

Connecting BroadCloud SIP Trunk to Microsoft® Lync 2010/2013 or Skype for Business Server 2015 using AudioCodes Mediant E-SBC

Version 7.0



Table of Contents

1	Introduction	5
1.1	Making BroadCloud Preparations	5
1.2	Component Information.....	6
1.2.1	AudioCodes E-SBC Version	6
1.2.2	BroadCloud SIP Trunking Version.....	6
1.2.3	Microsoft Skype for Business Server 2015 Version	6
1.2.4	Solution Topology	7
2	Installing the Hardware.....	9
2.1	Mediant 500L Media Gateway	9
2.1.1	Front Panel	9
2.1.2	Rear Panel.....	9
2.1.3	Cabling.....	10
2.1.3.1	Connecting Ethernet Interfaces.....	10
2.1.3.2	Connecting to the Power Supply.....	11
2.1.4	Powering the Device On / Off	12
2.2	Mediant 500 E-SBC	13
2.2.1	Cabling.....	13
2.2.1.1	Grounding the Device.....	13
2.2.1.2	Connecting Ethernet Interfaces.....	14
2.2.1.3	Connecting to the Power Supply	15
2.3	Mediant 800B E-SBC	16
2.3.1	Front Panel	16
2.3.2	Front Panel LEDs	16
2.3.2.1	Operational Status LEDs.....	16
2.3.3	Rear Panel.....	17
2.3.4	Cabling.....	17
2.3.4.1	Grounding the Device.....	17
2.3.4.2	Connecting to Ethernet.....	17
2.3.5	Powering up.....	18
2.4	Mediant 2600 E-SBC	20
2.4.1	Front Panel	20
2.4.2	Rear Panel.....	20
2.4.3	Cabling.....	21
2.4.3.1	Grounding the Device.....	21
2.4.3.2	Connecting to Ethernet.....	21
2.4.3.3	Connecting to the Power Supply	22
3	Connecting to the Management Interface	23
3.1	Default OAMP IP Address.....	23
3.2	Connecting to the Embedded Web Server.....	23
4	Configuring the Device	25
4.1	Step 1: Download, Install BroadCloud Certified Firmware / Configuration.....	25
4.2	Step 2: Configure a Network Interface for the Device	29
4.2.1	Step 2a: Configure Network Interfaces.....	30
4.2.2	Step 2b: Configure NAT.....	31
4.3	Step 3: Configure the UDP Ports for RTP between the SBC and Skype for Business.....	33
4.4	Step 4: Configure the Skype for Business Address	34
4.5	Step 5: Configure a SIP TLS Connection.....	35
4.5.1	Step 5a: Configure the NTP Server Address.....	35

4.5.2	Step 5b: Configure TLS Version 1.0.....	36
4.5.3	Step 5c: Configure a Certificate.....	37
4.6	Step 6: Configure SIP Host Name for Skype for Business	42
4.7	Step 7: Configure Dial Plan Rules (Optional).....	43
4.8	Step 8: Configure Registration to the BroadCloud Service	45
4.8.1	Configure Credentials.....	45
4.8.2	Configure the SIP Register Domain Name.....	46
4.9	Step 9: Check the SIP Trunk Registration Status	47
4.10	Step 10: Secure Device Access.....	48
4.10.1	Change Default Management User Login Passwords	48
4.10.2	Secure Management Access via WAN.....	48
4.11	Step 11: Save the Configuration, Connect to DMZ	49
A	Troubleshooting.....	51
A.1	Connecting to CLI	51
A.2	Enabling Logging on CLI.....	51

Notice

This document describes how to connect Microsoft's Lync Server 2010/2013 or Skype for Business Server 2015 to the BroadCloud SIP Trunk using AudioCodes' Mediant E-SBC product series.

Information contained in this document is believed to be accurate and reliable at the time of printing. However, due to ongoing product improvements and revisions, AudioCodes cannot guarantee accuracy of printed material after the Date Published, nor can it accept responsibility for errors or omissions. Updates to this document and other documents as well as software files can be viewed by registered customers at <http://www.audiocodes.com/downloads>.

© Copyright 2016 AudioCodes Ltd. All rights reserved.

This document is subject to change without notice.

Date Published: Aug-04-2016

1 Introduction

This Configuration Note shows how to set up AudioCodes' Enterprise Session Border Controller (referred to as E-SBC in this document) for interworking between BroadCloud's SIP Trunk and Microsoft's Skype for Business Server 2015 environment.

**Note:**

- The configuration was also verified with Microsoft Lync 2010 and 2013.
- Lync 2010/2013 users may therefore also use this guide.
- 'Skype for Business' is used synonymously with 'Lync' in this guide.

1.1 Making BroadCloud Preparations

Before reading and using this *Quick Setup Guide*, read the *BroadCloud SIP Trunking Service Definition* guide available from the BroadCloud knowledgebase (info.broadcloudpbx.com).



Note: The *BroadCloud SIP Trunking Service Definition* guide details how to provision SIP Trunk Groups, SIP Trunk Users and SIP Trunk Mobility Users. This guide assumes you've read that guide, and that the required provisioning has been completed.

When provisioning, select the appropriate Shared Device Type:

AudioCodes Mediant Device



Note: If you do not have this device type available in your service offering, contact your Account Manager who will arrange it for you.

1.2 Component Information

1.2.1 AudioCodes E-SBC Version

Table 1-1: AudioCodes E-SBC Version

SBC Vendor	AudioCodes
Models	<ul style="list-style-type: none"> ▪ Mediant 500L ▪ Mediant 500 ▪ Mediant 800
Software Version	SIP_F7.00A.044.007
Protocol	<ul style="list-style-type: none"> ▪ SIP/UDP (to the BroadCloud SIP Trunk) ▪ SIP/UDP or SIP/TCP (to Skype for Business)

1.2.2 BroadCloud SIP Trunking Version

Table 1-2: BroadCloud Version

Vendor/Service Provider	BroadCloud
SSW Model/Service	BroadWorks
Software Version	21
Protocol	SIP/UDP

1.2.3 Microsoft Skype for Business Server 2015 Version

Table 1-3: Microsoft Skype for Business Server 2015 Version

Vendor	Microsoft
Model	Skype for Business
Software Version	Release 2015 6.0.9319.0
Protocol	SIP
Additional Notes	None



Note:

- The configuration was also verified with Microsoft Lync 2010 and 2013.
- Lync 2010/2013 users may therefore also use this guide.
- 'Skype for Business' is used synonymously with 'Lync' in this guide.

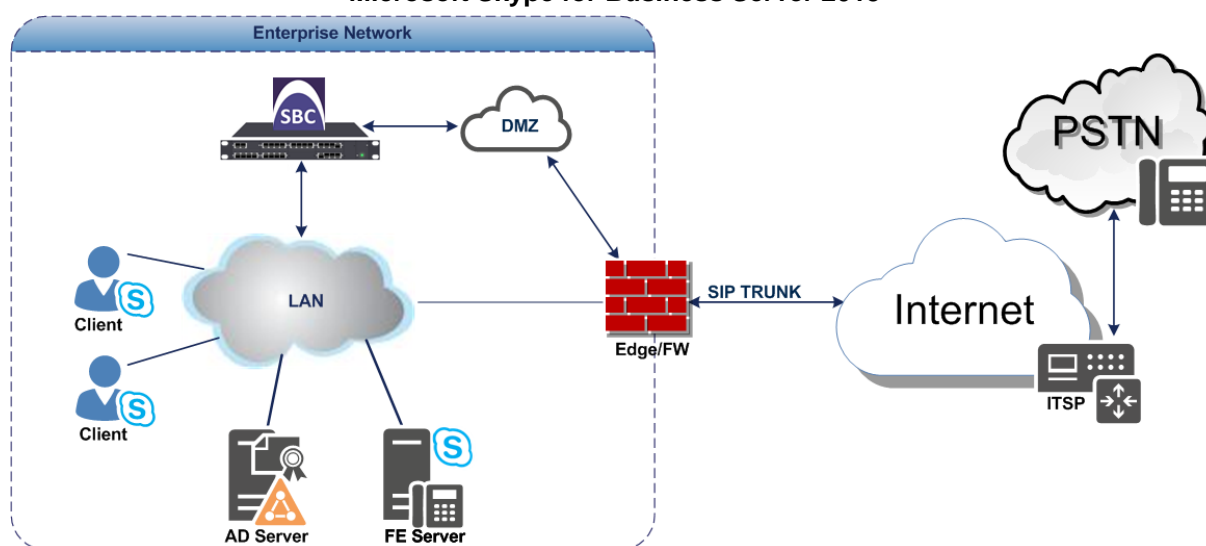
1.2.4 Solution Topology

Interoperability between BroadCloud SIP Trunk and Microsoft's Skype for Business Server 2015 using AudioCodes' Mediant E-SBC was achieved using the following test topology setup:

- Microsoft Skype for Business Server 2015 deployed in an enterprise's private network
- AudioCodes' Mediant E-SBC device connecting the enterprise's Skype for Business Server 2015 to the BroadCloud SIP trunking service over IP
- Internet/MPLS network connectivity to the BroadCloud SIP trunk service

The figure below illustrates this solution topology:

Figure 1-1: Network Topology: AudioCodes Mediant E-SBC Connects BroadCloud SIP Trunk to Microsoft Skype for Business Server 2015



This page is intentionally left blank.

2 Installing the Hardware

2.1 Mediant 500L Media Gateway

2.1.1 Front Panel

LEDs on the front panel indicate functionality statuses.

Figure 2-1: Front Panel - LEDs



When green, 1 (power LED) indicates power is on. Table 2-1 describes 2 (Status LED).

Table 2-1: Status LED


LED Color	LED State	Description
Green	On	Device is operational.
	Flashing	Initial rebooting stage.
Red	On	Boot failure.
-	Off	Advanced rebooting stage.

2.1.2 Rear Panel

Figure 2-2: Rear Panel



Table 2-2: Rear Panel

Item #	Label	Description
1	POWER 12V -- 3A	AC power supply plug entry to connect to the external AC power supply adapter.
2	ON / OFF	Power button which powers on the device when pressed in and powers off the device when pressed again (pressed out).
3	CONSOLE	RJ-45 port for RS-232 serial communication with the device.
4		USB 2.0 port, not applicable.
5	//	Reset pinhole button to reset the device or to restore to factory defaults. To restore to factory defaults: With a paper clip or any other similar pointed object, press and hold down the pinhole button for at least 12 seconds, but no longer than 25 seconds
6	S1 / FE LAN	Up to four Fast Ethernet (10/100Base-T) ports (RJ-45) to connect to LAN or WAN. These support full-duplex modes, auto-negotiation, and straight or crossover cable detection.

2.1.3 Cabling

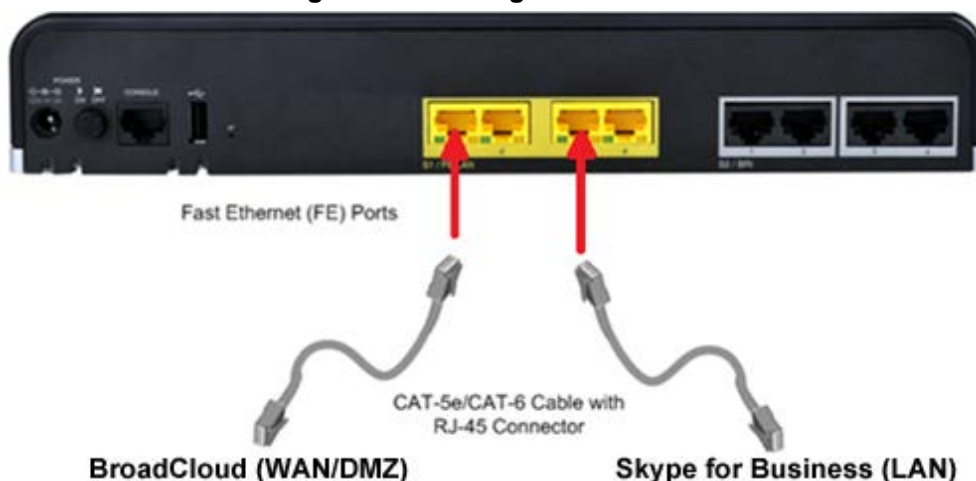
2.1.3.1 Connecting Ethernet Interfaces

Four Fast Ethernet (10/100Base-T) ports (supporting half- and full-duplex modes, auto-negotiation, and straight or crossover cable detection) allow connection to the LAN/WAN.

➤ **To connect the device to the BroadCloud service (WAN-DMZ):**

1. If the device's IP isn't configured yet, connect as shown in Section 3.
2. If the device's IP has already been configured:
 - a. Connect one end of a straight-through RJ-45 Cat 5e or Cat 6 cable to the RJ-45 port labeled S1 / FE LAN port 1.
 - b. Connect the other end to the DMZ port assigned by the IT administrator.

Figure 2-3: Cabling Ethernet Ports



➤ **To connect the device to Skype for Business (LAN):**

1. If the device's IP isn't configured yet, connect as shown in Section 3.
2. If the device's IP has already been configured:
 - a. Connect one end of a straight-through RJ-45 Cat 5e or Cat 6 cable to the RJ-45 port labeled S1 / FE LAN port 3.
 - b. Connect the other end to your local network LAN layer 2 switch port. This port will be used to communicate with Skype for Business.

2.1.3.2 Connecting to the Power Supply

The device is powered by an external 12V AC/DC power adapter (supplied), connected to a standard alternating current (AC) electrical wall outlet.

Table 2-3: Power Specifications

Item	Description
Power Supply	Single universal external AC power supply
Input Ratings	100-240 VAC, 50-60 Hz
Output Ratings	12V/3A



Warning: Use only the AC/DC power adapter supplied with the device.

The device is shipped with the AC/DC power adapter shown the figure below which also supports interchangeable plugs to suite the electrical wall outlet type requirement of the country in which the device is being installed.

Figure 2-4: AC/DC Power Adapter

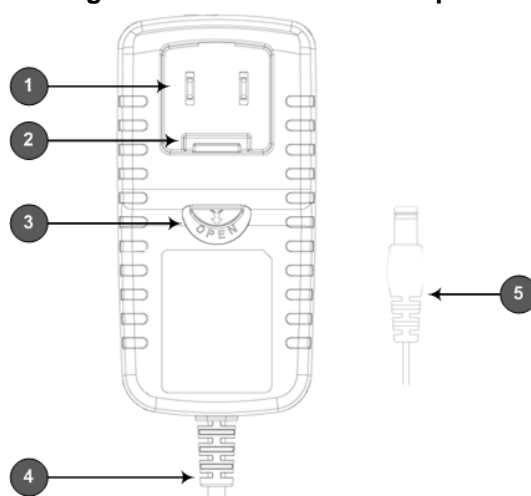


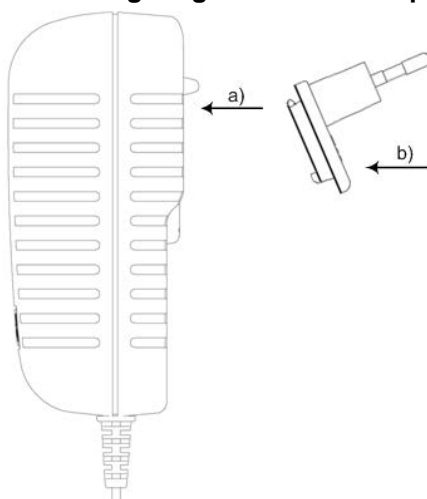
Table 2-4: Power Adapter with Interchangeable Plugs

Item	Description
1	Plug slot
2	Plug lock
3	Plug release lever
4	DC power cord
5	DC power plug

➤ **To connect the device to the power supply using the power adapter:**

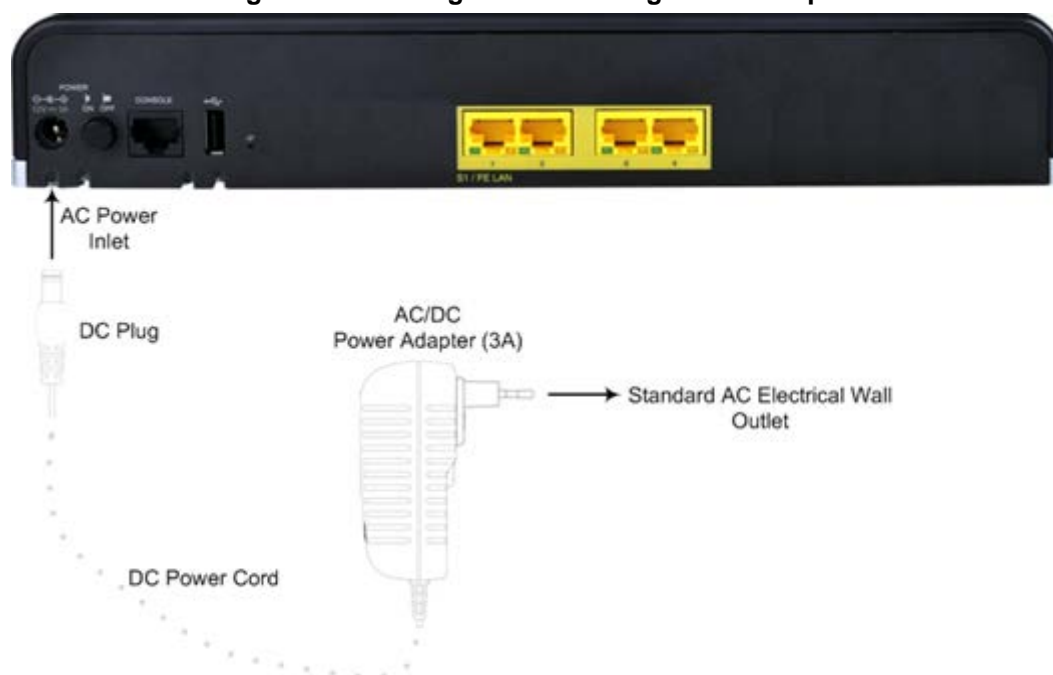
1. Insert the relevant AC plug into the housing power adapter:
 - a. Insert the top part of the plug into the upper part of the housing slot (1).
 - b. Press down on the bottom part of the plug until a click is heard, indicating that the plug is securely inserted in the housing slot. To remove the plug, push and slide down the OPEN plug release lever (3).

Figure 2-5: Inserting Plug into Power Adapter



2. Insert the DC plug (5) located at the end of the power cord (4) of the power adapter into the device's power socket located on the rear panel.

Figure 2-6: Cabling to Power using Power Adapter



3. Plug the power adapter directly into a standard electrical wall outlet.

2.1.4 Powering the Device On / Off

The power switch is located on its rear panel (see Section 2.1.2).

➤ To power on the device:

- Press in the power button; the device receives power and the **Power** LED on the front panel lights up.

➤ To power off the device:

- Press out the power button; the device powers off and the **Power** LED goes off.

2.2 Mediant 500 E-SBC

Figure 2-7: Front Panel - Ports



Table 2-5: Front Panel

Item #	Label	Description
1	POWER / STATUS	LEDs indicating the status of the power and reboot/initialization.
2	//	Reset pinhole button to reset and optionally to restore to factory defaults. To restore to factory defaults: Press and hold down the pinhole button for at least 12 seconds, but no longer than 25 seconds, with a paper clip or any other similar pointed object.
3	CONSOLE	RJ-45 port for RS-232 serial communication
4	LAN	Up to four Gigabit Ethernet (10/100/1000Base-T) ports to connect to LAN (IP phones, computers, or switches). These ports support half- and full-duplex modes, auto-negotiation, and straight or crossover cable detection.
6	USB	Two USB 2.0 ports. Do not use.

Figure 2-8: Rear Panel – Earth and Power

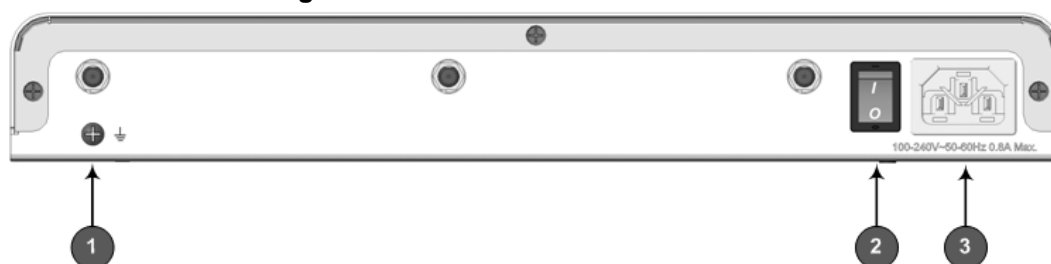



Table 2-6: Rear Panel

Item #	Label	Description
1		Protective earthing screw.
2	I / O	Power switch (O is off; I is on).
3	100-240V~50-60Hz 0.8A Max.	Three-prong AC power supply entry.

2.2.1 Cabling

2.2.1.1 Grounding the Device

The device must be connected to earth (grounded) using an equipment-earthing conductor.



Protective Earthing

The equipment is classified as Class I EN60950 and UL60950 and must be earthed at all times.

For Finland: Laite on liltettava suojamaadoituskoskettimilla varustettuun pistorasiaan.

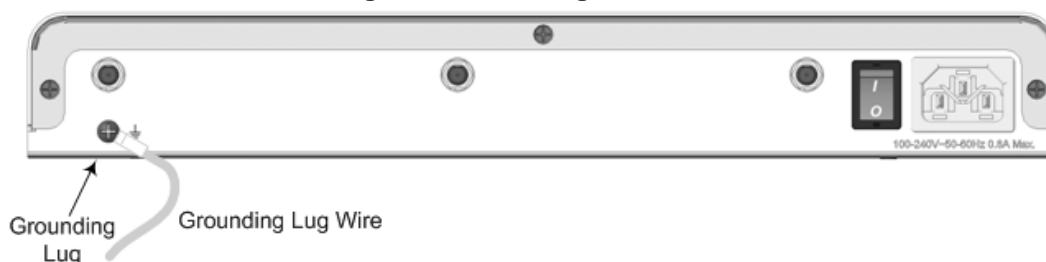
For Norway: Apparatet rna tilkoples jordet stikkontakt.

For Sweden: Apparaten skall anslutas till jordat uttag.

➤ To earth the device:

1. Connect an electrically earthed strap of 16 AWG wire (minimum) to the chassis' earthing screw (located on the rear panel), using the supplied washer.
2. Connect the other end of the strap to a protective earthing. This should be in accordance with the regulations enforced in the country of installation.

Figure 2-9: Earthing the Device



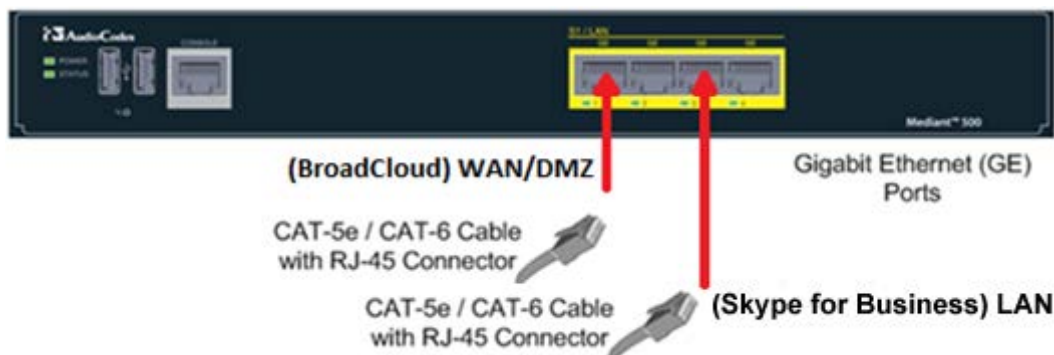
2.2.1.2 Connecting Ethernet Interfaces

Up to 4 Gigabit Ethernet (10/100/1000Base-T) ports supporting half- and full-duplex mode, auto-negotiation, and straight/crossover cable detection allow connection to LAN/WAN.

➤ To connect the device to the BroadCloud service (WAN-DMZ):

1. If the device's IP isn't configured yet, connect as shown in Section 3.
2. If the device's IP has already been configured:
 - a. Connect one end of a straight-through RJ-45 Cat 5e or Cat 6 cable to the RJ-45 port labeled S1 / LAN GE port 1.
 - b. Connect the other end to the DMZ port assigned by the IT administrator.

Figure 2-10: Cabling the Ethernet Ports



3. Connect the other end of the cable to the Gigabit Ethernet network.

➤ **To connect the device to Skype for Business (LAN):**

1. If the device's IP isn't configured yet, connect as shown in Section 3.
2. If the device's IP has already been configured:
 - a. Connect one end of a straight-through RJ-45 Cat 5e or Cat 6 cable to the RJ-45 port labeled S1 / LAN GE port 3.
 - b. Connect the other end to your local network LAN layer 2 switch port. This port is used to communicate with the local Skype for Business.

2.2.1.3 Connecting to the Power Supply

The device receives power from a standard alternating current (AC) electrical outlet. The connection is made using the supplied AC power cord.

Table 2-7: Power Specifications

Physical Specification	Value
Input Voltage	Single universal AC power supply 100 to 240V
AC Input Frequency	50 to 60 Hz
AC Input Current	0.8A

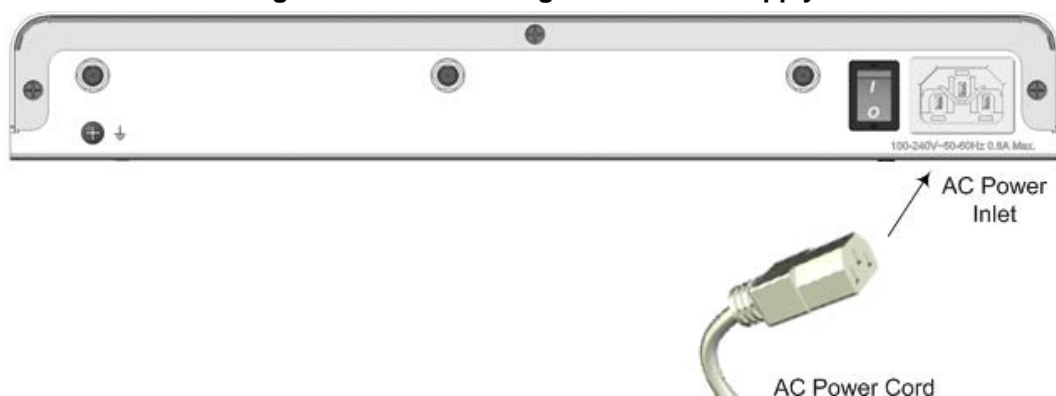


Warnings: The device must be connected to a socket-outlet providing a protective earthing connection. Use only the AC power cord that is supplied with the device.

➤ **To connect the device to the power supply:**

1. Connect the line socket of the AC power cord (supplied) to the device's AC power socket (labeled **100-240V~50-60 Hz 0.8A**), located on the rear panel.

Figure 2-11: Connecting to the Power Supply



2. Connect the plug at the other end of the AC power cord to a standard electrical outlet.
3. Press the power switch to on (I) position so that the device receives power; the **POWER** LED on the front panel is lit green.

2.3 Mediant 800B E-SBC

2.3.1 Front Panel

Figure 2-12: Front Panel

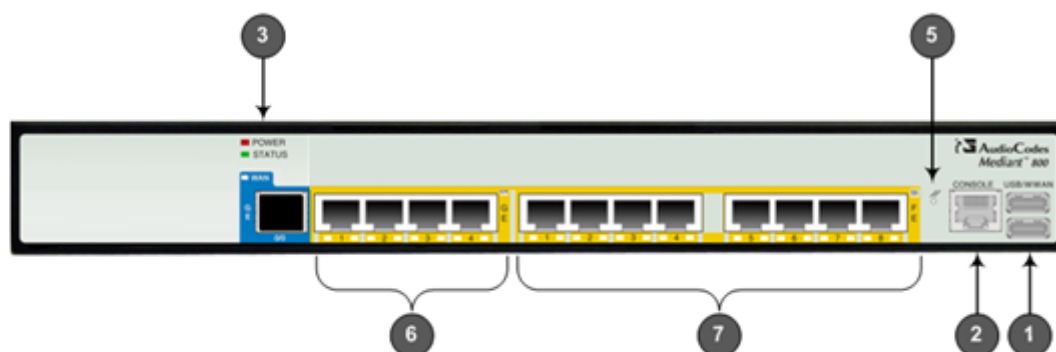


Table 2-8: Front Panel Description

Item #	Label	Description
1	USB/WWAN	N/A
2	RS-232	RS-232 port for serial communication. Cable not included.
3	POWER/STATUS	LEDs indicating power and reboot/initialization status. See also Section 2.3.2 on page 16.
5	-	Reset pinhole button to reset and optionally to restore factory defaults. To restore to factory defaults: Press and hold down the Reset pinhole button with a paper clip or similar pointed object, for at least 12 seconds but no more than 25 .
6	GE	Four 10/100/1000Base-T (Gigabit Ethernet) LAN/WAN ports.
7	FE	N/A

2.3.2 Front Panel LEDs

2.3.2.1 Operational Status LEDs

The **STATUS** LED indicates the operating status.

Table 2-9: STATUS LEDs


LED Color	LED State	Description
Green	On	The device is operational and in Standalone mode (not in High-Availability mode).
	Flashing	Initial rebooting stage.
	Slow Flash	HA mode - LED on Active device.
	Slow-Fast Flash	HA mode - LED on Redundant device.
Red	On	Boot failure.
	Off	Advanced rebooting stage.

2.3.3 Rear Panel

Figure 2-13: Rear Panel



Table 2-10: Rear Panel

Item #	Label	Description
1		Protective earthing screw.
2	100-240V~1.5A 50-60Hz	3-Prong AC power supply entry.

2.3.4 Cabling

2.3.4.1 Grounding the Device

The device must be connected to earth (grounded) using an equipment-earthing conductor.



Protective Earthing

The equipment is classified as Class I EN60950 and UL60950 and must be earthed at all times.

For Finland: Laite on liltettava suojamaadoituskoskettimilla varustettuun pistorasiaan.

For Norway: Apparatet rna tilkoples jordet stikkontakt.

For Sweden: Apparatens skall anslutas till jordat uttag.

➤ To ground the device:

1. Connect an electrically earthed strap of 16 AWG wire (minimum) to the chassis' grounding screw (located on the rear panel), using the supplied washer.

Figure 2-14: Grounding the Device



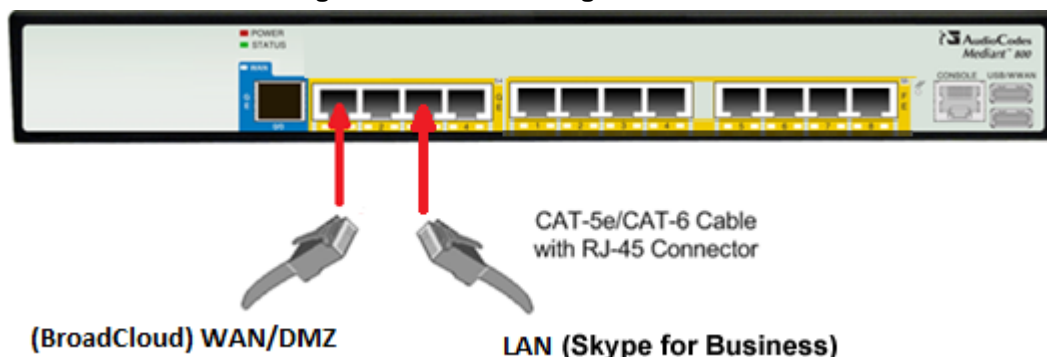
2. Connect the other end to a protective earthing (according local regulations).

2.3.4.2 Connecting to Ethernet

Up to four 10/100/1000Base-T (Gigabit Ethernet) RJ-45 ports supporting half- and full-duplex modes, auto-negotiation, and straight or crossover cable detection, allow connecting to the LAN/WAN.

- **To connect the device to the BroadCloud service (WAN-DMZ):**
 1. If the device's IP isn't configured yet, connect as shown in Section 3.
 2. If the device's IP has already been configured:
 - a. Connect one end of a straight-through RJ-45 Cat 5e or Cat 6 cable to the RJ-45 port labeled LAN GE port 1.
 - b. Connect the other end to the DMZ port assigned by the IT administrator.

Figure 2-15: Connecting the LAN Ports



- **To connect the device to Skype for Business (LAN):**
 1. If the device's IP isn't configured yet, connect as shown in Section 3.
 2. If the device's IP has already been configured:
 - a. Connect one end of a straight-through RJ-45 Cat 5e or Cat 6 cable to the RJ-45 port labeled LAN GE port 3.
 - b. Connect the other end to your local network LAN layer 2 switch port. This port is used to communicate with the local Skype for Business.

2.3.5 Powering up

The device receives power from a standard alternating current (AC) electrical outlet. The connection is made using the supplied AC power cord.

Table 2-11: Power Specifications

Physical Specification	Value
Input Voltage	Single universal AC power supply 100 to 240V
AC Input Frequency	50 to 60 Hz
AC Input Current	1.5A



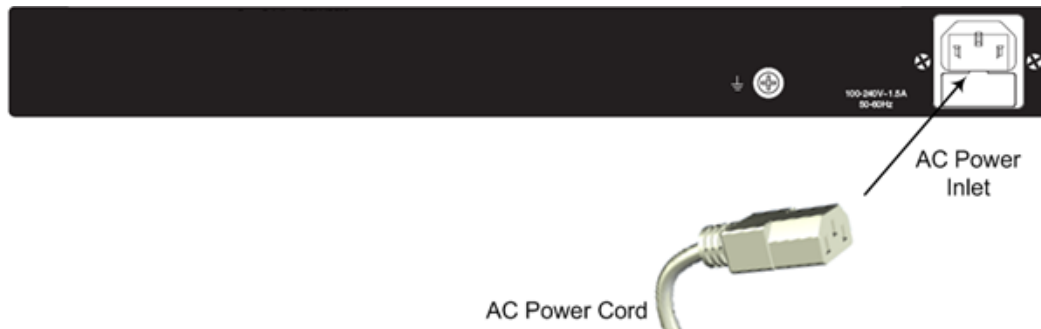
Warning:

- The device must be connected to a socket-outlet providing protective earthing.
- Use only the AC power cord that is supplied with the device.

➤ **To connect the device to the power supply:**

1. Connect the line socket of the AC power cord (supplied) to the device's AC power socket (labeled **100-240V 1.5A ~50-60 Hz**), located on the rear panel.

Figure 2-16: Connecting to the Power Supply



2. Connect the plug at the other end of the AC power cord to a standard electrical outlet. After cabling and powering up, the **POWER** LED on the front panel lights up green.

2.4 Mediant 2600 E-SBC

2.4.1 Front Panel

Figure 2-17: Front Panel – Port Interfaces

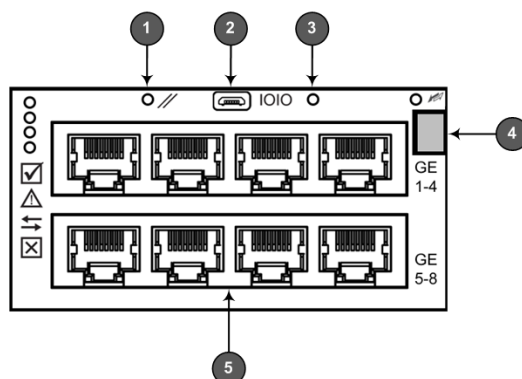



Table 2-12: Front Panel - Ports

Item #	Label	Description
1		Reset pinhole button: <ul style="list-style-type: none"> To reset the device, press it for at least 1 second but no longer than 10s. To reset to factory defaults, press for at least 12s but no longer than 25s.
2	IOIO	RS-232 port for serial communication with a computer.
3	-	Pinhole button (reserved for future use).
4	-	Handle of AMC module for installing and removing the module.
5	-	LAN sub-module, providing eight, 1000Base-T (Gigabit) Ethernet ports for connecting to the IP network. The Ethernet ports operate in pairs, where one port is active and the other standby, providing 1+1 Ethernet redundancy. These ports support half- and full-duplex modes, auto-negotiation, straight-through and crossover cable detection.

2.4.2 Rear Panel

Figure 2-18: Rear Panel

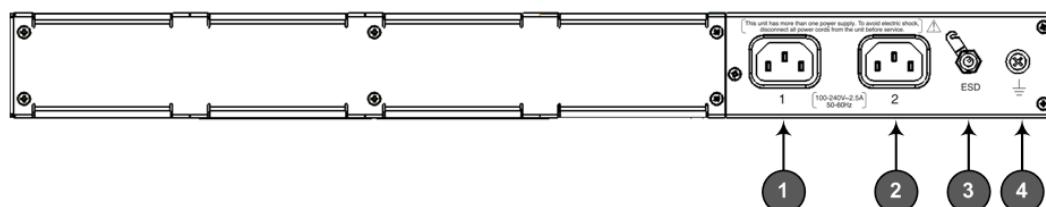



Table 2-13: Rear Panel Description

Item #	Label	Description
1	1	AC power supply inlet (100-240V~2.5A, 50-60 Hz) for power supply module No. 1.
2	2	AC power supply inlet (100-240V~2.5A, 50-60 Hz) for power supply module No. 2.
3	ESD	Electrostatic Discharge (ESD) socket.
4		Protective earthing screw.

2.4.3 Cabling

2.4.3.1 Grounding the Device

The device must be connected to earth (grounded) using an equipment-earthing conductor.



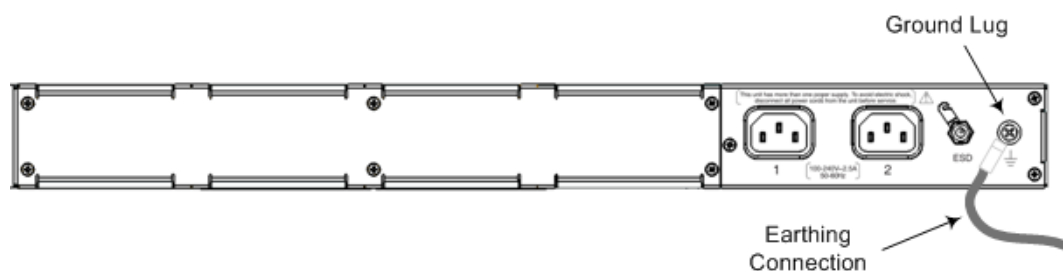
Protective Earthing

The equipment is classified as Class I according to EN-60950-1 and UL 60950-1 and must be earthed at all times (using an equipment-earthing conductor).

➤ To ground the device:

1. Connect an electrically earthed strap of 16 AWG wire (minimum) to the chassis' earthing screw (located on the rear panel), using the supplied washer.

Figure 2-19: Grounding the Device



2. Connect the other end of the strap to a protective earthing in accordance with the regulations enforced in the country in which the device is installed.

2.4.3.2 Connecting to Ethernet

➤ To connect the device to the BroadCloud service (WAN-DMZ):

1. If the device's IP isn't configured yet, connect as shown in Section 3. If the device's IP has already been configured:
 - a. Connect one end of a straight-through RJ-45 Cat 5e or Cat 6 cable to the RJ-45 port labeled LAN GE port 1.
 - b. Connect the other end to the DMZ port assigned by the IT administrator.

Figure 2-20: Connecting the LAN Ports



➤ To connect the device to the IP-PBX (LAN):

1. If the device's IP isn't configured yet, connect as shown in Section 3. If the device's IP has already been configured:
 - a. Connect one end of a straight-through RJ-45 Cat 5e or Cat 6 cable to the RJ-45 port labeled LAN GE port 3.
 - b. Connect the other end to your local network LAN layer 2 switch port. This port will be used to communicate with the local IP-PBX.

2.4.3.3 Connecting to the Power Supply

Table 2-14: Power Specifications

Item	Description
Power Supply	Up to two hot swappable, power supply modules for power load sharing and AC power redundancy in case of failure of one of the modules.
Input Ratings	Single universal power supply 100-240 VAC, 50-60 Hz, 2.5A max.
Output Ratings	12 VDC / 10 A max.
Connection to Electrical Outlet	AC power supply inlet.



Warning:

- The device must be connected (by service personnel) to a socket-outlet with a protective earthing connection.
- Use only the AC power cord supplied with the device.



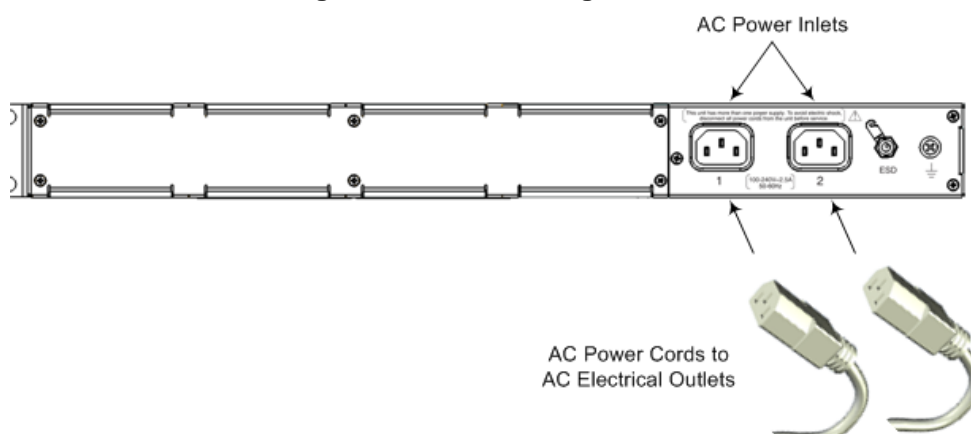
Note:

- You can connect PS modules (1 and 2) for 1+1 power load-sharing and redundancy. Each provides an AC power socket on the device's rear panel. If both are used, make sure you connect each one to a different AC supply socket.
- The two AC power sources must have the same ground potential.

➤ **To connect the device to the power supply:**

1. Connect the AC power cord (supplied) to one of the power sockets on the rear panel.

Figure 2-21: Connecting to Power



2. Connect the other end of the power cord to a standard AC electrical outlet (100-240V~50-60 Hz).
3. For load sharing and power redundancy, repeat steps 1 -2, but using the power socket of the second PS module and connecting this to a different supply circuit.
4. Turn on the power at the power source (if required).
5. Check that the **POWER** LED on each PS module (front panel) is lit green. This indicates that the device is receiving power.

3 Connecting to the Management Interface

This section shows how to connect to the device's management interface for the first time.

3.1 Default OAMP IP Address

The device is shipped with a factory default IP address for operations, administration, maintenance, and provisioning (OAMP), through its network interface. Use this address to initially access the device's embedded Web server. Default IP address is:

Table 3-1: Default VoIP LAN IP Address for OAMP

IP Address	Value
IP Address	192.168.0.2
Prefix Length	255.255.255.0 (24)
Default Gateway	192.168.0.1

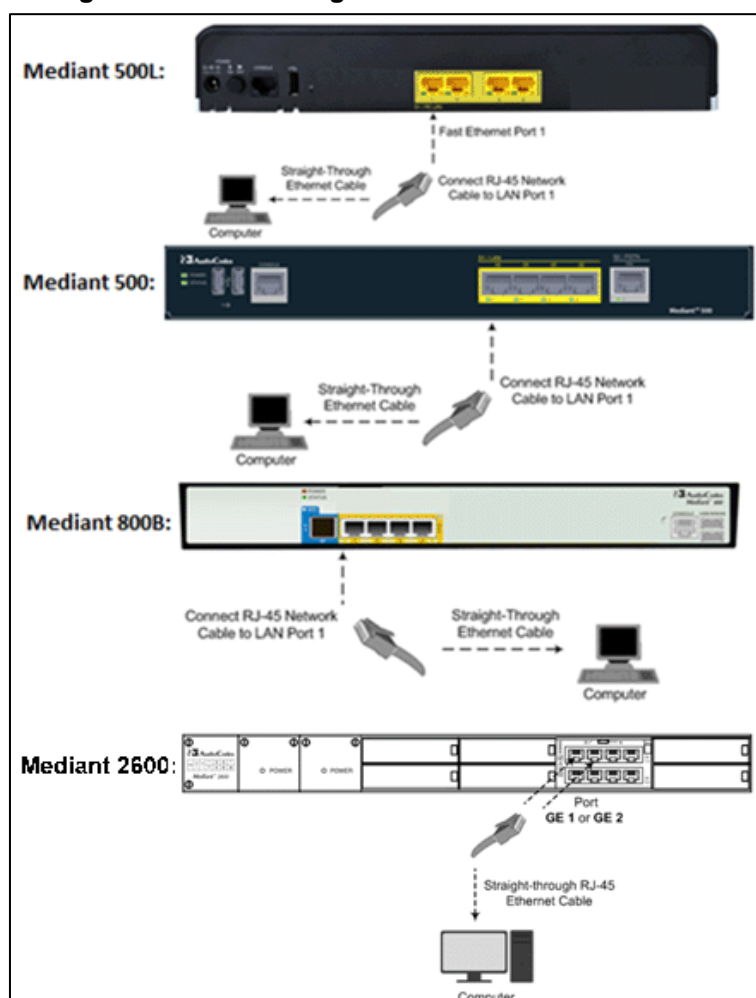
3.2 Connecting to the Embedded Web Server

This section shows how to connect to the embedded Web server.

➤ **To connect to the embedded Web server:**

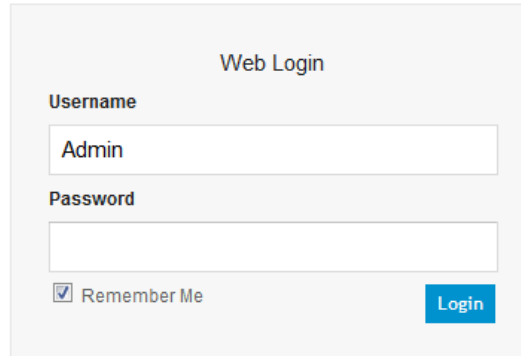
1. Connect Port 1 (leftmost LAN port) located on the front panel directly to the network interface of your computer, using a straight-through Ethernet cable.

Figure 3-1: Connecting to the Embedded Web Server



2. Change the IP address and subnet mask of your computer to correspond with the default OAMP IP address and subnet mask of the device.
3. Access the Web interface:
 - a. On your computer, start a Web browser and in the URL address field, enter the default IP address of the device; the Web interface's Web Login screen appears:

Figure 3-2: Web Login Screen

The image shows a web login interface with a light gray background. At the top center, the text "Web Login" is displayed. Below this, there are two input fields. The first is labeled "Username" and contains the text "Admin". The second is labeled "Password" and is empty. Below the password field, there is a checkbox labeled "Remember Me" which is checked. To the right of the checkbox is a blue button with the text "Login" in white.

- b. In the 'Username' and 'Password' fields, enter the case-sensitive, default login username (**Admin**) and password (**Admin**).
 - c. Click **Login**.

4 Configuring the Device

4.1 Step 1: Download, Install BroadCloud Certified Firmware / Configuration

This section shows how to download the certified BroadCloud firmware and configuration.

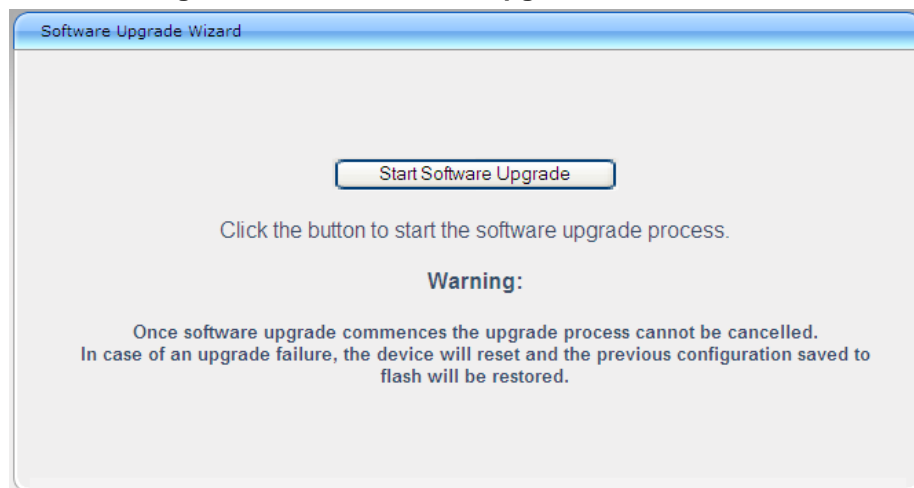
➤ **To download the certified BroadCloud firmware and configuration:**

1. Open a web browser, go to <http://www.audiocodes.com/broadcloud-resource-center>
2. Download the zip file associated with your device, unzip the package, and save the enclosed configuration_XXXX.ini file and firmware_XXX.cmp file to your local drive.
3. Download the Call Progress Tones file suitable for your country – call_progress_XXXXX.dat ('XXXXX' being the country name).
4. Enter the device's Software Upgrade Wizard.

➤ **To load files using the Software Upgrade Wizard:**

1. Open the Software Upgrade Wizard by performing one of the following:
 - Select the **Maintenance** tab, click the **Software Update** menu, and then click **Software Upgrade Wizard**.
 - On the toolbar, click **Device Actions**, and then choose **Software Upgrade Wizard**.

Figure 4-1: Start Software Upgrade Wizard Screen




2. Click **Start Software Upgrade**; the Wizard starts, prompting you to load a .cmp file:

3. Click **Start Software Upgrade**; the Wizard starts, prompting you to load a .cmp file:

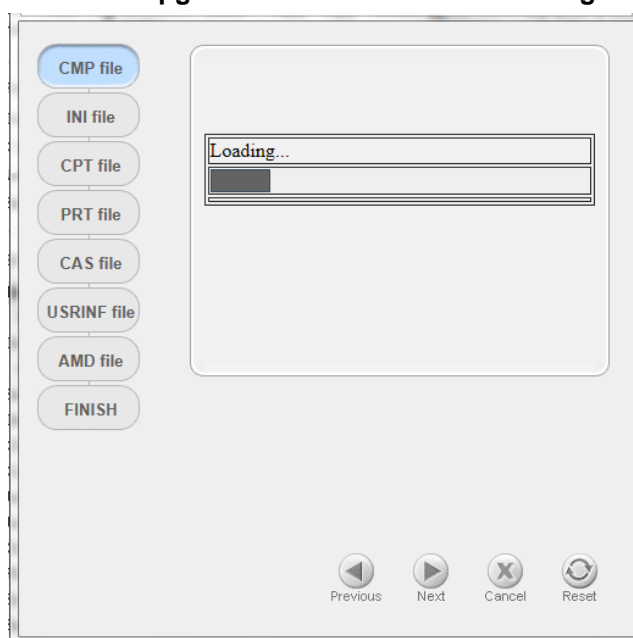
Figure 4-2: Software Upgrade Wizard - Load CMP File



Note: At this stage, you can quit the Software Upgrade Wizard without having to reset the device, by clicking **Cancel** . However, if you *continue* with the Wizard and start loading the cmp file, the upgrade process must be completed with a device reset.

4. Click **Browse**, and then navigate to where the .cmp file is located on your computer. Select the file, and then click **Open**.
5. Click **Load File**; the device begins to install the .cmp file. A progress bar displays the status of the loading process and a message informs you when file load successfully completes.

Figure 4-3: Software Upgrade Wizard – CMP File Loading Progress Bar




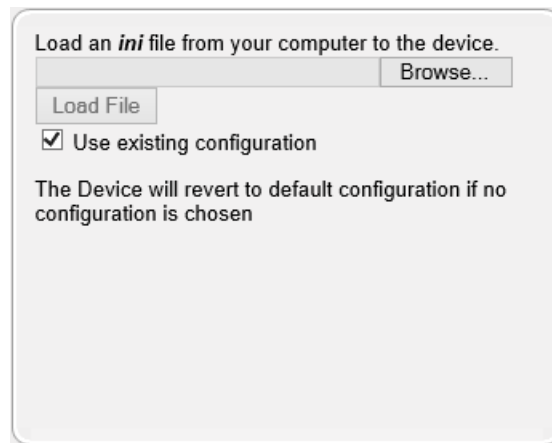
6. Select the upgrade option **System Reset Upgrade**
7. Press the **Next**  button to navigate through the Wizard.
8. In the Wizard's page for loading an ini file:
 - **Deselect** the 'Use existing configuration' option
 - **Load a new ini file:** In the 'Load an ini file...' field, click **Browse**, and then navigate to where the ini file is located on your computer. Select the file, and then click **Load File**; the device loads the ini file.

Figure 4-4: Software Upgrade Wizard – Load INI File




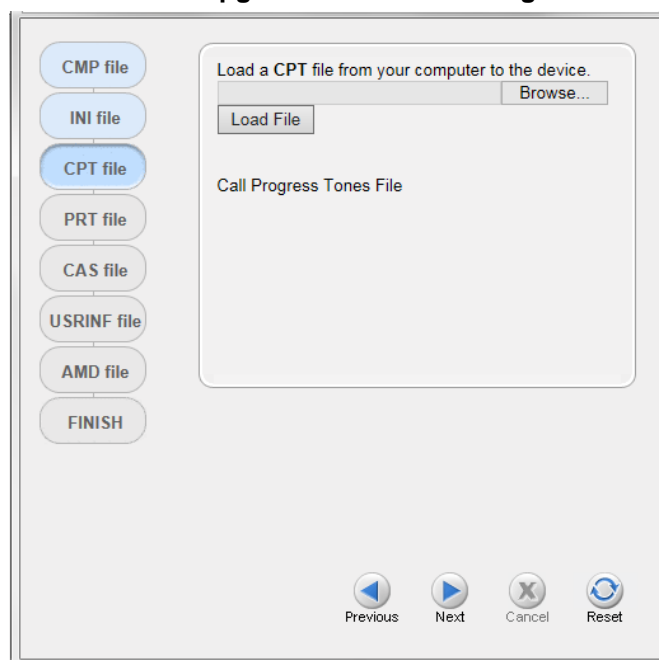
9. Press the **Next**  button to navigate to the Call Progress Tones (CPT) Wizard page.
10. In the Wizard's page for loading the Call Progress Tones (CPT) file, click **Browse**, and then navigate to where the call_progress_XXXXX.dat ('XXXXX' being the country name) file is located on your computer. Select it and click **Load File**; the device loads the tones file.

Figure 4-5: Software Upgrade Wizard – Loading the CPT File




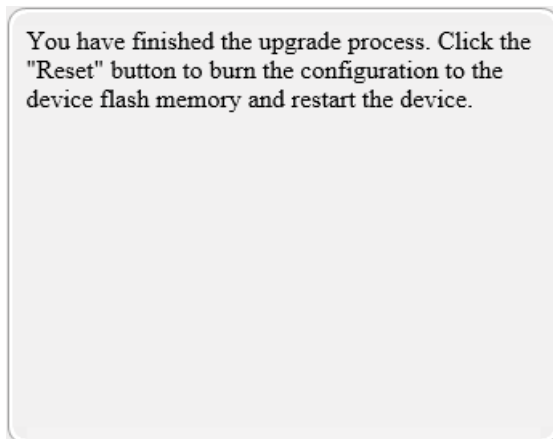

11. Click **Next**  until the last Wizard page appears (the **FINISH** button is highlighted in the left pane):

Figure 4-6: Software Upgrade Wizard – Files Loaded



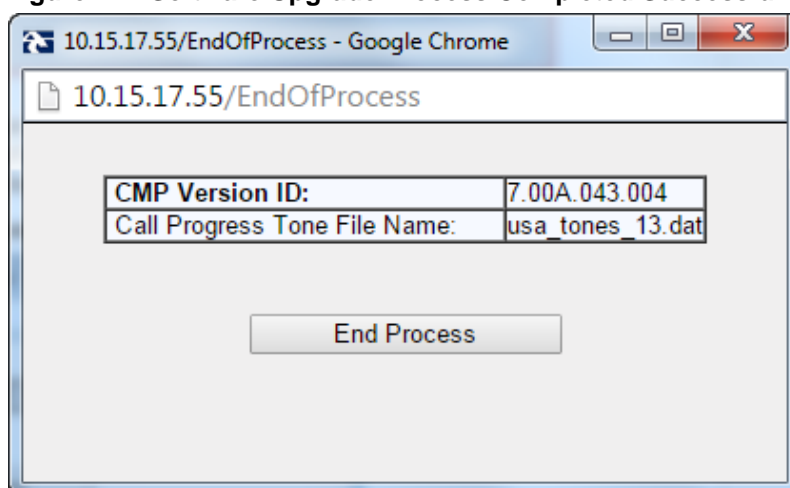
12. Click **Reset**  to burn the files to the device's flash memory; the 'Burn and reset in progress' message is displayed and the device 'burns' the newly loaded files to flash memory and then resets.



Note: The device's reset may take a few minutes (even up to 30 minutes) depending on the .cmp file version.

When the device finishes the installation process and resets, the following Wizard page is displayed, showing the installed software version and other files (ini file and auxiliary files) that you may also have installed:

Figure 4-7: Software Upgrade Process Completed Successfully

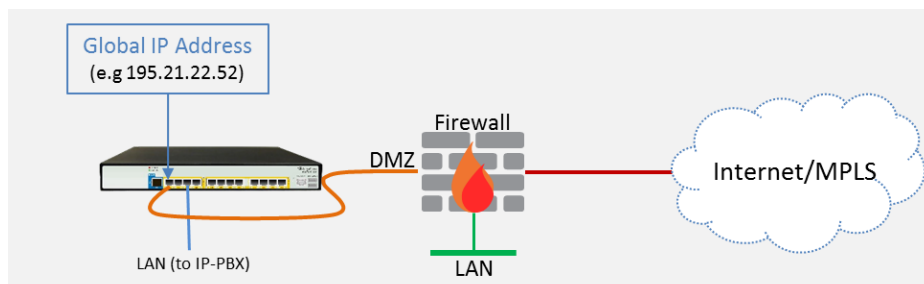


13. Click **End Process** to close the Wizard; the Web Login dialog appears.
14. Enter your login username and password (**Admin, Admin** respectively), and then click **Login**; a message box appears informing you of the new .cmp file version.
15. Click **OK**; the Web interface becomes active, reflecting the upgraded device.

4.2 Step 2: Configure a Network Interface for the Device

This section describes typical physical Ethernet port connections of the deployed device. There are two methods to connect the device to the DMZ:

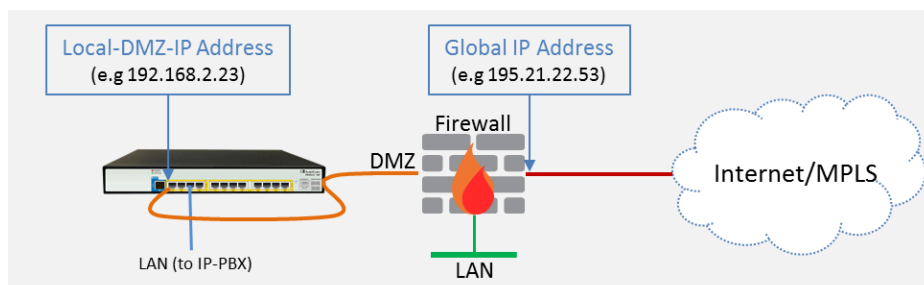
- Method A:** [Preferred method] With a 'Global IP Address' provided to the gateway device, without a NAT. The firewall is configured with the following rules (for example):



- FW allow rule:

Original			
	Source	Destination	Ports/Service
1	<any> (e.g. ITSP)	Global IP Address (public address)	SIP service: 5060 / UDP RTP service: 6000-8500 / UDP

- Method B:** With a 'local-DMZ-IP Address' behind a NAT. The firewall is configured with the following rules (for example):



- Firewall allow rule:

Original				Translated		
	Source	Destination	Ports/Service	Source	Destination	Ports/Service
1	<any> (e.g. ITSP)	Global IP Address (public address)	SIP service: 5060 / UDP RTP service: 6000-8500 / UDP	<any> (e.g. ITSP)	Local-DMZ-IP-Address	<as original>

- NAT rules (port forwarding):

	Source	Destination	Ports/Service	Source	Destination	Ports/Service
1	<any> (e.g. ITSP)	Global IP Address (public address)	SIP service: 5060 / UDP RTP service: 6000-8500 / UDP	<any> (e.g. ITSP)	Local-DMZ-IP-Address	<as original>
1	Local-DMZ-IP-Address	<any> (e.g. ITSP)	SIP service: 5060 / UDP RTP service: 6000-8500 / UDP	Global IP Address (public address)	<any> (e.g. ITSP)	<as original>

4.2.1 Step 2a: Configure Network Interfaces

This step describes how to configure the IP network interfaces for each of the following interfaces:

➤ **To configure the DMZ/WAN (BroadCloud SIP-Trunk) Interface:**

1. Open the IP Interfaces Table page (**Configuration** tab > **VoIP** menu > **Network** > **IP Interfaces Table**).
2. Modify the existing **WAN** ('WANSP') network interface (which will be available on eth port #1):
 - a. Select the 'Index 0' radio button of the **OAMP + Media + Control** table row, and then click **Edit**.
 - b. Configure the interface as follows:

Parameter	Value
Application Type	OAMP + Media + Control (leave as is)
IP Address	If working in <u>Method A</u> : Global-IP-Address (public address) If working in <u>Method B</u> : Local-DMZ-IP-Address
Prefix Length	Subnet mask in bits, e.g.28 (for 255.255.255.240)
Default Gateway	The default gateway IP address (In Method B: router's IP address)
Interface Name	WANSP (arbitrary descriptive name, you may change it)
Primary DNS Server IP Address	Primary DNS IP address
Secondary DNS Server IP Address	Secondary DNS IP address (optional)
Underlying Device	vlan 1

➤ **To configure the LAN (Skype for Business via local LAN-Switch) Interface:**

1. Modify the existing **LAN** ('Voice') interface (which will be available on eth port #3):
 - a. Select the 'Index 1' radio button of the **Media + Control** table row, and then click **Edit**.
 - b. Configure the interface as follows:

Parameter	Value
Application Type	Media + Control
IP Address	Assign a Local LAN IP address for the SBC to use to communicate with Skype for Business
Prefix Length	Subnet mask in bits, e.g.24 (subnet mask in bits for 255.255.255.0)
Default Gateway	The local LAN default gateway IP address
Interface Name	Voice (arbitrary descriptive name, you may change it) Use this interface for Skype for Business connectivity
Primary DNS Server IP Address	Primary DNS IP address
Secondary DNS Server IP Address	Secondary DNS IP address (optional)
Underlying Device	vlan 2

2. Click **Apply**, and then **Done**.

An example of configured IP network interfaces is shown below:

Figure 4-8: Configured Network Interfaces in IP Interfaces Table

Index	Interface Name	Application Type	Interface Mode	IP Address	Prefix Length	Default Gateway	Primary DNS	Secondary DNS	Underlying Device
0	WANSP	OAMP + Media + C	IPv4 Manual	195.189.192.139	25	195.189.192.129	80.179.52.100	80.179.55.100	vlan 1
1	Voice	Media + Control	IPv4 Manual	10.15.17.77	16	10.15.0.1	10.15.25.1	0.0.0.0	vlan 2

4.2.2 Step 2b: Configure NAT

Only applies if connecting according to [Method B](#) (described [above](#)).



Note: Configure this setting only if you are behind a firewall NAT.



Note: The 'NAT IP Address' is the Global-IP-address used in front of the firewall facing the BroadCloud service. If the DMZ holds the global-IP-address (no NAT is performed by the firewall) and the E-SBC is already assigned with the Global-IP-address as its address, skip this NAT configuration.

➤ To configure the Global address

1. Open the NAT Translation table (**Configuration** tab > **VoIP** menu > **VoIP Network** > **NAT Translation Table**).
2. Click **Add**; the following dialog appears:

Figure 4-9: NAT Translation Table - Add Row Dialog Box

Add Row [X]

Index:

Source Interface:

Target IP Address:

Source Start Port:

Source End Port:

Target Start Port:

Target End Port:

3. Use the table below as reference when configuring a NAT translation rule in the 'Add Row' dialog.

Table 4-1: NAT Translation Table Parameter Descriptions

Parameter	Description
Index	0
Source Interface	WANSP (the interface to apply this rule to)
Target IP Address	Global-IP-address. Defines the global (public) IP address.
Source Start Port	(Leave empty)
Source End Port	(Leave empty)
Target Start Port	(Leave empty)
Target End Port	(Leave empty)

4. Click **Add**.

4.3 Step 3: Configure the UDP Ports for RTP between the SBC and Skype for Business



Note: The default UDP port range is 6000 and up to 8499 (maximum UDP depends on the maximum capacity of the specific SBC license provided). You may skip this step if necessary.

➤ **To configure Media Realms:**

1. Open the Media Realm Table page (**Configuration** tab > **VoIP** menu > **VoIP Network** > **Media Realm Table**).
2. Edit the Media Realm for the LAN ('Voice') interface. For example:

Parameter	Value
Index	0
Media Realm Name	MRLan (descriptive name)
IPv4 Interface Name	Voice
Port Range Start	6000 (as required by the Skype for Business environment)
Number of Media Session Legs	250 (media sessions assigned with port range)

Figure 4-10: Configuring Media Realm for LAN

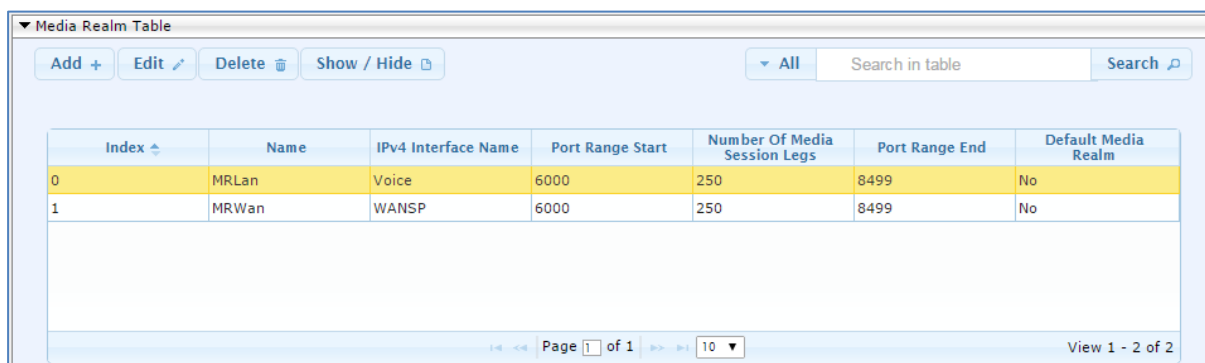
Edit Row

Index	0
Name	MRLan
IPv4 Interface Name	Voice
Port Range Start	6000
Number Of Media Session Legs	250
Port Range End	8499
Default Media Realm	No
QoS Profile	None
BW Profile	None

Save Cancel

The configured Media Realms are shown in the figure below:

Figure 4-11: Configured Media Realms in Media Realm Table



Index	Name	IPv4 Interface Name	Port Range Start	Number Of Media Session Legs	Port Range End	Default Media Realm
0	MRLan	Voice	6000	250	8499	No
1	MRWan	WANSP	6000	250	8499	No

4.4 Step 4: Configure the Skype for Business Address

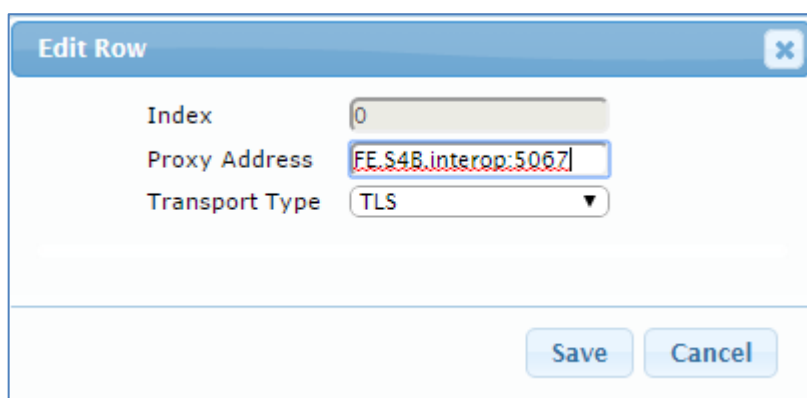
This section shows how to configure the Skype for Business address.

➤ To configure the Skype for Business address:

1. Open the Proxy Sets Table page (**Configuration** tab > **VoIP** menu > **VoIP Network** > **Proxy Sets Table**).
2. Edit the Proxy Set for Skype for Business (you can identify it by the 'Proxy Name' field)
3. Configure a Proxy Address Table for Proxy Set for Skype for Business:
 - Go to **Configuration** tab > **VoIP** menu > **VoIP Network** > **Proxy Sets Table** > **Proxy Address Table**.

Parameter	Value
Index	0
Proxy Address	Skype for Business Server 2015 IP address / FQDN and destination port e.g., FE.S4B.interop:5067
Transport Type	Network transport type (Select TLS or TCP according to what is configured on your Skype for Business), e.g., TLS (most commonly used)

Figure 4-12: Configuring Proxy Address for Skype for Business



Edit Row

Index: 0

Proxy Address: FE.S4B.interop:5067

Transport Type: TLS

Save Cancel

4.5 Step 5: Configure a SIP TLS Connection

This section shows how to configure the E-SBC to use a TLS connection with the Skype for Business Server 2015 Mediation Server, essential for a secure SIP TLS connection.



Note: If your Skype for Business is configured to operate with TCP, skip Step 5 and continue with Step 6.

4.5.1 Step 5a: Configure the NTP Server Address

This step shows how to configure the NTP server's IP address. Operating with TLS requires validating certificates. To validate certificates correctly, the device requires the date and the time from the NTP server.

➤ **To configure the NTP server address:**

1. Open the Application Settings page (**Configuration** tab > **System** > **Time And Date**).
2. In the 'Primary NTP Server Address' field, enter the IP address of the NTP server (e.g., **10.15.27.1**).

Figure 4-13: Configuring NTP Server

▼ NTP Server		
Primary NTP Server Address (IP or FQDN)	<input type="text" value="10.15.27.1"/>	
Secondary NTP Server Address (IP or FQDN)	<input type="text"/>	
NTP Update Interval	Hours: <input type="text" value="24"/>	Minutes: <input type="text" value="0"/>

3. Click **Submit**.

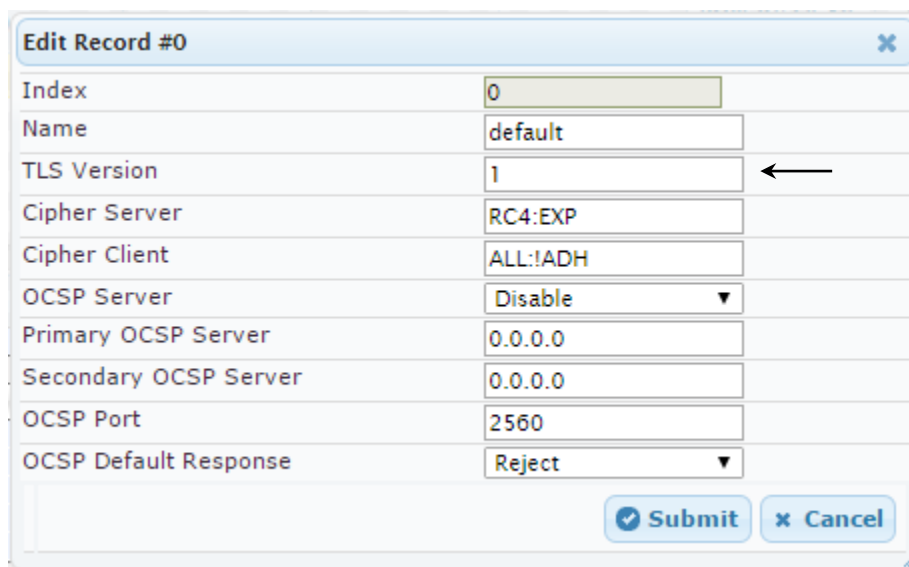
4.5.2 Step 5b: Configure TLS Version 1.0

This step shows how to configure the E-SBC to exclusively use TLS version 1.0.

➤ **To configure TLS version 1.0:**

1. Open the TLS Contexts page (**Configuration** tab > **System** menu > **TLS Contexts**).
2. In the TLS Contexts table, select index row 0 and click the **Edit** button.
3. In the 'TLS Version' field, enter **1** as shown in the figure below.

Figure 4-14: Configuring TLS Version 1.0



Edit Record #0	
Index	0
Name	default
TLS Version	1
Cipher Server	RC4:EXP
Cipher Client	ALL:!ADH
OCSF Server	Disable
Primary OCSF Server	0.0.0.0
Secondary OCSF Server	0.0.0.0
OCSF Port	2560
OCSF Default Response	Reject
<input type="button" value="Submit"/> <input type="button" value="Cancel"/>	

4. Click **Submit**.

4.5.3 Step 5c: Configure a Certificate

This step shows how to exchange a certificate with Microsoft Certificate Authority (CA). The certificate is used by the E-SBC to authenticate the connection with Skype for Business Server 2015.

The procedure involves the following main steps:

- a. Generating a Certificate Signing Request (CSR).
- b. Requesting Device Certificate from CA.
- c. Obtaining Trusted Root Certificate from CA.
- d. Deploying Device and Trusted Root Certificates on E-SBC.



Note: The 'Subject Name [CN]' field should be configured identically in the DNS Active Directory and Topology Builder.

➤ **To configure a certificate:**


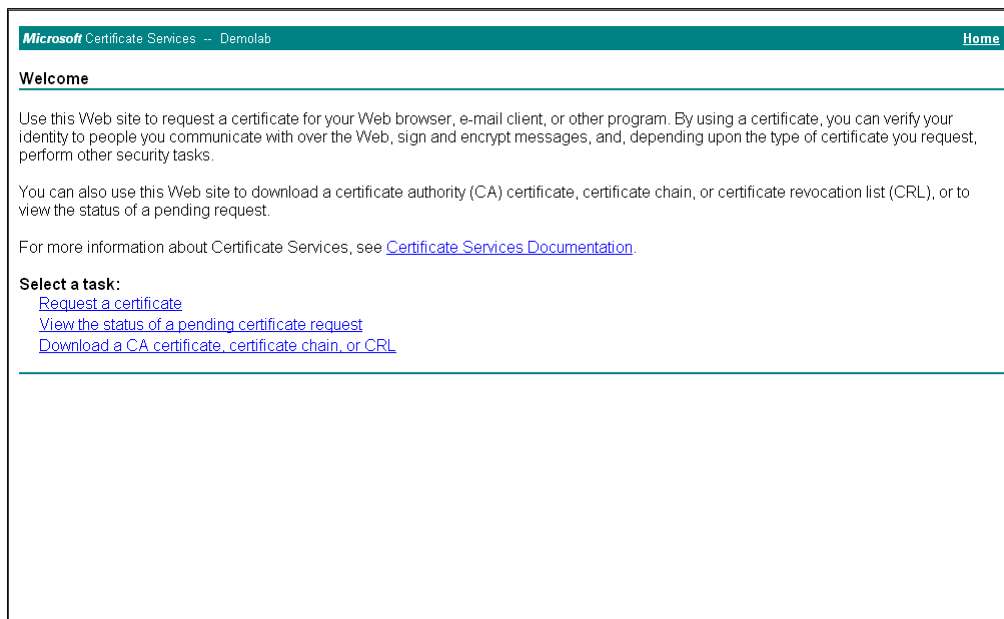
1. Open the TLS Contexts page (**Configuration** tab > **System** menu > **TLS Contexts**).
2. In the TLS Contexts table, select index row 0 and then click the **TLS Context Certificates**  button located at the bottom of the TLS Contexts page; the Context Certificates page appears.
3. Under the **Certificate Signing Request** group, do the following:
 - a. In the 'Subject Name [CN]' field, enter the E-SBC FQDN name (e.g., **ITSP.S4B.interop**).
 - b. Fill in the rest of the request fields according to your security provider's instructions.
4. Click the **Create CSR** button; a textual certificate signing request is displayed in the area below the button:

Figure 4-15: Certificate Signing Request – Creating CSR

Certificate Signing Request	
Subject Name [CN]	ITSP.S4B.interop
Organizational Unit [OU] (optional)	
Company name [O] (optional)	
Locality or city name [L] (optional)	
State [ST] (optional)	
Country code [C] (optional)	
<div style="border: 1px solid #ccc; display: inline-block; padding: 5px 15px; background-color: #f0f0f0;">Create CSR</div>	
<p>After creating the CSR, copy the text below (including the BEGIN/END lines) and send it to your Certification Authority for signing.</p> <pre style="font-family: monospace; font-size: 0.9em;"> -----BEGIN CERTIFICATE REQUEST----- MIIBWjCBxAIBADAbMRkwFwYDVQQDDBBjVFNQLlM0Q15pbmRlcm9wMIGfMA0GCSqG SIb3DQEBAQUAA4GNADCBiQKBgQCzEs8XTnY8be/t77eEDG7rTg747GQ3ODfOC4Rs x+e9KfberZgxMYqGT8u04AU0wU9LUPkq+8gI6w2bg3bow0kg/9hrnNL2rflTGcn 30oShPOSPiKMRNznCC090b03tbr9kuHm1wPRQ7yT6k7xS3XBbSigqT4LQbjBT1tt hDH3bQIDAQABoAAwDQYJKoZIhvcNAQEFBQADgYEAim/GA2ElzQbZaR6CZyIawilt u65w450NFHmaC1uHsyZ8keM8d1Ux14hkw7t5ygAD8KbxVkhRvACgcQrAK2v8u1Pf TVN+bwJ+kQ0d59CixA82e0o1WB3buPq5+qWdGTF+MyJWGVf8Sic1c6+zFoc+BEZY 7tQ8y0J8od0aDhStDfQ= -----END CERTIFICATE REQUEST----- </pre>	

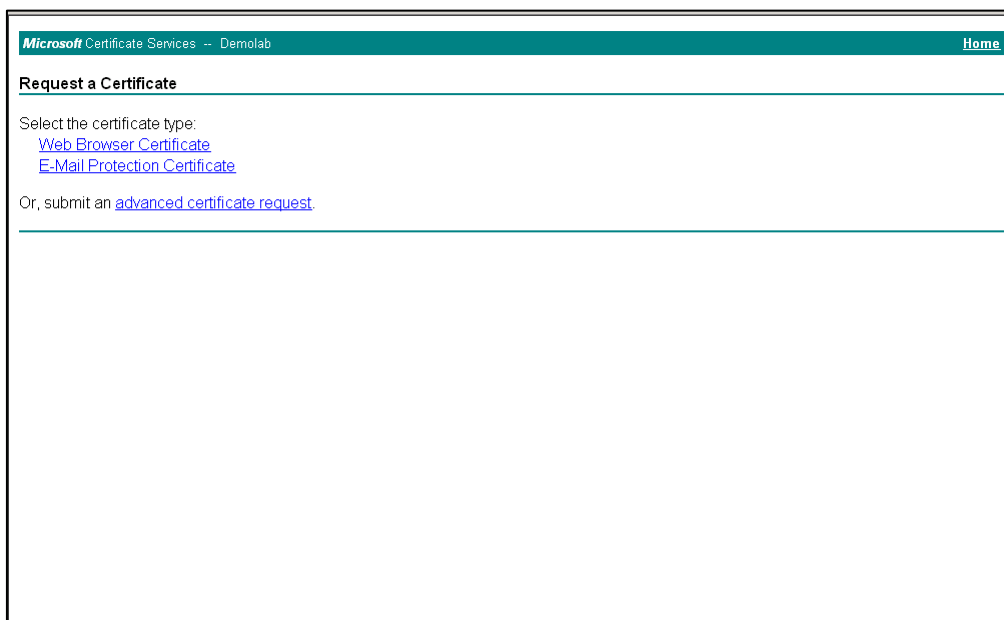
5. Copy the CSR, from the line "----BEGIN CERTIFICATE" to "END CERTIFICATE REQUEST----" inclusively, to a text file (such as Notepad), and then save it to a folder on your computer with the file name *certreq.txt*.
6. Open a Web browser and navigate to the Microsoft Certificate Services website at <http://<certificate server>/CertSrv>.

Figure 4-16: Microsoft Certificate Services Web Page



7. Click the link **Request a certificate**.

Figure 4-17: Request a Certificate Page



8. Click **advanced certificate request**, and then click **Next**.

Figure 4-18: Advanced Certificate Request Page

9. Click **Submit a certificate request...** and then click **Next**.

Figure 4-19: Submit a Certificate Request or Renewal Request Page


10. Open the *certreq.txt* file that you created and saved in Step 5, and then copy its contents to the 'Saved Request' field.
11. From the 'Certificate Template' dropdown, select **Web Server**.
12. Click **Submit**.

Figure 4-20: Certificate Issued Page

Certificate Issued

The certificate you requested was issued to you.

☐ DER encoded or ☒ Base 64 encoded


[Download certificate](#)
[Download certificate chain](#)

13. Select the **Base 64 encoded** option for encoding, and then click **Download certificate**.
14. Save the file as *gateway.cer* to a folder on your computer.
15. Click the **Home** button or navigate to the certificate server at <http://<Certificate Server>/CertSrv>.
16. Click **Download a CA certificate, certificate chain, or CRL**.

Figure 4-21: Download a CA Certificate, Certificate Chain, or CRL Page

Microsoft Certificate Services -- Demolab
Home

Download a CA Certificate, Certificate Chain, or CRL

To trust certificates issued from this certification authority, [install this CA certificate chain](#).

To download a CA certificate, certificate chain, or CRL, select the certificate and encoding method.

CA certificate:

Current [Demolab]

Encoding method:

☒ DER
☐ Base 64

[Download CA certificate](#)
[Download CA certificate chain](#)
[Download latest base CRL](#)

17. Under the 'Encoding method' group, select the **Base 64** option for encoding.
18. Click **Download CA certificate**.
19. Save the file as *certroot.cer* to a folder on your computer.


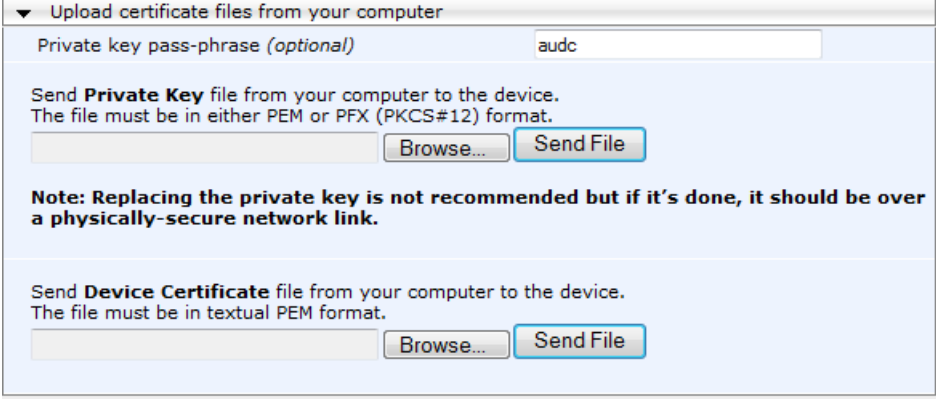
20. In the E-SBC's Web interface, return to the **TLS Contexts** page and do the following:
 - a. In the TLS Contexts table, select index row 0 and click the **TLS Context Certificates**  button located at the bottom of the TLS Contexts page; the Context Certificates page appears.
 - b. Scroll down to the **Upload certificates files from your computer** group, click the **Browse** button corresponding to the 'Send Device Certificate...' field, navigate to the *gateway.cer* certificate file that you saved on your computer in Step 14, and then click **Send File** to upload the certificate to the E-SBC.

Figure 4-22: Upload Device Certificate Files from your Computer Group



▼ Upload certificate files from your computer

Private key pass-phrase (optional)

Send **Private Key** file from your computer to the device.
The file must be in either PEM or PFX (PKCS#12) format.

Note: Replacing the private key is not recommended but if it's done, it should be over a physically-secure network link.

Send **Device Certificate** file from your computer to the device.
The file must be in textual PEM format.


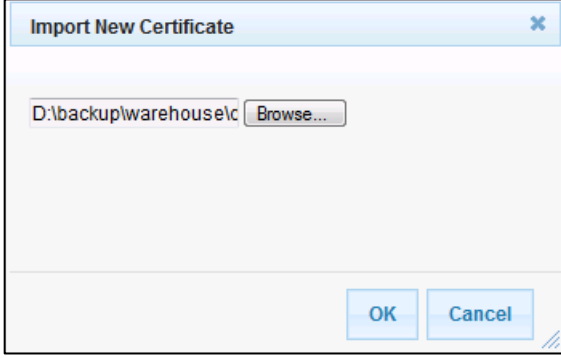
- c. In the E-SBC's Web interface, return to the **TLS Contexts** page.
- d. In the TLS Contexts table, select the required TLS Context index row, and then click the **TLS Context Trusted-Roots Certificates**  button, located at the bottom of the TLS Contexts page; the Trusted Certificates page appears.
- e. Click the **Import** button, and then select the certificate file to load.

Figure 4-23: Importing Root Certificate into Trusted Certificates Store



Import New Certificate

D:\backup\warehouse\c

21. Click **OK**; the certificate is loaded to the device and listed in the Trusted Certificates store.

4.6 Step 6: Configure SIP Host Name for Skype for Business

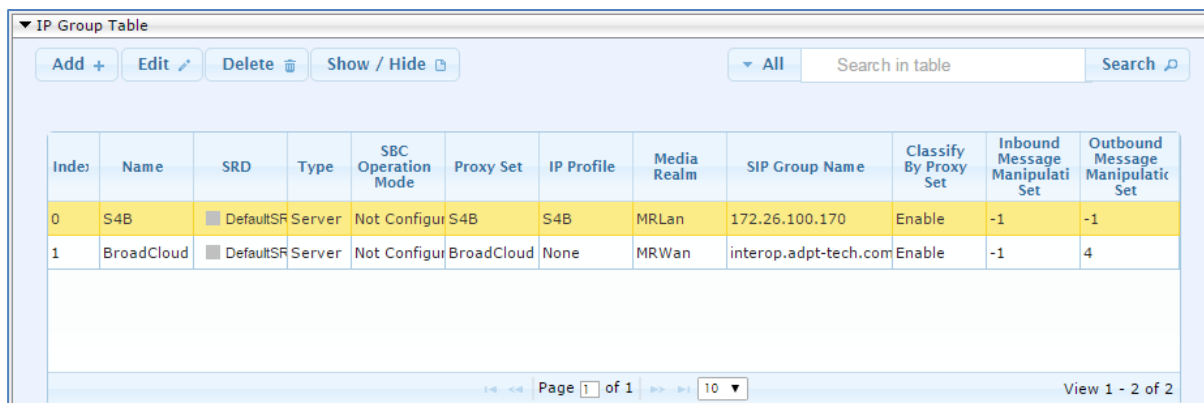
This section shows how to configure the SIP Host Name used in INVITE and REGISTER messages sent to Skype for Business. This is dependent on Skype for Business.

➤ To configure a SIP host name for Skype for Business:

1. Open the IP Group Table page (**Configuration** tab > **VoIP** menu > **VoIP Network** > **IP Group Table**).
2. Edit the SIP Host Name in the 'SIP Group Name' field, with the value required by the Skype for Business environment.

Parameter	Value
Index	0
Name	S4B
Type	Server
Proxy Set	S4B
IP Profile	S4B
Media Realm	MRLan
SIP Group Name	172.26.100.170 (according to the Skype for Business environment)

Figure 4-24: Configured IP Groups in IP Group Table



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
0	S4B	<input checked="" type="checkbox"/> DefaultSR	Server	Not Configured	S4B	S4B	MRLan	172.26.100.170	Enable	-1	-1
1	BroadCloud	<input checked="" type="checkbox"/> DefaultSR	Server	Not Configured	BroadCloud	None	MRWan	interop.adpt-tech.com	Enable	-1	4

4.7 Step 7: Configure Dial Plan Rules (Optional)

You can optionally configure rules to manipulate the source and / or destination number. The manipulation rules use the configured IP Groups to denote the source and destination of the call. IP Group 0 represents Skype for Business, and IP Group 1 represents BroadCloud SIP Trunk.

For example, a manipulation can be configured to add a prefix to the destination number for calls from Skype for Business IP Group to the BroadCloud SIP Trunk IP Group for specific destination username prefix.

➤ **To configure a number manipulation rule:**

1. Open the IP-to-IP Outbound Manipulation page (**Configuration** tab > **VoIP** menu > **SBC** > **Manipulations SBC** > **IP-to-IP Outbound**).
2. Click **Add**.
3. Use the following as an example reference for a dial plan rule for adding '+' towards Skype for Business:

Parameter	Value
Index	0
Name	Add + towards Skype for Business (arbitrary descriptive name)
Source IP Group	BroadCloud (i.e., calls coming from the BroadCloud SIP Trunk)
Destination IP Group	S4B (i.e., calls going to the Skype for Business environment)
Destination Username Prefix	* (asterisk sign)

Figure 4-25: Configuring IP-to-IP Outbound Manipulation Rule – Rule Tab

Edit Row

Index: 0
Routing Policy: Default_SBCRouting

Rule | Action

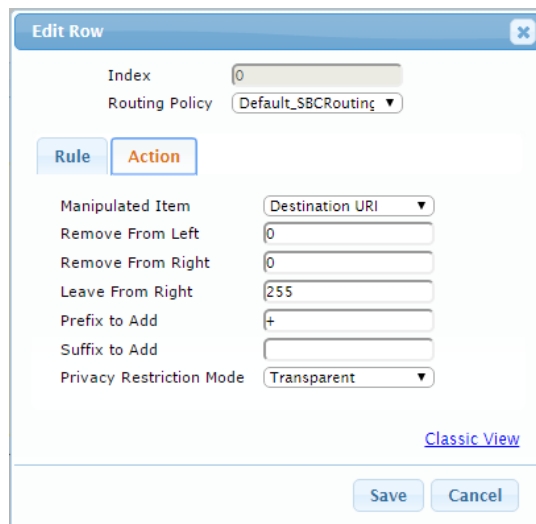
Name: Add + toward S4B
Additional Manipulation: No
Request Type: All
Source IP Group: BroadCloud
Destination IP Group: S4B
Source Username Prefix: *
Source Host: *
Source Tags:
Destination Username Prefix: *
Destination Host: *
Destination Tags:
Calling Name Prefix: *
Message Condition: None
Call Trigger: Any

Save Cancel

4. Click the **Action** tab, and then configure the parameters as follows:

Parameter	Value
Manipulated Item	Destination URI
Prefix to Add	+ (plus sign)

Figure 4-26: Configuring IP-to-IP Outbound Manipulation Rule - Action Tab



Edit Row

Index: 0
Routing Policy: Default_SBCRouting

Rule **Action**

Manipulated Item: Destination URI
Remove From Left: 0
Remove From Right: 0
Leave From Right: 255
Prefix to Add: +
Suffix to Add:
Privacy Restriction Mode: Transparent

[Classic View](#)

Save Cancel

5. Click **Submit**.

The above example shows how to configure the Mediant E-SBC rule to add the prefix '+' (plus sign) to the dialed digits towards Microsoft Skype for Business Server 2015, according to the E.164 number format requirement.

4.8 Step 8: Configure Registration to the BroadCloud Service

4.8.1 Configure Credentials

This step shows how to configure SIP registration towards the BroadCloud service. This is required so that the E-SBC can register with the BroadCloud SIP Trunk on behalf of Skype for Business. The BroadCloud SIP Trunk requires registration and authentication to provide service. These parameters should be supplied by the service provider.

➤ **To configure a registration account:**

1. Open the Account Table page (**Configuration** tab > **VoIP** menu > **SIP Definitions** > **Account Table**).
2. Edit the first row (index 0) to configure the account.

Parameter	Value
Application Type	SBC
Served IP Group	S4B
Serving IP Group	BroadCloud
Username	BroadCloud SIP User. The BroadCloud SIP User value is found on the BroadCloud MySite Trunk Group configuration page under the 'Device Settings for Authentication' section.
Password	BroadCloud SIP Password. The BroadCloud SIP Password value is found on the BroadCloud MySite Trunk Group configuration page under the 'Device Settings for Authentication' section.
Host Name	BroadCloud Register Domain. The BroadCloud Register Domain is found on the BroadCloud MySite Trunk Group configuration page under the 'Trunk Group Settings' section.
Register	Regular
Contact User	BroadCloud SIP User (as the 'Username' above) The BroadCloud SIP User is found on the BroadCloud My Trunk Group configuration page under the 'Device Settings for Authentication' section.

3. Click **Apply**.

Figure 4-27: Configuring SIP Registration Account

The screenshot shows a web interface titled 'Account Table'. It includes buttons for 'Add +', 'Edit', 'Delete', 'Action', and 'Show / Hide'. There is a search bar with 'All' selected and a 'Search in table' button. Below the buttons is a table with the following data:

Index	Application Type	Served Trunk Group	Served IP Group	Serving IP Group	User Name	Password	Host Name	Register	Contact User
0	SBC	-1	S4B	BroadCloud	8325624857	*	interop.adpt-te	Regular	8325624857

At the bottom of the table, there is a pagination control showing 'Page 1 of 1' and a 'View 1 - 1 of 1' indicator.

4.8.2 Configure the SIP Register Domain Name

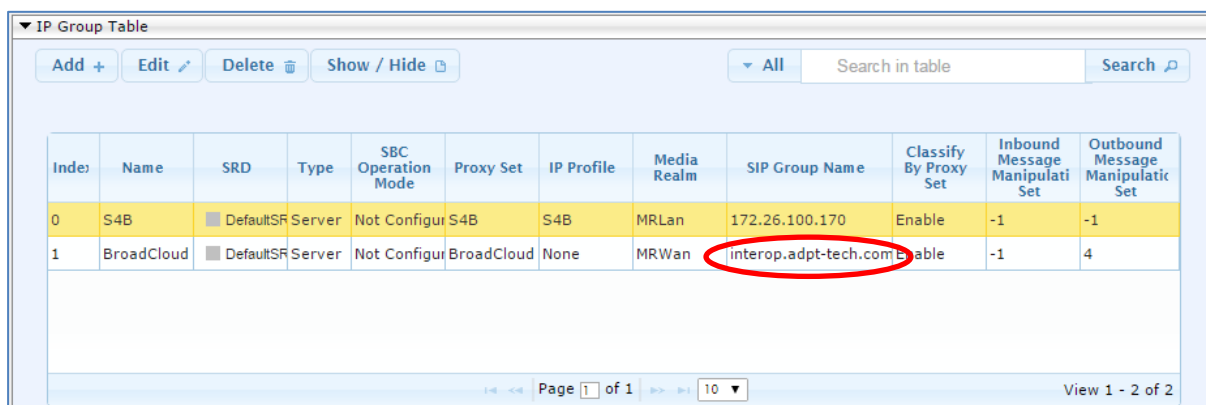
This section shows how to configure the SIP Register Domain Name.

➤ **To configure the SIP Register Domain Name:**

1. Open the IP Group Table page (**Configuration** tab > **VoIP** menu > **VoIP Network** > **IP Group Table**).
2. Edit the second row (index 1) host name in the 'SIP Group Name' field, with the value provided by BroadCloud.

Parameter	Value
Index	1
Name	BroadCloud
Type	Server
Proxy Set	BroadCloud
IP Profile	BroadCloud
Media Realm	MRWan
SIP Group Name	BroadCloud Register Domain. The BroadCloud Register Domain is found on the BroadCloud MySite Trunk Group configuration page under the 'Trunk Group Settings' section.

Figure 4-28: Configured IP Groups in IP Group Table



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
0	S4B	DefaultSR	Server	Not Configured	S4B	S4B	MRLan	172.26.100.170	Enable	-1	-1
1	BroadCloud	DefaultSR	Server	Not Configured	BroadCloud	None	MRWan	interop.adpt-tech.com	Enable	-1	4

4.9 Step 9: Check the SIP Trunk Registration Status

This section shows how to check the SIP Trunk Registration Status.

➤ **To check if the device successfully registered with the BroadCloud service:**

1. Open the Registration Status page (**Status & Diagnostics** tab > **VoIP Status** > **Registration Status**).
2. Check the registration status in the Accounts Registration Status Table.
A successful registration will show as REGISTERED (see the figure below).

Figure 4-29: Successful SIP Trunk Registration

The screenshot shows the 'Registration Status' page. The left sidebar has 'Status & Diagnostics' selected. The main content area shows the 'Registration Status' tab. The 'Accounts Registration Status' table is as follows:

Index	Group Type	Group Name	Status
0	IP Group	172.26.100.170	REGISTERED

Note: If the status of the device does not show REGISTERED, check your WAN connectivity:



- Check the WAN wiring
- Make sure the DMZ configuration is correct on the firewall
- Check WAN IP address configuration (**Configuration** tab > **VoIP** > **Network** > **IP Interface Table**)
- Check the BroadCloud credentials in the Accounts table (**Configuration** tab > **VoIP** menu > **SIP Definitions** > **Account Table**)
- Check the configuration of the BroadCloud Register Domain (**Configuration** tab > **VoIP** menu > **VoIP Network** > **IP Group Table**).

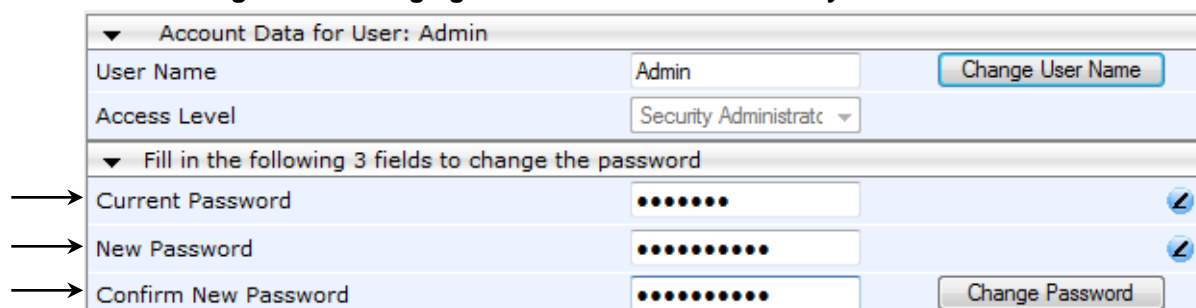
4.10 Step 10: Secure Device Access

4.10.1 Change Default Management User Login Passwords

To secure access to the device's Web management interface, follow these recommended guidelines:

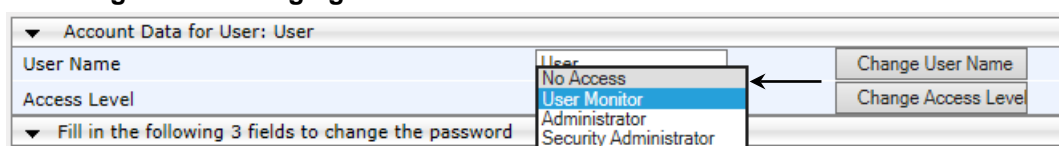
- The device is shipped with a default **Security Administrator** access-level user account – username 'Admin' and password 'Admin'. This user has full read-write access privileges to the device. It is recommended to change the default password to a hard-to-hack string. The login username and password are configured in the Web interface's User Accounts page (**Configuration** tab > **System** > **Web User Accounts**) using the 'Current Password', 'New Password', and 'Confirm New Password' fields, as shown below:

Figure 30: Changing Password of Default Security Administrator User



- The device is shipped with a default **Monitor** access-level user account - username 'User' and password 'User'. This user only has read access privileges to the device. The read access privilege is also limited to certain Web pages. However, this user can view certain SIP settings such as proxy server addresses. Therefore, to prevent an attacker from obtaining sensitive SIP settings that could result in possible call theft etc., change the access level of this user to **No Access** (see the figure below). In addition (or alternatively), change its default login password to a hard-to-hack string.

Figure 31: Changing Access Level to No Access of Default Monitor User



4.10.2 Secure Management Access via WAN

It's recommended that when leaving the device at the end customer's premises, its management interface will be accessible by remote only when required.

Request the end customer's IT administrator to disable the following ports:

- Port 80 - HTTP Web interface access
- Port 443 - HTTPS Web interface access
- Port 22 - SSH access
- Port 23 - Telnet access
- Ports 161 - SNMP access

If future remote management is required, first ask the end customer's IT administrator to open the appropriate port (e.g., HTTP or HTTPS port) in order to manage the device.

4.11 Step 11: Save the Configuration, Connect to DMZ



Note: Firewall settings for the DMZ must be in place before resetting the device. After the device is reset, its IP configuration is applied and it is no longer available for management via the default IP address. After reset, the device's management interface is via its WAN interface, via its global-IP-address, make sure the firewall allows the ports required for management. See Section 4.10.2 for details about the configuration of the required ports on the firewall.

➤ **To save the configuration and reset the device:**

1. On the toolbar, click **Device Actions** and then from the dropdown, choose **Reset**.
2. Under the 'Save Configuration' group, click the **BURN** button; a confirmation message appears when the configuration successfully saves.

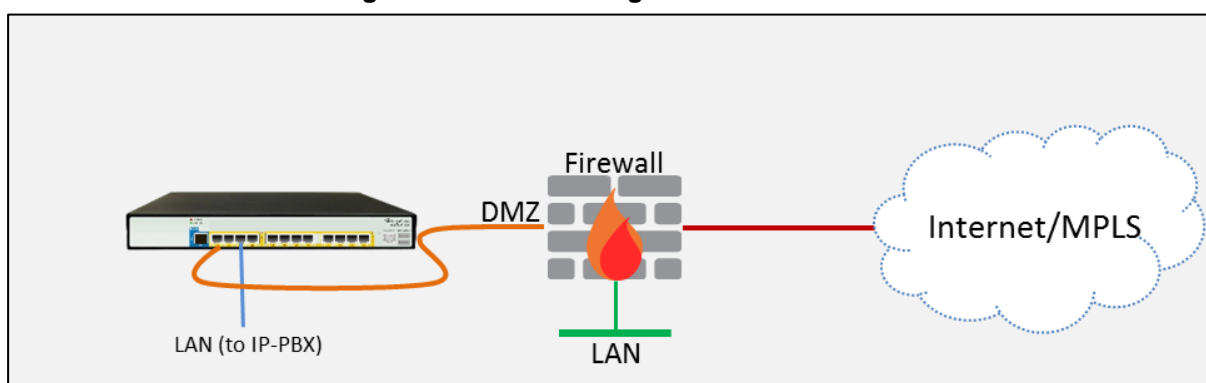
Figure 4-32: Maintenance Actions Page

▼ Reset Configuration	
Reset Board	<input type="button" value="Reset"/>
Burn To FLASH	Yes <input type="button" value="v"/>
Graceful Option	No <input type="button" value="v"/>
▼ LOCK / UNLOCK	
Lock	<input type="button" value="LOCK"/>
Graceful Option	No <input type="button" value="v"/>
Current Admin State	UNLOCKED
▼ Save Configuration	
Burn To FLASH	<input type="button" value="BURN"/>

➤ **To connect the device to DMZ:**

- After the device is reset, the IP address of the device changes to the address configured in Section 4.2, Step 2. At this point, disconnect your PC from the device and connect the Ethernet cable from the device's Ethernet port 1 (see Section 2) to the DMZ port provided by the local firewall and Ethernet port 3 to the local LAN network :

Figure 4-33: Connecting the Device to DMZ



This page is intentionally left blank.

A Troubleshooting

This section describes issues that can be encountered and shows how to solve them.

A.1 Connecting to CLI

Connect to the device's serial port labeled CONSOLE connecting a standard RJ-45 to DB-9 female serial cable to a PC (sold separately). Connect to the console CLI and then:

1. Establish a serial communication (e.g., Telnet) with the device using a terminal emulator program such as HyperTerminal, with the following communication port settings:
 - Baud Rate: 115,200 bps
 - Data Bits: 8
 - Parity: None
 - Stop Bits: 1
 - Flow Control: None
2. At the CLI prompt, type the username (default is **Admin** - case sensitive):
Username: Admin
3. At the prompt, type the password (default is **Admin** - case sensitive):
Password: Admin
4. At the prompt, type the following:
enable
5. At the prompt, type the password again:
Password: Admin

A.2 Enabling Logging on CLI

To enable the device to send the error messages (e.g. Syslog messages) to the CLI console, use the following commands:

1. Start the syslog on the screen by typing:
debug log
2. Enable SIP call debugging
debug sip 5
3. Stop Syslog on the screen by typing:
no debug log

International Headquarters

1 Hayarden Street,
Airport City
Lod 7019900, Israel
Tel: +972-3-976-4000
Fax: +972-3-976-4040

AudioCodes Inc.

27 World's Fair Drive,
Somerset, NJ 08873
Tel: +1-732-469-0880
Fax: +1-732-469-2298

Contact us: www.audiocodes.com/info

Website: www.audiocodes.com



Document #: LTRT-12540