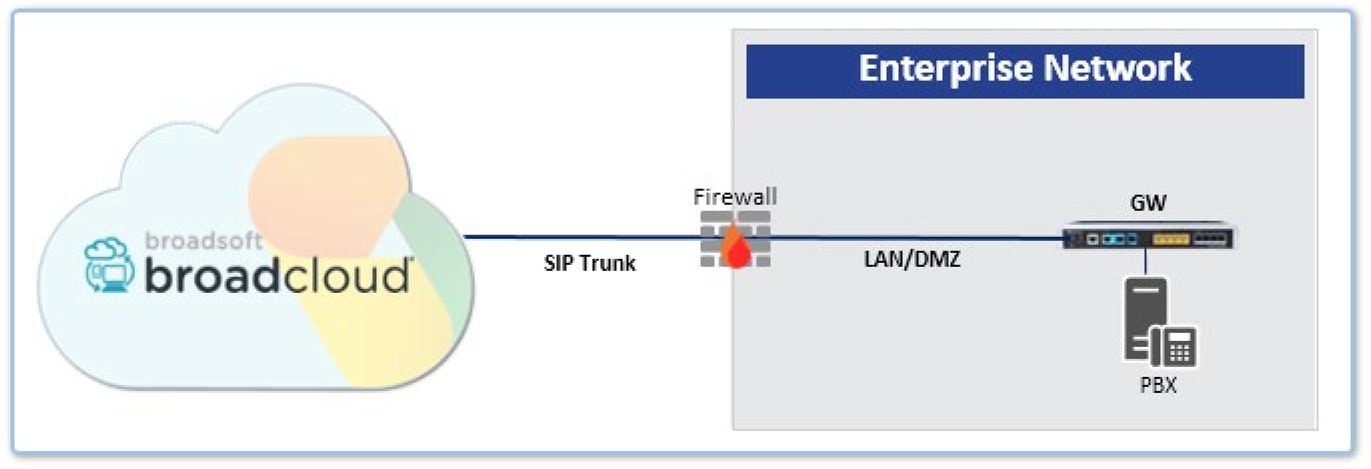
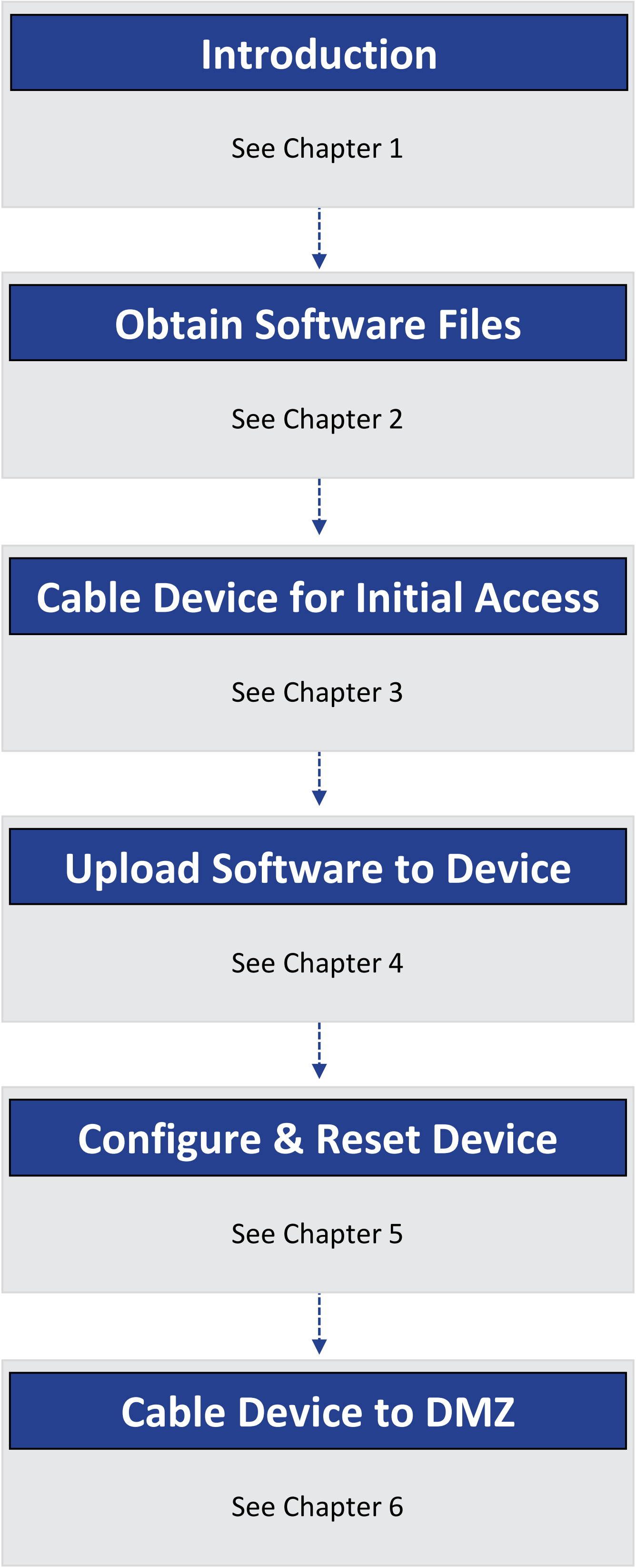
Quick Guide

AudioCodes Mediant™ Series BRI/PRI Media Gateways

Connecting PBX to BroadSoft's BroadCloud SIP Trunk using AudioCodes Mediant BRI/PRI Gateway



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' Mediant BRI/PRI Gateway for interworking between BroadCloud's SIP Trunk and PBX environment. For detailed information on each AudioCodes Mediant, refer to the corresponding *User's Manual* and *Hardware Installation Manual*.

1.1 Component Information

AudioCodes Mediant Gateway Version	
Gateway Vendor	AudioCodes
Models	Mediant 500L; Mediant 500; Mediant 800;
Software Version	7.20A.204.222
Protocol	▪ SIP/UDP or SIP/TCP or SIP/TLS for signaling and RTP or SRTP for media (to the BroadCloud SIP Trunk) ▪ BRI/PRI (to the 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.

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 Mediant, 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

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

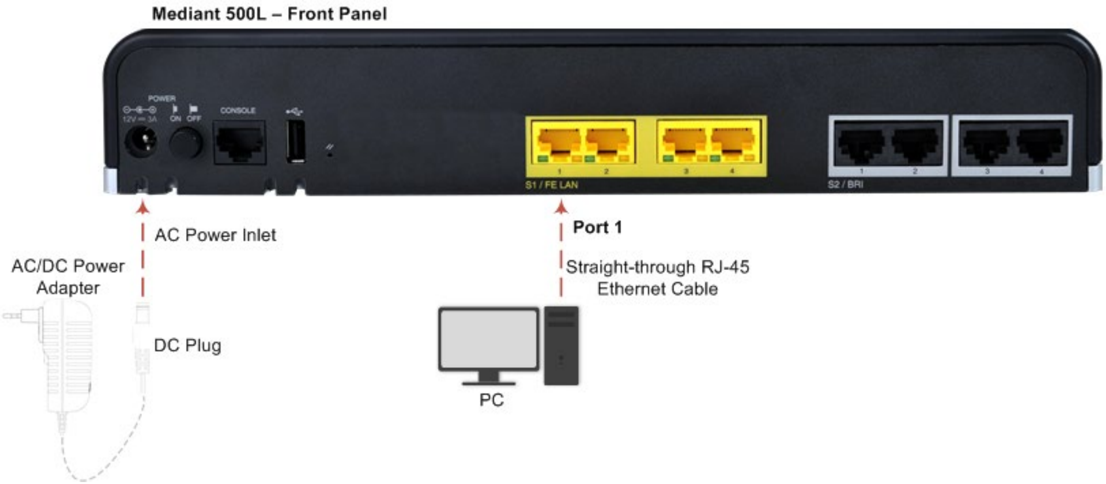


Figure 3-2: Mediant 500 Front Panel

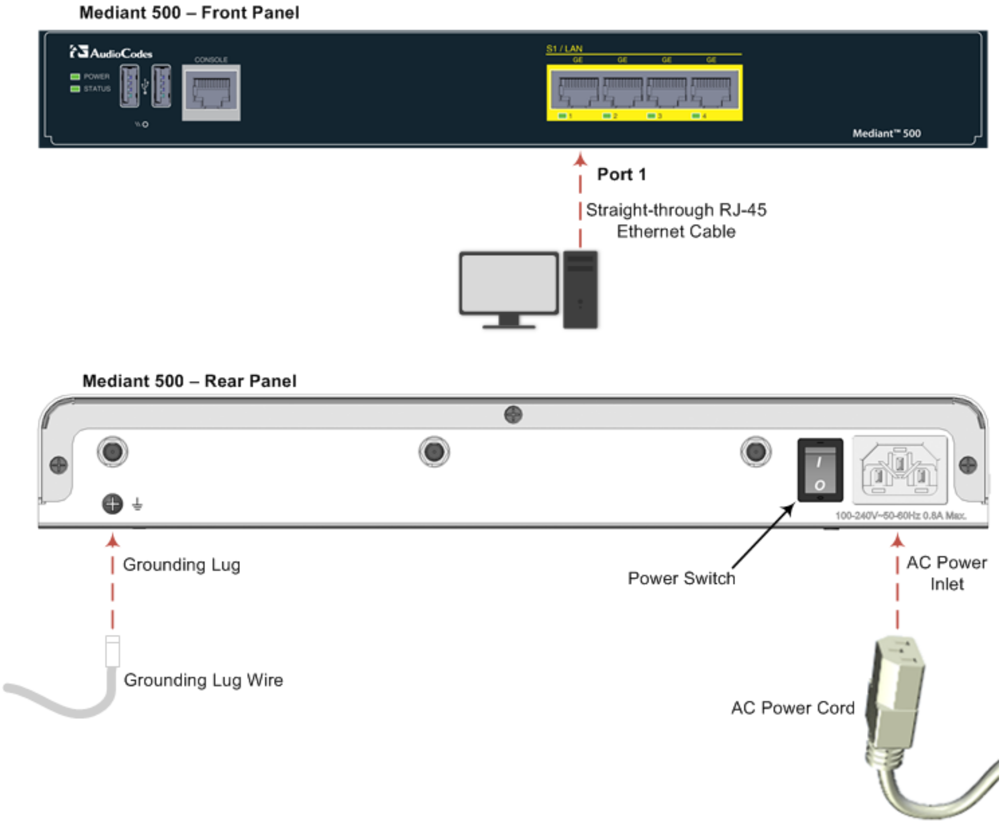
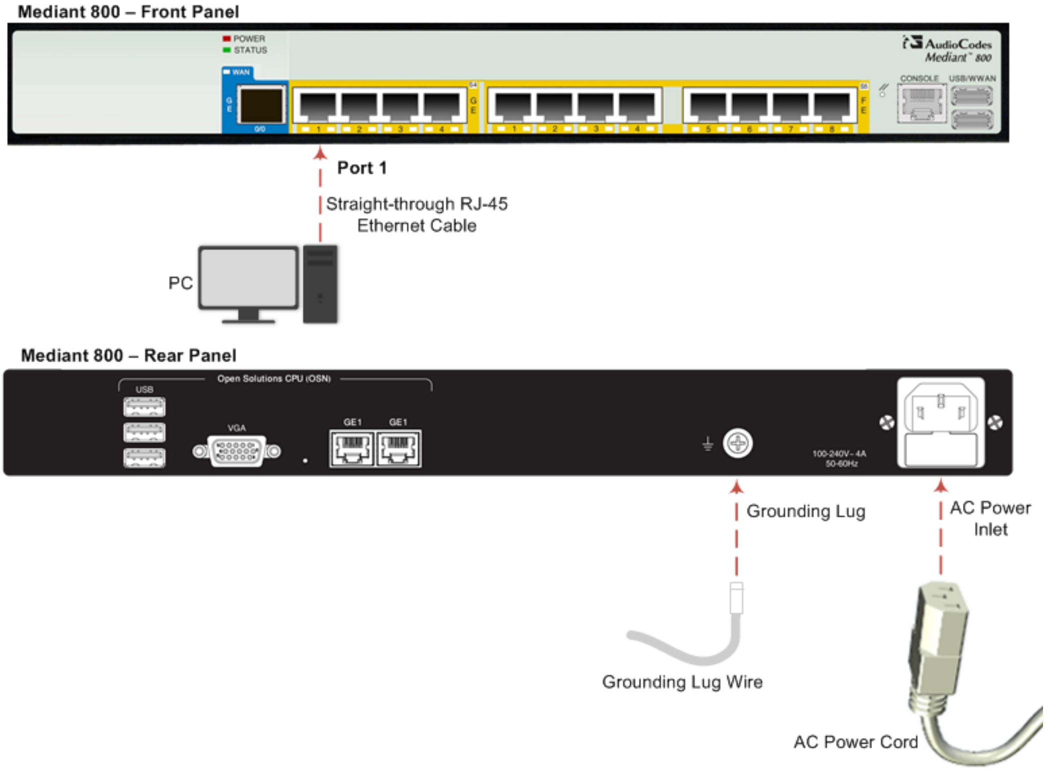


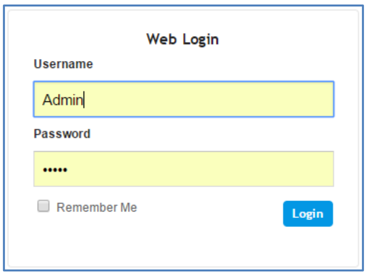
Figure 3-3: Mediant 800 Front Panel



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 3-4: Web Login



Web Login

Username

Admin

Password

•••••

□ Remember Me

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

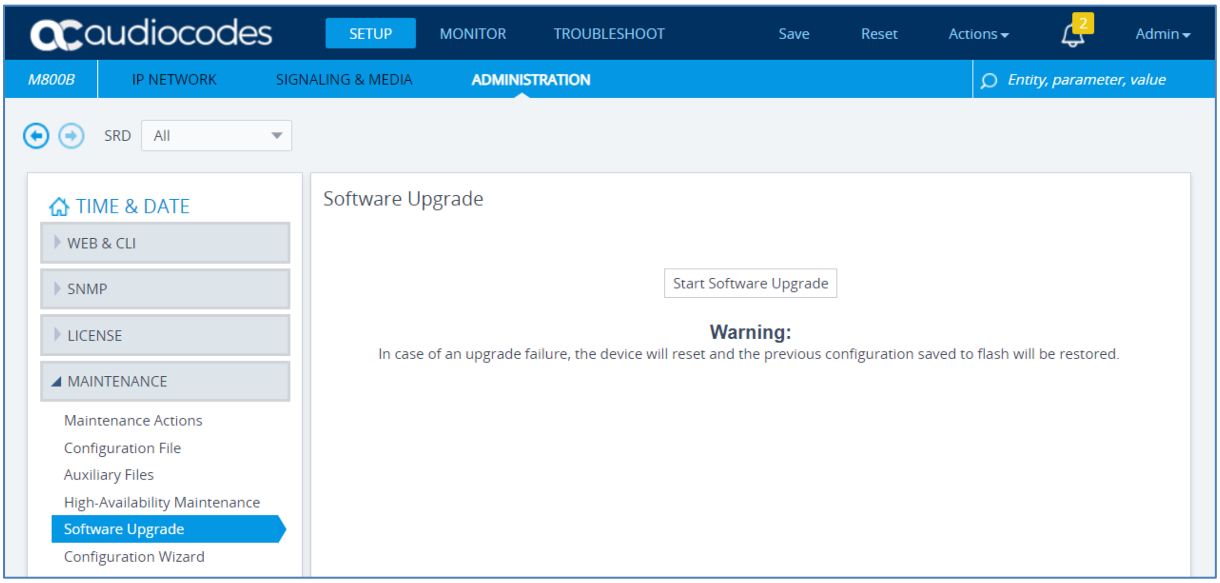
4 Upload Software to Device

Upload the certified software files, which you downloaded in Section Obtain Software Files, to the device:

1. 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**.

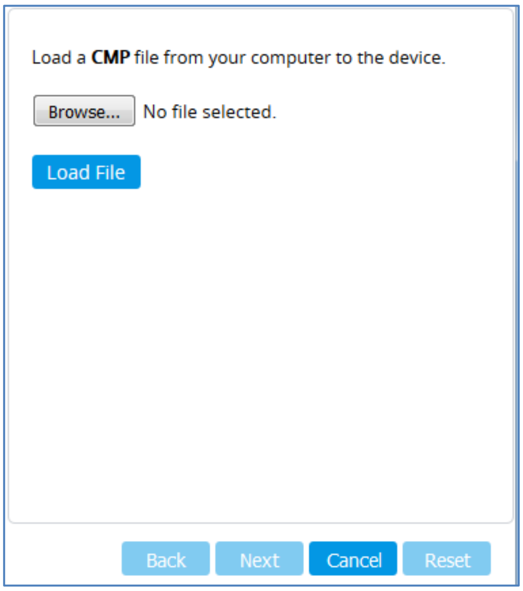
Figure 4-1: Device Setup



Warning:
In case of an upgrade failure, the device will reset and the previous configuration saved to flash will be restored.

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

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

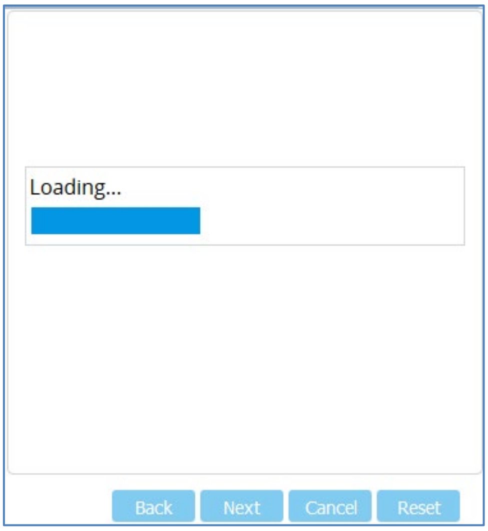


Load a **CMP** file from your computer to the device.

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.

3. Click **Browse**, and then navigate to and select the .cmp file.
4. Click **Load File**; the device begins to install the .cmp file and a progress bar displays the status of the loading process:

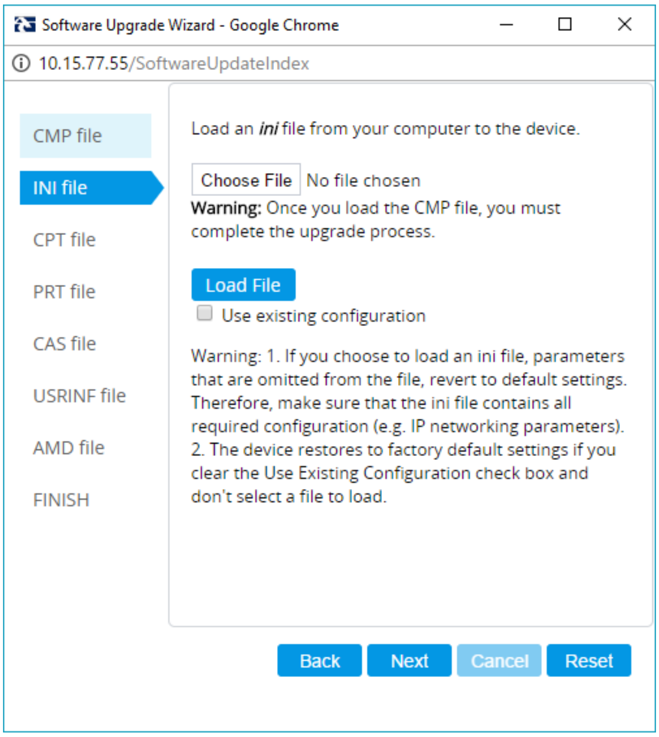
Figure 4-3: CMP File Loading Progress Bar



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

5. When successfully loaded, click **Next** to access the wizard page for loading the *ini* file.
6. 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



Load an *ini* file from your computer to the device.

No file chosen

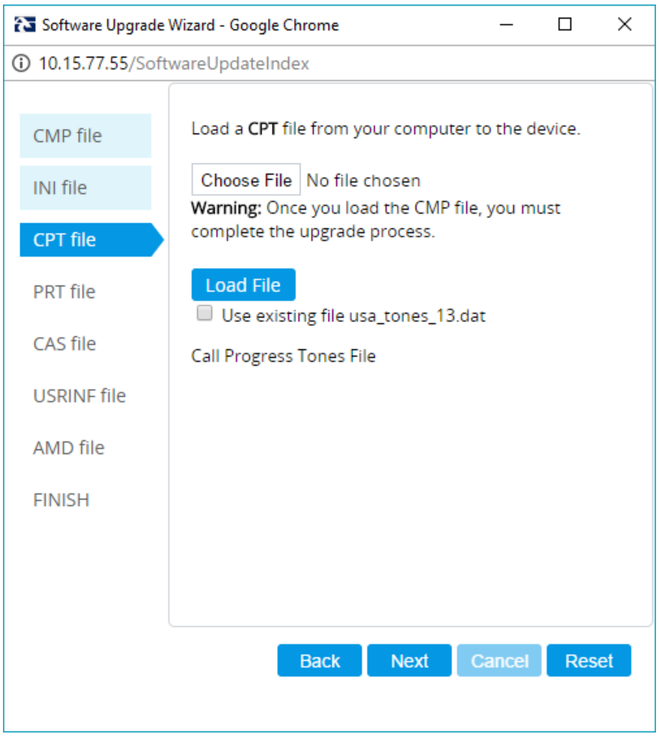
Warning: Once you load the CMP file, you must complete the upgrade process.

□ Use existing configuration

Warning: 1. If you choose to load an ini file, parameters that are omitted from the file, revert to default settings. Therefore, make sure that the ini file contains all required configuration (e.g. IP networking parameters). 2. The device restores to factory default settings if you clear the Use Existing Configuration check box and don't select a file to load.

7. Click **Next** to access the wizard page for loading the Call Progress Tones (CPT) file.
8. 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



Load a **CPT** file from your computer to the device.

No file chosen

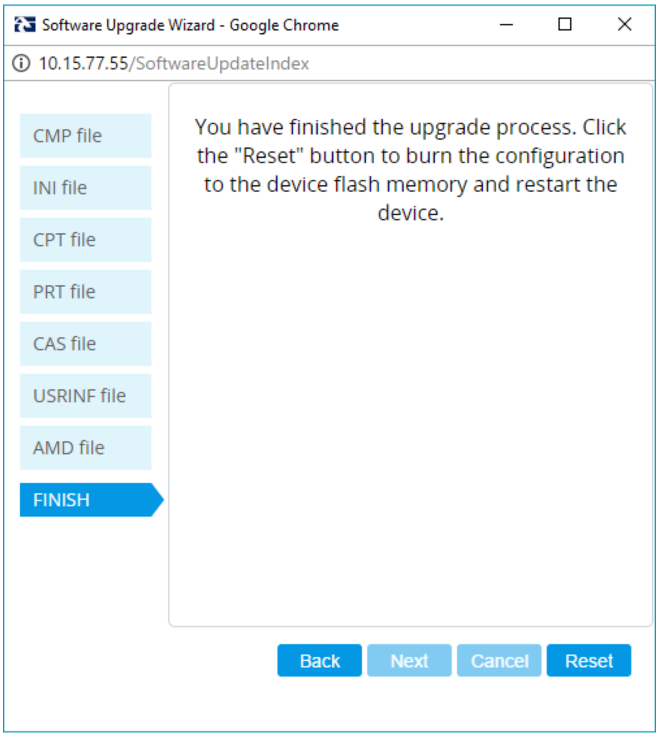
Warning: Once you load the CMP file, you must complete the upgrade process.

□ Use existing file usa_tones_13.dat

Call Progress Tones File

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

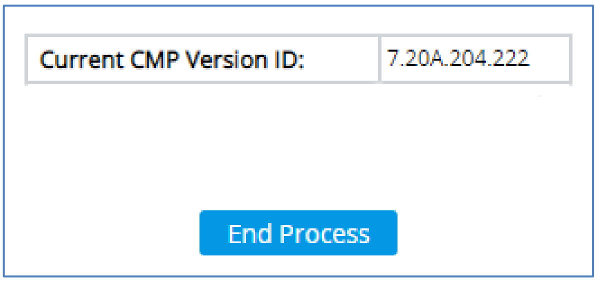
Figure 4-6: Finish



You have finished the upgrade process. Click the "Reset" button to burn the configuration to the device flash memory and restart the device.

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



Current CMP Version ID: 7.20A.204.222

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

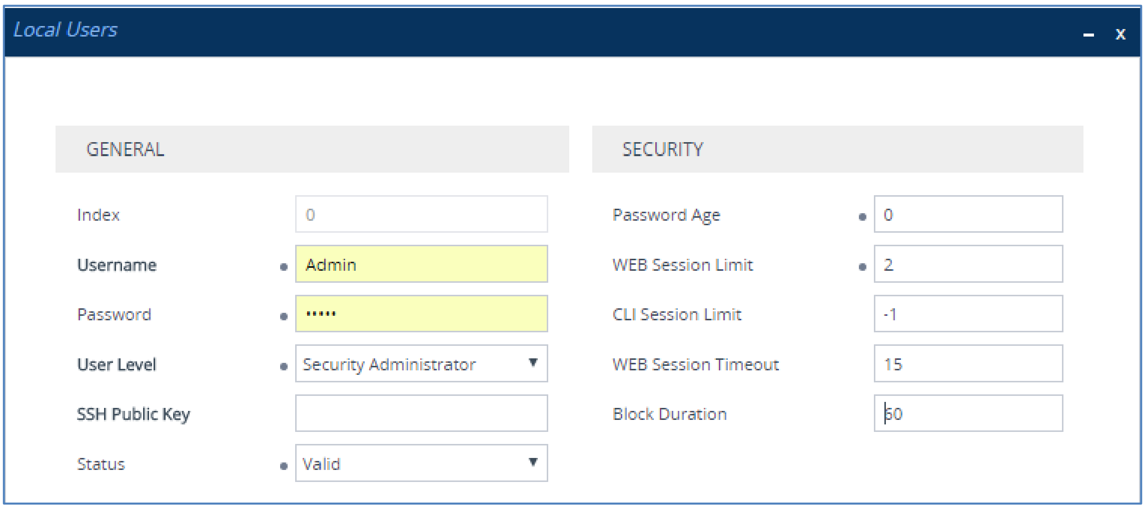
This section describes device configuration.

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



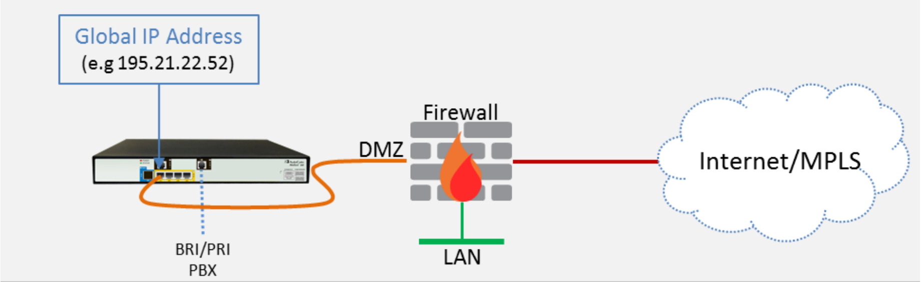
GENERAL		SECURITY	
Index	0	Password Age ●	0
Username ●	Admin	WEB Session Limit ●	2
Password ●	•••••	CLI Session Limit	-1
User Level ●	Security Administrator ▼	WEB Session Timeout	15
SSH Public Key		Block Duration	60
Status ●	Valid ▼		

- 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:

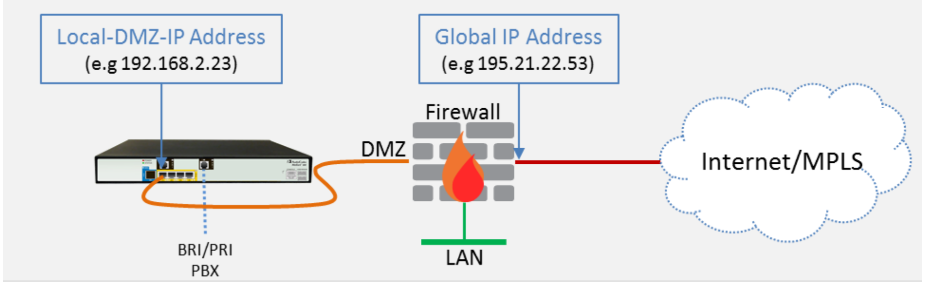
- **Method A**: (Preferred method) A global IP address is provided to the device (**without NAT**):



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 IP Address (public address)	<any> (e.g. ITSP)	<as original>

5.2.1 Configure Network Interface

Configure network interface for the DMZ/WAN (BroadCloud SIP-Trunk) interface, as described below:

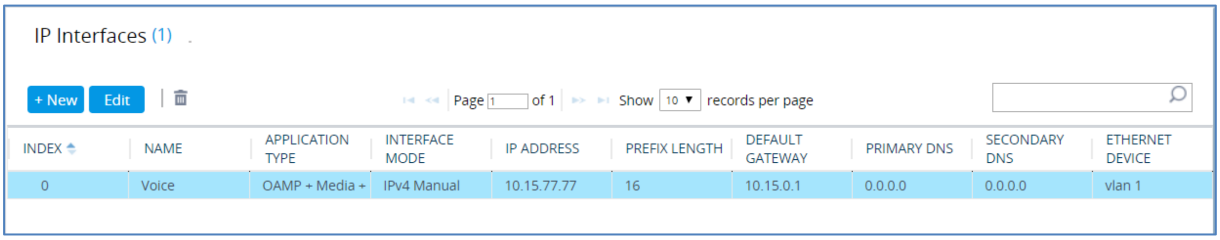
1. Open the IP Interfaces table (**Setup** menu > **IP Network** tab > **Core Entities** folder > **IP Interfaces**).
2. Configure the DMZ/WAN (BroadCloud SIP-Trunk) interface:
   a. Select the 'Index 0' radio button of the **OAMP + Media + Control** table row, and then click **Edit**. This is the existing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

Parameter	Value
Name	**Voice** (descriptive name, you may change it)
Application Type	**OAMP + Media + Control** (leave as is)
Ethernet Device	**vlan 1**
IP Address	▪ Method A: Global-IP-Address (public address) ▪ Method B: 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. Click **Apply**.

An example of configured IP network interfaces is shown below:

Figure 5-2: IP Network Interfaces



IP Interfaces (1)

INDEX	NAME	APPLICATION TYPE	INTERFACE MODE	IP ADDRESS	PREFIX LENGTH	DEFAULT GATEWAY	PRIMARY DNS	SECONDARY DNS	ETHERNET DEVICE
0	Voice	OAMP + Media +	IPv4 Manual	10.15.77.77	16	10.15.0.1	0.0.0.0	0.0.0.0	vlan 1

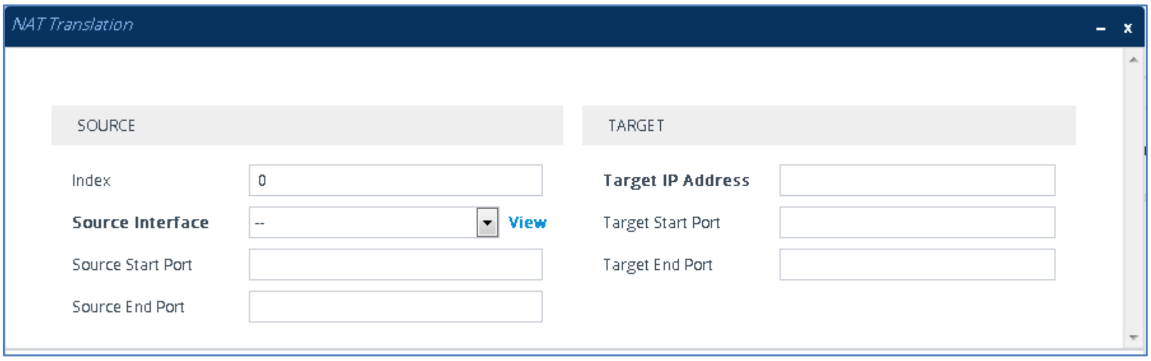
5.2.2 Configure NAT

> **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 Mediant 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

Index: 0

Source Interface: -- View

Source Start Port:

Source End Port:

TARGET

Target IP Address:

Target Start Port:

Target End Port:

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

Parameter	Description
Index	**0**
Source Interface	**Voice** (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)

3. Click **Apply**.

5.3 Configure PSTN Trunk Settings

This section shows how to configure PSTN (BRI/PRI) trunk settings.

> **Note:** Before configuring PSTN settings, collect all information about configuration on the other side (PBX configuration) which is necessary for the appropriate Mediant PSTN settings.

5.3.1 Configure the BRI PSTN Interface

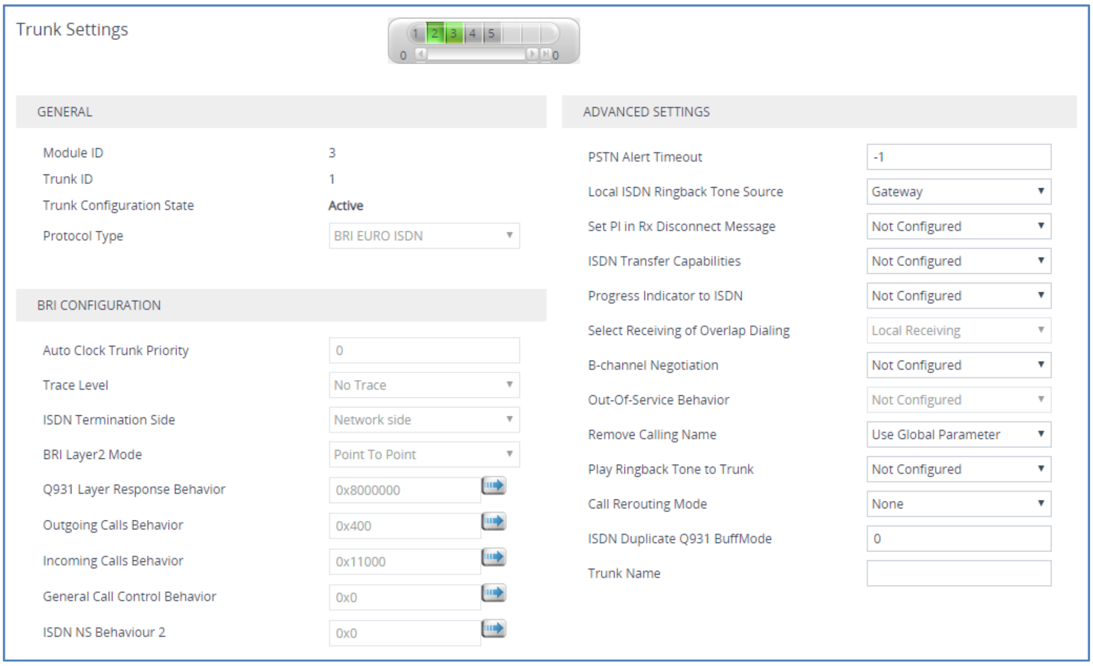
This section shows how to configure the BRI PSTN Interface. Skip to the next section if you have a PRI interface.

➢ **To configure the BRI PSTN interface:**

1. Open the Trunk Settings page (**Setup** menu > **Signaling & Media** tab > **Gateway** folder > **Trunks & Groups** > **Trunks**).
2. Configure following parameters:

Parameter	Value
Protocol Type	**BRI EURO ISDN** (according to PBX definitions)
ISDN Termination Side	**Network side** (for BRI PBX connection)
BRI Layer2 Mode	**Point To Point**
Q931 Layer Response Behavior	**0x8000000**
Outgoing Calls Behavior	**0x400**
Incoming Calls Behavior	**0x11000**
Select Receiving of Overlap Dialing	**Local Receiving**

Figure 5-4: Configuring BRI PSTN Interface



Trunk Settings

GENERAL

Module ID	3
Trunk ID	1
Trunk Configuration State	Active
Protocol Type	BRI EURO ISDN

BRI CONFIGURATION

Auto Clock Trunk Priority	0
Trace Level	No Trace
ISDN Termination Side	Network side
BRI Layer2 Mode	Point To Point
Q931 Layer Response Behavior	0x8000000
Outgoing Calls Behavior	0x400
Incoming Calls Behavior	0x11000
General Call Control Behavior	0x0
ISDN NS Behaviour 2	0x0

ADVANCED SETTINGS

PSTN Alert Timeout	-1
Local ISDN Ringback Tone Source	Gateway
Set PI in Rx Disconnect Message	Not Configured
ISDN Transfer Capabilities	Not Configured
Progress Indicator to ISDN	Not Configured
Select Receiving of Overlap Dialing	Local Receiving
B-channel Negotiation	Not Configured
Out-Of-Service Behavior	Not Configured
Remove Calling Name	Use Global Parameter
Play Ringback Tone to Trunk	Not Configured
Call Rerouting Mode	None
ISDN Duplicate Q931 BuffMode	0
Trunk Name	

3. Repeat for all BRI ports available on the device (Mediant 500L)

5.3.2 Configure the PRI PSTN Interface

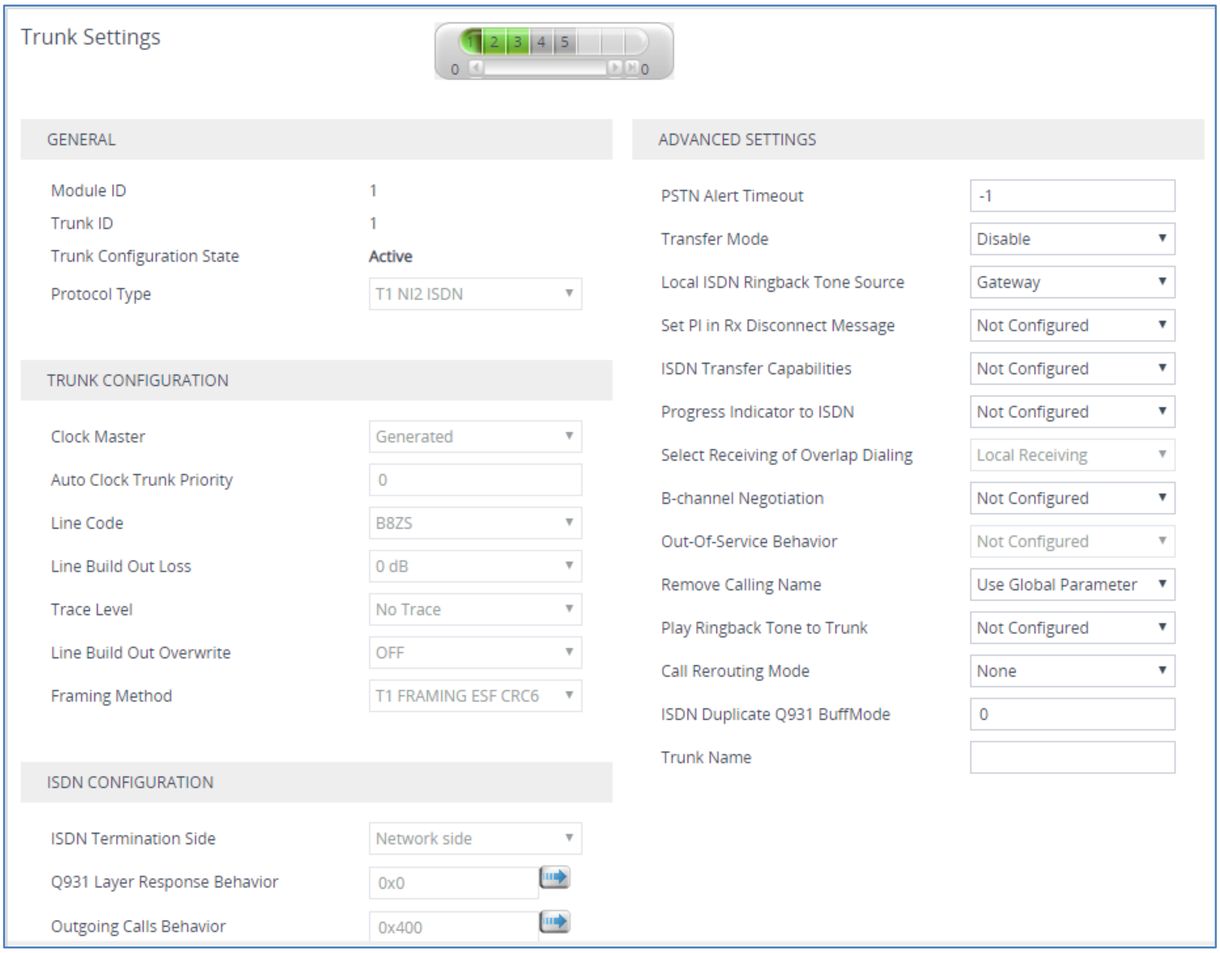
This section shows how to configure the PRI PSTN Interface.

➢ **To configure the PRI PSTN interface:**

1. Open the Trunk Settings page (**Setup** menu > **Signaling & Media** tab > **Gateway** folder > **Trunks & Groups** > **Trunks**).
2. Configure following parameters:

Parameter	Value
Protocol Type	**T1 NI2 ISDN** (according to PBX definitions)
Clock Master	**Generated** (The device is clock master) **Recovered** (The device slaves from the line clock)
Framing Method	**T1 Framing ESF CRC6** (according to PBX definitions)
ISDN Termination Side	**Network side** or **User side**

Figure 5-5: Configuring the PRI PSTN Interface



Trunk Settings

GENERAL

Module ID	1
Trunk ID	1
Trunk Configuration State	Active
Protocol Type	T1 NI2 ISDN

TRUNK CONFIGURATION

Clock Master	Generated
Auto Clock Trunk Priority	0
Line Code	B8ZS
Line Build Out Loss	0 dB
Trace Level	No Trace
Line Build Out Overwrite	OFF
Framing Method	T1 FRAMING ESF CRC6

ISDN CONFIGURATION

ISDN Termination Side	Network side
Q931 Layer Response Behavior	0x0
Outgoing Calls Behavior	0x400

ADVANCED SETTINGS

PSTN Alert Timeout	-1
Transfer Mode	Disable
Local ISDN Ringback Tone Source	Gateway
Set PI in Rx Disconnect Message	Not Configured
ISDN Transfer Capabilities	Not Configured
Progress Indicator to ISDN	Not Configured
Select Receiving of Overlap Dialing	Local Receiving
B-channel Negotiation	Not Configured
Out-Of-Service Behavior	Not Configured
Remove Calling Name	Use Global Parameter
Play Ringback Tone to Trunk	Not Configured
Call Rerouting Mode	None
ISDN Duplicate Q931 BuffMode	0
Trunk Name	

3. Repeat for all PRI ports available on the device (Mediant 800B).

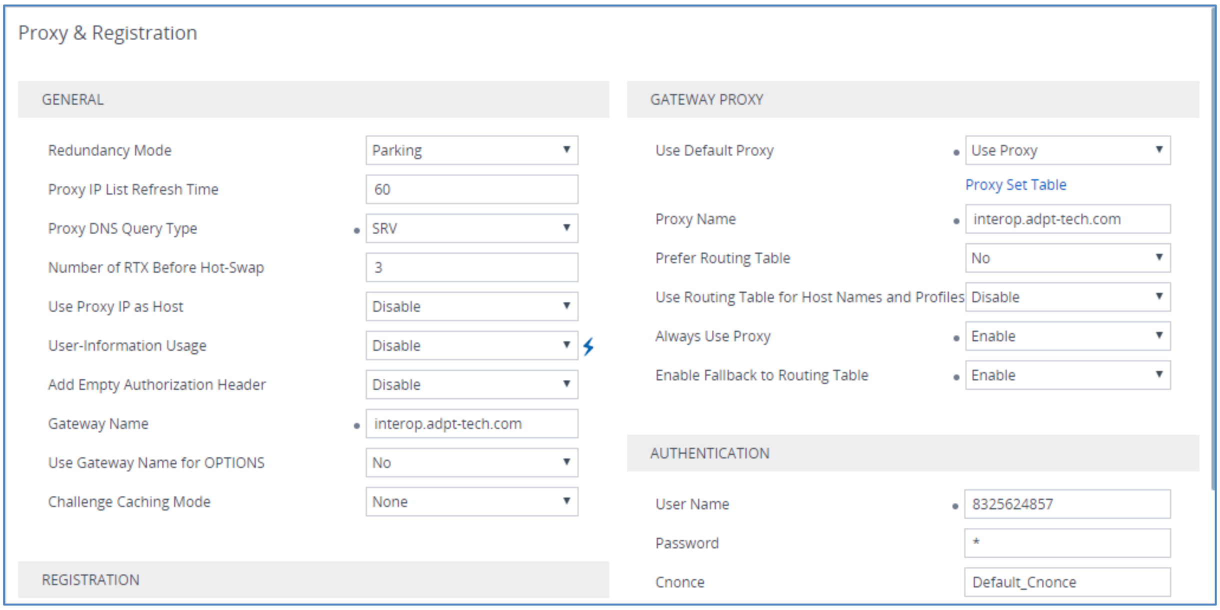
5.4 Configure Registration Parameters

This section shows how to configure the SIP Proxy and Registration parameters, including configuring a Proxy Name, Registrar Name, DNS query for the BroadCloud Proxy Set, Registration and Subscription modes.

➢ To configure the SIP Proxy & Registration parameters:

1. Open the Proxy & Registration page (**Setup** menu > **Signaling & Media** tab > **SIP Definitions** folder > **Proxy & Registration**).

Figure 5-6: Configuring Proxy & Registration Parameters



Proxy & Registration

GENERAL

Redundancy Mode	Parking
Proxy IP List Refresh Time	60
Proxy DNS Query Type	SRV
Number of RTX Before Hot-Swap	3
Use Proxy IP as Host	Disable
User-Information Usage	Disable
Add Empty Authorization Header	Disable
Gateway Name	interop.adpt-tech.com
Use Gateway Name for OPTIONS	No
Challenge Caching Mode	None

REGISTRATION

GATEWAY PROXY

Use Default Proxy	Use Proxy
	Proxy Set Table
Proxy Name	interop.adpt-tech.com
Prefer Routing Table	No
Use Routing Table for Host Names and Profiles	Disable
Always Use Proxy	Enable
Enable Fallback to Routing Table	Enable

AUTHENTICATION

User Name	8325624857
Password	*
Cnonce	Default_Cnonce

2. From the 'Proxy DNS Query Type' dropdown, select **SRV**.
3. For 'gateway Name', enter the domain name that can be found on the BroadCloud MySite Trunk Group configuration page, under the section 'Trunk Group Settings'.
4. From the 'Use Default Proxy' dropdown, select **Yes**.
5. For 'Proxy Name', enter the domain name that can be found on the BroadCloud MySite Trunk Group configuration page, under the section 'Trunk Group Settings'.
6. From the 'Always Use Proxy' dropdown, select **Enable**.
7. From the 'Enable Fallback to Routing Table' dropdown, select **Enable** (when PSTN Fallback is implemented on the Mediant Gateway).
8. In the 'User Name' field, configure **Trunk Group Pilot User**.
9. In the 'Password' field, configure **Trunk Group Pilot User Password**.
10. From the 'Enable Registration' dropdown, select **Enable**.
11. For 'Registrar Name', enter the domain name that can be found on the BroadCloud MySite Trunk Group configuration page, under the section 'Trunk Group Settings'.
12. Click **Apply**.

5.5 Configure Trunk Group Parameters

Note: This configuration is by default correct and should only be verified.

This section shows how to configure the device's channels, which includes assigning them to Trunk Groups. A Trunk Group is a logical group of physical trunks and channels. A Trunk Group can include multiple trunks and ranges of channels. To enable and activate the device's channels, Trunk Groups must be configured. Channels not configured in this table are disabled. After configuring Trunk Groups, use them to route incoming IP calls to the Tel side, represented by a specific Trunk Group (ID). You can also use Trunk Groups for routing Tel calls to the IP side.

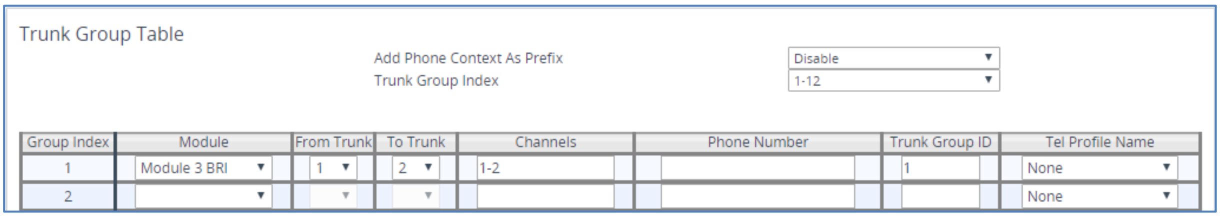
5.5.1 Configure the BRI Trunk Group (for Devices with BRI)

This section shows how to configure the BRI Trunk Group. If your device does not have BRI, skip this step.

➢ **To configure the BRI Trunk Group Table:**

1. Open the Trunk Group table (**Setup** menu > **Signaling & Media** tab > **Gateway** folder > **Trunks & Groups** > **Trunk Groups**).

Figure 5-7: Configuring BRI Trunk Group Table



Trunk Group Table

Add Phone Context As Prefix: Disable

Trunk Group Index: 1-12

Group Index	Module	From Trunk	To Trunk	Channels	Phone Number	Trunk Group ID	Tel Profile Name
1	Module 3 BRI	1	2	1-2		1	None
2							None

2. Configure each Trunk Group as required. If more than one BRI port is available, set “To Trunk” to the last BRI port to be used for incoming / outgoing calls between BroadCloud service and the PBX.

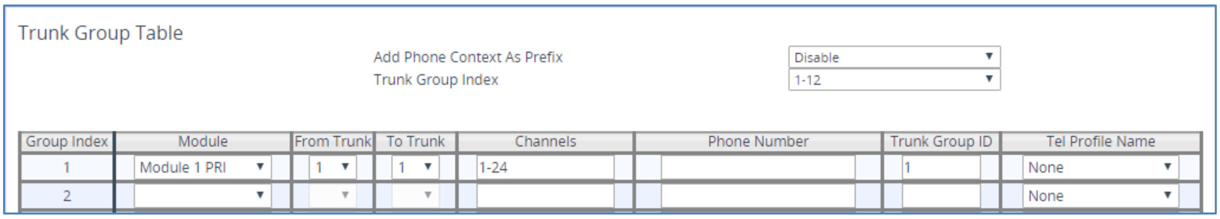
5.5.2 Configure the PRI Trunk Group (for Devices with PRI)

This section shows how to configure the PRI Trunk Group. If your device does not have PRI, skip this step.

➢ **To configure the PRI Trunk Group Table:**

1. Open the Trunk Group table (**Setup** menu > **Signaling & Media** tab > **Gateway** folder > **Trunks & Groups** > **Trunk Groups**).

Figure 5-8: Configuring PRI Trunk Group Table



Trunk Group Table

Add Phone Context As Prefix: Disable

Trunk Group Index: 1-12

Group Index	Module	From Trunk	To Trunk	Channels	Phone Number	Trunk Group ID	Tel Profile Name
1	Module 1 PRI	1	1	1-24		1	None
2							None

2. Configure each Trunk Group as required. If more than one PRI port is available, set 'To Trunk' to the last PRI port to be used for incoming / outgoing calls between BroadCloud service and the PBX.

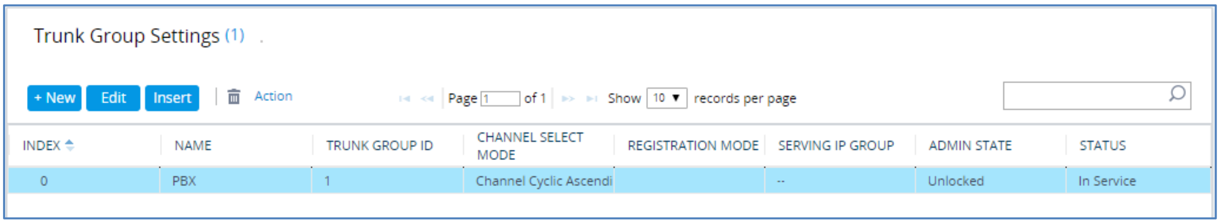
5.5.3 Configure Trunk Group Settings

The Trunk Group Settings page allows you to configure the Channel Select Mode by which IP-to-Tel calls are assigned to the Trunk Group's channels.

➢ **To configure the Trunk Group Settings:**

1. Open the Trunk Group Settings table (**Setup** menu > **Signaling & Media** tab > **Gateway** folder > **Trunks & Groups** > **Trunk Group Settings**).

Figure 5-9: Configuring Trunk Group Settings



INDEX	NAME	TRUNK GROUP ID	CHANNEL SELECT MODE	REGISTRATION MODE	SERVING IP GROUP	ADMIN STATE	STATUS
0	PBX	1	Channel Cyclic Ascendi		--	Unlocked	In Service

2. For each Trunk Group ID, from the 'Channel Select Mode' dropdown, select **Cyclic Ascending**.
3. Click **Apply** to apply your changes.

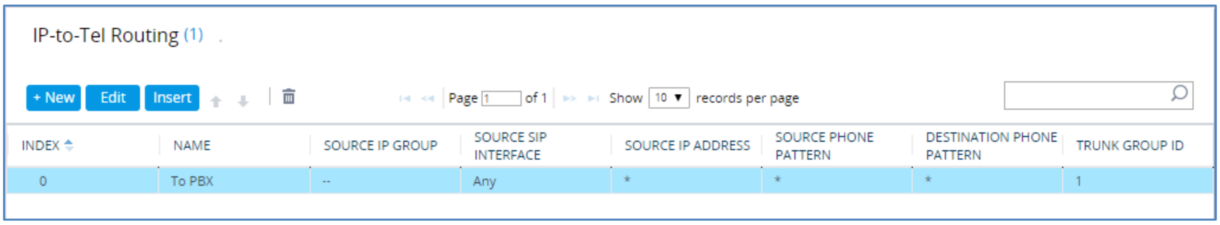
5.5.4 Configure Inbound IP Routing

This section shows configuring Mediant BRI/PRI Gateway Inbound (IP-to-Tel) Routing. When having more than one TDM interface (more than one BRI or PRI), you can choose to route calls based on incoming IP SIP call message to a specific TDM port i.e., Trunk Group.

➢ **To configure IP-to-Tel or Inbound IP Routing Rules:**

1. Open the IP-to-Tel Routing table (**Setup** menu > **Signaling & Media** tab > **Gateway** folder > **Routing** > **IP > Tel Routing**).

Figure 5-10: Configuring Inbound IP Routing Rules



INDEX	NAME	SOURCE IP GROUP	SOURCE SIP INTERFACE	SOURCE IP ADDRESS	SOURCE PHONE PATTERN	DESTINATION PHONE PATTERN	TRUNK GROUP ID
0	To PBX	--	Any	*	*	*	1

2. Configure a rule for all incoming IP calls, route them to **Trunk Group ID 1** (connected to the PBX).
3. Click **Apply** to apply definitions.

5.6 Configure the Number of Digits to be Present to the PBX (Optional)

This section shows how to configure the Mediant BRI/PRI Gateway's number manipulation rules, which implement on number of digits to be present to the PBX.
The number manipulation tables let you configure rules for manipulating source and destination telephone numbers for IP-to-Tel (BroadCloud to PBX) and Tel-to-IP (PBX-to-BroadCloud) calls. The number manipulation tables include the following:

- **Tel-to-IP calls:**
  - Source Phone Number Manipulation Table for Tel-to-IP Calls
  - Destination Phone Number Manipulation Table for Tel-to-IP Calls
- **IP-to-Tel calls:**
  - Source Phone Number Manipulation Table for IP-to-Tel Calls
  - Destination Phone Number Manipulation Table for IP-to-Tel Calls

Configuration of number manipulation rules includes two areas:

- **Match:** Defines the matching characteristics of the incoming call (e.g., prefix of destination number).
- **Action:** Defines the action that is done if the incoming call matches the characteristics of the rule (e.g., removes a user-defined number of digits from the left of the number).

Telephone number manipulation can be useful, for example, for the following:

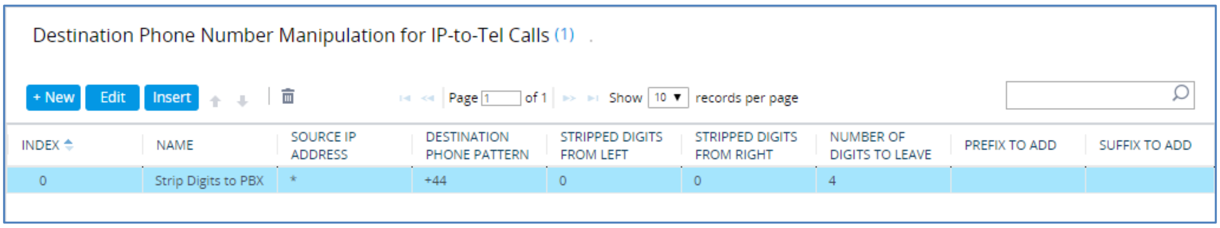
- Stripping or adding dialing plan digits from or to the number, respectively. For example, a user may need to first dial ‘9’ before dialing the phone number to indicate an external line. This number ‘9’ can then be removed by number manipulation before the call is setup.
- Allowing or blocking Caller ID information according to destination or source prefixes.
- Assigning Numbering Plan Indicator (NPI) and Type of Numbering (TON) to IP-to-Tel calls. The device can use a single global setting for NPI/TON classification or it can use the setting in the manipulation tables on a call-by-call basis.

The following procedure describes how to configure number manipulation rules in the Web interface.

➢ **To configure a number manipulation rule for IP-to-Tel:**

1. Open the required Phone Number Manipulation table (**Setup** menu > **Signaling & Media** tab > **Gateway** folder > **Manipulation** > **Dest Number IP->Tel**, **Dest Number Tel->IP**, **Source Number IP->Tel**, or **Source Number Tel->IP**).
2. Click **New** and configure a number manipulation rule according to PBX requirement:

Figure 5-11: Number Manipulation Table



Destination Phone Number Manipulation for IP-to-Tel Calls (1)

INDEX	NAME	SOURCE IP ADDRESS	DESTINATION PHONE PATTERN	STRIPPED DIGITS FROM LEFT	STRIPPED DIGITS FROM RIGHT	NUMBER OF DIGITS TO LEAVE	PREFIX TO ADD	SUFFIX TO ADD
0	Strip Digits to PBX	*	+44	0	0	4		

3. Click **Apply**.

The above example shows how to configure the Mediant BRI/PRI Gateway’s IP-to-Tel manipulation rule to strip digits from the ‘To’ SIP header and present only 4 digits to the PBX. In this case, when destination number has prefix +44 (e.g., +442079930256), all digits will be stripped except 4 from the right (0256).

5.7 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.

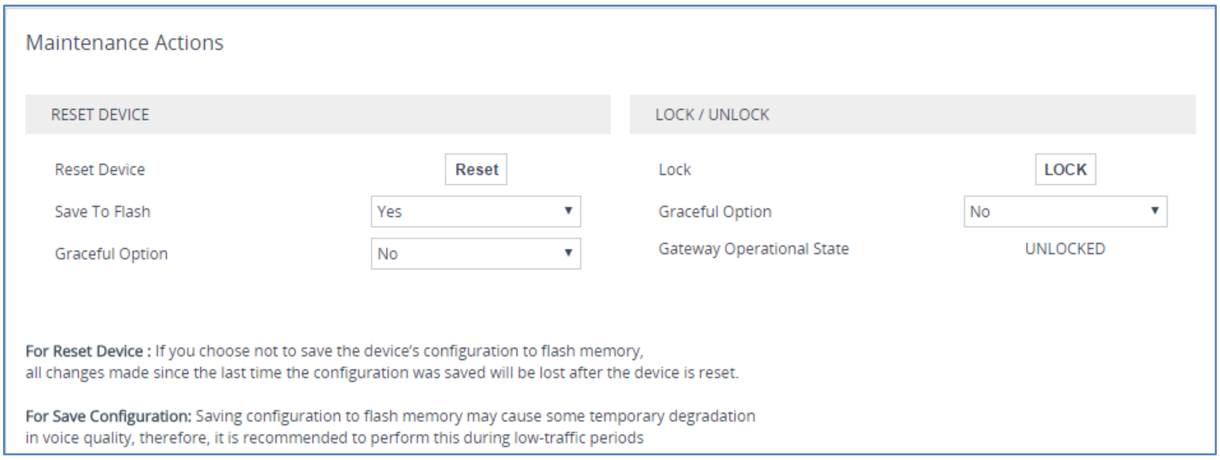
5.8 Save Configuration

> **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 5-12: Maintenance Actions



Maintenance Actions

RESET DEVICE

Reset Device: Reset

Save To Flash: Yes

Graceful Option: No

LOCK / UNLOCK

Lock: LOCK

Graceful Option: No

Gateway Operational State: UNLOCKED

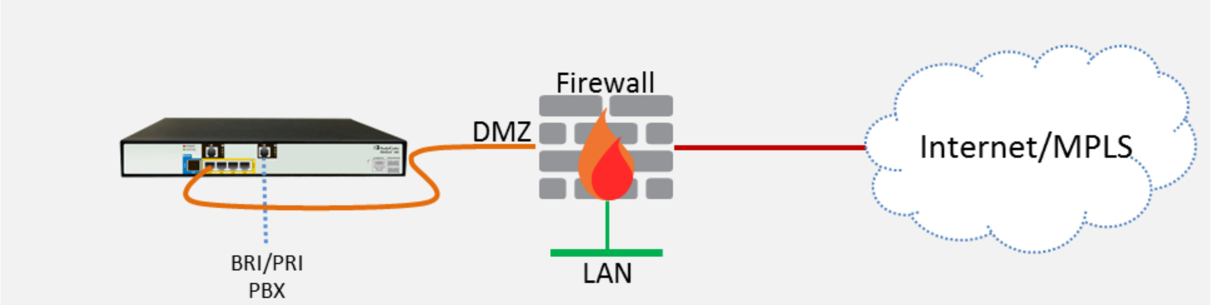
For Reset Device : If you choose not to save the device's configuration to flash memory, all changes made since the last time the configuration was saved will be lost after the device is reset.

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 BRI/PRI 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 PBX:
   a. For devices with BRI PSTN Interfaces, connect the RJ-45 cable to the device's BRI port (it's labeled S2 / BRI).
   b. For devices with PRI PSTN Interfaces, connect the E1/T1 trunk cable to the device’s E1/T1 port.
   c. Connect the other end of the cable to your ISDN PBX equipment.

Figure 6-2: Mediant 500L BRI Media Gateway

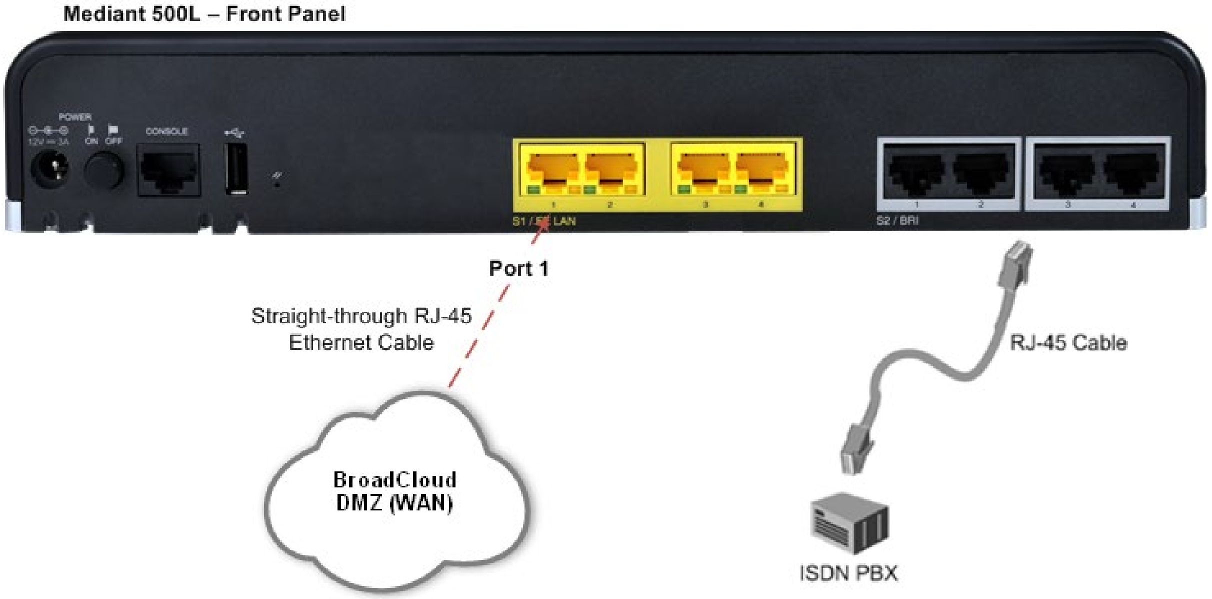


Figure 6-3: Mediant 500 PRI Media Gateway

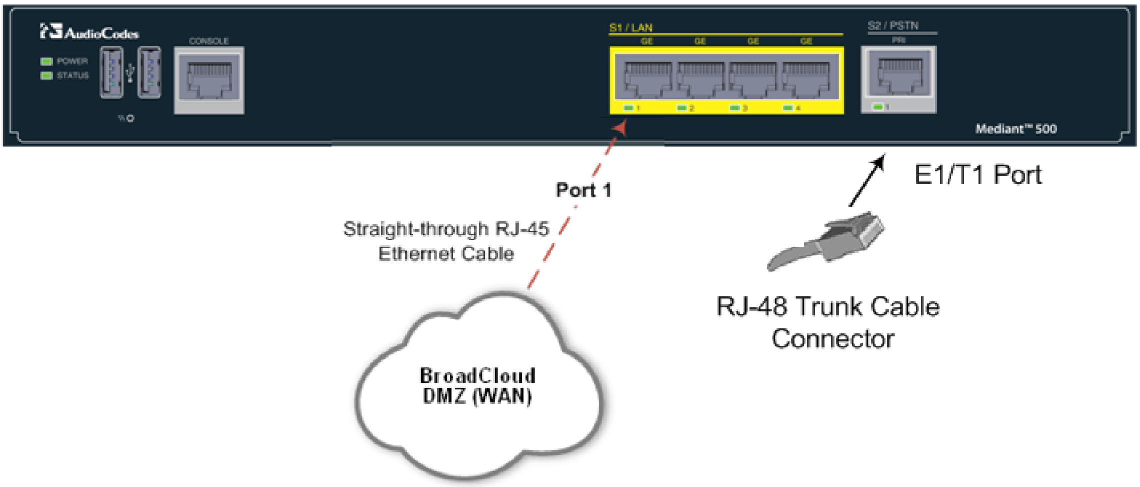
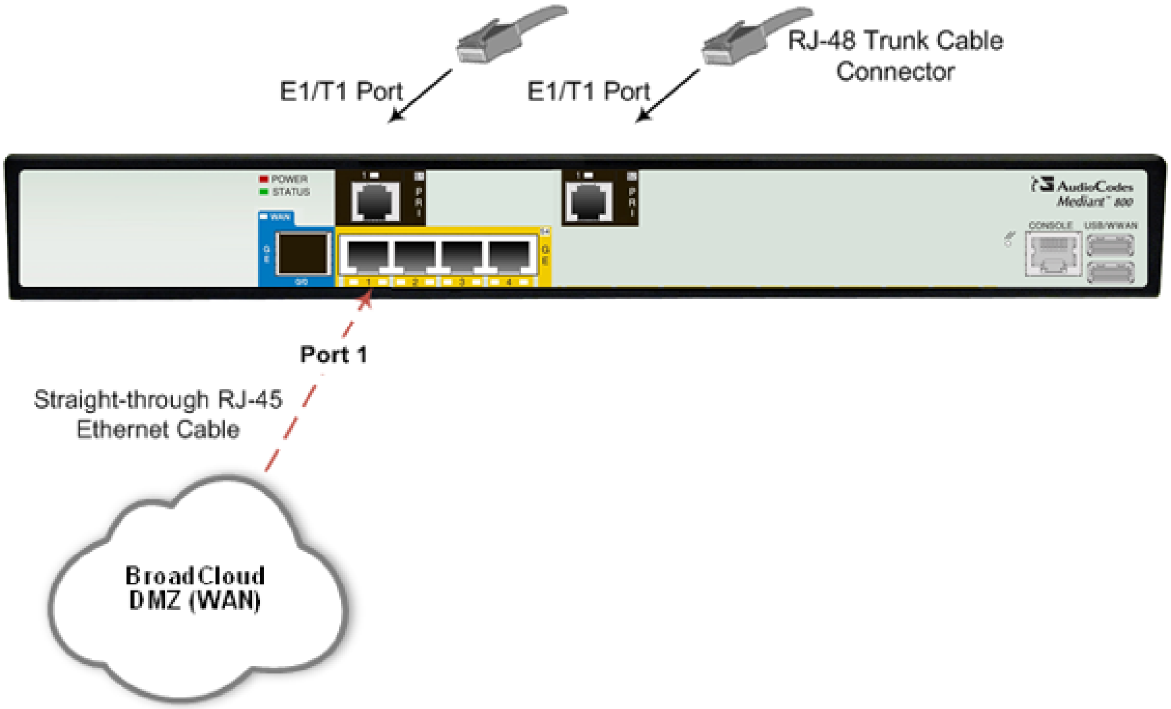


Figure 6-4: Mediant 800 BRI/PRI Media Gateway

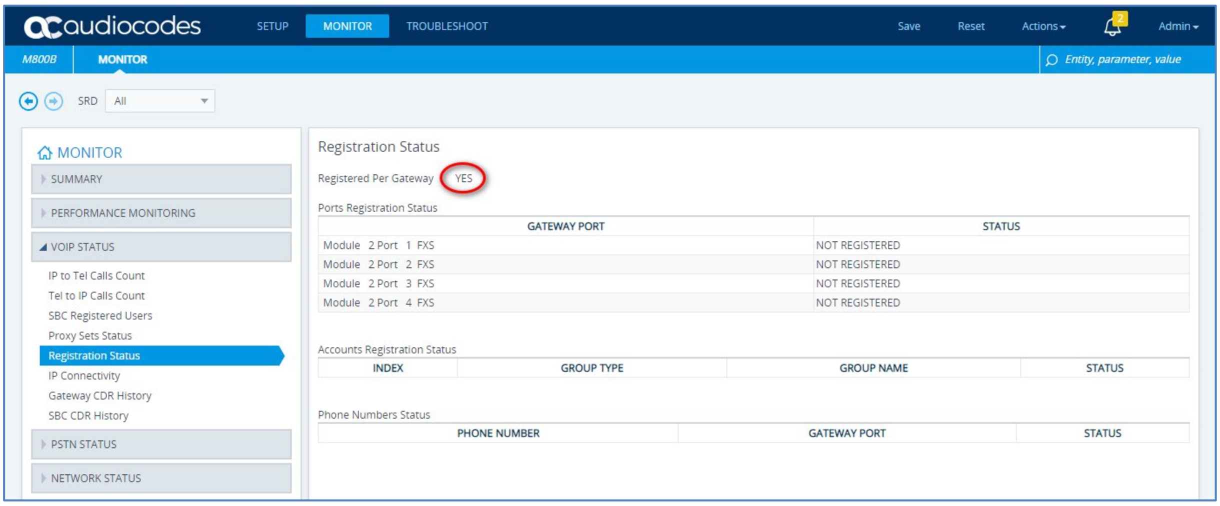


7 Verify SIP Trunk Registration Status

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. Check the registration status of the first row at the top of the screen: **Registered Per Gateway**. A successful registration will be displayed as YES (see the figure below).

Figure 7-1: SIP Trunk Registration Status



Registration Status

Registered Per Gateway YES

Ports Registration Status

GATEWAY PORT	STATUS
Module 2 Port 1 FXS	NOT REGISTERED
Module 2 Port 2 FXS	NOT REGISTERED
Module 2 Port 3 FXS	NOT REGISTERED
Module 2 Port 4 FXS	NOT REGISTERED

Accounts Registration Status

INDEX	GROUP TYPE	GROUP NAME	STATUS

Phone Numbers Status

PHONE NUMBER	GATEWAY PORT	STATUS

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

- Check the WAN wiring.
- Make sure the DMZ configuration is correct on the firewall (for example, port 8933 is open).
- Check the IP address configuration (**Setup** menu > **IP Network** tab > **Core Entities** folder > **IP Interfaces**).
- Check Proxy (SIP Trunk) configuration (**Setup** menu > **Signaling & Media** tab > **SIP Definitions** folder > **Proxy & Registration**).

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 BRI/PRI Gateway to work in secure mode (TLS/SRTP) towards BroadCloud SIP Trunk.

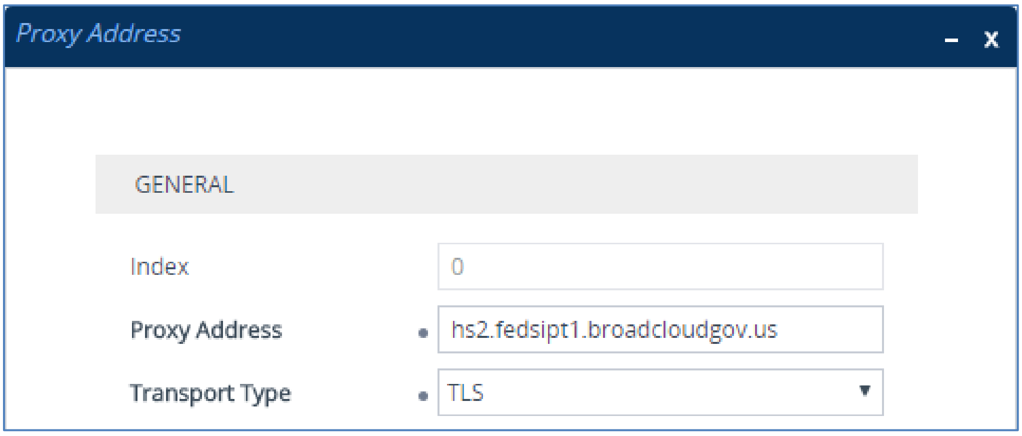
B.1 Change Signaling Connectivity to TLS

The Proxy Set configuration needs to be changed to move to TLS as transport type.

➢ **To change the Proxy Set:**

1. Open the Proxy Sets table (**Setup** menu > **Signaling & Media** tab > **Core Entities** folder >**Proxy Sets**).
2. Modify the default Proxy Set (Index 0). 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



Proxy Address

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**.

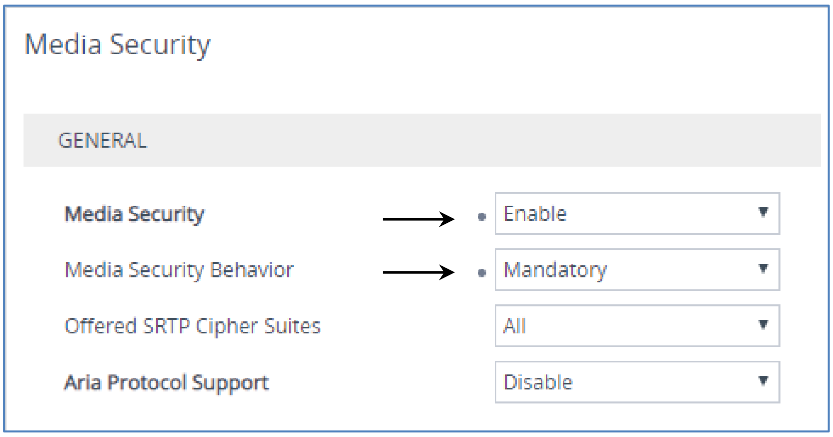
B.2 Configure SRTP

This section describes how to configure 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: Mandatory

Offered SRTP Cipher Suites: All

Aria Protocol Support: Disable

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

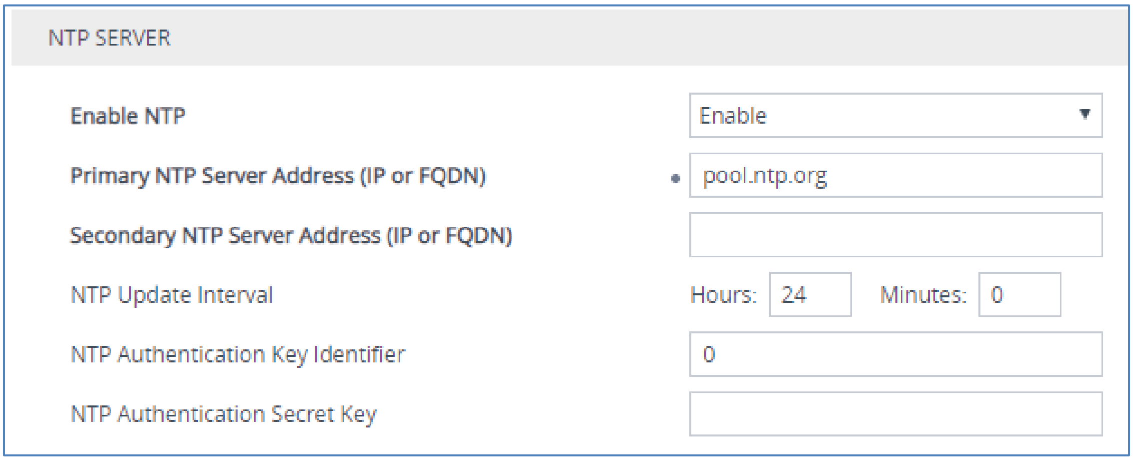
B.3 Configure the NTP Server Address

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 Gateway receives the accurate and current date and time. This is necessary for validating the 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-3: Configuring NTP Server Address



NTP SERVER

Enable NTP	Enable ▾
Primary NTP Server Address (IP or FQDN)	pool.ntp.org
Secondary NTP Server Address (IP or FQDN)	
NTP Update Interval	Hours: 24 Minutes: 0
NTP Authentication Key Identifier	0
NTP Authentication Secret Key	

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.

This procedure involves the following main steps:

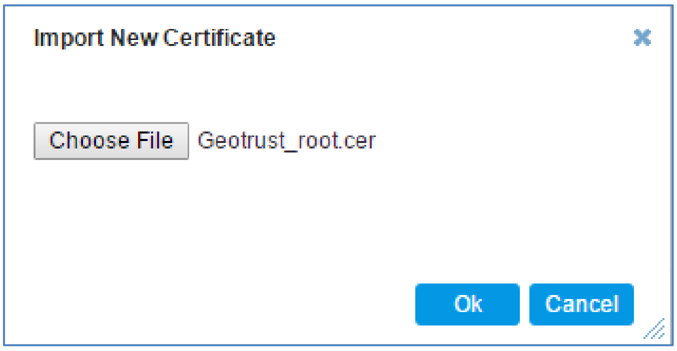
a. Obtaining a Trusted Root Certificate from the BroadCloud.

b. Deploying the BroadCloud Root Certificate as Trusted Root Certificates on the Mediant Gateway.

➢ **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-4: Importing the BroadCloud Root Certificate into Trusted Certificates Store



Import New Certificate

Choose File Geotrust_root.cer

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/