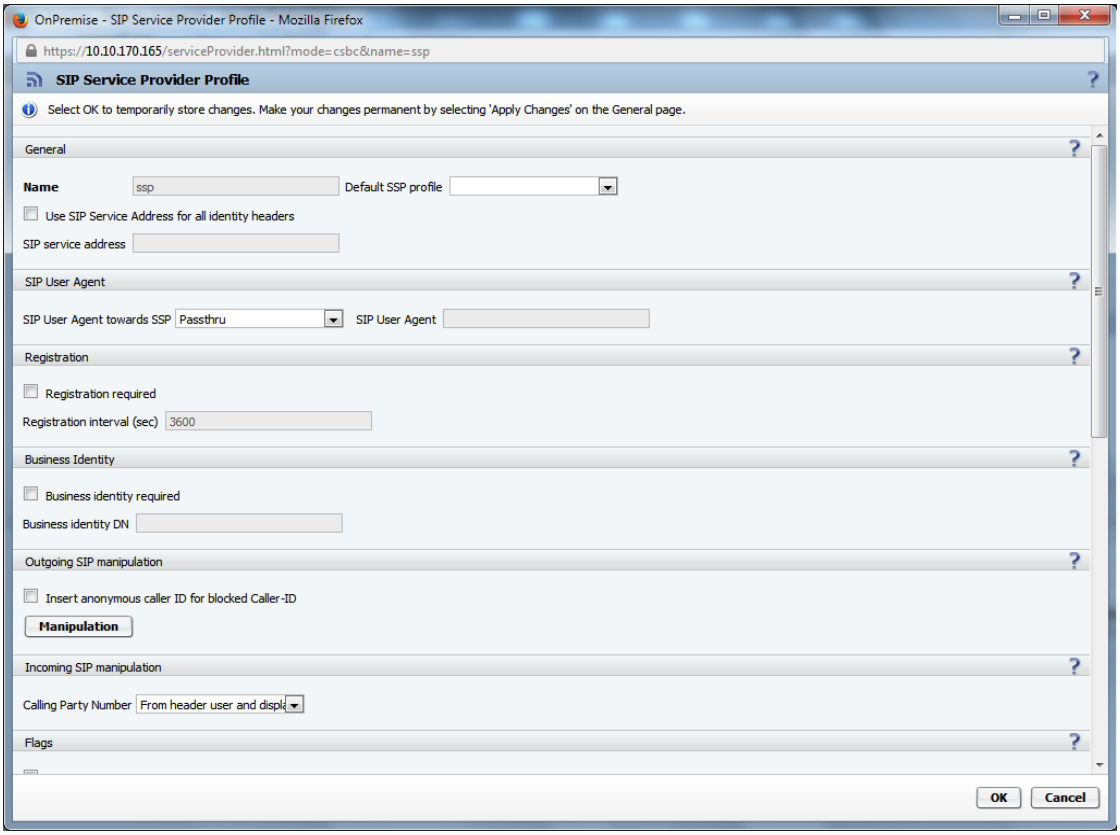
Once the flag is enable and the configuration is applied the Sip Server tab became empty and the dashboard will show in Operational mode the "Standalone". The Primary server is set to 127.0.0.1 and state should be green.



Standalone SBC dashboard

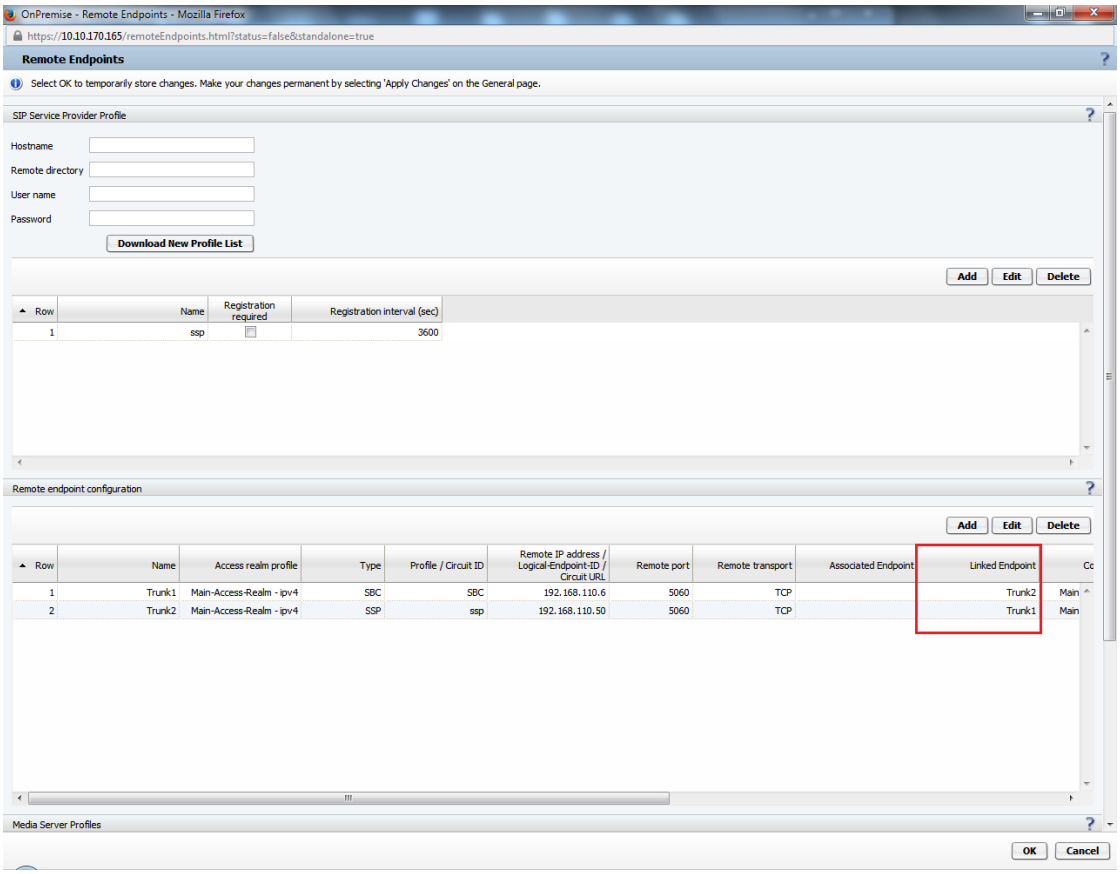
The remote endpoint configuration is changed to allow a remote endpoint of SSP type by linked to another endpoint of SSP type.

Create SSP profile.



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.



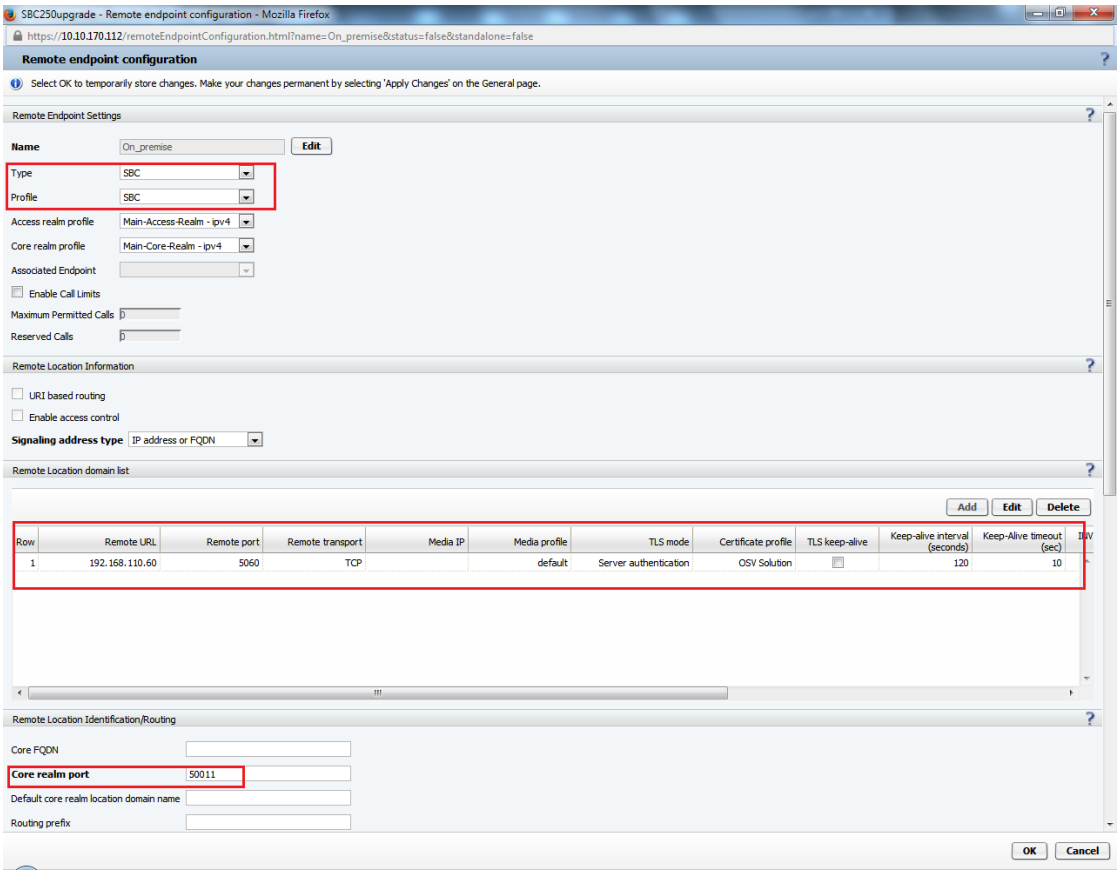
Please note that the above configuration applies when standalone on premise SBC is connected to SSP through a SBC.

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.

21.2.2 On premise SBC mode

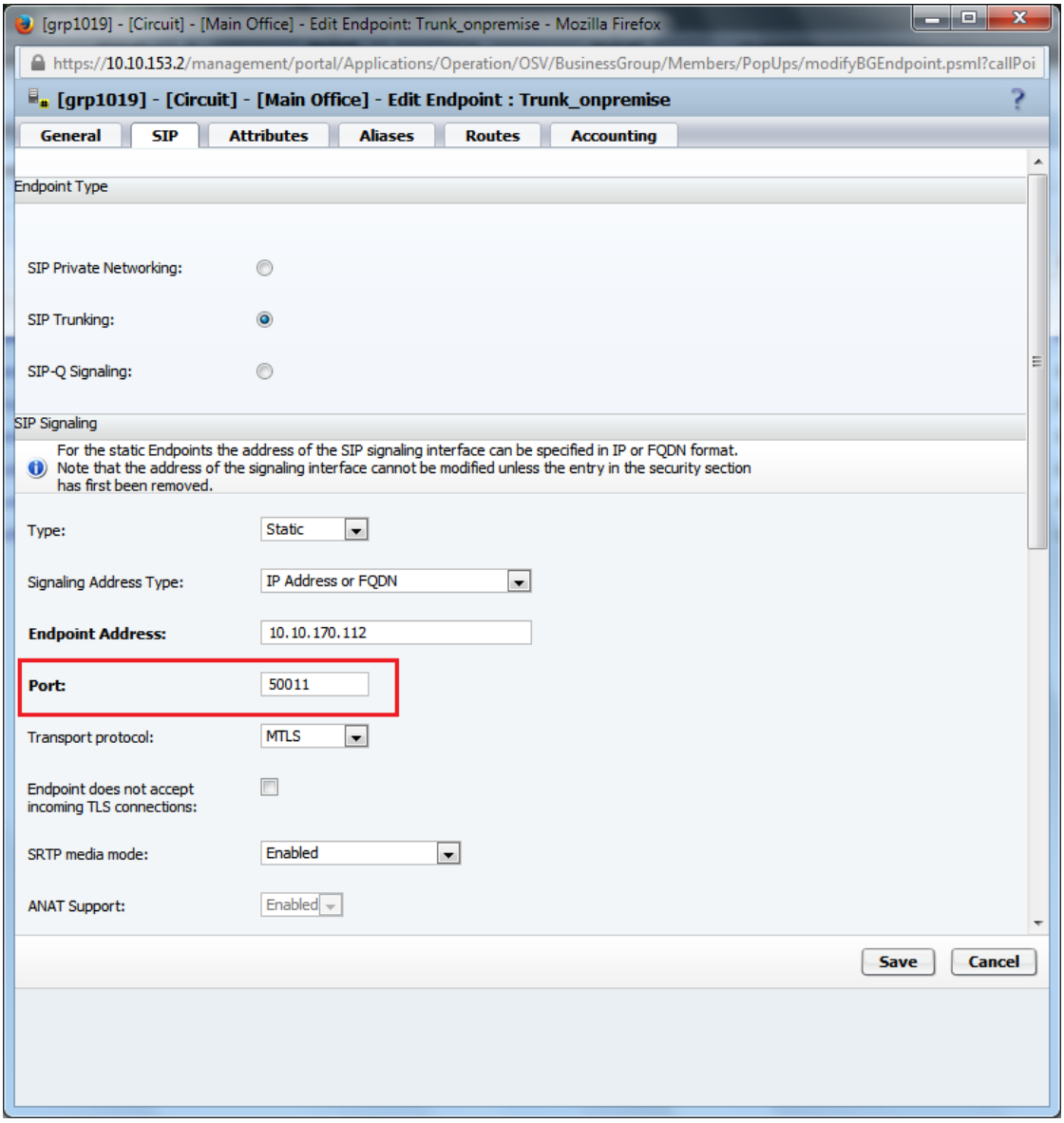
21.2.2.1 OSCloud Trunk SBC configuration

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.



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.

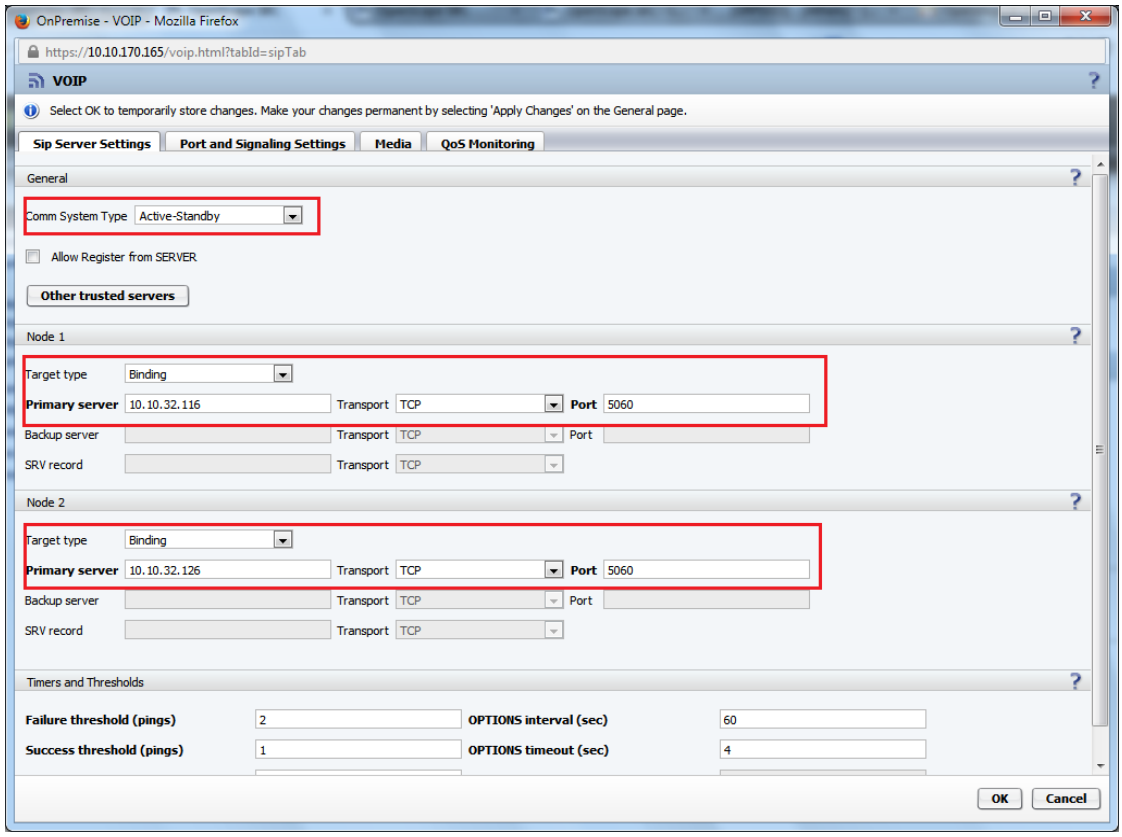


Endpoint configuration of the OSV

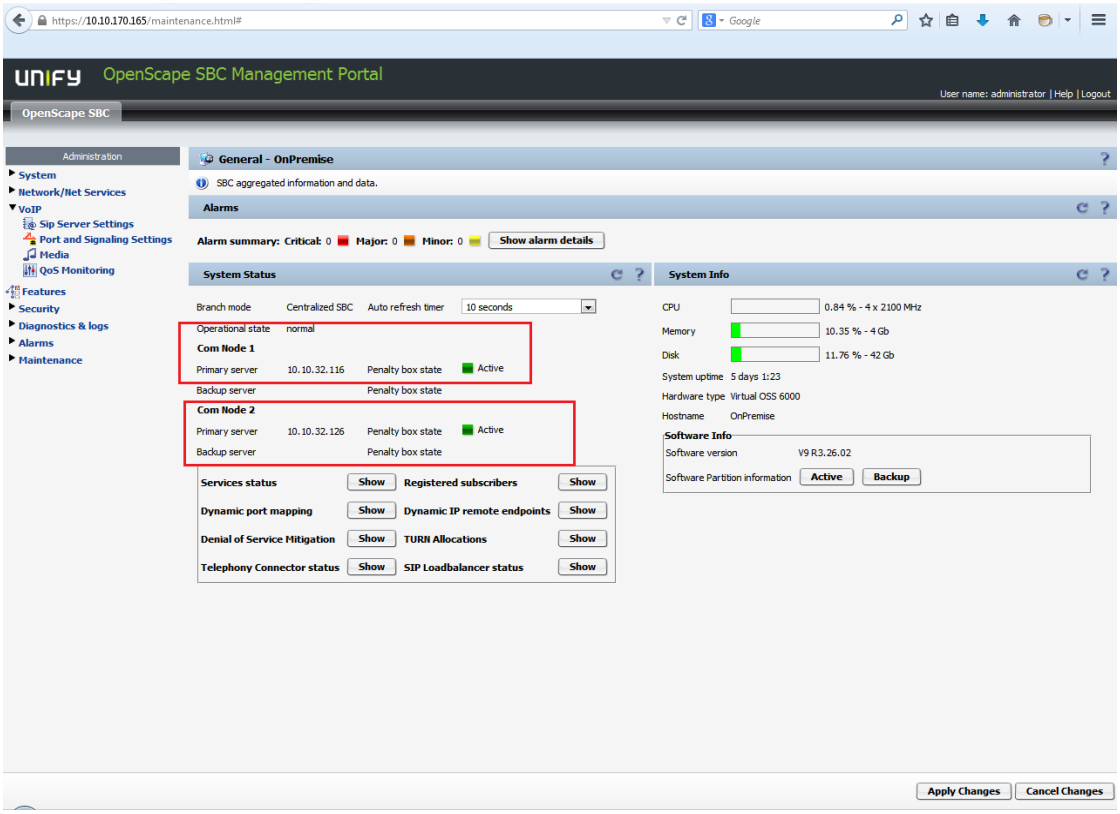
21.2.2.2 On premise SBC configuration

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.

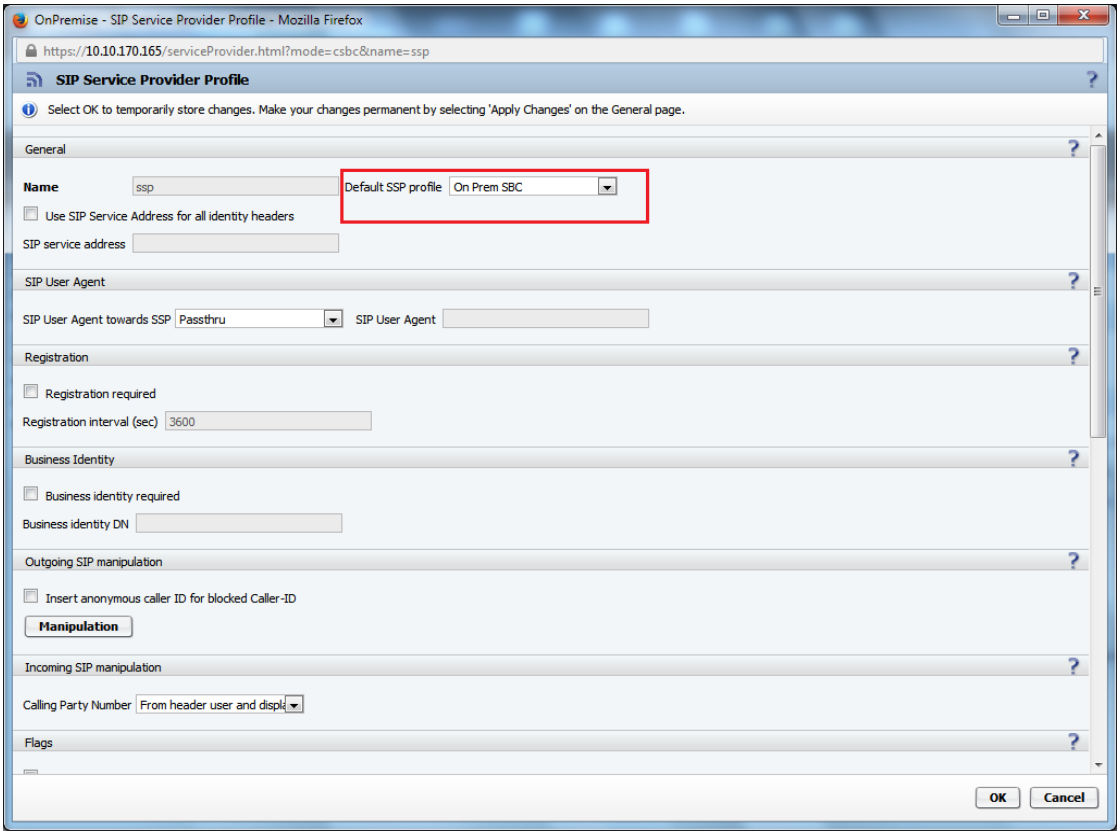


Primary server is set to customer sipsms active and standby, and the state should be green.

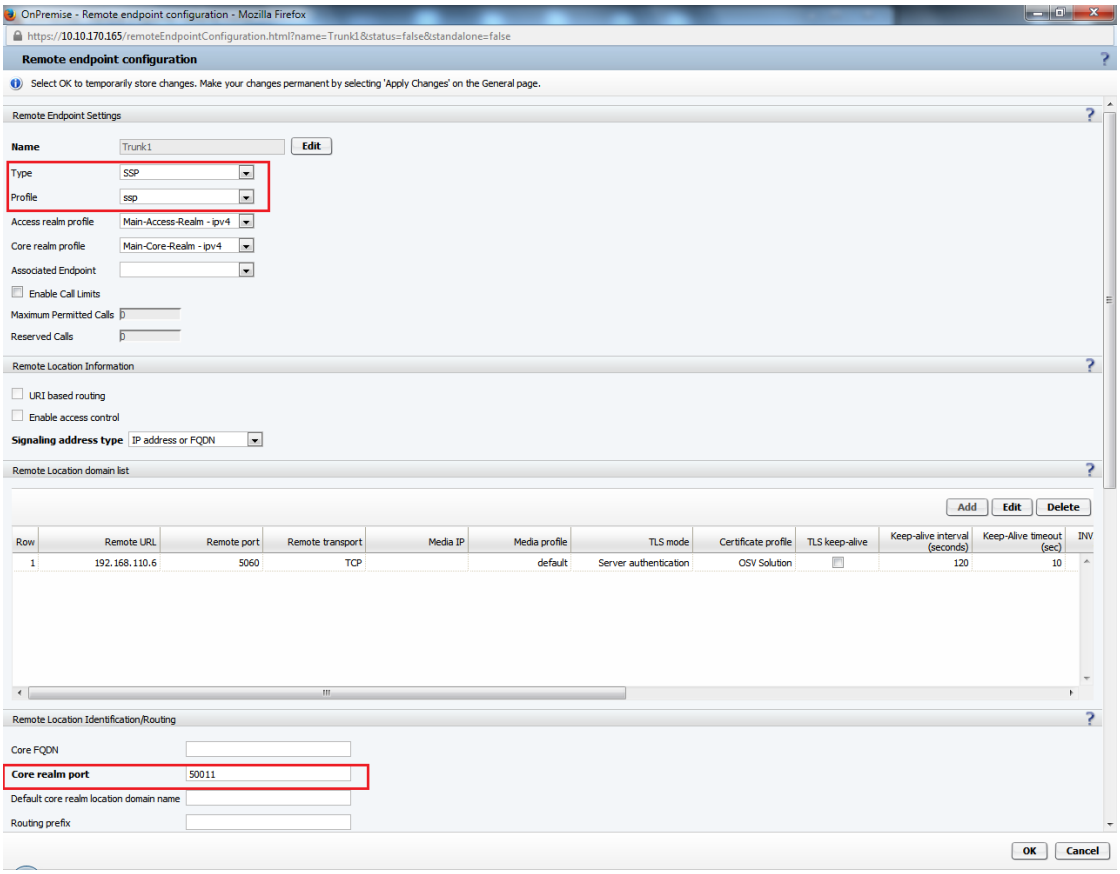


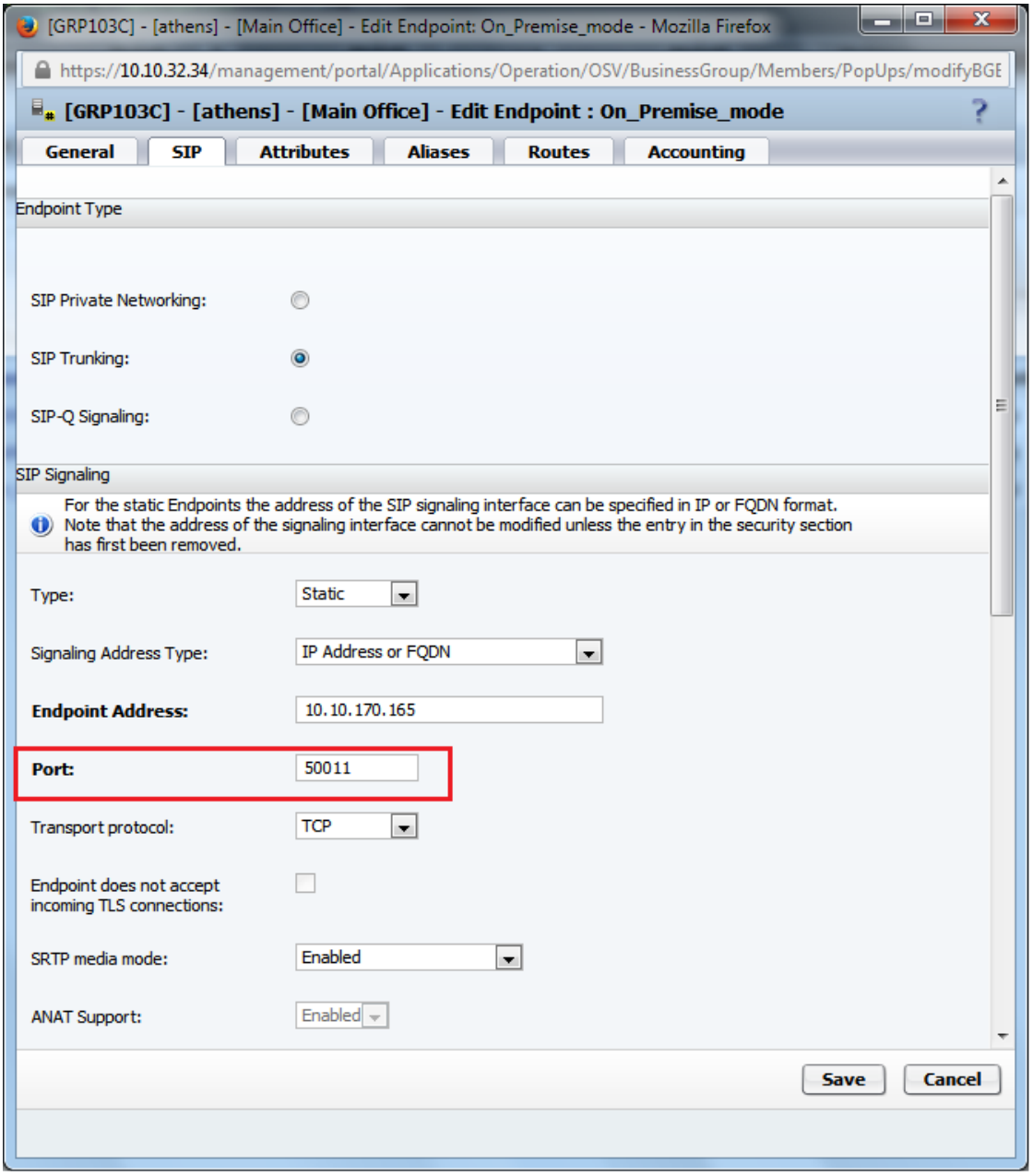
The remote endpoint configuration is changed to allow a remote endpoint of SSP type by connected to endpoint of TRUNK-SBC.

Create default SSP profile and select “On Prem SBC” from drop down menu.



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/remoteEndpointConfiguration.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
120
10
Remote Location Identification/Routing
Core FQDN
Core realm port
50011
Default core realm location domain name
Routing prefix
OK
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.

22 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 standardsand 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 diskdrive
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

mitel.com