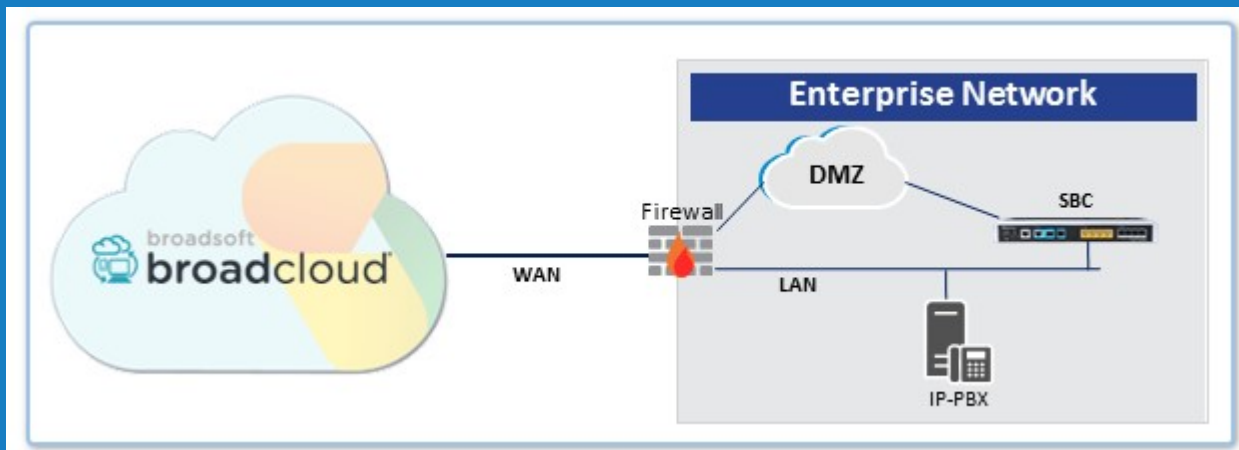


Connecting IP-PBX to BroadSoft's BroadCloud SIP Trunk using AudioCodes Mediant SBC



Version 7.2

Introduction

See Chapter 1



Obtain Software Files

See Chapter 2



Cable Device for Initial Access

See Chapter 3



Upload Software to Device

See Chapter 4



Configure & Reset Device

See Chapter 5



Cable Device to DMZ

See Chapter 6

1 Introduction

This document describes how to set up AudioCodes' Session Border Controller (hereafter, referred to as *SBC*) for interworking between BroadCloud's SIP Trunk and IP-PBX environment. For detailed information on each AudioCodes SBC, refer to the corresponding *User's Manual* and *Hardware Installation Manual*.

1.1 Component Information

AudioCodes SBC Version	
SBC Vendor	AudioCodes
Models	Mediant 500L; Mediant 500; Mediant 800; Mediant 2600; Mediant Software SBC (Virtual Edition (VE) and Server Edition (SE))
Software Version	7.20A.204.222
Protocol	<ul style="list-style-type: none"> ▪ SIP/UDP or SIP/TCP or SIP/TLS for signaling and RTP or SRTP for media (to the BroadCloud SIP Trunk) ▪ SIP/UDP or SIP/TCP (to the IP-PBX)
BroadCloud SIP Trunking Version	
Vendor/Service Provider	BroadCloud
SSW Model/Service	BroadWorks
Software Version	21
Protocol	SIP/UDP or SIP/TCP or SIP/TLS for signaling and RTP or SRTP for media

1.2 Prerequisites

1.2.1 Making BroadCloud Preparations

Prior to reading this Quick Guide, read the *BroadCloud SIP Trunking Service Definition* document, available from BroadCloud's Xchange portal at xchange.broadsoft.com. The document describes how to provision SIP Trunk Groups, SIP Trunk Users and SIP Trunk Mobility Users.



Note: This Quick Guide assumes you've read the *BroadCloud SIP Trunking Service Definition* document and that the required provisioning has been completed.

1.2.2 Mediant Software SBC Prerequisites

This Quick Guide assumes the following:

- The Appropriate Virtual Machine has already been installed according to *Mediant Virtual Edition SBC Installation Manual Ver. 7.2* document.
- The Mediant SE SBC already installed according to *Mediant Server Edition SBC Installation Manual Ver. 7.2* document.

2 Obtain Software Files

Download the certified BroadCloud firmware file (*firmware_xxx.cmp*), configuration file (*configuration_xxxx.ini*), and Call Progress Tones file (*call_progress_xxxxx.dat*, where "xxxxx" is the country name) of the specific AudioCodes SBC, from AudioCodes Website at <http://www.audiocodes.com/broadcloud-resource-center>. The files are downloaded together in a single zipped file. Once downloaded, unzip the file.

3 Cable Device for Initial Access



Note: This section is not relevant for the Mediant Software SBC. For the Mediant Software SBC, refer to *Mediant Virtual Edition SBC Installation Manual Ver. 7.2* and *Mediant Server Edition SBC Installation Manual Ver. 7.2* documents.

The device's factory default IP address for operations, administration, maintenance, and provisioning (OAMP) is **192.168.0.2/24** (default gateway 192.168.0.1).

1. Change your PC's IP address and subnet mask to correspond with the device's default IP address.
2. Cable as follows:
 - Connect the PC to the device's Ethernet port labelled **Port 1** (left-most port).
 - Ground the device using the grounding lug (except Mediant 500L).
 - Using the supplied AC power cable, connect the device's AC port to a standard electrical wall outlet.

Figure 3-1: Mediant 500L Front Panel

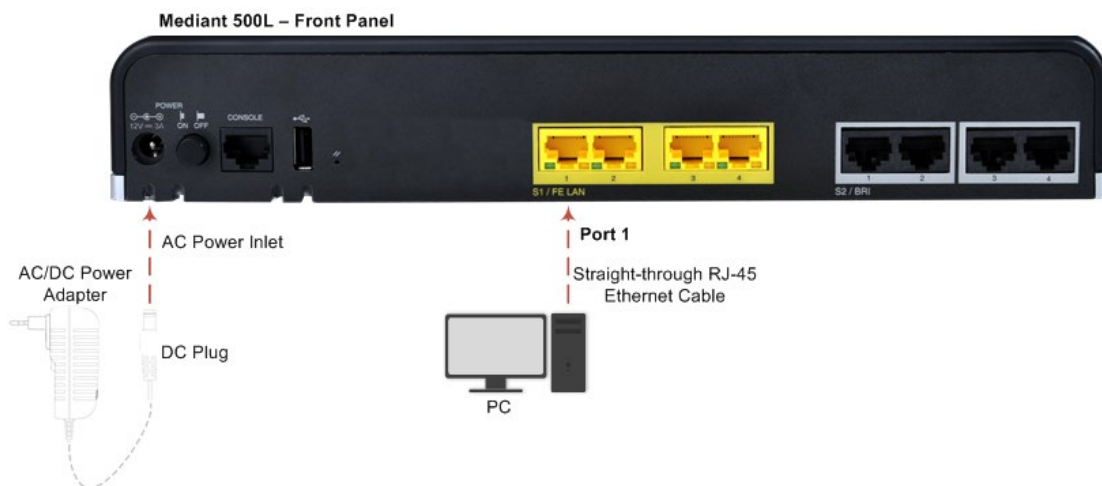


Figure 3-2: Mediant 500 Front Panel

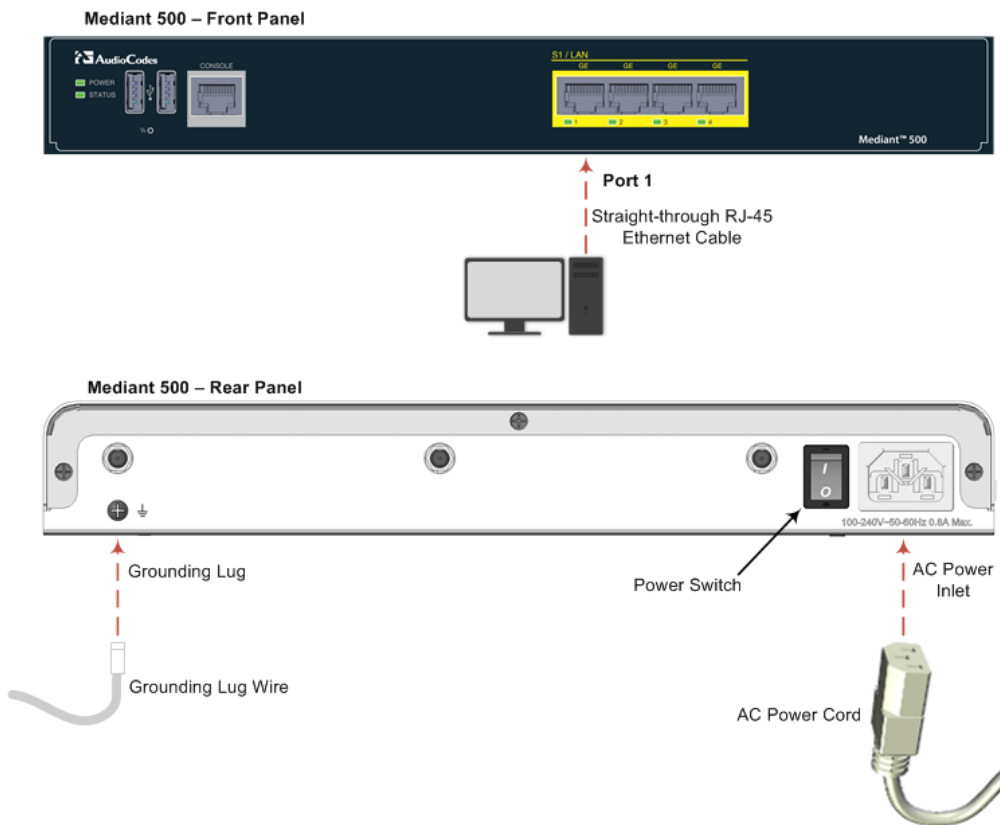


Figure 3-3: Mediant 800 Front Panel

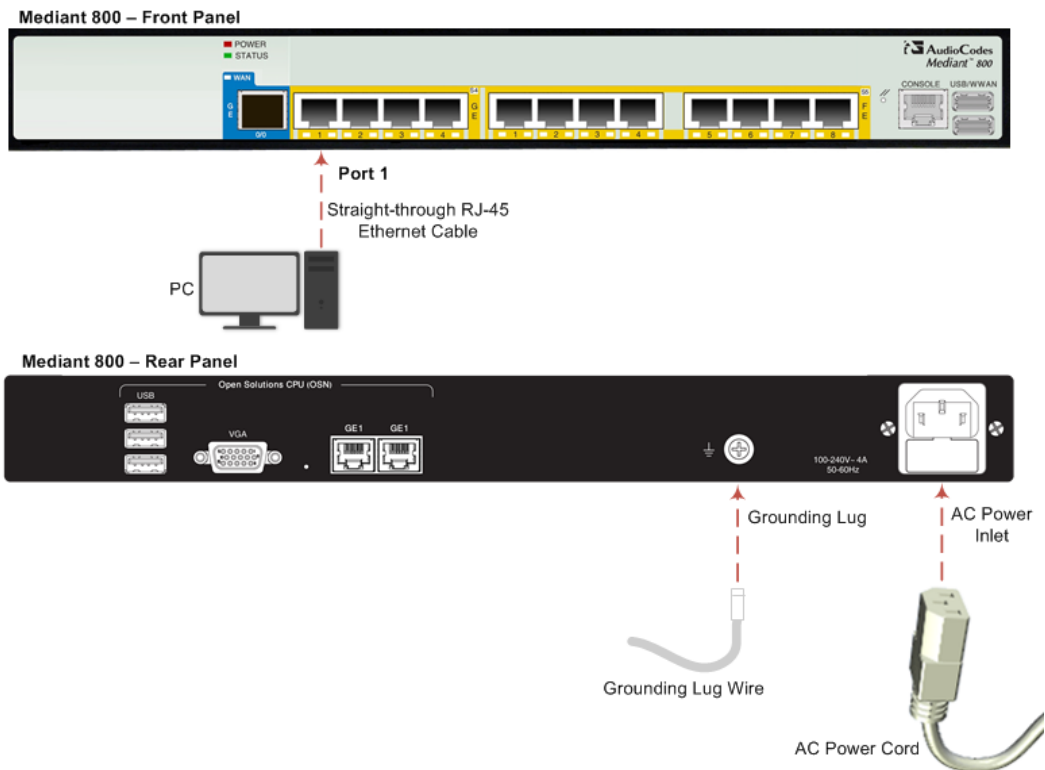
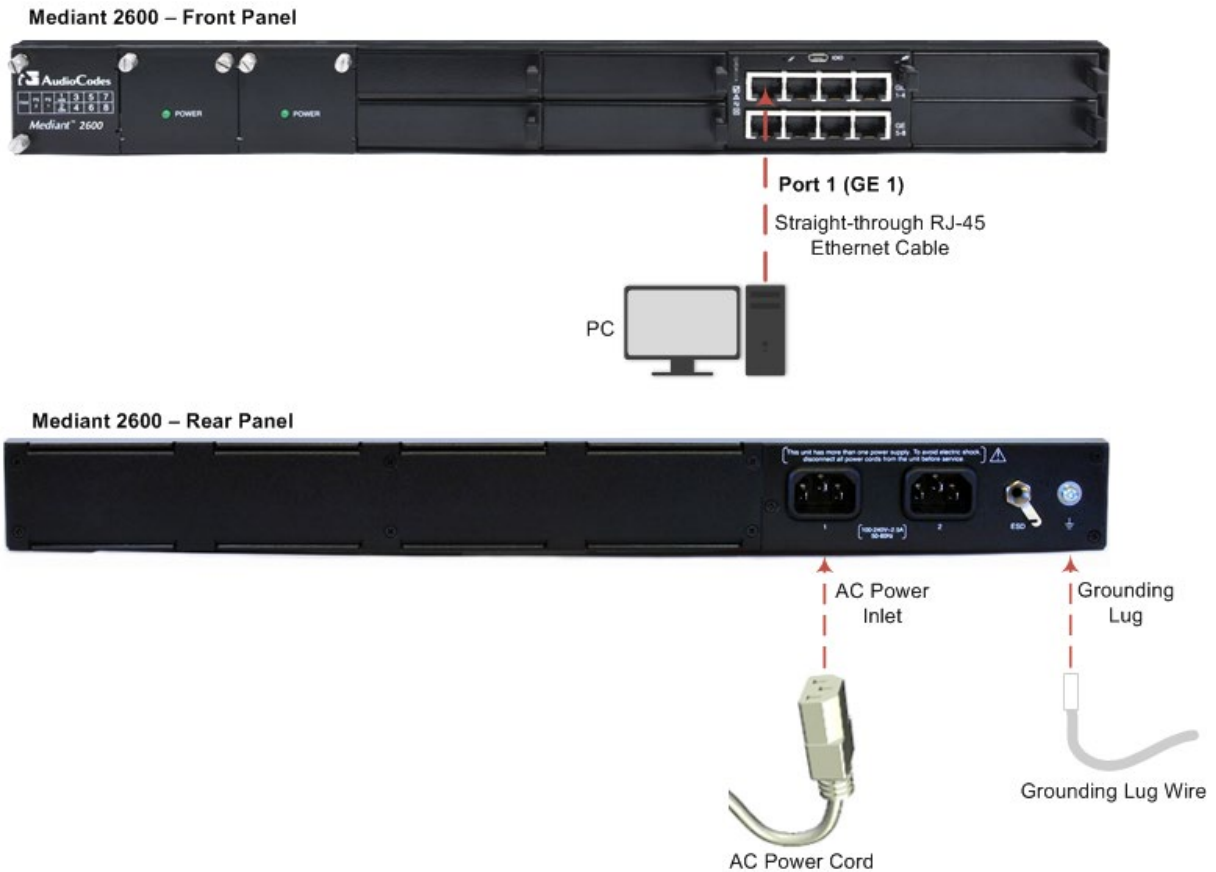


Figure 3-4: Mediant 2600 Front Panel



3. Access the device's Web-based management interface:
 - a. On your PC, start your Web browser and then in the URL address field, enter the device's default IP address; the following appears:

Figure 3-5: Web Login

Web Login

Username

Admin

Password

.....

Remember Me Login

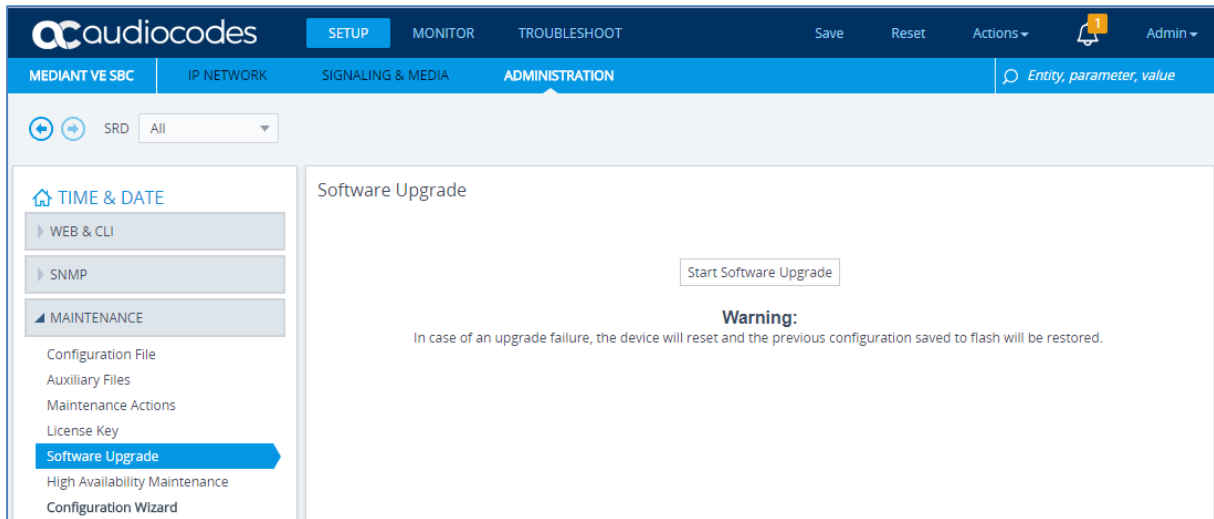
- b. In the 'Username' and 'Password' fields, enter the default login username ("Admin") and password ("Admin"), and then click **Login**.

4 Upload Software to Device

Upload the certified software files, which you downloaded in Section [Obtain Software Files](#), to the device:

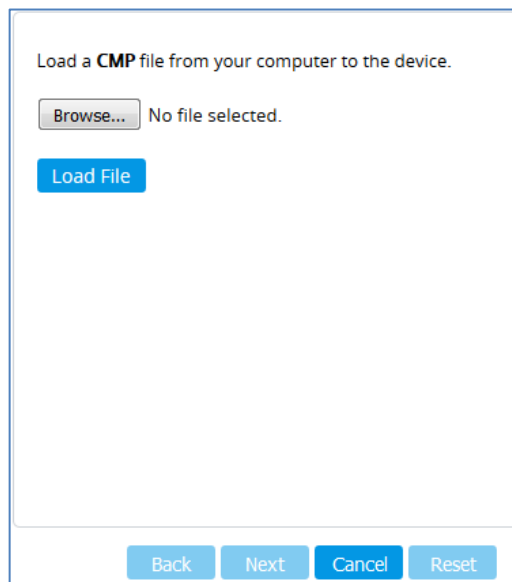
- In the Web interface, open the Software Upgrade Wizard:
 - Toolbar:** From the **ACTIONS** drop-down menu, choose **Software Upgrade**.
 - Navigation tree:** **Setup** menu > **Administration** tab > **Maintenance** folder > **Software Upgrade**.

Figure 4-1: Device Setup



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

Figure 4-2: Loading CMP File in Software Upgrade Wizard

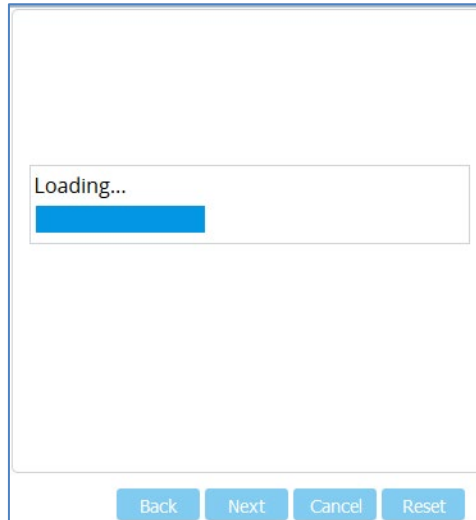


Note: At this stage, you can quit the Software Upgrade wizard without having to reset the device, by clicking **Cancel**. However, if you continue with the wizard and start loading the CMP file, the upgrade process must be completed with a device reset.

- Click **Browse**, and then navigate to and select the .cmp file.

- Click **Load File**; the device begins to install the .cmp file and a progress bar displays the status of the loading process:

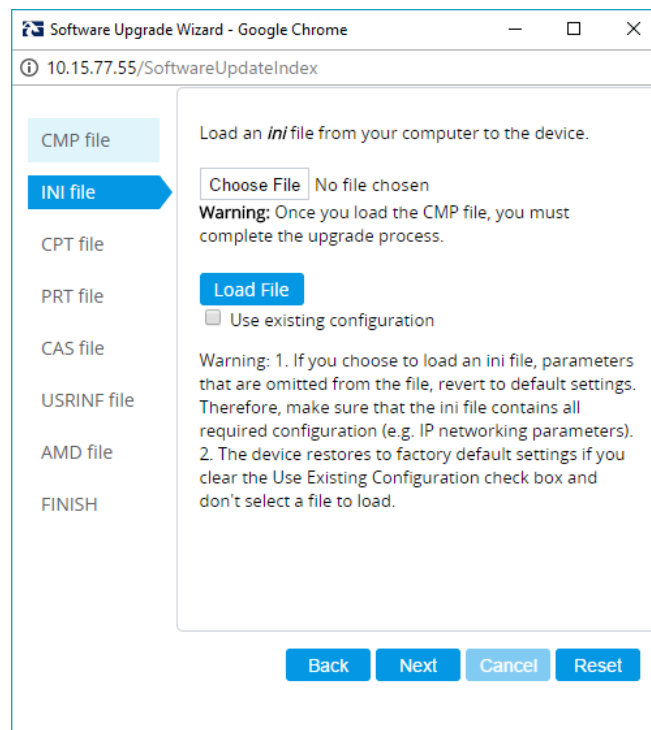
Figure 4-3: CMP File Loading Progress Bar



When the file is loaded, a message is displayed to inform you.

- When successfully loaded, click **Next** to access the wizard page for loading the *ini* file.
- Clear the **Use existing configuration** option, click **Browse** to select the configuration file (.ini) on your PC, and then click **Load File** to load the file:

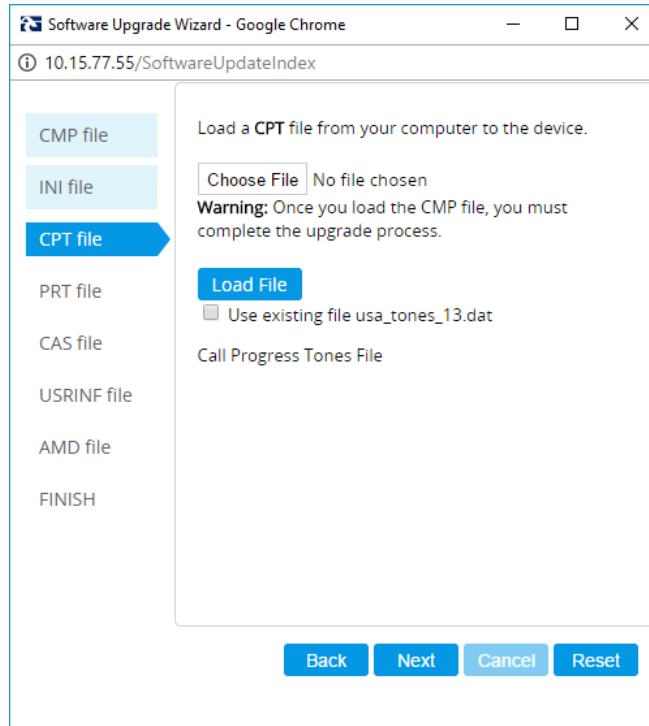
Figure 4-4: Load an INI File in the Software Upgrade Wizard



- Click **Next** to access the wizard page for loading the Call Progress Tones (CPT) file.

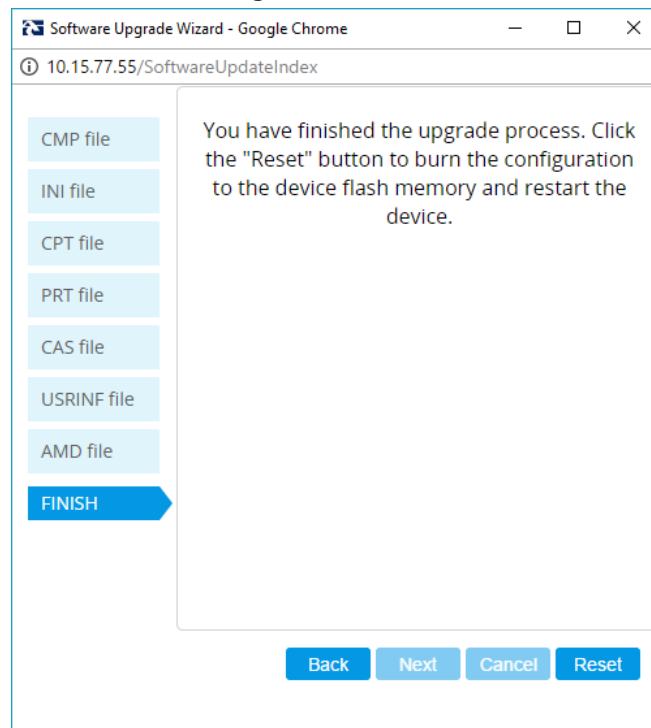
- Click **Browse** to select the **CPT** file on your PC, and then click **Load File** to load the file:

Figure 4-5: Load an CPT File in the Software Upgrade Wizard



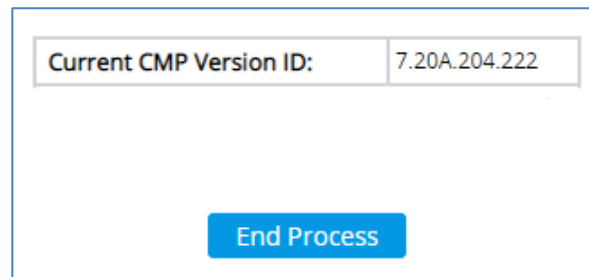
- Keep clicking **Next** until the last Wizard page appears (the **FINISH** button is highlighted in the left pane) and the following message appears:

Figure 4-6: Finish



10. Click **Reset** to install the files by saving them on the device's flash memory with a device. Once complete, the following is displayed:

Figure 4-7: Current CMP Version



11. Click **End Process** to close the wizard, and then log in again to the Web interface.
12. 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.
13. Click **OK**; the Web interface becomes active, reflecting the upgraded device.

5 Configure Device

This section describes device configuration.

5.1 Change Default Management User Login Passwords

To secure access to the device's Web management interface, follow these 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 Local Users page (**Setup** menu > **Administration** tab > **Web & CLI** folder > **Local Users**) using the 'Password' and 'Apply' fields:

Figure 5-1: Changing Password of Default Security Administrator User

The screenshot shows the 'Local Users' configuration window with two tabs: 'GENERAL' and 'SECURITY'. The 'GENERAL' tab is active, showing the following fields:

Field	Value
Index	0
Username	Admin
Password
User Level	Security Administrator
SSH Public Key	
Status	Valid

The 'SECURITY' tab is also visible, showing the following fields:

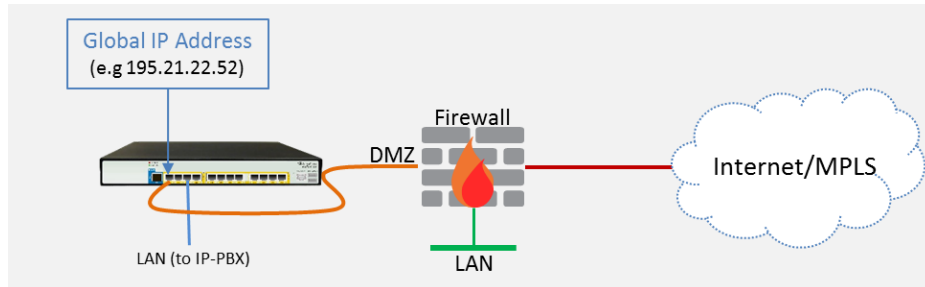
Field	Value
Password Age	0
WEB Session Limit	2
CLI Session Limit	-1
WEB Session Timeout	15
Block Duration	60

- The device is shipped with a default Monitor access-level user account - username and password: 'User' who has read access only and page viewing limitations but 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 its default login password to a hard-to-hack string.

5.2 Configure a Network Interface for the Device

You can connect the device to the DMZ network using one of the following methods:

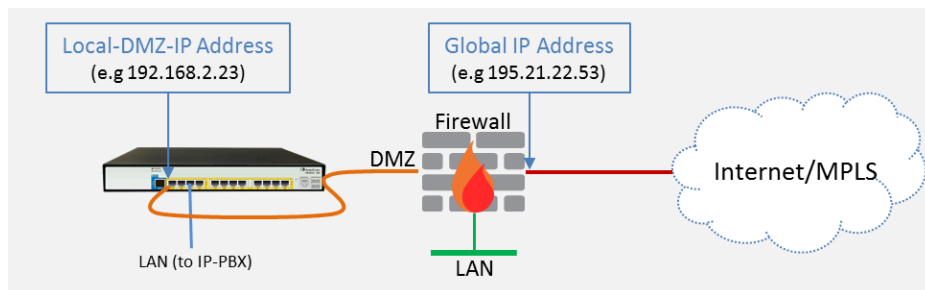
- Method A:** (Preferred method) A global IP address is provided to the device (**without NAT**):



The Enterprise firewall is configured with rules, for example:

Original		
Source	Destination	Ports/Service
<any> (e.g. ITSP)	Global IP Address (public address)	SIP service: 8933 / UDP RTP service: 6000-8500 / UDP

- Method B:** A local DMZ IP address **behind NAT**:



The firewall is configured with rules, for example:

Original			Translated		
Source	Destination	Ports/Service	Source	Destination	Ports/Service
<any> (e.g. ITSP)	Global IP Address (public address)	SIP service: 8933 / 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
<any> (e.g. ITSP)	Global IP Address (public address)	SIP service: 8933 / UDP RTP service: 6000-8500 / UDP	<any> (e.g. ITSP)	Local DMZ IP Address	<as original>
Local DMZ IP Address	<any> (e.g. ITSP)	SIP service: 8933 / UDP RTP service: 6000-8500 / UDP	Global Address (public address)	<any> (e.g. ITSP)	<as original>

5.2.1 Configure Network Interfaces

Configure network interfaces for the DMZ/WAN (BroadCloud SIP-Trunk) interface and LAN (IP-PBX via local LAN-Switch) interface, as described below:

1. Open the IP Interfaces table (**Setup** menu > **IP Network** tab > **Core Entities** folder > **IP Interfaces**).
2. Configure the DMZ/WAN (BroadCloud SIP-Trunk) interface:
 - a. Select the 'Index 0' radio button of the **OAMP + Media + Control** table row, and then click **Edit**. This is the existing **WAN** ("WANSP") interface (available on eth port #1).
 - a. Configure the interface as follows:

Parameter	Value
Name	WAN_IF (descriptive name, you may change it)
Application Type	OAMP + Media + Control (leave as is)
Ethernet Device	vlan 1
IP Address	<ul style="list-style-type: none"> ▪ <u>Method A</u>: Global-IP-Address (public address) ▪ <u>Method B</u>: Local-DMZ-IP-Address
Prefix Length	Subnet mask in bits , for example, 28 (255.255.255.240)
Default Gateway	Default gateway IP address (for Method B, this is the router's IP address).
Primary DNS Server IP Address	Primary DNS IP address
Secondary DNS Server IP Address	Secondary DNS IP address (optional)

3. Configure the LAN (IP-PBX via local LAN-Switch) interface:
 - a. Select the 'Index 1' radio button of the **Media + Control** table row, and then click **Edit**. This is the existing **LAN** ("Voice") interface (available on eth port #3):
 - b. Configure the interface as follows:

Parameter	Value
Name	Voice (descriptive name, you may change it). This interface will be associated with IP-PBX connectivity.
Application Type	Media + Control (<u>leave as is</u>)
Ethernet Device	vlan 2
IP Address	Local LAN IP address assigned for the SBC to use to communicate with the IP-PBX.
Prefix Length	Subnet mask in bits , for example, 24 (255.255.255.0).
Default Gateway	Local LAN default gateway IP address
Primary DNS Server IP Address	Primary DNS IP address (optional)
Secondary DNS Server IP Address	Secondary DNS IP address (optional)

4. Click **Apply**.

An example of configured IP network interfaces is shown below:

Figure 5-2: IP Network Interfaces

INDEX	NAME	APPLICATION TYPE	INTERFACE MODE	IP ADDRESS	PREFIX LENGTH	DEFAULT GATEWAY	PRIMARY DNS	SECONDARY DNS	ETHERNET DEVICE
0	WANSP	OAMP + Medi	IPv4 Manual	195.189.192.1	24	195.189.192.1	80.179.52.100	80.179.55.100	vlan 1
1	Voice	Media + Cont	IPv4 Manual	10.15.77.55	16	10.15.0.1	10.15.27.1	0.0.0.0	vlan 2

5.2.2 Configure NAT



Note:

- NAT configuration is applicable only if you are behind a firewall NAT (see [Method B](#)).
- 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 SBC is already assigned the Global-IP-address as its address, skip this NAT configuration.

Configure the global IP address as follows:

1. Open the NAT Translation table (**Setup** menu > **IP Network** tab > **Core Entities** folder > **NAT Translation**), and then click **Add**; the following dialog appears:

Figure 5-3: NAT Translation

NAT Translation

SOURCE	TARGET
Index: <input type="text" value="0"/>	Target IP Address: <input type="text"/>
Source Interface: <input type="text" value="--"/> View	Target Start Port: <input type="text"/>
Source Start Port: <input type="text"/>	Target End Port: <input type="text"/>
Source End Port: <input type="text"/>	

- Use the following table as reference when configuring a NAT translation rule:

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

- Click **Apply**.

5.3 Configure UDP Ports for RTP between SBC and IP-PBX



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). Skip this step if you don't need to change the default.

Configure media ports as follows:

- Open the Media Realm Table page (**Setup** menu > **Signaling & Media** tab > **Core Entities** folder > **Media Realms**), and then 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 IP-PBX)
Number of Media Session Legs	250 (media sessions assigned with port range)

Figure 5-4: Configure Media Realm

The configured Media Realms are shown in the figure below:

Figure 5-5: Media Realms

Media Realms (2)

+ New Edit | Page 1 of 1 | Show 10 records per page

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

5.4 Configure the IP-PBX IP Address

Configure the IP-PBX IP address as described below:

1. Open the Proxy Sets table (**Setup** menu > **Signaling & Media** tab > **Core Entities** folder > **Proxy Sets**).
2. Edit the Proxy Set for the IP-PBX (you can identify it by the 'Proxy Name' field).

- Click the **Proxy Address** link located below the table; the Proxy Address table opens:

Parameter	Value
Index	0
Proxy Address	IP-PBX IP address / FQDN and destination port, for example, 172.26.100.170:5060.
Transport Type	Network transport type for your IP-PBX, for example, UDP.

Figure 5-6: Proxy Address

The screenshot shows a configuration window titled "Proxy Address". Under the "GENERAL" tab, there are three fields: "Index" with the value "0", "Proxy Address" with the value "172.26.100.170:5060", and "Transport Type" with a dropdown menu currently set to "UDP".

5.5 Configure a SIP Host Name for IP-PBX

Configure the SIP host name used in SIP INVITE and REGISTER messages sent to the IP-PBX. This depends on the IP-PBX.

- Open the IP Groups table (**Setup** menu > **Signaling & Media** tab > **Core Entities** folder > **IP Groups**).
- Edit the SIP host name in the 'SIP Group Name' field, with the value required by the IP-PBX.

Parameter	Value
Index	1
Name	IP-PBX
Type	Server
Proxy Set	IP-PBX
IP Profile	IP-PBX
Media Realm	MRLan
SIP Group Name	172.26.100.170 (per IP-PBX requirement)

Figure 5-7: IP-PBX IP Groups

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	Default_IPG	DefaultSRD	Server	Not Configured	ProxySet_0	--	--		Disable	-1	-1
1	IP-PBX	DefaultSRD	Server	Not Configured	IP-PBX	IP-PBX	MRLan	172.26.100.170	Enable	-1	-1
2	BroadCloud	DefaultSRD	Server	Not Configured	BroadCloud	BroadCloud	MRWan	interop.adpt-tek	Enable	-1	4

5.6 Configure Dial Plan Rules (Optional)

You can optionally configure rules to manipulate the source and / or destination number. Manipulation rules use the configured IP Groups to denote the source and destination of the call. IP Group 1 represents IP-PBX, and IP Group 2 represents BroadCloud SIP Trunk. For example, manipulation can be configured to add a prefix to the destination number for calls from the IP-PBX IP Group to the BroadCloud SIP Trunk IP Group for specific destination username prefix.

The following procedure provides an example on how to configure the SBC to add prefix digits 0119723976 to the dialed four digits 4347, resulting in 01197239764347:

1. Open the Outbound Manipulations table (**Setup** menu > **Signaling & Media** tab > **SBC** folder > **Manipulation** > **Outbound Manipulations**), and then click **Add**.
2. Use the following as an example reference for a dial plan rule:

Parameter	Value
Index	0
Name	Call to desk (descriptive name)
Source IP Group	IP-PBX (i.e., calls coming from the IP-PBX)
Destination IP Group	BroadCloud (i.e. calls going to the BroadCloud Service)
Destination Username Prefix	4347 (number dialed from the IP-PBX toward the BroadCloud SIP-Trunk)
Manipulated Item	Destination URI
Prefix to Add	0119723976

Figure 5-8: Outbound Manipulations

Outbound Manipulations - x

Routing Policy
#0 [Default_SBCRoutingPolicy] ▼

GENERAL		ACTION	
Index	<input type="text" value="0"/>	Manipulated Item	<input style="background-color: #ffffcc;" type="text" value="Destination URI"/>
Name	<input style="background-color: #ffffcc;" type="text" value="Call to desk"/>	Remove From Left	<input type="text" value="0"/>
Additional Manipulation	<input style="background-color: #ffffcc;" type="text" value="No"/>	Remove From Right	<input type="text" value="0"/>
Call Trigger	<input style="background-color: #ffffcc;" type="text" value="Any"/>	Leave From Right	<input type="text" value="255"/>
MATCH		Prefix to Add	<input style="background-color: #ffffcc;" type="text" value="0119723976"/>
Request Type	<input style="background-color: #ffffcc;" type="text" value="All"/>	Suffix to Add	<input type="text" value=""/>
Source IP Group	<input style="background-color: #ffffcc;" type="text" value="#1 [IP-PBX]"/> View	Privacy Restriction Mode	<input style="background-color: #ffffcc;" type="text" value="Transparent"/>
Destination IP Group	<input style="background-color: #ffffcc;" type="text" value="#2 [BroadCloud]"/> View		

3. Click **Apply**.

5.7 Configure Registration for BroadCloud Service

This section describes configuration relating to registration with BroadCloud service.

5.7.1 Configure Credentials

Configure SIP registration toward the BroadCloud service. This is required so that the SBC can register with the BroadCloud SIP Trunk on behalf of the IP-PBX. The BroadCloud SIP Trunk requires registration and authentication to provide service. These parameters should be supplied by the service provider.

1. Open the Accounts table (**Setup** menu > **Signaling & Media** tab > **SIP Definitions** folder > **Accounts**), and then edit row index 0, as follows:

Parameter	Value
Application Type	SBC
Served IP Group	IP-PBX
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.

2. Click **Apply**.

Figure 5-9: Accounts

INDEX	APPLICATION TYPE	SERVED TRUNK GROUP	SERVED IP GROUP	SERVING IP GROUP	USER NAME	PASSWORD	HOST NAME	REGISTER	CONTACT USER
0	SBC	-1	IP-PBX	BroadCloud	8325624857	*	interop.adpt-te	Regular	8325624857

5.7.2 Configure the SIP Register Domain Name

Configure the SIP Register domain name.

1. Open the IP Group Table page (**Setup** menu > **Signaling & Media** tab > **Core Entities** folder > **IP Groups**), and then edit row index 1 so that the host name in the 'SIP Group Name' field is set to the value provided by BroadCloud.

Parameter	Value
Index	2
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 5-10: IP Group-BroadCloud

INDEX	NAME	SRD	TYPE	SBC OPERATION MODE	PROXY SET	IP PROFILE	MEDIA REALM	SIP GROUP NAME	CLASSIFY BY PROXY SET	INBOUND MESSAGE MANIPULAT SET	OUTBOUND MESSAGE MANIPULAT SET
0	Default_IPG	Default	Server	Not Configu	ProxySet_0	--	--		Disable	-1	-1
1	IP-PBX	Default	Server	Not Configu	IP-PBX	IP-PBX	MRLan	172.26.100.1	Enable	-1	-1
2	BroadCloud	Default	Server	Not Configu	BroadCloud	BroadCloud	MRWan	interop.adpt	Enable	-1	4

5.8 Secure Device Access



Note: Due to the vast number of potential attacks (such as DDoS), security of your VoIP network should be your paramount concern. The AudioCodes device provides a wide range of security features to support perimeter defense. For recommended security configuration for your AudioCodes device, refer to AudioCodes' *Security Guidelines* document.

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**. If not 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) to manage the device.

5.9 Save Configuration



Note: Firewall settings for the DMZ must be in place before resetting the device. After the device is reset, its new IP configuration is applied and it is no longer available for management from the LAN. After reset, the device's management interface is through its WAN interface. Therefore, make sure the firewall allows the ports required for call handling. See Section 5.2 for more information.

Save configuration as follows:

1. Open the Maintenance Actions page:
 - Toolbar: Click the **Reset** button.
 - Navigation tree: **Setup** menu > **Administration** tab > **Maintenance** folder > **Maintenance Actions**.
2. From the 'Save To Flash' drop-down list, select **Yes**; a confirmation message appears when the configuration is successfully saved

Figure 5-11: Maintenance Actions

Maintenance Actions

<div style="background-color: #f0f0f0; padding: 2px; margin-bottom: 5px;">RESET DEVICE</div> <p>Reset Device <input type="button" value="Reset"/></p> <p>Save To Flash <input type="text" value="Yes"/></p> <p>Graceful Option <input type="text" value="No"/></p>	<div style="background-color: #f0f0f0; padding: 2px; margin-bottom: 5px;">LOCK / UNLOCK</div> <p>Lock <input type="button" value="LOCK"/></p> <p>Graceful Option <input type="text" value="No"/></p> <p>Gateway Operational State UNLOCKED</p>
---	---

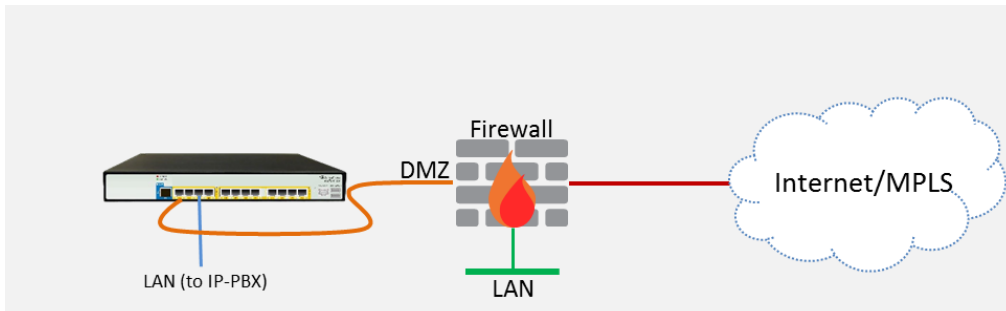
For **Reset Device**: If you choose not to save the device's configuration to flash memory, all changes made since the last time the configuration was saved will be lost after the device is reset.

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

6 Cable Device to DMZ

Once you the device has reset with your new configuration (as described in the previous section), its IP address changes to your newly configured address. You can now cable the device to your DMZ network and local LAN IP-PBX:

Figure 6-1: Cable Device to DMZ



1. Disconnect the cable connecting the device to your PC.
2. Cable to the DMZ Network:
 - a. Connect one end of a straight-through RJ-45 Ethernet cable (Cat 5e or Cat 6) to Port 1.
 - b. Connect the other end of the cable to your DMZ network.
3. Cable to the IP-PBX:
 - a. Connect one end of a straight-through RJ-45 Ethernet cable (Cat 5e or Cat 6) to Port 3.
 - b. Connect the other end of the cable to your LAN Layer-2 switch port, which is used to communicate with your local IP-PBX.

Figure 6-2: Mediant 500L Front Panel

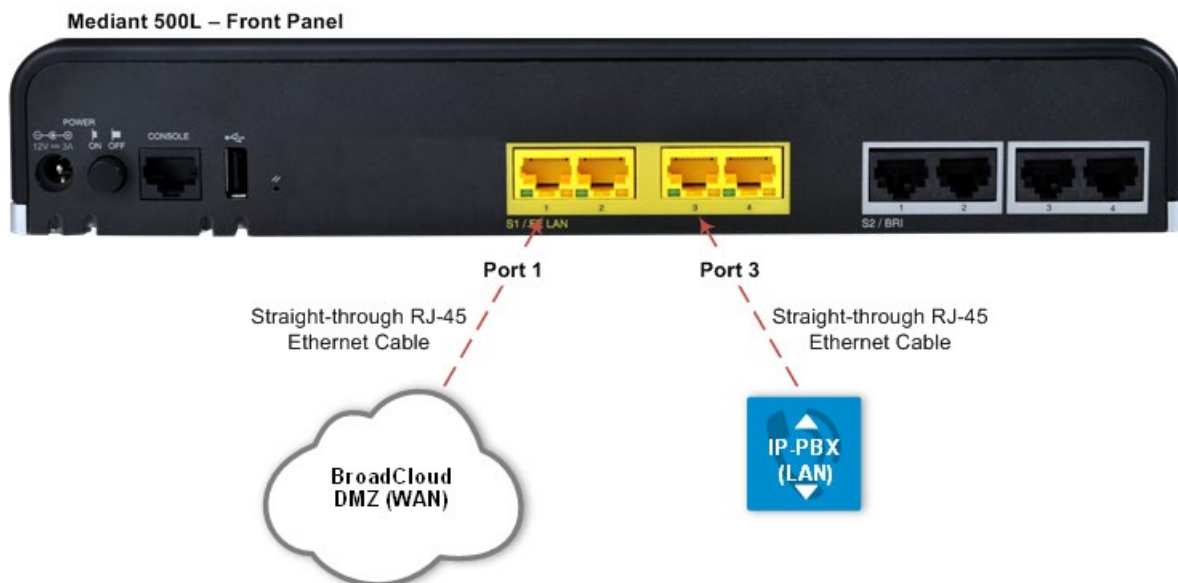


Figure 6-3: Mediant 500 Front Panel

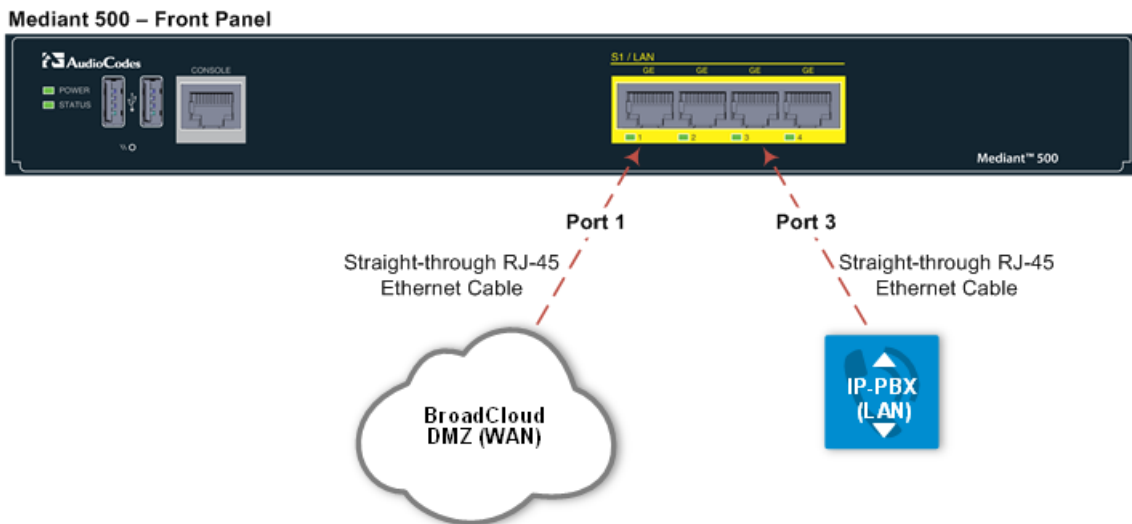


Figure 6-4: Mediant 800 Front Panel

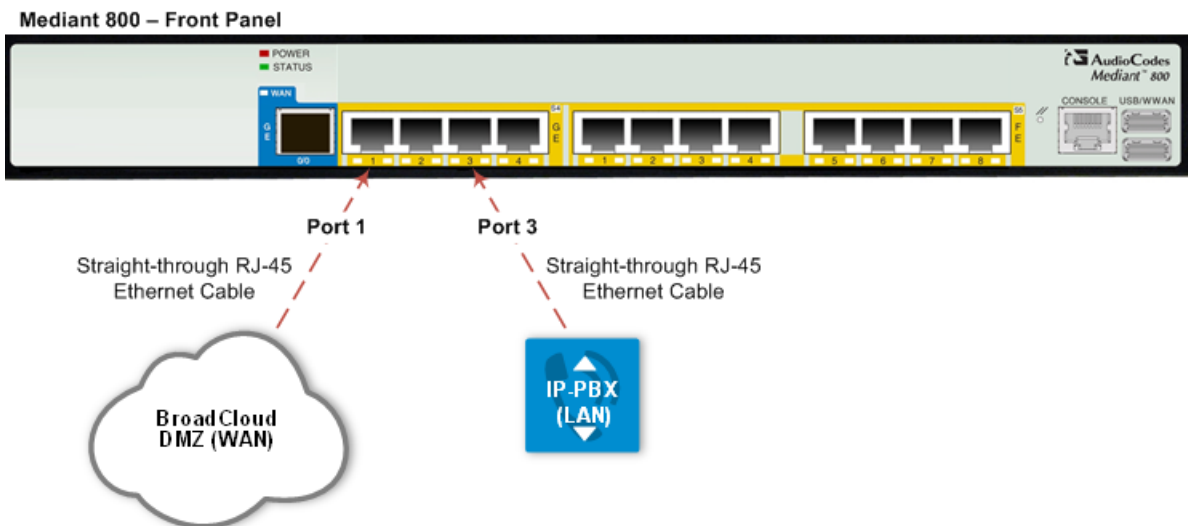
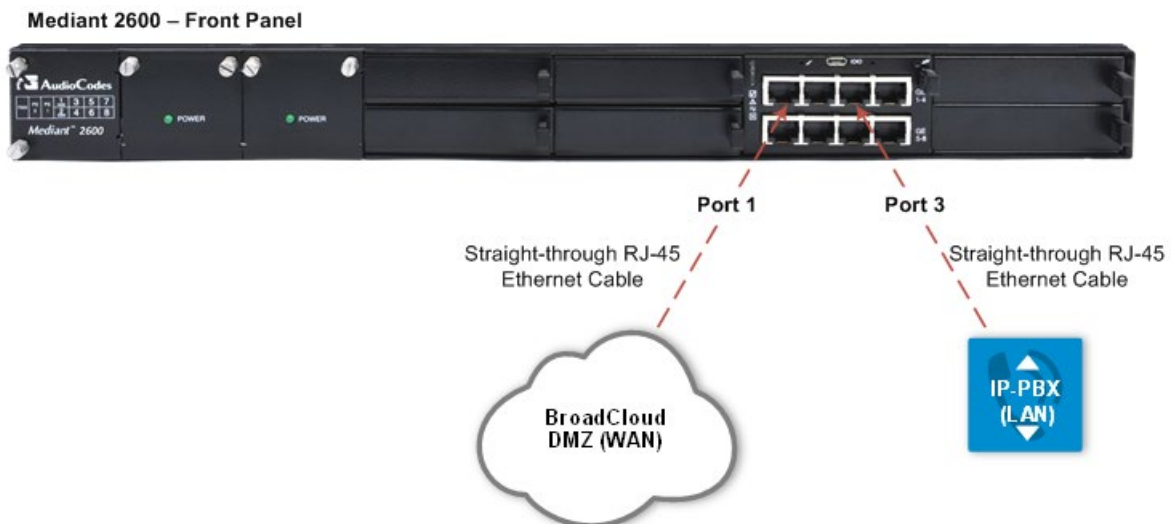


Figure 6-5: Mediant 2600 Front Panel

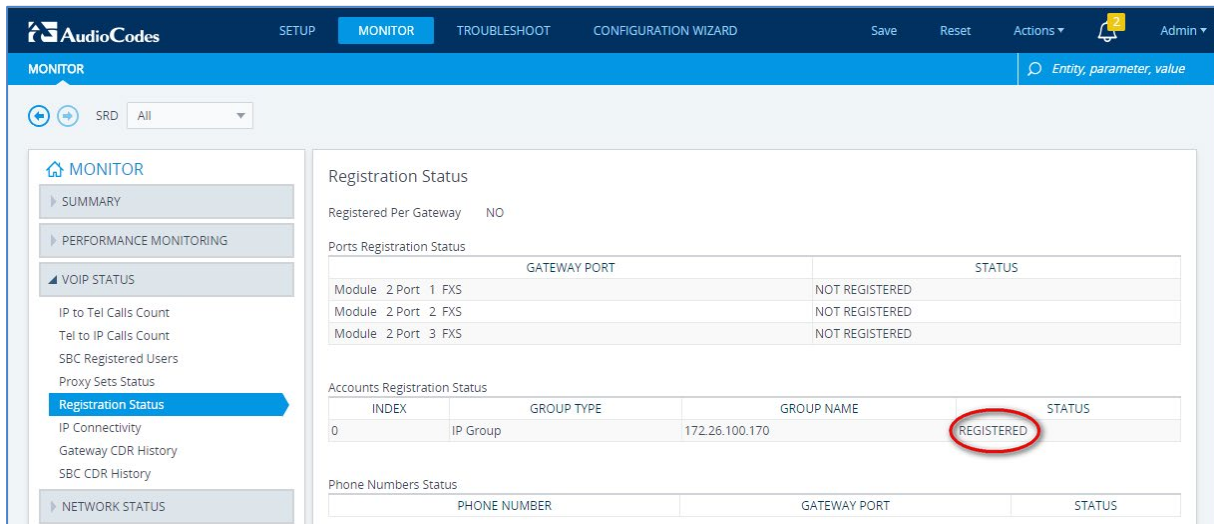


7 Verify SIP Trunk Registration Status

Verify that the device successfully registered with the BroadCloud service (SIP Trunk registration status), as described below:

1. Open the Registration Status table (**Monitor** menu > **Monitor** tab > **VoIP Status** folder > **Registration Status**).
2. If registered successfully, the Status column in the Accounts Registration Status table displays "REGISTERED":

Figure 7-1: SIP Trunk Registration Status



The screenshot shows the AudioCodes Mediant SBC Monitor interface. The 'MONITOR' tab is selected, and the 'VOIP STATUS' folder is expanded to show the 'Registration Status' table. The 'Accounts Registration Status' table is visible, with the following data:

INDEX	GROUP TYPE	GROUP NAME	STATUS
0	IP Group	172.26.100.170	REGISTERED

The 'REGISTERED' status in the table is circled in red.

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 (for example, port 8933 is opened).
- Check the WAN IP address configuration (**Setup** menu > **IP Network** tab > **Core Entities** folder > **IP Interfaces**).
- Check the BroadCloud credentials in the Accounts table (**Setup** menu > **Signaling & Media** tab > **SIP Definitions** folder > **Accounts**).
- Check the configuration of the BroadCloud Register Domain (**Setup** menu > **Signaling & Media** tab > **Core Entities** folder > **IP Groups**).



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 SIP Logging

To enable the device to send SIP messages (in Syslog message format) to the CLI console, use the following commands:

1. Start the Syslog:
debug log
2. Enable SIP call debugging:
debug sip 5
3. Stop Syslog:
no debug log

B Changing connectivity to TLS/SRTP (Optional)

This section shows how to configure the Mediant SBC to work in secure mode (TLS/SRTP) towards BroadCloud SIP Trunk.

B.1 Change Signaling connectivity to TLS

Proxy Set configuration need to be changed in order to move to TLS as transport type. To change Proxy Set:

1. Open the Proxy Sets table (**Setup** menu > **Signaling & Media** tab > **Core Entities** folder > **Proxy Sets**).
2. Modify the BroadCloud Proxy Set (Index 2). Click the **Proxy Address** link located below the table; the Proxy Address table opens.
3. Click **Edit**, the following dialog box appears:

Figure B-1: Configuring Proxy Address for BroadCloud SIP Trunk

GENERAL	
Index	0
Proxy Address	• hs2.fedsipt1.broadcloudgov.us
Transport Type	• TLS ▼

4. For 'Proxy Address', enter the domain name of the BroadCloud Server (e.g., **hs2.fedsipt1.broadcloudgov.us**).
5. From the 'Transport Type' dropdown, select **TLS**.
6. Click **Apply**.

B.2 Configure SRTP

B.2.1 Enable Media Security

This section describes how to enable media security. To configure media security:

1. Open the Media Security page (**Setup** menu > **Signaling & Media** tab > **Media** folder > **Media Security**).

Figure B-2: Configuring SRTP

Media Security

GENERAL

Media Security → • Enable ▼

Media Security Behavior Preferable ▼

Offered SRTP Cipher Suites All ▼

Aria Protocol Support Disable ▼

2. From the 'Media Security' drop-down list, select **Enable** to enable SRTP.
3. Click **Apply**.

B.2.2 Change Media Security Mode to SRTP

This section describes how to change media security mode to SRTP for BroadCloud SIP Trunk. To change media security mode:

1. Open the IP Profiles table (**Setup** menu > **Signaling & Media** tab > **Coders & Profiles** folder > **IP Profiles**).
2. Choose BroadCloud IP Profile and from the 'SBC Media Security Mode' drop-down list, select **SRTP**.

Figure B-3: Configuring SRTP

IP Profiles [BroadCloud]

GENERAL

Index 1

Name • BroadCloud

Created by Routing Server No

MEDIA SECURITY

SBC Media Security Mode • SRTP ← ▼

B.3 Configure the NTP Server Address

This section describes how to configure the NTP server's IP address. It is recommended to implement an NTP server to ensure that the Mediant SBC receives the accurate and current date and time. This is necessary for validating certificates of remote parties. To configure the NTP server address:

1. Open the Time & Date page (**Setup** menu > **Administration** tab > **Time & Date**).
2. In the 'Primary NTP Server Address' field, enter the IP address of the NTP server (e.g., **pool.ntp.org**).

Figure B-4: Configuring NTP Server Address

3. Click **Apply**.

B.4 Configure a Certificate for Operation with the BroadCloud SIP Trunk

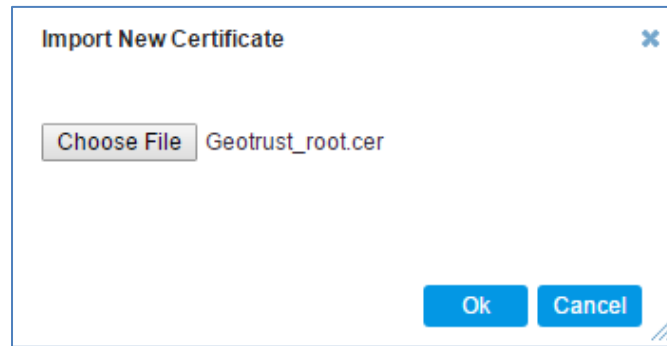
This step describes how to load the BroadCloud Root Certificate as a Trusted Root Certificate. This certificate is used by the Mediant Gateway to authenticate the connection with the BroadCloud SIP Trunk.

The procedure involves the following main steps:

- a. Obtaining a Trusted Root Certificate from the BroadCloud.
- b. Deploying the BroadCloud Root Certificate as Trusted Root Certificates on the Mediant SBC.

➤ **To load a certificate:**

1. Open the TLS Contexts page (**Setup** menu > **IP Network** tab > **Security** folder > **TLS Contexts**).
2. In the TLS Contexts page, select the required TLS Context index row (usually **default** index 0 will be used), and then click the **Trusted Root Certificates** link, located at the bottom of the TLS Contexts page; the Trusted Certificates page appears.
3. Click the **Import** button, and then select the certificate file to load.

Figure B-5: Importing the BroadCloud Root Certificate into Trusted Certificates Store

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

International Headquarters

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

AudioCodes Inc.

200 Cottontail Lane
Suite A101E
Somerset NJ 08873
Tel: +1-732-469-0880
Fax: +1-732-469-2298

Contact us: <https://www.audiocodes.com/corporate/offices-worldwide>

website: <https://www.audiocodes.com/>

©2018 AudioCodes Ltd. All rights reserved. AudioCodes, AC, HD VoIP, HD VoIP Sounds Better, IPmedia, Mediant, MediaPack, What's Inside Matters, OSN, SmartTAP, User Management Pack, VMAS, VoIPerfect, VoIPerfectHD, Your Gateway To VoIP, 3GX, VocaNom, AudioCodes One Voice and CloudBond are trademarks or registered trademarks of AudioCodes Limited. All other products or trademarks are property of their respective owners. Product specifications are subject to change without notice.

Document #: LTRT-12557

