

BroadCloud Hosted UC Solution using AudioCodes Mediant™ CRP

Version 7.2



Table of Contents

1	Introduction	5
1.1	Making BroadCloud Preparations	5
1.2	Component Information.....	5
1.2.1	AudioCodes CRP Version	5
1.2.2	BroadCloud Hosted UC Version.....	5
1.2.3	Solution Topology	6
2	Installing the Hardware.....	7
2.1	Mediant 500L	7
2.1.1	Front Panel	7
2.1.2	Rear Panel.....	7
2.1.3	Cabling.....	8
2.1.3.1	Connecting Ethernet Interfaces.....	8
2.1.3.2	Connecting to the Power Supply.....	9
2.1.4	Powering the Device On / Off	10
2.2	Mediant 500	11
2.2.1	Cabling.....	12
2.2.1.1	Grounding the Device.....	12
2.2.1.2	Connecting Ethernet Interfaces.....	12
2.2.1.3	Connecting to the Power Supply	13
2.3	Mediant 800B.....	15
2.3.1	Front Panel	15
2.3.2	Front Panel LEDs	15
2.3.2.1	Operational Status LEDs.....	15
2.3.3	Rear Panel.....	16
2.3.4	Cabling.....	16
2.3.4.1	Grounding the Device.....	16
2.3.4.2	Connecting to Ethernet.....	16
2.3.5	Powering up.....	17
2.4	Mediant 2600	19
2.4.1	Front Panel	19
2.4.2	Rear Panel.....	19
2.4.3	Cabling.....	20
2.4.3.1	Grounding the Device.....	20
2.4.3.2	Connecting to Ethernet.....	20
2.4.3.3	Connecting to the Power Supply	21
3	Connecting to the Management Interface	23
3.1	Default OAMP IP Address.....	23
3.2	Connecting to the Embedded Web Server.....	23
3.2.1	Change Default Management User Login Passwords	24
4	Configuring the Device	25
4.1	Step 1: Download, Install BroadCloud Certified Firmware / Configuration.....	25
4.2	Step 2: Configure a Network Interface for the Device	30
4.2.1	Step 2a: Configure Network Interfaces.....	31
4.2.2	Step 2b: Configure NAT.....	32
4.3	Step 3: Configure the UDP Ports for RTP between CRP and IP-Phones and/or ATA Devices.....	34
4.4	Step 4: Adopt Classification Policy for CRP Users (if Required).....	36
4.5	Step 5: Check the Connectivity and Registration Status.....	37

4.6	Step 6: Secure Device Access.....	39
4.6.1	Secure Management Access via WAN.....	39
4.7	Step 7: Save the Configuration, Connect to DMZ.....	40
A	Configure PSTN FallBack (if Required).....	41
A.1	Step 1: Cabling.....	41
A.1.1	Connecting BRI to the Mediant 500L.....	41
A.1.2	Connecting ISDN PRI (E1/T1) Trunk to the Mediant 500 and Mediant 800B.....	42
A.2	Step 2: Configure PSTN Trunk Settings.....	43
A.2.1	Step 2a: Configure the BRI PSTN Interface.....	43
A.2.2	Step 2b: Configure PCM Law Select.....	44
A.2.3	Step 2c: Configure the PRI PSTN Interface.....	45
A.3	Step 3: Configure Trunk Group Parameters.....	46
A.3.1	Step 3a: Configure the BRI Trunk Group (for Devices with BRI PSTN Interface)...	46
A.3.2	Step 3b: Configure the PRI Trunk Group (for Devices with PRI PSTN Interface)...	46
A.4	Step 4: Configure CRP Gateway Routing.....	47
A.5	Step 5: Configure SIP Parameters for CRP PSTN Fallback.....	47
A.5.1	Step 5a: Enable the CRPGatewayFallback Parameter.....	47
A.5.2	Step 5b: Update the CRP Gateway Proxy Set.....	48
B	Troubleshooting.....	49
B.1	Connecting to CLI.....	49
B.2	Enabling Logging on CLI.....	49

Notice

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

This document is subject to change without notice.

Date Published: September-07-2017

1 Introduction

This guide shows how to set up AudioCodes' Cloud Resilience Package (referred to as *CRP* in this document) for interworking between BroadCloud's Hosted UC and IP-Phones and/or ATA devices environment.

1.1 Making BroadCloud Preparations

Before reading and using this *Quick Setup Guide*, read the *BroadCloud Hosted Survivability Service Definition* guide available from the BroadCloud knowledgebase (info.broadcloudpbx.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.

1.2 Component Information

1.2.1 AudioCodes CRP Version

Table 1-1: AudioCodes CRP Version

CRP Vendor	AudioCodes
Models	<ul style="list-style-type: none">Mediant 500LMediant 500Mediant 800BMediant 2600 (Without PSTN connectivity)
Software Version	F7.20A.152.003
Protocol	<ul style="list-style-type: none">SIP/UDP (to the BroadCloud Hosted UC Service)SIP/UDP or SIP/TCP (to the IP-Phones and/or ATA devices)

1.2.2 BroadCloud Hosted UC Version

Table 1-2: BroadCloud Version

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

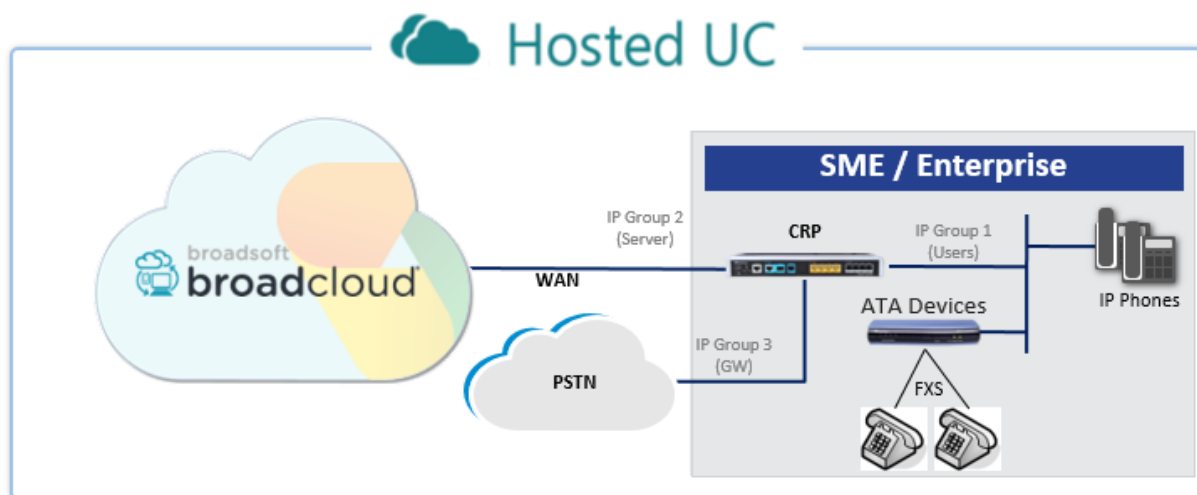
1.2.3 Solution Topology

Interoperability between AudioCodes CRP and BroadCloud Hosted UC Service with the IP-Phones and/or ATA devices was achieved using the following topology setup:

- Enterprise IP-Phones and/or ATA devices
- AudioCodes Mediant CRP device, connecting the enterprise's IP-Phones and/or ATA devices to the BroadCloud Hosted UC service over IP
- Internet/MPLS network connectivity to the BroadCloud Hosted UC service

The figure below illustrates this solution's topology:

Figure 1-1: Solution Topology between CRP, IP-Phones and/or ATA Devices with BroadCloud Hosted UC Service



2 Installing the Hardware

2.1 Mediant 500L

2.1.1 Front Panel

LEDs on the front panel indicate functionality statuses.

Figure 2-1: Front Panel - LEDs



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

Table 2-1: Status LED

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


2.1.2 Rear Panel

Figure 2-2: Rear Panel



Table 2-2: Rear Panel

Item #	Label	Description
1	POWER 12V - - 3A	AC power supply plug entry to connect to the external AC power supply adapter.
2	ON / OFF	Power button which powers on the device when pressed in and powers

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

2.1.3 Cabling

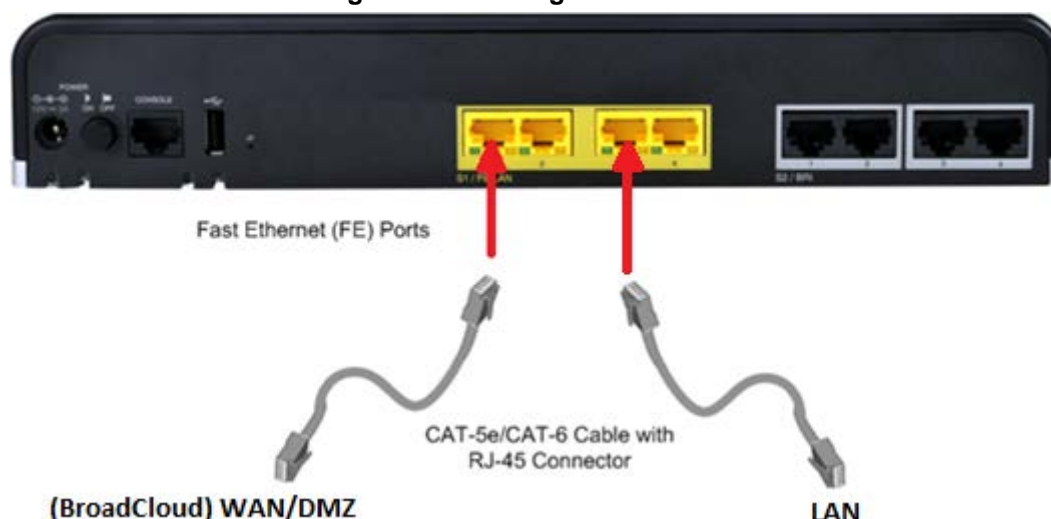
2.1.3.1 Connecting Ethernet Interfaces

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

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

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

Figure 2-3: Cabling Ethernet Ports



➤ **To connect the device to the Enterprise LAN:**

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

2.1.3.2 Connecting to the Power Supply

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

Table 2-3: Power Specifications

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



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

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

Figure 2-4: AC/DC Power Adapter

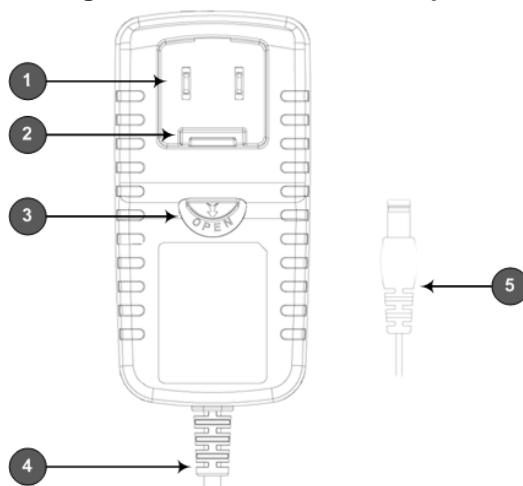


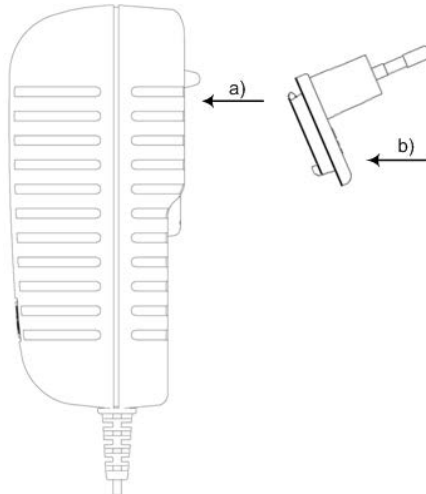
Table 2-4: Power Adapter with Interchangeable Plugs

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

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

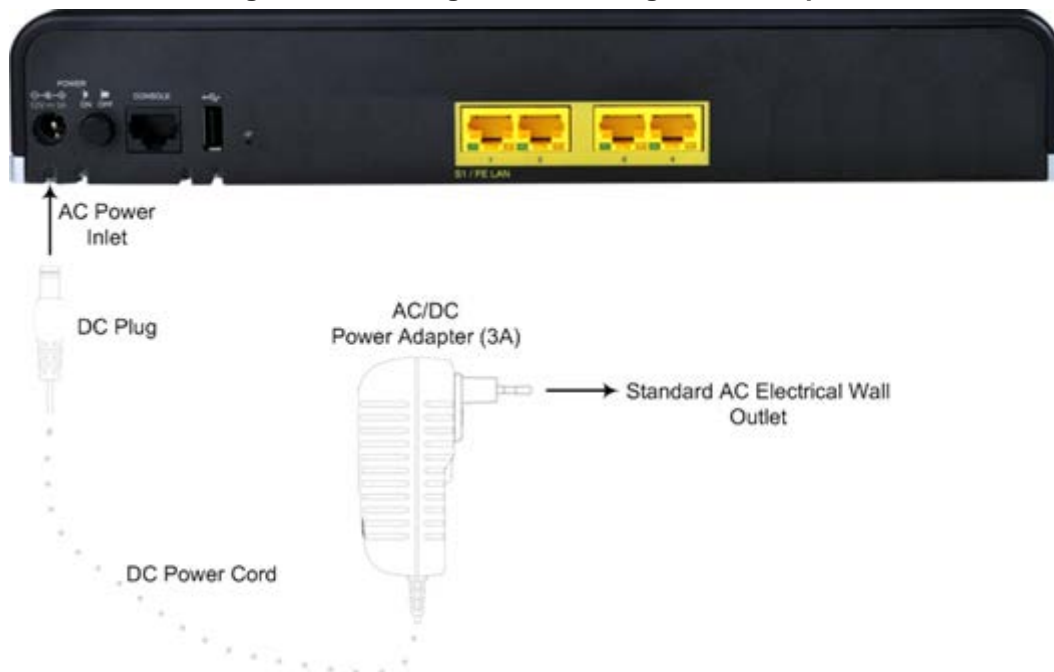
1. Insert the relevant AC plug into the housing power adapter:
 - a. Insert the top part of the plug into the upper part of the housing slot (1).
 - b. Press down on the bottom part of the plug until a click is heard, indicating that the plug is securely inserted in the housing slot. To remove the plug,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

Figure 2-5: Inserting Plug into Power Adapter



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

Figure 2-6: Cabling to Power using Power Adapter



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

2.1.4 Powering the Device On / Off

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

➤ To power on the device:

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

➤ To power off the device:

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

2.2 Mediant 500

Figure 2-7: Front Panel - Ports



Table 2-5: Front Panel

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

Figure 2-8: Rear Panel – Earth and Power

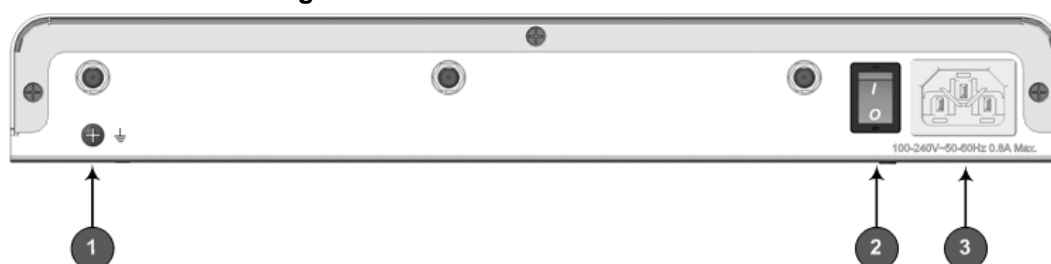



Table 2-6: Rear Panel

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

2.2.1 Cabling

2.2.1.1 Grounding the Device

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



Protective Earthing

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

For Finland: Laite on liltettava suojamaadoituskoskettimilla varustettuun pistorasiaan.

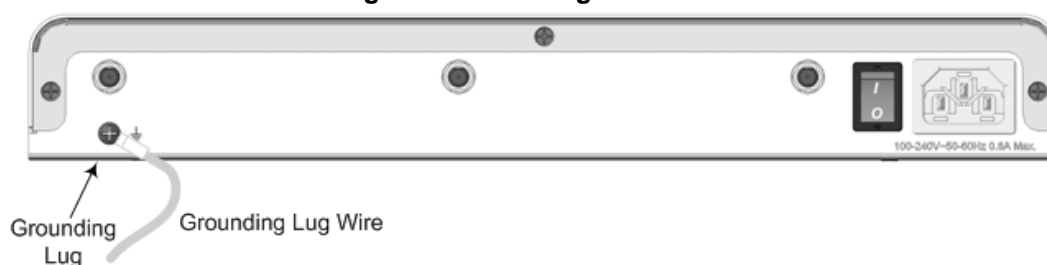
For Norway: Apparatet rna tilkoples jordet stikkontakt.

For Sweden: Apparatens skall anslutas till jordat uttag.

➤ To earth the device:

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

Figure 2-9: Earthing the Device



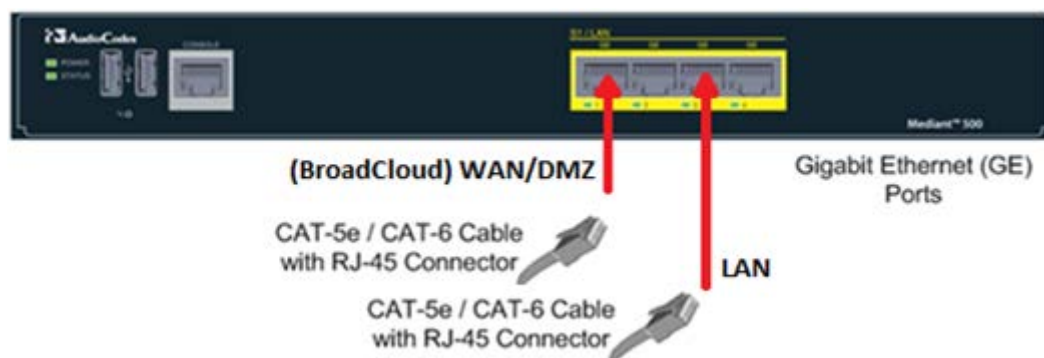
2.2.1.2 Connecting Ethernet Interfaces

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

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

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

Figure 2-10: Cabling the Ethernet Ports



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

➤ **To connect the device to the enterprise LAN:**

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

2.2.1.3 Connecting to the Power Supply

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

Table 2-7: Power Specifications

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

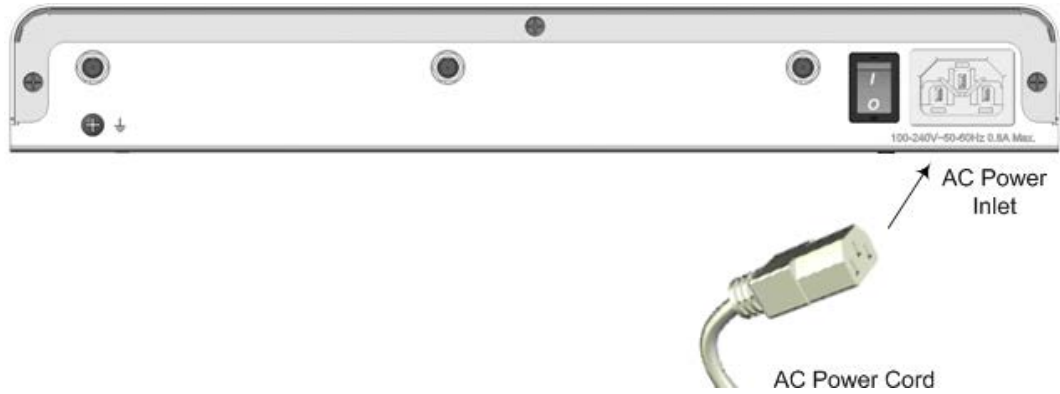


Warnings: The device must be connected to a socket-outlet providing a protective earthing connection. Use only the AC power cord that is supplied with the device.

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

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

Figure 2-11: Connecting to the Power Supply



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

2.3 Mediant 800B

2.3.1 Front Panel

Figure 2-12: Front Panel

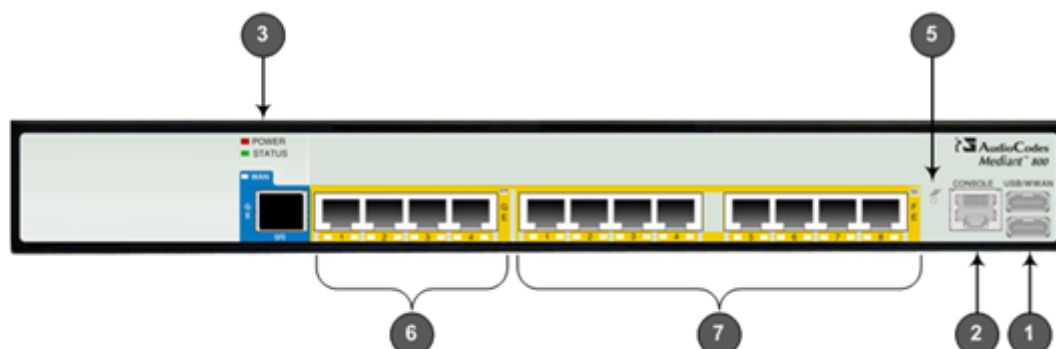


Table 2-8: Front Panel Description

Item #	Label	Description
1	USB/WWAN	N/A
2	RS-232	RS-232 port for serial communication. Cable not included.
3	POWER/STATUS	LEDs indicating power and reboot/initialization status. See also Section 2.3.2 on page 15.
5	-	Reset pinhole button to reset and optionally to restore factory defaults. To restore to factory defaults: Press and hold down the Reset pinhole button with a paper clip or similar pointed object, for at least 12 seconds but no more than 25 .
6	GE	Four 10/100/1000Base-T (Gigabit Ethernet) LAN/WAN ports.
7	FE	N/A

2.3.2 Front Panel LEDs

2.3.2.1 Operational Status LEDs

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

Table 2-9: STATUS LEDs


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

2.3.3 Rear Panel

Figure 2-13: Rear Panel



Table 2-10: Rear Panel

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

2.3.4 Cabling

2.3.4.1 Grounding the Device

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



Protective Earthing

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

For Finland: Laite on liltettava suojamaadoituskoskettimilla varustettuun pistorasiaan.

For Norway: Apparatet rna tilkoples jordnet stikkontakt.

For Sweden: Apparatens skall anslutas till jordat uttag.

➤ To ground the device:

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

Figure 2-14: Grounding the Device

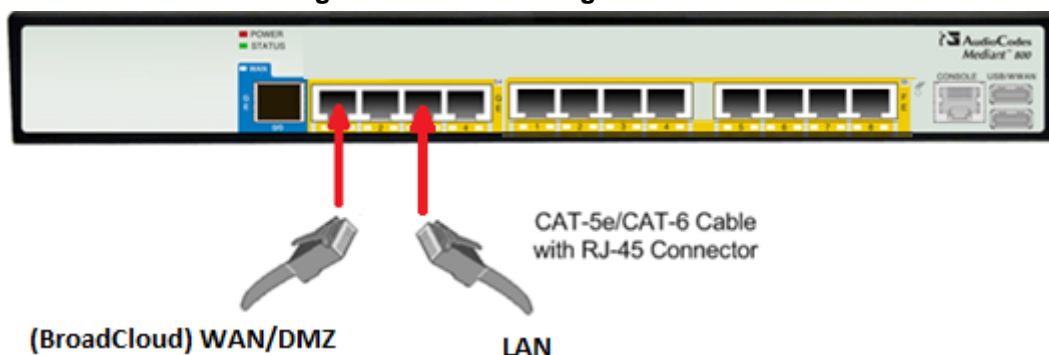


2. Connect the other end to a protective earthing (according local regulations).

2.3.4.2 Connecting to Ethernet

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

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

Figure 2-15: Connecting the LAN Ports

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

2.3.5 Powering up

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

Table 2-11: Power Specifications

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


Warning:

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

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

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

Figure 2-16: Connecting to the Power Supply



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

2.4 Mediant 2600

2.4.1 Front Panel

Figure 2-17: Front Panel – Port Interfaces

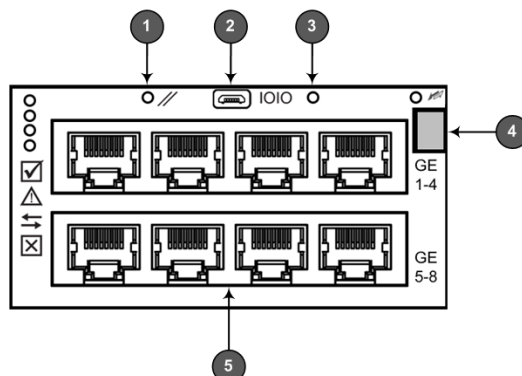


Table 2-12: Front Panel - Ports

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

2.4.2 Rear Panel

Figure 2-18: Rear Panel

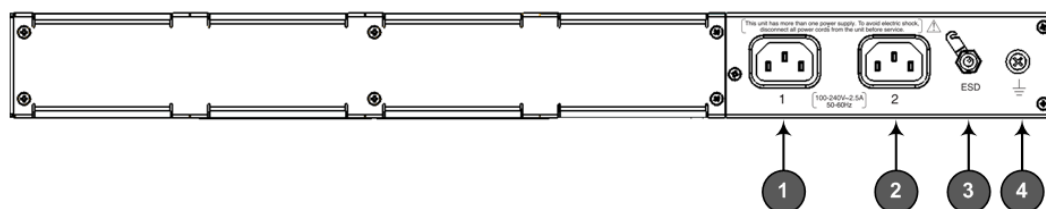


Table 2-13: Rear Panel Description

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

2.4.3 Cabling

2.4.3.1 Grounding the Device

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



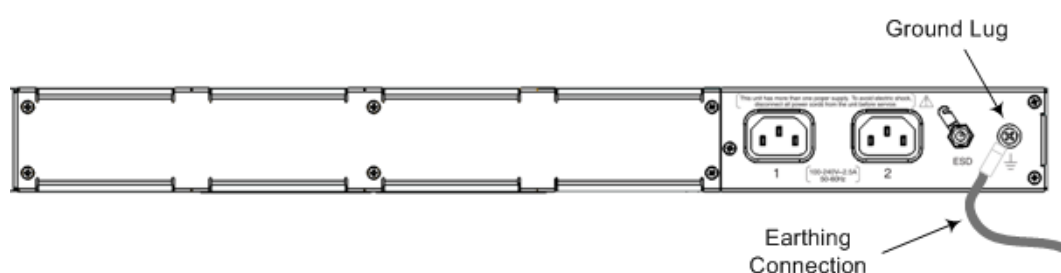
Protective Earthing

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

➤ To ground the device:

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

Figure 2-19: Grounding the Device



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

2.4.3.2 Connecting to Ethernet

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

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

Figure 2-20: Connecting the LAN Ports



➤ To connect the device to the enterprise LAN:

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

- b. Connect the other end to your local network LAN layer 2 switch port. This port will be used to communicate with the IP-Phones and/or ATA Devices.

2.4.3.3 Connecting to the Power Supply

Table 2-14: Power Specifications

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



Warning:

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



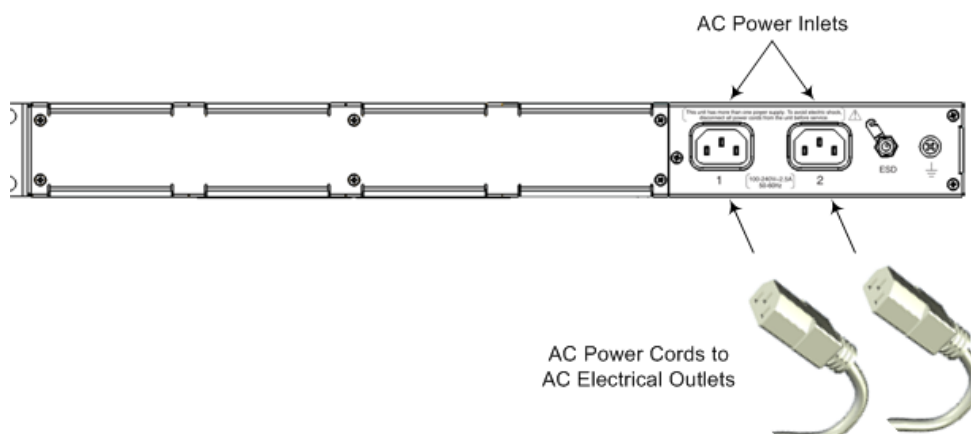
Note:

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

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

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

Figure 2-21: Connecting to Power



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

This page is intentionally left blank.

3 Connecting to the Management Interface

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

3.1 Default OAMP IP Address

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

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

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

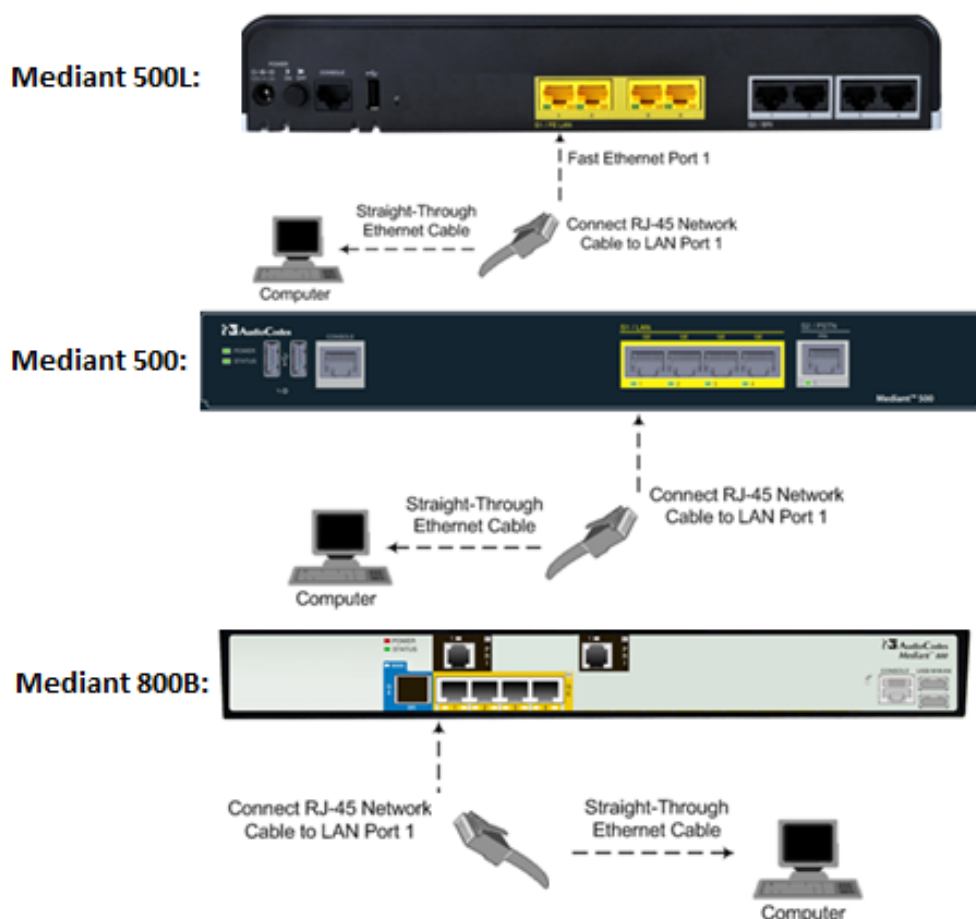
3.2 Connecting to the Embedded Web Server

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

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

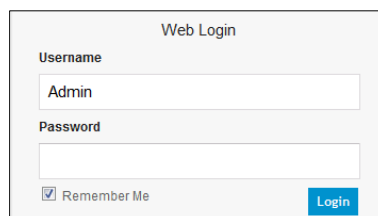
1. Connect Port 1 (leftmost LAN port) located on the front panel directly to the network interface of your computer, using a straight-through Ethernet cable.

Figure 3-1: Connecting to the Embedded Web Server



Mediant 2600:


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

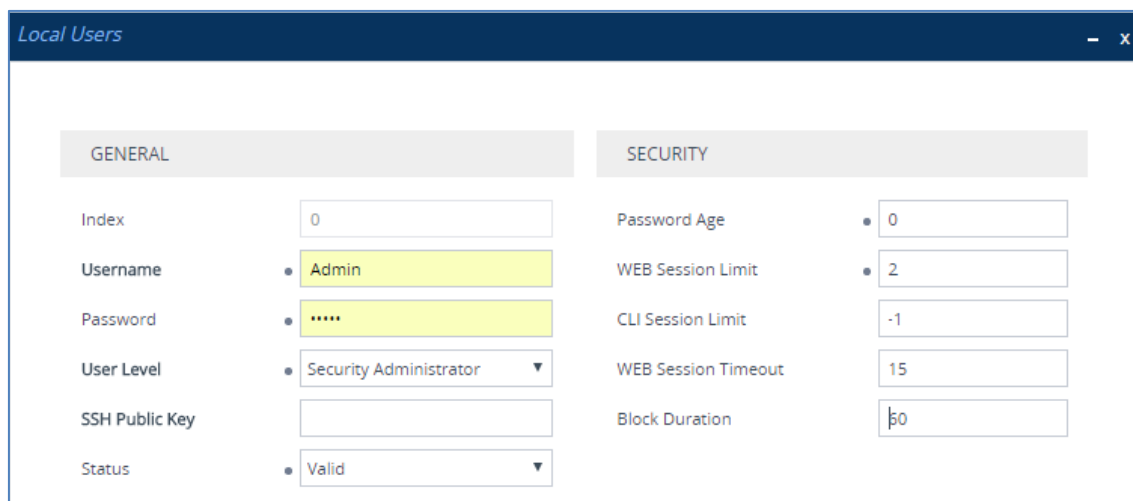
Figure 3-2: Web Login Screen


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

3.2.1 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 3: 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.

4 Configuring the Device

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

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

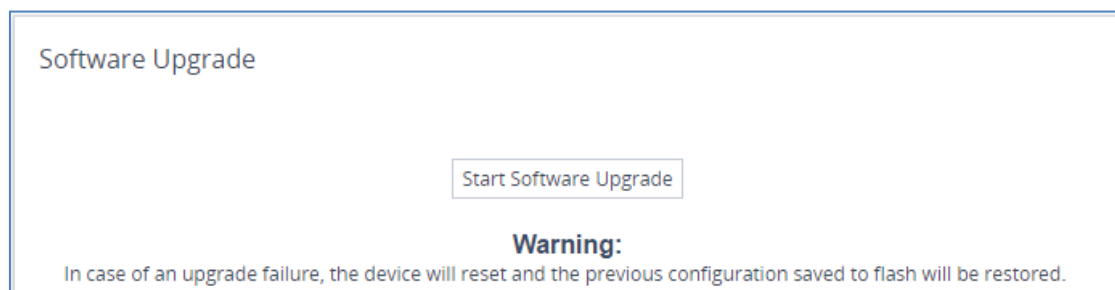
➤ **To download the certified BroadCloud firmware and configuration:**

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

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

1. Open the Software Upgrade Wizard by performing one of the following:
 - **Toolbar:** From the **Actions** drop-down menu, choose **Software Upgrade**.
 - **Navigation tree:** **Setup** menu > **Administration** tab > **Maintenance** folder > **Software Upgrade**.

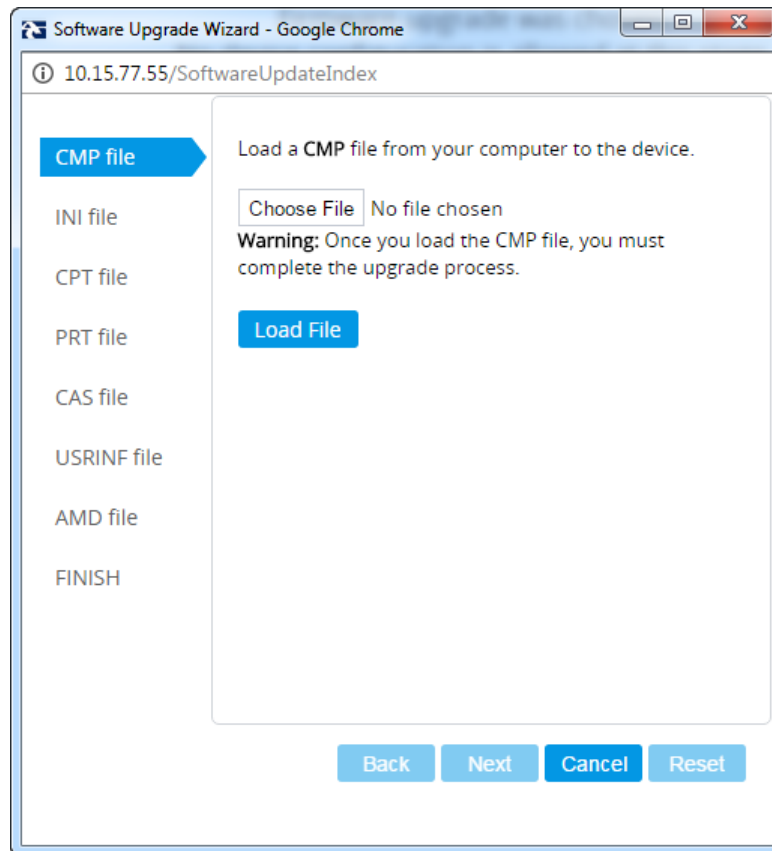
Figure 4-1: Start Software Upgrade Wizard Screen



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

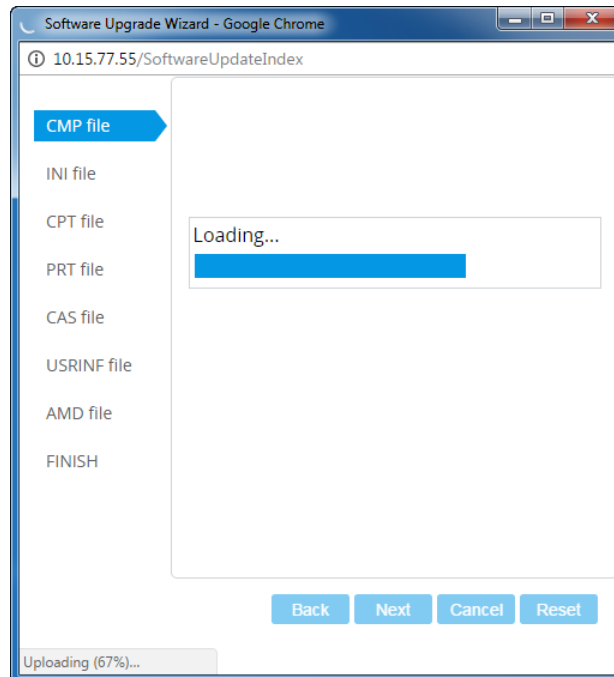
3. Click **Start Software Upgrade**; the Wizard starts, prompting you to load a .cmp file:

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

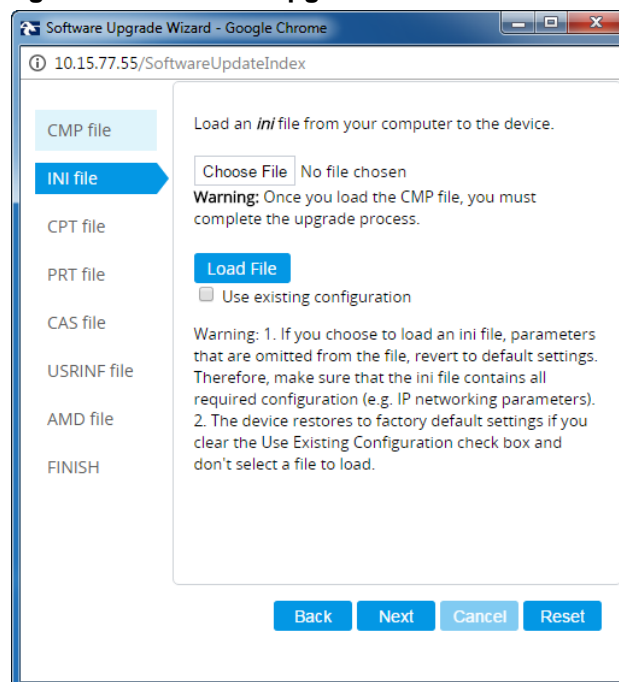


Note: At this stage, you can quit the Software Upgrade Wizard without having to reset the device, by clicking **Cancel**. However, if you *continue* with the Wizard and start loading the .cmp file, the upgrade process must be completed with a device reset.

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

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

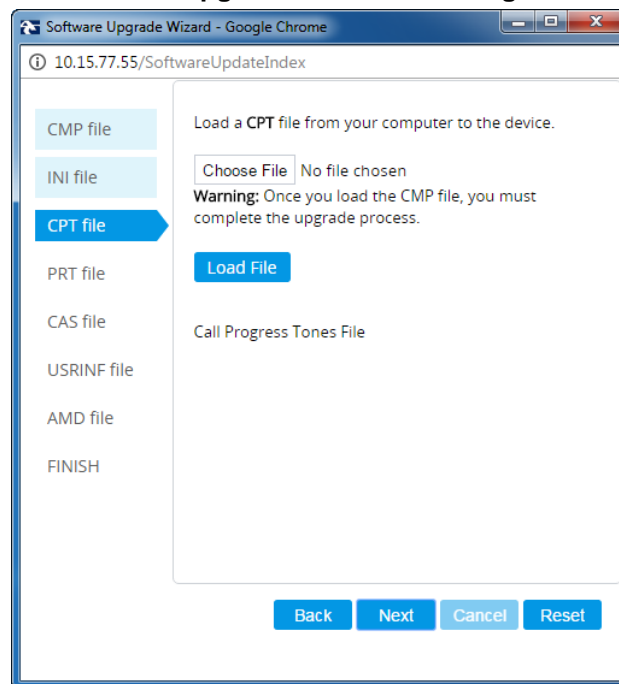
6. Press the **Next** button to navigate through the Wizard.
7. In the Wizard's page for loading an INI file:
 - **Deselect** the 'Use existing configuration' option
 - **Load a new ini file:** In the 'Load File' field, click **Choose File**, and then navigate to where the ini file is located on your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

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

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

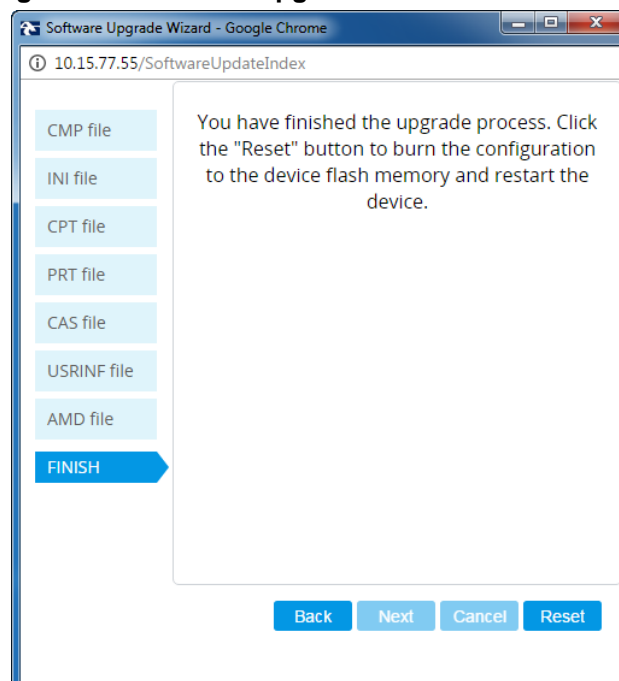
the tones file.

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



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

Figure 4-6: Software Upgrade Wizard – Files Loaded



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

**Note:**

- The device's reset may take a few minutes (even up to 30 minutes) depending on the .cmp file version.
- After the reset, the device's IP address will be the 'default' IP address 192.168.0.2 (see also Section 3.1).

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

Figure 4-7: Software Upgrade Process Completed Successfully

Current CMP Version ID:	7.20A.152.003
-------------------------	---------------

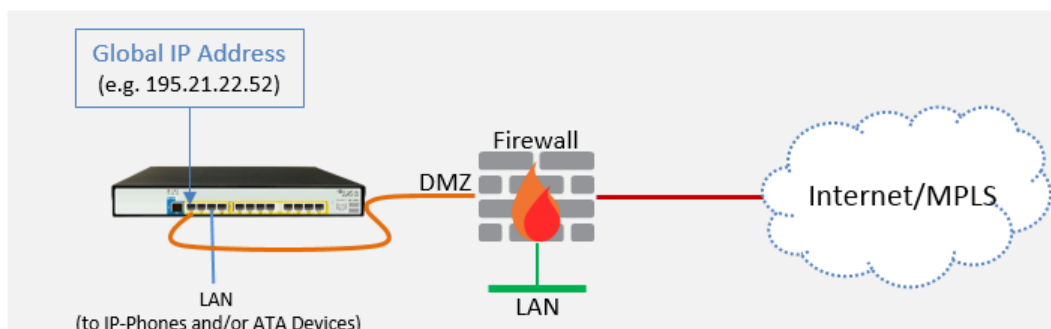
End Process

12. Click **End Process** to close the Wizard; the Web Login dialog appears.
13. 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.
14. Click **OK**; the Web interface becomes active, reflecting the upgraded device.

4.2 Step 2: Configure a Network Interface for the Device

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

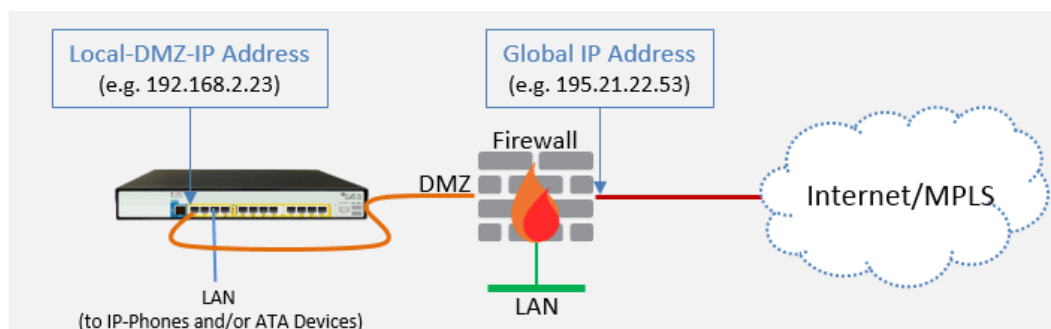
- Method A:** [Preferred method] With a 'Global IP Address' provided to the gateway device, without a NAT. The firewall is configured with the following rules (for example):



- FW allow rule:

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

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



- Firewall allow rule:

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

- NAT rules (port forwarding):

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

4.2.1 Step 2a: Configure Network Interfaces

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

➤ **To configure the DMZ/WAN (BroadCloud Hosted UC) Interface:**

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

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

➤ **To configure the LAN (IP-Phones and/or ATA Devices) Interface:**

1. Modify the existing **LAN** ('Voice') interface (which will be available on eth port #3):
 - a. Select the 'Index 1' option of the **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) This interface will be associated with the IP-Phones
Application Type	Media + Control (<u>leave as is</u>)
Ethernet Device	vlan 2
IP Address	Local LAN IP address assigned for the CRP to use to communicate with the IP-Phones and/or ATA Devices
Prefix Length	Subnet mask in bits, e.g.24 (subnet mask in bits for 255.255.255.0)
Default Gateway	The local LAN default gateway IP address
Primary DNS Server IP Address	Primary DNS IP address (optional)
Secondary DNS Server IP Address	Secondary DNS IP address (optional)

2. Click **Apply**.

An example of configured IP network interfaces is shown below:

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

IP Interfaces (2)

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

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

4.2.2 Step 2b: Configure NAT

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



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




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

➤ To configure the Global address

1. Open the NAT Translation table (**Setup** menu > **IP Network** tab > **Core Entities** folder > **NAT Translation**).
2. Click **New**; the following dialog appears:

Figure 4-9: NAT Translation Table - Dialog Box

NAT Translation

SOURCE		TARGET	
Index	0	Target IP Address	
Source Interface	--  View	Target Start Port	
Source Start Port		Target End Port	
Source End Port			

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

Table 4-1: NAT Translation Table Parameter Descriptions

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

4. Click **Apply**.

4.3 Step 3: Configure the UDP Ports for RTP between CRP and IP-Phones and/or ATA Devices



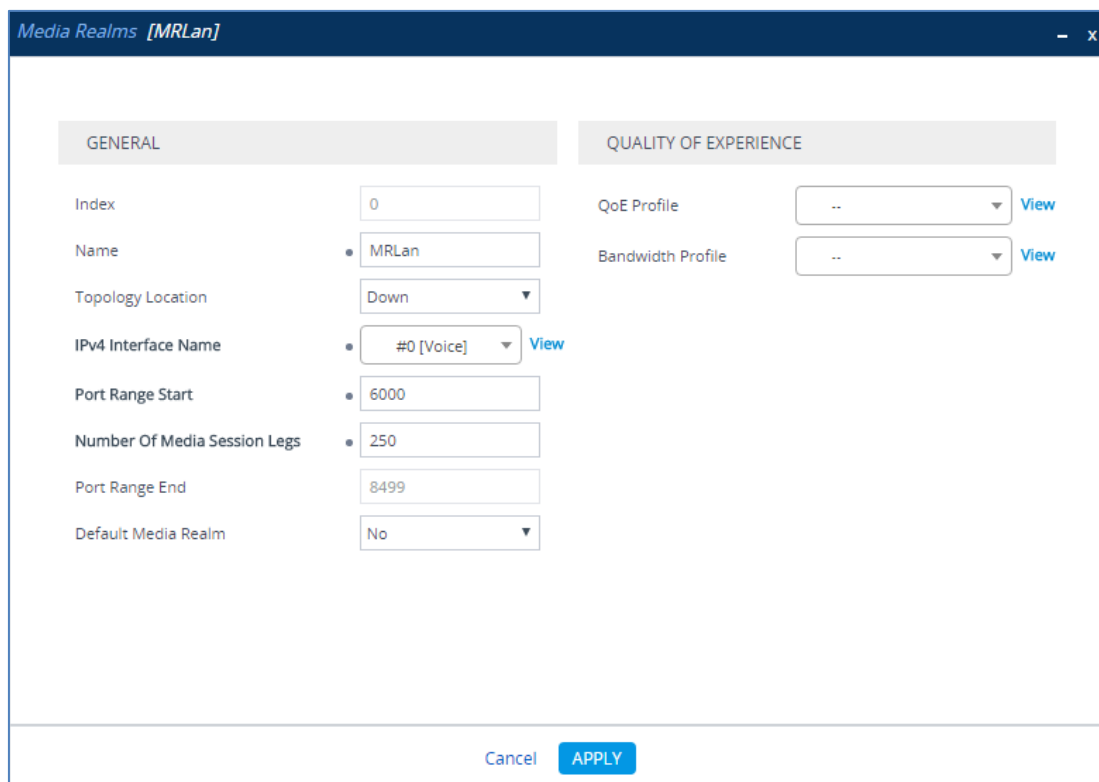
Note: The default UDP port range is 6000 and up to 8499 (maximum UDP depends on the maximum capacity of the specific CRP license provided). Skip this step if you do not need to change the default.

➤ **To configure Media Realms:**

1. Open the Media Realms table (**Setup** menu > **Signaling & Media** tab > **Core Entities** folder > **Media Realms**).
2. Edit the Media Realm for the LAN ('Voice') interface. For example:

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

Figure 4-10: Configuring Media Realm for LAN



Media Realms [MRLan]

GENERAL

Index: 0

Name: MRLan

Topology Location: Down

IPv4 Interface Name: #0 [Voice]

Port Range Start: 6000

Number Of Media Session Legs: 250

Port Range End: 8499

Default Media Realm: No

QUALITY OF EXPERIENCE

QoE Profile: --

Bandwidth Profile: --

Cancel APPLY

The configured Media Realms are shown in the figure below:

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

Media Realms (2)						
<div> + New Edit </div> <div> << >> Page 1 of 1 Show 10 records per page </div>						
INDEX	NAME	IPV4 INTERFACE NAME	PORT RANGE START	NUMBER OF MEDIA SESSION LEGS	PORT RANGE END	DEFAULT MEDIA REALM
0	MR Lan	Voice	6000	250	8499	No
1	MR Wan	WAN SP	6000	250	8499	No

4.4 Step 4: Adopt Classification Policy for CRP Users (if Required)

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



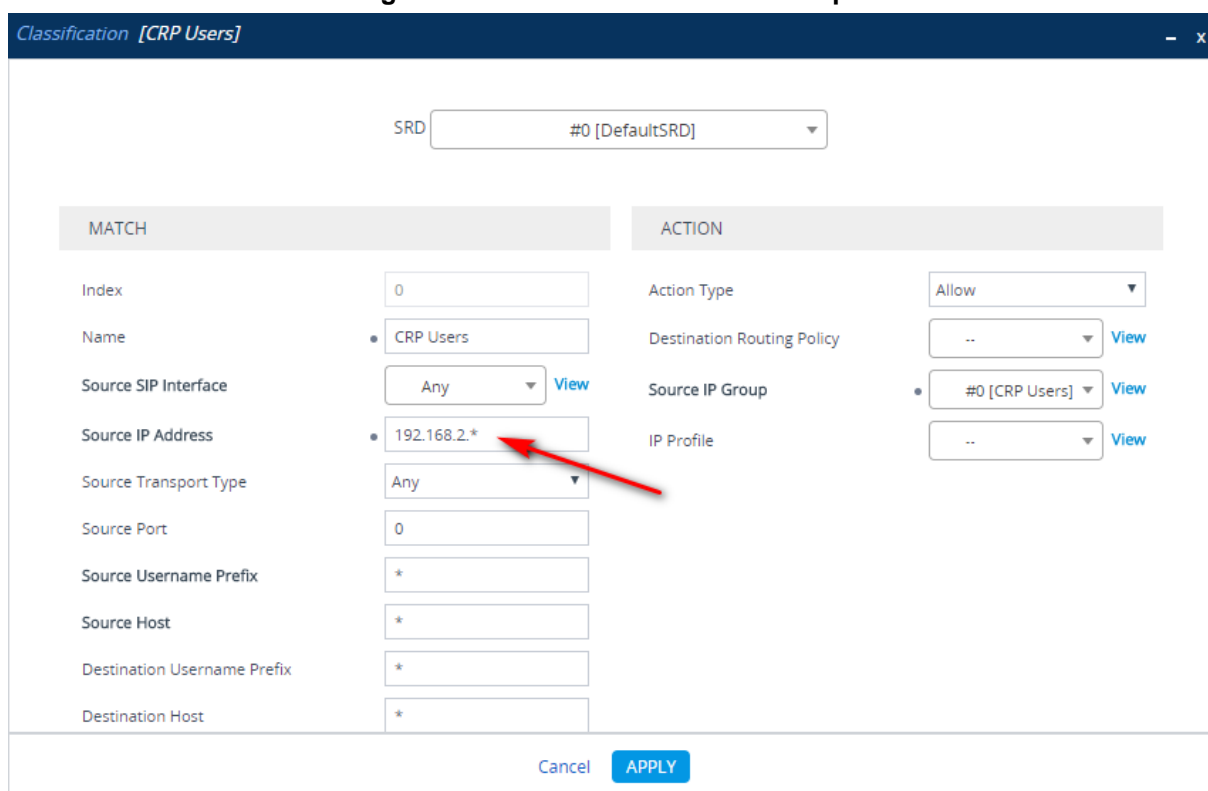
Note: The template INI file is already preconfigured with Classification rules to allow CRP users with source port 8933 and transport type UDP only. Skip this step if you do not need to change these preconfigured settings.

➤ **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 4-12: Classification Rule Example



Classification [CRP Users]

SRD: #0 [DefaultSRD]

MATCH		ACTION	
Index	0	Action Type	Allow
Name	• CRP Users	Destination Routing Policy	.. View
Source SIP Interface	Any View	Source IP Group	• #0 [CRP Users] View
Source IP Address	• 192.168.2.*	IP Profile	.. View
Source Transport Type	Any		
Source Port	0		
Source Username Prefix	*		
Source Host	*		
Destination Username Prefix	*		
Destination Host	*		

Cancel APPLY

3. Click **Apply**.

4.5 Step 5: Check the Connectivity and Registration Status

This section shows how to check the connectivity and Registration Status.

➤ **To check connectivity of the CRP with BroadCloud Hosted UC Server:**

1. Open the Active Proxy Set Status page (**Monitor** menu > **Monitor** tab > **VoIP Status** folder > **Proxy Sets Status**).
2. Check the status in the Proxy Sets Status Table.
A successful connectivity will show as ONLINE (see the figure below).

Figure 4-13: Successful Connectivity with BroadCloud Hosted UC Server

The screenshot shows the AudioCodes Mediant Monitor interface. The left sidebar has a 'MONITOR' section with 'VOIP STATUS' expanded, showing 'Proxy Sets Status' as the selected item. The main area displays the 'Proxy Sets Status' table, which refreshes every 60 seconds. The table has columns: PROXY SET ID, MODE, KEEP ALIVE, ADDRESS, PRIORITY, WEIGHT, SUCCESS COUNT, FAILURE COUNT, and STATUS. Two rows are shown: Proxy Set 0 (Parking, Disabled) and Proxy Set 1 (Parking, Enabled). Proxy Set 1 is associated with the address 'as.iop1.broadworks.net(199.19.193.10) (*)' and has a success count of 2 and failure count of 0. Its status is 'ONLINE', which is circled in red. The first row has a status of 'NOT RESOLVED'.

PROXY SET ID	MODE	KEEP ALIVE	ADDRESS	PRIORITY	WEIGHT	SUCCESS COUNT	FAILURE COUNT	STATUS
0	Parking	Disabled						NOT RESOLVED
1	Parking	Enabled	as.iop1.broadworks.net(199.19.193.10) (*)	-	-	2	0	ONLINE
			as.iop1.broadworks.net(199.19.193.11)	-	-	0	0	ONLINE

➤ **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 4-14: Successful IP-Phones Registration

The screenshot shows the AudioCodes Mediant Monitor interface. The left sidebar has a 'MONITOR' section with 'VOIP STATUS' expanded, showing 'SBC Registered Users' as the selected item. The main area displays the 'SBC Registered Users' table. The table has two columns: ADDRESS OF RECORD and CONTACT. A single row is shown with the address '3015551003@as.iop1.broadworks.net' and the contact information '<sjp:3015551003@10.15.77.195:5060>; Associated Contact: FEU_CID1; IPG#1; ResourceID#99; LegType:OVR; Profile ID:-1; Routing Policy:0'.

ADDRESS OF RECORD	CONTACT
3015551003@as.iop1.broadworks.net	<sjp:3015551003@10.15.77.195:5060>; Associated Contact: FEU_CID1; IPG#1; ResourceID#99; LegType:OVR; Profile ID:-1; Routing Policy:0

**Note:**

- If the status of the BroadCloud Proxy Set does not show ONLINE, check your WAN connectivity:
 - ✓ Check the WAN wiring.
 - ✓ Make sure the DMZ configuration is correct on the firewall.
 - ✓ Check the WAN IP address configuration (**Setup** menu > **IP Network** tab > **Core Entities** folder > **IP Interfaces**).

4.6 Step 6: 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.

4.6.1 Secure Management Access via WAN

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

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

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

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

4.7 Step 7: Save the Configuration, Connect to DMZ



Note: Firewall settings for the DMZ must be in place before resetting the device. After the device is reset, its IP configuration is applied and it is no longer available for management via the default IP address. After reset, the device's management interface is via its WAN interface, via its global-IP-address, so make sure the firewall allows the ports required for management. See Section 4.6.1 for details about the configuration of the required ports on the firewall.

➤ To save the configuration and reset the device:

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 4-15: Maintenance Actions Page

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

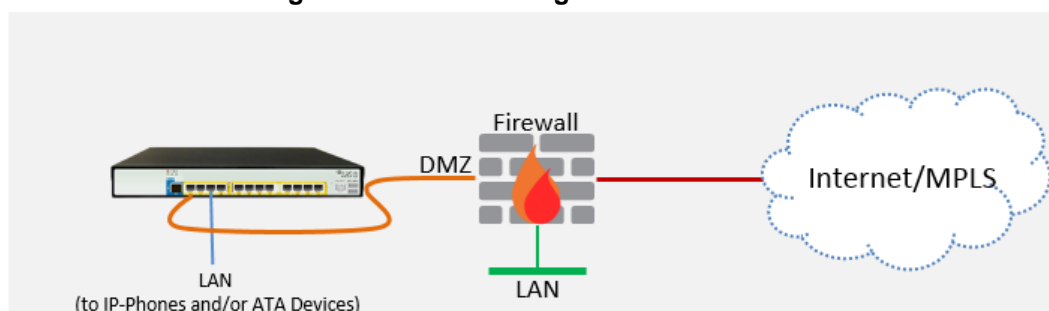
For Reset Device : If you choose not to save the device's configuration to flash memory, all changes made since the last time the configuration was saved will be lost after the device is reset.

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

➤ To connect the device to DMZ:

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

Figure 4-16: Connecting the Device to DMZ



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 Step 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

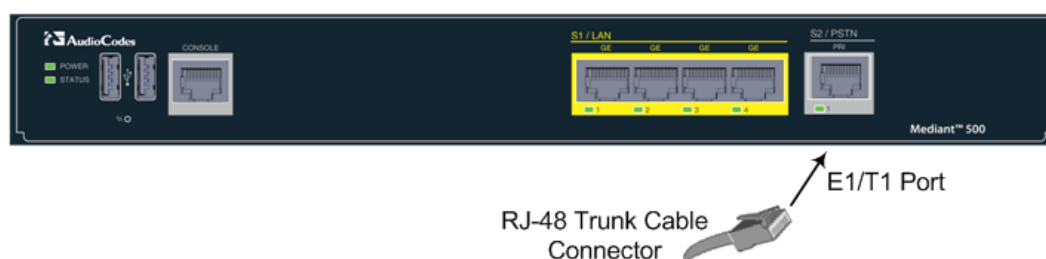
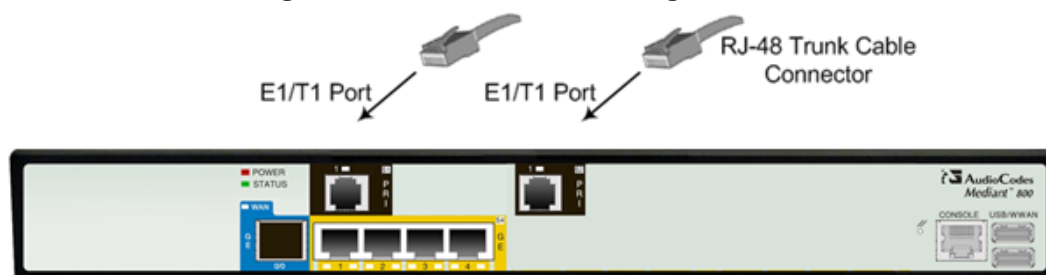


Figure A-3: Mediant 800B Cabling E1/T1 Port



A.2 Step 2: Configure PSTN Trunk Settings

This step shows how to configure PSTN trunk settings.

A.2.1 Step 2a: 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
ISDN Termination Side	User side
BRI Layer2 Mode	Point To Point
Q931 Layer Response Behavior	0x8000000
Outgoing Calls Behavior	0x0
Incoming Calls Behavior	0x11000
Select Receiving of Overlap Dialing	Local Receiving

Figure A-4: Configuring BRI PSTN Interface

The screenshot shows the configuration interface for the BRI PSTN Interface. The left sidebar contains a navigation tree with 'Trunks' selected. The main area is divided into three sections: GENERAL, BRI CONFIGURATION, and ADVANCED SETTINGS. Arrows indicate the following configurations:

- 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 (User 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 (PBX), Set 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 Paramet), Play Ringback Tone to Trunk (Not Configured), Call Rerouting Mode (None), ISDN Duplicate Q931 BuffMode (0), Trunk Name (empty).

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

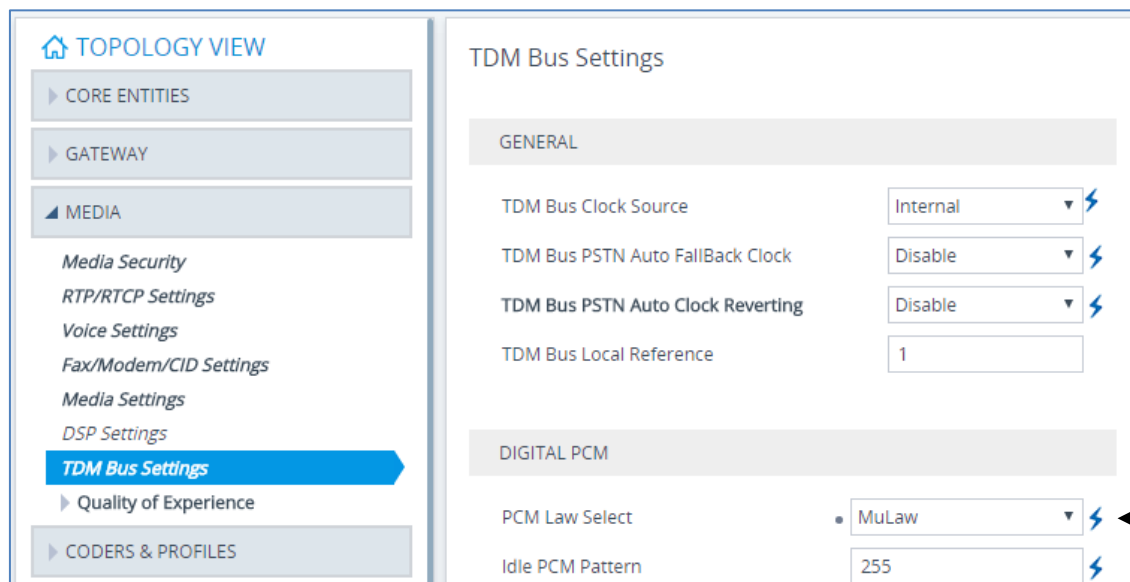
A.2.2 Step 2b: Configure PCM Law Select

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 Step 2c: 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

The screenshot shows the configuration page for a PRI trunk. The left sidebar contains a tree view with 'Trunks' selected. The main area has three tabs: GENERAL, TRUNK CONFIGURATION, and ISDN CONFIGURATION. The GENERAL tab is active, showing fields for Module ID (1), Trunk ID (1), Trunk Configuration State (Not Configured), and Protocol Type (E1 EURO ISDN). The TRUNK CONFIGURATION tab shows fields for Clock Master (Recovered), Auto Clock Trunk Priority (0), Line Code (B8ZS), Line Build Out Loss (0 dB), Trace Level (No Trace), Line Build Out Overwrite (OFF), and Framing Method (E1 FRAMING MFF CRC4 !). The ISDN CONFIGURATION tab shows fields for ISDN Termination Side (User side) and Q931 Layer Response Behavior (0x0). Arrows point to the Protocol Type, Clock Master, Framing Method, and ISDN Termination Side fields.

3. Repeat for PRI trunk #2 if applicable (Mediant 800B)
4. **Reset the device with a save-to-flash for your settings to take effect.**

A.3 Step 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 Step 3a: 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

Group Index	Module	From Trunk	To Trunk	Channels	Phone Number	Trunk Group ID	Tel Profile Name
1	Module 3 BRI	1	4	1-2		1	None
2							None
3							None
4							None

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 Step 3b: 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

Group Index	Module	From Trunk	To Trunk	Channels	Phone Number	Trunk Group ID	Tel Profile Name
1	Module 1 PRI	1	1	1-31		1	None
2							None
3							None

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 Step 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

INDEX	NAME	SOURCE TRUNK GROUP ID	SOURCE PHONE PREFIX	DESTINATION PHONE PREFIX	DESTINATION IP GROUP	SIP INTERFACE	DESTINATION IP ADDRESS	FORKING GROUP	CONNECTIVITY STATUS
0	PSTNFallback	1	*	*	..	PSTNFallback	10.15.77.10	-1	Not Available

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 Step 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 Step 5a: 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

Image Load to Device
ini Parameters
Back to Main

Parameter Name:
CRPGATEWAYFALLBACK

Enter Value:
1

Apply New Value

Output Window
Parameter Name: CRPGATEWAYFALLBACK
Parameter New Value: 1
Parameter Description: Enable fallback route from Proxy to Gateway

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 Step 5b: Update the CRP Gateway Proxy Set

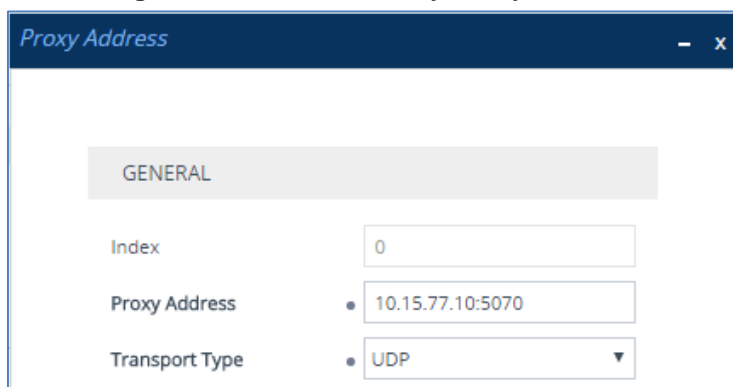
This section shows how to update the CRP Gateway Proxy Set in order to enable PSTN Fallback routing.

- **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 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/contact

Website: www.audiocodes.com

© 2017 AudioCodes Ltd. All rights reserved. AudioCodes, AC, HD VoIP, HD VoIP Sounds Better, IPmedia, Mediant, MediaPack, What's Inside Matters, OSN, SmartTAP, User Management Pack, VMAS, VoIPerfect, VoIPerfectHD, Your Gateway To VoIP, 3GX, VocaNom, AudioCodes One Voice and CloudBond are trademarks or registered trademarks of AudioCodes Limited. All other products or trademarks are property of their respective owners. Product specifications are subject to change without notice.

Document #: LTRT-29836

