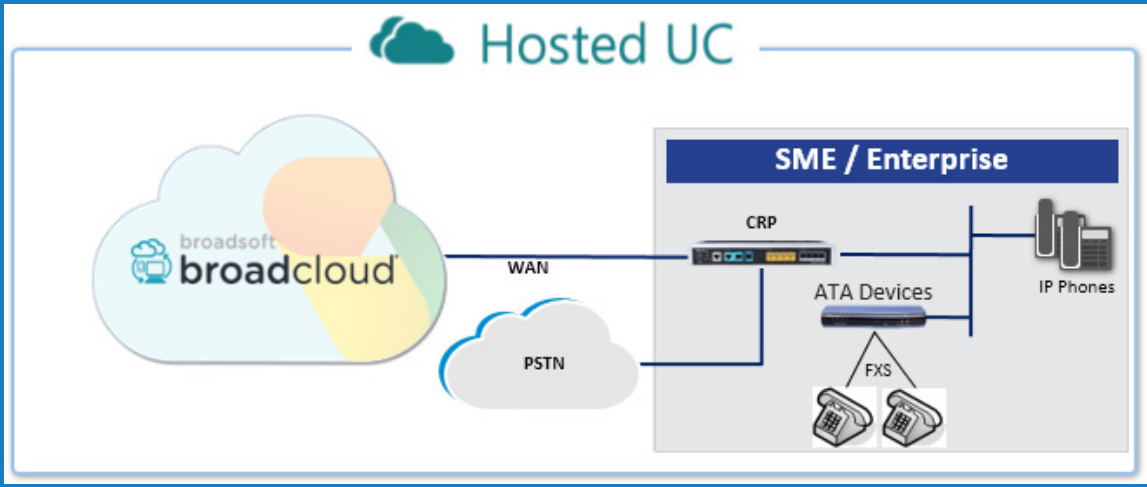
Quick Guide

AudioCodes Mediant™ Series

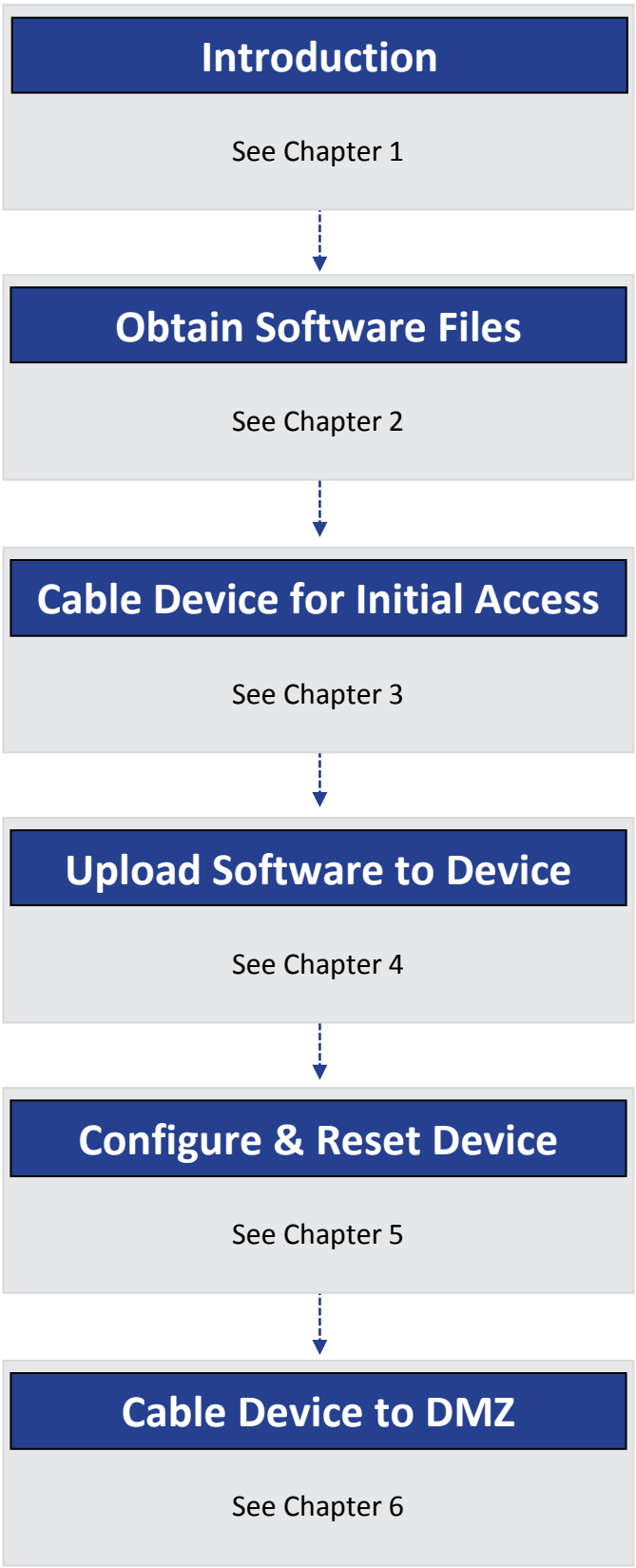
BroadCloud Hosted UC Solution using AudioCodes Mediant™ CRP



Version 7.2

broadsoft broadcloud

audiocodes


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' Cloud Resilience Package (hereafter, referred to as *CRP*) for interworking between BroadCloud's Hosted UC and IP-Phones and/or ATA devices environment. For detailed information on each AudioCodes CRP, refer to the corresponding *User's Manual* and *Hardware Installation Manual*.

1.1 Component Information

AudioCodes CRP Version	
CRP Vendor	AudioCodes
Models	Mediant 500L; Mediant 500; Mediant 800B; Mediant 2600 (Without PSTN connectivity
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 UC Service) ▪ SIP/UDP or SIP/TCP (to the IP-Phones and/or ATA devices)
BroadCloud Hosted UC 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 Hosted Survivability Service Definition* guide, available from BroadCloud's Xchange portal at xchange.broadsoft.com.

Note: The *BroadCloud Hosted Survivability Service Definition Guide* details how to provision the Survivability device and the Survivability 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.

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 CRP, from AudioCodes Website at http://www.audiocodes.com/broadcloud-hosted-uc-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 Cabling

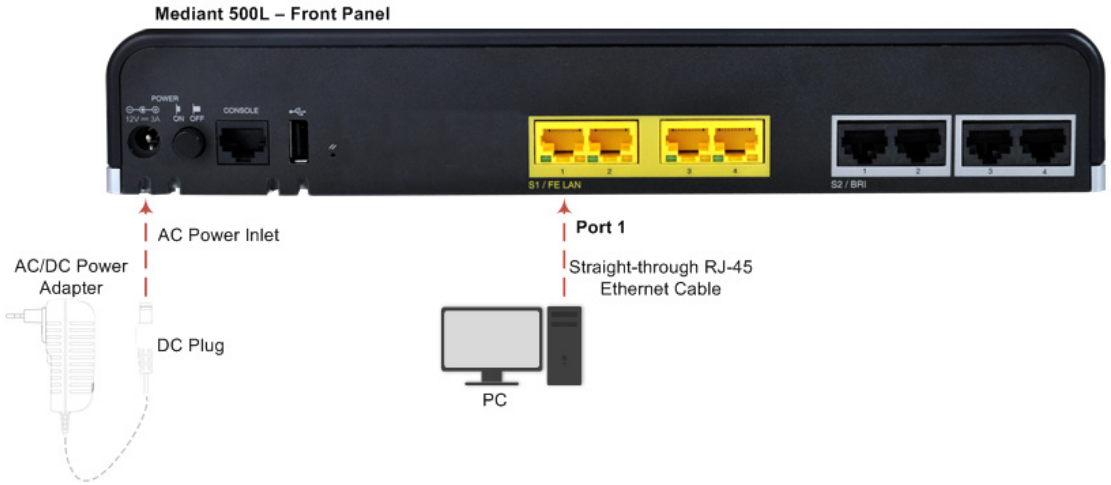


Figure 3-2: Mediant 500 Cabling

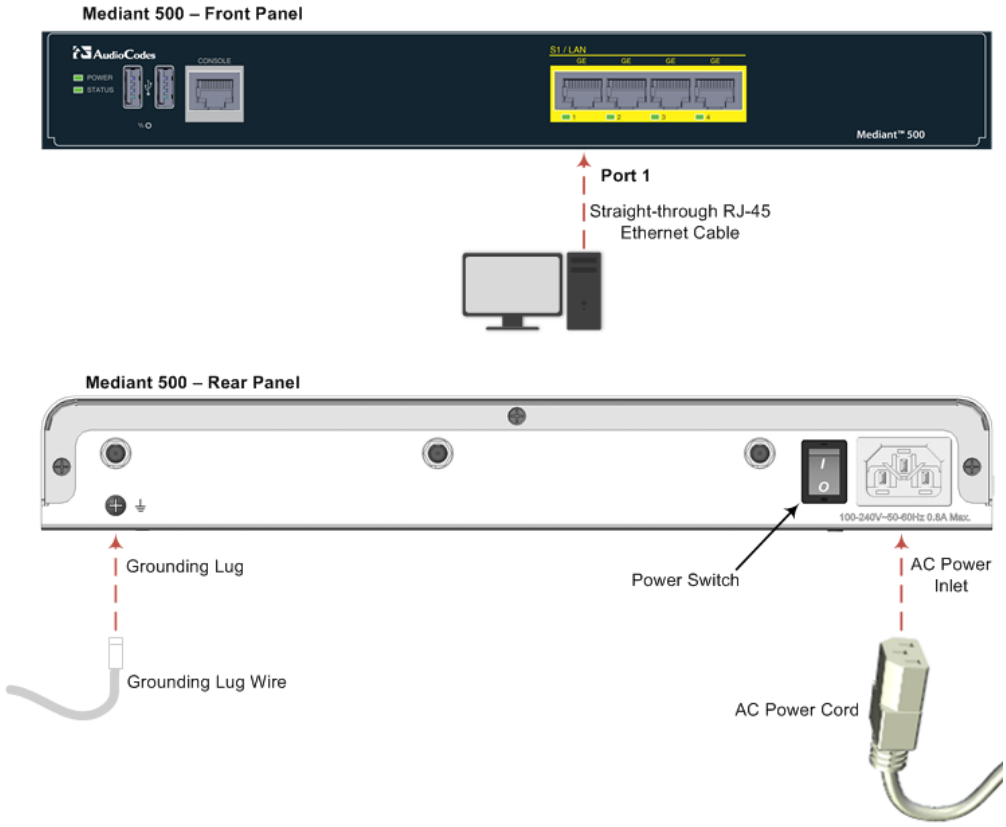


Figure 3-3: Mediant 800 Cabling

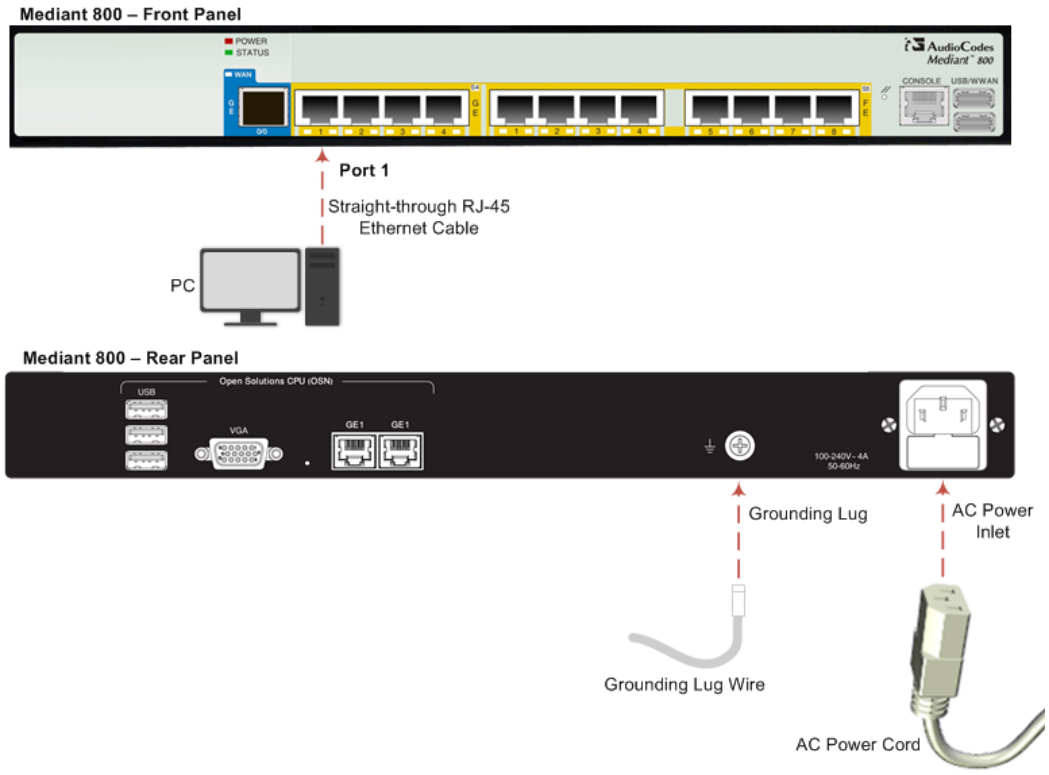
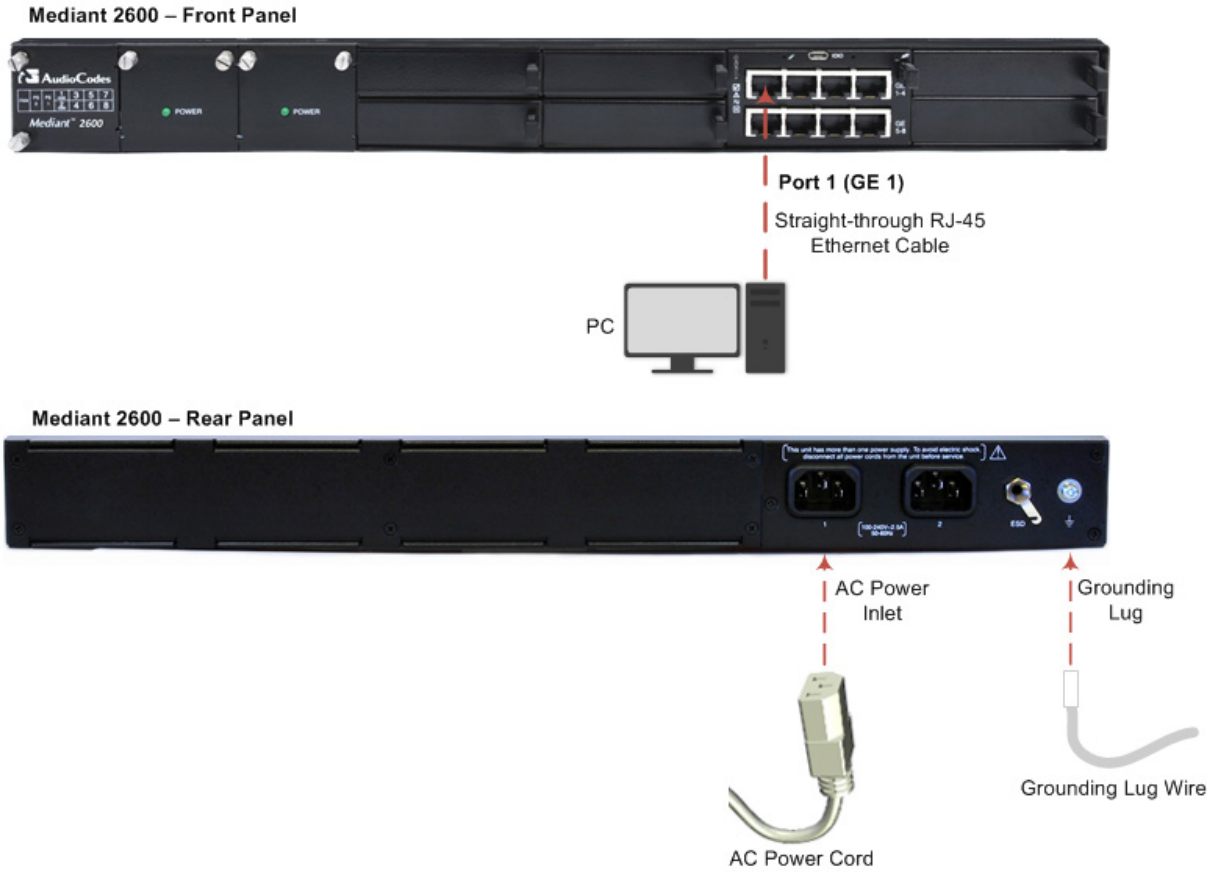
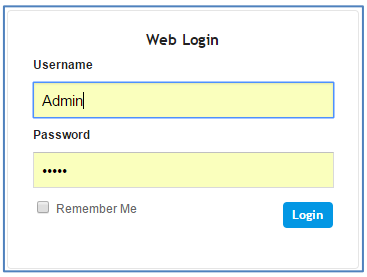


Figure 3-4: Mediant 2600 Cabling



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



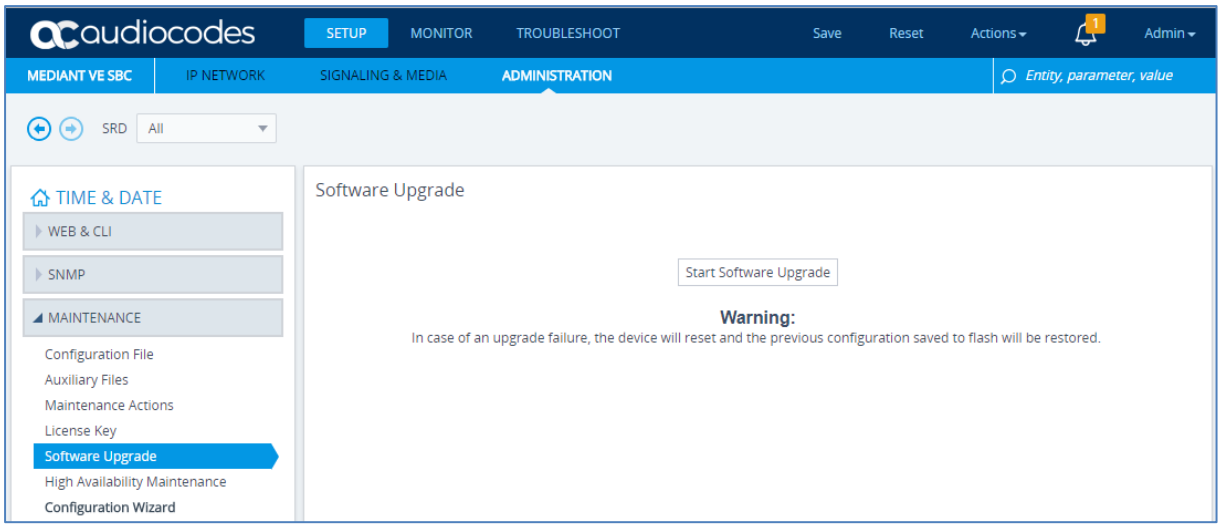
   b. In the 'Username' and 'Password' fields, enter the default login username ("**Admin**") and password ("**Admin**"), and then click **Login**.

4 Upload Software to Device

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

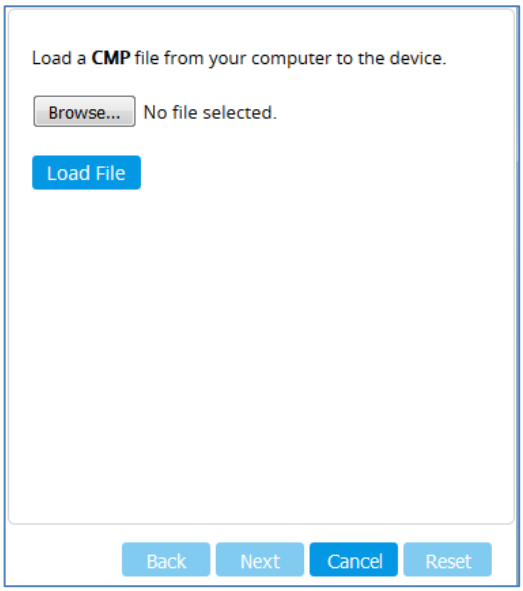
1. In the Web interface, open the Software Upgrade Wizard:
   - **Toolbar:** From the **Actions** drop-down menu, choose **Software Upgrade**.
   - **Navigation tree: Setup** menu > **Administration** tab > **Maintenance** folder > **Software Upgrade**.

Figure 4-1: Device Setup



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

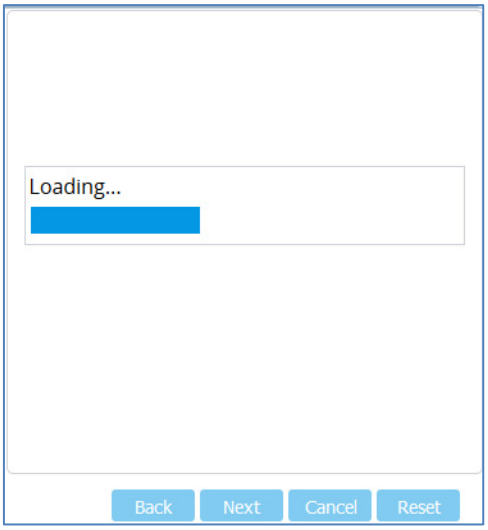


Note: At this stage, you can quit the Software Upgrade wizard without having to reset the device, by clicking **Cancel**. However, if you continue with the wizard and start loading the CMP file, the upgrade process must be completed with a device reset.

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:

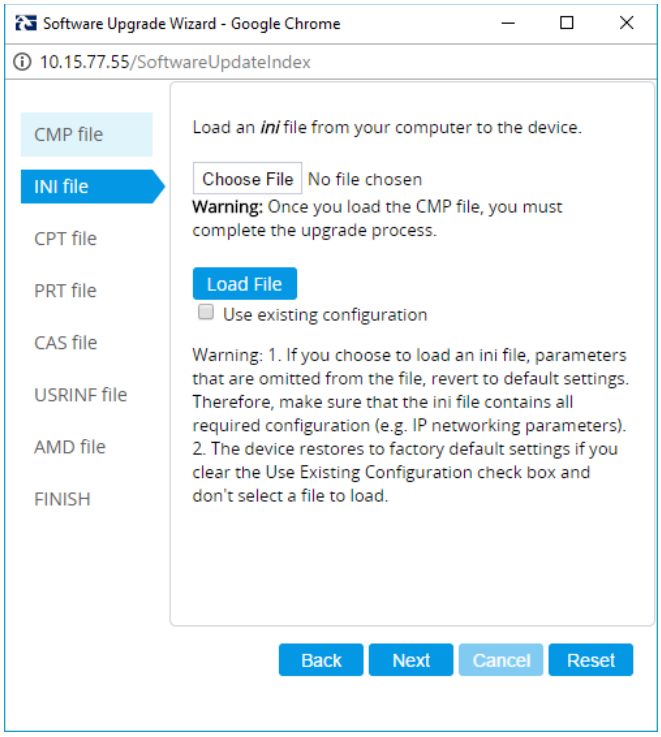
Figure 4-3: CMP File Loading Progress Bar



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:

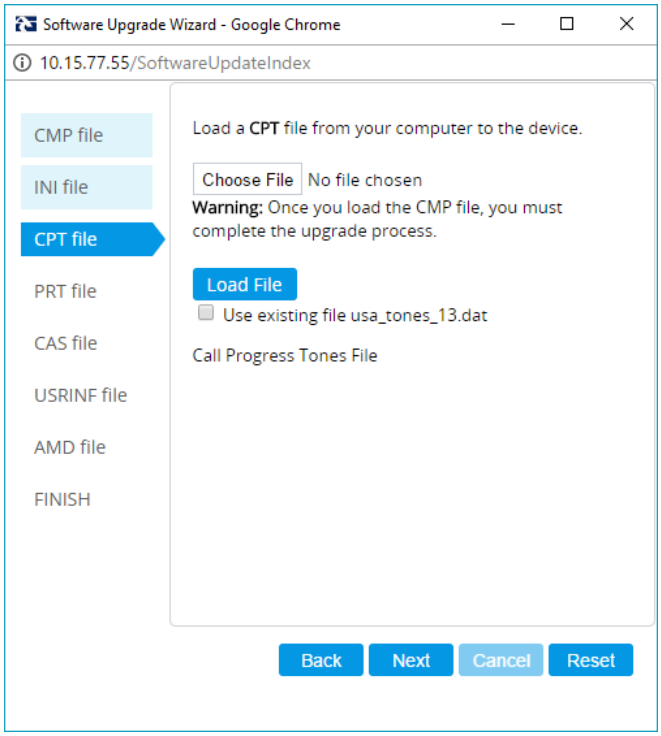
Figure 4-4: Load an INI File in the Software Upgrade Wizard



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

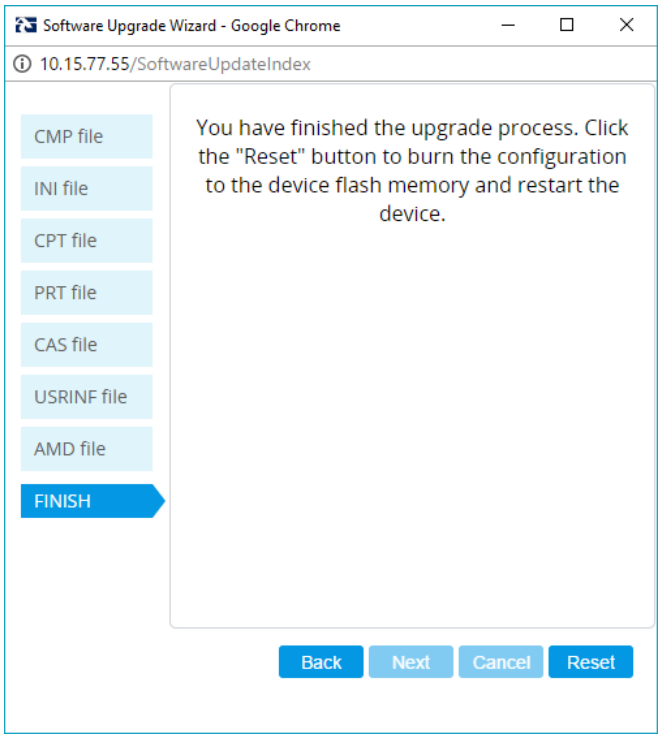
8. Click **Browse** to select the **CPT** file on your PC, and then click **Load File** to load the file:

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



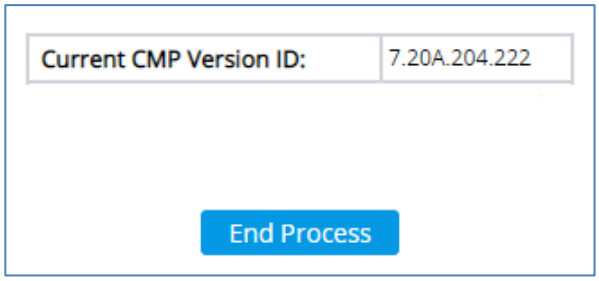
9. Keep clicking **Next** until the last Wizard page appears (the **FINISH** button is highlighted in the left pane) and the following message appears:

Figure 4-6: Finish



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

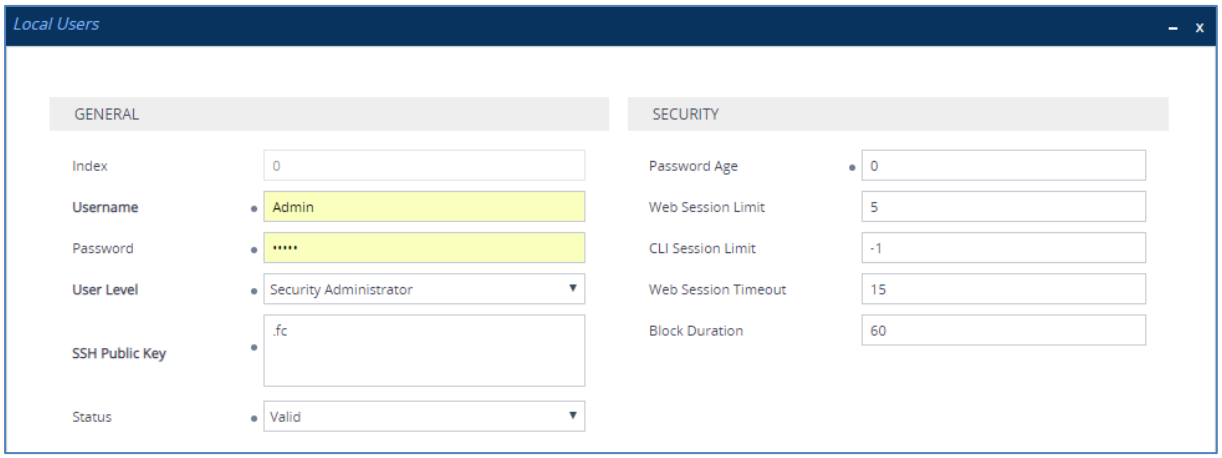
This section describes device configuration.

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

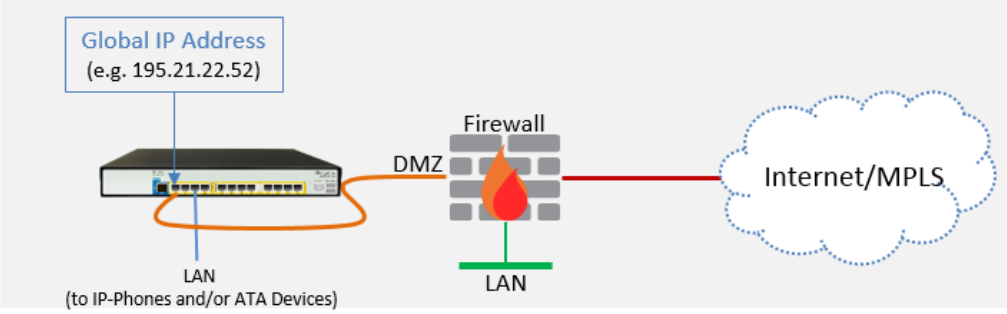


- The device is shipped with a default Monitor access-level user account - username and password: 'User' who has read access only and page viewing limitations but can view certain SIP settings such as proxy server addresses. Therefore, to prevent an attacker from obtaining sensitive SIP settings that 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:

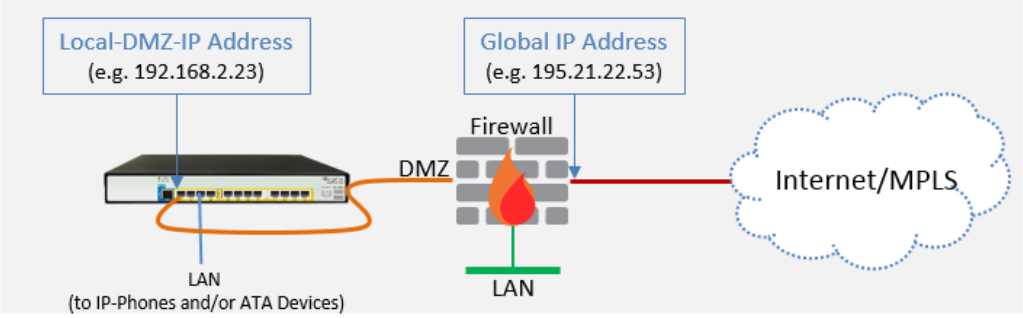
- **Method A**: (Preferred method) A global IP address is provided to the device (**without NAT**):



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 Interfaces

Configure network interfaces for the DMZ/WAN (BroadCloud Hosted UC) interface and LAN (IP-Phones and/or ATA Devices 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 Hosted UC) 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	**WANSP** (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)

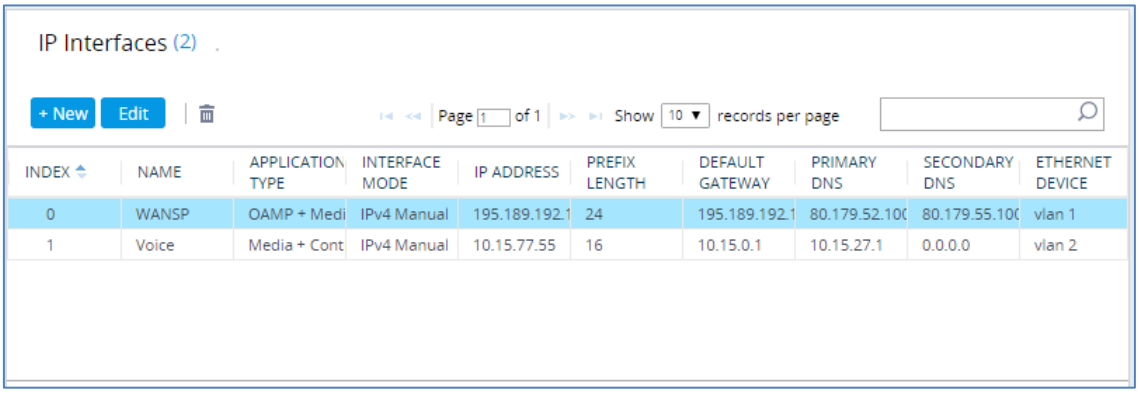
3. Configure the LAN (IP-Phones and/or ATA Devices via local LAN-Switch) interface:
   a. Select the 'Index 1' radio button of the Media + Control table row, and then click **Edit**. This the existing **LAN** ("Voice") interface (available on eth port #3):
   b. Configure the interface as follows:

Parameter	Value
Name	**Voice** (descriptive name, you may change it). This interface will be associated with IP-PBX connectivity.
Application Type	**Media + Control** (leave as is)
Ethernet Device	**vlan 2**
IP Address	**Local LAN IP address** assigned for the CRP 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



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 CRP 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

2. 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)

3. Click **Apply**.

5.3 Configure UDP Ports for RTP between CRP and IP-Phones and/or ATA Devices

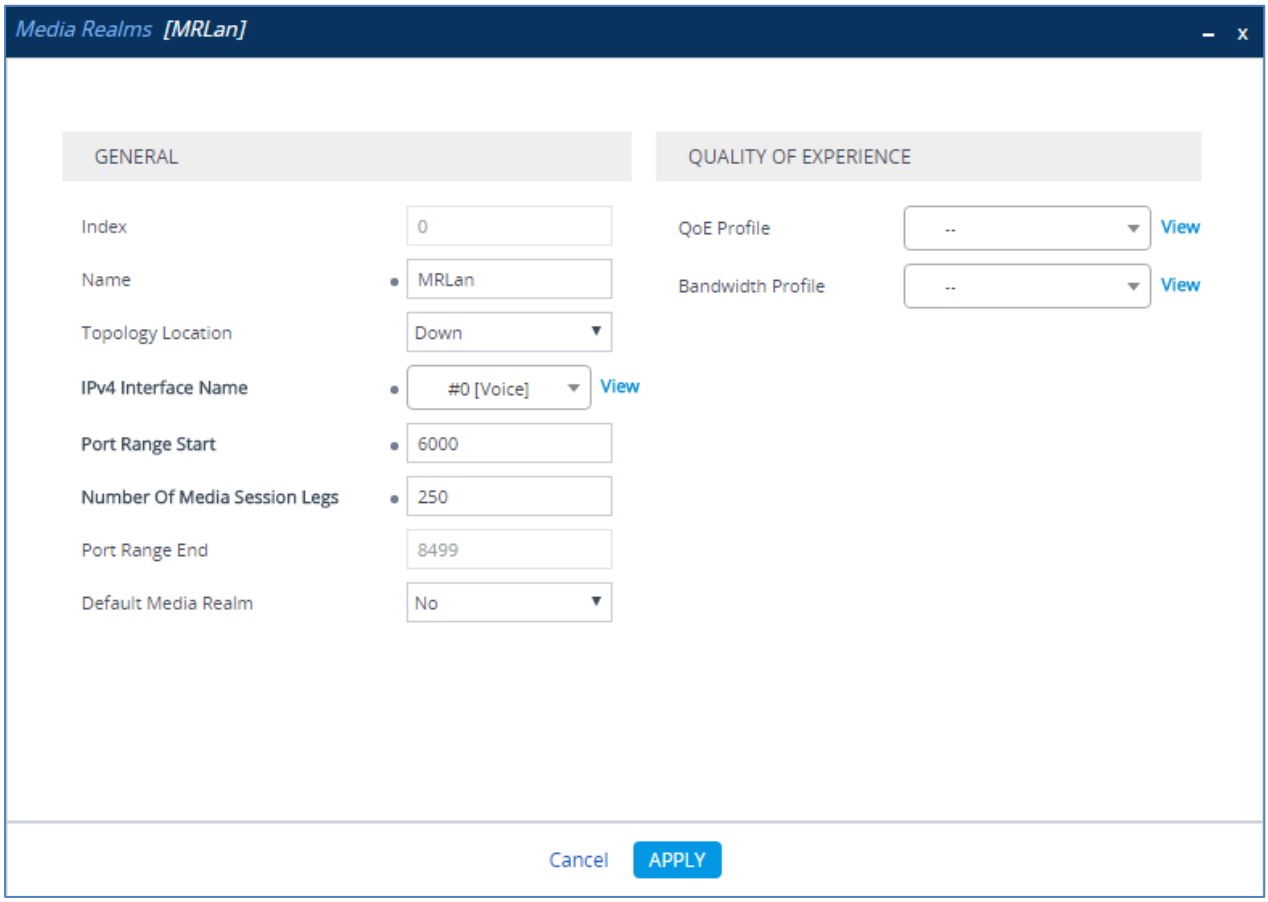
Note: The default UDP port range is 6000 and up to 8499 (maximum UDP depends on the maximum capacity of the specific CRP license provided). Skip this step if you don't need to change the default.

Configure media ports as follows:

1. 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:

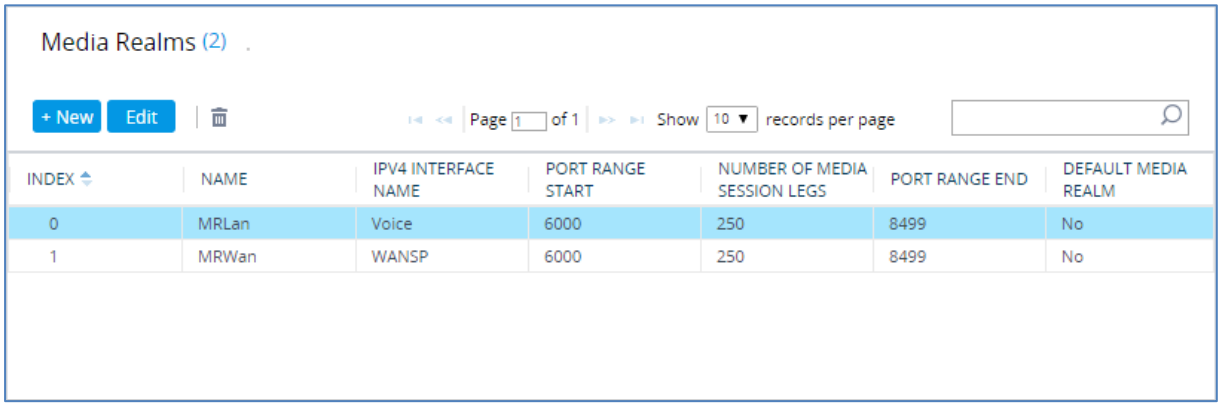
Parameter	Value
Index	**0**
Media Realm Name	**MRLan** (descriptive name)
IPv4 Interface Name	**Voice**
Port Range Start	**6000** (as required by the IP-PBX)
Number of Media Session Legs	**250** (media sessions assigned with port range)

Figure 5-4: Configure Media Realm



The configured Media Realms are shown in the figure below:

Figure 5-5: Media Realms



5.4 Adopt Classification Policy for CRP Users (if Required)

This section describes how to adopt the device's Classification policy per specific customer requirement.

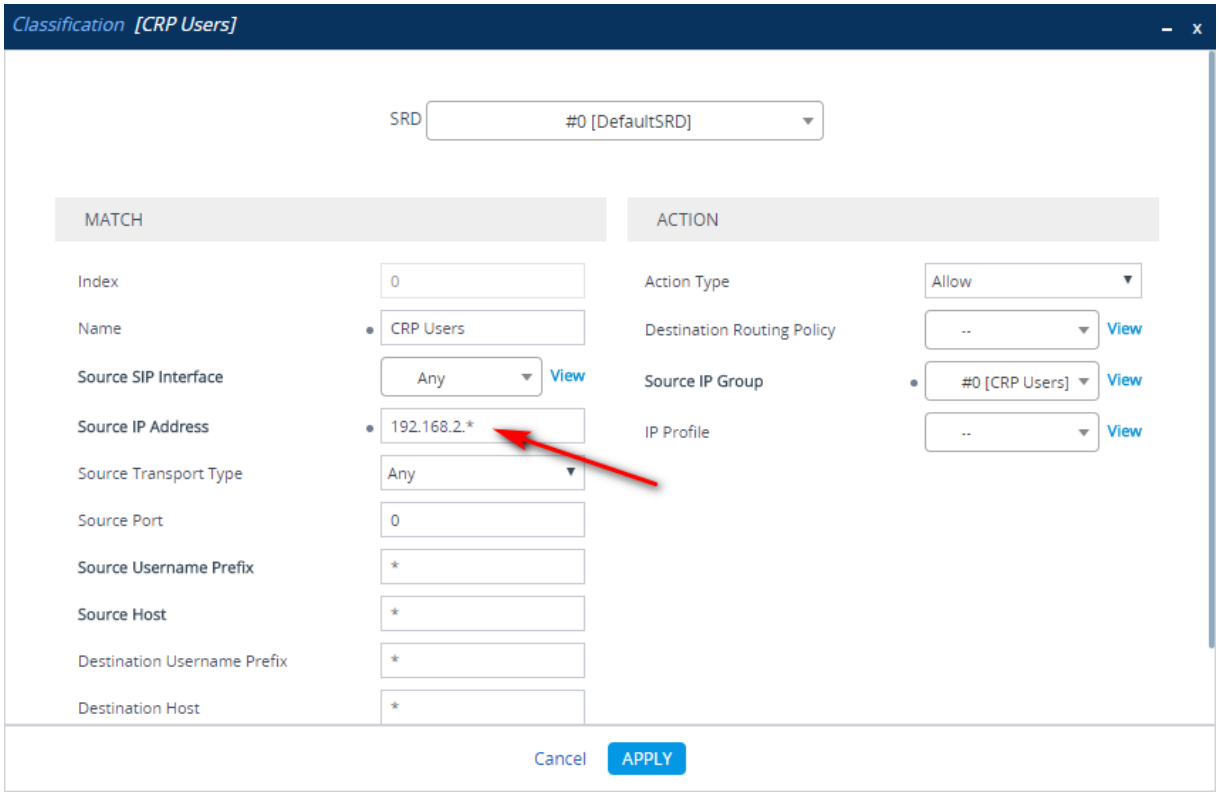
Note: The template INI file is already preconfigured with Classification rules to allow CRP users with source port 8933 and transport type UDP only. Skip this step if you do not need to change these preconfigured settings.

➢ **To configure Classification rules:**

1. Open the Classification table (**Setup** menu > **Signaling & Media** tab > **SBC** folder > **Classification**).
2. Configure Classification rules per customer requirement.

   The Classification rule example below classifies calls only from a specific subnet (192.168.2.*) as CRP users:

Figure 5-6: Classification Rule Example



3. Click **Apply**.

5.5 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.

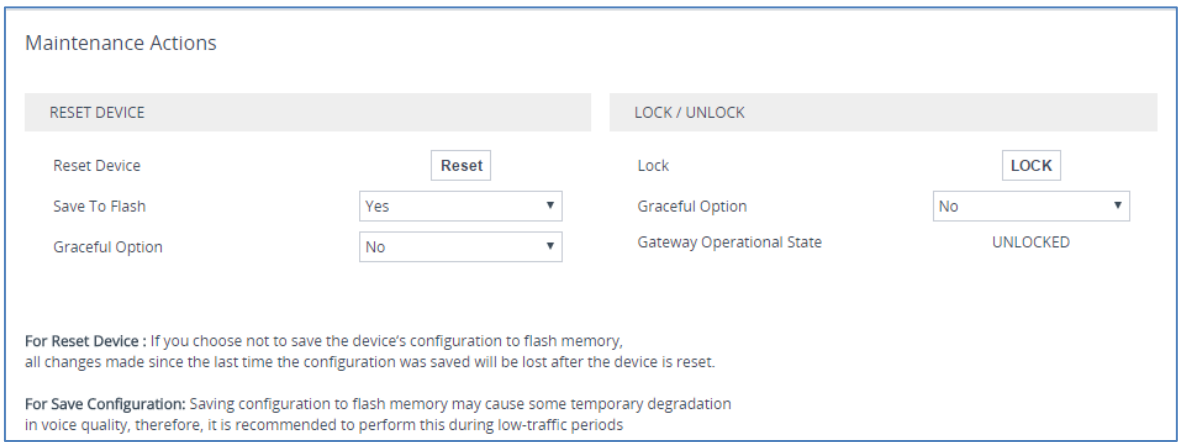
5.6 Save Configuration

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

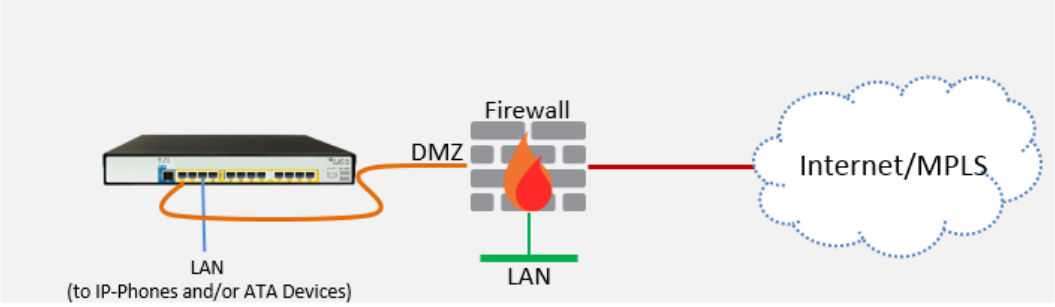
Figure 5-7: Maintenance Actions



6 Cable Device to DMZ

Once the device has reset with your new configuration (as described in the previous section), its IP address changes to your newly configured address. At this point, disconnect your PC from the device and now you can cable the device to your DMZ network and local LAN.

Figure 6-1: Cable Device to DMZ

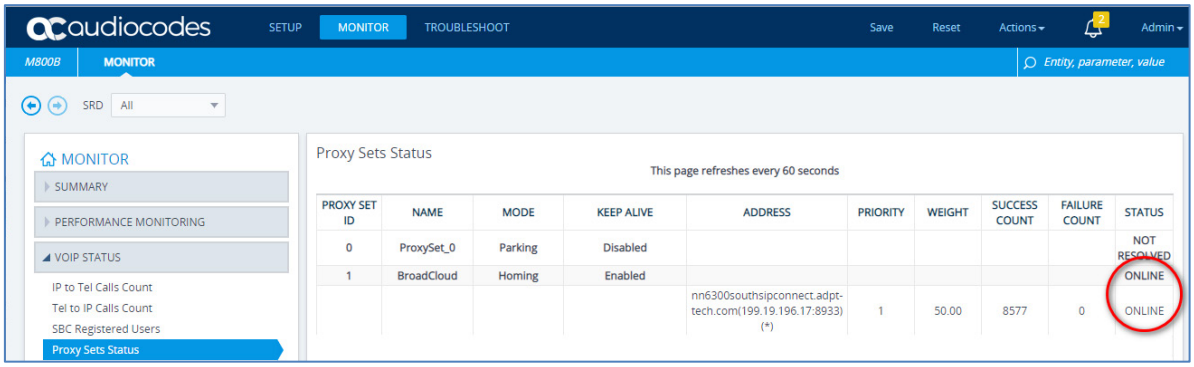


7 Check the Connectivity and Registration Status

Verify that the device successfully registered with the BroadCloud Hosted UC Service, as described below:

1. Open the Registration Status table (**Monitor** menu > **Monitor** tab > **VoIP Status** folder > **Proxy Sets Status**).
2. If registered successfully, the Status column in the Proxy Sets Status table displays "ONLINE" (see the figure below).

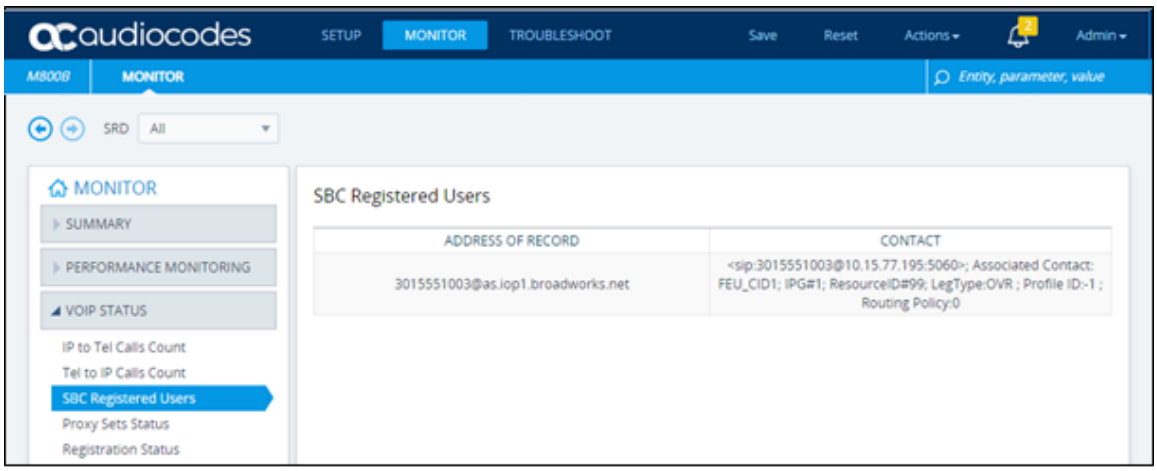
Figure 7-1: Successful Connectivity with BroadCloud Hosted UC Server



To check if the IP-Phones and/or ATA Devices successfully registered with BroadCloud Hosted UC service:

1. Open the SBC Registered Users page (**Monitor** menu > **Monitor** tab > **VoIP Status** folder > **SBC Registered Users**).
2. Check the registration status in the SBC Registered Users Status Table.
   A successful registration will be shown in the CRP AOR Table (see the figure below).

Figure 7-2: Successful IP-Phones Registration



Note: If the status of the device does not show ONLINE, 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**).

A Configure PSTN FallBack (if Required)

This section shows how to configure CRP PSTN Fallback.

Note: Only applies to devices with a PSTN interface, i.e., Mediant 500L/500/800B.

A.1 Cabling

A.1.1 Connecting BRI to the Mediant 500L

This section shows how to connect the device's BRI ports to the PBX.

Warning: To protect against electrical shock and fire, use a 26 AWG min wire.

To connect a BRI line:

1. Connect the RJ-45 cable to the device's BRI port on the rear panel (it's labeled S2 / BRI).
2. Connect the other end of the cable to your ISDN PBX equipment.

Figure A-1: Cabling BRI Ports

A.1.2 Connecting ISDN PRI (E1/T1) Trunk to the Mediant 500 and Mediant 800B

This section shows how to cable the device's E1/T1 (PRI) trunk interface.

Warning: To protect against electrical shock and fire, use a 26 AWG min wire to connect the E1 / T1 port to the PSTN.

To connect the E1/T1 trunk interface:

1. Connect the E1/T1 trunk cable to the device's E1/T1 port.
2. Connect the other end of the trunk cable to your PBX switch.

Figure A-2: Mediant 500 Cabling E1/T1 Port

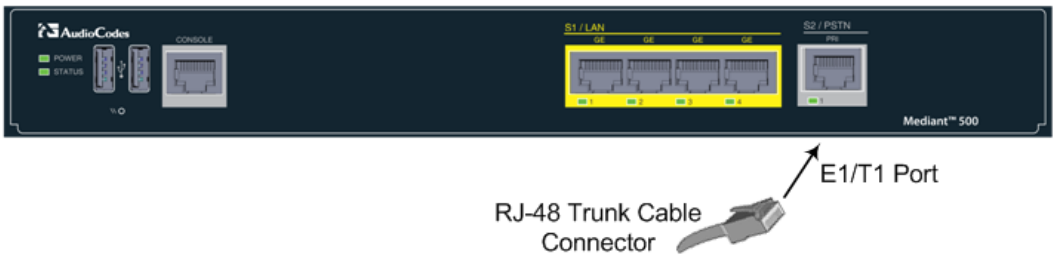
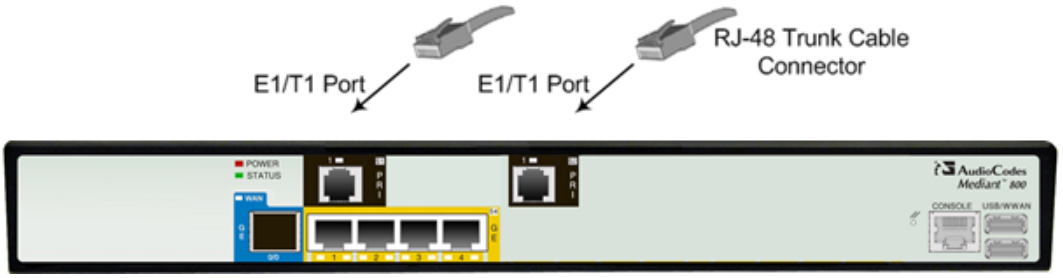


Figure A-3: Mediant 800B Cabling E1/T1 Port



A.2 Configure PSTN Trunk Settings

This step shows how to configure PSTN trunk settings.

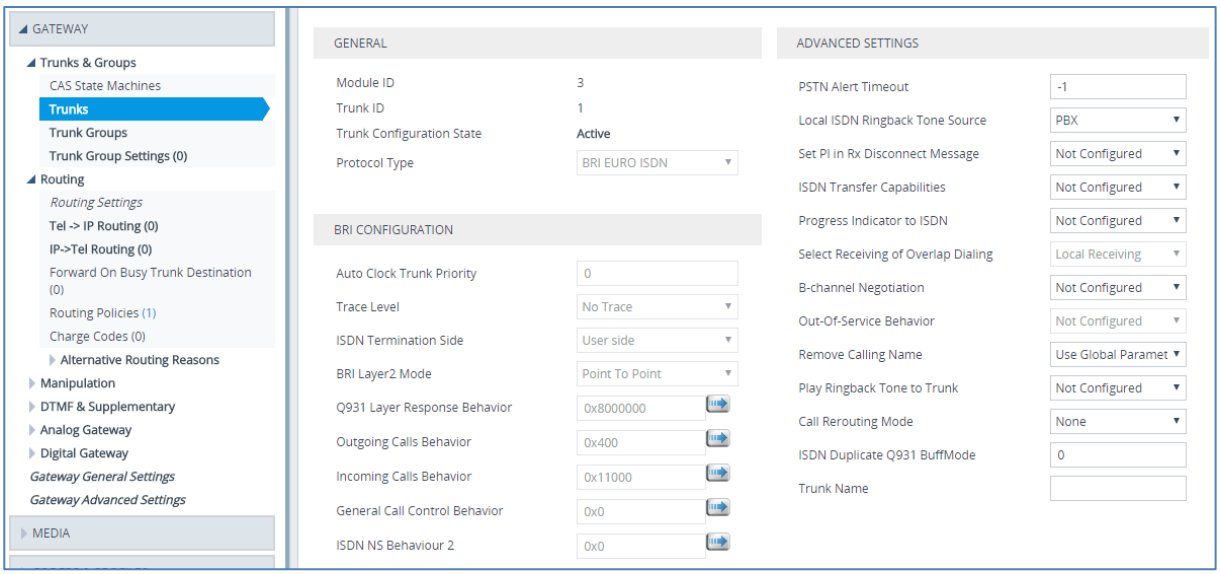
A.2.1 Configure the BRI PSTN Interface

This step shows how to configure the BRI PSTN Interface. Skip to the next step 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 according to PSTN network:

Parameter	Value
Protocol Type	**BRI EURO ISDN** (for Europe and Australia) or **BRI NI2 ISDN** (for USA)
ISDN Termination Side	**User side**
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 A-4: Configuring BRI PSTN Interface



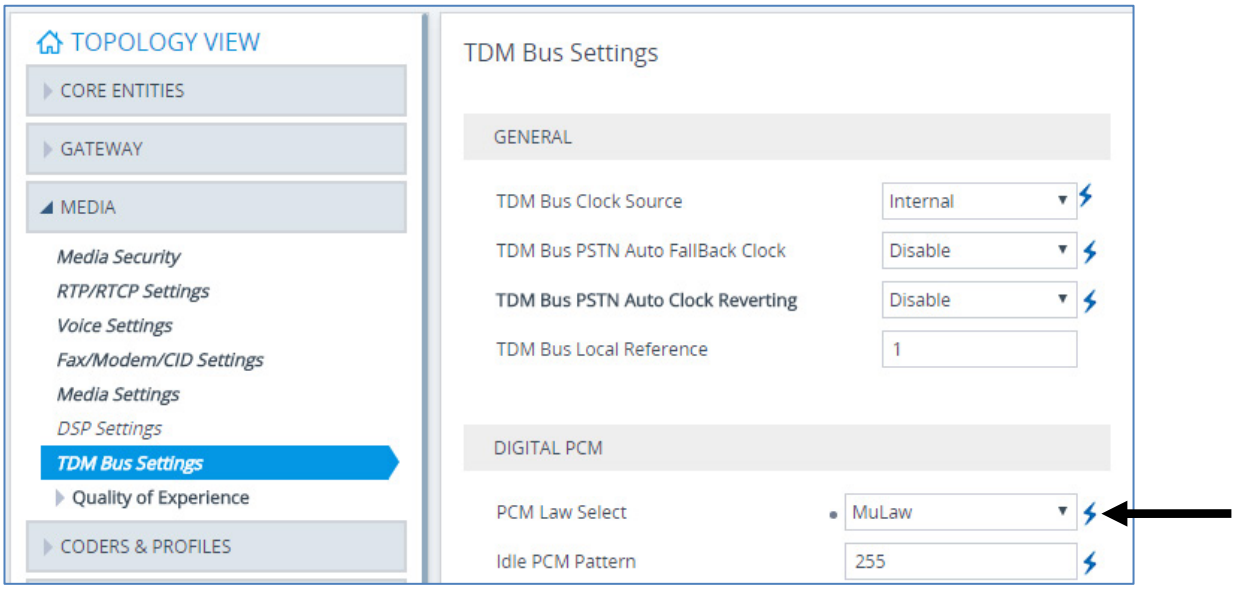
3. Repeat for all BRI ports available on the device (Mediant 500L)

A.2.2 Configure PCM Law Select

This step shows how to configure the PCM law Select. To configure the PCM Law Select:

1. Open the TDM Bus Settings page (**Setup** menu > **Signaling & Media** tab > **Media** folder > **TDM Bus Settings**).
2. From the 'PCM Law Select' drop-down list, select **Alaw** for E1/BRI or **MuLaw** for T1 trunks.

Figure A-5: Configuring PCM Law Select



3. Click **Apply** to apply definitions.

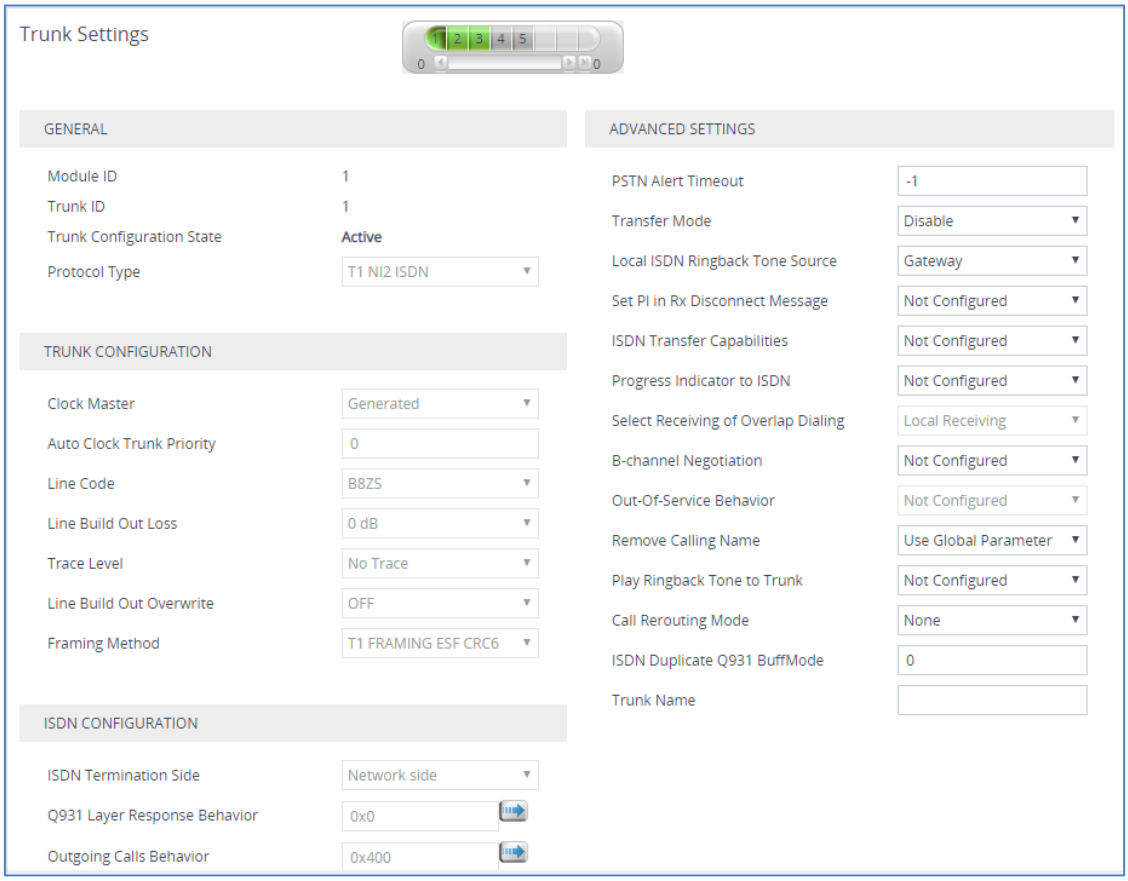
A.2.3 Configure the PRI PSTN Interface

This step 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 according to PSTN network:

Parameter	Value
Protocol Type	**E1 EURO ISDN** (for Europe and Australia) or **T1 NI2 ISDN** (for USA)
Clock Master	**Generated** (The device is clock master) **Recovered** (The device slaves from the line clock)
Framing Method	**E1 Framing MFF CRC4 Ext** for E1 or **Extended Super Frame** for T1 (according to remote side, PBX or PSTN, definitions)
ISDN Termination Side	**Network side** or **User side** (according to remote side definitions)

Figure A-6: Configuring the PRI PSTN Interface



3. Repeat for all PRI ports available on the device (Mediant 800B).
4. Reset the device with a save-to-flash for your settings to take effect.

A.3 Configure Trunk Group Parameters

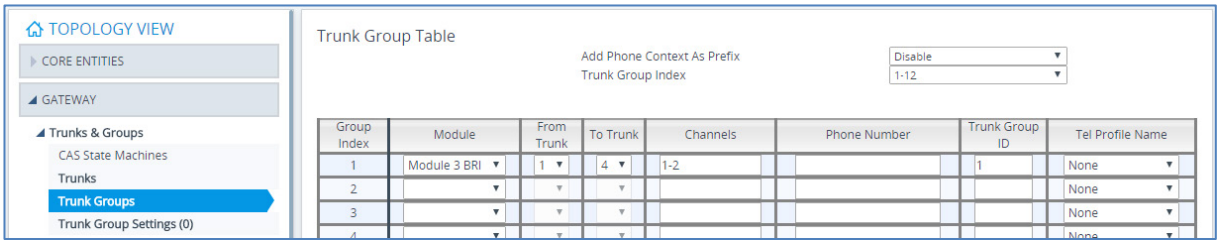
This step shows how to configure the device's channels, which includes assigning them to Trunk Groups. A Trunk Group is a logical group of physical trunks and channels. A Trunk Group can include multiple trunks and ranges of channels. To enable and activate the device's channels, Trunk Groups must be 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.

A.3.1 Configure the BRI Trunk Group (for Devices with BRI PSTN Interface)

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 A-7: Configuring BRI Trunk Group Table



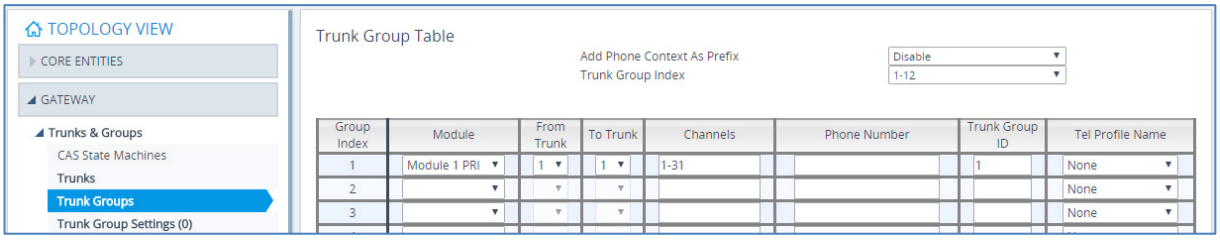
2. Configure each Trunk Group as required. If more than one BRI port is available, on line 1 of the table above, set **To Trunk** to the last BRI port to be used for PSTN Fallback.

A.3.2 Configure the PRI Trunk Group (for Devices with PRI PSTN Interface)

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 A-8: Configuring PRI Trunk Group Table



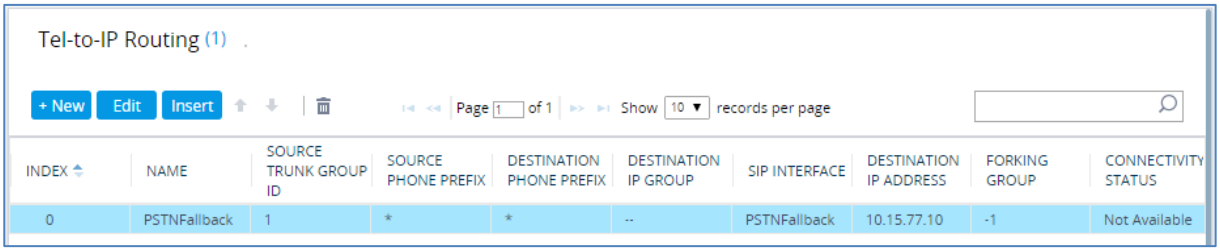
2. Configure each Trunk Group as required. If more than one PRI port is available, on line 1 of the table above, set 'To Trunk' to the last PRI port (2) to be used PSTN Fallback.

A.4 Configure CRP Gateway Routing

This section shows how to configure Mediant CRP Gateway Outbound (Tel-to-IP) Routing. To configure IP-to-Tel or Inbound IP Routing Rules:

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

Figure A-9: Configuring Outbound Routing Rules



3. Configure a rule for all outgoing calls from Trunk Group ID 1 (configured in the step 3 above), assign them to the PSTNFallback (CRP Gateway) SIP Interface and route them to the device's LAN IP address and port 5060.
4. Click **Apply** to apply definitions.

A.5 Configure SIP Parameters for CRP PSTN Fallback

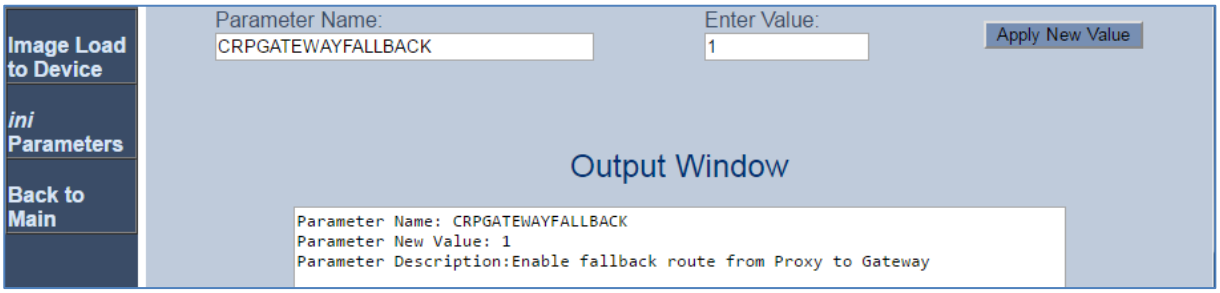
This section shows how to enable the CRP to route emergency calls (or PSTN-intended calls) such as "911" from the Proxy server (BroadCloud IP Group) to the PSTN (CRP Gateway IP Group). In addition, for calls from the Proxy server to Users (CRP Users IP Group), the device searches for a matching user in its Users Registration database and if not located, it sends the call to the PSTN (CRP Gateway IP Group), as an alternative route.

A.5.1 Enable the CRPGatewayFallback Parameter

This section shows how to enable CRPGatewayFallback parameter. To Enable CRPGatewayFallback parameter:

1. Open the Admin page: Append the case-sensitive suffix 'AdminPage' to the device's IP address in your Web browser's URL field (e.g., http://10.15.77.10/AdminPage).
2. In the left pane of the page that opens, click ***ini* Parameters**.

Figure A-10: Enable CRPGatewayFallback Parameter



3. Enter these values in the 'Parameter Name' and 'Enter Value' fields:

Parameter	Value
CRPGATEWAYFALLBACK	**1** (enables CRP Gateway Fallback)

4. Click the **Apply New Value** button for each field.

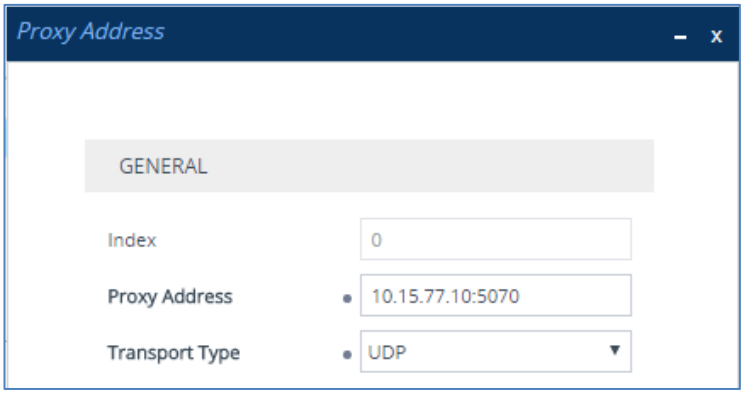
A.5.2 Update the CRP Gateway Proxy Set

This section shows how to update the CRP Gateway Proxy Set in order to enable PSTN Fallback routing. To update the CRP Gateway Proxy Set configuration:

1. Open the Proxy Sets table (**Setup** menu > **Signaling & Media** tab > **Core Entities** folder >**Proxy Sets**).
2. Identify the Proxy Set for the CRP Gateway by the 'Proxy Name' field **PSTNFallback**.
3. Click the **Proxy Address** link located below the table.
4. Configure a Proxy Address and port for Proxy Set for CRP Gateway:

Parameter	Value
Index	**0**
Proxy Address	CRP LAN IP address and port e.g. **10.15.77.10:5070**
Transport Type	**UDP** (leave as is)

Figure A-11: CRP Gateway Proxy Address



5. Click **Apply** to apply definitions.

B Troubleshooting

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

B.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
   ```

B.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
   ```

C Changing connectivity to TLS/SRTP (Optional)

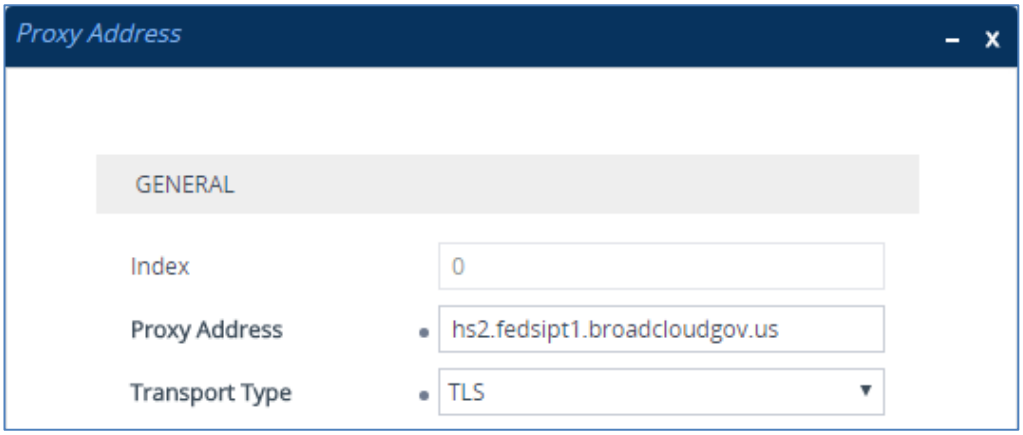
This section shows how to configure the Mediant CRP to work in secure mode (TLS/SRTP) towards BroadCloud Hosted UC.

C.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 1). Click the **Proxy Address** link located below the table; the Proxy Address table opens.
3. Click **Edit**, the following dialog box appears:

Figure C-1: Configuring Proxy Address for BroadCloud Hosted UC



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**.

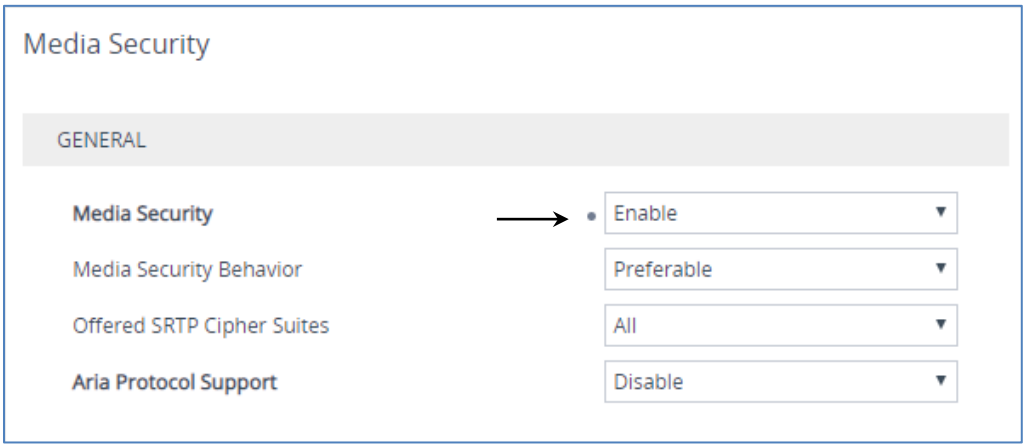
C.2 Configure SRTP

C.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 C-2: Configuring SRTP



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

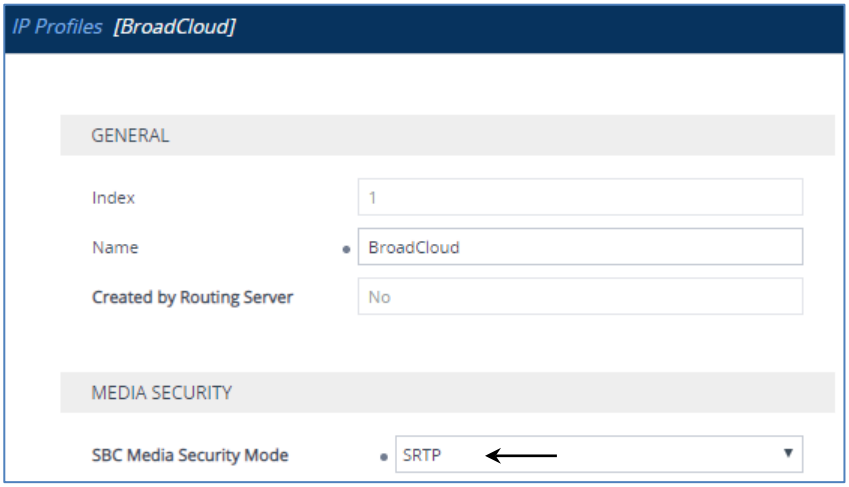
C.2.2 Change Media Security Mode to SRTP

This section describes how to change media security mode to SRTP for BroadCloud Hosted UC.

➢ **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 C-3: Configuring SRTP

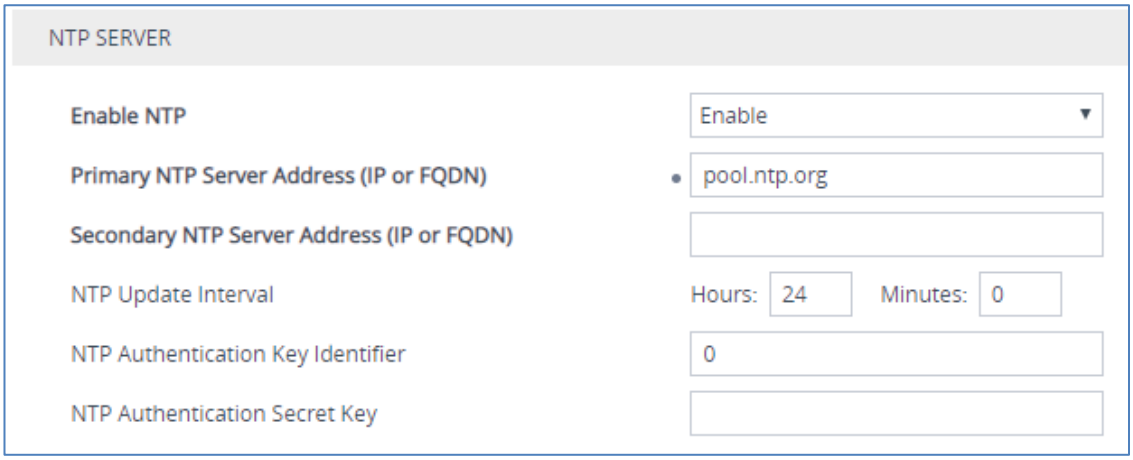


C.3 Configure the NTP Server Address

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 CRP 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 C-4: Configuring NTP Server Address



3. Click **Apply**.

C.4 Configure a Certificate for Operation with the BroadCloud Hosted UC

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 Hosted UC.

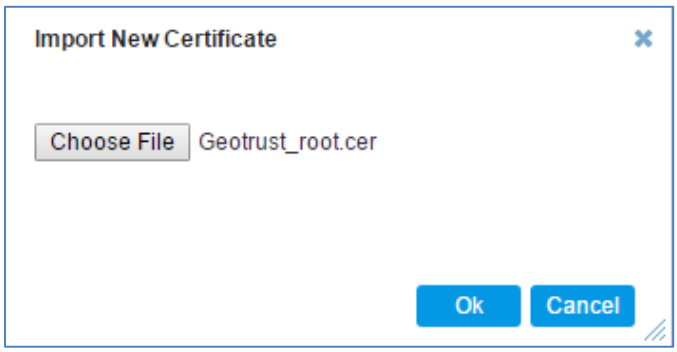
The procedure involves the following main steps:

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

➢ **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 C-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/

Document #: LTRT-29837