Quick Guide

AudioCodes Mediant™ Gateway

Connecting PBX to BroadSoft SIP Trunk using AudioCodes Mediant 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' PRI Gateway (hereafter, referred to as *Gateway*) for interworking between BroadSoft's SIP Trunk and PBX environment. For detailed information on each AudioCodes Gateway, refer to the corresponding *User's Manual* and *Hardware Installation Manual*.

1.1 Component Information

Table 1-1: Component Information

AudioCodes Gateway Version	
Gateway Vendor	AudioCodes
Models	Mediant 500; Mediant 800B; Mediant 1000B
Software Version	7.20A.104.001
Protocol	▪ SIP/UDP (to the BroadSoft SIP Trunk) ▪ PRI (to the PBX)
BroadSoft SIP Trunking Version	
Vendor/Service Provider	
SSW Model/Service	
Software Version	
Protocol	SIP/UDP

This page is intentionally left blank.

2 Obtain Software Files

Download the certified firmware file (*firmware_xxx.**cmp***), configuration file (*configuration_xxx.**ini***) and Call Progress Tones file (*call_progress_uk**.dat***), of the specific AudioCodes PRI Gateway (referred as "xxx"), from Support Centre.

This page is intentionally left blank.

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.
   - Using the supplied AC power cable, connect the device's AC port to a standard electrical wall outlet.

Figure 3-1: Mediant 500 – Front and Rear Panels

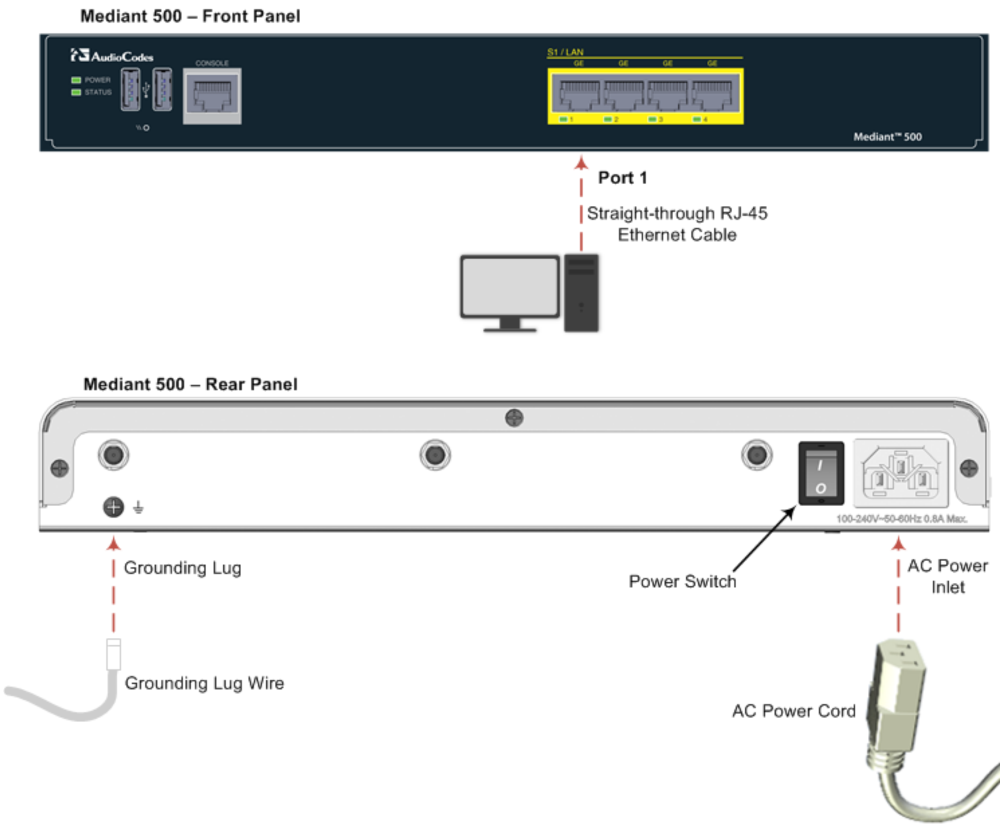


Figure 3-2: Mediant 800 – Front and Rear Panels

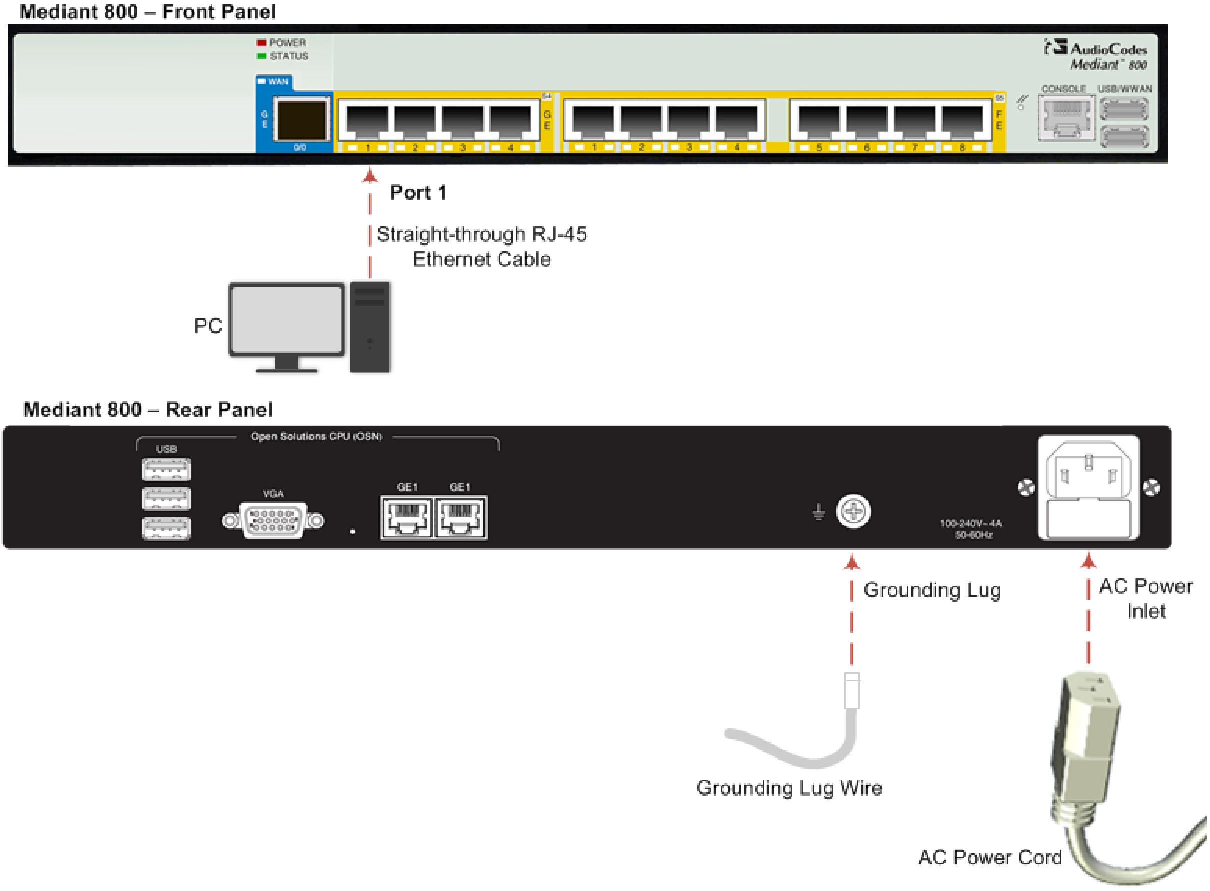
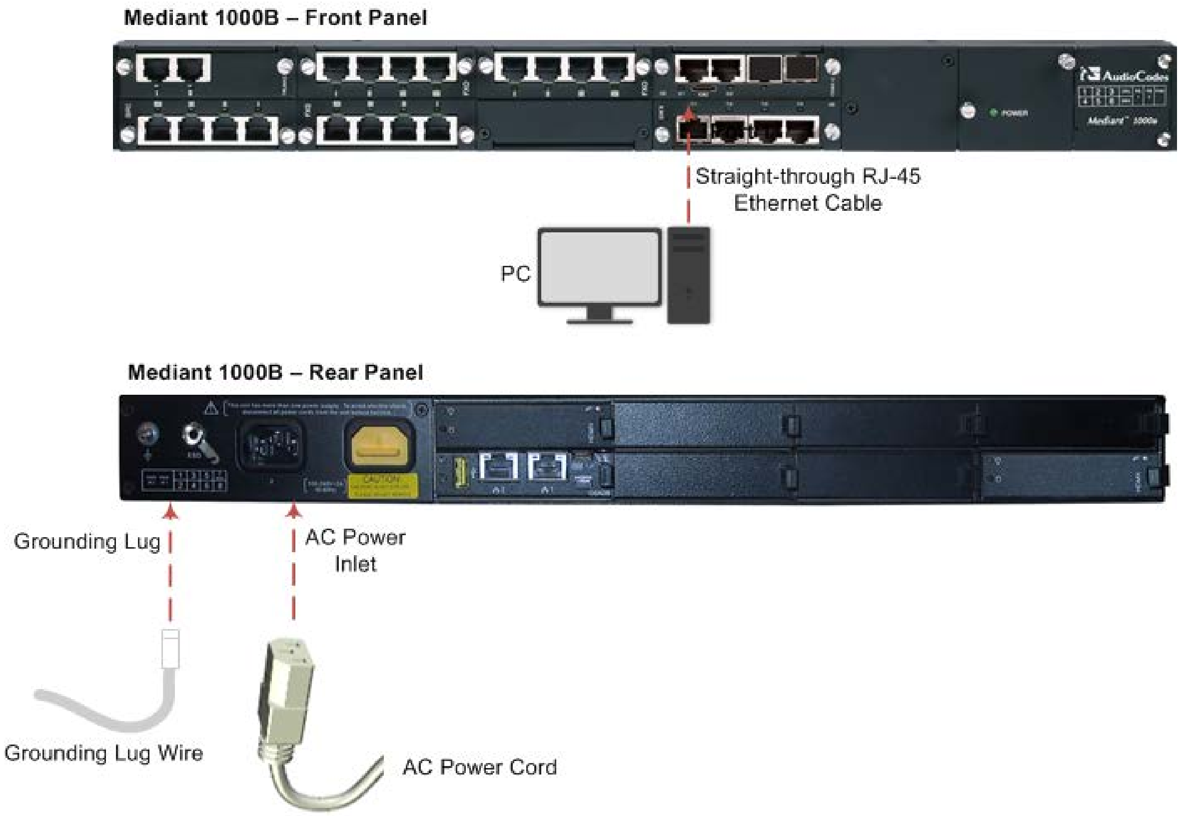


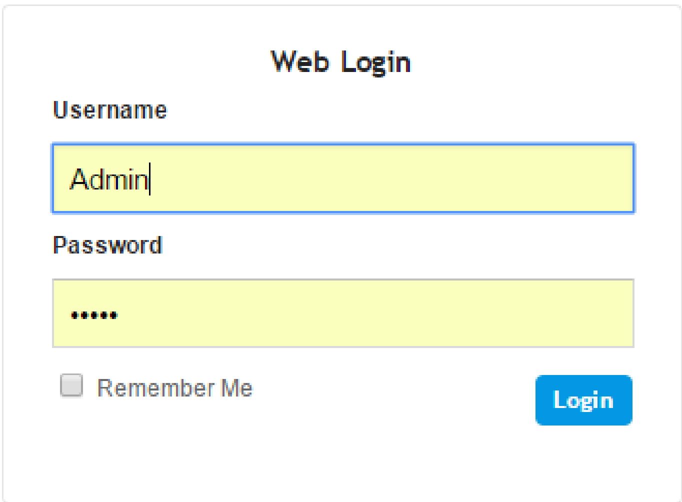
Figure 3-3: Mediant 1000B – Front and Rear Panels



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



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

This page is intentionally left blank.

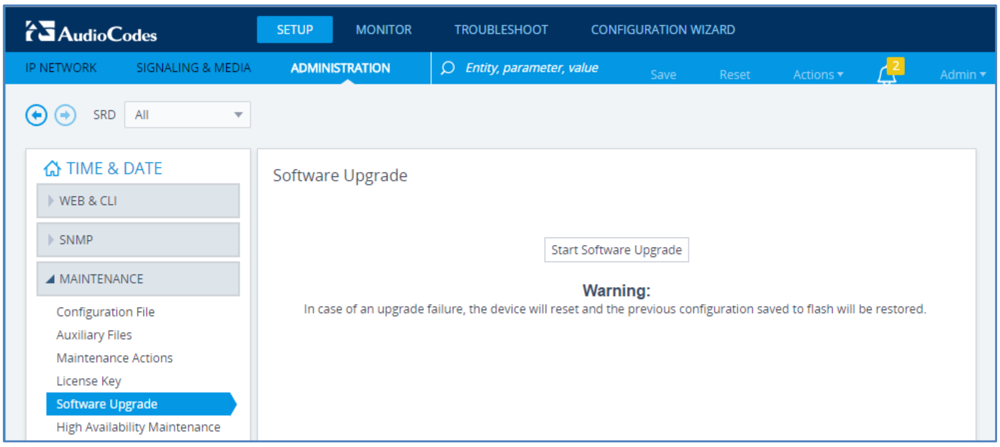
4 Upload Software to Device

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:

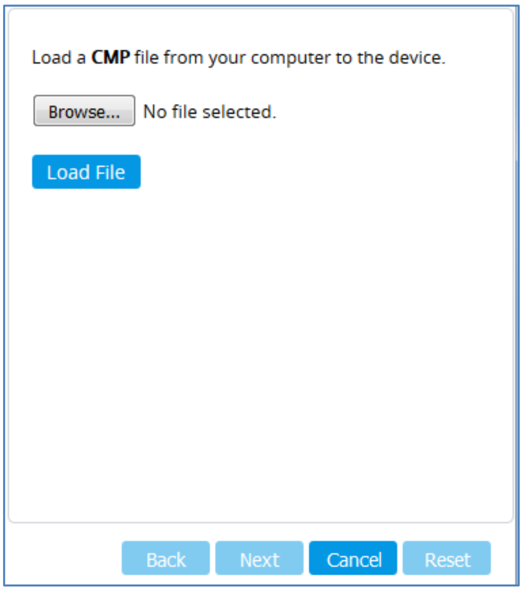
- **Toolbar:** From the **Actions** drop-down menu, choose **Software Upgrade**.
- **Navigation tree: Setup** menu > **Administration** tab > **Maintenance** folder > **Software Upgrade**.

Figure 4-1: Software Upgrade Page



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

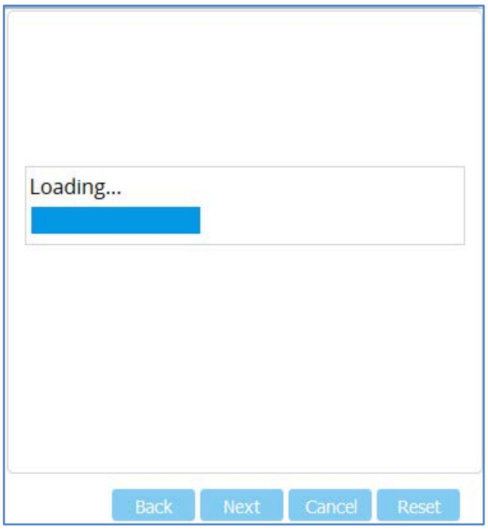


Note: At this stage, you can quit the Software Upgrade wizard without having to reset the device, by clicking **Cancel**. However, if you continue with the wizard and start loading the CMP file, the upgrade process must be completed with a device reset.

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:

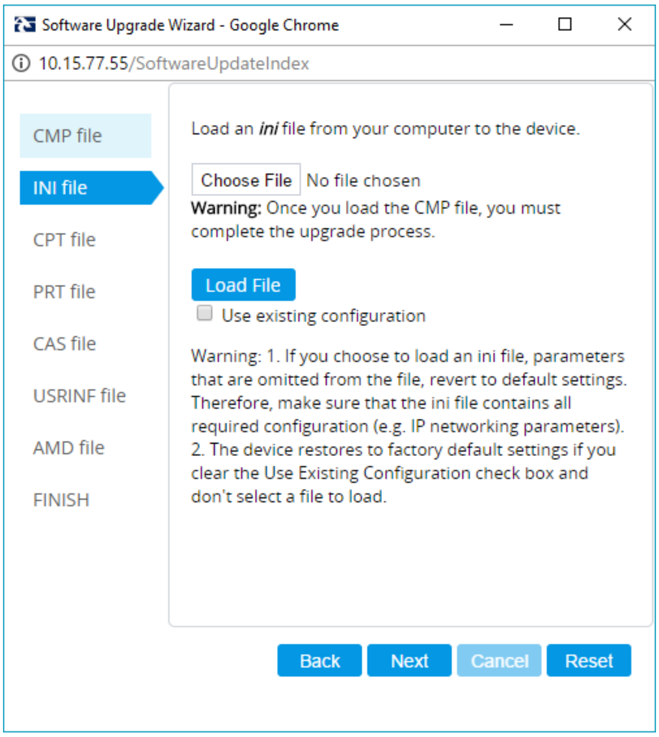
Figure 4-3: CMP File Loading Progress Bar



A message is displayed to inform you that the file has been loaded,.

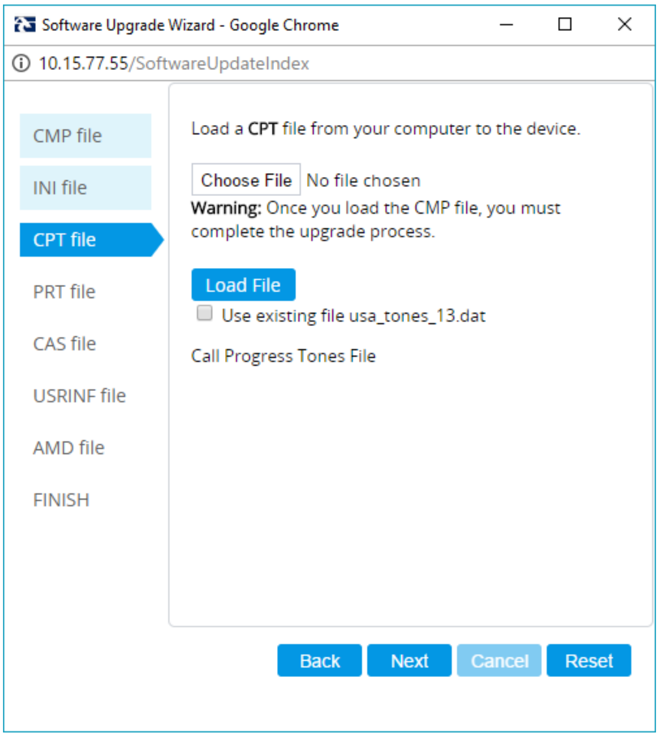
5. When successfully loaded, click **Next** to access the wizard page for loading the *ini* file.
6. Clear the **Use existing configuration** option, click **Browse** to select the configuration file (.ini) on your PC, and then click **Load File** to load the file:

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



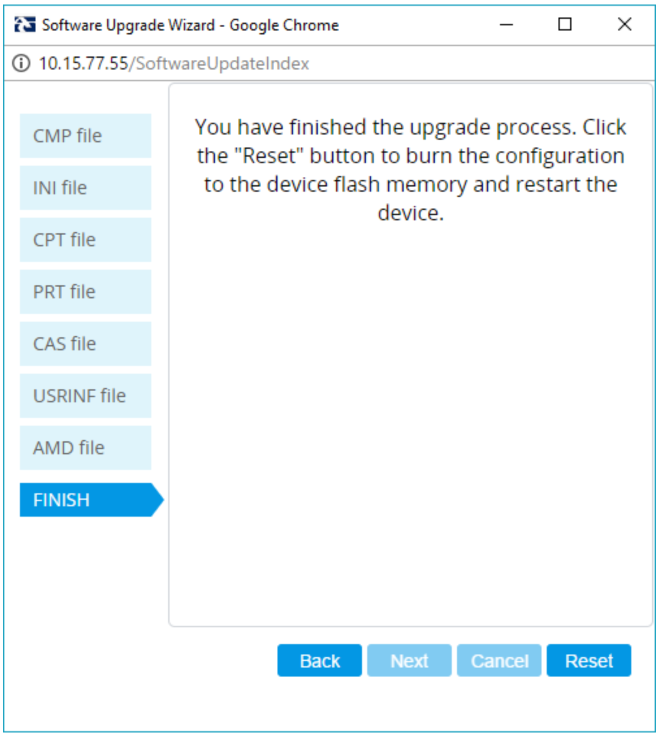
7. Click **Next** to access the wizard page for loading the Call Progress Tones (CPT) file.
8. Click **Browse** to select the **CPT** file on your PC, and then click **Load File** to load the file:

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



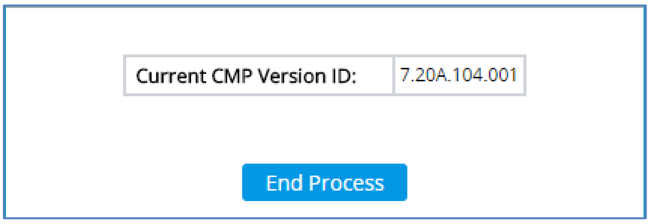
9. Keep clicking **Next** until the last Wizard page appears (the **FINISH** button is highlighted in the left pane) and the following message appears:

Figure 4-6: Software Upgrade Wizard – Google Chrome



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 ID



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

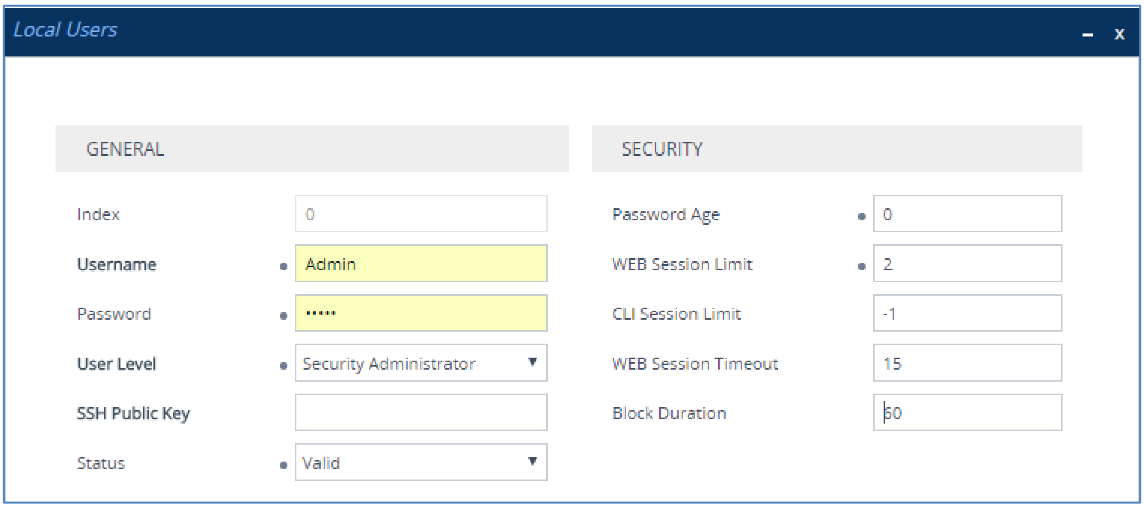
This section describes device configuration.

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



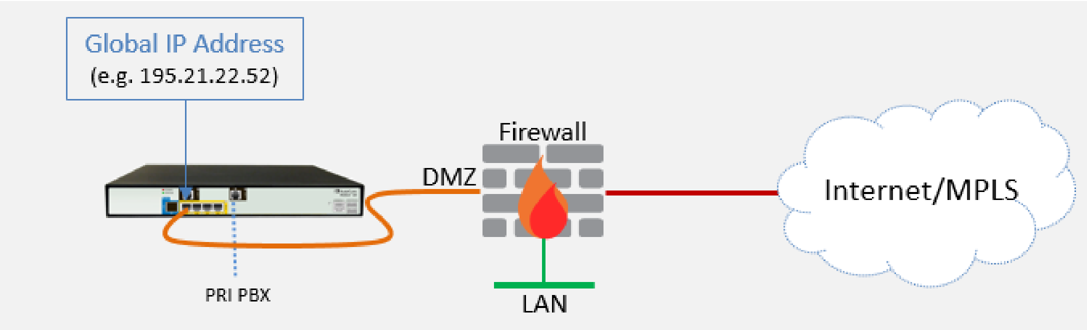
- The device is shipped with a default **Monitor** access-level user account - username and password: 'User' who has read access only and page viewing limitations but can view certain SIP settings such as proxy server addresses. Therefore, to prevent an attacker from obtaining sensitive SIP settings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

Figure 5-2: Method A

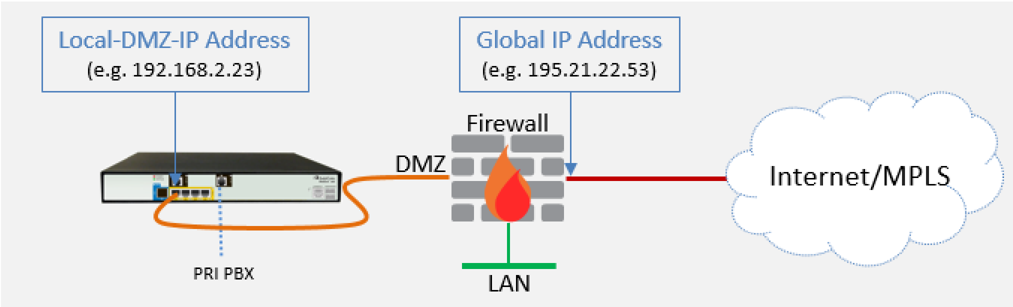


The Enterprise firewall is configured with rules, for example:

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

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

Figure 5-3: Method B



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: 5060 / UDP RTP service: 6000-8500 / UDP	<any> (e.g. ITSP)	Local DMZ IP Address	<as original>

NAT rules (port forwarding):

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

5.2.1 Configure Network Interface

Configure network interface, as described below:

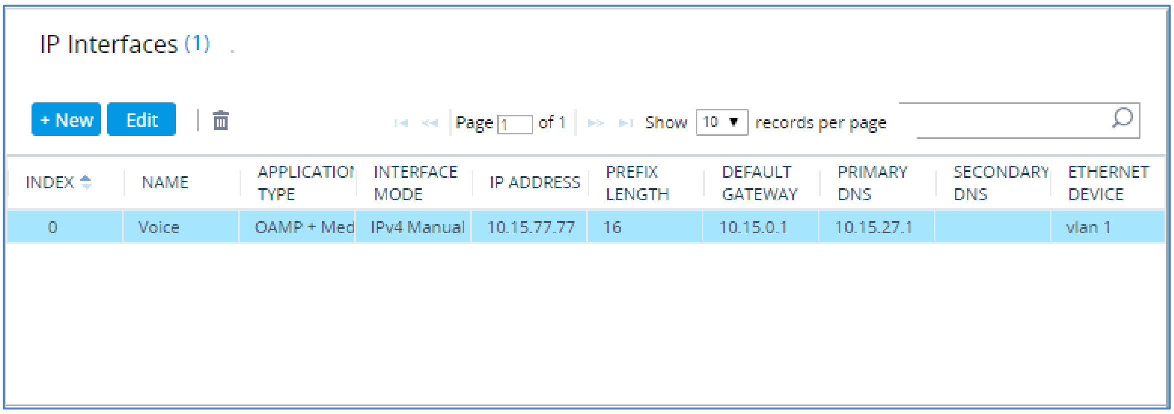
1. Open the IP Interfaces table (**Setup** menu > **IP Network** tab > **Core Entities** folder > **IP Interfaces**).
2. Modify the existing network interface ('Voice'):
   a. Select the 'Index' radio button of the **OAMP + Media + Control** table row, and then click **Edit**.
   b. Configure the interface as follows:

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

3. Click **Apply**.

The figure below shows an example of a configured IP network interface.

Figure 5-4: Example of a Configured Network Interface in IP Interfaces Table



5.2.2 Configure NAT

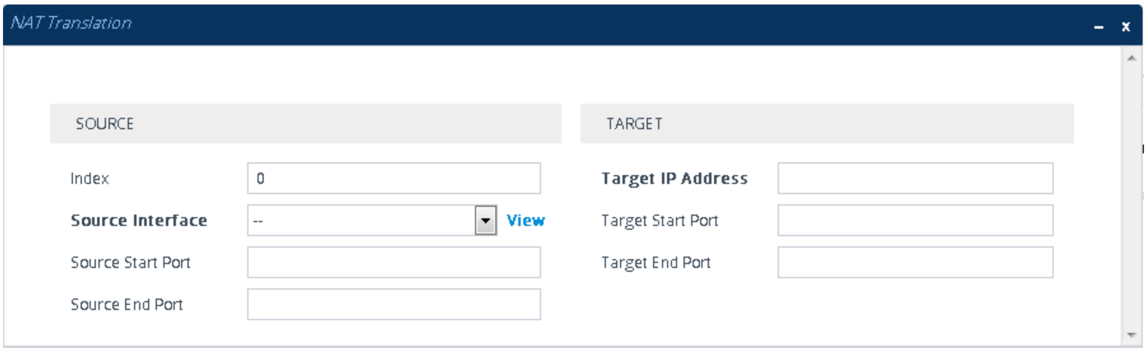
Note:

- 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 BroadSoft service. If the DMZ holds the global-IP-address (no NAT is performed by the firewall) and the Gateway 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**).
2. Click **New**; the following dialog appears:

Figure 5-5: NAT Translation Table - Dialog Box



3. Use the table below as reference when configuring a NAT translation rule.

Figure 5-6: NAT Translation Table Parameter Descriptions

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

4. Click **Apply**.

5.3 Configure General SIP Parameters

This step identifies the device configuration needed to support the SIP General Parameters configuration.

5.3.1 Configure SIP General Settings

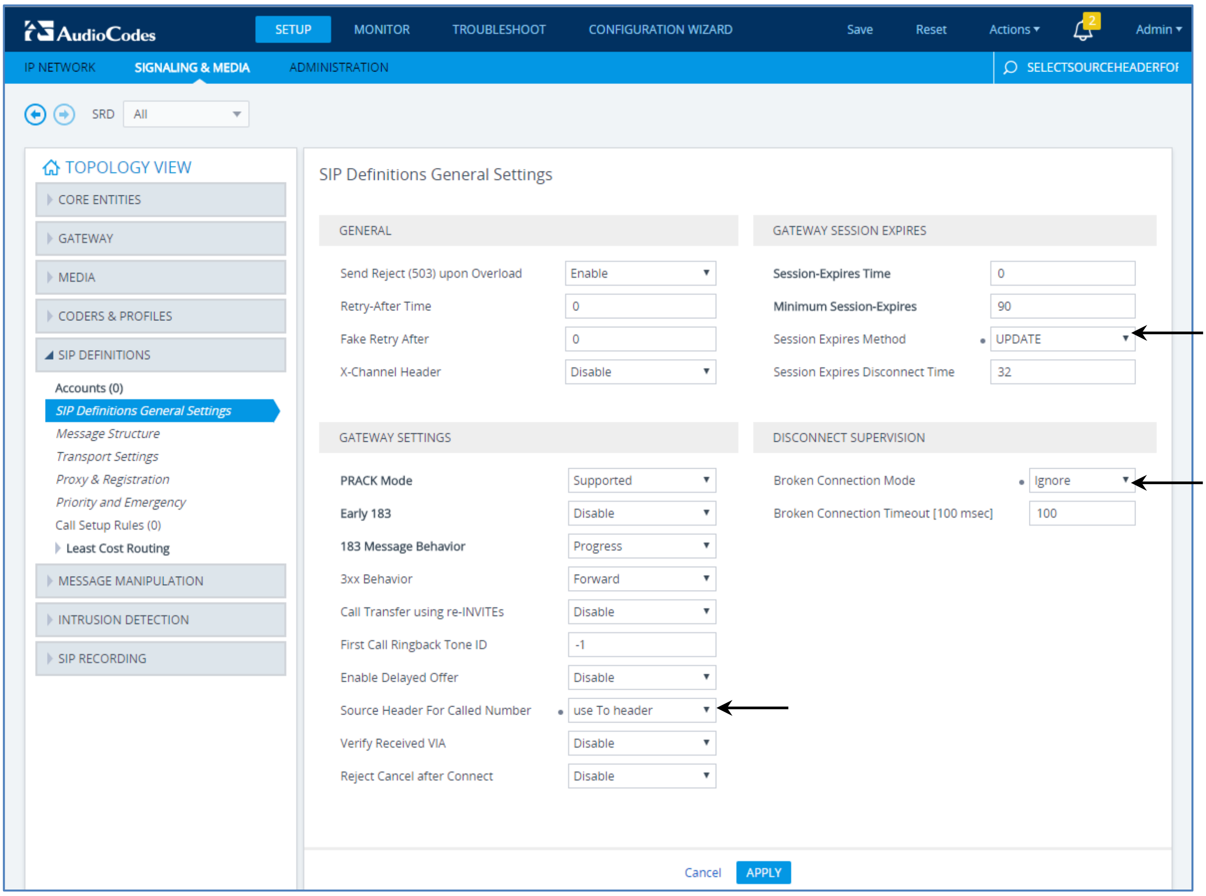
This step shows how to configure the SIP General Settings.

➢ **To configure the SIP General Settings parameters:**

1. Open the SIP Proxy & Registration Parameters page (**Setup** menu > **Signaling & Media** tab > **SIP Definitions** folder > **SIP Definitions General Settings**).
2. Configure following parameters:

Parameter	Value
Gateway Settings	
Source Header For Called Number	**Use To header**
Gateway Session Expires	
Session Expires Method	**Update**
Disconnect Supervision	
Broken Connection Mode	**Ignore**

Figure 5-7: Configuring SIP General Settings Parameters



3. Click **Apply**.

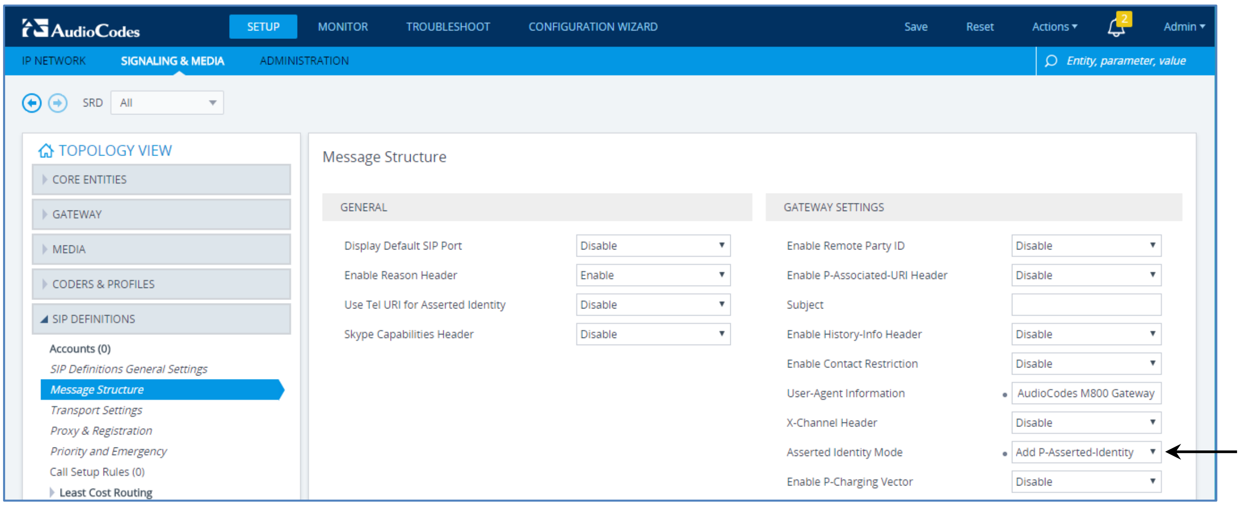
5.3.2 Configure SIP Message Structure Parameters

This step shows how to add SIP P-Asserted Header.

➢ **To configure the SIP Message Structure parameters:**

1. Open the SIP Proxy & Registration Parameters page (**Setup** menu > **Signaling & Media** tab > **SIP Definitions** folder > **Message Structure**).
2. From the 'Asserted Identity Mode' dropdown, select **Add P-Asserted-Identity**.

Figure 5-8: Configuring SIP Message Structure Parameters



3. Click **Apply**.

5.3.3 Configure Registration Parameters

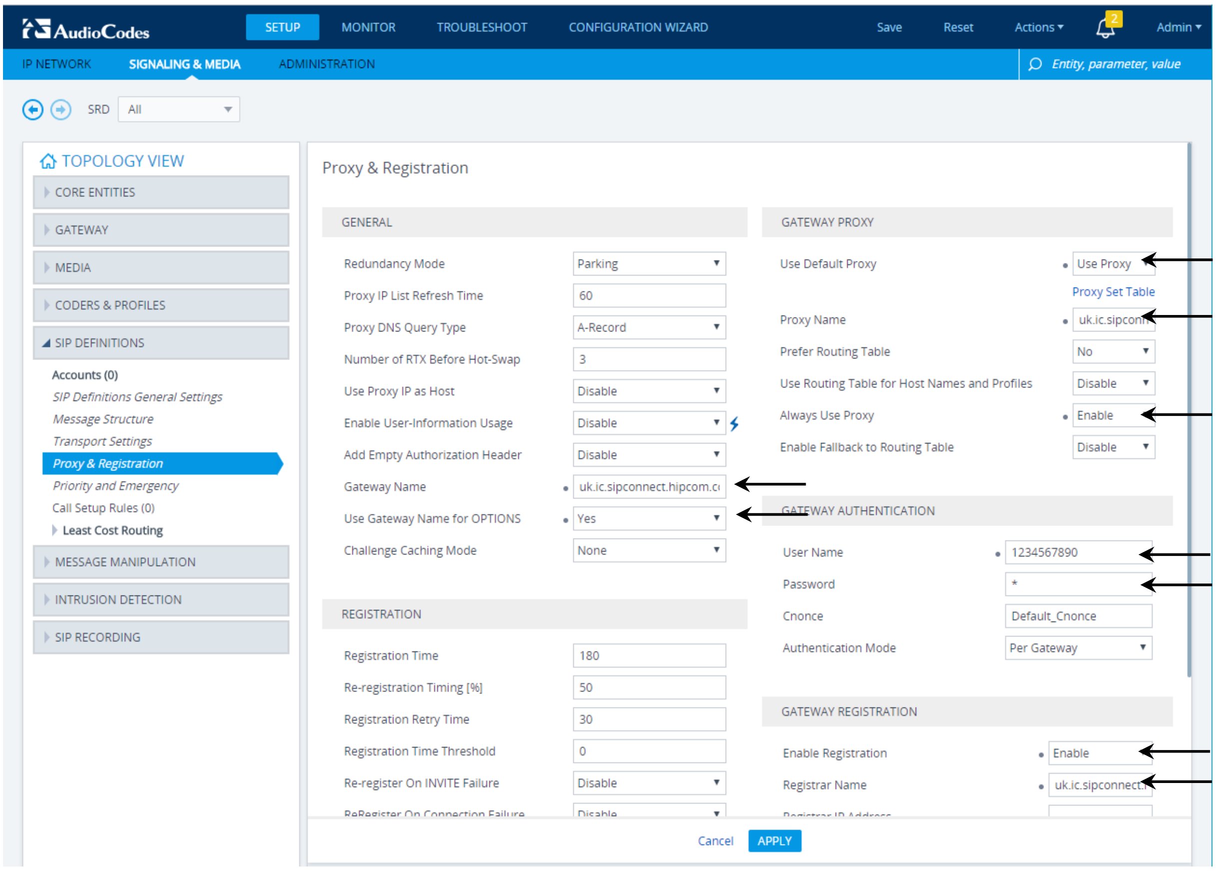
This step shows how to configure the SIP Proxy and Registration parameters, including configuring a Proxy Name, Registrar Name, Registration and Subscription modes.

➢ **To configure the SIP Proxy & Registration parameters:**

1. Open the SIP Proxy & Registration Parameters page (**Setup** menu > **Signaling & Media** tab > **SIP Definitions** folder > **Proxy & Registration**).
2. Configure following parameters:

Parameter	Value
Gateway Name	**uk.ic.sipconnect.hipcom.co.uk**
Use Gateway Name for OPTIONS	**Yes**
Use Default Proxy	**Use Proxy**
Proxy Name	Per SIP Trunk requirement
Always Use Proxy	**Enable**
Gateway Authentication	
User Name	Trunk Group Pilot User
Password	Trunk Group Pilot User Password
Authentication Mode	**Per Gateway**
Gateway Registration	
Enable Registration	**Enable**
Registrar Name	**uk.ic.sipconnect.hipcom.co.uk**

Figure 5-9: Configuring Proxy & Registration Parameters



5.3.4 Configure the SIP Trunk IP Address

This step shows how to configure the Proxy Set toward SIP Trunk. The Proxy Set defines the destination address (IP address or FQDN) of the IP entity server. Proxy Sets can also be used to configure load balancing between multiple servers.

➢ **To configure Proxy Set:**

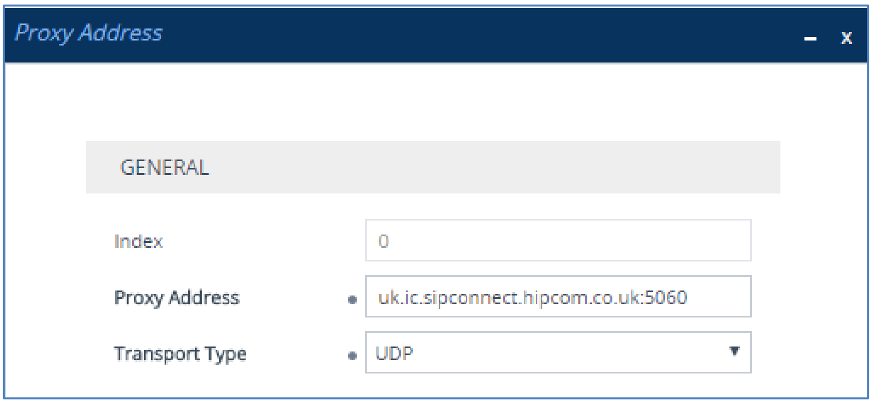
1. Open the Proxy Sets table (**Setup** menu > **Signaling & Media** tab > **Core Entities** folder >**Proxy Sets**).
2. Edit the Proxy Set 0 (you can identify it by the 'Proxy Name' field).

Parameter	Value
Index	**0**
Proxy Keep-Alive	**Using Options**

a. Click the **Proxy Address** link located below the table; the Proxy Address table opens.

b. Click **New**; the following dialog box appears:

Figure 5-10: Configuring Proxy Address for SIP Trunk



c. Configure the address of the Proxy Set per the parameters described in the table below.

Parameter	Value
Index	**0**
Proxy Address	**uk.ic.sipconnect.hipcom.co.uk:5060** (SIP Trunk IP address / FQDN and destination port)
Transport Type	**UDP** (Network transport type for the SIP Trunk)

d. Click **Apply**.

5.3.5 Configure Message Manipulation Rules

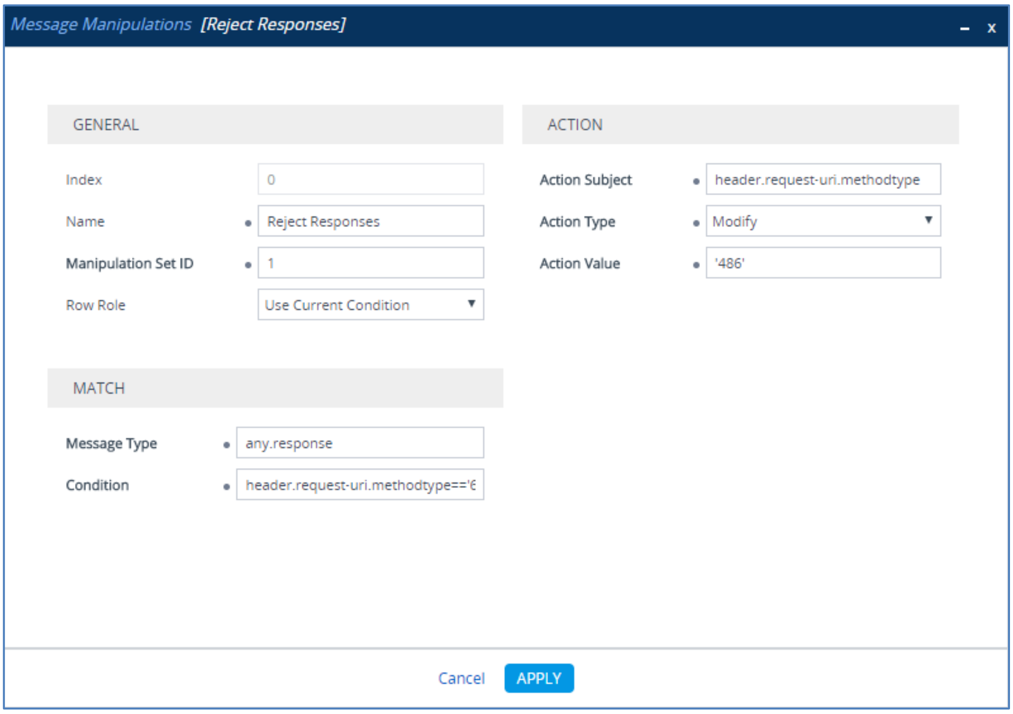
This step describes how to configure SIP message manipulation rules, which can include insertion, removal, and/or modification of SIP headers. Manipulation rules are grouped into Manipulation Sets, enabling you to apply multiple rules to the same SIP message (IP entity). Configured SIP message manipulation rules will be assigned as gateway outbound message manipulation set and will be applied to all outbound messages.

➢ **To configure SIP message manipulation rule:**

1. Open the Message Manipulations page (**Setup** menu > **Signaling & Media** tab > **Message Manipulation** folder > **Message Manipulations**).
2. Configure a new manipulation rule (Manipulation Set 1) for BroadSoft SIP Trunk. This rule applies to response messages sent to the BroadSoft SIP Trunk for Rejected Calls initiated by the PBX. This replaces the '503' and '603' method types with the value '486', because BroadSoft SIP Trunk not recognizes these method types.

Parameter	Value
Index	**0**
Name	**Reject Responses**
Manipulation Set ID	**1**
Message Type	**any.response**
Condition	**header.request-uri.methodtype=='603' OR header.request-uri.methodtype=='503'**
Action Subject	**header.request-uri.methodtype**
Action Type	**Modify**
Action Value	**'486'**

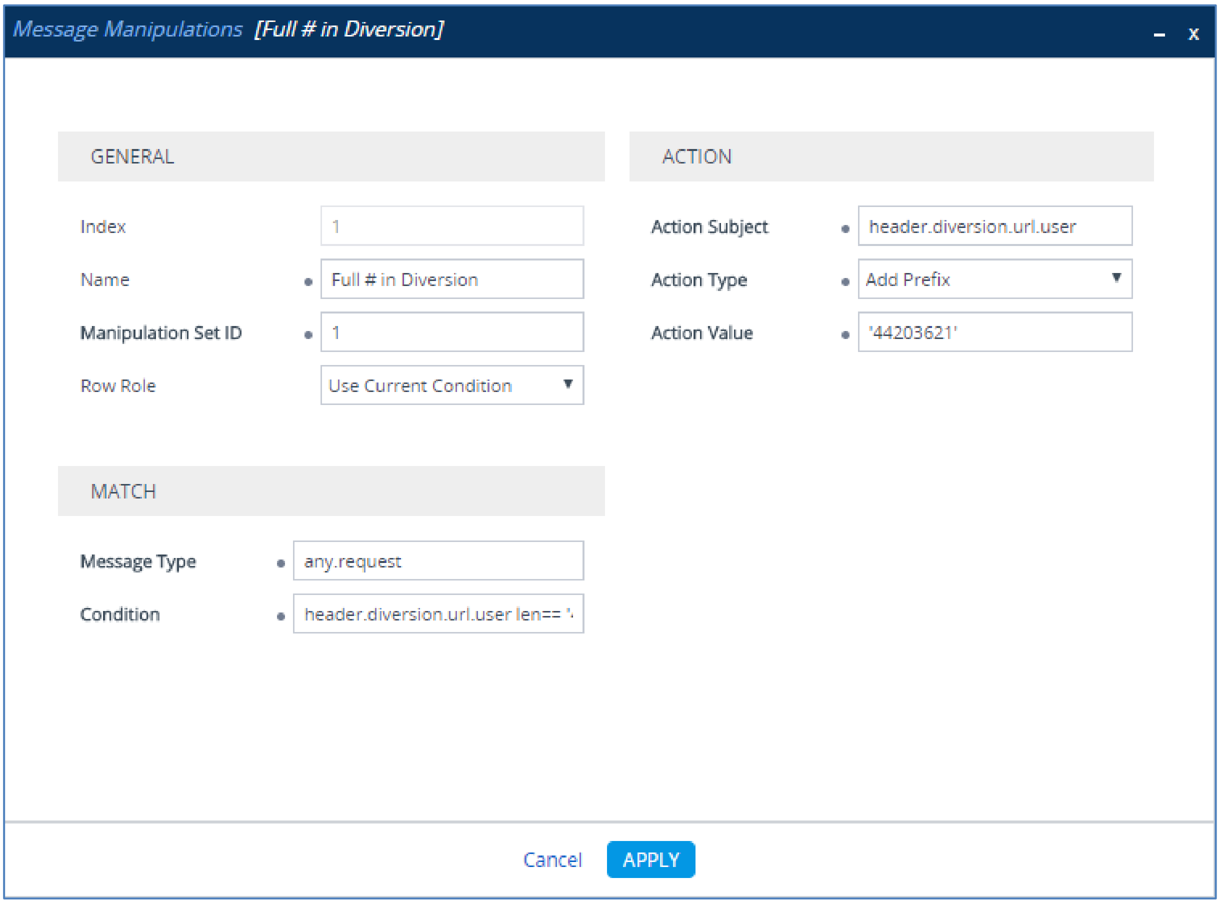
Figure 5-11: Configuring SIP Message Manipulation Rule 0 (for BroadSoft SIP Trunk)



3. Configure another manipulation rule (Manipulation Set 1) for BroadSoft SIP Trunk. This rule applies to messages sent to the BroadSoft SIP Trunk in a call forward scenario. This add prefix to the user part of SIP Diversion Header to complete to the full number.

Parameter	Value
Index	**1**
Name	**Full # in Diversion**
Manipulation Set ID	**1**
Message Type	**any.request**
Condition	**header.diversion.url.user len== '4'**
Action Subject	**header.diversion.url.user**
Action Type	**Add Prefix**
Action Value	**'44203621'**

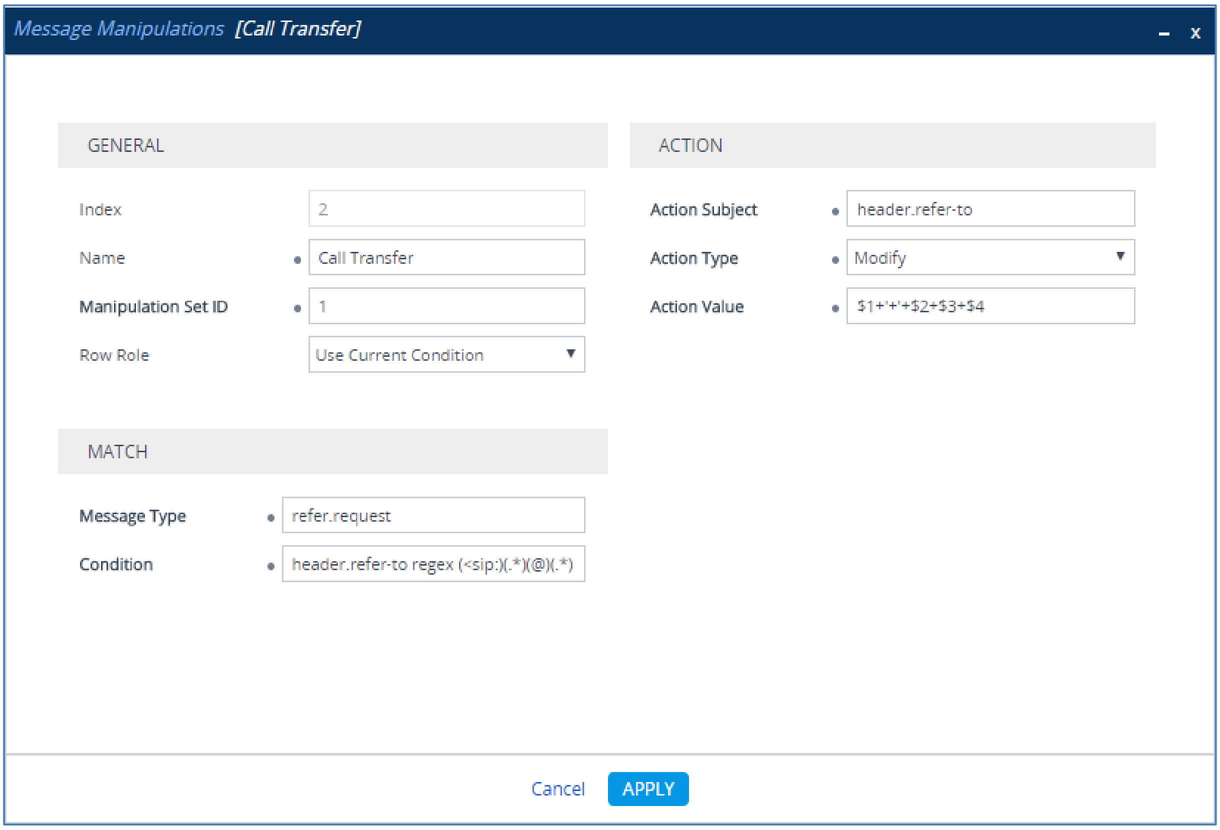
Figure 5-12: Configuring SIP Message Manipulation Rule 1 (for BroadSoft SIP Trunk)



4. Configure another manipulation rule (Manipulation Set 1) for BroadSoft SIP Trunk. This rule applies to messages sent to the BroadSoft SIP Trunk in a call transfer scenario. This will add '+' prefix to the user part of SIP Refer-To Header to complete the BroadSoft SIP Trunk number conversion.

Parameter	Value
Index	**2**
Name	**Call Transfer**
Manipulation Set ID	**1**
Message Type	**refer.request**
Condition	**header.refer-to regex (<sip:)(.*)(@)(.*)**
Action Subject	**header.refer-to**
Action Type	**Modify**
Action Value	**$1+'+'+$2+$3+$4**

Figure 5-13: Configuring SIP Message Manipulation Rule 2 (for BroadSoft SIP Trunk)



5. Configure another manipulation rule (Manipulation Set 1) for BroadSoft SIP Trunk. This rule applies to messages sent to the BroadSoft SIP Trunk in a call forward scenario. This replaces the user part of the SIP From Header with the value from the SIP Diversion Header.

Parameter	Value
Index	**3**
Name	**Call Forward**
Manipulation Set ID	**1**
Message Type	**invite**
Condition	**header.diversion exists**
Action Subject	**header.from.url.user**
Action Type	**Modify**
Action Value	**header.diversion.url.user**

Figure 5-14: Configuring SIP Message Manipulation Rule 3 (for BroadSoft SIP Trunk)

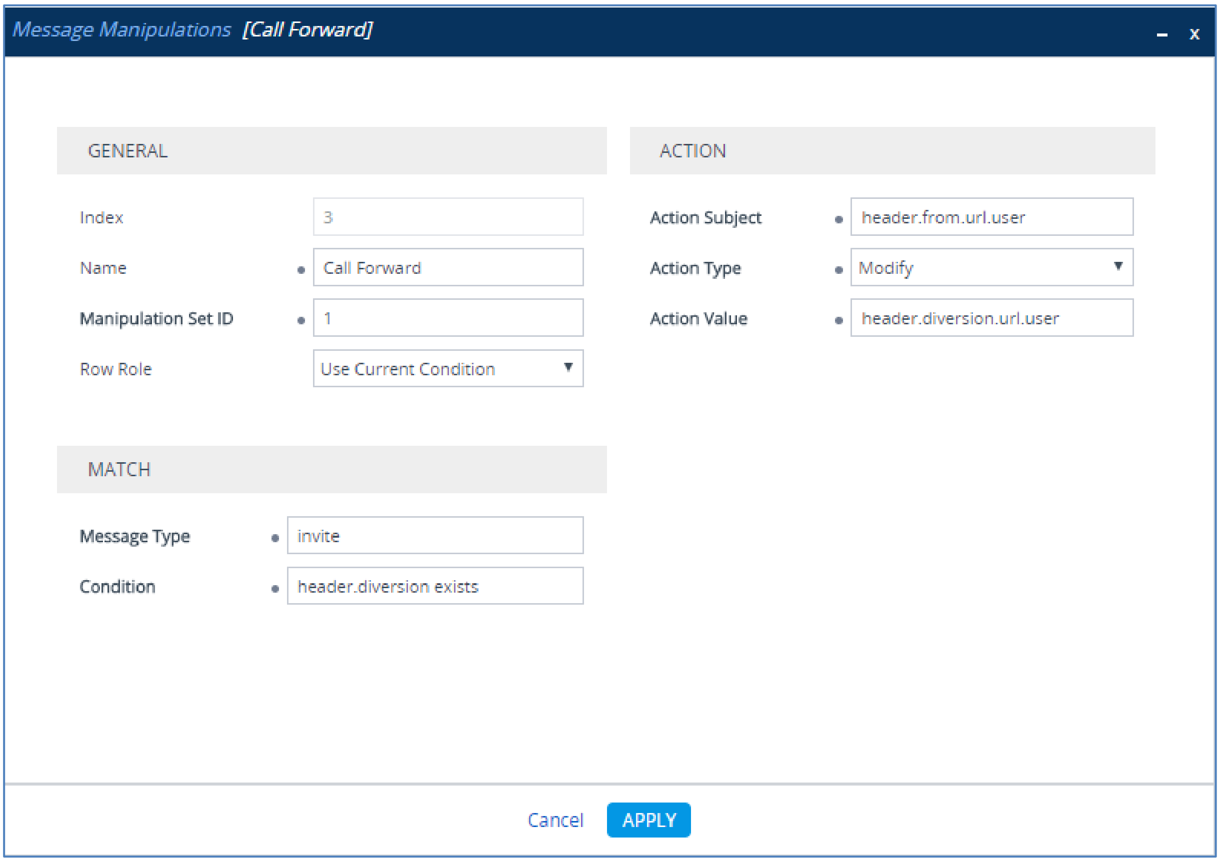
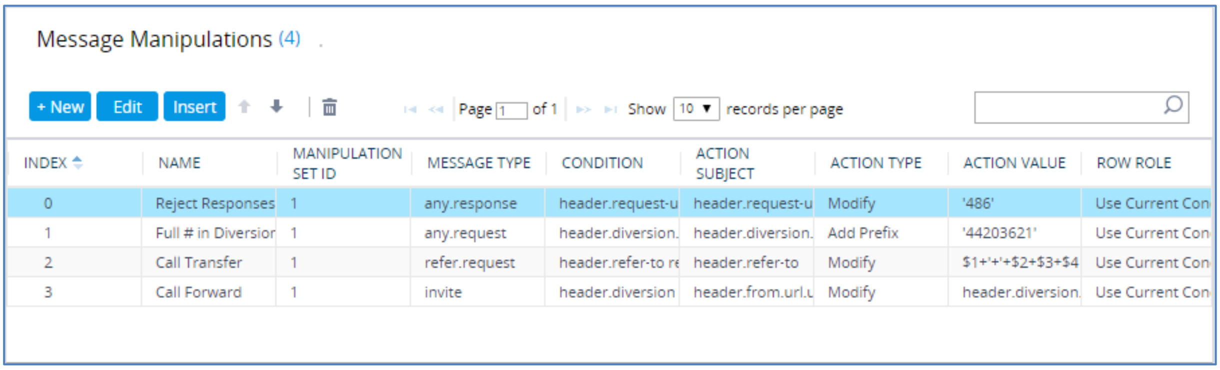


Figure 5-15: Example of Configured SIP Message Manipulation Rules


Message Manipulations (4)

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

INDEX	NAME	MANIPULATION SET ID	MESSAGE TYPE	CONDITION	ACTION SUBJECT	ACTION TYPE	ACTION VALUE	ROW ROLE
0	Reject Responses	1	any.response	header.request-u	header.request-u	Modify	'486'	Use Current Con
1	Full # in Diversior	1	any.request	header.diversion.	header.diversion.	Add Prefix	'44203621'	Use Current Con
2	Call Transfer	1	refer.request	header.refer-to re	header.refer-to	Modify	$1+'+'+$2+$3+$4	Use Current Con
3	Call Forward	1	invite	header.diversion	header.from.url.u	Modify	header.diversion.	Use Current Con

The table displayed below includes SIP message manipulation rules which are grouped together under Manipulation Set ID 1 and which are executed for messages sent to the BroadSoft SIP Trunk. These rules are specifically required to enable proper interworking between BroadSoft SIP Trunk and PBX. Refer to the *User's Manual* for further details concerning the full capabilities of header manipulation.

Rule Index	Rule Description	Reason for Introducing Rule
0	This rule applies to response messages sent to the BroadSoft SIP Trunk for Rejected Calls initiated by the PBX. This replaces the '503' and '603' method types with the value '486'.	The BroadSoft SIP Trunk not recognizes these method types and continue to try to setup call to the PBX.
1	This rule applies to messages sent to the BroadSoft SIP Trunk in a call forward scenario. This add prefix to the user part of SIP Diversion Header to complete to the full number.	If the PBX is configured with endpoints in 4-digits format in the Call Forward scenario, SIP Diversion Header will present a 4-digit number, that will cause a problem in the Forward Call setup.
2	This rule applies to messages sent to the BroadSoft SIP Trunk in a call transfer scenario. This will add '+' prefix to the user part of SIP Refer-To Header.	For complete the BroadSoft SIP Trunk number conversion.
3	This rule applies to messages sent to the BroadSoft SIP Trunk in a call forward scenario. This replaces the user part of the SIP From Header with the value from the SIP Diversion Header.	For Call Forward scenarios, BroadSoft SIP Trunk needs that User part in SIP From Header will be defined number. In order to do this, User part of the SIP From Header replaced with the value from the SIP Diversion Header.

5.4 Configure Coders

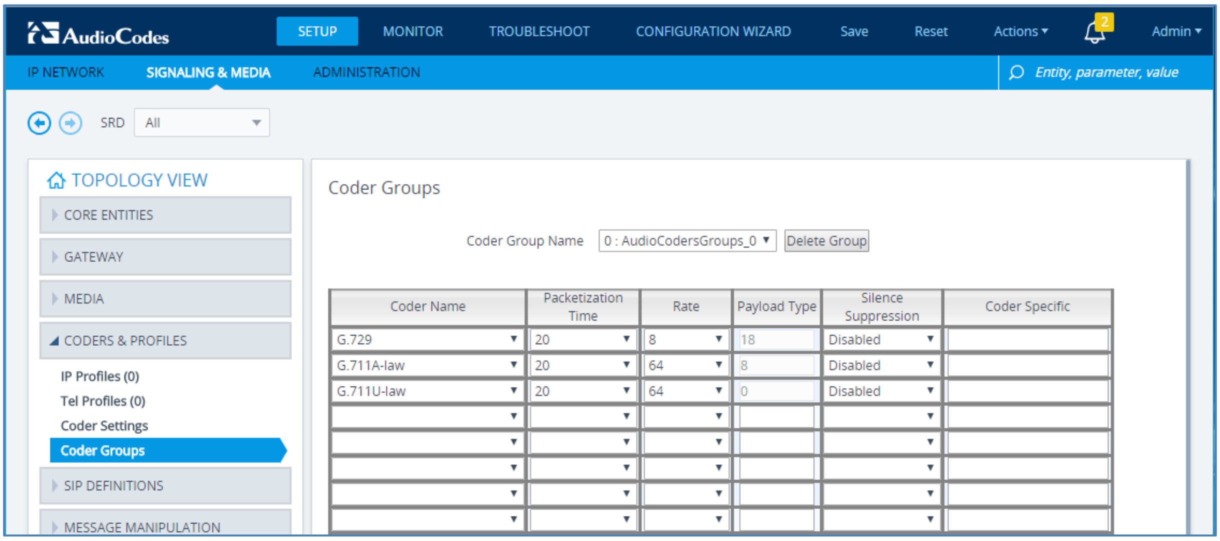
This step describes how to configure coders (termed *Coder Group*) per BroadSoft SIP Trunk requirement.

➢ **To configure coders:**

1. Open the Coder Groups table (**Setup** menu > **Signaling & Media** tab > **Coders & Profiles** folder > **Coder Groups**).
2. Configure a Default Coder Group:

Parameter	Value
Coder Group Name	**AudioCodersGroups_0**
Coder Name	**G.729**
Coder Name	**G.711A-law**
Coder Name	**G.711U-law**

Figure 5-16: Configuring a Default Coder Group



5.5 Configure PSTN Interface

This section describes the configuration of the public switched telephone network (PSTN) related parameters.

5.5.1 Configure PRI Trunk Settings

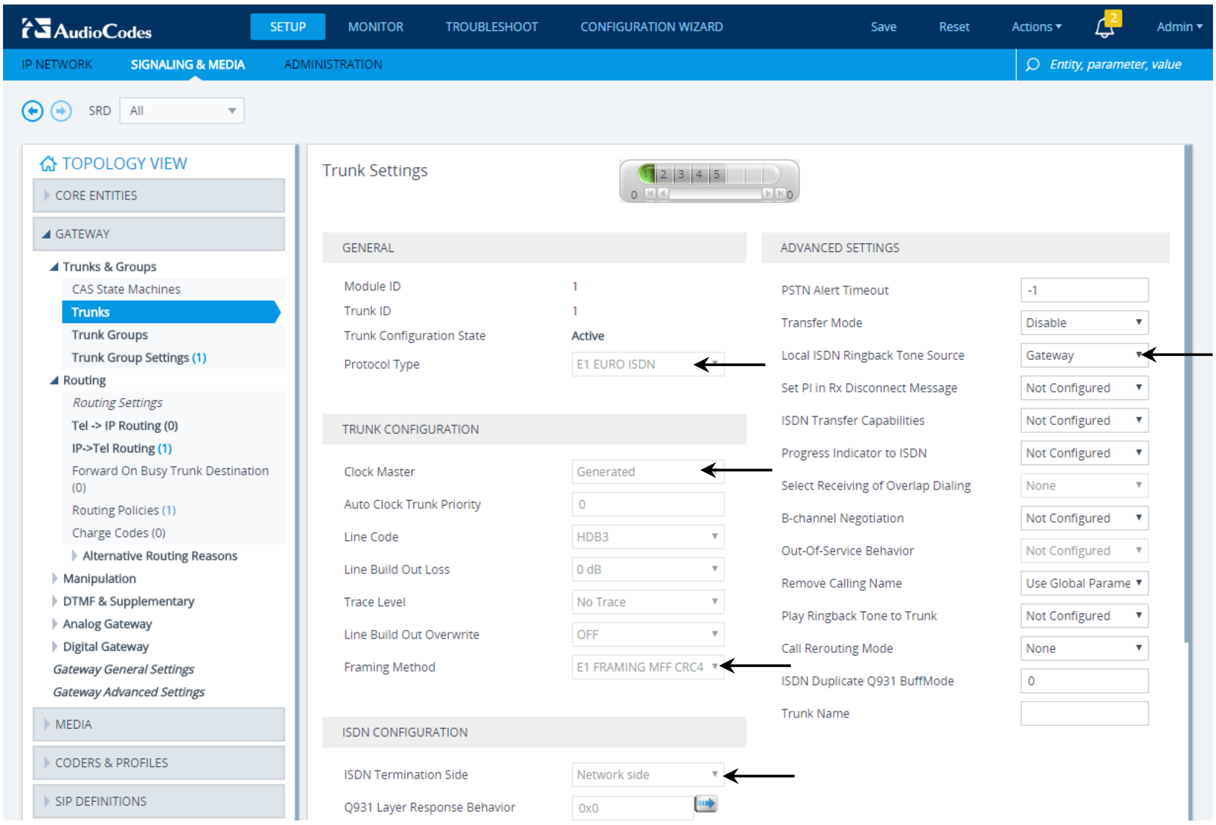
This step shows how to configure the PRI Trunk.

➢ **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 per PSTN network:

Parameter	Value
Protocol Type	**E1 EURO ISDN**
Clock Master	**Generated** (The device is clock master) **Recovered** (The device slaves from the line clock)
Framing Method	**E1 Framing MFF CRC4 Ext** (per remote side, PBX or PSTN, definitions)
ISDN Termination Side	**Network side** or **User side** (per remote side definitions)
Local ISDN Ringback Tone Source	**Gateway**

Figure 5-17: Configuring the PRI PSTN Interface



3. Repeat for another PRI trunks if applicable (Mediant 800B and Mediant 1000B)
4. **Reset the device with a save-to-flash for your settings to take effect.**

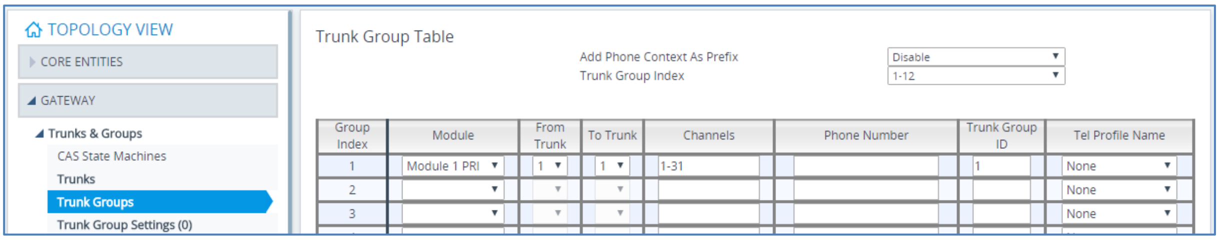
5.5.2 Configure Trunk Group Parameters

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.

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

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

Figure 5-18: 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).

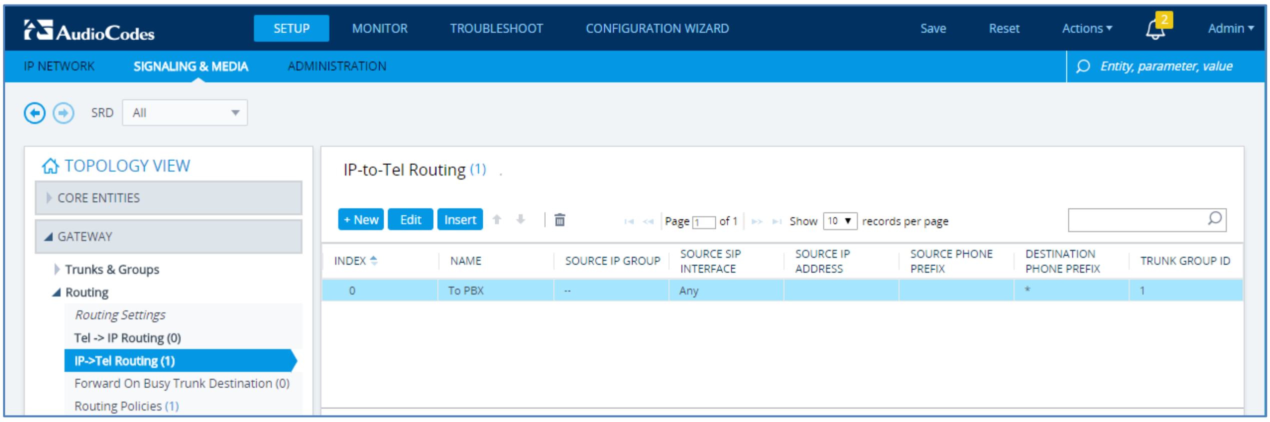
5.5.3 Configure Inbound IP Routing

This section shows configuring Mediant PRI Gateway Inbound (IP-to-Tel) Routing. When having more than one TDM interface, 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 5-19: Configuring Inbound IP Routing Rules



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

5.6 Miscellaneous Configuration

This section describes miscellaneous Mediant gateway configuration.

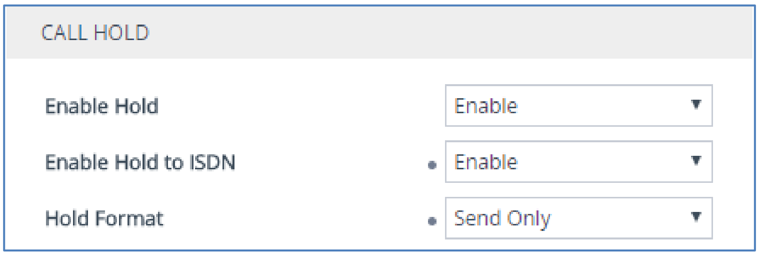
5.6.1 Configure Supplementary Services

This step describes how to configure Hold Format.

➢ **To configure Hold Format:**

1. Open the Gateway Supplementary Services Settings page (**Setup** menu > **Signaling & Media** tab > **Gateway** folder > **DTMF & Supplementary** > **Supplementary Services Settings**).
2. From the 'Enable Hold to ISDN' drop-down list, select **Enable**.
3. From the 'Hold Format' drop-down list, select **Send Only**.

Figure 5-20: Configuring Hold Format



4. Click **Apply**.

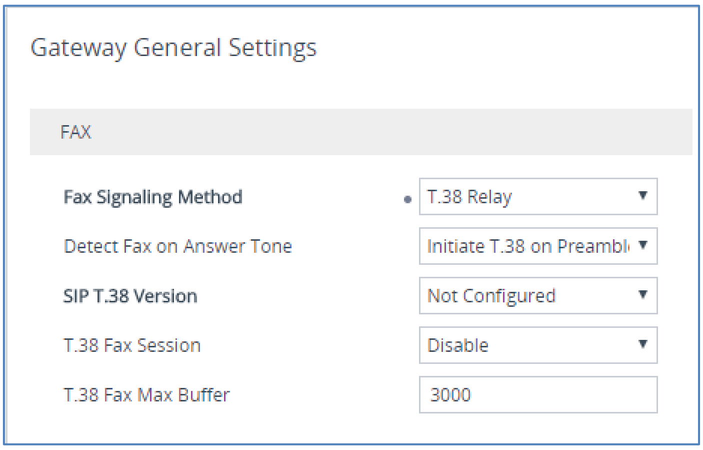
5.6.2 Configure Gateway General Settings

This step describes how to configure the Mediant Gateway to enable T.38 Fax Signaling Method and to play ring-back tone to PRI trunk.

➢ **To configure Gateway General Settings:**

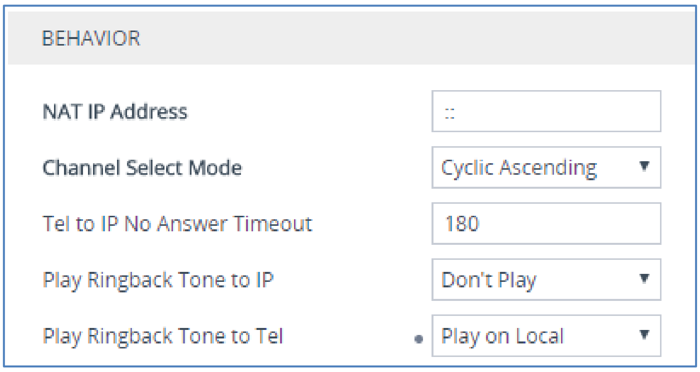
1. Open the Gateway General Settings page (**Setup** menu > **Signaling & Media** tab > **Gateway** folder > **Gateway General Settings**).
2. From the 'Fax Signaling Method' drop-down list, select **T.38 Relay**.

Figure 5-21: Configuring Fax Signaling Method



3. From the 'Play Ringback Tone to Tel' drop-down list, select **Play on Local**.

Figure 5-22: Configuring to play ringback tone to PSTN



4. Click **Apply**.

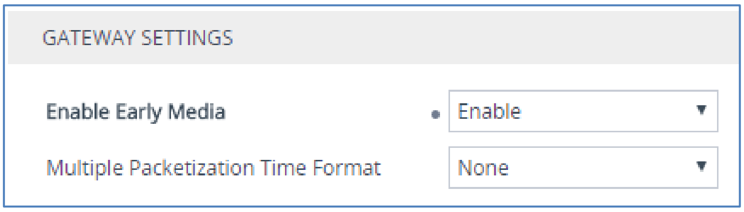
5.6.3 Configure Early Media

This step describes how to configure the Mediant Gateway to enable Early Media.

➢ **To configure Early Media:**

1. Open the Media Settings page (**Setup** menu > **Signaling & Media** tab > **Media** folder > **Media Settings**).
2. From the 'Enable Early Media' drop-down list, select **Enable**.

Figure 5-23: Configuring Early Media



3. Click **Apply**.

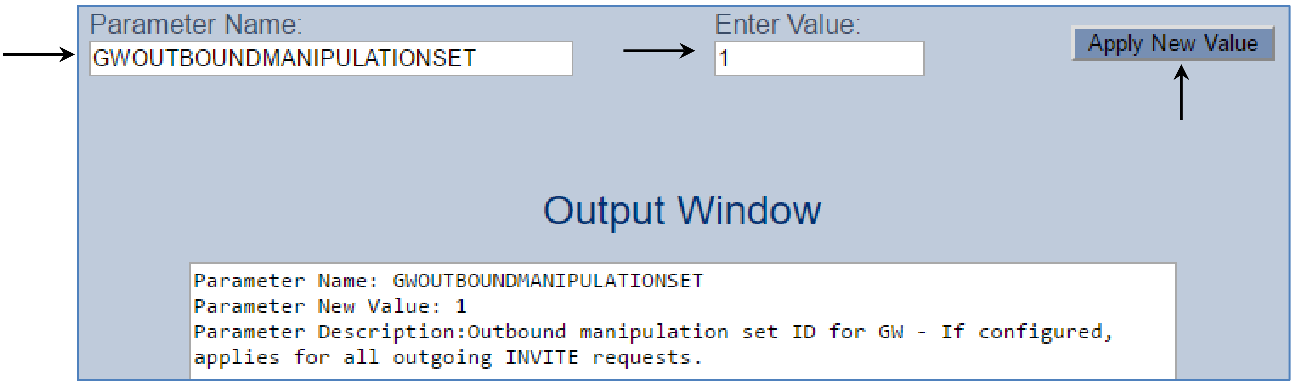
5.6.4 Configure Gateway Manipulation Set

This step describes how to configure the Mediant Gateway outbound manipulation set number.

➢ **To configure Gateway Outbound Manipulation Set number:**

1. Open the Admin page.
2. Append the case-sensitive suffix ‘AdminPage’ to the device's IP address in your Web browser's URL field (e.g., http://10.15.77.55/AdminPage).
3. In the left pane of the page that opens, click ***ini* Parameters**.

Figure 5-24: Configuring Gateway Outbound Manipulation Set number in AdminPage



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

Parameter	Value
GWOUTBOUNDMANIPULATIONSET	**1**

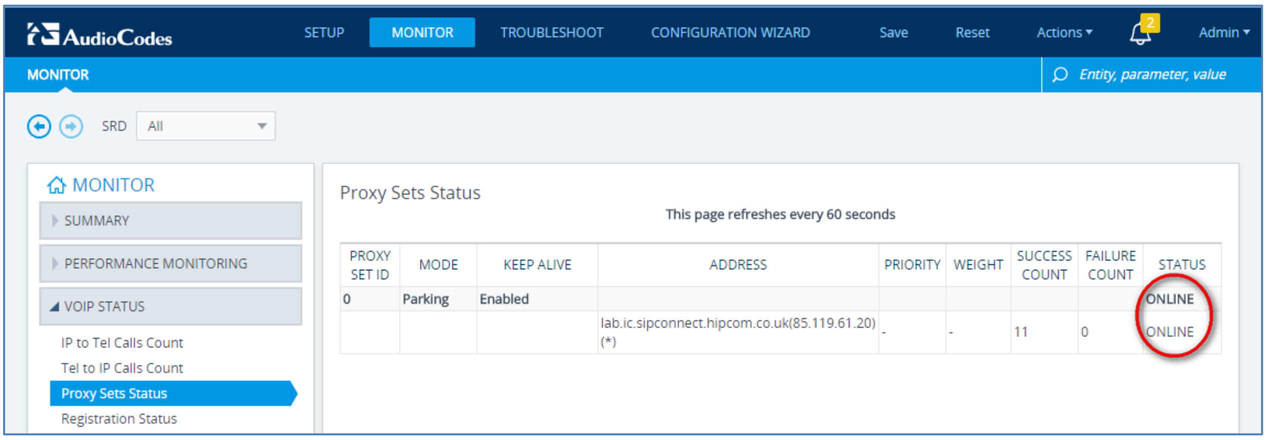
5. Click the **Apply New Value** button for each field.

5.7 Check the SIP Trunk Registration Status

➢ To check if the device successfully registered with BroadSoft service:

1. Open the Registration Status page (**Status** & **Diagnostics** tab > **VoIP Status** > **Registration Status**).
2. Check the **Proxy Sets Status**. A successful registration will show as **ONLINE** (see the figure below).

Figure 5-25: Successful SIP Trunk Registration



Note: If the status of the Proxy Sets shows OFFLINE, check your WAN connectivity:

- Check Ethernet wiring
- DMZ configuration may not be correct on the enterprise firewall
- Check IP address configuration (**Setup** menu > **IP Network** tab > **Core Entities** folder > **Static Routes**)
- Check proxy (SIP Trunk) configuration (**Setup** menu > **Signaling & Media** tab > **SIP Definitions** folder > **Proxy & Registration**)

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

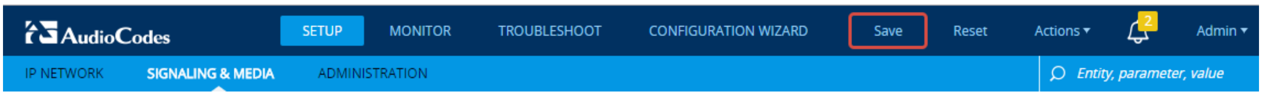
If future remote management is required, first ask the end customer's IT administrator to open the appropriate port (e.g., HTTP or HTTPS port) to manage the device.

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. Therefore, make sure the firewall allows the ports required for call handling. See Section 5.2 for more information.

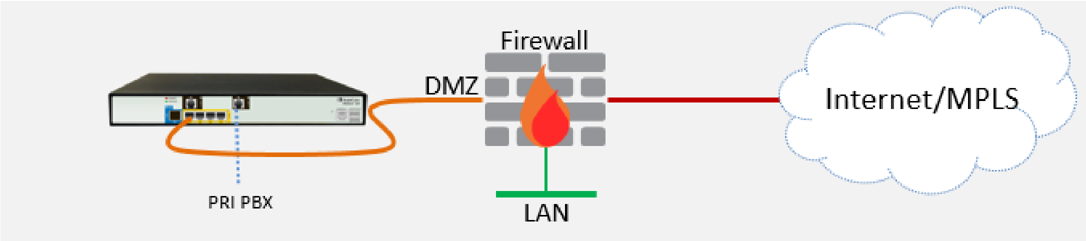
Save configuration as follows:

1. On the toolbar, click **Save** button:



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:



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. Connect the E1/T1 trunk interface:
   a. Connect the E1/T1 trunk cable to the device's E1/T1 port.
   b. Connect the other end of the trunk cable to your PBX switch.

Figure 6-1: Mediant 500 Cabling E1/T1 Port

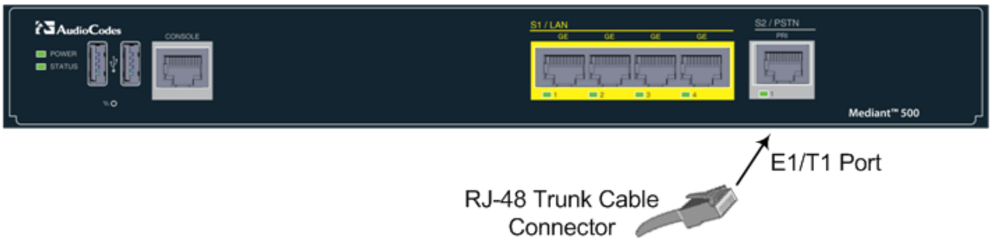


Figure 6-2: Mediant 800B Cabling E1/T1 Port

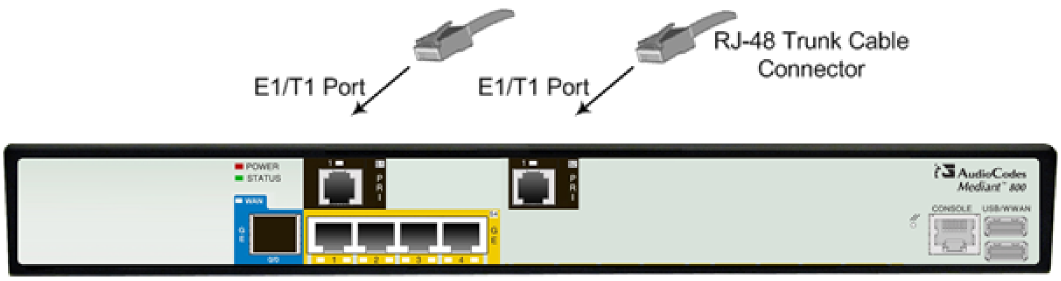


Figure 6-2: Mediant 1000B Cabling E1/T1 Port

This page is intentionally left blank.

A Troubleshooting

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

A.1 Connecting to CLI

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

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

A.2 Enabling Logging on CLI

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

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

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

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

Contact us: www.audiocodes.com/info
Website: www.audiocodes.com

Document #: LTRT-14020