

Alcatel-Lucent OpenTouch™ Session Border Controller – R7.4

Configuration Guide

1.	Scope	4
2.	OTSBC general Overview	5
2.1	Using OTSBC to secure conversations on corporate LAN and on WAN (Internet)	5
2.2	WAN secured OTC clients VoIP short operating mode	6
2.2.1	Software clients	6
2.2.2	OTC Web with WebRTC	7
3.	OTSBC Configuration	8
3.1	OTSBC software installation and basic network connectivity setting	8
3.1.1	Installation of a virtual machine (Virtual Edition) in VMware environment	8
3.2	OTSBC main maintenance procedures	9
3.2.1	License file installation	9
3.2.2	Software Upgrade with a .cmp file – Software Upgrade Wizard	11
3.3	OTSBC Configuration procedure	12
3.3.1	Configuring an OTSBC using the AudioCodes wizard tool	12
3.3.2	OTSBC web admin menu	19
3.3.3	Physical ports, Ethernet devices, Ethernet groups and IP interfaces	20
3.3.4	General Media Setting for NAT Traversal	23
3.3.5	Media Security (SRTP) configuration	24
3.3.6	Media Realms configuration	25
3.3.7	SRD configuration	26
3.3.8	SIP interfaces configuration	27
3.3.9	IP Profile configuration	28
3.3.10	Proxy Sets configuration	32
3.3.11	SIP Messages Manipulations configuration	35
3.3.12	Message Conditions	39
3.3.13	IP Group configuration	41
3.3.14	IP to IP Routing configuration	45
3.3.15	Configure Classification	48
3.3.16	Configure certificate based Security	51
3.3.17	NAT Translation configuration	54
3.3.18	NTP configuration	55
3.4	HTTP/S Proxy server configuration	55
3.4.1	Enable Reverse Proxy on OT-SBC	55
3.4.2	Reverse Proxy configuration	56
3.4.3	Template_interface_ed02.ini	57
3.4.4	Template_rp_ed02.ini	57
3.4.5	Configuring VNA proxy	59
3.4.6	Template_ldap_ed01.ini	61
3.4.7	Template_ot_before2_4_ed01.ini	61
3.4.8	Template_vna_ed01.ini	61
3.5	LDAP Authentication	62
3.5.1	LDAP Authentication on internal OTSBC reverse proxy	62
3.6	OTSBC Admin Page	65
3.6.1	Remote Workers devices	65
3.6.2	Others	66
3.7	OTSBC Monitoring	67
3.7.1	SBC VoIP Status	67
3.7.2	SBC Active Alarms	68
3.8	OTSBC Administration	69

3.8.1	User Accounts	69
3.8.2	Web Security Settings	70
3.8.3	Telnet and SSH Settings	70
3.8.4	Configure Web and Telnet Access List	71
4.	Some security recommendations	72
4.1	Administration	72
4.2	OTSBC operation	72
5.	AudioCodes troubleshooting tools for OTSBC	73
5.1	ACSyslog tool	73
5.2	Debug Recording tool	75
6.	SBC profiles configuration in OT using 8770	76
6.1	Creation of the SBC profile for OTCT Remote Workers	76
6.2	Creation and association of the SBC profile for OTCWeb Remote Workers with WebRTC	77
6.3	HTTP proxy server configuration	78
7.	OTC devices configuration	79
7.1	OTC PC Remote Worker in OXE Nomadic SIP mode	79
7.2	OTC PC Remote Worker with OTC Smartphone	80
7.3	OTC PC Remote Worker in OXE SIP Extension mode	80
7.3.1	Configuration of the public Device Management Server	80
7.3.2	SIP extension user and device configuration	82
7.3.3	Considering OXE audio domains with specific audio coders settings	84
7.4	OTC PC Remote Worker video configuration	85
7.4.1	OXE configuration	85
7.4.2	User configuration	86
8.	ALES Remote Worker configuration	87
8.1	HTTP Proxy for DM access	87
8.1.1	Create Upstream Group	87
8.1.2	Add Upstream Host to Upstream Group	88
8.1.3	Create HTTP Directive set	89
8.1.4	Add directives to Directive set	89
8.1.5	Create HTTP Proxy Server	90
8.1.6	Create HTTP Location for Proxy Server	91
8.2	Internal LDAP search for Remote Workers	92
8.2.1	TLS contexts for LDAP	92
8.2.2	Create Upstream Group for LDAP server	92
8.2.3	Create Upstream Hosts for Upstream group	93
8.2.4	Create TCP/UDP Proxy Server	94
9.	Annexes	95
9.1	Procedure to change default UDP port between kamailio-wasp and SIP proxy	95
9.2	Embedded Nginx in a non-IPv6 environment	97

1. Scope

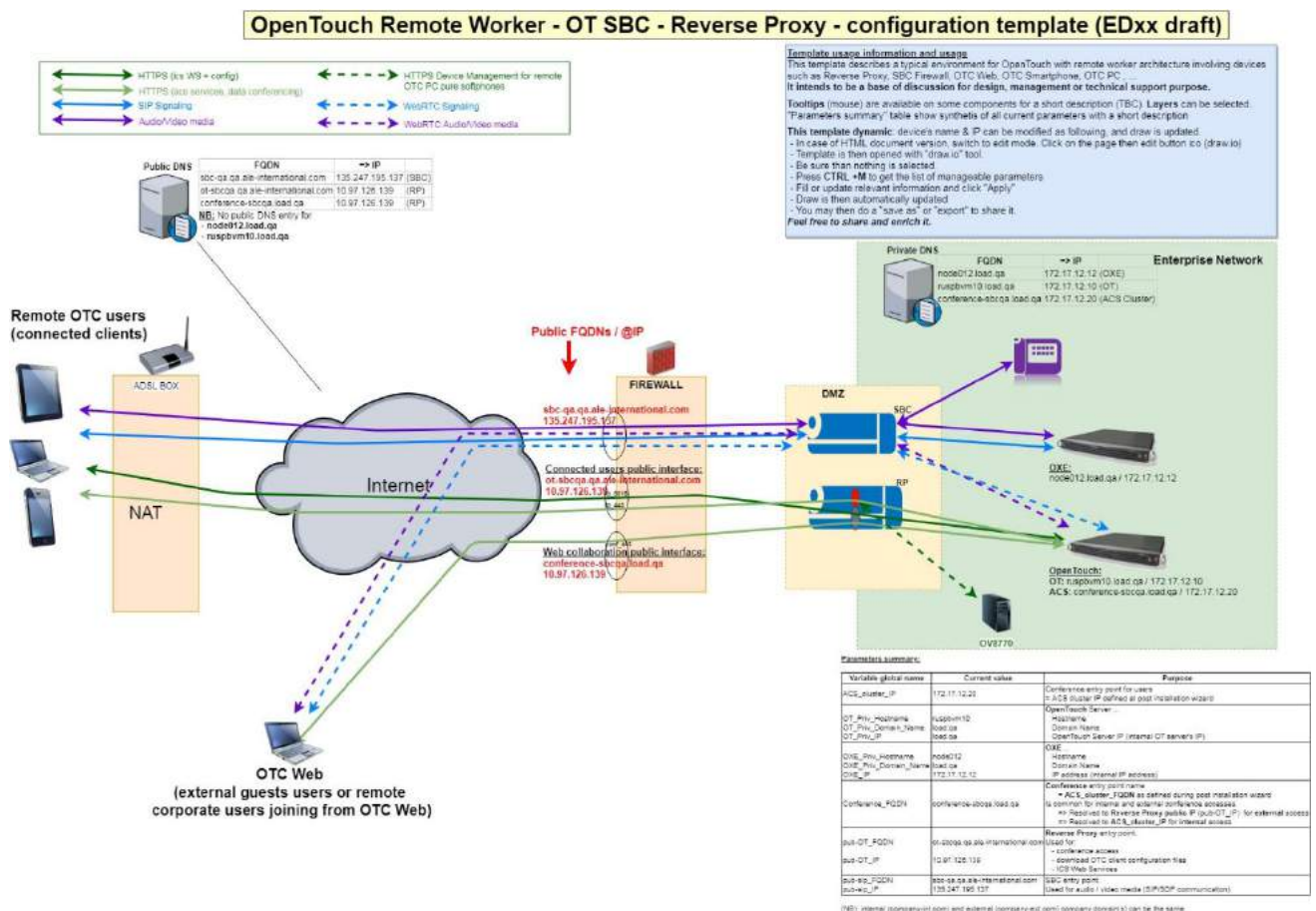
This document describes the recommended configuration of the AudioCodes OTSBC 7.4 device to enable the use of ALES clients in Remote Worker configuration, and OTC clients in VoIP Remote Workers mode. Also, it includes a guide to internal reverse proxy server enabling procedure.

2. OTSBC general Overview

OTSBC 7.4 is used to enable secured communications with SIP TLS signaling and encrypted conversations (SRTP Media) between the compatible SIP devices in the context of OpenTouch solution:

- with Remote Worker users connected to OT/OXE servers from WAN (Internet) domain thanks to
 - o OTC applications on PC, Android smartphones and iPhone devices for OT and OXE servers
 - o Reverse Proxy

2.1 Using OTSBC to secure conversations on corporate LAN and on WAN (Internet)



One considers here 2 interfaces / 2 networks on OTSBC:

- One on corporate LAN domain for OpenTouch and OXE servers that work in non-secured mode (SIP/UDP or SIP/TCP, RTP/UDP),
- One for the WAN domain, allowing SIP secured (SIP/TLS and SRTP) Remote Worker clients to operate with internal OpenTouch and OXE servers through OTSBC in SIP secured mode.

It is possible to use internal Reverse Proxy.

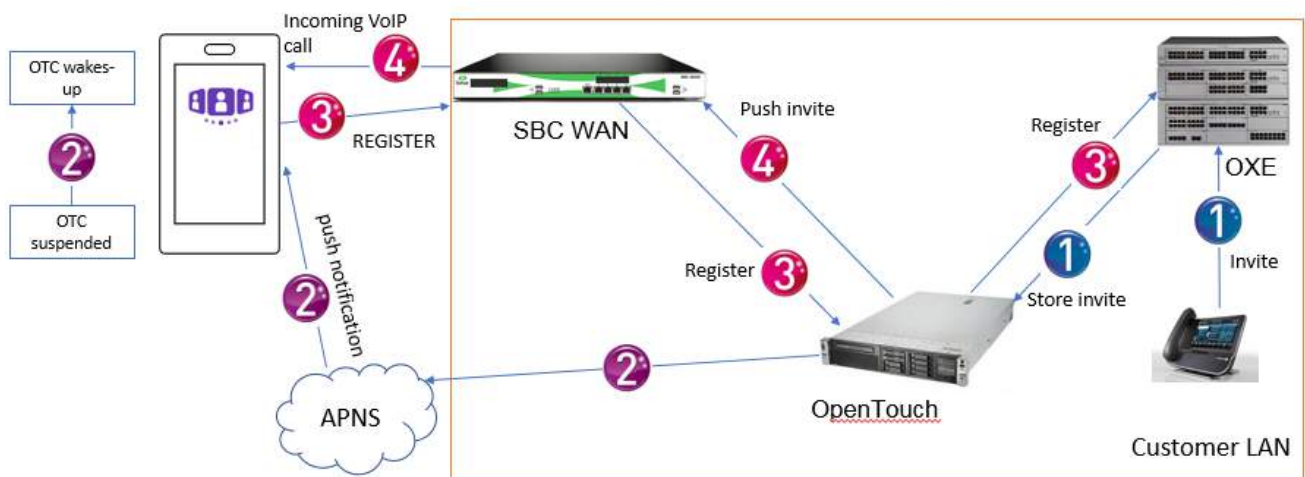
2.2 WAN secured OTC clients VoIP short operating mode

2.2.1 Software clients

OTC software client users have to authenticate both on Reverse Proxy and on OpenTouch server. OTC clients have to accept the certificates of the different edge components (Reverse Proxy, SBC). Providing that VoIP on WAN domain is allowed to OTC client by configuration, OTC client will SIP Register from WAN domain to OpenTouch or OXE server through OTSBC device, allowing some subsequent calls in VoIP mode, in secured mode on WAN side of OTSBC device.

The feature iPhone VOIP everywhere, available from OpenTouch 2.5, requires these SBC additional settings. When the iPhone is in a deep sleep mode, the iPhone can be only waked up by an Apple Notification event (From APNS). When it is received, the OTC application sends a SIP register, to the OXE, to be able to receive calls. A new OpenTouch component "Kamailio" has been added to manage the SIP dialogue with the OXE and the OTC iPhone. "Kamailio" must be added in the SBC configuration like a dedicated SIP Proxy between SBC and OXE

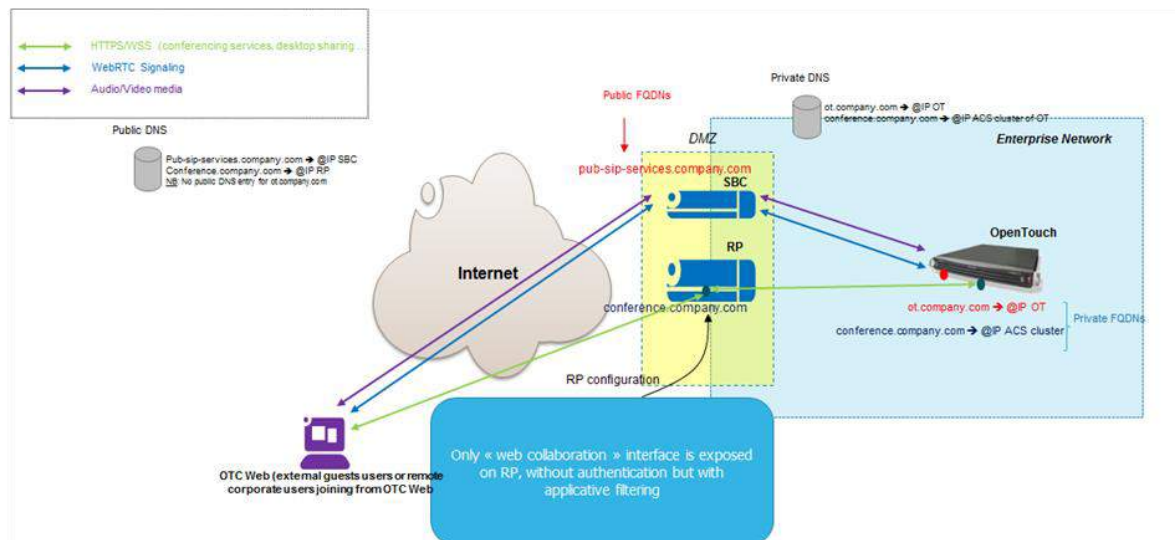
High level Architecture scheme:



2.2.2 OTC Web with WebRTC

OTC-Web application is a pure Web client that runs on any recent browser. Anonymous guest users can simply join an OT conference by typing its valid URI in their browser. Anonymous guest users are not authenticated on Reverse Proxy nor OT. The https conference flows between OTC-Web client on WAN domain and OT server in corporate LAN are handled by the Reverse Proxy by configuration.

By using the WebRTC technology embedded in recent browsers, OTC-Web enables to participate to conferences with audio without the need of a physical telephone. The OTSBC device secures the SIP dialog by Secure web sockets encapsulation and the media by SRTP-DTLS on WAN domain.



3. OTSBC Configuration

This section describes the OTSBC Configuration procedure.

IPv4 only protocol configuration is described in this document.

3.1 OTSBC software installation and basic network connectivity setting

3.1.1 Installation of a virtual machine (Virtual Edition) in VMware environment

The installation of a VM server is described in:

[LTRT-10837 Mediant Virtual Edition\(VE\) SBC Installation Manual Ver. 7.4](#)

1. Deploy the .ovf file

The recommended VMware ESXi Host Server specifications are:

Resource Hypervisor: VMware ESXi version en5.5 or more

Processors: 2 Cores. 4 cores if Transcoding is needed

Memory: 4 GB or more

Disk space: at least 10 GB

Network: two preconfigured virtual networks: one for WAN side (DMZ - untrusted) and one for LAN side (trusted)

- **To configure the admin LAN IP address (using CLI):**

1. Use the VGA monitor and keyboard to connect to the Mediant Software OTSBC's CLI management interface.

2. At the prompt, type the username (default is **Admin** - case sensitive), and then press ENTER:

Username: **Admin**

3. At the prompt, type the password (default is **Admin** - case sensitive), and then press ENTER:

Password: **Admin**

4. At the prompt, type **enable** and press ENTER:

Mediant SW> **enable**

5. At the prompt, type the password again and press ENTER:

Password: **Admin**

6. At the prompt, type the following commands to access the network interface configuration:

Mediant SW# **configure voip**

Mediant SW(config-voip)# **interface network-if 0**

Mediant SW(network-if-0)#

7. At the prompt, type the following commands to configure the corporate network used for LAN users and SBC management (IP address, prefix length and default gateway):

Mediant SW(network-if-0)# **set ip-address 172.26.45.32**

Mediant SW(network-if-0)# **set prefix-length 24**

Mediant SW(network-if-0)# **set gateway 172.26.45.1**

At the prompt, type **exit** to complete the network-if-0 configuration:

Mediant SW(network-if-0)# **exit**

8. If Mediant Software OTSBC is connected to the IP network that uses a VLAN ID (e.g. 10 here), type the following command to configure it (otherwise skip to step 9):

Mediant SW(config-voip)# **interface network-dev 0**


```
Mediant SW(network-dev-0)# vlan-id 10
Mediant SW(network-dev-0)# exit
```

9. At the prompt, type **exit** to complete the configuration:

```
Mediant SW(config-voip)# exit
```

10. At the prompt, type **write** to write the configuration and auxiliary files to NV memory:

```
Mediant SW# write
```

11. At the prompt, type **reload now** to reset the device and activate the new configuration:

```
Mediant SW# reload now
```

12. After the OTSBC restart, connect to its Web interface using the IP address of network-if-0 to continue the provisioning.

3.2 OTSBC main maintenance procedures

3.2.1 License file installation

A valid license file according to the OTSBC serial Number, release and the features needed must be installed to enable the Session Border Controller full functionality:

- Licenses delivered for R&D QA activities are linked to the VM device MAC address.

To find the Device Information:

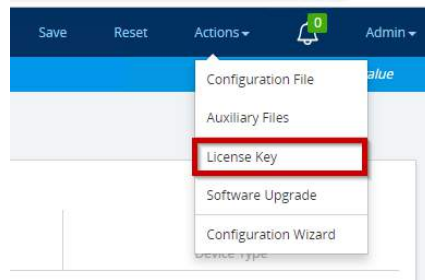
- Open the 'Device Information' page (**Monitor** tab > **Summary** > **Device Information** menu)

The screenshot displays the 'Device Information' page in the OTSBC web interface. The left sidebar shows the navigation menu with 'MONITOR' selected, and 'Device Information' highlighted under the 'SUMMARY' tab. The main content area is divided into two panels. The left panel, titled 'GENERAL SETTINGS', lists various device parameters: MAC Address (00305658621F), Serial Number (176340085386322), Product Key, Board Type (73), Device Up Time (0d:1h:18m:28.91s), Device Administrative State (Unlocked), Device Operational State (Enabled), Flash Size (0 Bytes), RAM Size (7837 Bytes), and CPU Speed (2197 MHz). The right panel, titled 'VERSIONS', shows: Version ID (7.20A.256.399), DSP Type (0), DSP Software Version (0), DSP Software Name (SOPTDSP), and Flash Version (0). A third section, 'LOADED FILES', shows 'Loaded Call Progress Tones' and 'Default Progress Tones'.

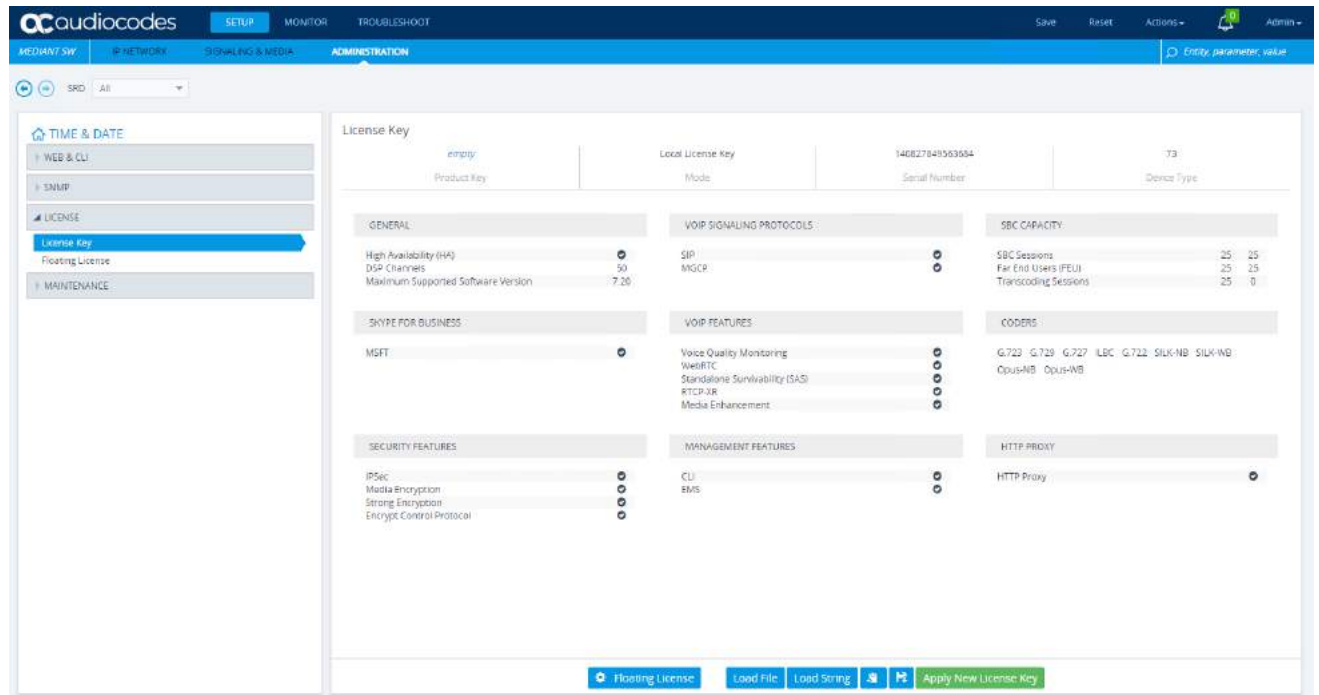
You can also view the Serial Number by CLI (Mediant SW# **show system version**) or in the *Board.ini* configuration file or in Setup/Administration / Maintenance / License Key webadmin menu.

To configure the license Key:

- Open the 'License Key' page (**Setup** tab > **Administration** > **License** tab > **License Key** menu)
- Also it is possible to open 'License Key' page by "Actions" sub-menu.



Put the Software Key file on your PC. 'Load File' or 'Load String' and push 'Apply New License Key'.



Important: preserve the **License Key**. It may be returned for getting a new one if the OTSBC VM is replaced by a new VM with a new MAC Address.

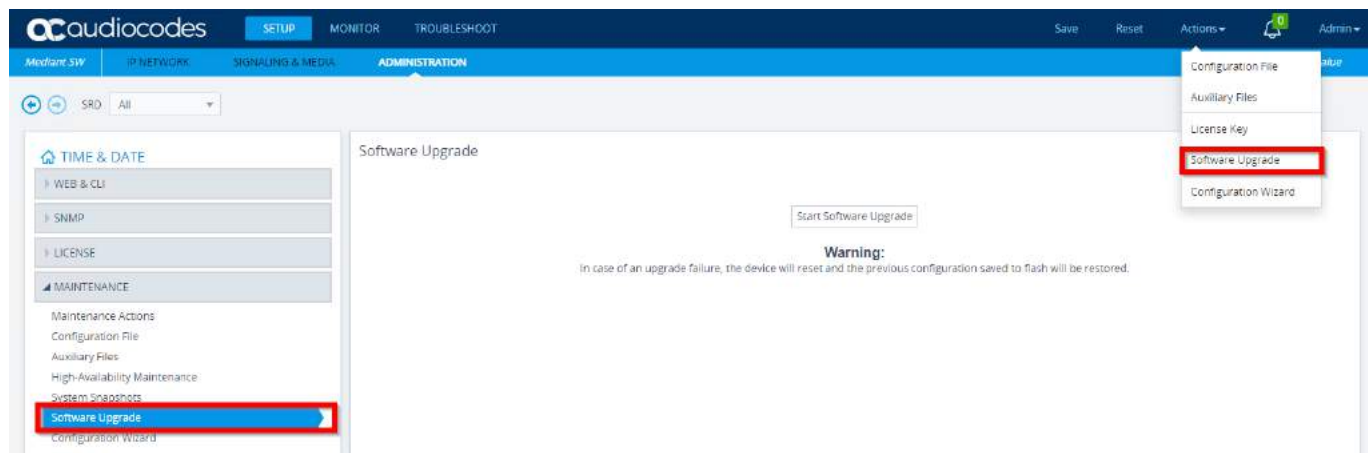
Important: the License Key may content a maximum release domain. Check for its value before upgrading the OTSBC system, elsewhere the network connectivity may be lost.

3.2.2 Software Upgrade with a .cmp file – Software Upgrade Wizard

Note: upgrading OTSBC with a .cmp allows a smooth upgrade from a release 'A' to release 'B':
License key, server certificates and configuration .ini file are not destroyed by this process

To configure the Software Upgrade Wizard:

- Open the 'Software Upgrade Wizard' page (**Setup > Administration > Maintenance > Software Upgrade** menu or **Actions > Software Upgrade**)



- Click on 'Start Software Upgrade' button to start the software upgrade process
- When the Wizard window is opened, browse the .cmp OTSBC software file and push 'Load File'.
- After loading: **'File SWSBC_SIP_F7.XXX.xxx.cmp was successfully loaded into the device'**, push the 'Next' button to load an INI file or to use the existing configuration.
- You can choose to load a PRT file (Prerecorded Tones File) at this step or to continue by clicking 'Next'.
- Then finish by clicking 'Next': **'You have finished the upgrade process. Click the 'Reset' button to burn the configuration to the device flash memory and restart the device.'**



Caution: A License Key file may content a maximum release compatibility domain.
So it may be mandatory to replace the software key before some upgrades.

3.3 OTSBC Configuration procedure

This section describes how to navigate in the Web server navigation tree of the OTSBC.

To connect on OTSBC (after its first network settings done): `http:// "IP address of OTSBC"`

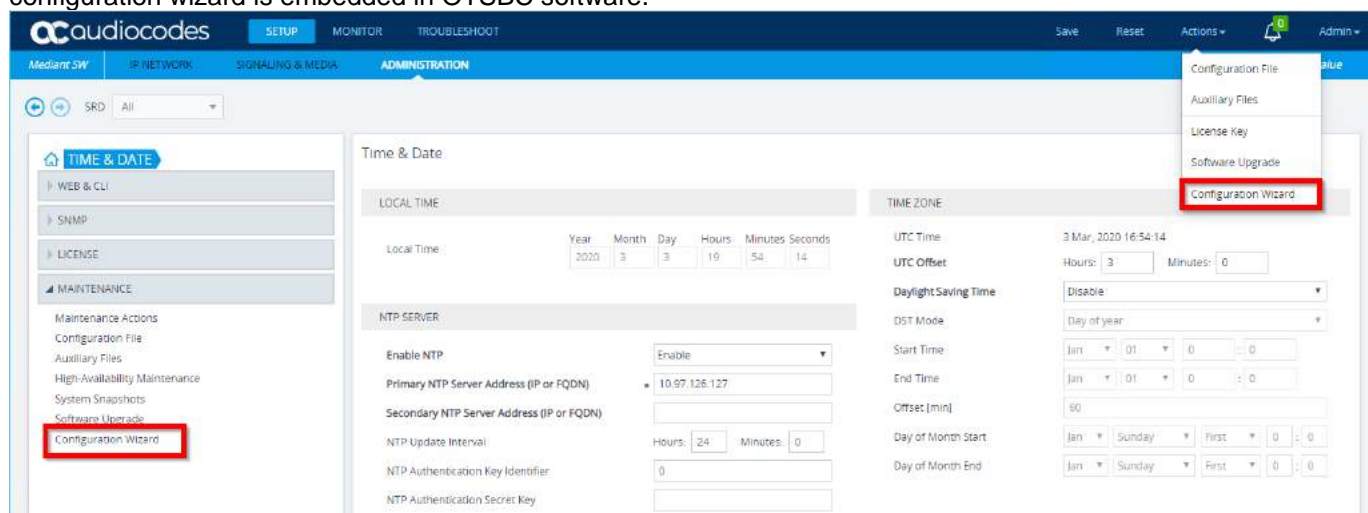
Login (default): **Admin** password (default): **Admin**

HTTP and telnet (non-secured mode) are enabled by default. *To secure the access to the device configuration and maintenance, you can change later the values of the Web Security and Telnet/SSH settings in System/Management.*

For any SBC configuration from scratch for Remote Worker use case, it is recommended to use the AudioCodes internal Configuration Wizard tool.

3.3.1 Configuring an OTSBC using the AudioCodes wizard tool

AudioCodes SBC wizard tool is the easiest way to start the SBC configuration from scratch. Since 7.2, a configuration wizard is embedded in OTSBC software.



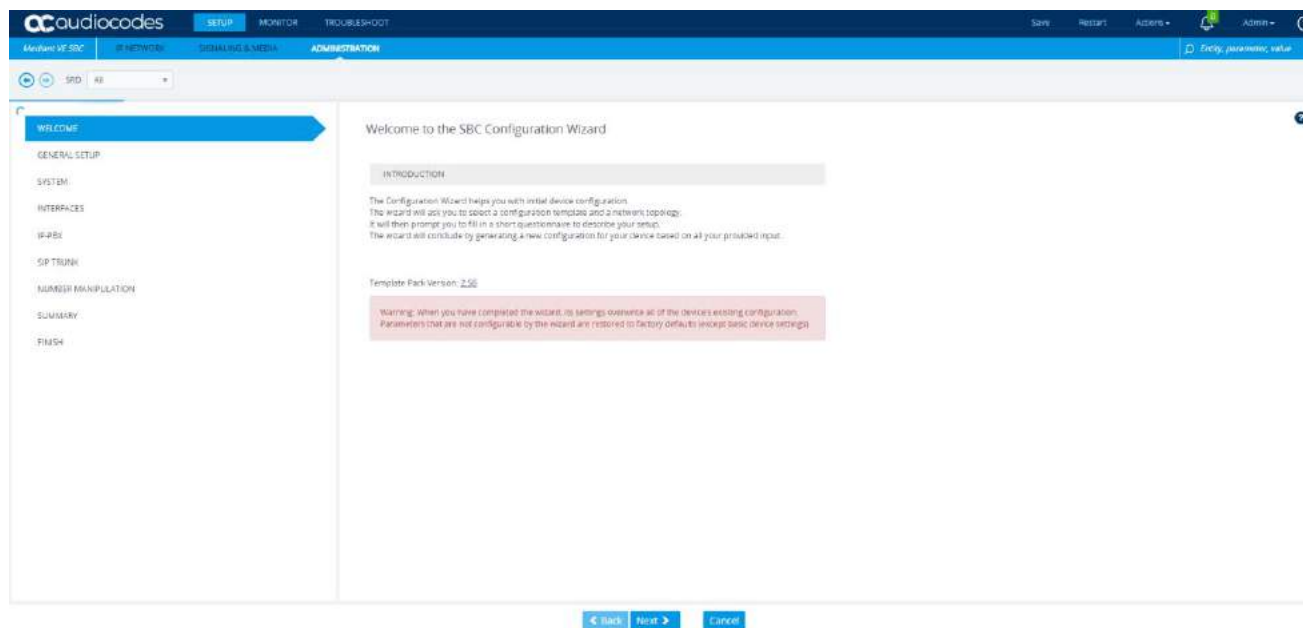
Notes:

- The "external" PC configuration wizard still exist and can be used instead.
- The wizard tools automatically check for updates at start if the device has a direct access to Internet (there must be no proxy configured).

The wizard generates a configuration file (.ini) for your SBC device using some pre-loaded templates according to the applications /use cases needed (OTC Remote Workers, with or without SIP trunking) and the network deployment topology (one or two SBC IP interfaces, OT node with or without OXE node, secure/non-secure domains, IP/VLAN/FQDNs in use).

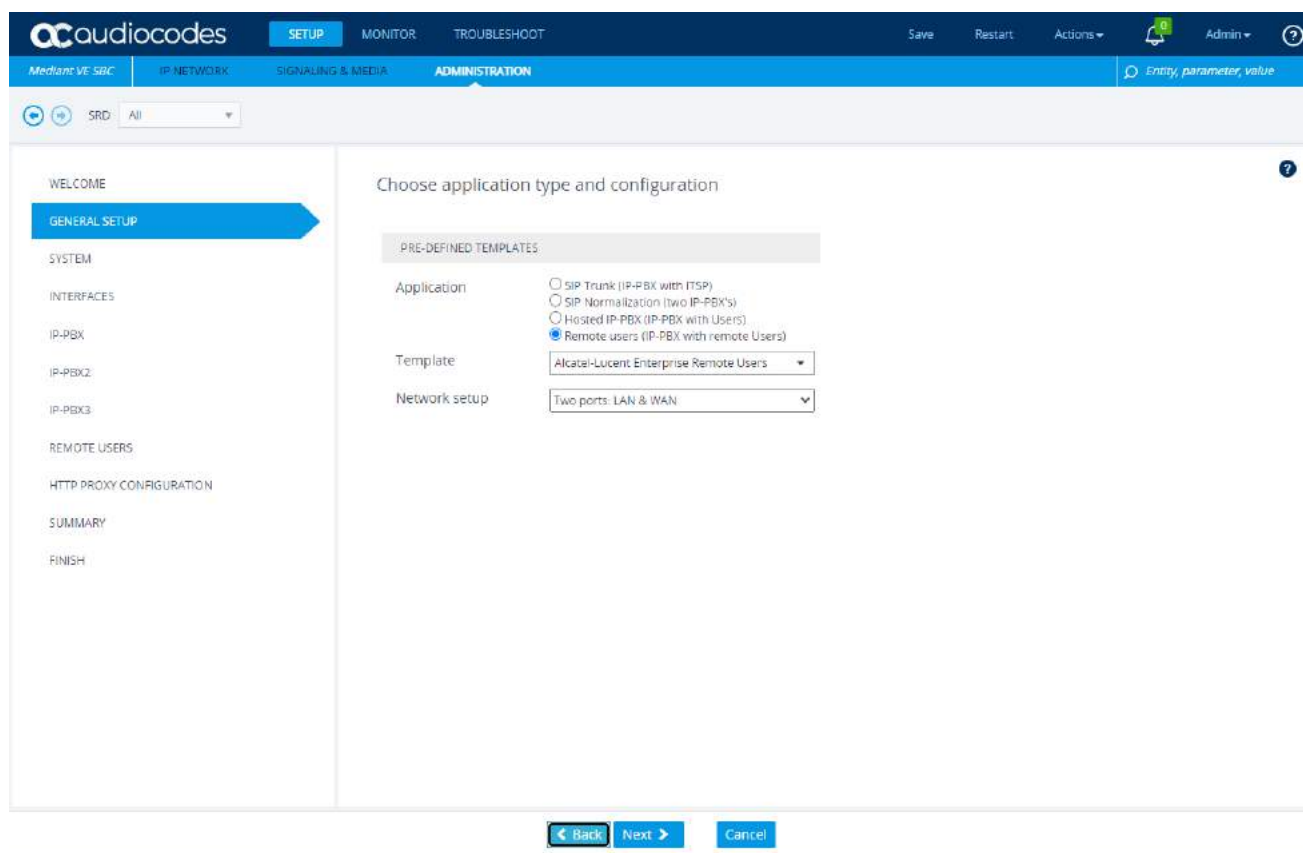
Here is an example of OTSBC 7.4 embedded wizard run for Alcatel-Lucent Enterprise Remote users use case:

- **Step 1 “Welcome”**



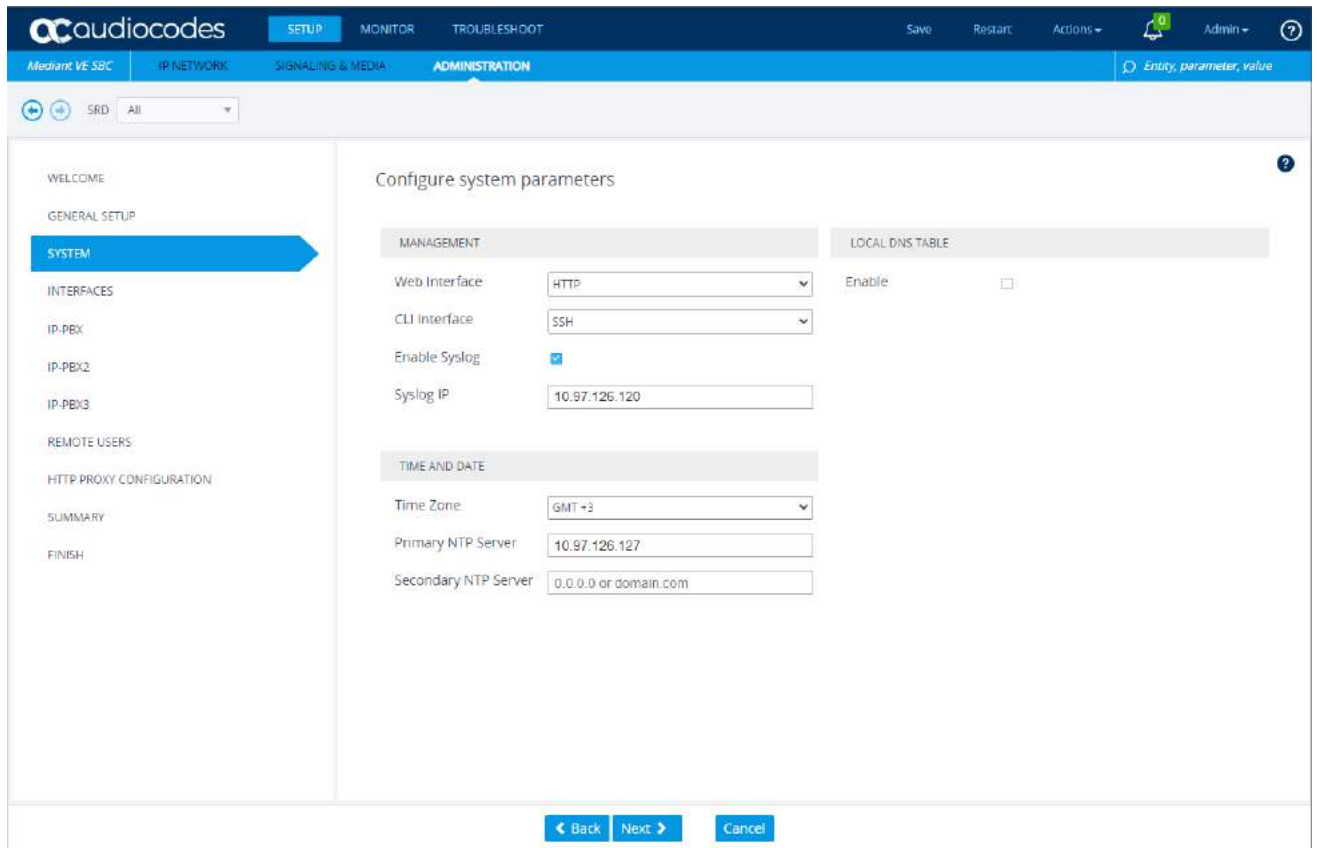
The screenshot shows the Audiocodes SBC Configuration Wizard. The left sidebar contains a navigation menu with the following items: WELCOME, GENERAL SETUP, SYSTEM, INTERFACES, IP-PBX, SIP TRUNK, NUMBER MANIPULATION, SUMMARY, and FINISH. The 'WELCOME' item is highlighted. The main content area displays the 'Welcome to the SBC Configuration Wizard' message. Below this, there is an 'INTRODUCTION' section explaining the wizard's purpose. A 'Template Pack Version: 2.56' is noted. A warning message states: 'Warning: When you have completed the wizard, its settings override all of the devices existing configuration. Parameters that are not configurable by the wizard are restored to factory defaults (except basic device settings)'. At the bottom, there are 'Back', 'Next', and 'Cancel' buttons.

- **Step 2 “General Setup”**: choose “Remote Users” Application IP-PBX with Remote Users”,
- apply the Template “Alcatel-Lucent Remote Users”
 - choose a “Two ports: LAN and WAN” network setup for SBC: the WAN side interfaces to the corporate FW/NAT, while the LAN side interfaces to the Voice/Applications servers OT and OXE



The screenshot shows the Audiocodes SBC Configuration Wizard - General Setup screen. The left sidebar contains the same navigation menu as the previous screen, with 'GENERAL SETUP' highlighted. The main content area displays the 'Choose application type and configuration' section. Under 'PRE-DEFINED TEMPLATES', there are three radio buttons for 'Application': 'SIP Trunk (IP-PBX with ITSP)', 'SIP Normalization (two IP-PBX's)', and 'Hosted IP-PBX (IP-PBX with Users)'. The 'Remote users (IP-PBX with remote Users)' option is selected. Below this, there are two dropdown menus: 'Template' (set to 'Alcatel-Lucent Enterprise Remote Users') and 'Network setup' (set to 'Two ports: LAN & WAN'). At the bottom, there are 'Back', 'Next', and 'Cancel' buttons.

- **Step 3 “System”**: declare your primary NTP server, change the Time Zone if necessary, choose https preferably as the web interface protocol, configure syslog if needed.



The screenshot shows the Audiocodes Mediant VE SBC configuration interface. The top navigation bar includes 'SETUP', 'MONITOR', and 'TROUBLESHOOT'. The left sidebar lists various configuration sections: WELCOME, GENERAL SETUP, SYSTEM (highlighted), INTERFACES, IP-PBX, IP-PBX2, IP-PBX3, REMOTE USERS, HTTP PROXY CONFIGURATION, SUMMARY, and FINISH. The main content area is titled 'Configure system parameters' and contains two sections: 'MANAGEMENT' and 'LOCAL DNS TABLE'.

MANAGEMENT

- Web Interface: HTTP
- CLI Interface: SSH
- Enable Syslog: ☒
- Syslog IP: 10.97.126.120

TIME AND DATE

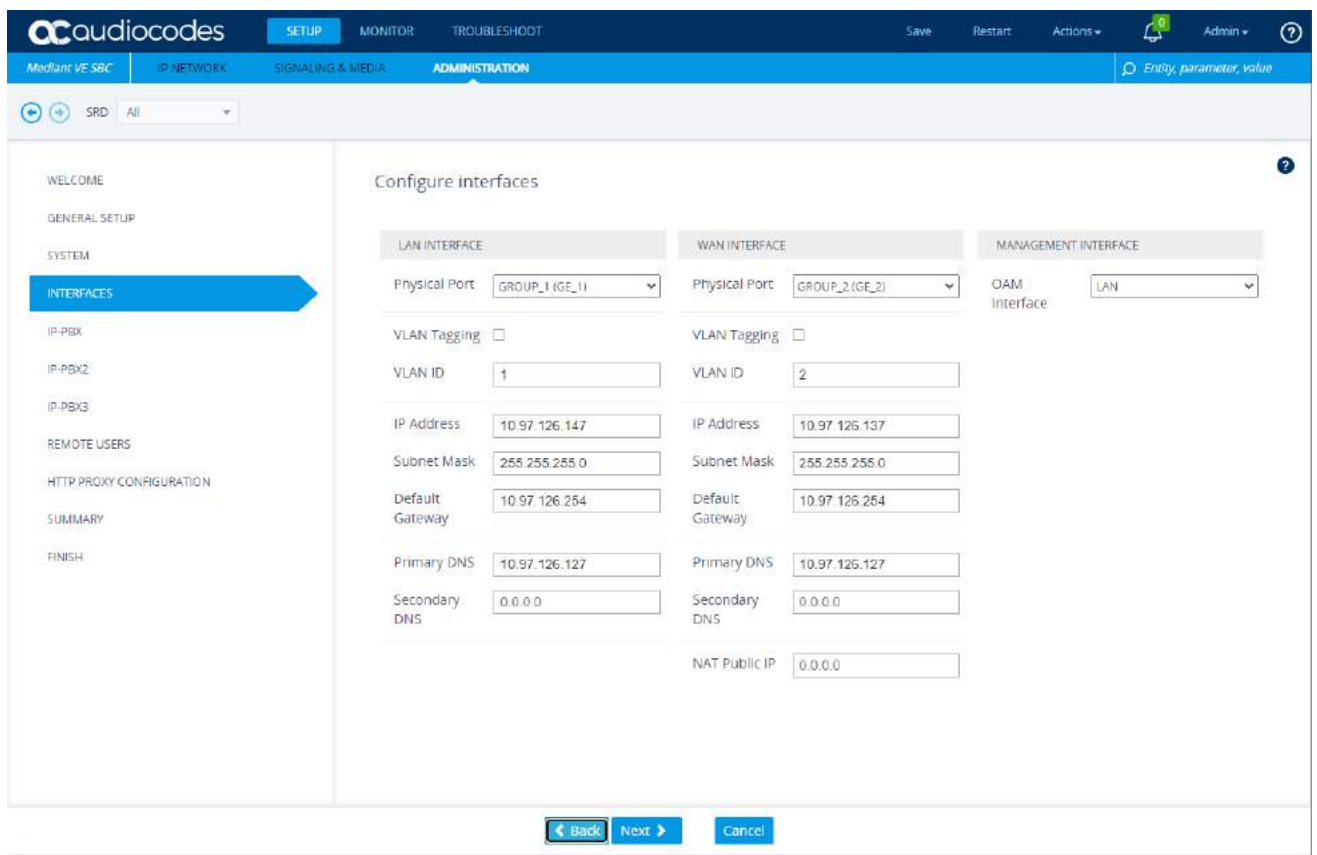
- Time Zone: GMT +3
- Primary NTP Server: 10.97.126.127
- Secondary NTP Server: 0.0.0.0 or domain.com

LOCAL DNS TABLE

- Enable: ☐

At the bottom of the screen are buttons for 'Back', 'Next', and 'Cancel'.

- **Step 4 "Interfaces":** configure the LAN and the WAN interfaces. Declare the public NAT IP address.



The screenshot shows the Audiocodes Mediant VE SBC configuration interface. The top navigation bar includes 'SETUP', 'MONITOR', and 'TROUBLESHOOT'. The left sidebar lists various configuration sections: WELCOME, GENERAL SETUP, SYSTEM, INTERFACES (highlighted), IP-PBX, IP-PBX2, IP-PBX3, REMOTE USERS, HTTP PROXY CONFIGURATION, SUMMARY, and FINISH. The main content area is titled 'Configure interfaces' and contains three sections: 'LAN INTERFACE', 'WAN INTERFACE', and 'MANAGEMENT INTERFACE'.

LAN INTERFACE

- Physical Port: GROUP_1 (GE_1)
- VLAN Tagging: ☐
- VLAN ID: 1
- IP Address: 10.97.126.147
- Subnet Mask: 255.255.255.0
- Default Gateway: 10.97.126.254
- Primary DNS: 10.97.126.127
- Secondary DNS: 0.0.0.0

WAN INTERFACE

- Physical Port: GROUP_2 (GE_2)
- VLAN Tagging: ☐
- VLAN ID: 2
- IP Address: 10.97.126.137
- Subnet Mask: 255.255.255.0
- Default Gateway: 10.97.126.254
- Primary DNS: 10.97.126.127
- Secondary DNS: 0.0.0.0
- NAT Public IP: 0.0.0.0

MANAGEMENT INTERFACE

- OAM Interface: LAN

At the bottom of the screen are buttons for 'Back', 'Next', and 'Cancel'.

- **Step 5 "IP-PBX":** declare the OXE IP address its FQDN in SIP Domain field. Change only if necessary the default 5060 SIP port, Media port start and/or planned max quantity of OTCT sessions values.

The screenshot shows the Audiocodes Mediant VE-SBC configuration interface. The left sidebar contains a navigation menu with options: WELCOME, GENERAL SETUP, SYSTEM, INTERFACES, IP-PBX (highlighted), IP-PBX2, IP-PBX3, REMOTE USERS, HTTP PROXY CONFIGURATION, SUMMARY, and FINISH. The main content area is titled "IP-PBX configuration" and contains the following fields:

- NETWORK INTERFACE:** Network Type (LAN)
- IP-PBX:** Address (172.17.12.12), Backup Address (0.0.0.0 or domain.com), SIP Domain (node012.load.qa), Keep Alive (checkbox)
- SIP INTERFACE:** Transport Type (UDP), Destination Port (5060), Listening Port (5060)
- MEDIA PORTS (REALM):** Media Protocol (RTP), Base Port (6000), Number Of Sessions (30)

At the bottom of the configuration area are buttons for "Back", "Next", and "Cancel".

- **Step 6 "IP-PBX2":** declare the OpenTouch IP address and its FQDN node in SIP Domain field. Change only if necessary the default 5260 SIP port, Media port start and/or planned max quantity of sessions.

The screenshot shows the Audiocodes Mediant VE-SBC configuration interface. The left sidebar contains a navigation menu with options: WELCOME, GENERAL SETUP, SYSTEM, INTERFACES, IP-PBX, IP-PBX2 (highlighted), IP-PBX3, REMOTE USERS, HTTP PROXY CONFIGURATION, SUMMARY, and FINISH. The main content area is titled "IP-PBX2 configuration" and contains the following fields:

- REMOTE USERS:** Use additional server for Remote Users (checkbox)
- NETWORK INTERFACE:** Network Type (LAN)
- IP-PBX2:** Address (172.17.12.10), Backup Address (0.0.0.0 or domain.com), SIP Domain (ruspbvm10.load.qa), Keep Alive (checkbox)
- SIP INTERFACE:** Transport Type (UDP), Destination Port (5260), Listening Port (5260)
- MEDIA PORTS (REALM):** Media Protocol (RTP), Base Port (6200), Number Of Sessions (30)

At the bottom of the configuration area are buttons for "Back", "Next", and "Cancel".

- **Step 7 "IP-PBX3":** declare the OpenTouch IP address and its FQDN node in SIP Domain field. Change only if necessary the default 5160 and 5260 SIP ports, Media port start and/or planned max quantity of OTCT sessions.

The screenshot shows the Audiocodes Mediant VE SBC configuration interface. The left sidebar contains a navigation menu with options: WELCOME, GENERAL SETUP, SYSTEM, INTERFACES, IP-PBX, IP-PBX2, IP-PBX3 (highlighted), REMOTE USERS, HTTP PROXY CONFIGURATION, SUMMARY, and FINISH. The main content area is titled 'IP-PBX3 configuration'. It includes sections for 'REMOTE USERS' (with a checkbox 'Use additional server for Remote Users' checked), 'NETWORK INTERFACE' (Network Type: LAN), 'IP-PBX3' (Address: 172.17.12.10, Backup Address: 0.0.0.0 or domain.com, SIP Domain: ruspbvm10.load.qa, Keep Alive: unchecked), 'SIP INTERFACE' (Transport Type: UDP, Destination Port: 5160, Listening Port: 5260), and 'MEDIA PORTS (REALM)' (Media Protocol: RTP, Base Port: 6400, Number Of Sessions: 30). At the bottom are 'Back', 'Next', and 'Cancel' buttons.

- **Step 8 “Remote Users”:** declare in SIP CLIENTS (OXE) ‘SIP Domain’ the public FQDN used by OTCT to reach OT and OXE servers via the SBC device. Change the default SIP ports and secured protocol values only if necessary. Replace the default value in OTC WEBRTC ‘SIP Domain’ by the LAN FQDN of OT server.

The screenshot shows the Audiocodes Mediant VE SBC configuration interface. The left sidebar contains a navigation menu with options: WELCOME, GENERAL SETUP, SYSTEM, INTERFACES, IP-PBX, IP-PBX2, IP-PBX3, REMOTE USERS (highlighted), HTTP PROXY CONFIGURATION, SUMMARY, and FINISH. The main content area is titled 'Remote Users configuration'. It includes sections for 'NETWORK INTERFACE' (Network Type: WAN, NAT Public IP: empty), 'MEDIA PORTS (REALM)' (Base Port: 6600, Number Of Sessions: 30), 'SIP CLIENTS (OXE)' (Enabled: checked, Transport Type: TLS, Listening Port: 5261, Media Protocol: SRTP, SIP Domain: sbc-qa.qa.ale-international.com), 'OTC IPHONE (OXE)' (Enabled: checked, Transport Type: TLS, Listening Port: 5261, Media Protocol: SRTP, Enable SIP Domain: unchecked, SIP Domain: sbc-qa.qa.ale-international.com), and 'OTC WEBRTC (OPENTOUCH)' (Enabled: checked, Transport Type: WebRTC, Listening Port: 8061, Media Protocol: SRTP, Enable SIP Domain: checked, SIP Domain: ruspbvm10.load.qa). At the bottom are 'Back', 'Next', and 'Cancel' buttons.

- **Step 9 “HTTP proxy configuration”:** This option is used for ALES clients to access DM files on the OXE. Enable “Use HTTP proxy”, uncheck “Use LDAP Authentication” if not needed. Enter external

FQDN for Reverse Proxy in "External Domain Name" field. Fill "Internal Host" with OXE FQDN or IP. If LDAP Authentication is used, fill "LDAP URL", "Username" and "Password"

The screenshot displays the Audiocodes Mediant VE SBC Administration web interface. The top navigation bar includes tabs for SETUP, MONITOR, and TROUBLESHOOT. The left sidebar lists various configuration sections, with 'HTTP PROXY CONFIGURATION' highlighted in blue. The main content area is titled 'HTTP proxy configuration' and contains three sections: 'HTTP PROXY', 'GENERIC', and 'LDAP AUTHENTICATION'. In the 'HTTP PROXY' section, 'Use HTTP proxy' and 'Use LDAP Authentication' are both checked. The 'GENERIC' section includes fields for 'External Domain Name' (ot-sbc.qa.ale-international.com), 'URL Path' (/DM/dmssoftphone/), and 'Internal Host' (172.17.12.12). The 'LDAP AUTHENTICATION' section includes fields for 'LDAP URL' (ldap://ldap.server.local:389/CN=Users,DC=), 'Username' (Administrator), and 'Password' (Password). At the bottom of the form are buttons for 'Back', 'Next', and 'Cancel'.

HTTP PROXY	
Use HTTP proxy	<input checked="" type="checkbox"/>
Use LDAP Authentication	<input checked="" type="checkbox"/>

GENERIC	
External Domain Name	ot-sbc.qa.ale-international.com
URL Path	/DM/dmssoftphone/
Internal Host	172.17.12.12

LDAP AUTHENTICATION	
LDAP URL	ldap://ldap.server.local:389/CN=Users,DC=
Username	Administrator
Password	Password

Known issue (not reproduced in the external wizard tool):

[CROT-10720](#) : SBC internal wizard does not add the Reverse Proxy configuration to the ini file

- **Step 10 “Summary”**: check for the overall values and modify if necessary using “Back”

Configuration Summary

Category	Parameter	Value
General Setup	Network setup	Two ports: LAN & WAN
	Application	RemoteUsers
	Template	Alcatel-Lucent Enterprise Remote Users
System	Web Interface	HTTP
	CLI Interface	SSH
	Syslog IP	10.97.126.120
	Primary NTP Server	10.97.126.127
Interfaces	Physical Port	GROUP_1 (GE_1)
	VLAN ID	1
	OAM Interface	LAN
	VLAN Tagging	No
	IP Address	10.97.126.147
	Subnet Mask	255.255.255.0
	Default Gateway	10.97.126.254
	Primary DNS	10.97.126.127
	Physical Port	GROUP_2 (GE_2)
	VLAN ID	2
IP-PBX	Media Protocol	RTP
	Transport Type	UDP
	Network Type	LAN
	Address	172.17.12.12
	SIP Domain	node012.load.qa
	Keep Alive	No
	Base Port	6000
	Number Of Sessions	30
	Destination Port	5060
	Listening Port	5060

- Use “Save INI file” on the local PC or/and “Apply & Reset” the configuration file to the OTSBC device.

Congratulations!

You have successfully completed the SBC Configuration wizard. Click "Apply & Reset" button to activate the new configuration. Note that device will be restarted and it may take up to 4 minutes before it completes activation. The generated configuration file is a good "starting point" that enables successful establishment of basic calls. For complete device configuration you may need to configure additional functionality. For example, you may need to add security configuration (e.g. Firewalls, IDS) to ensure that SBC is protected from malicious user activity and DoS attacks. Refer to the User Manual for more information.

WARNING: Applying this configuration will overwrite all of the existing device configuration.

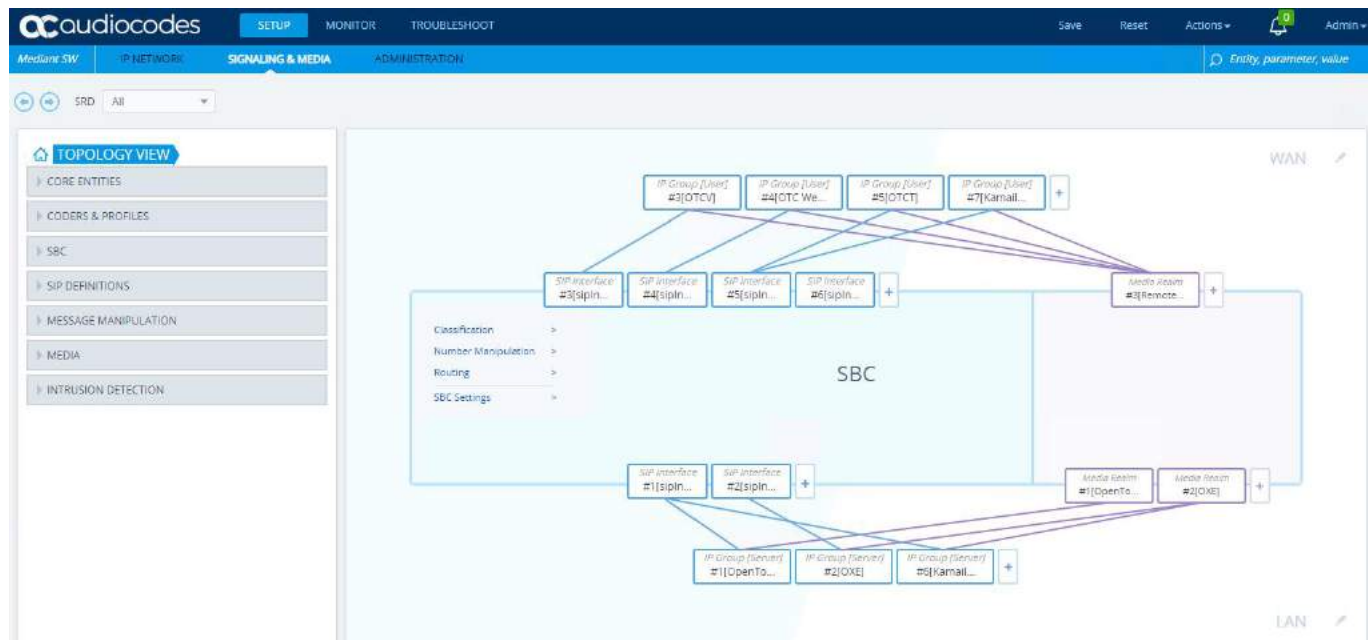
Apply & Reset

3.3.2 OTSBC web admin menu

[http\(s\)://<OTSBC admin IP address>](http(s)://<OTSBC admin IP address>) or [http\(s\)://<OTSBC admin FQDN>](http(s)://<OTSBC admin FQDN>)

Topology view:

SBC webadmin shows by default the TOPOLOGY VIEW which is a functional view of the running configuration: here WAN and LAN domains along with their SIP interfaces, SIP servers (IP-PBXs) and Remote workers types configured by Wizard. It is located under **SETUP > SIGNALING & MEDIA**.



The upper bar always gives a quick access to SET UP (configuration), MONITOR, TROUBLESHOOT, Save, Reset, Alarms monitoring and direct Actions (configuration file management, Auxiliary Files management, License Key management, Software Upgrade management and Configuration Wizard).

Device Information view:

- Select MONITOR / MONITOR.
- Main General Information
- Alarms – color changes from green to orange if any alarm is on. Alarms can be displayed by clicking on 'Alarms' button (same as in MONITOR > Summary > Active Alarms)
- Network ports – color changes when disconnect – some information displayed by clicking on them (same as in MONITOR > Network status > Ethernet Port Information)

Mediant SW Monitor

Address: 10.97.126.147 | Firmware: 7.20A.256.399 | Mediant SW Type: | S/N: 176340035360122

SBC Metrics:

- Active Calls: 0
- Average Success Ratio (ASR): N/A
- Average Call Duration (ACD): N/A
- Calls per Sec.: 0
- Transactions per Sec.: 0
- Registered Users: 0

3.3.3 Physical ports, Ethernet devices, Ethernet groups and IP interfaces

Unless when noted, all these objects are already configured if wizard has been used.

To manually configure / modify the Ethernet Device table :

- Open 'Ethernet Devices' page (**SETUP > IP NETWORK > CORE ENTITIES > Ethernet Devices**)

Ethernet Devices (2)

INDEX	VLAN ID	UNDERLYING INTERFACE	NAME	TAGGING	MTU
0	1	GROUP_1	LAN_DEV	Untagged	1500
1	2	GROUP_2	WAN_DEV	Untagged	1500

#0[LAN_DEV]

GENERAL

Name: LAN_DEV

VLAN ID: 1

Underlying interface: GROUP_1 [View](#)

Tagging: Untagged

MTU: 1500

Note: Native VLANs (VLAN IDs) and Names must be different for each Ethernet Port, even without tagging. Use the real VLAN numbers if tagging is used.

The Physical Ports Table:

The physical ports have been created along with the Ethernet Devices.

The screenshot shows the Audiocodes configuration interface. The left sidebar contains a 'NETWORK VIEW' menu with options like 'CORE ENTITIES', 'IP Interfaces (3)', 'Ethernet Devices (2)', 'Ethernet Groups (15)', 'Physical Ports (2)', 'Static Routes (0)', 'HA Settings', 'HA Network Monitor (0)', 'NAT Translation (5)', 'SECURITY', 'QUALITY', 'DNS', 'WEB SERVICES', 'HTTP PROXY', 'RADIUS & LDAP', 'MEDIA CLUSTER', and 'ADVANCED'. The main area displays the 'Physical Ports (2)' table. Below the table, the details for '#0[GE_1]' are shown, including a 'GENERAL' section with fields for Name, Description, Mode, and Speed and Duplex, and an 'ETHERNET GROUP' section with fields for Member of Ethernet Group and Group Status.

INDEX	NAME	MODE	SPEED AND DUPLEX	DESCRIPTION	MEMBER OF ETHERNET GROUP	GROUP STATUS
0	GE_1	Enable	Auto Negotiation	LAN Port	GROUP_1	Active
1	GE_2	Enable	Auto Negotiation	WAN Port	GROUP_2	Active

#0[GE_1]

GENERAL

Name	GE_1
Description	LAN Port
Mode	Enable
Speed and Duplex	Auto Negotiation

ETHERNET GROUP

Member of Ethernet Group	GROUP_1
Group Status	Active

The Ethernet Groups :

Ethernet Groups enable link redundancy capability. By default the configured mode is 'single'.

The screenshot shows the Audiocodes configuration interface. The left sidebar contains a 'NETWORK VIEW' menu with options like 'CORE ENTITIES', 'IP Interfaces (3)', 'Ethernet Devices (2)', 'Ethernet Groups (15)', 'Physical Ports (2)', 'Static Routes (0)', 'HA Settings', 'HA Network Monitor (0)', 'NAT Translation (5)', 'SECURITY', 'QUALITY', 'DNS', 'WEB SERVICES', 'HTTP PROXY', 'RADIUS & LDAP', 'MEDIA CLUSTER', and 'ADVANCED'. The main area displays the 'Ethernet Groups (15)' table. Below the table, the details for '#0[GROUP_1]' are shown, including a 'GENERAL' section with fields for Name, Mode, Member 1, and Member 2.

INDEX	NAME	MODE	MEMBER 1	MEMBER 2
0	GROUP_1	SINGLE	GE_1	---
1	GROUP_2	SINGLE	GE_2	---
2	GROUP_3	NONE	---	---
3	GROUP_4	NONE	---	---
4	GROUP_5	NONE	---	---
5	GROUP_6	NONE	---	---
6	GROUP_7	NONE	---	---
7	GROUP_8	NONE	---	---
8	GROUP_9	NONE	---	---
9	GROUP_10	NONE	---	---

#0[GROUP_1]

GENERAL

Name	GROUP_1
Mode	SINGLE
Member 1	GE_1 View
Member 2	--- View

The IP Interfaces :

To manually configure / modify the IP Interfaces table:

- Open the 'IP Interfaces' page (SETUP > IP NETWORK > CORE ENTITIES > IP Interfaces)

The screenshot shows the 'IP Interfaces' configuration page in the Alcatel-Lucent OTSBC interface. The left sidebar contains a 'NETWORK VIEW' menu with options like Ethernet Devices, Ethernet Groups, Physical Ports, Static Routes, HA Settings, HA Network Monitor, and NAT Translation. The main area displays a table of IP Interfaces with columns: INDEX, NAME, APPLICATION TYPE, INTERFACE MODE, IP ADDRESS, PREFIX LENGTH, DEFAULT GATEWAY, PRIMARY DNS, SECONDARY DNS, and ETHERNET DEVICE. Below the table, the configuration details for the selected interface '#0[eth0]' are shown, including General, IP Address, and DNS settings.

INDEX	NAME	APPLICATION TYPE	INTERFACE MODE	IP ADDRESS	PREFIX LENGTH	DEFAULT GATEWAY	PRIMARY DNS	SECONDARY DNS	ETHERNET DEVICE
0	eth0	OAMP + Media + Control	IPv4 Manual	10.97.126.147	24	10.97.126.254	10.97.126.127		LAN_DEV
1	eth1	Media + Control	IPv4 Manual	10.97.126.137	24	10.97.126.254	10.97.126.127		WAN_DEV
2	RP	Media + Control	IPv4 Manual	10.97.126.139	24	10.97.126.254	10.97.126.127	0.0.0.0	LAN_DEV

Configuration details for #0[eth0]:

GENERAL		IP ADDRESS	
Name	* eth0	Interface Mode	IPv4 Manual
Application Type	* OAMP + Media + Control	IP Address	* 10.97.126.147
Ethernet Device	* LAN_DEV	Prefix Length	* 24
		Default Gateway	* 10.97.126.254

DNS settings:

DNS	
Primary DNS	* 10.97.126.127
Secondary DNS	*

- Set the following parameter for LAN, WAN and RP(if you want to use integrated NGINX instead of HTTP Reverse Proxy server (see 4.4)) interfaces:

Application Type: set 'OAMP + Media + Control' on LAN interface. Avoid using OAMP function -Web management interface- on WAN side. Set "Media + Control" on WAN and RP interfaces.

IP-Address: LAN: <OAMP and Voice LAN IP-Address> WAN: <DMZ IP-Address> RP: <DMZ IP-Address>

Prefix Length: The Subnet Mask length in bits (e.g., 24 for 255.255.255.0).

Gateway: <Default Gateway>

Primary DNS Server IP Address: <First DNS server available for this interface>

Secondary DNS Server IP Address: <Second DNS server available for this interface>

Underlying Device: <name of Underlying Interface Ethernet device>

Note: Whenever a reset with Save to Flash is required, the Save and Reset buttons are encircled with red in the upper line:



The screenshot shows the Audiocodes Mediant SW Administration interface. The left sidebar contains a menu with 'TIME & DATE' and 'MAINTENANCE' expanded. Under 'MAINTENANCE', 'Maintenance Actions' is selected. The main content area is titled 'Maintenance Actions' and contains two sections: 'RESET DEVICE' and 'LOCK / UNLOCK'. In the 'RESET DEVICE' section, there are three rows: 'Reset Device' with a red arrow pointing to a 'RESET' button, 'Save To Flash' with a dropdown set to 'Yes', and 'Graceful Reset' with a dropdown set to 'No'. In the 'LOCK / UNLOCK' section, there are three rows: 'Lock' with a 'LOCK' button, 'Graceful Option' with a dropdown set to 'No', and 'Disconnect Client Connections' with a dropdown set to 'Disable'. The 'Device Operational State' is shown as 'UNLOCKED'. Below these sections, there is a note: 'For Reset Device: If you choose not to save the device's configuration to flash memory, all changes made since the last time the configuration was saved will be lost after the device is reset. For Save Configuration: Saving configuration to flash memory may cause some temporary degradation in voice quality, therefore, it is recommended to perform this during low-traffic periods.'

3.3.4 General Media Setting for NAT Traversal

To enable NAT Traversal for media:

- Open the 'Media Settings' page (**SETUP > SIGNALING & MEDIA > MEDIA > Media Settings**)
- Set NAT Traversal to 'Enable NAT Only If Necessary'

The screenshot shows the Audiocodes Mediant SW Administration interface. The left sidebar contains a menu with 'TOPOLOGY VIEW' and 'MEDIA' expanded. Under 'MEDIA', 'Media Settings' is selected. The main content area is titled 'Media Settings' and contains two sections: 'GENERAL' and 'ROBUSTNESS'. In the 'GENERAL' section, 'NAT Traversal' is highlighted with a red box and has a dropdown set to 'Enable NAT Only If Necessary'. Other settings in 'GENERAL' include 'Enable Continuity Tones' (Disable), 'Number of Media Channels' (10000), 'Enforce Media Order' (Disable), and 'SDP Session Owner' (AudiocodesGW). In the 'ROBUSTNESS' section, there are several settings: 'Inbound Media Latch Mode' (Dynamic), 'New RTP Stream Packets' (3), 'New RTCP Stream Packets' (3), 'New SRTP Stream Packets' (3), 'New SRTP Stream Packets' (3), 'Timeout To Relatch RTP (msec)' (200), 'Timeout To Relatch SRTP (msec)' (200), 'Timeout To Relatch Silence (msec)' (10000), and 'Timeout To Relatch RTCP (msec)' (10000).

3.3.5 Media Security (SRTP) configuration

Not Done by Wizard

To configure Media Security:

- Open the 'Media Security' page (**SETUP > SIGNALING & MEDIA > MEDIA > Media Security**)

The screenshot shows the Audiocodes configuration interface for Media Security. The left sidebar contains a 'TOPOLOGY VIEW' with categories like CORE ENTITIES, CODERS & PROFILES, SBC, SIP DEFINITIONS, MESSAGE MANIPULATION, MEDIA, and INTRUSION DETECTION. The 'MEDIA' category is expanded, showing 'Media Security' as the selected option. The main content area displays the 'Media Security' configuration page. The 'GENERAL' tab is active, showing settings for 'Media Security' (Enable), 'Media Security Behavior' (Mandatory), and 'Offered SRTP Cipher Suites' (AES-CM-128-HMAC-SHA1-80). The 'AUTHENTICATION & ENCRYPTION' tab is also visible, showing settings for RTP and RTCP packets.

Set 'Media security': 'Enable' for SRTP enabling

Set 'Media Security Behavior':

- 'Preferable' (default value): encrypted call is initiated. If the cipher suite negotiation fails, an unencrypted call is established
- 'Mandatory': only encrypted calls are allowed

Set the "Offered SRTP Cipher Suites: AES-CM-128-HMAC-SHA1-80"

3.3.6 Media Realms configuration

To configure Media Realms (partly done if wizard has been used):

- Open the 'Media Realms' page (**SETUP > SIGNALING & MEDIA > CORE ENTITIES > Media Realms**)

The screenshot shows the Audiocodes configuration interface. The left sidebar contains a 'TOPOLOGY VIEW' menu with options like 'CORE ENTITIES', 'SIP Interfaces (4)', 'Media Realms (4)', 'Proxy Sets (3)', 'IP Groups (8)', 'CODERS & PROFILES', 'SBC', 'SIP DEFINITIONS', 'MESSAGE MANIPULATION', 'MEDIA', and 'INTRUSION DETECTION'. The main area is titled 'Media Realms (4)' and contains a table with the following data:

INDEX	NAME	IPv4 INTERFACE NAME	UDP PORT RANGE START	NUMBER OF MEDIA SESSION LEGS	UDP PORT RANGE END	DEFAULT MEDIA REALM
1	OpenTouch	eth0	6000	30	6149	No
2	ONE	eth0	6200	30	6349	No
3	RemotaUsers	eth1	6000	30	6149	No
5	Kamailio	eth0	6400	30	6549	No

Below the table, the configuration for the first realm, #1[OpenTouch], is shown in detail. It includes a 'GENERAL' section with fields for Name, Topology Location, IPv4 Interface Name, UDP Port Range Start, Number of Media Session Legs, UDP Port Range End, TCP Port Range Start, TCP Port Range End, and Default Media Realm. A 'QUALITY OF EXPERIENCE' section includes fields for QoE Profile and Bandwidth Profile. The interface also includes a search bar, pagination controls, and a 'New' button.

- Create one per leg (use '+New' button):
 - Media Realm Name:** set a relevant name
 - IPv4 Interface Name:** set the same name as in **IP Interfaces Table**
 - Port Range Start:** set a different value for each use
 - Number of Media Session legs:** set the max quantity of the media legs

Notes:

The Port Range End value is set automatically by wizard depending on Port Range Start value and the number of Media Sessions. The port ranges must not overlap.

The media realms (and behaviour) are associated to the IP Groups objects.

3.3.7 SRD configuration

One **SRD** object is meant to be used as **one Tenant/one Company signaling domain**. Therefore, if installed from scratch using the wizard, an OTSBC will only have a single SRD instance: 'defaultSRD' (some SRD instances can be added later in case of multi-tenant deployment).

To configure SRD :

- Open the 'SRDs' page (**SETUP > SIGNALING & MEDIA > CORE ENTITIES > SRDs**) : SRD "defaultSRD":

The screenshot shows the Audiocodes OTSBC configuration interface. The left sidebar contains a navigation menu with the following items: TOPOLOGY VIEW, CORE ENTITIES (expanded), SRDs (1) (selected), SIP Interfaces (6), Media Realms (3), Proxy Sets (3), IP Groups (7), CODERS & PROFILES, SBC, SIP DEFINITIONS, MESSAGE MANIPULATION, MEDIA, and INTRUSION DETECTION. The main area displays the 'SRDs (1)' configuration page. It includes a table with the following columns: INDEX, NAME, SHARING POLICY, SBC OPERATION MODE, SBC ROUTING POLICY, MAX. NUMBER OF REGISTERED USERS, and USER SECURITY MODE. The table contains one entry: 1, defaultSRD (1), Shared, B2BUA, defaultSBCRoutingPolicy, -1, and Accept All. Below the table, the configuration details for '#1[defaultSRD]' are shown. The 'GENERAL' tab includes fields for Name (defaultSRD), Sharing Policy (Shared), SBC Operation Mode (B2BUA), SBC Routing Policy (defaultSBCRoutingPolicy), Used By Routing Server (Not Used), Dial Plan (—), and CAC Profile (—). The 'REGISTRATION' tab includes fields for Max. Number of Register... (-1), User Security Mode (Accept All), and Enable Un-Authenticated... (Enable).

Parameters:

Max Number of Registered Users: -1 No limitation

Enable un-authenticated Registrations: Enable - *leave as is, this parameter must be configured in SIP Interface objects*

3.3.8 SIP interfaces configuration

To configure SIP interfaces (done for servers and Remote workers if wizard has been used):

- Open the 'SIP Interfaces' page (**SETUP > SIGNALING & MEDIA > CORE ENTITIES > SIP Interfaces**) :
- Create a SIP Interface per destination type: OT on LAN, OXE on LAN, OTCV on WAN, OTCT on WAN, WebSocket on WAN (done by wizard), Encrypted phones on LAN if needed (not done by wizard):
 - Click **'+New'**, give a relevant **Name** (wizard starts by default with 'SipInterface1', it can be renamed as 'SipIf1_OT' for SIP interface for OT and so on), associate the default **SRD name** previously created, associate the relevant **Network Interface** previously created in IP Interface Table, the **Application Type**: 'SBC', the signaling **ports**: TCP port 5260 for OT on LAN, UDP port 5060 for OXE on LAN, TLS port 5261 for OTCT Remote workers, 8061 for WebSocket – done by wizard.

Enable un-authenticated Registrations setting:

- Set 'Disable' for all WAN SIP interfaces**(Disable = Registers are sent to the SIP Proxy Server, the user registration is added to the database only if authenticated by the proxy server)
- Other choices: **'Not Configured'** (default) **to use with OXE and OT SIP interfaces**, **'Enable'** = the SBC device adds any REGISTER requests to its database even if the requests are not authenticated by a SIP proxy (**forbidden for WAN domain**)

User Security Mode settings:

- 'Accept Registered Users'** = blocks any SIP requests from unregistered users – to apply to all WAN SIP interfaces
- Other choices: **'Not configured'** (default value), **'Accept all'** = calls from unregistered users are not blocked (forbidden for WAN domain), **'Accept Registered Users from Same Source'**

The screenshot displays the Audiocodes management interface for SIP Interfaces. On the left, a sidebar shows the navigation menu with options like TOPOLOGY VIEW, CORE ENTITIES, SIP Interfaces (4), Media Realms (4), Proxy Sets (3), IP Groups (6), CODERS & PROFILES, SBC, SIP DEFINITIONS, MESSAGE MANIPULATION, MEDIA, and INTRUSION DETECTION. The main area shows a table of SIP Interfaces with columns: INDEX, NAME, SRD, NETWORK INTERFACE, APPLICATION TYPE, UDP PORT, TCP PORT, TLS PORT, ENCAPSULATING PROTOCOL, and MEDIA REALM. Below the table, the configuration details for a selected interface (#1[sipinterface1]) are shown, including GENERAL, MEDIA, SECURITY, and CLASSIFICATION sections.

INDEX	NAME	SRD	NETWORK INTERFACE	APPLICATION TYPE	UDP PORT	TCP PORT	TLS PORT	ENCAPSULATING PROTOCOL	MEDIA REALM
1	sipinterface1	defaultSRD (#1)	eth0	SBC	5260	0	0	No encapsulation	--
2	sipinterface2	defaultSRD (#1)	eth0	SBC	5060	0	0	No encapsulation	--
4	sipinterface4	defaultSRD (#1)	eth1	SBC	0	0	8061	Websockets	--
5	sipinterface5	defaultSRD (#1)	eth1	SBC	0	0	5261	No encapsulation	--

#1[sipinterface1] defaultSRD

GENERAL		MEDIA	
Name	sipinterface1	Media Realm	--
Topology Location	Down	Direct Media	Disable
Network Interface	eth0		
Application Type	SBC		
UDP Port	5260		
TCP Port	0		
TLS Port	0		
SCTP Port	0		
SCTP Secondary Network Interface	--		
Additional UDP Ports	Always Open		
Additional UDP Ports Mode	Always Open		
Encapsulating Protocol	No encapsulation		
Enable TCP Keepalive	Disable		
Used By Routing Server	Not Used		
Pre-Parsing Manipulation Set	--		
CAC Profile	--		

SECURITY	
TLS Context Name	default
TLS Mutual Authentication	--
Message Policy	--
User Security Mode	Not Configured
Enable Un-Authenticated Regs...	Not configured
Max. Number of Registered Us...	-1

CLASSIFICATION	
Classification Failure Response T...	500
Pre-classification Manipulation S...	-1
Call Group Rules Set ID	-1

3.3.9 IP Profile configuration

To check after Wizard!

To configure IP Profile Settings:

- Open the 'IP Profiles' page (SETUP > SIGNALING & MEDIA > CODERS & PROFILES > IP Profiles).
- Set IP Profile for OpenTouch (index '1' here):

The screenshot shows the Audiocodes configuration interface. The left sidebar contains a navigation menu with 'IP Profiles (5)' selected. The main area displays the configuration for profile #1 (OpenTouch). The 'SBC MEDIA' section is expanded, showing various settings. The 'SBC Media Security Mode' is set to 'Not Secured' and the 'Alternative DTMF Method' is set to 'As Is'.

INDEX #	NAME
1	OpenTouch
2	ONE
4	OTC kuwRTC
5	OTCT
7	OTC iPhone
8	Kamailio

#1[OpenTouch]

GENERAL		SBC SIGNALING	
Name	* OpenTouch	PRACK Mode	Transparent
Created by Routing Server	No	P-Asserted Identity Header Mode	As Is
		Diversion Header Mode	As Is
		History Info Header Mode	As Is
		Session Expires Mode	Transparent
		SIP UPDATE Support	Supported
		Remote re-INVITE	Supported
		Remote Delayed Offer Support	Supported
		MSRP re-INVITE/UPDATE	Supported
		MSRP Offer Setup Role	ActPass
		MSRP Empty Message Format	Default
		Remote Representation Mode	According to Operation Mode
		Keep Incoming Via Headers	According to Operation Mode
		Keep Incoming Routing Headers	According to Operation Mode
		Keep User-Agent Header	According to Operation Mode
		Handle X-Device	No
		ISUP Body Handling	Transparent
		ISUP Variant	ITU62
		Max Call Duration (min)	0

SBC MEDIA	
Mediation Mode	RTP Mediation
Extension Coders Group	--
Allowed Audio Coders	-- View
Allowed Coders Mode	Restriction
Allowed Video Coders	-- View
Allowed Media Types	
Direct Media Tag	
RFC 2833 Mode	As Is
RFC 2833 DTMF Payload Type	0
Alternative DTMF Method	As Is
Send Multiple DTMF Methods	Disable

SBC Media Security Mode: 'Not Secured'

Alternative DTMF Method: 'As Is'

- Set IP Profile for OXE (index '2' here):

IP Profiles (6)

INDEX	NAME
1	OpenTouch
2	OXE
4	OTC WABRTC
5	OTCT
7	OTC Phone
8	Kamailio

#2[OXE]

GENERAL

Name: OXE
Created by Routing Server: No

MEDIA SECURITY

SBC Media Security Mode: **Not Secured**
Symmetric MVI: Disable
MVI Size: 0
SBC Enforce MVI Size: Don't enforce
SBC Media Security Method: SDP
Reset SRTP Upon Re-key: Disable
Generate SRTP Keys Mode: Only if Required
SBC Remove Crypto Lifetime in ...: No
SBC Remove Unknown Crypto: No

SBC SIGNALING

PRACK Mode: Transparent
P-Asserted-Identity Header Mo...: As Is
Division Header Mode: As Is
History-Info Header Mode: As Is
Session Expires Mode: Transparent
SIP UPDATE Support: Supported
Remote re-INVITE: Supported
Remote Delayed Offer Support: Supported
MSRP re-INVITE/UPDATE: Supported
MSRP Offer Setup Role: Accept
MSRP Empty Message Format: Default
Remote Representation Mode: According to Operation Mode
Keep Incoming Via Headers: According to Operation Mode
Keep Incoming Routing Headers: According to Operation Mode
Keep User-Agent header: According to Operation Mode
Handle 3-Digest: No
GUP Body Handling: Transparent
GUP Variant: Full
Max Call Duration [min]: 6

SBC FORWARD AND TRANSFER

Remote REFER Mode: Regular
Remote Replaces Mode: **Keep as is**
Play RBT To Transferee: No
Remote 3xx Mode: Transparent

SBC Media Security Mode: 'Not Secured'

Remote Replaces Mode: Keep as is (Not done by Wizard)

- Set IP Profile for OTCT on WAN domain (index '5' here):

IP Profiles (6)

INDEX	NAME
1	OpenTouch
2	OXE
3	OTCT
4	OTC WABRTC
5	OTCT
6	Kamailio

#5[OTCT]

GENERAL

Name: OTCT
Created by Routing Server: No

MEDIA SECURITY

SBC Media Security Mode: **Secured**
Symmetric MVI: Disable
MVI Size: 0
SBC Enforce MVI Size: Don't enforce
SBC Media Security Method: SDP
Reset SRTP Upon Re-key: Disable
Generate SRTP Keys Mode: Only if Required
SBC Remove Crypto Lifetime in ...: No
SBC Remove Unknown Crypto: No

SBC SIGNALING

PRACK Mode: Transparent
P-Asserted-Identity Header Mode: As Is
Division Header Mode: As Is
History-Info Header Mode: As Is
Session Expires Mode: Transparent
SIP UPDATE Support: Supported
Remote re-INVITE: Supported
Remote Delayed Offer Support: Supported
MSRP re-INVITE/UPDATE: Supported
MSRP Offer Setup Role: Accept
MSRP Empty Message Format: Default
Remote Representation Mode: According to Operation Mode
Keep Incoming Via Headers: According to Operation Mode
Keep Incoming Routing Headers: According to Operation Mode
Keep User-Agent header: According to Operation Mode
Handle 3-Digest: No
GUP Body Handling: Transparent
GUP Variant: Full
Max Call Duration [min]: 6

MEDIA	
Broken Connection Mode	Ignore
Media IP Version Preference	Only IPv4
RTP Redundancy Depth	Disable

SBC Media Security Mode: 'Secured'

Broken Connection Mode: 'Ignore' (Not done by Wizard)

- Set IP Profile for Websocket (OTC WebRTC) domain (index '4' here):

The screenshot shows the Audiocodes SBC configuration interface. On the left, the 'IP Profiles (8)' are listed. Profile 4, named 'OTC WebRTC', is selected. The configuration for this profile is shown on the right. Under the 'MEDIA SECURITY' section, the following settings are highlighted with red boxes:

- SBC Media Security Mode:** Secured
- SBC Media Security Method:** DTLS

Other visible settings include:

- GENERAL:** Name: OTC WebRTC, Created by Routing Server: No
- SBC SIGNALING:** P-Asserted-Identity Header Mode: As Is, Diversion Header Mode: As Is, History-Info Header Mode: As Is, Session Expires Mode: Transparent, SIP UPDATE Support: Supported, Remote re-INVITE: Supported, Remote Delayed Offer Support: Supported, MSRP re-INVITE/UPDATE: Supported, MSRP Offer Setup Role: AdPass, MSRP Empty Message Format: Default, Remote Representation Mode: According to Operation Mode, Keep Incoming Via Headers: According to Operation Mode, Keep Incoming Routing Headers: According to Operation Mode

SBC MEDIA	
Mediation Mode	RTP Mediation
Extension Coders Group	--
Allowed Audio Coders	-- View
Allowed Coders Mode	Restriction
Allowed Video Coders	-- View
Allowed Media Types	
Direct Media Tag	
RFC 2833 Mode	Disallow
RFC 2833 DTMF Payload Type	0
Alternative DTMF Method	As Is
Send Multiple DTMF Methods	Disable
Adapt RFC2833 BW to Voice code...	Disabled
SDP Prime Answer	Remote Answer
Preferred PTime	0
Use Silence Suppression	Transparent
RTP Redundancy Mode	As Is
RTCP Mode	Transparent
Jitter Compensation	Disable
ICE Mode	Lite
SDP Handle RTCP	Don't Care
RTCP Mux	Supported
RTCP Feedback	Feedback On
Voice Quality Enhancement	Disable
Max Opus Bandwidth	0
Generate No-Op Packets	Disable
Enhanced PLC	Disable
SBC Multiple Coders	Not Supported

SBC Media Security Mode: 'Secured'

Media Security Method: 'DTLS'

RFC 2833 Mode: 'Disallow'

Alternative DTMF Method: 'As Is'

ICE mode: 'Lite'

RTCP Mux: 'Supported'

RTCP Feedback: 'Feedback On'

• Set IP Profile for iPhone (index '7' here):

The screenshot shows the Audiocodes SIP Manager interface. On the left, the 'CORE ENTITIES' menu is expanded, and 'IP Profiles (8)' is selected. The main panel displays the configuration for IP Profile #7 (OTC iPhone). The 'SBC Media Security Mode' is set to 'Secured' (highlighted with a red box). Below this, the 'Broken Connection Mode' is set to 'Ignore' (also highlighted with a red box). Other settings include 'SBC Enforce MKI Size' set to 'Don't enforce' and 'SBC Media Security Method' set to 'SDS'.

SBC Media Security Mode: 'Secured'

Broken Connection Mode: 'Ignore' (Not done by Wizard)

• Set IP Profile for Kamailio (index '8' here):

The screenshot shows the Audiocodes SIP Manager interface. On the left, the 'CORE ENTITIES' menu is expanded, and 'IP Profiles (8)' is selected. The main panel displays the configuration for IP Profile #8 (Kamailio). The 'SBC Media Security Mode' is set to 'Not Secured' (highlighted with a red box). Other settings include 'SBC Enforce MKI Size' set to 'Don't enforce' and 'SBC Media Security Method' set to 'SDS'.

SBC Media Security Mode: 'Not Secured'

3.3.10 Proxy Sets configuration

To configure the Proxy Sets:

- Open the 'Proxy Sets' page (**SETUP > SIGNALING & MEDIA > CORE ENTITIES > Proxy Sets**)

Note: Proxy Set ID 0 must not be used; this is the device's default proxy

3.3.10.1 Proxy set for OT (index 1 here):

- Click '**+New**'

Name: give a name for OT proxy: 'OpenTouch'

SRD: 'defaultSRD'

SIP IPv4 Interface: choose the right SIP interface created for OT on LAN

Classification Input: 'IP Address only'

INDEX	NAME	SRD	SBC IPv4 SIP INTERFACE	PROXY KEEP-ALIVE TIME (SEC)	REDUNDANCY MODE	PROXY HOT SWAP
1	OpenTouch	defaultSRD (PT)	spinterface1	60	Hotting	Enable
2	ONE	defaultSRD (PT)	spinterface2	60	Hotting	Enable
4	Kamelo	defaultSRD (PT)	spinterface1	60	Hotting	Enable

#1[OpenTouch] defaultSRD

GENERAL

Name: OpenTouch

SBC IPv4 SIP Interface: spinterface1

TLS Context Name: -

KEEP-ALIVE

Proxy Keep-Alive: Disable

Proxy Keep-Alive Time (Sec): 60

Keep-Alive Failure Responses: -

Success Detection Retries: 1

Success Detection Interval: 10

Failure Detection Retransmissions: 1

REDUNDANCY

Redundancy Mode: Hotting

Proxy Hot Swap: Enable

Proxy Load Balancing Method: -

Min. Active Servers for Load Bal.: 1

ADVANCED

Classification Input: IP Address only

DNS Resolve Method: -

PROXY ADDRESS

172.17.12.10:5260

TYPE

UDP

Proxy Address (use the link on the bottom of the page): IP Address (or FQDN) of OT server: 5260 (it differs from default 5060 port):

INDEX	PROXY ADDRESS	TRANSPORT TYPE
0	172.17.12.10:5260	UDP

#0

GENERAL

Proxy Address: 172.17.12.10:5260

Transport Type: UDP

Proxy Priority: 0

Proxy Random Weights: 0

3.3.10.2 Proxy set for OXE (index 2 here):

- Click '+New'

Name: give a name for OXE proxy: OXE

SRD: 'defaultSRD'

SIP IPv4 Interface: choose the right SIP interface created for OXE on LAN

Classification Input: 'IP Address only'

Proxy Sets (3)

INDEX #	NAME	SRD	SBC IPv4 SIP INTERFACE	PROXY KEEP-ALIVE TIME (SEC)	REDUNDANCY MODE	PROXY HOT SWAP
1	OpenTelemetry	defaultSRD (#1)	sipinterface1	60	Hotstandby	Enable
2	OXE	defaultSRD (#1)	sipinterface2	60	Hotstandby	Enable
3	Kamailio	defaultSRD (#1)	sipinterface1	60	Hotstandby	Enable

#2[OXE] defaultSRD

GENERAL

Name: OXE

SBC IPv4 SIP Interface: sipinterface2

TLS Context Name: --

KEEP ALIVE

Proxy Keep-Alive: Disable

Proxy Keep-Alive Time (sec): 60

Keep-Alive Failure Responses: 1

Success Detection Retries: 10

Failure Detection Retransmissions: -1

REDUNDANCY

Redundancy Mode: Hotstandby

Proxy Hot Swap: Enable

Proxy Load Balancing Method: Disable

Min. Active Servers for Load Bal.: 1

ADVANCED

Classification Input: IP Address only

DAG Resolve Method: --

PROXY ADDRESS

TYPE
172.17.12.12:5060

Proxy Address 1 items

Proxy Address (use the link on the bottom of the page):

- if OXE standalone: IP Address or FQDN of OXE node: 5060, or
- if redundancy mode: OXE main role address (or FQDN): 5060

Proxy Sets (#2) > Proxy Address (1)

INDEX #	PROXY ADDRESS	TRANSPORT TYPE
0	172.17.12.12:5060	UDP

#0

GENERAL

Proxy Address: 172.17.12.12:5060

Transport Type: UDP

Proxy Priority: 0

Proxy Random Weights: 0

3.3.10.3 Proxy set for Kamailio (index 4 here):

- Click '**+New**'
- Name:** Kamailio
- SRD:** 'defaultSRD'
- SIP IPv4 Interface:** choose the right SIP interface created for OT on LAN
- Classification Input:** 'IP Address only'

The screenshot shows the Audiocodes configuration interface. On the left, the 'TOPOLOGY VIEW' sidebar is expanded, showing 'CORE ENTITIES' with 'Proxy Sets (9)' selected. The main area displays 'Proxy Sets (9)' with a table listing various proxy sets. The row for 'Kamailio' (index 4) is highlighted with a red box. Below the table, the configuration details for '#4[Kamailio]' are shown, including 'GENERAL', 'REDUNDANCY', 'KEEP ALIVE', and 'ADVANCED' sections. The 'CLASSIFICATION INPUT' is set to 'IP Address only'. At the bottom, a link for 'Proxy Address (1 item)' is visible.

INDEX	NAME	SRD	SBC (IPv4 SIP INTERFACE)	PROXY KEEP-ALIVE TIME (SEC)	REDUNDANCY MODE	PROXY HOT SWAP
1	OpenTouch	defaultSRD (RT)	sipinterface1	60	Hotting	Enable
2	CSE	defaultSRD (RT)	sipinterface2	60	Hotting	Enable
4	Kamailio	defaultSRD (RT)	sipinterface1	60	Hotting	Enable

#4[Kamailio] defaultSRD

GENERAL

Name: Kamailio

SBC IPv4 SIP Interface: sipinterface1

TLS Context Name: -

KEEP ALIVE

Proxy Keep-Alive: Disable

Proxy Keep-Alive Time (sec): 60

Keep-Alive Failure Responses: -

Success Detection Retries: 1

Success Detection Interval: 10

Failure Detection Retransmissions: -1

REDUNDANCY

Redundancy Mode: Hotting

Proxy Hot Swap: Enable

Proxy Load Balancing Method: -

Min. Active Servers for Load Bal.: 1

ADVANCED

Classification Input: IP Address only

DNS Resolve Method: -

PROXY ADDRESS

112.17.12.10.5160

TYPE

UDP

Proxy Address (use the link on the bottom of the page): IP Address (or FQDN) of OT server: 5160:

The screenshot shows the Audiocodes configuration interface. On the left, the 'TOPOLOGY VIEW' sidebar is expanded, showing 'CORE ENTITIES' with 'Proxy Sets (9)' selected. The main area displays 'Proxy Sets (9) > Proxy Address (1)' with a table listing proxy addresses. The row for '112.17.12.10.5160' (index 0) is highlighted. Below the table, the configuration details for '#0' are shown, including 'GENERAL' and 'ADVANCED' sections.

INDEX	PROXY ADDRESS	TRANSPORT TYPE
0	112.17.12.10.5160	UDP

#0

GENERAL

Proxy Address: 112.17.12.10.5160

Transport Type: UDP

Proxy Priority: 0

Proxy Random Weight: 0

3.3.11 SIP Messages Manipulations configuration

The Message Manipulations table can include up to 1500 Message Manipulation rules (index). A Message Manipulation rule defines a manipulation sequence for SIP messages. SIP message manipulation enables the normalization of SIP messaging fields between communicating network segments (WAN and LAN here)

Each manipulation rule can be assigned to any Manipulation Set ID which are groups (sets) of manipulation rules.

To configure Message Manipulations:

- Open the 'Message Manipulations' page (**SETUP > SIGNALING & MEDIA > MESSAGE MANIPULATION > Message Manipulations**).

Note: The wizard doesn't give any names to the manipulation rules. A good practice is to name them according to their role, 'manip_for_OT', 'manip_for_OXE', ...

For more advanced use of message manipulations, refer to [LTRT-42097 Mediat Software SBC User's Manual Ver. 7.4](#)

3.3.11.1 SIP manipulations rules needed for OT remote users

The manipulation Sets ID1, 7 and 8 are necessary for the OT remote users:

The screenshot displays the 'Message Manipulations' configuration page in the Audiocodes Mediat Software SBC. The table shows 36 rules. Rules 1 and 2 are highlighted in blue. Below the table, the configuration for rule #11 is shown, including General, Match, and Action sections.

INDEX	NAME	MANIPULATION SET ID	MESSAGE TYPE	CONDITION	ACTION SUBJECT	ACTION TYPE	ACTION VALUE	ROW ROLE
1		1			header.to.url.host	Modify	'ruspblvm10.load.qa:5260'	Use Current Condition
2		1			header.from.url.host	Modify	'ruspblvm10.load.qa'	Use Current Condition
3		2			header.to.url.host	Modify	'ruspblvm12.load.qa'	Use Current Condition
4		2			header.from.url.host	Modify	'ruspblvm12.load.qa'	Use Current Condition
11		4			header.to.url.host	Modify	'ruspblvm10.load.qa'	Use Current Condition
12		4			header.from.url.host	Modify	'ruspblvm10.load.qa'	Use Current Condition
13		4	refer request	header.Refer-To exists	header.Refer-To.url.host	Modify	'ruspblvm10.load.qa:8061'	Use Current Condition
14		4	refer request	header.Referred-By exists	header.Referred-By.url.host	Modify	'ruspblvm10.load.qa:8061'	Use Current Condition
15		5			header.to.url.host	Modify	'sbc.qa.qa.ale-international'	Use Current Condition
16		5			header.from.url.host	Modify	'sbc.qa.qa.ale-international'	Use Current Condition
17		5	refer request	header.Refer-To exists	header.Refer-To.url.host	Modify	'sbc.qa.qa.ale-international'	Use Current Condition
18		5	refer request	header.Referred-By exists	header.Referred-By.url.host	Modify	'sbc.qa.qa.ale-international'	Use Current Condition
19		7			header.to.url.host	Modify	'sbc.qa.qa.ale-international'	Use Current Condition
21		7			header.from.url.host	Modify	'sbc.qa.qa.ale-international'	Use Current Condition
32		7	refer request	header.Refer-To exists	header.Refer-To.url.host	Modify	'sbc.qa.qa.ale-international'	Use Current Condition
33		7	refer request	header.Referred-By exists	header.Referred-By.url.host	Modify	'sbc.qa.qa.ale-international'	Use Current Condition
34		7	refer request	header.Refer-To exists	header.Refer-To.url.transp	Modify	'1'	Use Current Condition
35		7	refer request	header.Referred-By exists	header.Referred-By.url.transp	Modify	'1'	Use Current Condition
36		8			header.to.url.host	Modify	'ruspblvm10.load.qa:5160'	Use Current Condition

Below the table, the configuration for rule #11 is shown:

GENERAL

Name: Manipulation Set ID: 4 Row Role: Use Current Condition

MATCH

Message Type: Condition

ACTION

Action Subject: header.to.url.host
Action Type: Modify
Action Value: 'ruspblvm10.load.qa'

- Index 1 and 2 (Manip Set ID 1) modify all 'From' and 'To' URL host headers of all SIP messages sent by OTSBC to OT from remote users.

INDEX	NAME	MANIPULATION SET ID	MESSAGE TYPE	CONDITION	ACTION SUBJECT	ACTION TYPE	ACTION VALUE	ROW ROLE
1		1			header.to.url.host	Modify	'ruspblvm10.load.qa:5260'	Use Current Condition
2		1			header.from.url.host	Modify	'ruspblvm10.load.qa'	Use Current Condition

- Index 30 to 33 (first part of Manipulation set ID 7) modify all 'From', 'To', 'Refer-To' and 'Referred-By' URL host headers sent by OTSBC from OT to iPhone remote users. 'Refer-To' and 'Referred-By' must be replaced by the public URI with SIP TLS port 5261. This rule is acting with the OTSBC Remote Refer Behavior in the IP Profile Settings (Transparent) of all SIP messages sent to remote users.

30		7			header.to.url.host	Modify	'sbc.qa.qa.ale-international'	Use Current Condition
31		7			header.from.url.host	Modify	'sbc.qa.qa.ale-international'	Use Current Condition
32		7	refer request	header.Refer-To exists	header.Refer-To.url.host	Modify	'sbc.qa.qa.ale-international'	Use Current Condition
33		7	refer request	header.Referred-By exists	header.Referred-By.url.host	Modify	'sbc.qa.qa.ale-international'	Use Current Condition

#30

Edit

GENERAL		ACTION	
Name		Action Subject	* header.to.url.host
Manipulation Set ID	* 7	Action Type	* Modify
Row Role	Use Current Condition	Action Value	* 'sbc-qa.ale-international.com'

MATCH	
Message Type	
Condition	

#31

Edit

GENERAL		ACTION	
Name		Action Subject	* header.from.url.host
Manipulation Set ID	* 7	Action Type	* Modify
Row Role	Use Current Condition	Action Value	* 'sbc-qa.ale-international.com'

MATCH	
Message Type	
Condition	

#32

Edit

GENERAL		ACTION	
Name		Action Subject	* header.Refer-To.url.host
Manipulation Set ID	* 7	Action Type	* Modify
Row Role	Use Current Condition	Action Value	* 'sbc-qa.ale-international.com:5261'

MATCH	
Message Type	* refer.request
Condition	* header.Refer-To exists

#33

Edit

GENERAL		ACTION	
Name		Action Subject	* header.Referred-By.url.host
Manipulation Set ID	* 7	Action Type	* Modify
Row Role	Use Current Condition	Action Value	* 'sbc-qa.ale-international.com:5261'

MATCH	
Message Type	* refer.request
Condition	* header.Referred-By exists

- Index 34 and 35 (last part of Manipulation set ID 7) forces transport to TLS.

34		7	refer.request	header.Refer-To exists	header.Refer-to.url.transpo	Modify	2'	Use Current Condition
35		7	refer.request	header.Referred-By exists	header.Referred-By.url.tran	Modify	2'	Use Current Condition

#34

Edit

GENERAL		ACTION	
Name		Action Subject	* header.Refer-to.url.transporttype
Manipulation Set ID	* 7	Action Type	* Modify
Row Role	Use Current Condition	Action Value	* '2'

MATCH	
Message Type	* refer.request
Condition	* header.Refer-To exists

#35

Edit

GENERAL		ACTION	
Name		Action Subject	* header.Referred-By.url.transporttype
Manipulation Set ID	* 7	Action Type	* Modify
Row Role	Use Current Condition	Action Value	* '2'

MATCH	
Message Type	* refer.request
Condition	* header.Referred-By.exists

- Index 36 and 37 (Manip Set ID 8) modify all 'From' and 'To' URL host headers of all SIP messages sent by OTSBC to OT from remote users with iPhones.

36	8			header.to.url.host	Modify	'russbvm10.load.qa:5160'	Use Current Condition
37	8			header.from.url.host	Modify	'russbvm10.load.qa'	Use Current Condition

3.3.11.2 Manipulations rules needed for OXE remote users

The manipulation Sets ID2 and 5 are necessary for OXE remote users (OTCT):

- Index 3 and 4 (Manipulation Set ID 2) modify all 'From' and 'To' headers of all SIP messages sent by OTSBC to OXE node from OTCT remote users.

3	2			header.to.url.host	Modify	'node012.load.qa'	Use Current Condition
4	2			header.from.url.host	Modify	'node012.load.qa'	Use Current Condition

- Index 15 to 18 (Manipulation set ID 5) modify all 'From', 'To', 'Refer-To' and 'Referred-By' URL host headers sent by OTSBC from OXE to OTCT remote users. 'Refer-To' and 'Referred-By' must be replaced by the public URI with SIP TLS port 5261.

15	5			header.to.url.host	Modify	'sbc-qa.qa.ale-international.c'	Use Current Condition
16	5			header.from.url.host	Modify	'sbc-qa.qa.ale-international.c'	Use Current Condition
17	5	refer.request	header.Refer-To.exists	header.Refer-To.url.host	Modify	'sbc-qa.qa.ale-international.c'	Use Current Condition
18	5	refer.request	header.Referred-By.exists	header.Referred-By.url.host	Modify	'sbc-qa.qa.ale-international.c'	Use Current Condition

#15

Edit

GENERAL		ACTION	
Name		Action Subject	* header.to.url.host
Manipulation Set ID	* 5	Action Type	* Modify
Row Role	Use Current Condition	Action Value	* 'sbc-qa.qa.ale-international.com'

MATCH	
Message Type	
Condition	

#16

Edit

GENERAL		ACTION	
Name		Action Subject	* header.from.url.host
Manipulation Set ID	* 5	Action Type	* Modify
Row Role	Use Current Condition	Action Value	* 'sbc-qa.qa.ale-international.com'

MATCH	
Message Type	
Condition	

#17

Edit

GENERAL		ACTION	
Name		Action Subject	* header.Refer-To.url.host
Manipulation Set ID	* 5	Action Type	* Modify
Row Role	Use Current Condition	Action Value	* 'sbc-qa.qa.ale-international.com:5261'

MATCH	
Message Type	* refer.request
Condition	* header.Refer-To.exists

#18

Edit

GENERAL		ACTION	
Name		Action Subject	* header.Referred-By.url.host
Manipulation Set ID	* 5	Action Type	* Modify
Row Role	Use Current Condition	Action Value	* 'sbcc-qc.qc.ale-international.com:5261'

MATCH	
Message Type	* refer.request
Condition	* header.Referred-By exists

3.3.11.3 Manipulation rules for OTC Web remote users

The manipulation set ID4 (Index 11 to 14) is automatically created by wizard if websockets have been selected in the configuration wizard.

11		4			header.to.url.host	Modify	'russpbvm10.load.qc'	Use Current Condition
12		4			header.from.url.host	Modify	'russpbvm10.load.qc'	Use Current Condition
13		4	refer.request	header.Refer-To exists	header.Refer-To.url.host	Modify	'russpbvm10.load.qc:8061'	Use Current Condition
14		4	refer.request	header.Referred-By exists	header.Referred-By.url.host	Modify	'russpbvm10.load.qc:8061'	Use Current Condition

#11

Edit

GENERAL		ACTION	
Name		Action Subject	* header.to.url.host
Manipulation Set ID	* 4	Action Type	* Modify
Row Role	Use Current Condition	Action Value	* 'russpbvm10.load.qc'

MATCH	
Message Type	
Condition	

#12

Edit

GENERAL		ACTION	
Name		Action Subject	* header.from.url.host
Manipulation Set ID	* 4	Action Type	* Modify
Row Role	Use Current Condition	Action Value	* 'russpbvm10.load.qc'

MATCH	
Message Type	
Condition	

#13

Edit

GENERAL		ACTION	
Name		Action Subject	* header.Refer-To.url.host
Manipulation Set ID	* 4	Action Type	* Modify
Row Role	Use Current Condition	Action Value	* 'russpbvm10.load.qc:8061'

MATCH	
Message Type	* refer.request
Condition	* header.Refer-To exists

#14

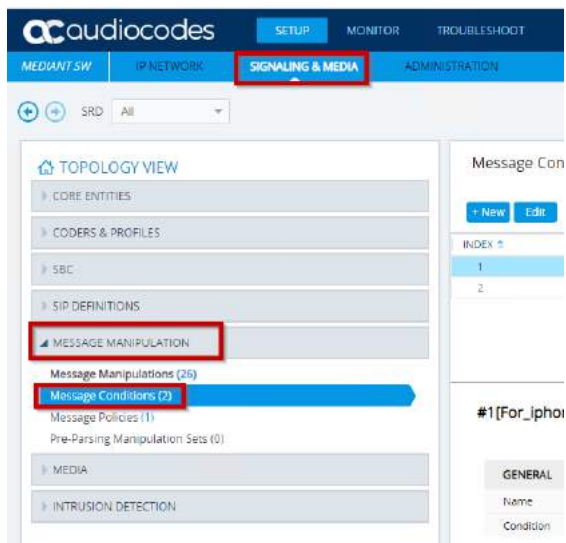
Edit

GENERAL		ACTION	
Name		Action Subject	* header.Referred-By.url.host
Manipulation Set ID	* 4	Action Type	* Modify
Row Role	Use Current Condition	Action Value	* 'russpbvm10.load.qc:8061'

MATCH	
Message Type	* refer.request
Condition	* header.Referred-By exists

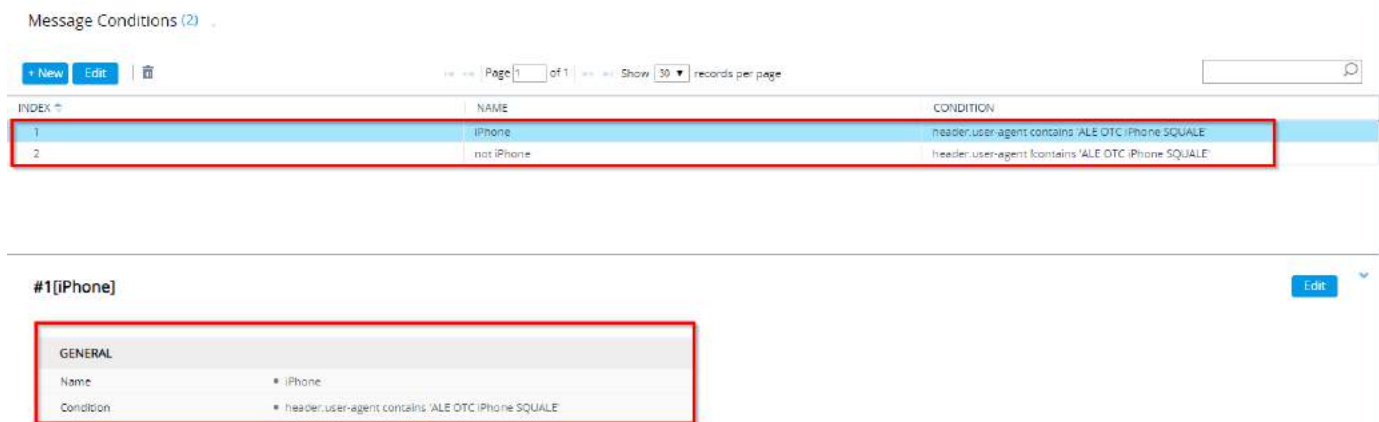
3.3.12 Message Conditions

To create new Message Conditions (**SIGNALING & MEDIA > MESSAGE MANIPULATION>Message Conditions**)



iPhone: Header.User-Agent contains 'ALE OTC iPhone SQUALE'

not iPhone: Header.User-Agent !contains 'ALE OTC iPhone SQUALE'



Message Conditions [iPhone]

GENERAL

Index

1

Name

•

iPhone

Condition

•

header.user-agent contains 'ALE OTC iPhone SQUALE'

Editor

Cancel

APPLY

Message Conditions [not iPhone]

GENERAL

Index

2

Name

•

not iPhone

Condition

•

header.user-agent !contains 'ALE OTC iPhone SQUALE'

Editor

Cancel

APPLY

3.3.13 IP Group configuration

The IP Group page allows you to create up to 32 logical IP entities called *IP Groups*.

IP Group ID 0 cannot be used: this IP Group is set to default values and is used by the device when IP Groups are not implemented.

Filling the SIP group name with a value will push that value in 'Request-URI' and 'To' header for all outgoing SIP message for servers declared in the IP Group.

To configure IP Group (already done for OT and OXE servers, OTCT and OTCV clients if wizard has been used):

- Open the 'IP Group' page (**SETUP > SIGNALING & MEDIA > CORE ENTITIES > IP Groups**):

3.3.13.1 IP Group for OT Server

The screenshot displays the 'IP Groups' configuration page in the Alcatel-Lucent management interface. The left sidebar shows the navigation menu with 'CORE ENTITIES' selected. The main area shows a table of IP Groups. The first group, 'OpenTouch' (Index 1), is selected, and its configuration details are shown on the right. The configuration details include:

- GENERAL:** Name: OpenTouch, Topology/Location: Down, Type: Server, Proxy Set: OpenTouch, IP Profile: OpenTouch, Media Realm: OpenTouch, Internal Media Realm: -, Contact User: -, SIP Group Name: ruspohm10.10.10.10, Created By Routing Server: No, Used By Routing Server: Not Used, Proxy Set Connectivity: N/A.
- SBC GENERAL:** Classify by Proxy Set: Enable, SBC Operation Mode: Not Configured.
- QUALITY OF EXPERIENCE:** QoS Profile: -, Bandwidth Profile: -.
- MESSAGE MANIPULATION:** Inbound Message Manipulation: -1, Outbound Message Manipulation: 1, Message Manipulation User Defined: -, Message Manipulation User Defined: -, Proxy Keep Alive Using IP Group: Disable.
- SBC REGISTRATION AND AUTHENTICATION:** Max. Number of Registered Users: -1, Registration Mode: User Initiates Registration, User Stickiness: Disable, User UDP Port Assignment: Disable, Authentication Mode: User Authenticates.

- Set the following parameters for **OT** (Index '1' here):
Type: 'Server'.
Proxy Set: <proxy name for OpenTouch>
SIP group name: <OT SIP Request-URI FQDN>
Media Realm, IP Profile ID: set the values configured for OT on LAN side
Classify by Proxy set: enable
Outbound Message Manipulation Set: <Manipulation Set number> defined in the Message Manipulations table for the headers contents of the SIP messages sent to OT server

3.3.13.2 IP Group for OXE server

The screenshot shows the Audiocodes Mediant SW interface. The left sidebar contains navigation options: TOPOLOGY VIEW, CORE ENTITIES, CODES & PROFILES, SBC, SIP DEFINITIONS, MESSAGE MANIPULATION, MEDIA, and INTRUSION DETECTION. The main area displays the IP Groups configuration. A table lists IP Groups with columns: INDEX, NAME, SRD, TYPE, SBC OPERATION MODE, PROXY SET, IP PROFILE, MEDIA REALM, SIP GROUP NAME, CLASSIFY BY PROXY SET, INBOUND MESSAGE MANIPULATION SET, and OUTBOUND MESSAGE MANIPULATION SET. The table shows 8 groups, with group #2 (OXE) highlighted. Below the table, the configuration for group #2 (OXE) is shown, including fields for Name, Topology/Location, Type, Proxy Set, IP Profile, Media Realm, Internal Media Realm, Contact User, SIP Group Name, Created By Routing Server, Used By Routing Server, and Proxy Set Connectivity. The configuration is set for a Server type, with Proxy Set OXE, IP Profile OXE, Media Realm OXE, and SIP Group Name nsp012.10.10.10. The Quality of Experience section shows QoS Profile and Bandwidth Profile. The Message Manipulation section shows Inbound Message Manipulation Set, Outbound Message Manipulation Set, Message Manipulation User Defined, and Proxy Keep-Alive using IP Group. The SBC Registration and Authentication section shows Max. Number of Registered UEs, Registration Mode, and User Stickiness.

- Set the following parameters for **OXE** (Index '2' here):
Type: 'Server'
Proxy Set: <proxy name for OXE>
SIP group name: <OXE node or role SIP Request-URI FQDN>
Media Realm, IP Profile ID: set the values configured for OXE on LAN side
Classify by proxy set: enable
Outbound Message Manipulation Set: <Manipulation Set number> defined in the Message Manipulations table for the headers contents of the SIP messages sent to OXE server

3.3.13.3 IP Group for OXE Remote Workers (OTCT clients on WAN)

The screenshot shows the Audiocodes Mediant SW interface. The left sidebar contains navigation options: TOPOLOGY VIEW, CORE ENTITIES, CODES & PROFILES, SBC, SIP DEFINITIONS, MESSAGE MANIPULATION, MEDIA, and INTRUSION DETECTION. The main area displays the IP Groups configuration. A table lists IP Groups with columns: INDEX, NAME, SRD, TYPE, SBC OPERATION MODE, PROXY SET, IP PROFILE, MEDIA REALM, SIP GROUP NAME, CLASSIFY BY PROXY SET, INBOUND MESSAGE MANIPULATION SET, and OUTBOUND MESSAGE MANIPULATION SET. The table shows 8 groups, with group #5 (OTCT) highlighted. Below the table, the configuration for group #5 (OTCT) is shown, including fields for Name, Topology/Location, Type, Proxy Set, IP Profile, Media Realm, Internal Media Realm, Contact User, SIP Group Name, Created By Routing Server, Used By Routing Server, and Proxy Set Connectivity. The configuration is set for a User type, with Proxy Set OTCT, IP Profile OTCT, Media Realm RemoteUsers, and SIP Group Name nsp012.10.10.10. The Quality of Experience section shows QoS Profile and Bandwidth Profile. The Message Manipulation section shows Inbound Message Manipulation Set, Outbound Message Manipulation Set, Message Manipulation User Defined, and Proxy Keep-Alive using IP Group. The SBC Registration and Authentication section shows Max. Number of Registered UEs, Registration Mode, and User Stickiness.

- Set the following parameters for OXE Remote workers (index '5' here):

Type: 'User'

Topology Location: Up

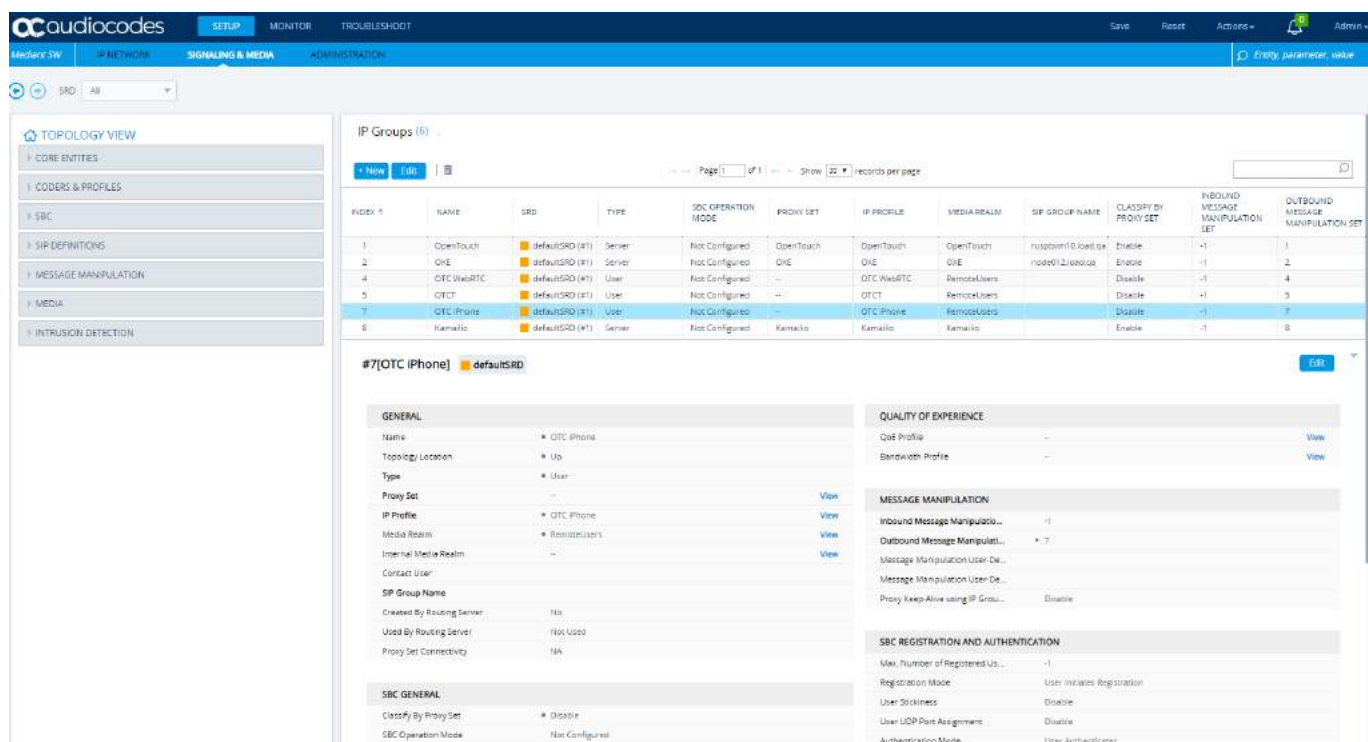
Media Realm: set the value configured for OXE Remote workers

IP Profile ID: set the value configured for the OXE Remote workers

Classify by proxy set: disable for any Remote workers

Outbound Message Manipulation Set: <Manipulation Set number> defined in the Message Manipulations table for the headers contents of the SIP messages sent to OTCT Remote workers

3.3.13.4 IP Group for iPhone users on WAN



The screenshot shows the Audiocodes SBC configuration interface. On the left is a navigation menu with options like TOPOLOGY VIEW, CORE ENTITIES, CODERS & PROFILES, SBC, SIP DEFINITIONS, MESSAGE MANIPULATION, MEDIA, and INTRUSION DETECTION. The main area displays a table of IP Groups. The table has columns for INDEX, NAME, SRD, TYPE, SBC OPERATION MODE, PROXY SET, IP PROFILE, MEDIA REALM, SIP GROUP NAME, CLASSIFY BY PROXY SET, INBOUND MESSAGE MANIPULATION SET, and OUTBOUND MESSAGE MANIPULATION SET. The table lists several groups, with index 7 highlighted. Below the table, the configuration details for #7[OTC iPhone] are shown, including GENERAL, QUALITY OF EXPERIENCE, MESSAGE MANIPULATION, and SBC REGISTRATION AND AUTHENTICATION sections.

INDEX	NAME	SRD	TYPE	SBC OPERATION MODE	PROXY SET	IP PROFILE	MEDIA REALM	SIP GROUP NAME	CLASSIFY BY PROXY SET	INBOUND MESSAGE MANIPULATION SET	OUTBOUND MESSAGE MANIPULATION SET
1	OpenTouch	defaultSRD (RT)	Server	Not Configured	OpenTouch	OpenTouch	OpenTouch	rustyvm10.100.100.100	Enable	-1	1
2	OXE	defaultSRD (RT)	Server	Not Configured	OXE	OXE	OXE	node012.100.100.100	Enable	-1	2
4	OTC WebRTC	defaultSRD (RT)	User	Not Configured	OTC WebRTC	OTC WebRTC	RemoteUsers		Disable	-1	4
5	OTCT	defaultSRD (RT)	User	Not Configured	OTCT	OTCT	RemoteUsers		Disable	-1	5
7	OTC iPhone	defaultSRD (RT)	User	Not Configured	OTC iPhone	OTC iPhone	RemoteUsers		Disable	-1	7
8	Kamailio	defaultSRD (RT)	Server	Not Configured	Kamailio	Kamailio	Kamailio		Enable	-1	8

#7[OTC iPhone] defaultSRD

GENERAL

Name: OTC iPhone
 Topology Location: Up
 Type: User
 Proxy Set: -
 IP Profile: OTC iPhone
 Media Realm: RemoteUsers
 Internal Media Realm: -
 Contact User: -
 SIP Group Name: -
 Created By Routing Server: No
 Used By Routing Server: No Used
 Proxy Set Connectivity: NA

QUALITY OF EXPERIENCE

QoS Profile: -
 Bandwidth Profile: -

MESSAGE MANIPULATION

Inbound Message Manipulation: -1
 Outbound Message Manipulation: 7
 Message Manipulation User De: -
 Message Manipulation User De: -
 Proxy Keep-Alive using IP Group: Enable

SBC REGISTRATION AND AUTHENTICATION

Max. Number of Registered Us: -1
 Registration Mode: User Initiates Registration
 User Stickiness: Disable
 User UDP Port Assignment: Disable
 Authentication Mode: User Authentication

- Set the following parameters for Remote workers with iPhones (index '7' here):

Type: 'User'

Topology Location: Up

Media Realm: set the value configured for OXE Remote workers

IP Profile ID: set the value configured for the Remote workers with iPhone

Classify by proxy set: disable for any Remote workers

Outbound Message Manipulation Set: <Manipulation Set number> defined in the Message Manipulations table for the headers contents of the SIP messages sent to Remote workers with iPhones

3.3.13.5 IP Group for OT server for iPhones

The screenshot shows the Audiocodes Mediant 319 configuration interface. The left sidebar contains a navigation menu with options like TOPOLOGY VIEW, CORE ENTITIES, CODERS & PROFILES, SBC, SIP DEFINITIONS, MESSAGE MANIPULATION, MEDIA, and INTRUSION DETECTION. The main area displays a table of IP Groups. The table has columns for INDEX, NAME, SRD, TYPE, SBC OPERATION MODE, PROXY SET, IP PROFILE, MEDIA REALM, SIP GROUP NAME, CLASSIFY BY PROXY SET, INBOUND MESSAGE MANIPULATION SET, and OUTBOUND MESSAGE MANIPULATION SET. The table lists 8 groups, with the 8th group, #8[Kamailio], highlighted. Below the table, the configuration details for the #8[Kamailio] group are shown, including GENERAL, SBC GENERAL, QUALITY OF EXPERIENCE, MESSAGE MANIPULATION, and SBC REGISTRATION AND AUTHENTICATION sections.

INDEX	NAME	SRD	TYPE	SBC OPERATION MODE	PROXY SET	IP PROFILE	MEDIA REALM	SIP GROUP NAME	CLASSIFY BY PROXY SET	INBOUND MESSAGE MANIPULATION SET	OUTBOUND MESSAGE MANIPULATION SET
1	OpenTouch	defaultSRD (RT)	Server	Not Configured	OpenTouch	OpenTouch	OpenTouch	vsipm110.100.0.0	Enable	-1	1
2	OXE	defaultSRD (RT)	Server	Not Configured	OXE	OXE	OXE	nodeOT.L100.0.0	Enable	-1	2
4	OTC WebRTC	defaultSRD (RT)	User	Not Configured	-	OTC WebRTC	RemoteUsers	-	Disable	-1	4
5	OTCT	defaultSRD (RT)	User	Not Configured	-	OTCT	RemoteUsers	-	Disable	-1	5
7	OTC iPhone	defaultSRD (RT)	User	Not Configured	-	OTC iPhone	RemoteUsers	-	Disable	-1	7
8	Kamailio	defaultSRD (RT)	Server	Not Configured	Kamailio	Kamailio	Kamailio	-	Enable	-1	8

#8[Kamailio] defaultSRD

GENERAL

Name: Kamailio
 Topology Location: Down
 Type: Server
 Proxy Set: Kamailio
 IP Profile: Kamailio
 Media Realm: Kamailio
 Internal Media Realm: -
 Contact User: -
 SIP Group Name: -
 Created By Routing Server: No
 Used By Routing Server: Not Used
 Proxy Set Connectivity: NA

SBC GENERAL

Classify By Proxy Set: Enable
 SBC Operation Mode: Not Configured
 SBC Claims Parking Mode: Sequential

QUALITY OF EXPERIENCE

QoS Profile: -
 Bandwidth Profile: -

MESSAGE MANIPULATION

Inbound Message Manipulation: -1
 Outbound Message Manipulation: 8
 Message Manipulation User-De: -
 Message Manipulation User-De: -
 Proxy Keep-Alive Using IP Group: Disable

SBC REGISTRATION AND AUTHENTICATION

Max. Number of Registered Us: -1
 Registration Mode: User Initiates Registration
 User SoSiness: Disable
 User UDP Port Assignment: Disable
 Authentication Mode: User Authentication
 Authentication Method List: -

- Set the following parameters for **Kamailio** (Index '1' here):

Type: 'Server'.

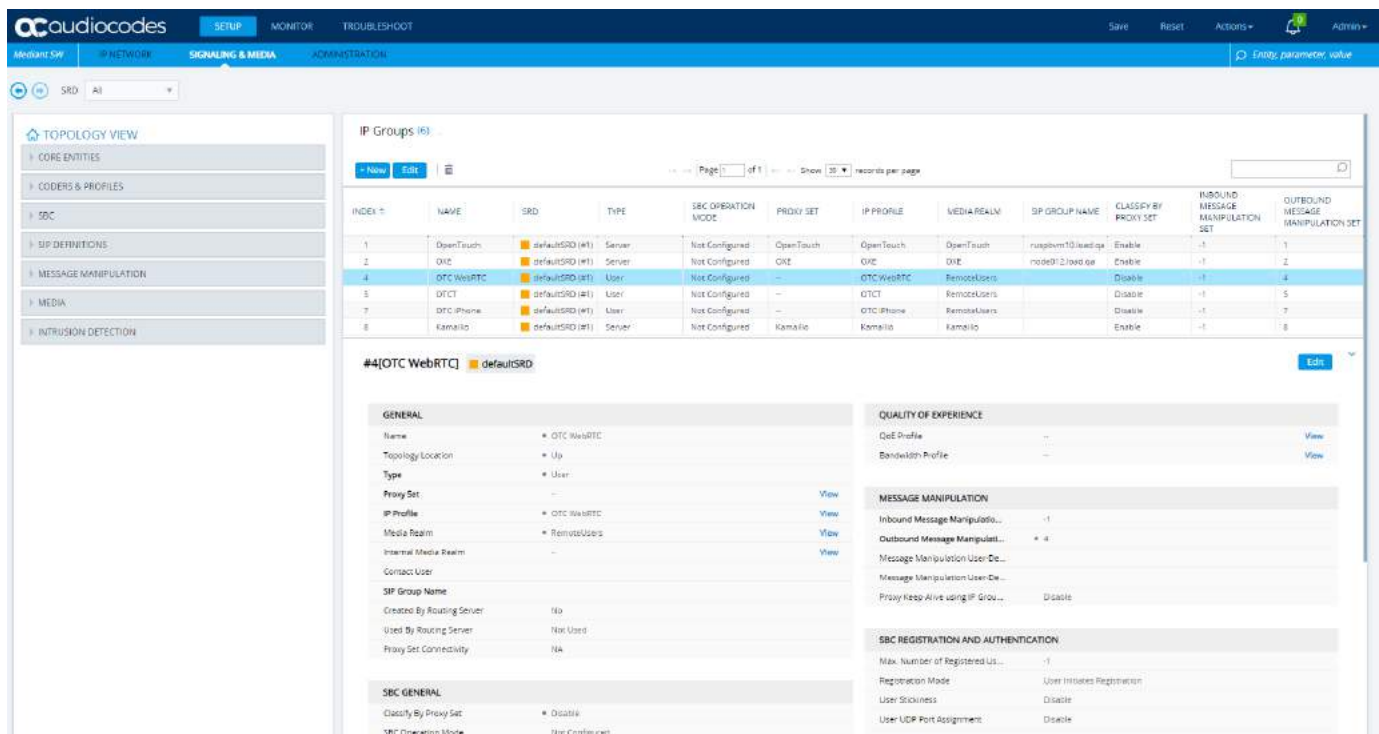
Proxy Set: <proxy name for Kamailio>

Media Realm, IP Profile ID: set the values configured for Kamailio on LAN side

Classify by Proxy set: enable

Outbound Message Manipulation Set: <Manipulation Set number> defined in the Message Manipulations table for the headers contents of the SIP messages sent to OT server from iPhone users.

3.3.13.6 IP Group for OTCWeb / webRTC users on WAN



The screenshot shows the Audiocodes configuration interface. On the left is a sidebar with navigation options: TOPOLOGY VIEW, CORE ENTITIES, CODERS & PROFILES, SBC, SIP DEFINITIONS, MESSAGE MANIPULATION, MEDIA, and INTRUSION DETECTION. The main area displays a table of IP Groups (index 4). Below the table, the configuration details for #4[OTC WebRTC] are shown, including General, Quality of Experience, Message Manipulation, and SBC Registration and Authentication sections.

INDEX	NAME	SRD	TYPE	SBC OPERATION MODE	PROXY SET	IP PROFILE	MEDIA REALM	SIP GROUP NAME	CLASSIFY BY PROXY SET	INBOUND MESSAGE MANIPULATION SET	OUTBOUND MESSAGE MANIPULATION SET
1	OpenTouch	defaultSRD (41)	Server	Not Configured	OpenTouch	OpenTouch	OpenTouch	rupdcm10.lead-qa	Enable	-1	1
2	OTC	defaultSRD (41)	Server	Not Configured	OTC	OTC	OTC	node012.lead-qa	Enable	-1	2
4	OTC WebRTC	defaultSRD (41)	User	Not Configured	---	OTC WebRTC	RemoteUsers	---	Disable	-1	4
5	OTCT	defaultSRD (41)	User	Not Configured	---	OTCT	RemoteUsers	---	Disable	-1	5
7	OTC iPhone	defaultSRD (41)	User	Not Configured	---	OTC iPhone	RemoteUsers	---	Disable	-1	7
8	Kamailio	defaultSRD (41)	Server	Not Configured	Kamailio	Kamailio	Kamailio	---	Enable	-1	8

#4[OTC WebRTC] defaultSRD

GENERAL

- Name: OTC WebRTC
- Topology Location: Up
- Type: User
- Proxy Set: ---
- IP Profile: OTC WebRTC
- Media Realm: RemoteUsers
- Internal Media Realm: ---
- Contact User: ---
- SIP Group Name: ---
- Created By Routing Server: No
- Used By Routing Server: Not Used
- Proxy Set Connectivity: No

QUALITY OF EXPERIENCE

- QoS Profile: ---
- Bandwidth Profile: ---

MESSAGE MANIPULATION

- Inbound Message Manipulation: -1
- Outbound Message Manipulation: -4
- Message Manipulation User-Def: ---
- Message Manipulation User-Def: ---
- Proxy Keep Alive using IP Group: Disable

SBC REGISTRATION AND AUTHENTICATION

- Max. Number of Registered Users: -1
- Registration Mode: User Initiates Registration
- User Stickiness: Disable
- User UDP Port Assignment: Disable

- Set the following parameters for OTCWeb / webRTC Guests / Remote workers (index '4' here):

Type: 'User'

Media Realm: set the value configured for OT Remote workers

IP Profile ID: set the value configured for OTC WebRTC users

Classify by proxy set: disable for any Remote workers

Outbound Message Manipulation Set: Wizard sets a usable value

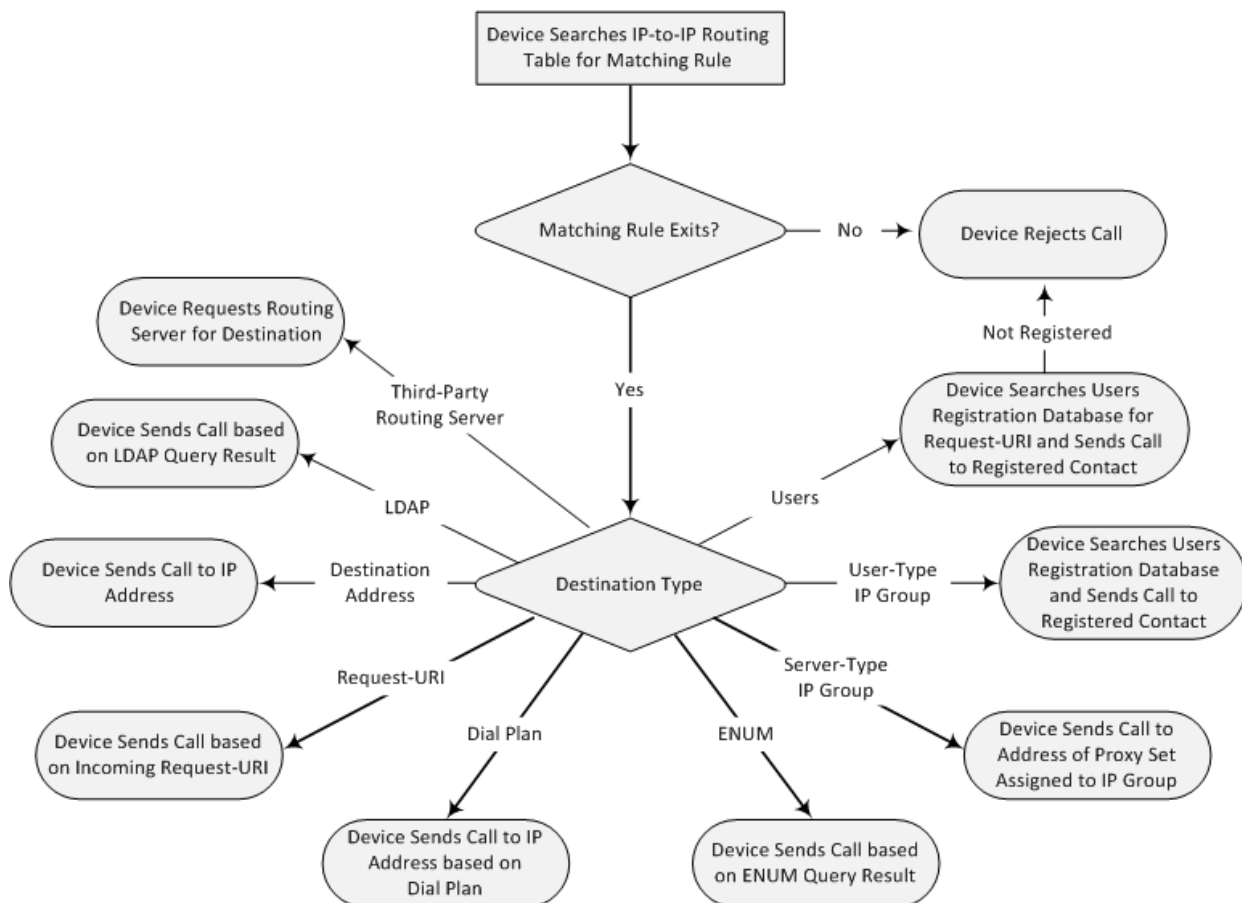
3.3.14 IP to IP Routing configuration

The IP-to-IP Routing table lets you configure up to 9,000 SBC IP-to-IP routing rules. An IP-to-IP routing rule routes the received SIP dialog messages (e.g., INVITE) to any of the following configurable IP destinations:

- According to registered user Contact listed in the device's registration database (only for User-type IP Groups)
- IP Group - the destination is the address configured for the Proxy Set associated with the IP Group
- IP address in dotted-decimal notation or FQDN. Routing to a host name can be resolved using NAPTR/SRV/A-Record
- Any registered user in the registration database. If the Request-URI of the incoming INVITE exists in the database, the call is sent to the corresponding contact address specified in the database
- According to result of an ENUM query
- (Hunt Group - used for call survivability of call centers)

(IP address according to a specified Dial Plan index listed in the loaded Dial Plan file)

(According to result of LDAP query)



The configuration of an IP-to-IP routing rule includes two areas:

Rule: Defines the matching characteristics of an incoming SIP message (e.g., IP Group that sent the message).

Action: Defines the operation that must be done if the incoming SIP message matches the characteristics of the rule (i.e., the device routes the message to the configured destination).

If the characteristics of an incoming call do not match the first rule in the table, the call characteristics are compared to those of the second rule, and so on until a matching rule is located. If no rule is matched, the call is rejected.

To configure and apply an IP-to-IP Routing rule, the rule must be associated with a Routing Policy. The Routing Policy associates the routing rule with an SRD(s). Therefore, the Routing Policy lets you configure routing rules for calls belonging to specific SRD(s).

However, multiple Routing Policies are relevant only for multi-tenant deployments (if needed). For most deployments, only a single Routing Policy is required (typ. Customer Premise Equipment deployment for one company) along with a single SRD ("defaultSRD"). As the device provides a default Routing Policy ("defaultSBCRoutingPolicy"), when only one Routing Policy is required, the device automatically assigns the default Routing Policy to the routing rule.

For more specific cases, please refer to AudioCodes doc LRT-41871.

To configure IP to IP Routing:

- Open the 'IP to IP Routing' page (**SETUP > SIGNALING & MEDIA > SBC > Routing > IP-to-IP**)

This IP-to-IP routing table has been configured by wizard:

The screenshot displays the Alcatel-Lucent SBC configuration interface. The left sidebar shows the navigation menu with 'IP NETWORK' selected. The main area shows the 'IP-to-IP Routing' table with 10 entries. The first entry, 'OpenTouch -> users', is selected, and its configuration details are shown on the right.

INDEX	NAME	ROUTING POLICY	ALTERNATIVE ROUTE OPTIONS	SOURCE IP GROUP	REQUEST TYPE	SOURCE USERNAME PATTERN	DESTINATION USERNAME PATTERN	DESTINATION TYPE	DESTINATION IP GROUP	DESTINATION SIP INTERFACE	DESTINATION ADDRESS
1	OpenTouch -> users	defaultSBCRoutingP	Route Row	OpenTouch	All	*	*	All Users
3	OIE -> users	defaultSBCRoutingP	Route Row	OIE	All	*	*	All Users
5	OTC WebRTC -> Ope	defaultSBCRoutingP	Route Row	OTC WebRTC	All	*	*	IP Group	OpenTouch
7	OTCT -> OIE	defaultSBCRoutingP	Route Row	OTCT	All	*	*	IP Group	OIE
9	OTC Phone -> Kame	defaultSBCRoutingP	Route Row	OTC Phone	All	*	*	IP Group	Kamailo
10	Kamailo -> users	defaultSBCRoutingP	Route Row	Kamailo	All	*	*	All Users

The configuration details for the selected rule '#1[OpenTouch -> users]' are shown below:

GENERAL	ACTION
Name: OpenTouch -> users	Destination Type: All Users
Alternative Route Options: Route Row	Destination IP Group: ... View
	Destination SIP Interface: ... View
	Destination Address: ...
	Destination Port: 0
	Destination Transport Type: ... View
	IP Group Set: ... View
	Call Setup Rules Set ID: 1
	Group Policy: Sequential
	Cost Group: ... View
	Routing Tag Name: default
	Internal Action: ...
	Modified Destination User Name: ...

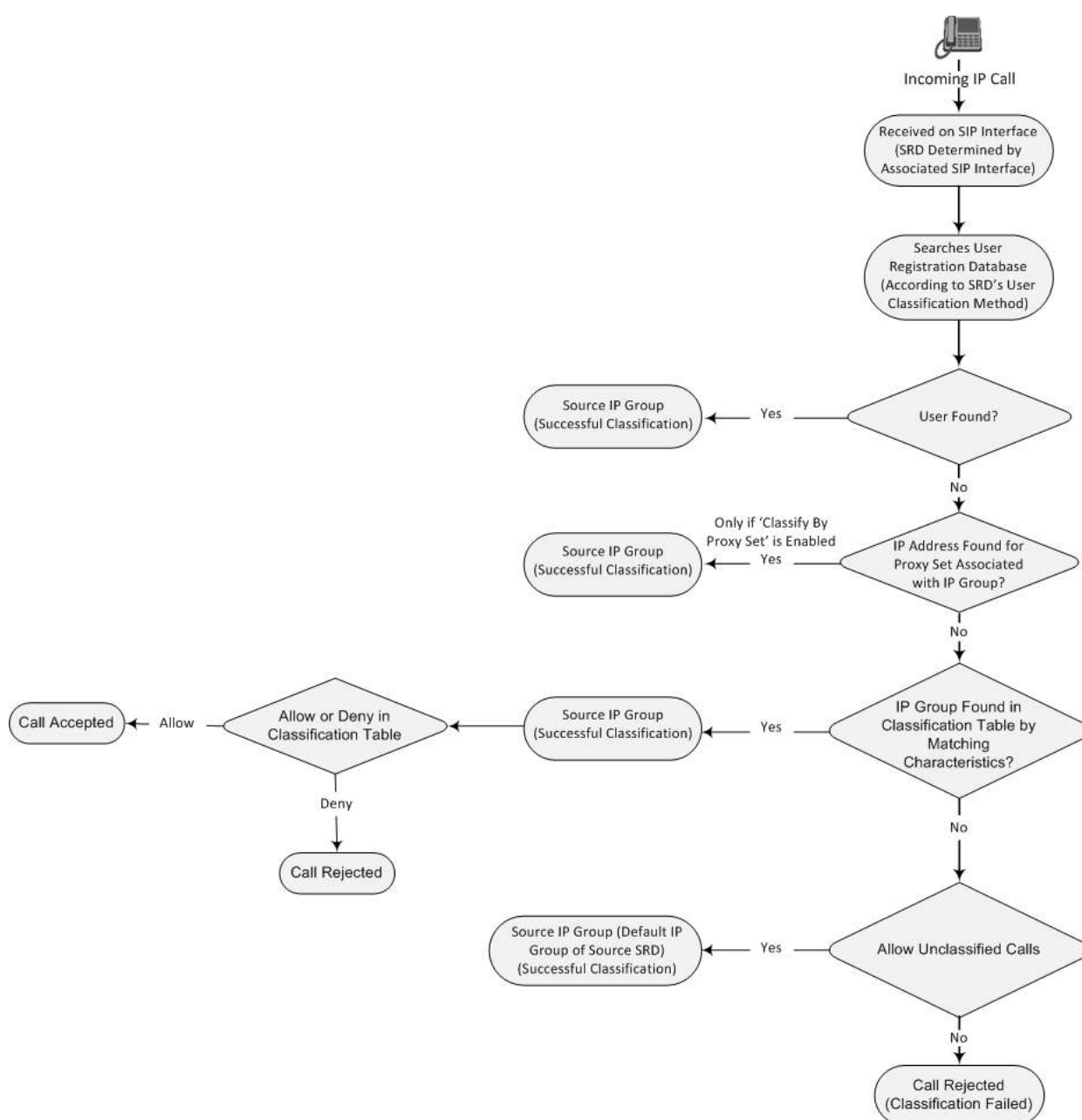
3.3.15 Configure Classification

Classification rules are used to classify incoming SIP dialog-initiating requests (e.g., INVITE messages) to source IP Groups from where the SIP dialog request originated. The Classification table lets you configure up to 1,500 Classification rules.

If the classification rule is defined as a white-list (Action Type set to 'Allow'), the SIP dialog is allowed and proceeds in the manipulation, routing and other processes. If the classification rule is defined as a blacklist (Action Type set to 'Deny'), the SIP dialog is denied.

The Classification table is used to classify the incoming SIP dialog request only if classification based on the device's registration database and Proxy Set fails. The classification process is as follows: Classification starts with the device's registration database, where it searches for a match by checking if the request arrived from a registered user in the database:

- Compares Contact header of the received SIP dialog to the Contact of the registered user
- Compares P-Asserted/From URL to the registered AOR



To configure Classification:

- Open the 'Classification' page (**SETUP > SIGNALING & MEDIA > SBC > Classification**)

Classification for OTCT Remote users (done by wizard):

The screenshot shows the Audiocodes SBC Configuration Wizard. The left sidebar displays the 'TOPOLOGY VIEW' with 'SBC' selected. The main area shows the 'Classification (3)' page. A table lists three classification rules:

INDEX	NAME	SRD	SOURCE SIP INTERFACE	SOURCE USERNAME PATTERN	SOURCE HOST	DESTINATION USERNAME PATTERN	DESTINATION HOST	ACTION TYPE	SOURCE IP GROUP
1	OTCT WebRTC	defaultSRD (P1)	sipinterface1	*	*	*	ruibum10.bsd.qa	Allow	OTCT WebRTC
2	OTCT	defaultSRD (P1)	sipinterface1	*	*	*	sdic.qa.ale-international	Allow	OTCT
3	OTCT iPhone	defaultSRD (P1)	sipinterface1	*	*	*	sdic.qa.ale-international	Allow	OTCT iPhone

The details for rule #2 [OTCT] are shown below:

MATCH

- Name: OTCT
- Source SIP Interface: sipinterface1
- Source IP Address: *
- Source Transport Type: Any
- Source Port: 0
- Source Username Pattern: *
- Source Host: *
- Destination Username Pattern: *
- Destination Host: sdic.qa.ale-international.com
- Message Condition: not iPhone

ACTION

- Action Type: Allow
- Destination Routing Policy: *
- IP Group Selection: Source IP Group
- Source IP Group: OTCT
- IP Group Tag Name: default
- IP Profile: *

Classification for iPhone users (done by wizard):

The screenshot shows the Audiocodes SBC Configuration Wizard. The left sidebar displays the 'TOPOLOGY VIEW' with 'SBC' selected. The main area shows the 'Classification (3)' page. A table lists three classification rules:

INDEX	NAME	SRD	SOURCE SIP INTERFACE	SOURCE USERNAME PATTERN	SOURCE HOST	DESTINATION USERNAME PATTERN	DESTINATION HOST	ACTION TYPE	SOURCE IP GROUP
1	OTCT WebRTC	defaultSRD (P1)	sipinterface1	*	*	*	ruibum10.bsd.qa	Allow	OTCT WebRTC
2	OTCT	defaultSRD (P1)	sipinterface1	*	*	*	sdic.qa.ale-international	Allow	OTCT
3	OTCT iPhone	defaultSRD (P1)	sipinterface1	*	*	*	sdic.qa.ale-international	Allow	OTCT iPhone

The details for rule #3 [OTCT iPhone] are shown below:

MATCH

- Name: OTCT iPhone
- Source SIP Interface: sipinterface1
- Source IP Address: *
- Source Transport Type: Any
- Source Port: 0
- Source Username Pattern: *
- Source Host: *
- Destination Username Pattern: *
- Destination Host: sdic.qa.ale-international.com
- Message Condition: iPhone

ACTION

- Action Type: Allow
- Destination Routing Policy: *
- IP Group Selection: Source IP Group
- Source IP Group: OTCT iPhone
- IP Group Tag Name: default
- IP Profile: *

Classification for OTCWeb WebRTC Guest Remote users (done by wizard):

The screenshot shows the Audiocodes Mediant SW interface. The left sidebar contains navigation options: TOPOLOGY VIEW, CORE ENTITIES, CODERS & PROFILES, SBC, Routing, SIP DEFINITIONS, MESSAGE MANIPULATION, MEDIA, and INTRUSION DETECTION. The main area displays the 'Classification (3)' configuration. A table lists three classifications:

INDEX	NAME	SBC	SOURCE SIP INTERFACE	SOURCE USERNAME PATTERN	SOURCE HOST	DESTINATION USERNAME PATTERN	DESTINATION HOST	ACTION TYPE	SOURCE IP GROUP
1	OTCWebRTC	defaultSRD (#1)	sipInterface4	*	*	*	ruspbvm10.load.qa	Allow	OTCWebRTC
2	OTCT	defaultSRD (#1)	sipInterface5	*	*	*	sbc-qa.qa.ale-international.com	Allow	OTCT
3	OTC iPhone	defaultSRD (#1)	sipInterface5	*	*	*	sbc-qa.qa.ale-international.com	Allow	OTC iPhone

The detailed view for the selected classification '#1[OTCWebRTC]' shows the following configuration:

MATCH

- Name: OTCWebRTC
- Source SIP Interface: sipInterface4
- Source IP Address: *
- Source Transport Type: Any
- Source Port: 0
- Source Username Pattern: *
- Source Host: *
- Destination Username Pattern: *
- Destination Host: ruspvm10.load.qa
- Message Condition: --

ACTION

- Action Type: Allow
- Destination Routing Policy: --
- IP Group Selection: Source IP Group
- Source IP Group: OTCWebRTC
- IP Group Tag Name: default
- IP Profile: --

- OTCT remote users SIP REGISTER classification examples:
 - A SIP REGISTER message of an OTCT Remote worker comes on 'sipInterface5' on IP interface 'eth1' (WAN) and addresses the FQDN sbc-qa.qa.ale-international.com-> the classification succeeds to Source IP Group 'OTCT' (index '2' here).
 - A SIP REGISTER message of an OTCT Remote worker with iPhone comes on 'sipInterface5' on IP interface 'eth1' (WAN) and addresses the FQDN sbc-qa.qa.ale-international.com-> the classification succeeds to Source IP Group 'OTC iPhone' (index '3' here).
 - A SIP REGISTER message of an OTCWeb Remote worker comes on 'sipInterface4' on IP interface 'eth1' (WAN) and addresses the FQDN ruspvm10.load.qa -> the classification succeeds to Source IP Group 'OTC webRTC' (index '1' here).

3.3.16 Configure certificate based Security

The Transport Layer Security (TLS), also known as Secure Socket Layer (SSL), is used to secure the device's SIP signaling connections, Web interface, and Telnet server and/or SSH if configured. The TLS/SSL protocol provides confidentiality, integrity, and authenticity between two communicating applications over TCP/IP.

SBC device uses "TLS Contexts" configuration objects to manage different TLS contexts, each with their own security characteristics.

TLS context '0' is available by default and is used by the webadmin in https mode (if activated). It includes a default self-signed poor security certificate and poor security conditions:

The screenshot shows the Audiocodes webadmin interface. On the left is a navigation menu with categories like NETWORK VIEW, CORE ENTITIES, SECURITY, QUALITY, DNS, WEB SERVICES, HTTP-PROXY, RADIUS & LDAP, MEDIA CLUSTER, and ADVANCED. The 'SECURITY' section is expanded, showing 'TLS Contexts (2)' and 'Firewall (3)'. The main area displays 'TLS Contexts (2)' with a table:

INDEX	NAME	TLS VERSION	DTLS VERSION	CIPHER SERVER
0	default	TLSv1.0	Any	AES-RC4
1	TLSContext_1	TLSv1.0, TLSv1.1 and TLSv1.2	Any	AES-RC4

Below the table, the configuration for context #0 (default) is shown. It includes a 'GENERAL' section with fields like Name (default), TLS Version (TLSv1.0), DTLS Version (Any), Cipher Server (AES-RC4), Cipher Client (ALL:!ADH), Strict Certificate Extension Valid... (Disable), DH key Size (1024), and TLS Renegotiation (Disable). There is also a 'OCSP' section with fields like OCSP Server (Disable), Primary OCSP Server, Secondary OCSP Server, OCSP Port (2560), and OCSP Default Response (Reject).

The default TLS context could be applied to all contexts: internal secured connections, as well as SIP/TLS for Remote Workers/Internet connections to the device.

But a much better practice is:

- to create one (or more) new strong TLS context with a new private key (2048 or more) with a SHA256 certificate and to apply it to all Remote users use cases, and,
- to harden the TLS context '0' for administration (webadmin https / ssh)

3.3.16.1 Adding a new strong TLS Context with a new private key and generating a new device certificate

General method:

1. Access to the device's webadmin
2. Add a new TLS Context, select the TLS version:
 - Use the most secure transport protocol according to your environment capabilities: 'TLS1.2' only. Use 'TLSv1.0 TLSv1.1 TLSv1.2' only if compatibility issues occur with some parts of the solution (it should not happen with OT2.3). Never authorize 'SSLv3'.
 - Default server cipher suite is 'AES:RC4'. It can be hardened: 'AES256:AES128:!aNULL:!MD5'
 - Default cipher client configured is 'ALL:!ADH'. It can be hardened: 'HIGH:MEDIUM'
3. Select the new TLS Context and generate a new Private Key with size =2048
4. Still within the new TLS Context, fill in the appropriate values in the Certificate Signing Request page (consult your security manager if necessary) and press Create CSR -> the CSR is generated and displayed on the page

5. Copy the CSR text from ----BEGIN CERTIFICATE REQUEST to END CERTIFICATE REQUEST----, paste it into a basic text editor (e.g. Notepad) and save it as a .txt file on your PC
6. Copy the text and send it to your security provider (CA) to sign this request.
7. When the CA sends you the server certificate, save it as text file (cert.txt). Ensure that the file is a plain-text file containing the "BEGIN CERTIFICATE" header, as shown in the example of a Base64-Encoded X.509 Certificate below:
 -----BEGIN CERTIFICATE-----
 MIIDKzCCAnugAwIBAgIEAgAAADANBgkqhkiG9w0BAQQFADA/MQswCQYDVQQGEwJG
 UjETMBEGA1UEChMKQ2VydGlwb3N0ZTEbMBkGA1UEAxMSQ2VydGlwb3N0ZSBTZXJ2
 ZXVyb3N0ZSBTZXJ2MDYyNDA4MDAwMFoXDTE4MDYyNDA4MDAwMFowPzELMAkGA1UE
 BhMCRlIxIzEzARBgNVBAoTCkNlcuRpcG9zdGUxGzAZBgNVBAMTEkNlcuRpcG9zdGUxGz
 VydmV1cjCCASEwDQYJKoZIhvcNAQEBBQADggEAOADCCAQkCggEAPqd4MziR4spWld
 GRx8bQrhZkonWnNm`+Yhb7+4Q67ecf1janH7GcN/SXsfx7jJpreWULf7v7Cvpr4R7qIJcmdH
 Intmf7JPM5n6cDBv17uSW63er7NkVnMFHwK1QaGFLMybFkzaeGrvFm4k3lRefiXDmuOe
 +FhJgHYezYHf44LvPRPwhSrzi9+Aq3o8pWDguJuZDIUP1F1jMa+LPwvREXfFcUW+w==
 -----END CERTIFICATE-----
8. Scroll down to the **Upload certificates files from your computer** group, click the **Browse** button corresponding to the 'Send Device Certificate...' field, navigate to the cert.pem file, and then click **Send File**.
9. After the certificate successfully loads to the device, save the configuration with a device reset.
10. Open the TLS Contexts page again, select the TLS Context index row, and then verify that under the **Certificate Information** group, the 'Private key' field displays "OK"; otherwise, consult your security administrator
11. If MTLS and/or chained certificates are going to be implemented, the Web interface can also be used to download the Authority-Signed Root Certificate and/or intermediate certificates to the AudioCodes device.

3.3.16.2 Assign the new strong TLS Context to the relevant SIP Interfaces

To check after Wizard!

To be effectively used by OTSBC, the newly created strong TLS Context must be assigned to the SIP interfaces that have to deal with TLS:

- SIP interfaces assigned to WAN domain (here index 5 for Remote Workers and index 4 for WebSocket)
- Open the 'Sip Interface' page (**SETUP > SIGNALING & MEDIA > CORE ENTITIES > SIP Interfaces**),
- Assign the new strong TLS context to the TLS Context Name of the relevant SIP interfaces

SIP Interfaces (4)

INDEX	NAME	SRD	NETWORK INTERFACE	APPLICATION TYPE	UDP PORT	TCP PORT	TLS PORT	ENCAPSULATING PROTOCOL	MEDIA REALM
1	sipinterface1	defaultSRD (R1)	eth0	SBC	5200	0	0	No encapsulation	--
2	sipinterface2	defaultSRD (R1)	eth0	SBC	5060	0	0	No encapsulation	--
4	sipinterface4	defaultSRD (R1)	eth1	SBC	0	0	8061	WebSocket	--
5	sipinterface5	defaultSRD (R1)	eth1	SBC	0	0	5261	No encapsulation	--

#5[sipinterface5] defaultSRD

GENERAL

- Name: sipinterface5
- Topology Location: Up
- Network Interface: eth1
- Application Type: SBC
- UDP Port: 0
- TCP Port: 0
- TLS Port: 5261
- SCTP Port: 0
- SCTP Secondary Network Interf...: --
- Additional UDP Ports: --

MEDIA

- Media Realm: --
- Direct Media: Disable

SECURITY

- TLS Context Name:** TLSContext_1
- TLS Mutual Authentication: --
- Message Policy: --
- User Security Mode: Accept Registered Users
- Enable Un-Authenticated Regis...: Disable
- Max. Number of Registered Us...: -1

3.3.16.3 Assign the new TLS Context to OTCWeb IP Group

To check after Wizard!

The new TLS Context must also be assigned to the IP Group for OTCWeb (if configured).

- Open the 'IP Groups' page (**SETUP > SIGNALING & MEDIA > CORE ENTITIES > IP Groups**)
- Select the OTCWeb IP Group, 'Media TLS Context' field: replace the default value 'default' by the new strong TLS Context value:

IP Groups (8)

INDEX	NAME	SRD	TYPE	SBC OPERATION MODE	PRIORITY SET	IP PROFILE	MEDIA REALM	SIP GROUP NAME	CLASSIFY BY PROXY SET	INBOUND MESSAGE MANIPULATION SET	OUTBOUND MESSAGE MANIPULATION SET
1	OpenTouch	defaultSRD (R1)	Server	Not Configured	OpenTouch	OpenTouch	OpenTouch	indatv10-load-qe	Enable	-1	1
2	OTC	defaultSRD (R1)	Server	Not Configured	OTC	OTC	OTC	indatv10-load-qe	Enable	-1	2
4	OTCWebRTC	defaultSRD (R1)	User	Not Configured	--	OTCWebRTC	RemotUsers	--	Disable	-1	4
5	OTCT	defaultSRD (R1)	User	Not Configured	--	OTCT	RemotUsers	--	Disable	-1	5
7	OTC iPhone	defaultSRD (R1)	User	Not Configured	--	OTC iPhone	RemotUsers	--	Disable	-1	7
8	Kamailio	defaultSRD (R1)	Server	Not Configured	Kamailio	Kamailio	Kamailio	--	Enable	-1	8

#4[OTCWebRTC] defaultSRD

GENERAL

- Name: OTCWebRTC
- Topology Location: Up

QUALITY OF EXPERIENCE

- QoS Profile: --
- Bandwidth Profile: --

SBC ADVANCED		
Source URI Input		
Destination URI Input		
SIP Connect	No	
SBC PSAP Mode	Disable	
Route Using Request URI Port	Disable	
Media TLS Context	• TLSContexts_1	View
Keep Original Call-ID	No	
Dial Plan	--	View
Call Setup Rules Set ID	-1	
Tags		
SBC Alternative Routing Reason...	--	View
Teams Media Optimization Han...	None	
Teams Media Optimization Initia...	DirectMedia	

3.3.17 NAT Translation configuration

If NAT is used on WAN side, the NAT translation table must be filled in with all the necessary ports used by the OTC Remote Worker applications.

To configure NAT:

- Open the 'NAT Translation' page (**SETUP > IP NETWORK > CORE ENTITIES > NAT Translation**)
- Configure an index for each types of destination: SIP-TLS port for OTCT, SRTP Media port range and Secured Web Socket port for OTCWeb WebRTC clients:

The screenshot shows the Audiocodes Management System (MS) interface. The left sidebar contains a 'NETWORK VIEW' section with a tree structure including 'CORE ENTITIES', 'IP Interfaces (3)', 'Ethernet Devices (2)', 'Ethernet Groups (15)', 'Physical Ports (2)', 'Static Routes (0)', 'HA Settings', 'HA Network Monitor (0)', 'NAT Translations (3)', 'SECURITY', 'QUALITY', 'DNS', 'WEB SERVICES', and 'HTTP PROXY'. The main content area is titled 'NAT Translation (3)' and shows a table of NAT translation rules. The table has columns: INDEX, SOURCE INTERFACE, TARGET IP ADDRESS, SOURCE START PORT, SOURCE END PORT, TARGET START PORT, and TARGET END PORT. The table contains three rules, with rule #1 highlighted. Below the table, a detailed view of rule #1 is shown, with 'SOURCE' and 'TARGET' sections. The 'SOURCE' section shows 'Source Interface' as 'eth1', 'Source Start Port' as '6000', and 'Source End Port' as '6000'. The 'TARGET' section shows 'Target IP Address' as '195.210.2.137', 'Target Start Port' as '6000', and 'Target End Port' as '6000'.

INDEX	SOURCE INTERFACE	TARGET IP ADDRESS	SOURCE START PORT	SOURCE END PORT	TARGET START PORT	TARGET END PORT
1	eth1	195.210.2.137	6000	6000		
3	eth1	195.210.2.137	6001	6001		
4	eth1	195.210.2.137	5281	5281		

#1

SOURCE		TARGET	
Source Interface	eth1	Target IP Address	195.210.2.137
Source Start Port	6000	Target Start Port	
Source End Port	6000	Target End Port	

3.3.18 NTP configuration

To configure NTP Server:

- Open the 'Time And Date' page (**SETUP > ADMINISTRATION > TIME AND DATE**)
- Set the Primary NTP server Address:

3.4 HTTP/S Proxy server configuration

3.4.1 Enable Reverse Proxy on OT-SBC

Enable HTTP Proxy application

Set the following parameters:

HTTP Proxy application: Enable.

Primary DNS Server IP Address: <First DNS server available for this interface>

Secondary DNS Server IP Address: <Second DNS server available for this interface>

- Save and Reset

3.4.2 Reverse Proxy configuration

Current Technical Communication explains how to configure the Reverse Proxy on OT-SBC using 4 templates delivered with this Technical Communication. All templates must be customized according to customer architecture before loading them in OT-SBC. These templates must be loaded in OT-SBC in the following way:

- template_interface_ed02.ini (optional)

Use this template if you want to create a new interface on OT-SBC for the Reverse Proxy. This means you add a new WAN interface on OT-SBC for the Reverse Proxy. If you don't use this template, it means the Reverse Proxy interface will be the same as SBC interface so the OT public FQDN and OT public IP address will be the same as SBC public FQDN and SBC public IP address (in this configuration no certificate for the reverse proxy is necessary as we reuse the same certificate already installed on SBC interface).

- template_rp_ed02.ini (mandatory)

Template to modify according to customer architecture.

- template_ldap_ed02.ini (optional)

Template to modify if ldap authentication need to be managed on Reverse Proxy. A dedicated machine is necessary to run the ldap-auth daemon (see chapter 4.5).

- template_ot_before2_4_ed02.ini (optional)

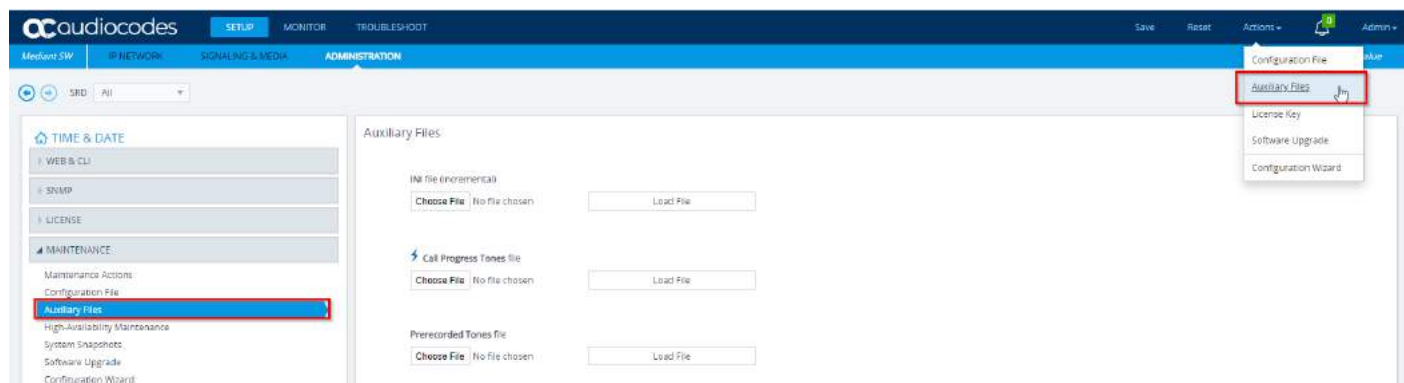
Template to modify if redirection to 8770 is require for remote workers connection users (for OT Release < R2.4 only).

- template_vna_ed01.ini (optional)

Template to modify according to customer architecture.

These templates must be loaded using the incremental method via the button "Load File"

- Open the 'Auxiliary files' page (**SETUP > ADMINISTRATION > MAINTENANCE > Auxiliary files**)



- Load template .ini file



3.4.3 Template_interface_ed02.ini

Open template_interface_ed02.ini file in any text editor and modify it with “find – replace” function.
Find and replace the following attributes:

Search for	Replace by
1.1.1.1	<Reverse Proxy IP address in DMZ>
24	Subnet Mask length in bits (e.g., 24 for 255.255.255.0)
2.2.2.2	<Default Gateway>
RP_Interface	Reverse Proxy interface name
3.3.3.3	<First DNS server available for this interface>
0.0.0.0	<Second DNS server available for this interface> or keep 0.0.0.0 if there is no second DNS server for this interface
WAN_DEV	<Name of Underlying Interface Ethernet device>

3.4.4 Template_rp_ed02.ini

Note from IP Interfaces table the name of interfaces. These names will be useful in current chapter to redirect https requests from Reverse Proxy inbound interface to Reverse Proxy outbound interface :

- WAN_IF if Reverse Proxy inbound interface = SBC inbound interface
- RP if Reverse proxy inbound interface is a new interface created at chapter 4.3.3
- LAN_IF used as SBC and Reverse Proxy outbound interface

As for SBC the inbound and outbound interface for Reverse Proxy could be the same.

INDEX	NAME	APPLICATION TYPE	INTERFACE MODE	IP ADDRESS	PREFIX LENGTH	DEFAULT GATEWAY	PRIMARY DNS	SECONDARY DNS	ETHERNET DEVICE
0	eth0	OSMO + Media + Control	IPv4 Manual	10.97.126.147	24	10.97.126.254	10.97.126.127		LAN_DEV
1	em1	Media + Control	IPv4 Manual	10.97.126.137	24	10.97.126.254	10.97.126.127		WAN_DEV
2	RP	Media + Control	IPv4 Manual	10.97.126.139	24	10.97.126.254	10.97.126.127	0.0.0.0	LAN_DEV

Open template_rp_ed02.ini file in any text editor and modify it with “find – replace” function.
Find and replace the following attributes:

Search for	Replace by
RP_Inbound_Interface	Reverse Proxy inbound interface name
RP_Outbound_Interface	Reverse Proxy outbound interface name
TLSContexts	TLS context name
ot.public_fqdn.company.com	OT public FQDN (ex: ot_publicname.company.com)
.public_domain.company.com	OT public domain (ex: .company.com)
conference_fqdn.company.com	conference server FQDN (ex: conference_name. company.com)
conference_name	conference server name (ex: conference_name)
.conference_domain.company.com	conference server domain (ex: .company.com)
ot.private-fqdn.company.com	OT private FQDN (ex: ot_privatename.int_company.com)
ot.private-name	OT private name (ex: ot_privatename)
ot.private-ip	OT internal IP address
.private-domain.company.com	OT private domain (ex: .int_company.com)

Since SBC 7.4 there is a new parameter in HTTP Proxy Servers - 'Bind to Device'. It is set to 'Enable' by default, but this parameter will interfere with nginx configuration, so it must be set to 'Disable'.

The screenshot shows the Alcatel-Lucent SBC configuration interface. The 'IP NETWORK' tab is selected. On the left, the 'NETWORK VIEW' sidebar shows 'HTTP Proxy Servers (3)' under 'WEB SERVICES'. The main area displays a table of HTTP Proxy Servers. The 'Bind to Device' column is highlighted with a red box, showing 'Disable' for all three entries. Below the table, the configuration for the first entry, #0(rp_443), is shown in the 'GENERAL' section.

INDEX	NAME	DOMAIN NAME	LISTENING INTERFACE	HTTP LISTENING PORT	HTTPS LISTENING PORT	TLS CONTEXT	BIND TO DEVICE	VERIFY CLIENT CERTIFICATE	ADDITIONAL DIRECTIVE SET
0	rp_443	ot-sbcqa.qa.ale-intern	RP		443	TLSContexts_1	Disable	No	rp_sbsredubr
1	rp_8016	ot-sbcqa.qa.ale-intern	RP		8016	TLSContexts_1	Disable	No	rp_sbsredubr
2	conf_443	conference-sbcqa.qa	RP		443	TLSContexts_1	Disable	No	conf_443_global

#0(rp_443)

GENERAL	
Name	rp_443
Domain Name	ot-sbcqa.qa.ale-international.com
Listening Interface	RP View
HTTP Listening Port	
HTTPS Listening Port	443
TLS Context	TLSContexts_1 View

3.4.5 Configuring VNA proxy

We expect you already have configuration of reverse proxy for OT.
Create HTTP directives set for VNA proxy:

The screenshot shows the 'HTTP Directive Sets (20)' configuration page. The left sidebar lists various configuration categories, with 'HTTP PROXY' expanded. The main table lists 20 directive sets. The set named 'vna_443' is highlighted in blue and selected. Below the table, the configuration details for '#29' are shown, including the 'GENERAL' tab with 'Set Name' as 'vna_443' and 'Description' as 'vna location /'. A red box highlights the 'HTTP Directives 4 items' link.

INDEX	SET NAME	DESCRIPTION
1	rp_443	rp directives port 443 location /
3	rp_443_share	rp directives port 443 location /share/
4	rp_8016	rp directives port 8016 location /
5	rp_servedURL	rp_servedURL
7	conf_443_global	conf 443 directives
8	at_re_451	pass to OT with no limit 451
9	conf_r451_buddies_attach	pass to OT with some limit for file sharing 451
10	at_re_453	Event page http chunk (c.action.openserver interface 453)
11	at_re_453	pass to OT with rate limit 453
12	at_re_rest_456	pass to OT for REST API 456
13	conf_443_order_storegwand	conf directives for location /order/ the OTWeb_gateway
14	conf_443_OTCSharing	conf directives for file OTCSharing/OTCSharing.msi
15	conf_443_share	conf directives for /share/ #Desktop sharing
16	conf_r451	return 451
17	conf_r455_451	455 return 455 or return 451
18	conf_r453	return 453
19	at_re_web_limit_conf_r453	at_re_web_limit_conf_r453 and 403
20	conf_r456	conf returns 456 api port
29	vna_443	vna location /

#29

GENERAL

Set Name: vna_443

Description: vna location /

HTTP Directives 4 items

The screenshot shows the 'HTTP Directive Sets (#29) > HTTP Directives (4)' configuration page. The left sidebar is the same as the previous screenshot. The main table lists 4 directives. The directive named 'proxy_buffering off;' is highlighted in blue and selected. Below the table, the configuration details for '#2' are shown, including the 'GENERAL' tab with 'Directive' as 'proxy_buffering off;'.

INDEX	DIRECTIVE
1	proxy_set_header Host \$host;
2	proxy_buffering off;
3	client_body_timeout 3600;
4	proxy_read_timeout 900;

#2

GENERAL

Directive: proxy_buffering off;

For this proxy add next directives:
 proxy_set_header Host \$host;
 proxy_buffering off;
 client_body_timeout 3600;
 proxy_read_timeout 900;

Create Upstream Group for VNA server and Upstream Host inside Upstream Group:

The screenshot shows the 'Upstream Groups (4)' configuration page. The left sidebar lists various configuration categories, with 'HTTP PROXY' expanded. The main table lists 4 upstream groups. The group named 'vna_http' is highlighted in blue and selected. Below the table, the configuration details for '#9[vna_http]' are shown, including the 'GENERAL' tab with 'Name' as 'vna_http', 'Protocol' as 'HTTP/HTTPS', 'Load Balancing Mode' as 'IP Hash', and 'Max Connections' as '0'.

INDEX	NAME	PROTOCOL	LOAD BALANCING MODE	MAX CONNECTIONS
0	ot_443	HTTP/HTTPS	IP Hash	0
1	ot_8016	HTTP/HTTPS	IP Hash	0
2	conf_internal_443	HTTP/HTTPS	IP Hash	0
9	vna_http	HTTP/HTTPS	IP Hash	0

#9[vna_http]

GENERAL

Name: vna_http

Protocol: HTTP/HTTPS

Load Balancing Mode: IP Hash

Max Connections: 0

Upstream Hosts 1 items

Upstream Groups (#9) > Upstream Hosts (1)

INDEX	HOST	PORT	WEIGHT	BACKUP
0	192.200.1.1	443	1	Disable

#0

GENERAL

Host: 192.200.1.1

Port: 443

Weight: 1

Backup: Disable

Upstream host option Host – internal VNA server domain name / IP.

Create HTTP proxy server and HTTP Location:

Domain Name – VNA server common FQDN, same for LAN and WAN.

Don't forget set Bind To Device to Disable.

In HTTP Location set Upstream Group and Additional Directive Set to previously created objects.

HTTP Proxy Servers (4)

INDEX	NAME	DOMAIN NAME	LISTENING INTERFACE	HTTP LISTENING PORT	HTTPS LISTENING PORT	TLS CONTEXT	BIND TO DEVICE	VERIFY CLIENT CERTIFICATE	ADDITIONAL DIRECTIVE SET
0	rp_443	ot-storops.eu.alcatel-lucent.com	RP		443	TLSContexts_1	Disable	No	rp_directiveURL
1	rp_8016	ot-storops.eu.alcatel-lucent.com	RP		8016	TLSContexts_1	Disable	No	rp_directiveURL
2	conf_443	ot-storops.eu.alcatel-lucent.com	RP		443	TLSContexts_1	Disable	No	conf_443_directive
3	vna_443	vna-storops.eu.alcatel-lucent.com	RP		443	TLSContexts_1	Disable	No	rp_directiveURL

#9[vna_443]

GENERAL

Name: vna_443

Domain Name: vna-storops.eu.alcatel-lucent.com

Listening Interface: RP

HTTP Listening Port: 443

HTTPS Listening Port: 443

TLS Context: TLSContexts_1

Bind To Device: Disable

Verify Client Certificate: No

Additional Directive Set: rp_directiveURL

HTTP Locations: 1 items >>

HTTP Proxy Servers (#9) > HTTP Locations (1)

INDEX	URL PATTERN	URL PATTERN TYPE	UPSTREAM SCHEME	UPSTREAM GROUP	UPSTREAM PATH	OUTBOUND INTERFACE	TLS CONTEXT	VERIFY CERTIFICATE	CACHE
0	/	Prefix	HTTPS	vna_705p	/	RP	TLSContexts_1	No	No

#0

GENERAL

URL Pattern: /

URL Pattern Type: Prefix

Upstream Scheme: HTTPS

Upstream Group: vna_705p

Upstream Path: /

Outbound Interface: RP

Additional Directive Set: vna_443

Cache: No

SSL

TLS Context: TLSContexts_1

Verify Certificate: No

3.4.6 Template_ldap_ed01.ini

Open template_ldap_ed02.ini file in any text editor and modify it with “find – replace” function.
Find and replace the following attributes:

Search for	Replace by
RP_Outbound_Interface	Reverse Proxy outbound interface name
TLSContexts	TLS context name
lpad_daemon_ip	IP address of the machine with lpad_daemon
lpad_pwd	ldap password to connect on ldap server
cn=admin,dc=mydomain	Login to connect on ldap server (BindDN)
ou=people,dc=mydomain	Ldap branch (BaseDN)

3.4.7 Template_ot_before2_4_ed01.ini

Open template_ot_before2_4_ed02.ini file in any text editor and modify it with “find – replace” function.

Find and replace the following attributes:

Search for	Replace by
RP_Outbound_Interface	Reverse Proxy outbound interface name
TLSContexts	TLS context name
8770-fqdn.company.com	Omnivista 8770 FQDN
8770-ip_address	Omnivista 8770 server IP address

3.4.8 Template_vna_ed01.ini

Open template_rp_ed02.ini file in any text editor and modify it with “find – replace” function.

Find and replace the following attributes:

Search for	Replace by
RP_Inbound_Interface	Reverse Proxy inbound interface name
RP_Outbound_Interface	Reverse Proxy outbound interface name
TLSContexts	TLS context name
vna-host.company.com	VNA public FQDN
10.10.10.253	VNA server FQDN/IP

3.5 LDAP Authentication

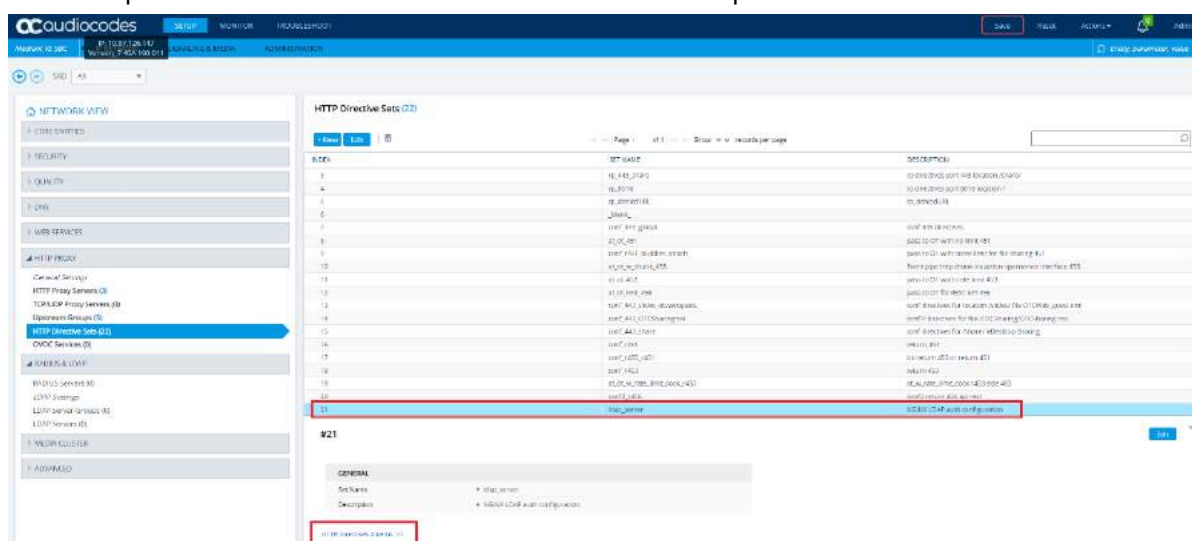
3.5.1 LDAP Authentication on internal OTCBC reverse proxy

AudioCodes has implemented a built-in Nginx LDAP authentication module. NGINX can perform authentication with an external LDAP server. This feature relies on the NGINX add-on module “nginx-auth-ldap-module”, which has been integrated into the NGINX offering on the SBC.

Customize the URL, DN password, and any other attributes of the query as needed. Details of the syntax supported for the LDAP server declarations can be found in <https://github.com/kvspb/nginx-auth-ldap/blob/master/README.md>

Create “HTTP Directive set” for LDAP authentication configuration

- Create new **Directive set** with name “**ldap_server**” (**Setup > IP network > HTTP Proxy > HTTP Directive Sets**)
- Open **HTTP Directives** in **Directive Set** from first step



- Create **HTTP Directives** for each line. For example, the configuration below is suitable for MS AD on Windows Server 2019

```
ldap_server ad_1 {
    url "ldap://[LDAP IP]:389/,DC=swc19,DC=tlab?sAMAccountName?sub?(objectClass=person)";
    binddn "\"CN=Administrator,CN=Users,DC=swc19,DC=tlab\"";
    binddn_passwd password;
    group_attribute member;
    group_attribute_is_dn on;
    satisfy any;
    require group "\"CN=Domain Admins,CN=Users,DC=swc19,DC=tlab\"";
    require group "\"CN=Domain Users,CN=Users,DC=swc19,DC=tlab\"";
    require valid_user;
}
```

url: User search base

binddn: Bind as member with required permissions

binddn_passwd: Password for **binddn** user

group_attribute: Group attribute name which contains member object

group_attribute_is_dn: search for full DN in member object

satisfy: matching algorithm (any / all)

require group: optional list of allowed groups

require: optional list of allowed users, **valid_user** is a superset and cannot be used together with 'user'. It is able to filter users with LDAP query: *require user !"<YOUR LDAP QUERY>"*;

- Open items in (Setup > IP network > HTTP Proxy > HTTP Directive Sets) «HTTP Context Directives» (Default index :0) and add new HTTP Directive «<@Include ldap_server@>» at the end of the list

- Open items in (**Setup > IP network > HTTP Proxy > HTTP Directive Sets**) «sbc_443» (Default index :1) and add two **HTTP directives** at the end of the list
 - **auth_ldap "Restricted Access";**
 - **auth_ldap_servers ad_1;**

INDEX	DIRECTIVE
0	#auth_request /auth-proxy;
1	proxy_set_header Host \$host;
2	proxy_buffering off;
3	proxy_read_timeout 900;
4	client_max_body_size 10m;
5	client_body_timeout 3600;
6	sub_filter_types *;
7	sub_filter_once off;
8	sub_filter "/acsfdr443/" "otpublic_name/443/";
9	sub_filter "/acsfdr443/" "otpublic_name/443/";
10	sub_filter "server-6acsfdr" "server-6otpublic_name";
11	sub_filter "6acsfdr443" "6otpublic_name/443/";
12	sub_filter "6acsfdr443" "6otpublic_name/443/";
13	trunked_transfer_encoding on;
14	auth_ldap "Restricted Access";
15	auth_ldap_servers ad_1;

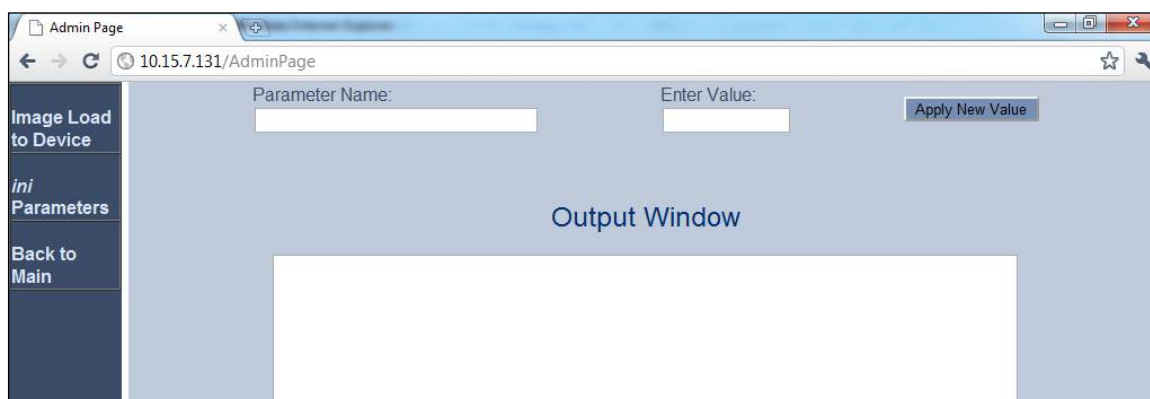
You can add a second LDAP server with the same syntax but with another **ldap_server** name and add **HTTP Directive «auth_ldap_servers»** in «sbc_443» Directive set.

3.6 OTSBC Admin Page

All parameters that can be set by Web admin have an equivalent parameter in the AdminPage. Some parameters, although, are not accessible by the Web admin and can only be managed using AdminPage.

To consult and/or configure some .ini parameters using the AdminPage:

1. Open the 'AdminPage' page ([HTTP://<SBC IP>/AdminPage](http://<SBC IP>/AdminPage))
2. Click on 'ini Parameters':

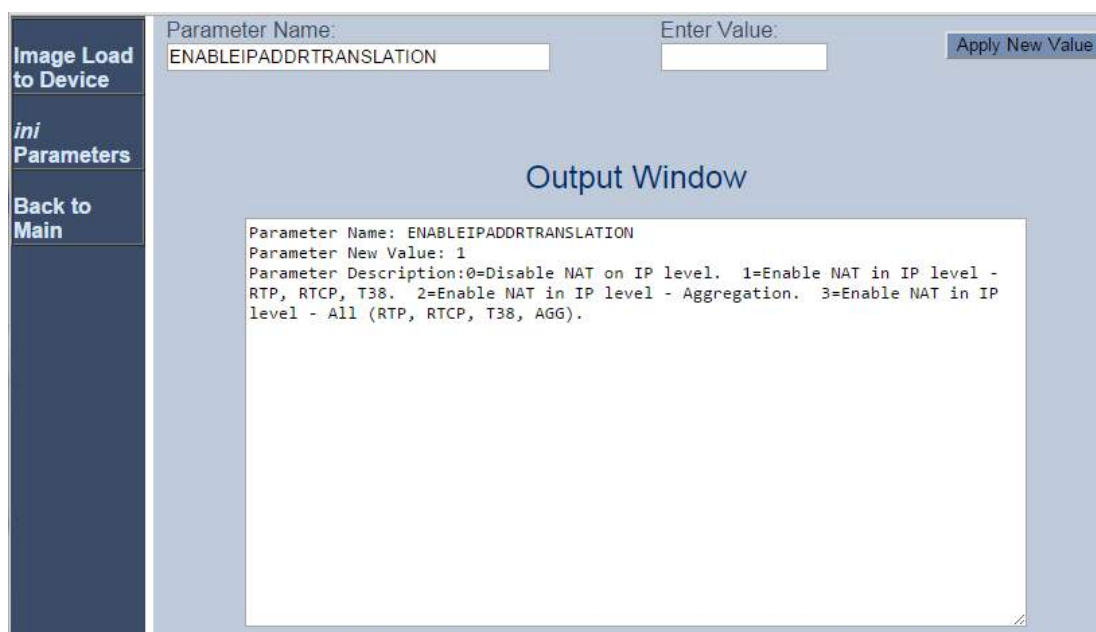


3. To check for a current parameter value, just enter its name in 'Parameter Name' field and click on 'Apply New Value' button while leaving the 'Enter value' field empty.
4. To modify a parameter value, fill in the 'Parameter Name' field and set its new value in 'Enter value' field, then click on 'Apply New Value' button. After a setting modification made using AdminPage, you need to click on 'Back to Main' button to go back to web interface and click on 'Burn' button to save the modification

3.6.1 Remote Workers devices

For a successful NAT traversal we need:

- **DisableNAT =0** (default value - means NAT is optional) or 2 (NAT is forced). (1 means NAT is disabled). This variable is also managed by webadmin in §4.3.5.
- **EnableIPAddrTranslation =1**
- **EnableUDPPortTranslation=1**



3.6.2 Others

- **NUMOFSUBSCRIBES** ='-1' by default, for automatic calculation according the running OTSBC license. If needed and for test purpose only, this parameter may be edited if the following warning message is showed: '[WARNING] Inbound SUBSCRIBE dialog rejected' due to exceeded allowed resource allocation.

3.7 OTSBC Monitoring

This section gives some basic information about VoIP status (User Registration, Proxy sets, SBC Call Detail Recording) and active alarms status. The most useful table is 'SBC Registered Users'.

3.7.1 SBC VoIP Status

3.7.1.1 SBC Registered Users

- Open the 'SBC Registered Users' page (**MONITOR > VoIP Status > SBC Registered Users**)

The screenshot shows the Audiocodes Monitor interface with the 'MONITOR' tab selected. The left sidebar contains a menu with 'SBC Registered Users' highlighted. The main content area displays a table titled 'SBC Registered Users' with two columns: 'ADDRESS OF RECORD' and 'CONTACT'.

ADDRESS OF RECORD	CONTACT
2093100@sbc-qa.ala-international.com	"reg20100_1 reg20100_1" <sip:2093100@192.168.1.33:5061>transport=TLS>expires=720 Associated Contact: FEU_CID1 IP: 7 515 NAT: 10.97.128.254:57528 ID: 17
2093601@sbc-qa.ala-international.com	"reg20601_1 reg20601_1" <sip:2093601@10.113.66.21:5061>transport=TLS>expires=720 Associated Contact: FEU_CID1 IP: 5 515 NAT: 10.97.128.254:58037 ID: 20
2092101@sbc-qa.ala-international.com	"reg20101_1 reg20101_1" <sip:2092101@192.168.1.181:5061>transport=TLS>expires=3600 Associated Contact: FEU_CID1 IP: 5 515 NAT: 10.97.128.254:58277 ID: 24

3.7.1.2 Proxy sets status

- Open the 'Proxy Sets Status' page (**MONITOR > VoIP Status > Proxy Sets Status**)

The screenshot shows the Audiocodes Monitor interface with the 'MONITOR' tab selected. The left sidebar contains a menu with 'Proxy Sets Status' highlighted. The main content area displays a table titled 'Proxy Sets Status' with a refresh rate of 60 seconds. The table has columns: 'PROXY SET ID', 'NAME', 'MODE', 'KEEP ALIVE', 'ADDRESS', 'PRIORITY', 'WEIGHT', 'SUCCESS COUNT', 'FAILURE COUNT', and 'STATUS'.

PROXY SET ID	NAME	MODE	KEEP ALIVE	ADDRESS	PRIORITY	WEIGHT	SUCCESS COUNT	FAILURE COUNT	STATUS
1	OpenTouch	Homing	Disabled	172.17.12.10:5260(*)	-	-	0	0	ONLINE
2	OKE	Homing	Disabled	172.17.12.12(*)	-	-	0	0	ONLINE
3	Kamallo	Homing	Disabled	172.17.12.10:5160(*)	-	-	0	0	ONLINE

3.7.1.3 Call Detail Record History

- Open the 'SBC CDR History' page (**MONITOR > VoIP Status > SBC CDR History**)

CALL END TIME	ENDPOINT TYPE	IP GROUP	CALLER	CALLER	DIRECTION	REMOTE IP	DURATION	TERMINATION REASON	SESSION ID
11:48:11.056 UTC Thu M	SBC	Kamaliq_server	2084100	FEU541-7-18-1	Incoming	172.17.12.10	0:00:03	NORMAL_CALL_CLEAR	83621F62-2021
11:48:11.056 UTC Thu M	SBC	Kamaliq_Phone	2084100	FEU541-7-18-1	Outgoing	10:87:126.254	0:00:03	NORMAL_CALL_CLEAR	83621F62-2021
11:48:05.144 UTC Thu M	SBC	Kamaliq_server	2084100	FEU541-7-18-1	Outgoing	10:87:126.254	0:00:03	NORMAL_CALL_CLEAR	83621F62-2019
11:48:05.144 UTC Thu M	SBC	Kamaliq_Phone	2084100	FEU541-7-18-1	Incoming	172.17.12.10	0:00:03	NORMAL_CALL_CLEAR	83621F62-2019
11:47:10.936 UTC Thu M	SBC	Kamaliq_server	2084100	FEU541-7-18-1	Incoming	172.17.12.10	0:00:03	NORMAL_CALL_CLEAR	83621F62-2018
11:47:10.936 UTC Thu M	SBC	Kamaliq_Phone	2084100	FEU541-7-18-1	Outgoing	10:87:126.254	0:00:03	NORMAL_CALL_CLEAR	83621F62-2018
11:47:03.610 UTC Thu M	SBC	Kamaliq_server	2084100	FEU541-7-18-1	Incoming	172.17.12.10	0:00:03	NORMAL_CALL_CLEAR	83621F62-2016
11:47:03.610 UTC Thu M	SBC	Kamaliq_Phone	2084100	FEU541-7-18-1	Outgoing	10:87:126.254	0:00:03	NORMAL_CALL_CLEAR	83621F62-2016
11:46:49.150 UTC Thu M	SBC	Kamaliq_server	2084100	FEU541-7-18-1	Incoming	172.17.12.10	0:00:14	NORMAL_CALL_CLEAR	83621F62-2006
11:46:49.150 UTC Thu M	SBC	Kamaliq_Phone	2084100	FEU541-7-18-1	Outgoing	10:87:126.254	0:00:14	NORMAL_CALL_CLEAR	83621F62-2006
11:46:46.080 UTC Thu M	SBC	OTCT	20100	FEU541-5-24-1	Outgoing	10:87:126.254	0:00:11	NORMAL_CALL_CLEAR	83621F62-2013
11:46:46.080 UTC Thu M	SBC	OYE	20100	FEU541-5-24-1	Incoming	172.17.12.12	0:00:11	NORMAL_CALL_CLEAR	83621F62-2013
11:46:34.947 UTC Thu M	SBC	OTCT	20050	FEU541-5-24-1	Outgoing	10:87:126.254	0:00:08	NORMAL_CALL_CLEAR	83621F62-2013
11:46:34.947 UTC Thu M	SBC	OYE	20050	FEU541-5-24-1	Incoming	172.17.12.12	0:00:08	NORMAL_CALL_CLEAR	83621F62-2013
11:46:21.281 UTC Thu M	SBC	OTCT	2082101	20100	Incoming	10:87:126.254	0:00:13	NORMAL_CALL_CLEAR	83621F62-2004
11:46:21.281 UTC Thu M	SBC	OYE	2082101	20100	Outgoing	172.17.12.12	0:00:13	NORMAL_CALL_CLEAR	83621F62-2004
11:46:00.286 UTC Thu M	SBC	OTCT	2082101	20100	Incoming	10:87:126.254	0:00:03	NO_ANSWER	83621F62-1996
11:46:00.286 UTC Thu M	SBC	OYE	2082101	20100	Outgoing	172.17.12.12	0:00:03	NO_ANSWER	83621F62-1996
11:20:00.425 UTC Thu M	SBC	OYE	20601	FEU541-5-20-1	Incoming	172.17.12.12	0:00:07	NORMAL_CALL_CLEAR	83621F62-1988
11:20:00.425 UTC Thu M	SBC	OTCT	20601	FEU541-5-20-1	Outgoing	10:87:126.254	0:00:07	NORMAL_CALL_CLEAR	83621F62-1988
11:20:53.740 UTC Thu M	SBC	Kamaliq_server	2084100	FEU541-7-18-1	Incoming	172.17.12.10	0:00:03	NORMAL_CALL_CLEAR	83621F62-1967
11:20:53.740 UTC Thu M	SBC	Kamaliq_Phone	2084100	FEU541-7-18-1	Outgoing	10:87:126.254	0:00:03	NORMAL_CALL_CLEAR	83621F62-1967
19:10:27.740 UTC Wed A	SBC	OTCT	20601	FEU541-5-20-1	Outgoing	10:87:126.254	0:00:01	NORMAL_CALL_CLEAR	83621F62-141
19:10:27.740 UTC Wed A	SBC	OYE	20601	FEU541-5-20-1	Incoming	172.17.12.12	0:00:01	NORMAL_CALL_CLEAR	83621F62-141
19:10:28.440 UTC Wed A	SBC	OTCT	20601	FEU541-5-20-1	Outgoing	10:87:126.254	0:00:06	NORMAL_CALL_CLEAR	83621F62-136
19:10:28.440 UTC Wed A	SBC	OYE	20601	FEU541-5-20-1	Incoming	172.17.12.12	0:00:06	NORMAL_CALL_CLEAR	83621F62-136
19:10:10.187 UTC Wed A	SBC	Kamaliq_server	2084100	FEU541-7-21-1	Incoming	172.17.12.10	0:02:13	NORMAL_CALL_CLEAR	83621F62-82
19:10:10.187 UTC Wed A	SBC	Kamaliq_Phone	2084100	FEU541-7-21-1	Outgoing	10:87:126.254	0:02:13	NORMAL_CALL_CLEAR	83621F62-82
19:10:13.124 UTC Wed A	SBC	OTCT	20601	FEU541-5-20-1	Outgoing	10:87:126.254	0:02:14	NORMAL_CALL_CLEAR	83621F62-90
19:10:13.124 UTC Wed A	SBC	OYE	20601	FEU541-5-20-1	Incoming	172.17.12.12	0:02:14	NORMAL_CALL_CLEAR	83621F62-90

3.7.2 SBC Active Alarms

- Open the " page (**MONITOR > SUMMARY > Active Alarms**)

SEQUENTIAL #	SEVERITY	SOURCE	DESCRIPTION	TIME
<div>Page 1 of 2</div> <div>This page refreshes every 60 seconds</div>				

3.8 OTSBC Administration

This section gives some information about OTSBC device administration accounts and security settings.

3.8.1 User Accounts

- Open the 'WEB User Accounts' page (**SETUP > ADMINISTRATION > WEB & CLI > Local Users**)

The screenshot displays the 'Local Users' configuration page in the OTSBC web interface. The page has a sidebar with navigation options like 'TIME & DATE', 'WEB & CLI', 'SNMP', 'LICENSE', and 'MAINTENANCE'. The main content area shows a table of local users. The table has the following data:

INDEX	USERNAME	PASSWORD	STATUS	PASSWORD AGE	WEB SESSION LIMIT	CLI SESSION LIMIT	WEB SESSION TIMEOUT	BLOCK DURATION	USER LEVEL
0	Admin	*	Valid	0	2	-1	15	60	Security Administrator
1	User	*	Valid	0	2	-1	15	60	Monitor

Below the table, there are two tabs: 'GENERAL' and 'SECURITY'. The 'GENERAL' tab shows the following fields:

Field	Value
Username	* Admin
Password	*
User Level	* Security Administrator
SSH Public Key	
Status	* Valid

The 'SECURITY' tab shows the following fields:

Field	Value
Password Age	* 0
Web Session Limit	* 2
CLI Session Limit	-1
Web Session Timeout	15
Block Duration	60

Each Web user account is composed of three attributes:

- User name and password:** enables access (login) to the Web interface :
 - Primary Account:** User Name: **Admin** Password: **Admin**(default values)
 - Secondary Account:** User Name: **User** Password: **User**
- User level:** determines the extent of the access (i.e., availability of pages and read / write privileges). The available access levels and their corresponding privileges are :

Master

Security Administrator: Read / write privileges for all pages => **Admin account**
Administrator: 100 (?) read / write privileges for all pages except security-related pages, which are read-only

Monitor: No access to security-related and file-loading pages; read-only access to the other pages. This read-only access level is typically applied to the secondary Web user account => **User account**

3.8.2 Web Security Settings

To configure the WEB Security Settings:

- Open the 'WEB Settings' page (**SETUP > ADMINISTRATION > WEB & CLI > WEB Settings**)

Web Connection can be 'HTTPS only' or 'HTTP and HTTPS'

➔ For security matters, better use 'HTTPS only'.

- But check before that you have already configured the default TLS_Context with a server certificate well known by the browsers used for administration.
- A device reset is necessary after changing Secured Web Connection setting

HTTPS cipher suite by default is 'RC4:AES128'.

3.8.3 Telnet and SSH Settings

To configure the Telnet and SSH Settings:

- Open the 'WEB User Accounts' page (**SETUP > ADMINISTRATION > WEB & CLI > CLI Settings**)

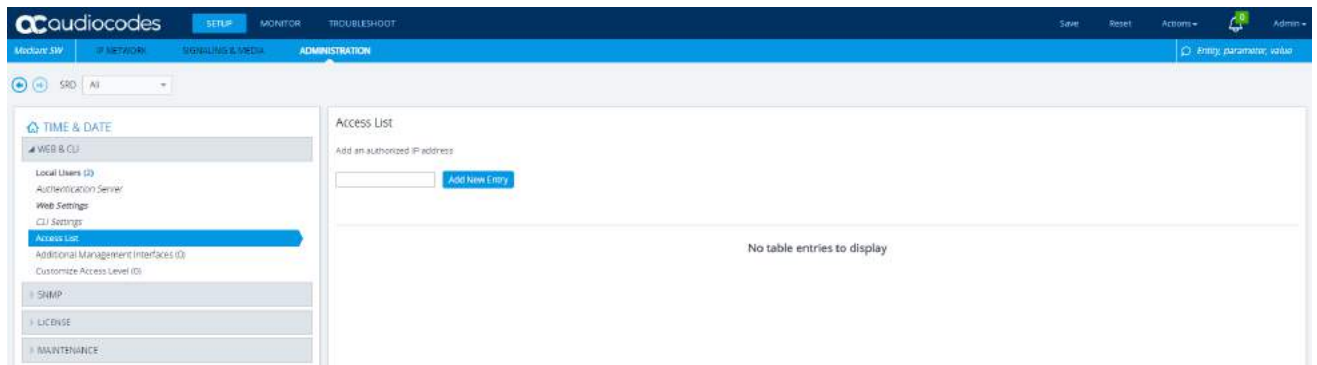
By default only unsecured telnet is activated.

➔ for security matters, better disable telnet and enable SSH. A device reset is necessary then.

3.8.4 Configure Web and Telnet Access List

To configure the WEB and Telnet Access List:

- Open the 'Access List' page (**SETUP > ADMINISTRATION > WEB & CLI > Access List**)



The Web & Telnet Access List page is used to define IP addresses (up to ten) that are permitted to access the device's Web, Telnet, and SSH interfaces.



If active, access from an undefined IP address is denied. If no IP address is defined, this security feature is inactive and the device can be accessed by any IP addresses.

4. Some security recommendations

4.1 Administration

- SSH/HTTPS only have to be activated for maintenance (unsecured telnet and http have to be prohibited)
- IP access list for maintenance has to be activated when SBC is deployed 'As a Service' or in the customer premises.

4.2 OTSBC operation

- Reject "Unclassified Calls" by SBC configuration (**SETUP > SIGNALING & MEDIA > SBC > Manipulation > SBC General Settings**)
- Secure routing rules
- Define call admission control rules
- Increase topology hiding with Messages Manipulation Set (for example remove User Agent header for messages going on unsecured network)
- If possible use non standard ports for application
- Activate the IDS

Document **Ref Audc:** [LTRT-30212 Recommended Security Guidelines Ver 7.4](#)

5. AudioCodes troubleshooting tools for OTSBC

5.1 ACSyslog tool

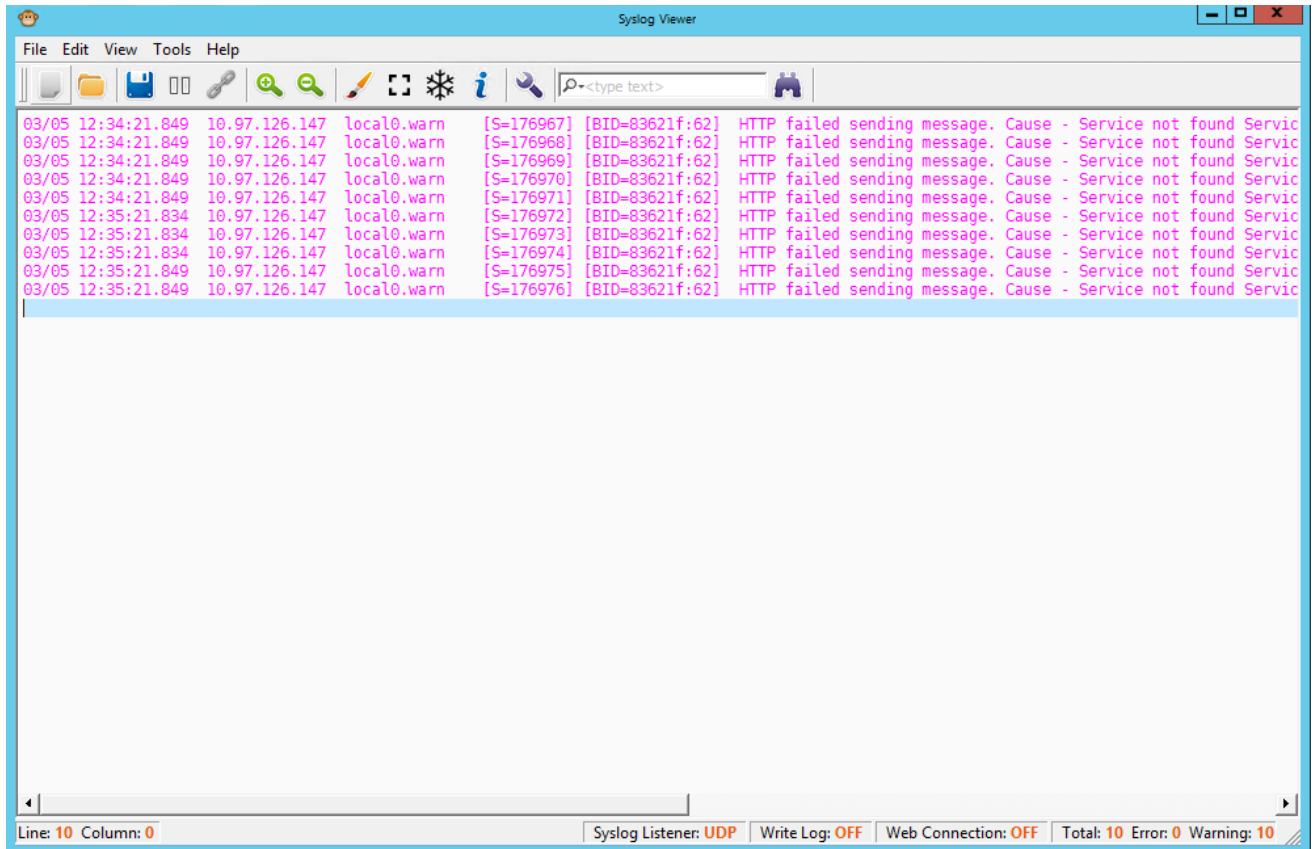
The ACSyslog tool is an AudioCodes software that helps monitoring the SIP calls and the events from the OTSBC device point of view. It can be installed on any PC that is reachable by OTSBC device. All the SIP messages are displayed, even when SIP/TLS protocol is used. ACSyslog traces do not include the media flows (RTP/SRTP). To analyze also the media flows, use Debug Recording Tool (§ 6.2)

To configure Syslog Settings on OTSBC device:

- Open 'Syslog Settings' page (**TROUBLESHOOT > LOGGING > Logging Settings**)
- Enter the IP address of the PC/Server running syslog for 'Syslog Server IP'
- Enable 'Enable Syslog'
- Set 'Debug Level' to 'Detailed'

To configure ACSyslog tool:

- Start the ACSyslog tool on your PC
- Open **Help** tab > **Overview** and follow the document.

To operate ACSyslog tool:

means ACSyslog is collecting the logs.



means ACSyslog is not listening to SBC logs.

Catch the trace and save it by

You can also copy the trace or part of trace by selecting some lines – then click right and select Copy.

5.2 Debug Recording tool

The Debug Recording tool allows displaying the acsyslog traces in a Wireshark format thanks to an AudioCodes proprietary plug-in for Wireshark tool. It can be downloaded from the AudioCodes official website. The plug-in provides proprietary Filter attributes in the Wireshark 'Filter' field, selected by typing 'acdr'.

To install the plug-in on the Wireshark PC:

- Copy the Audiocodes plug-in .dll files (Ac5xPacketRecording_Mii_Wireshark.dll, Ac5xPacketRecording_Wireshark.dll, ...) under \Program Files\Wireshark\plugins\<Wireshark release>.
- Restart Wireshark. (*Wireshark release: 1.10.12 minimum*)

To configure Logging Settings using the Web admin:

- Open the 'Logging settings' page (**TROUBLESHOOT > LOGGING > Logging Settings**)
- Set the Debug Recording Destination IP, then Apply

To configure Logging Filters Table:

- Open the 'Logging filters' page (**TROUBLESHOOT > LOGGING > Logging Filters**)
- If not already available, Add a Logging Filter index '0' with Capture Type = 'Signaling & Media & PCM' and Mode = 'Enable'

6. SBC profiles configuration in OT using 8770

6.1 Creation of the SBC profile for OTCT Remote Workers

- Declare a profile for OTCT Remote Workers to access to OTSBC in secured mode (SIP TLS, SRTP strict mode) from WAN domain. Set Port value = 5261.

The screenshot displays the Alcatel-Lucent 8770 OT configuration interface. On the left, a vertical navigation pane shows various system components: Network, Users, Devices, Configuration, Alarms, Topology, Audit, and Maintenance. The main window is divided into three sections: OT, Profile, and Features. The OT section is active, showing a tree view of the system configuration. Under the 'IT server' folder, the 'sbc-ct' profile is selected. The right pane shows the configuration details for the 'sbc-ct' profile, including a search bar, a 'Where' field, and a table of configuration parameters.

Name	sbc-ct
FQDN	sbc-qa.qa.ale-international.com
Network type	WAN
Transport protocol	TLS
Port	5261
URI schema	SIP
SRTP Mode	Strict
DTMF mode	RFC2833
Keep alive	<input type="checkbox"/>
SwitchOver timer in seconds	60

At the bottom of the right pane, there is a tab labeled '*General'.

6.2 Creation and association of the SBC profile for OTCWeb Remote Workers with WebRTC

- Declare a profile for OTCWeb Remote Workers with WebRTC to access to OTSBC in Web Socket Secured mode (WSS) and SRTP Strict mode from WAN domain. Set Port value = 8061.

The screenshot displays the Alcatel-Lucent OT configuration interface. On the left, a navigation pane shows various categories: Network, Users, Devices, Configuration (highlighted), Alarms, Topology, Audit, and Maintenance. The 'Configuration' section is expanded, showing a tree structure under 'OT' with folders like 'Users and devices', 'Eco system', 'IT server', 'System services', 'Serviceability', and 'Resources'. The 'sbc-wan' profile is selected under the 'IT server' folder.

The main panel shows the configuration details for the 'sbc-wan' profile. A search bar at the top contains 'SBC server'. Below it, a 'Where' field is set to 'Name'. The 'OT Directory' tab is active, displaying a table of configuration parameters:

Name	sbc-wan
FQDN	sbc-qa.qa.ale-international.com
Network type	WAN
Transport protocol	WSS
Port	8061
URI schema	SIP
SRTP Mode	Strict
DTMF mode	RFC2833
Keep alive	<input type="checkbox"/>
SwitchOver timer in seconds	60

At the bottom of the main panel, there is a tab labeled '*General'.

- Associate the profile to the WAN SBC field available in the collaboration configuration:

The screenshot shows the OT 8770 configuration interface. On the left is a navigation pane with icons for Users, Devices, Configuration, Alarms, Topology, Audit, and Maintenance. The main pane displays a tree view of the configuration hierarchy. The 'Collaboration configuration' folder is expanded, showing the 'DEFAULT' profile. The right pane shows the configuration details for the 'DEFAULT' profile, including a search bar and a table of settings.

Collaboration configuration	
Internet access	
WAN SBC	sbc-wan
Session refresh requests interval (seconds)	3600
Session timer refresher	UAC

At the bottom of the interface, there are tabs for 'IM & Presence federation', '*WebRTC conferencing access', and 'Conferencing'.

6.3 HTTP proxy server configuration.

OT server must have access to the Internet, if HTTP proxy server is used declare a profile for HTTP proxy server.

The screenshot shows the OT 8770 configuration interface. On the left, the 'Eco system' folder is expanded, and the 'ALE HTTP proxy' profile is selected. The right pane shows the configuration details for the 'ALE HTTP proxy' profile, including a search bar and a table of settings.

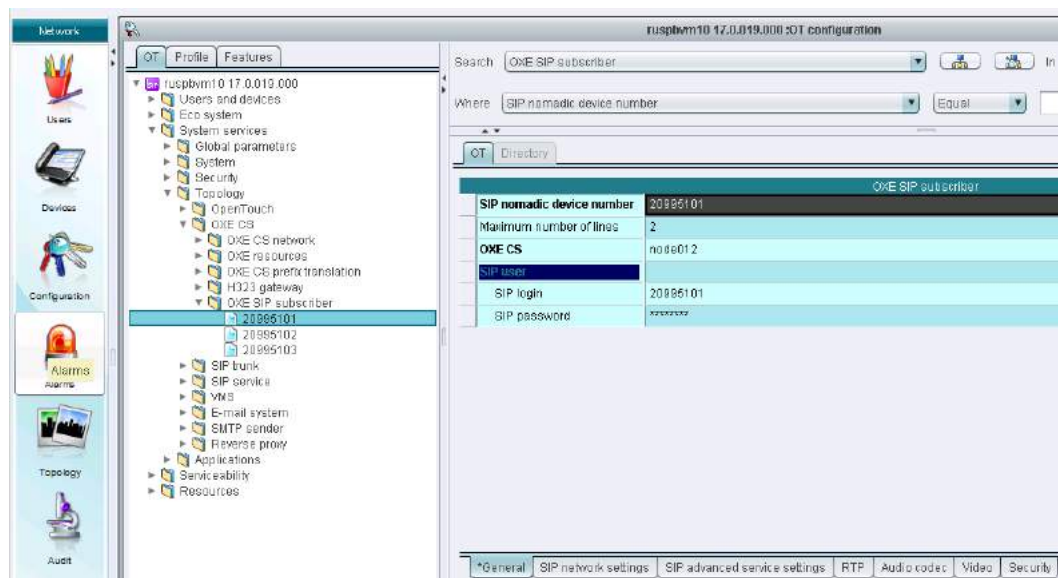
HTTP proxy	
Name	ALE HTTP proxy
FOON	192.168.254.48
Proxy port	8080
Proxy type	HTTP
Proxy username	
Proxy password user	
Proxy authentication method	GASIC
SSL certificate authentication file	
PRG SSL client certificate	
PRG SSL client certificate type	PEM
PRG SSL client key	
PRG SSL client key type	PEM
PRG SSL client key password	

7. OTC devices configuration

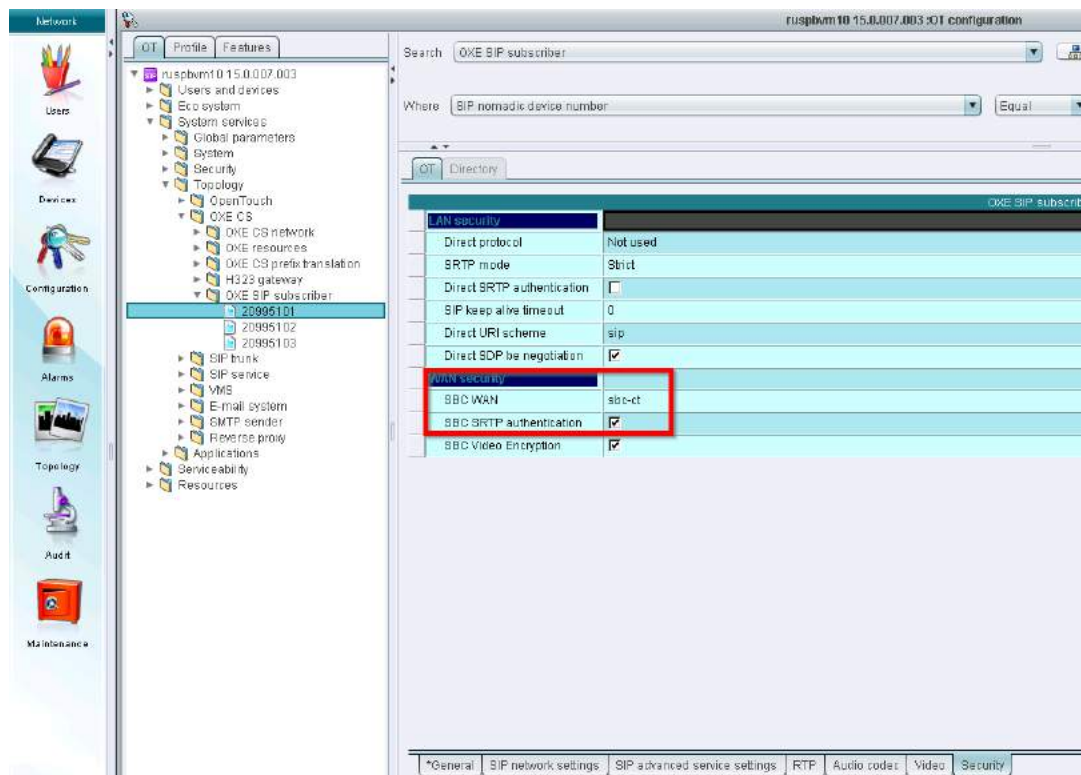
7.1 OTC PC Remote Worker in OXE Nomadic SIP mode

To be operational, the OTCT PC client in Nomadic mode needs an 'OXE SIP Subscriber' (Virtual Ghost SIP) configured in the OXE server as a SIP Device and in the OT server. A pool of 'OXE SIP Subscribers' must be created. Its range depends on the overall quantity of OTCT nomadic users to be declared on the system.

- The SIP password must be the same as configured on OXE side:



- For using the OTC PC client OXE Nomadic in Remote Worker SIP secured mode, apply the SBC profile previously created (§7.1). SBC SRTP authentication is required:



7.2 OTC PC Remote Worker with OTC Smartphone

Go to device configuration > Network tab.

For using the OTC Smartphone client in Remote Worker SIP secured mode, apply the SBC profile previously created (§7.1).

The screenshot shows the configuration interface for a device named 2093100. The left sidebar lists various devices, including 2093100 OTC Smartphone. The main panel shows the configuration for this device, with the Network tab selected. The SBC WAN profile is set to 'sbc-ct', which is highlighted with a red arrow. Other settings include Local SIP port 5160, Protocol UDP, Register expiration, Register duration 720, Session time 3600, Use session timer checked, Session time refresher uac, and SIP IP DSCP 0.

Configuration	Value
LAN	
SBC LAN	
WAN	
SBC WAN	sbc-ct
SIP	
Local SIP port	5160
Protocol	UDP
Register expiration	
Register duration	720
SIP advanced service setting	
Session time	3600
Use session timer	<input checked="" type="checkbox"/>
Session time refresher	uac
SIP IP DSCP	0

7.3 OTC PC Remote Worker in OXE SIP Extension mode

The OTC PC used in OXE SIP extension mode is a standalone client, without any deskphone set.

7.3.1 Configuration of the public Device Management Server

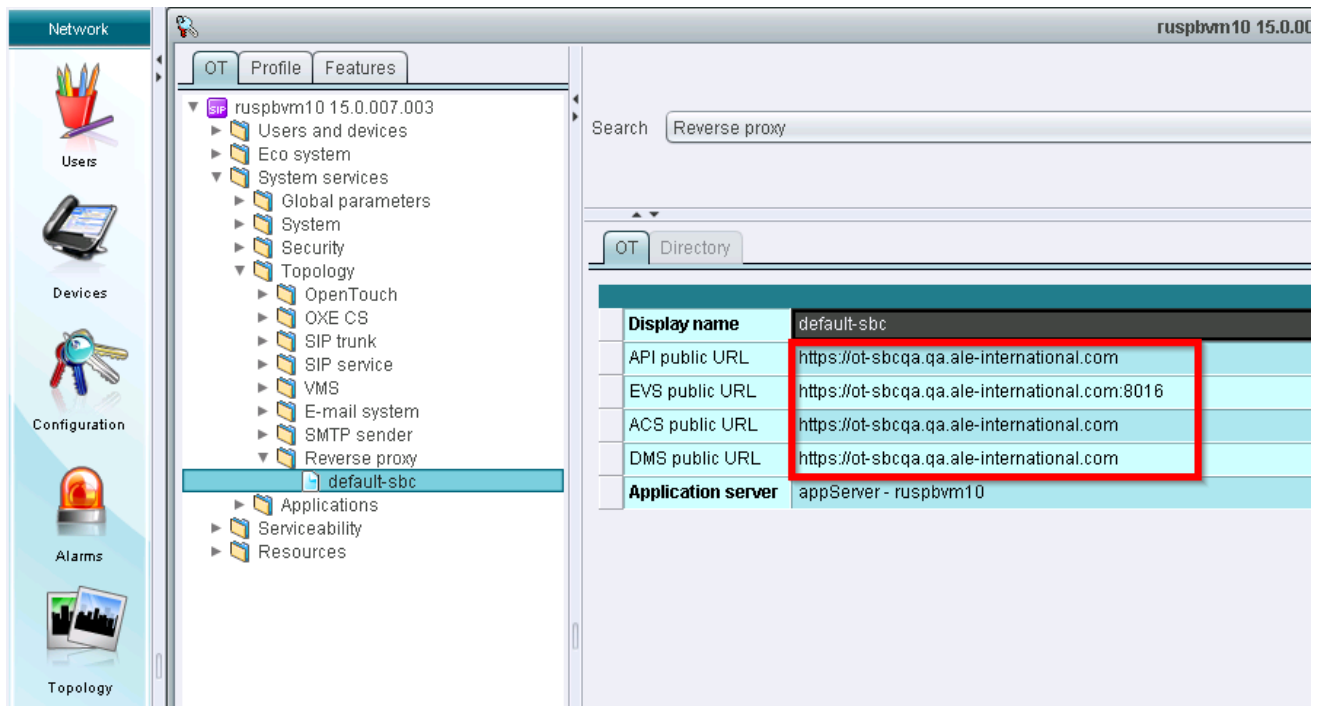
Device Management server must be declared in Eco_system of OT and configured with the corporate LAN FQDN and port 443:

The screenshot shows the configuration interface for the Device Management Server. The left sidebar lists various devices, including ruspbvm10 15.0.007.003. The main panel shows the configuration for this device, with the Network tab selected. The SBC WAN profile is set to 'dm'. The FQDN is set to 'ruspbvm10.load.qa' and the Port is set to 443. The 'Element created during post-installation' checkbox is unchecked.

Configuration	Value
Name	dm
FQDN	ruspbvm10.load.qa
Element created during post-installation	<input type="checkbox"/>
Port	443

The 8770 DM server is also reached by OTC PC SIP Extension from WAN domain via the Reverse Proxy thanks to a specific policy.

The DM service public URL must be configured with the public FQDN for OT server (public Reverse Proxy access):



The screenshot displays the configuration interface for a Reverse proxy service. The left sidebar shows the navigation menu with categories like Users, Devices, Configuration, Alarms, and Topology. The main panel shows the configuration tree for 'ruspbvm10 15.0.007.003', with the 'Reverse proxy' section expanded and 'default-sbc' selected. The 'OT' tab is active, and the 'Directory' sub-tab is selected. A search bar contains the text 'Reverse proxy'. Below the search bar, a table lists the configuration details for 'default-sbc'.

Display name	default-sbc
API public URL	https://ot-sbcqa.qa.ale-international.com
EVS public URL	https://ot-sbcqa.qa.ale-international.com:8016
ACS public URL	https://ot-sbcqa.qa.ale-international.com
DMS public URL	https://ot-sbcqa.qa.ale-international.com
Application server	appServer - ruspbvm10

7.3.2 SIP extension user and device configuration

Declare the public FQDN of OTSBC for connection users in SBC address field, along with the following security parameters:

Go to Device configuration Security tab.

The screenshot displays the configuration interface for a SIP user. On the left, a tree view shows the hierarchy: Alcatel-Lucent Enterprise [13] > irg20001 | irg20001_f [1] > 20001 OTC PC. The main panel shows the configuration for user 20001. The 'Security' tab is selected, and a red box highlights the SBC address and security parameters.

20001	
Direct URI scheme	SIP
Direct protocol	Not used
Direct security level	Clear and encrypted
Direct SRTP authentication	<input checked="" type="checkbox"/>
Direct SDP BE negotiation	<input checked="" type="checkbox"/>
SBC address	sbq-qa.qa.ale-international.com
SBC port	5261
SBC URI scheme	SIP
SBC protocol	TLS
SBC security level	Encrypted only
SBC STRP authentication	<input checked="" type="checkbox"/>
SBC SDP BE negotiation	<input checked="" type="checkbox"/>
SIP keep alive timeout	0
Audio_Crypto_Suites_Security []	
Audio_Crypto_Suite_Security	AES_CM_128_HMAC_SHA1_80
Audio_Crypto_Suite_Security	AES_CM_128_HMAC_SHA1_80
Audio_Crypto_Suite_Security	AES_CM_128_HMAC_SHA1_80
Audio_Crypto_Suite_Security	AES_CM_128_HMAC_SHA1_80
Audio_Crypto_Suite_Security	AES_CM_128_HMAC_SHA1_80
Audio_Crypto_Suite_Security	AES_CM_128_HMAC_SHA1_80
Audio_Crypto_Suite_Security	AES_CM_128_HMAC_SHA1_80
Audio_Crypto_Suite_Security	AES_CM_128_HMAC_SHA1_80

At the bottom, a tab bar shows: General | SIP user | Network | *Advanced services | RTP | Audio codec settings | Video | Security.

And change audio codec settings:

The screenshot shows the configuration interface for an Alcatel-Lucent Enterprise system. On the left, a tree view shows the hierarchy: Alcatel-Lucent Enterprise [13] > irg20001_l irg20001_f [1] > 20001 OTC PC. The main panel displays the configuration for user 20001. The 'Audio codec settings' tab is selected, showing a table of codec orders and their parameters.

20001	
G729 codec order	3
PCMU codec order	2
PCMA Codec order	1
G723 Codec order	4
G729	
Codec framing	20
Codec payload	18
Codec sampling	8000
PCMU	
Codec framing	20
Codec payload	0
Codec sampling	8000
PCMA	
Codec framing	20
Codec payload	8
Codec sampling	8000
G723	
Codec framing	30
Codec bitrate	6.3
Codec payload	4
Codec sampling	8000

At the bottom, a navigation bar includes tabs for General, SIP user, Network, *Advanced services, RTP, Audio codec settings (selected), Video, and Security.

7.3.3 Considering OXE audio domains with specific audio coders settings

A freshly created OXE node operates by default in VoIP 'with compression' mode and all its VoIP 'Connection' users belong to its 'Default' IP domain '0'. The preferred audio operation of OT 'Conversations' desk-phones is Wide Band audio by default (high quality audio), while the OTCv 'Conversation' devices operate preferably in non-compressed audio.

If IT admin wants to keep a compressed mode (G.729A or G.723) for the OXE users domain along with a non-compressed audio (PCMA or PCMU) and WideBand Audio for the OT users, a specific OXE IP domain has to be set for with OTSBC LAN IP address as follow (IP domain '5' here) to avoid any troubles in codec negotiation and possible unidirectional audio conversation.

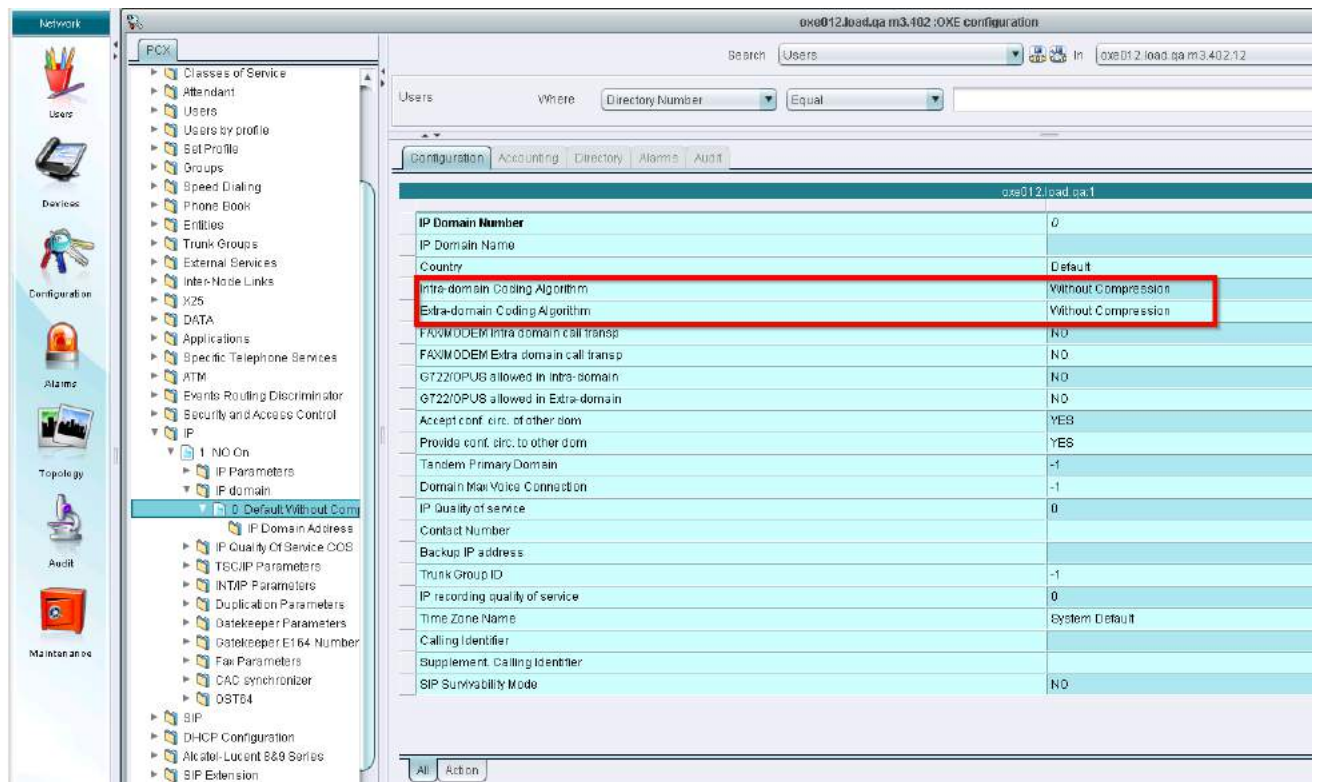
The screenshot shows the PCX configuration interface. On the left, the 'IP' tree is expanded, and '5 For OTSBC Default Without Compression With' is selected. On the right, the 'Configuration' tab is active, showing the configuration for 'ice-qa-ref-2-oxe:1'.

Parameter	Value
IP Domain Number	5
IP Domain Name	For OTSBC
Country	Default
Intra-domain Coding Algorithm	Without Compression
Extra-domain Coding Algorithm	With Compression
Voice Services Broadcast	YES
FAX/MODEM Intra domain call transp	NO
FAX/MODEM Extra domain call transp	NO
G722 allowed in Intra-domain	NO
G722 allowed in Extra-domain	NO
Tandem Primary Domain	-1
Domain Max Voice Connection	-1
IP Quality of service	0
IP Domain Type	IP
Contact Number	
Backup IP address	
Trunk Group ID	-1
IP recording quality of service	0
Time Zone Name	System Default

The screenshot shows the PCX configuration interface. On the left, the 'IP' tree is expanded, and '5 For OTSBC Default Without Compression With' is selected. On the right, the 'Configuration' tab is active, showing the configuration for 'ice-qa-ref-2-oxe:1:5'.

Parameter	Value
IP Address Low	172.26.46.63
IP Address Mode	IP version 4
IP Address High	172.26.46.63
IP NetMask	255.255.255.0
IP Address Type	Host Address

It is not necessary to manage IP domains if the OXE VoIP mode is set to 'without compression' value.

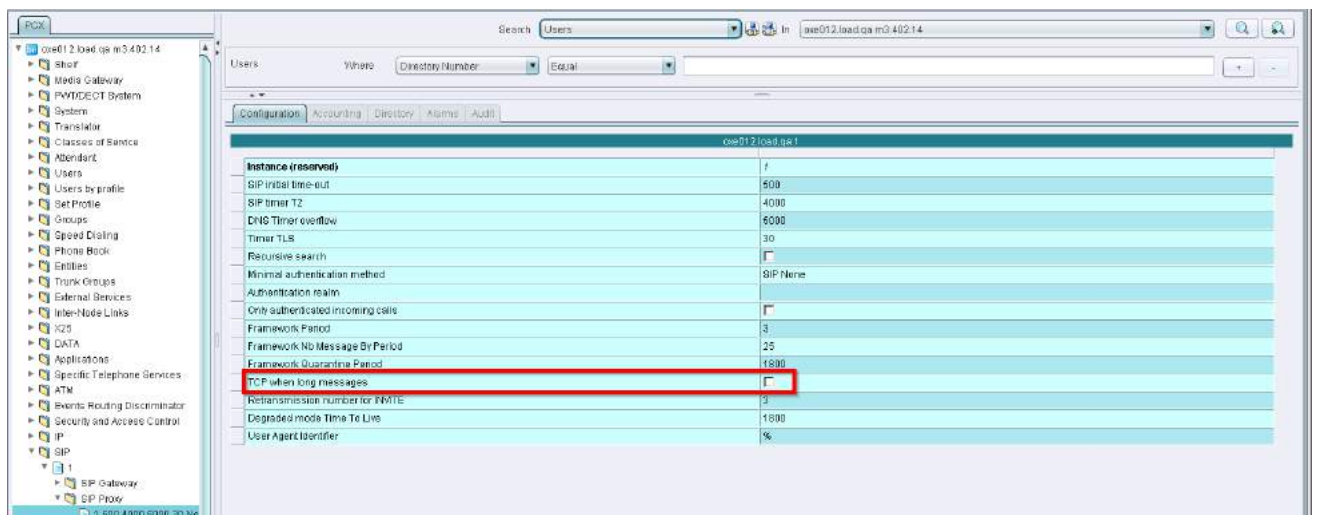


7.4 OTC PC Remote Worker video configuration.

7.4.1 OXE configuration

Go to OXE configuration: SIP > SIP Proxy.

“TCP when long messages” should be untaged.



7.4.2 User configuration

To enable Video in Remote Worker mode go to OTC PC Video tab:

- IP TOS: 7
- SBC encryption: TrueProfile: Medium

The screenshot displays the configuration interface for the '20001 OTC PC' user profile. The left sidebar shows a tree view of users, with '20001 OTC PC' selected. The main panel shows the 'General' tab for the '20001' profile. A red box highlights the 'IP TOS' (7) and 'SBC encryption' (checked) settings. The 'Ciphers suites for video' section shows 'Cipher suite 1' as 'AES_CM_128_HMAC_SHA1_80' and 'Cipher suite 2' as 'AES_CM_128_HMAC_SHA1_32'.

20001	
Enable	<input checked="" type="checkbox"/>
IP TOS	7
SBC encryption	<input checked="" type="checkbox"/>
Profile	Medium
RTP MAP	
Cipher suites for video	
Cipher suite 1	AES_CM_128_HMAC_SHA1_80
Cipher suite 2	AES_CM_128_HMAC_SHA1_32

8. ALES Remote Worker configuration

8.1 HTTP Proxy for DM access

This part can be configured via SBC Wizard

Known issue (not reproduced in the external wizard tool):

[CROT-10720](#): SBC internal wizard does not add the Reverse Proxy configuration to the ini file

For LDAP Authentication on internal OTSBC reverse proxy please refer to section [4.5 of this document](#)

8.1.1 Create Upstream Group

Go to (**Setup > IP Network > HTTP Proxy > Upstream Groups**) and create Upstream group for OXE DM Access

The screenshot shows the Audiocodes Mediant VE SBC configuration interface. The left sidebar contains a 'NETWORK VIEW' menu with various categories like CORE ENTITIES, SECURITY, QUALITY, DNS, WEB SERVICES, and HTTP PROXY. The main area displays 'Upstream Groups (4)' with a table listing existing groups. The group 'OXE_DM_Access' is highlighted with a red box. Below the table, the configuration details for this group are shown under the '#3[OXE_DM_Access]' header. The 'GENERAL' tab is active, showing fields for Name, Protocol, Load Balancing Mode, and Max Connections. The 'Name' and 'Protocol' fields are highlighted with a red box.

INDEX	NAME	PROTOCOL	LOAD BALANCING MODE	MAX CONNECTIONS
0	ot_443	HTTP\HTTPS	IP Hash	0
1	ot_8016	HTTP\HTTPS	IP Hash	0
2	conf_internal_443	HTTP\HTTPS	IP Hash	0
3	OXE_DM_Access	HTTP\HTTPS	Round Robin	0

#3[OXE_DM_Access]

GENERAL

Name	OXE_DM_Access
Protocol	HTTP\HTTPS
Load Balancing Mode	Round Robin
Max Connections	0

Upstream Hosts 0 items >>

Enter Upstream group **name** and **Protocol**: HTTP\HTTPS

8.1.2 Add Upstream Host to Upstream Group

Press “Upstream hosts” link in (**Setup > IP Network > HTTP Proxy > Upstream Groups**) and add OXE host

The screenshot displays the Audiocodes Mediant VE SBC configuration interface. The top navigation bar includes 'SETUP', 'MONITOR', and 'TROUBLESHOOT' tabs. The left sidebar shows the 'IP NETWORK' section with various configuration options. The main content area is titled 'Upstream Groups [#3] > Upstream Hosts (1)'. A table lists the upstream hosts, with the first entry highlighted by a red box:

INDEX	HOST	PORT	WEIGHT	BACKUP
0	node012.load.qa	443	1	Disable

Below the table, the configuration for group #0 is shown under the 'GENERAL' tab. The 'Host' and 'Port' fields are highlighted by a red box:

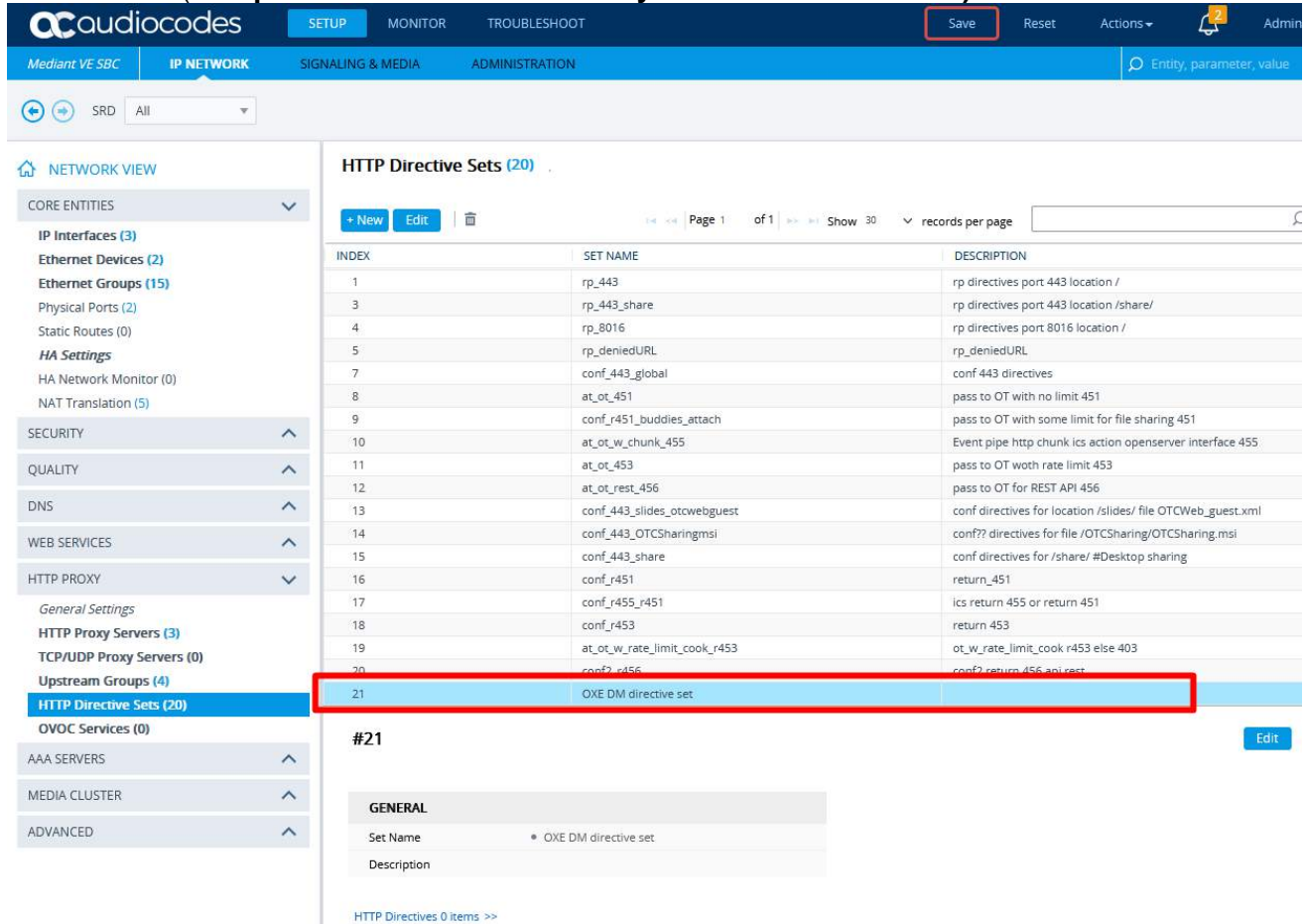
GENERAL	
Host	• node012.load.qa
Port	• 443
Weight	1
Backup	Disable

Host: OXE IP or FQDN

Port: DM access port

8.1.3 Create HTTP Directive set

Go to (Setup > IP Network > HTTP Proxy > HTTP Directive Sets)



HTTP Directive Sets (20)

INDEX	SET NAME	DESCRIPTION
1	rp_443	rp directives port 443 location /
3	rp_443_share	rp directives port 443 location /share/
4	rp_8016	rp directives port 8016 location /
5	rp_deniedURL	rp_deniedURL
7	conf_443_global	conf 443 directives
8	at_ot_451	pass to OT with no limit 451
9	conf_r451_buddies_attach	pass to OT with some limit for file sharing 451
10	at_ot_w_chunk_455	Event pipe http chunk ics action opensever interface 455
11	at_ot_453	pass to OT with rate limit 453
12	at_ot_rest_456	pass to OT for REST API 456
13	conf_443_slides_otcwebguest	conf directives for location /slides/ file.OTCWeb_guest.xml
14	conf_443_OTCSharingmsi	conf?? directives for file /OTCSharing/OTCSharing.msi
15	conf_443_share	conf directives for /share/ #Desktop sharing
16	conf_r451	return_451
17	conf_r455_r451	ics return 455 or return 451
18	conf_r453	return 453
19	at_ot_w_rate_limit_cook_r453	ot_w_rate_limit_cook r453 else 403
20	conf2_r456	conf2 return 456 api rest
21	OXE DM directive set	

#21

GENERAL

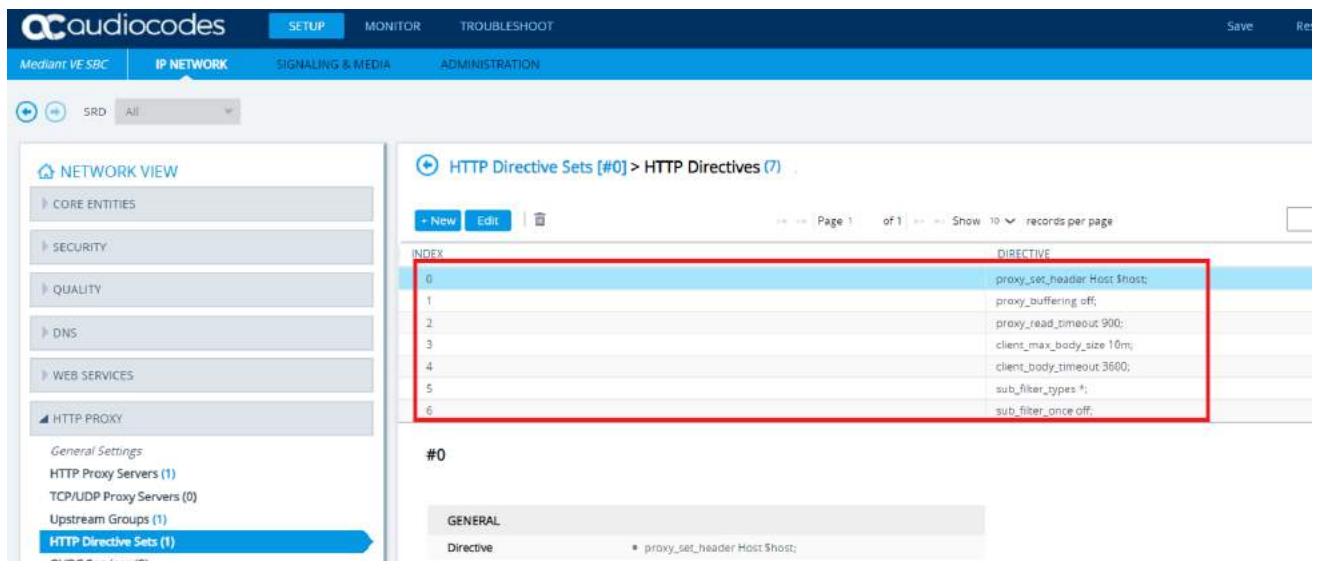
Set Name: OXE DM directive set

Description: Any

Name and Description: Any

8.1.4 Add directives to Directive set

Go to (Setup > IP Network > HTTP Proxy > HTTP Directive Sets -> OXE Directive set -> HTTP Directives)



HTTP Directive Sets [#0] > HTTP Directives (7)

INDEX	DIRECTIVE
0	proxy_set_header Host \$host;
1	proxy_buffering off;
2	proxy_read_timeout 900;
3	client_max_body_size 16m;
4	client_body_timeout 3600;
5	sub_filter_types *;
6	sub_filter_once off;

#0

GENERAL

Directive: proxy_set_header Host \$host;

Add new directives line by line:

```
proxy_set_header Host $host;
proxy_buffering off;
proxy_read_timeout 900;
client_max_body_size 10m;
client_body_timeout 3600;
sub_filter_types *;
sub_filter_once off;
```

8.1.5 Create HTTP Proxy Server

Go to (Setup > IP Network > HTTP Proxy > HTTP Proxy Servers)

The screenshot shows the Alcatel-Lucent Mediant VE SBC configuration interface. The left sidebar displays the navigation menu with 'HTTP Proxy Servers (4)' selected under 'HTTP PROXY'. The main area shows a table of HTTP Proxy Servers. The table has columns: INDEX, NAME, DOMAIN NAME, LISTENING INTERFACE, HTTP LISTENING PORT, HTTPS LISTENING PORT, TLS CONTEXT, BIND TO DEVICE, VERIFY CLIENT CERTIFICATE, and ADDITIONAL DIRECTIVE SET. The row with INDEX 3 is highlighted with a red box. Below the table, the configuration details for '#3[OXE DM Access]' are shown. The 'GENERAL' section is expanded, and the following fields are highlighted with red boxes:

- Name:** OXE DM Access
- Domain Name:** oxe-sbcqa.qa.ale-international.com
- Listening Interface:** RP
- HTTP Listening Port:** (empty)
- HTTPS Listening Port:** 443
- TLS Context:** TLSContexts_1
- Bind To Device:** Disable
- Verify Client Certificate:** No

The 'Additional Directive Set' field is also visible, showing 'OXE DM dire'.

Name: Any

Domain Name: External SBC FQDN for OXE RP

Listening Interface: New or existing external interface for OXE RP

HTTPS Listening Port: External port for OXE RP access

Bind To Device: Disable

Additional Directive Set: [OXE DM Directive set](#)

8.1.6 Create HTTP Location for Proxy Server

Go to (Setup > IP Network > HTTP Proxy > HTTP Proxy Servers -> HTTP Locations)

The screenshot shows the Alcatel-Lucent Mediant VE SBC configuration interface. The left sidebar contains a tree view with categories like Physical Ports, Static Routes, HA Settings, NAT Translation, SECURITY, QUALITY, DNS, WEB SERVICES, and HTTP PROXY. Under HTTP PROXY, 'HTTP Proxy Servers (1)' is selected. The main area displays a table of HTTP Proxy Servers. The first entry is highlighted with a red box. Below the table, the configuration details for this entry are shown in a form with two tabs: GENERAL and SSL. The GENERAL tab is active, showing fields for URL Pattern, URL Pattern Type, Upstream Scheme, Upstream Group, Upstream Path, Outbound Interface, Additional Directive Set, and Cache. The SSL tab shows fields for TLS Context and Verify Certificate.

INDEX	URL PATTERN	URL PATTERN TYPE	UPSTREAM SCHEME	UPSTREAM GROUP	UPSTREAM PATH	OUTBOUND INTERFACE	TLS CONTEXT	VERIFY CERTIFICATE	CACHE
1	/DM/dmsoftphone/	Prefix	HTTPS	oxe_443	/DM/dmsoftphone/	RP	TLSContexts_1	No	No

#1

GENERAL

URL Pattern: /DM/dmsoftphone/

URL Pattern Type: Prefix

Upstream Scheme: HTTPS

Upstream Group: oxe_443

Upstream Path: /DM/dmsoftphone/

Outbound Interface: RP

Additional Directive Set: -

Cache: No

SSL

TLS Context: TLSContexts_1

Verify Certificate: No

URL Pattern: /DM/dmsoftphone/

Upstream Scheme: HTTPS

Upstream Group: OXE Upstream Group from step 9.1.1

Upstream Path: /DM/dmsoftphone/

Outbound Interface: New or existing external interface for OXE RP

Cache: No

TLS Context: TLS Contexts for OXE DM

8.2 Internal LDAP search for Remote Workers

For LDAP search in Remote Worker, the external FQDN with LDAPS port should be resolved by local DNS as a local LDAP server. Only secure connections are allowed on both sides. Need to set external FQDN with LDAPS protocol in DM file configuration.

8.2.1 TLS contexts for LDAP

Create or update existing [TLS contexts](#) with certificates for LDAP public and local FQDN. In the root certificates of this TLS context, need to add the LDAP server certificate.

8.2.2 Create Upstream Group for LDAP server

Create new Upstream Group for access to LDAP server. Go to **(SETUP > IP NETWORK > HTTP PROXY > Upstream Groups)**

The screenshot shows the Audiocodes Mediant VE SBC configuration interface. The left sidebar contains a 'NETWORK VIEW' section with various categories like CORE ENTITIES, SECURITY, QUALITY, DNS, WEB SERVICES, HTTP PROXY, and AAA SERVERS. The 'HTTP PROXY' section is expanded, showing 'Upstream Groups (5)'. The main area displays a table of upstream groups. The group 'LDAP_ALES_Access' (index 4) is highlighted with a red box. Below the table, the configuration details for this group are shown, with the 'Name' and 'Protocol' fields also highlighted by a red box.

INDEX	NAME	PROTOCOL	LOAD BALANCING MODE	MAX CONNECTIONS
0	ot_443	HTTP/HTTPS	IP Hash	0
1	ot_8016	HTTP/HTTPS	IP Hash	0
2	conf_internal_443	HTTP/HTTPS	IP Hash	0
3	OVE_DM_Access	HTTP/HTTPS	Round Robin	0
4	LDAP_ALES_Access	TCP/UDP	Round Robin	0

#4[LDAP_ALES_Access]

GENERAL

Name	* LDAP_ALES_Access
Protocol	* TCP/UDP
Load Balancing Mode	Round Robin
Max Connections	0

Upstream Hosts 0 items >>

Name: Any
Protocol: TCP/UDP

8.2.3 Create Upstream Hosts for Upstream group

Create new Upstream Host. Go to **(SETUP > IP NETWORK > HTTP PROXY > Upstream Groups > Upstream Hosts)**

The screenshot displays the Alcatel-Lucent Mediant VE SBC configuration interface. The top navigation bar includes tabs for SETUP, MONITOR, TROUBLESHOOT, and a highlighted Save button. Below the navigation bar, the IP NETWORK section is active, showing a list of entities on the left and a table of Upstream Groups on the right. The table has columns for INDEX, HOST, PORT, WEIGHT, MAX CONNECTIONS, and BACKUP. A single row is shown with index 0, host 135.247.192.62, port 636, weight 1, max connections 0, and backup disabled. Below the table, the configuration details for group #0 are shown, with the Host and Port fields highlighted in a red box.

INDEX	HOST	PORT	WEIGHT	MAX CONNECTIONS	BACKUP
0	135.247.192.62	636	1	0	Disable

GENERAL

Host	135.247.192.62
Port	636
Weight	1
Max Connections	0
Backup	Disable

Host: LDAP Server local IP or FQDN

Port: 636 (Or configured secured LDAPS port)

8.2.4 Create TCP/UDP Proxy Server

Create new TCP/UDP Proxy Server. Go to **(SETUP > IP NETWORK > HTTP PROXY > Upstream Groups > TCP/UDP Proxy Servers)**

The screenshot shows the Audiocodes configuration interface. The left sidebar contains a 'NETWORK VIEW' menu with categories like CORE ENTITIES, SECURITY, QUALITY, DNS, WEB SERVICES, and HTTP PROXY. Under HTTP PROXY, 'TCP/UDP Proxy Servers (1)' is selected. The main area displays a table of 'TCP/UDP Proxy Servers (1)' with one entry: index 0, name 'LDAP ALES Search', listening interface 'RP_IF', TCP listening port 636, and various other settings. Below the table, the configuration details for '#0[LDAP ALES Search]' are shown in three sections: GENERAL, LISTEN PARAMETERS, and UPSTREAM PARAMETERS. Red boxes highlight the following fields:

- GENERAL:** Name (LDAP ALES Search)
- LISTEN PARAMETERS:** Listening Interface (RP_IF), TCP Listening Port (636), Listen Side SSL (Enable), Listen TLS Context (ALES TLS Context)
- UPSTREAM PARAMETERS:** Upstream Group (ALES_Exchange_LDAP), Outbound Interface (LAN_LDAP_IF), Upstream Side SSL (Enable), Upstream TLS Context (ALES TLS Context), Upstream Verify Certificate (Yes)

Name: Any

Listening Interface: WAN interface for LDAP access

TCP Listening Port: 636 (Or same port as on local LDAP secured access)

Listen Side SSL: Enable

Listen TLS Context: TLS Context with LDAP server certificate for external FQDN

Upstream Group: Upstream group for local LDAP server

Outbound Interface: Local interface to access LDAP server

Upstream Side SSL: Enable

Upstream TLS Context: TLS Context for local LDAP server

Upstream Verify Certificate: Yes

9. Annexes

9.1 Procedure to change default UDP port between kamailio-wasp and SIP proxy

If you need to change 5160 port to 5060 port connect to OpenTouch for any reason.

You can use the following script:

```
cd /usr/kamailio-wasp/
```

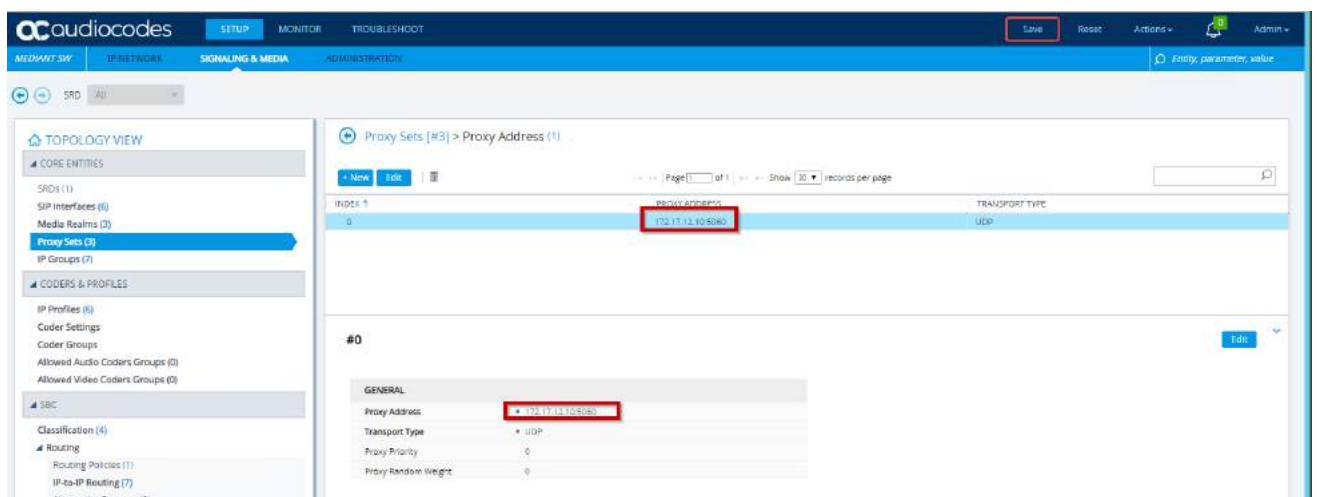
```
./setdefaultsiport.sh (to see the configuration)
```

```
./setdefaultsiport.sh wasp (to set port 5060 for iPhones)
```

```
./setdefaultsiport.sh proxy (to move back port 5160 for iPhones)
```

Also you need to change port in SBC configuration:

- Open the 'Proxy Sets' page (**SETUP > SIGNALING & MEDIA > CORE ENTITIES > Proxy Sets**)
- Choose 'Kamailio'
- Open the **Proxy Address** (use the link on the bottom of the page): IP Address (or FQDN) of OT server: 5060:



- Open the 'Message Manipulations' page (**SETUP > SIGNALING & MEDIA > MESSAGE MANIPULATION > Message Manipulations**).
- Index 36 (Manip Set ID 8) modify port to 5060.

audiocodes SETUP MONITOR TROUBLESHOOT Save Reset Actions Admin

Module SW IP NETWORK SIGNALING & MEDIA ADMINISTRATION Entity, parameter, value

SBD All

TOPOLOGY VIEW

- CORE ENTITIES
- CODERS & PROFILES
- SBC
- SIP DEFINITIONS
- MESSAGE MANIPULATION
 - Message Manipulations (20)**
 - Message Conditions (2)
 - Message Policies (1)
 - Pre-Parsing Manipulation Sets (0)
- MEDIA
- INTRUSION DETECTION

Message Manipulations (20)

New Edit Insert Page 1 of 1 Show 20 records per page

Index	NAME	MANIPULATION SET ID	MESSAGE TYPE	CONDITION	ACTION SUBJECT	ACTION TYPE	ACTION VALUE	ROW ROLE
2		1			header:from:uri:host	Modify	*:russpvm10:load:qsl	Use Current Condition
3		2			header:to:uri:host	Modify	*:russpvm10:load:qsl	Use Current Condition
4		3			header:from:uri:host	Modify	*:russpvm10:load:qsl	Use Current Condition
11		4			header:to:uri:host	Modify	*:russpvm10:load:qsl	Use Current Condition
12		4			header:from:uri:host	Modify	*:russpvm10:load:qsl	Use Current Condition
13		4	refer request	header:Refer-To exists	header:Refer-To:uri:host	Modify	*:russpvm10:load:qsl:8061	Use Current Condition
14		4	refer request	header:Refer-To exists	header:Refer-To:uri:host	Modify	*:russpvm10:load:qsl:8061	Use Current Condition
15		5			header:to:uri:host	Modify	*:russpvm10:load:qsl:8061	Use Current Condition
16		5			header:from:uri:host	Modify	*:russpvm10:load:qsl:8061	Use Current Condition
17		5	refer request	header:Refer-To exists	header:Refer-To:uri:host	Modify	*:russpvm10:load:qsl:8061	Use Current Condition
18		5	refer request	header:Refer-To exists	header:Refer-To:uri:host	Modify	*:russpvm10:load:qsl:8061	Use Current Condition
30		7			header:to:uri:host	Modify	*:russpvm10:load:qsl:8061	Use Current Condition
31		7			header:from:uri:host	Modify	*:russpvm10:load:qsl:8061	Use Current Condition
32		7	refer request	header:Refer-To exists	header:Refer-To:uri:host	Modify	*:russpvm10:load:qsl:8061	Use Current Condition
33		7	refer request	header:Refer-To exists	header:Refer-To:uri:host	Modify	*:russpvm10:load:qsl:8061	Use Current Condition
34		7	refer request	header:Refer-To exists	header:Refer-To:uri:trunkip	Modify	*:russpvm10:load:qsl:8061	Use Current Condition
35		7	refer request	header:Refer-To exists	header:Refer-To:uri:trunkip	Modify	*:russpvm10:load:qsl:8061	Use Current Condition
36		8			header:to:uri:host	Modify	*:russpvm10:load:qsl:8061	Use Current Condition
37		8			header:from:uri:host	Modify	*:russpvm10:load:qsl:8061	Use Current Condition

#36 Edit

GENERAL

Name

Manipulation Set ID **#**

Row Role Use Current Condition

ACTION

Action Subject * header:to:uri:host

Action Type * Modify

Action Value * *:russpvm10:load:qsl:8061

MATCH

Message Type

Condition

9.2 Embedded Nginx in a non-IPv6 environment.

To avoid possible problems with Nginx address resolution if you are not using IPv6 in your office network, an additional step should be performed to prevent Nginx from trying to resolve IPv6 records. This is known to cause problems with OTC Web.

To do this, navigate to the AdminPage of your SBC: [http\(s\)://<your SBC address>/AdminPage](http(s)://<your SBC address>/AdminPage)

and introduce a new variable “NGINXRESOLVERPARAMS” with a value “ipv6=off” and press “Apply New Value” button. You should get an output similar to the screenshot below:

The screenshot shows the SBC AdminPage interface. On the left is a sidebar with links: "Image Load to Device", "ini Parameters", and "Back to Main". The main area has a form with "Parameter Name:" set to "NGINXRESOLVERPARAMS" and "Enter Value:" set to "ipv6=off". An "Apply New Value" button is in the top right. Below the form is an "Output Window" displaying the following text:

```
Parameter Name: NGINXRESOLVERPARAMS
Parameter New Value: ipv6=off
Parameter Description:
```

After that, go back to the regular SBC page and reset your device with “Save To Flash” option checked:

The screenshot shows the SBC Administration page. The top navigation bar includes "audiodcodes", "SETUP", "MONITOR", "TROUBLESHOOT", "Save", "Reset" (highlighted with a red box), "Actions", and "Admin". The "ADMINISTRATION" tab is selected. On the left is a sidebar with "TIME & DATE" and "MAINTENANCE" sections. The "Maintenance Actions" section is expanded, showing "Configuration File", "Auxiliary Files", "High-Availability Maintenance", "System Snapshots", "Software Upgrade", and "Configuration Wizard". The "Maintenance Actions" panel has two tabs: "RESET DEVICE" and "LOCK / UNLOCK". Under "RESET DEVICE", there are three rows: "Reset Device" with a "RESET" button (highlighted with a red box), "Save To Flash" with a dropdown menu set to "Yes" (highlighted with a red box), and "Graceful Reset" with a dropdown menu set to "No". Under "LOCK / UNLOCK", there are three rows: "Lock" with a "LOCK" button, "Graceful Option" with a dropdown menu set to "No", and "Disconnect Client Connections" with a dropdown menu set to "Disable". The "Device Operational State" is shown as "UNLOCKED".