Video Collaboration Bar User's and Administrator's Manual

AudioCodes Room Experience (RX) Suite

RXV81 MTRA

Version 3.0

Notice

Information contained in this document is believed to be accurate and reliable at the time of publishing. However, due to ongoing product improvements and revisions, AudioCodes cannot guarantee accuracy of published material after the Date Published nor can it accept responsibility for errors or omissions. Updates to this document can be downloaded from https://www.audiocodes.com/library/technical-documents.

This document is subject to change without notice.

Date Published: March-31-2026

WEEE EU Directive

Pursuant to the WEEE EU Directive, electronic and electrical waste must not be disposed of with unsorted waste. Please contact your local recycling authority for disposal of this product.

Security Vulnerabilities

All security vulnerabilities should be reported to vulnerability@audiocodes.com.

Customer Support

Customer technical support and services are provided by AudioCodes or by an authorized AudioCodes Service Partner. For more information on how to buy technical support for AudioCodes products and for contact information, please visit our website at https://www.audiocodes.com/services-support/maintenance-and-support.

Documentation Feedback

AudioCodes continually strives to produce high quality documentation. If you have any comments (suggestions or errors) regarding this document, please fill out the Documentation Feedback form on our website at https://online.audiocodes.com/documentation-feedback.

Stay in the Loop with AudioCodes

Related Documentation

Document Name
RXV81 RXV200 RX-PAD RX-PANEL Release Notes
RXV81 MTRA Video Collaboration Bar User's and Administrator's Manual
One Voice Operation Center (OVOC) User’s Manual
Device Manager Administrator’s Manual

Document Revision Record

LTRT	Description
18266	Update Version 2.8.208
18268	Update Version 2.8.574 (M1); AlphaSSL certificate; preferred HDMI IN source; return to previous version
09988	Updated to Version 2.8.855 (M2)
09991	Updated to Version 2.8.917 (M3) 802.1x authentication parameters
09995	Updated to Version 3.0; provisioning source auto discovery; admin password brute force protection Revised Getting Started section

Table of Contents

1 Introduction

AudioCodes' RXV81 Bring Your Own Device (BYOD) is a cost-effective, UC-agnostic collaboration bar designed for small and medium rooms, huddle rooms, focus rooms and executive rooms.

As a peripheral device, RXV81 BYOD with its integrated camera, microphones and speaker is connected in the room via USB to a PC or laptop running the UC application (which may be Teams, Zoom, and so on). If only used as a peripheral, RXV81 BYOD does not require any UC license to be installed on it.

From a pure peripheral, RXV81 BYOD can be upgraded via software license (purchased separately) to a full Android MTR. For details about configuring and using an RXV81 MTRA, refer to the RXV81 MTRA Video Collaboration Bar User's and Administrator's Manual.

RXV81 BYOD is fully managed by the AudioCodes One Voice Operations Center (OVOC) Device Manager (a plugin of OVOC), allowing admins to remotely oversee and easily upgrade all deployed devices from anywhere.

RXV81 BYOD can be operated with a Remote Control Unit (RCU) or RX PAD Meeting Room Controller.

- The RCU is bundled in the RXV81P bundle to control meetings.
- The RX PAD is bundled in the RXV81P-B10 bundle to control meetings.

For details, see Bundles on the next page.

A/V control functions include camera on / off, camera settings, mute / unmute and volume up / down.

Deployment is straightforward with its robust mounting element and minimal cable connections.

Microsoft Teams Android devices now utilize Intune Android Open Source Project (AOSP) device management. AOSP device management is a mobile device management (MDM) platform specifically designed for Teams devices. This update delivers more reliable user experience, an enhanced deployment process for administrators, and serves as the foundation for future innovations and advanced management capabilities for Microsoft Teams Android devices, including Teams Rooms, Teams panels, Teams phones, and Teams displays.

AOSP Device Management replaces the legacy Android Device Administrator solution previously used to manage Teams devices.

For detailed information on the AOSP migration process, please refer to the relevant Microsoft documentation.

Highlights

RXV81 feature highlights are:

- **Upgradable to a full Android MTR.** As a pure peripheral, RXV81 can be upgraded via software license (purchased separately) to a full Android MTR.
- **Plug-and-play simplicity for fast setup**

  An easy-to-use mounting element and minimal cable connections enable quick and simple deployment.
- Control – either of the following, depending on the bundle (see):
  - **RX-PAD Meeting Room Controller**

    Makes meeting room functions readily accessible to all participants and provides easy access to camera settings.
  - **Bluetooth Remote Controller**

    Leverages Bluetooth for full control and bi-directional communication. Intuitive. Illuminated ‘Mute’ and ‘Teams’ buttons.
- **Intuitive meeting experience**

  Fast access to meetings with one click to join using Microsoft Teams Room Android (MTRA).
- **High quality video and audio.**

  Outstanding Full HD image clarity and superb surround sound ensures that everyone in the meeting room is seen and heard.
- **Wide-angle 4K camera**

  Covers a 110° viewing angle capturing every seat in the room even in tight spaces with challenging lighting conditions. D: 120º/ H: 110º/ V: 75º
- **Easy to manage from anywhere.**

  Enhance the meeting experience with centralized device management and monitoring from any location.

Benefits

- Easy-to-use mounting element and minimal cable connections for quick and simple deployment
- Effortlessly manage meetings using the dedicated Bluetooth remote control or RX-PAD
- Optional centralized management with AudioCodes’ OVOC / Device Manager (see Management on the next page)

Bundles

RXV81 BYOD is available in the bundles listed in the following table:

Name of Bundle	Details
RXV81P	■ Executive Offices | Huddle Rooms ■ RXV81 main unit ■ Bluetooth Remote Controller Unit (RCU)
RXV81P-B10	■ Huddle Rooms | Small and Medium Meeting Rooms ■ 5-8 participants ■ RXV81 main unit ■ RX-PAD Meeting Room Controller

- Wide-angle lens with 110° field of view (FoV) covers every seat in the meeting room. D: 120º/ H: 110º/ V: 75º
- Adjustable camera position with ePTZ support - 5x zoom - digital 5x zoom in. Manually vertically (up/down) adjustable ±15º.
- 6-element microphone array with 4.5 m pickup range for mid-size rooms and a 10W speaker
- Stylish design and finish
- Built-in dual band Wi-Fi and Bluetooth
- High Dynamic Range (HDR) automatically ON - Wide Dynamic Range (WDR)

Management

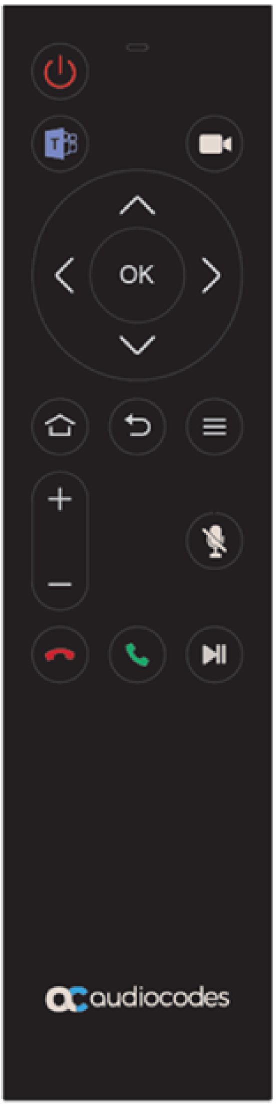
RXV81 BYOD bundles are managed using AudioCodes' On-prem or Live Platform Device Manager, enabling IT admins to monitor and upgrade the devices from anywhere. Using Device Manager, IT admins can easily monitor and manage all bundled devices from a centralized location. Management includes:

- Monitoring
- Firmware management / upgrade
- Alarm management
- Provisioning of device language, date, and time settings

Admins can monitor the status of the device's software modules from the System State screen (see Monitor the System Status on page 33).

Remote Controller Unit (RCU)

The AudioCodes RCU is part of the **RXV81P** bundle (see Bundles on the previous page).



RCU feature highlights:

- The software on the RCU is managed by RXV81.
- The RCU leverages Bluetooth which enables full control and bi-directional communication, similar to a touch control.
- The keys on the RCU (Mute, Teams) are illuminated.

> ⚠ The RCU flashes if the connection to RXV81 fails.

Specifications

- For RX-PAD specifications (included in RXV81P-B10 Bundles on page 2), see the RX-PAD datasheet.

The following table shows RXV81 BYOD specifications:

Feature	Details
Video capabilities	■ Ultra HD 4k image sensor ■ Super-wide angle horizontal field of view: 110° ■ Lens: Fixed focus ■ ePTZ capable, digital 5x zoom in ■ Output resolution: 1080p ■ Frame rate: 30 fps ■ Manually adjustable, vertically (up/down) ±15º ■ High Dynamic Range (HDR) automatically ON - Wide Dynamic Range (WDR).
Audio	■ Full duplex, noise suppression, acoustic Echo Cancellation, voice separation ■ 6x beamforming microphone array ■ Voice pickup range: 4.5m (15ft) ■ 10W speaker
Device Interfaces	■ HDMI Output to TV ■ Power/reset button ■ USB 3.0 Type A (host) marked 1 to allow touch LCD or connectivity to wireless KB via BT USB dongle. Do not connect to power! ■ Ethernet: 10/100 Mbps (RJ-45) network interface ■ USB2.0 Type-C (device) marked 2 to connect to PC/MAC BYOD device (peripheral mode) ■ 3 status LEDs indicating camera on/off, mute on, call state, device health ■ Wi-Fi (dual band support) ■ Bluetooth 5.0 ■ 12V/3A DC power input ■ Remote Controller (Bluetooth managed) or RX-PAD Meeting Room Controller
Design	■ DIMENSIONS (W X D X H) 462 x 93 x 76 mm ■ WEIGHT 1.464 kg
Network	■ TCP/IP (IPv4), DHCP/ static IP; Time and date synchronization via

Feature	Details
Provisioning	SNTP; VLAN support; QoS support: IEEE 802.1p/Q tagging (VLAN) ■ Layer 3 TOS and DSCP RTCP support: (RFC 1889) ■ IP address configuration: TCP/IP (IPv4), DHCP/static IP Time and date synchronization: SNTP ■ QoS support: IEEE 802.1p/Q tagging (VLAN), Layer 3 TOS and DSCP RTCP support: (RFC 1889)
OS	■ Android 12
Security	■ Encryption: TLS (Transport Layer Security), SRTP encryption for media, AES256 ■ Network Access Control: IEEE 802.1x ■ Built-in certificate (i.e., DigiCert, AlphaSSL, etc.)
Management	■ AudioCodes Device Manager, a plugin of AudioCodes One Voice Operations Center (OVOC)
RXV81 Device Feature Set	■ Camera settings with different privileges for user and Admin ■ In idle (Admin) and during a call/meeting (all users), Admins can: ✓ Define / edit a new preset ✓ Move to different presets ✓ Change all settings options ■ Video quality: Resolution of 1080p on the decoder side and 720p on the encoding side ■ RXV81 integration with AudioCodes OVOC-DM ■ RXV81 Alerts to AudioCodes OVOC-Device Manager: ✓ Notification sent to screen/TV and to Device Manager if Remote Control is disconnected or if it’s malfunctioning ✓ Notification sent to screen/TV and to Device Manager if Remote Control battery voltage level falls low, indicating what percentage level remains unused ✓ Remote Control flashes if the connection to RXV81 fails. ■ Camera frequency set per power supply: ✓ 110V – 60Hz ✓ 220V – 50Hz

Feature	Details
	■ Shortcut keys for administrators to manually perform recovery operations

Security Guidelines

For detailed security guidelines regarding AudioCodes Native Teams Android-based devices, refer to the document Security Guidelines for AudioCodes Native Teams Android based Devices.

2 Getting Started

Getting started with RXV81 BYOD consists of:

1. Installingthe RXV81 unit:
   - Reviewing the
   - Positioning
   - Mounting
   - Cabling
   - Powering up
2. Pairing and setting up the RXV81 unit with RX-PAD or with the Remote Controller Unit (see Pairing RXV81 with RX-PAD or Pair RXV81 with the RCU below).
3. Configuring and operating the RXV81 using the paired RX-PAD or RCU, as described in the following sections of this manual.

   For a detailed description of the RX-PAD and its operation, refer to the RX-PAD Room Controller User's and Administrator's Manual.

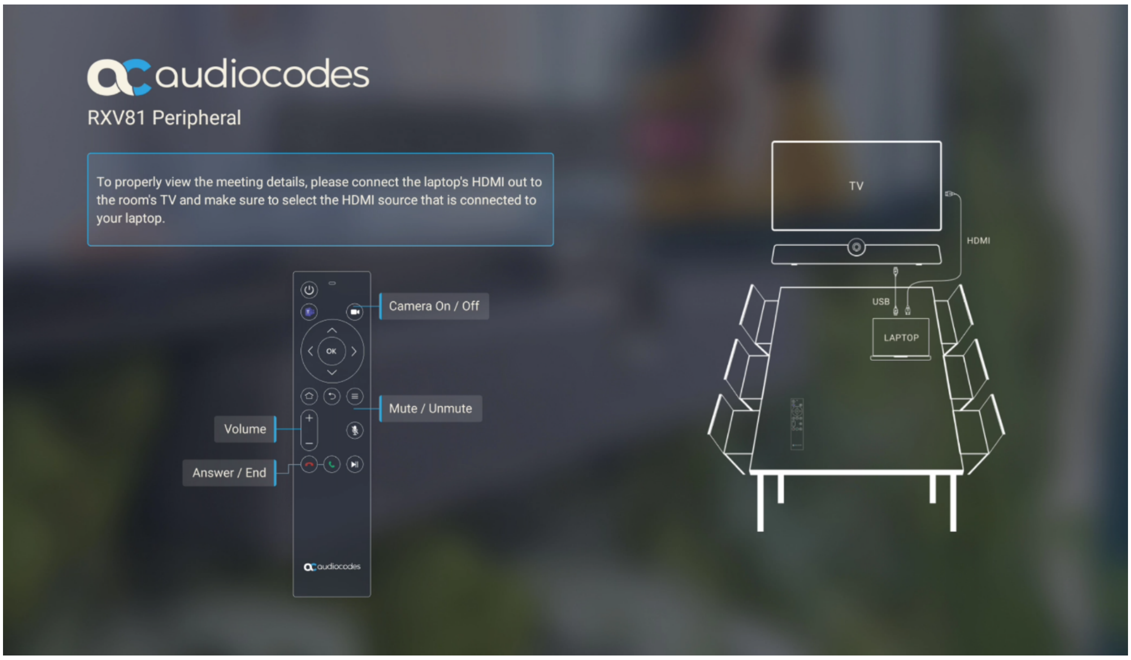
⚠ You can remotely sign-in and provision Android Teams devices via the Microsoft Teams Admin Center. For details, refer to the relevant Microsoft documentation.

Pair RXV81 with the RCU

Customers that acquired a **RXV81P** bundle (see Bundles on page 2) need to pair the RXV81 with the RCU.

➢ To pair the RXV81 with the RCU:

1. After cabling, remove the RCU from its packaging and insert the batteries supplied into it.
2. Follow instructions on the display.
3. On the RCU, simultaneously press and hold ⌂ + ≡ until the RCU and the RXV81 are connected.



audiocodes

RXV81 Peripheral

To properly view the meeting details, please connect the laptop's HDMI out to the room's TV and make sure to select the HDMI source that is connected to your laptop.

3 Camera Settings

⚠ Configuring Camera Settings instructions are *not* relevant for RXV81 *BYOD* systems, because their camera settings are configured from the connected PC.

4 User Settings

RXV81s are delivered configured with their default settings. Users can customize some of them from the 'Settings' page to suit their personal preferences, without needing Admin login:

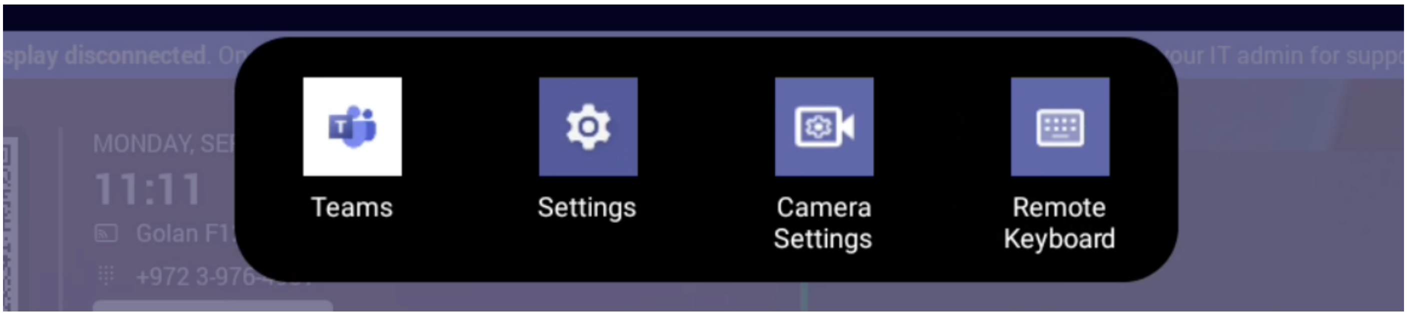
- Adjust the Volume on the next page
- Configure Accessibility Settings on page 13
- View Information on page 13
- Reboot the Device on page 13

To access the 'Settings' page, see Access User Settings below.

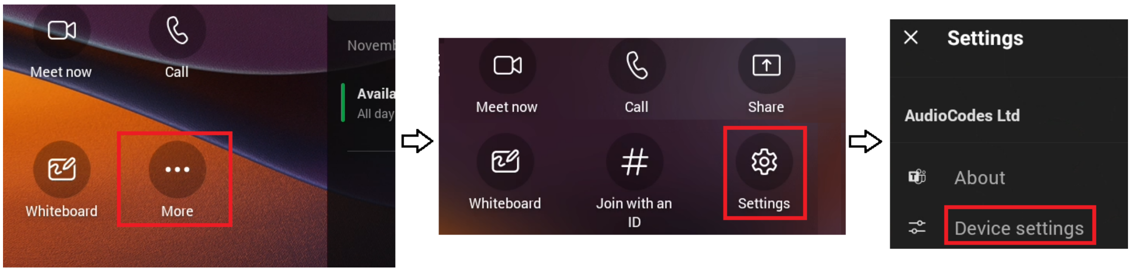
Access User Settings

There are several ways to access the 'Settings' page from the homepage:

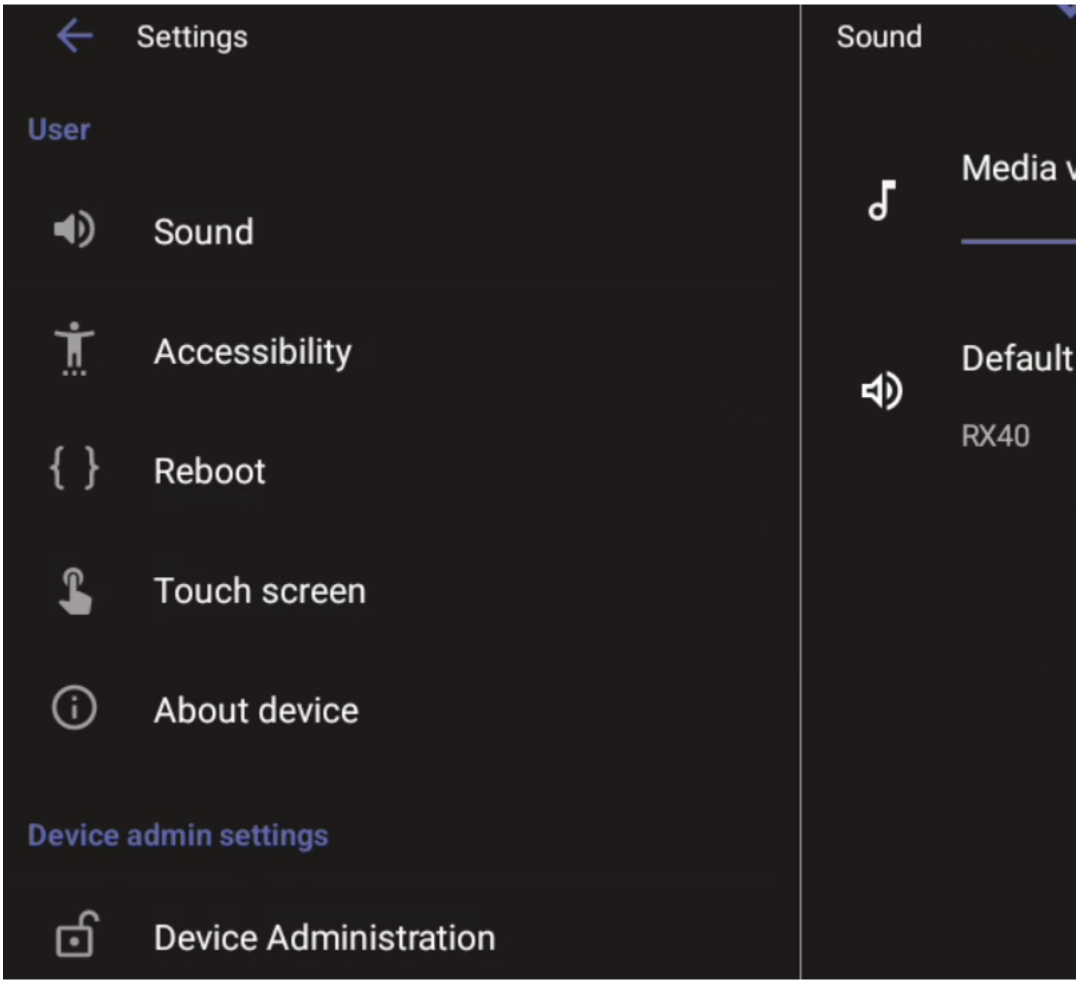
- Swipe down to display the main menu tray, then tap **Settings**.



- Tap the **More** option, then tap the **Settings** option, then tap **Device Settings**.



Any user can configure User settings:

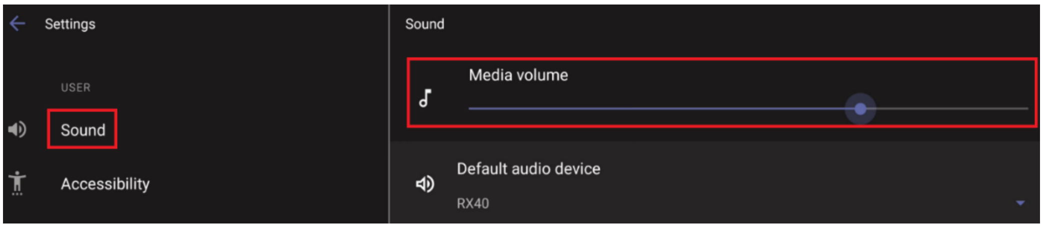


⚠ Viewing and configuring Device Admin settings requires Admin login. For details, see Admin Settings on page 15.

Adjust the Volume

You can customize the media volume for a friendlier user experience. To do this:

1. Navigate to 'Settings' (see Access User Settings on the previous page).
2. Under 'Users", tap **Sound** and set the requested volume.



⚠ The above screen lets you also specify the default audio device, but AudioCodes recommend that only admins do this.

Configure Accessibility Settings

This option allows users to customize the screen to be reader-friendlier.

➢ To configure the Accessibility setting:

1. Navigate to 'Settings' (see Access User Settings on page 11).
2. Under 'User', tap Accessibility.
3. Adjust the settings to suit personal requirements.

Feature	Description
TalkBack	If turned on, provides spoken feedback, which is helpful for vision-impaired users.
Font Size	Increases or decreases the font size on the screen.
High Contrast Text	High contrast display modes to improve readability for users with visual impairments
Color Correction	Adjusts colors for users with color blindness.

View Information

The 'About' screen gives you quick access to information about the deployment.

➢ To access the About page:

1. Navigate to 'Settings' (see Access User Settings on page 11).
2. Under 'User', tap **About device**.

⚠ Admins can monitor the status of the device's software modules from the System State page (see Monitoring the System Status).

Reboot the Device

Rebooting allows you to exit from and reconnect without needing to sign in again.

⚠ ⚠ If your system includes an RCU, you can reboot it by long-pressing the RCU power on/off button for about five seconds, instead of the following procedure.

➢ To reboot:

1. Navigate to ‘Settings’ (see Access User Settings on page 11).
2. Under ‘User’, tap **Reboot**.
3. Tap .
4. Confirm the reboot.

⚠ For an explanation on how to reboot, shut down, or turn on the device using its Power button, seePerform Recovery Operations using the Power Button on page 38.

5 Admin Settings

Admin Settings are IT level settings that require admin login prior to access (see Accessing Admin Settings). These settings are set up with initial default values. Admins can view or modify them to suit their enterprise requirements.

- Select the Default Audio Device on page 18
- Configure the Display on page 18
- Set Date and Time on page 19
- Configure Wi-Fi on page 20
- Configure Power Saving on page 24
- Configure UI Language and Input on page 24
- Modify IP Network Settings on page 24
- Enroll Certificates using SCEP on page 29
- Provision Certificates in .pfx Format on page 30

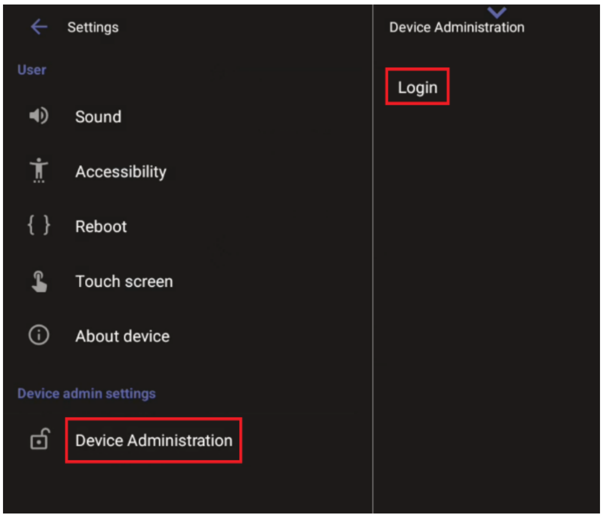
Access Device Admin Settings

To view and access Device Admin settings, you need to be logged into Device Administration (see Log in to Device Administration below).

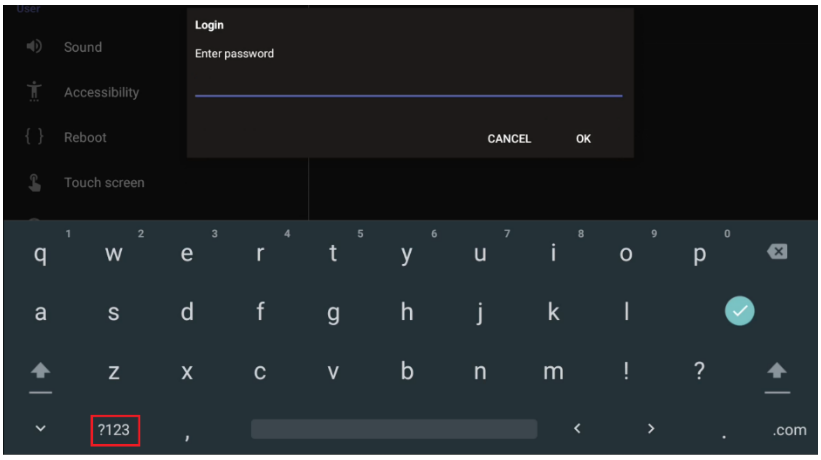
Log in to Device Administration

➢ **To log into Device Administration:**

1. Navigate to the 'Settings' page (see Access User Settings on page 11).
2. Under ‘Device Admin Settings’, tap **Device Administration**, then tap **Login**.



3. Enter the password using the virtual keyboard, then tap **OK**.



Login

Enter password

> The virtual keyboard pops up for all 'Settings' fields to allow inputting characters and / or numbers. Two virtual keyboard types can be displayed: Numeric or QWERTY. To switch between these types, use the **?123** / **ABC** toggle key.

Upon successful login, the available device admin options appear under 'Device Administration' and can be set as required. If you log out or the admin login timeout has passed, the admin options disappear.

> Upon initial login, you are required to change the default password (which is **1234**).

Brute Force Protection for Admin Password

After 5 consecutive wrong login attempts, retry is blocked during a period of 1 minute. This period increases with the number of failed attempts to 5, 10, and 15 minutes.

Failed logins can be at the UI and SSH levels and are added up together for both. For example, 2 wrong passwords at the UI level and 1 wrong password for SSH access are counted as 3 attempts.

Change the Admin Password

➢ Default Password Change at Initial Login

Upon initial login, you are prompted to change the password using the virtual keyboard. The new password must follow the following conventions:

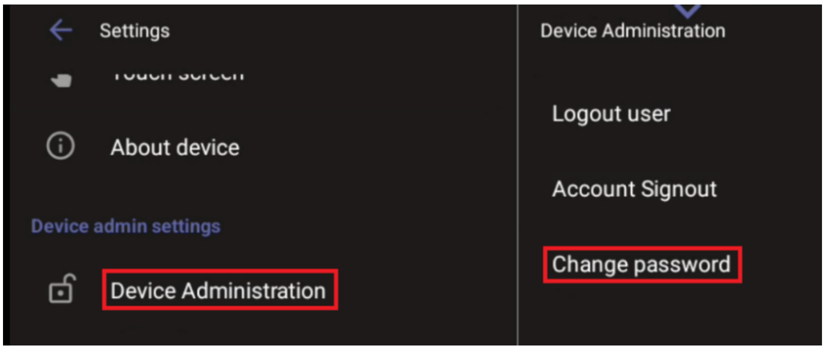
- The password length must be greater than or equal to 8.
- The password must contain one or more uppercase characters.
- The password must contain one or more lowercase characters.
- The password must contain one or more numeric values.
- The password must contain one or more special characters.

- The default password must be changed before access to the device via SSH is allowed.
- The default password can be changed per device from the GUI, or via bulk configuration of multiple devices using Microsoft’s TAC or AudioCodes’ Device Manager.

➢ Subsequent Password Changes

You can change the Admin password at any time. To do this:

1. Log in as Admin with the current password.
2. Tap **Device Administration**, then tap **Change Password**, and specify the new password.



Show or Hide Password Characters While Typing

By default, when the login password is typed in, the characters are briefly displayed. To not display the characters:

1. If not already logged in, log in to Device Administration to get admin access (see Log in to Device Administration on page 15).
2. Under ‘Device Admin Settings’, scroll down and tap **Security**.
3. Tap the **Show passwords** toggle option to turn it off (or back on).

Configure the Admin Login Timeout

The Admin login timeout can be configured using the following cfg configuration file parameter:

```
settings/admin_logout_timeout,values=3
```

- Default: 3 (minutes)
- Valid values: 1-10 (minutes)

- Timing begins when exiting the 'Device Settings' menu.
- When the timeout expires, the device logs out automatically.
- The functionality works for both registered and unregistered devices.

➢ Manual Logout

When logged in to Device Administration, you can manually log out to instantly return the MTRA to non-admin mode:

1. On the RX-PAD, under ‘Device admin settings’, tap **Device Administration**.
2. Tap **Logout User** and then confirm.

Sign out

You can also sign out of the (Teams) and optionally sign back in with another account.

➢ To sign out:

1. Under ‘Device admin settings’, tap **Device Administration**.
2. Tap **Account Signout** and then confirm.

Optionally, remote sign-out can be performed from Microsoft Teams admin center (TAC). Network administrators can provision the from the TAC, remotely sign in, and sign out.

➢ To sign out of the MTRA using Microsoft TAC:

■ Navigate to the 'Devices' > 'Teams Rooms' screen. From the **...** menu located in the uppermost right corner of the screen, select **Actions** and then **Sign out**.

Select the Default Audio Device

You can select the default audio device if there's more than one audio device option available.

➢ To select the default audio device:

1. Navigate to the ‘Settings’ screen (see Access User Settings on page 11).
2. Under ‘User’, tap **Sound** and select the requested default device.

Configure the Display

Modify these settings to suit your preferences related to the look and feel of the user interface.

➢ To configure Display settings:

1. If not already logged in, log in to Device Administration to get admin access (see Log in to Device Administration on page 15).
2. Under ‘Device admin settings’, scroll down and tap **Display**.
3. To decrease or increase screen brightness, tap the **Brightness level** scale.
4. To set the screen timeout, tap **Screen timeout**. Tap the option of your choice and then tap ← to go back to the previous screen.
5. To set or deactivate a screen saver, tap **Screen saver**.
    - To activate or deactivate the screen saver, tap the **Off** toggle.
    - To specify the screen saver display, tap **Current screen saver**, then select the requested screen saver and tap ← to go back.

Set Date and Time

➢ To configure Date & Time settings:

1. If not already logged in, log in to Device Administration to get admin access (see Log in to Device Administration on page 15).
2. Under ‘Device admin settings’, scroll down and tap **Date & Time**.
3. Adjust according to your preferences.

➢ Configuring time zones on Teams devices

> ⚠
>
> - AudioCodes recommends using Geolocation (the default setting) as the time zone configuration method.
>
>   With Geolocation, if no other changes to the time zone settings are made, the device retrieves the time from its geographical location.
> - Manual time zone setting is **NOT** recommended. Choosing a time zone manually may cause retrieval of the incorrect time zone, and cause functionality issues.

You can configure the time zone using one of the following methods, which are listed in order of preference for best performance:

- **Geolocation (Default):**
    - The default geolocation method uses a device’s public IP address to obtain its location. If the devices are behind NAT, they use a STUN server to discover their public IP addresses.
    - A common STUN server example is Google's publicly accessible server: stun.l.google.com:19302 (default URL).
- **DHCP Option 100/101 (posix/tzdbx):**

- Configuration is obtained from DHCP server (once defined as available).

■ **Admin Provisioning:**

Use one of the following:

- Device Manager, created in configuration parameters setup.
- AudioCodes Device Manager supports provisioning of the device’s language, and date and time setting.

The supported parameters for Device Manager configuration can be found in product specific Admin and User guides. For Teams Admin Center, see the relevant Microsoft documentation on creating a configuration profile.

Configure Wi-Fi

The device can connect to an Access Point via Wi-Fi.

Network administrators can configure Wi-Fi parameters for the device. The parameters are concealed from the user's view. Users can enable or disable Wi-Fi in the device’s user interface.

> ⚠ Wi-Fi *cannot* be enabled or disabled using SSH command.

The Wi-Fi connection is transparent to users; which frequency is used, 2.4 GHz or 5 GHz, is made for users by the device; users cannot disable one or the other.

Connect to an Available Wi-Fi Network

> ⚠ Make sure to first disconnect your Ethernet cable. If it's connected, the device will not be able to connect to a Wi-Fi network.

➢ **To connect to an available Wi-Fi network:**

1. If not already logged in, log in to Device Administration to get admin access (see Log in to Device Administration on page 15).
2. Under ‘Device admin settings’, scroll down and tap **Wi-Fi**.
3. Activate **Use Wi-Fi** and then view a list of available connections.
4. Select the Wi-Fi network you want and then use the virtual keyboard displayed to enter the password.

Connect Manually to a Wi-Fi Network

➢ **To manually connect to a Wi-Fi network:**

1. **Make sure to first disconnect your Ethernet cable. If it's connected, the device will not be able to connect to a Wi-Fi network.**

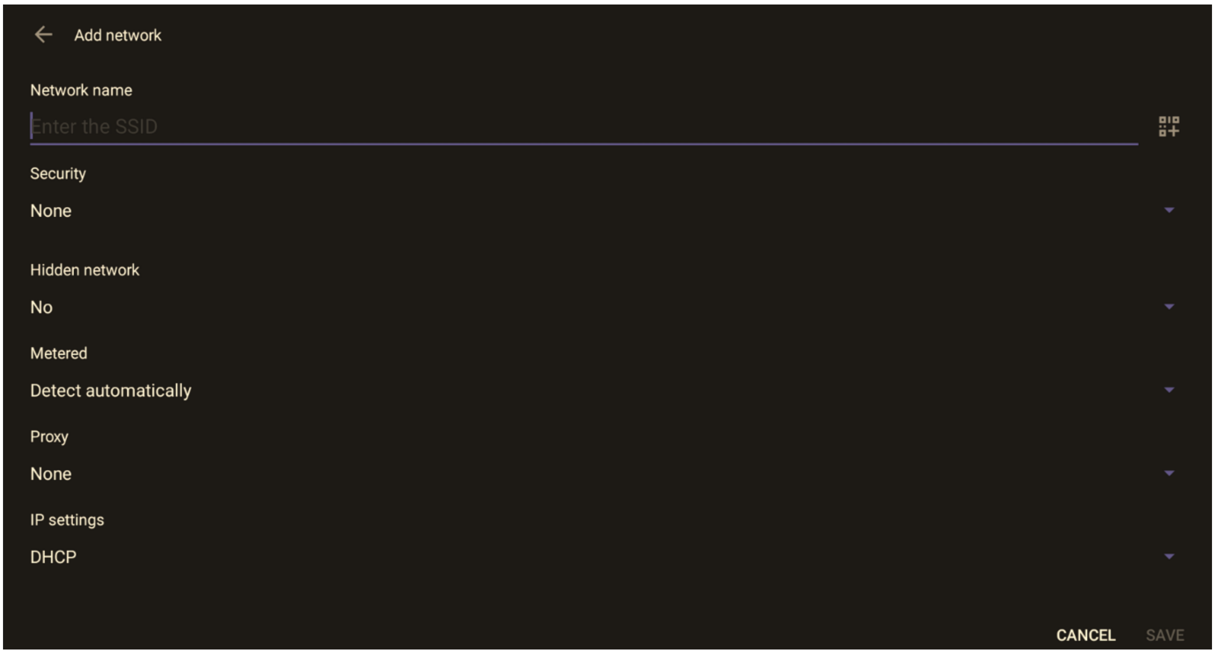
2. If not already logged in, log in to Device Administration to get admin access (see Log in to Device Administration on page 15).

3. Under 'Device admin settings', scroll down and tap **Wi-Fi**.

4. Tap **Add network** and then enter the SSID of the network to add manually.

5. From the 'Security' drop-down, select a security key strength (encryption method). For certificate based authentication, see also Configure Wi-Fi Security with Certificate-based Authentication on page 23.

6. Tap **Advanced options** and optionally meter the selected network:
   - Leave the setting at its default value of **Detect automatically** if you don't want to meter the network.
   - Select a **Metered** option to meter it.



Add network

Network name

Enter the SSID

Security

None

Hidden network

No

Metered

Detect automatically

Proxy

None

IP settings

DHCP

- 'Proxy' and 'DHCP' will automatically be configured by the network.
- Enabling the setting **Turn on Wi-Fi automatically** allows the device to automatically connect in the future to the highest signal-quality network remembered by the device.

As an alternative to manually configuring Wi-Fi settings via the device's user interface, you can configure the Wi-Fi settings described in the following table, using the Configuration File.

Table 5-1: Configuration File Wi-Fi Parameters

Parameter	Description
network/wireless/adavanced_ options/dns1	Defines the IP of the wireless DNS1.

Parameter	Description
network/wireless/adavanced_ options/dns2	Defines the IP of the wireless DNS2.
network/wireless/adavanced_ options/gateway	Defines the IP address of the wireless gateway
network/wireless/adavanced_ options/hidden_network	Defines the name of the wireless hidden network.
network/wireless/adavanced_ options/ip_addr	Defines the IP address of the static Wi-Fi network if you’re operating with a static Wi-Fi network.
network/wireless/adavanced_ options/ip_settings	Used to define DHCP.
network/wireless/adavanced_ options/network_prefix_length	Defines the network prefix length to be used.
network/wireless/adavanced_ options/proxy	Defines the proxy wireless server source.
network/wireless/adavanced_ options/proxy/auto_config/pac_url	Defines the URL of the PAC file.
network/wireless/adavanced_ options/proxy/manual/exclusion_list	Defines the list of IP addresses that will be blocked.
network/wireless/adavanced_ options/proxy/manual/proxy_ hostname	Defines the name of the proxy host.
network/wireless/adavanced_ options/proxy/manual/proxy_port	Defines the proxy port.
network/wireless/anon_identity	Defines the anonymous wireless users who won’t be seen.
network/wireless/ca_cert	Defines which CA certificate to use.
network/wireless/client_cert	Defines which client certificate to use.
network/wireless/domain	Defines the domain name.
network/wireless/eap_method	Defines the EAP method.

Parameter	Description
network/wireless/identity	Defines the identity of the user.
network/wireless/password	Defines the password of the network.
network/wireless/phase2_method NONE,MSCHAPV2,GTC,PAP,MSCHAP	Defines the encryption method. Phase 2 applies only to the 802.1x EAP method.
network/wireless/security	Defines the security method (encryption protocol).

Configure Wi-Fi Security with Certificate-based Authentication

To configure a Wi-Fi network using certificate-based authentication (**EAP-TLS**), administrators must first load the required certificates into the device. This includes the **client certificate** and its associated **private key**. Certificates can be loaded either manually or via provisioning, using the following parameters:

```
security/device_certificate_url=
security/device_private_key_url=
security/CA certificate/0/uri=
```

Once the certificates are loaded, the administrator can configure a secure Wi-Fi connection via the user interface under **Wi-Fi menu > Add Network** (see Connect Manually to a Wi-Fi Network on page 20).

To use **EAP-TLS** for authentication, configure the following parameters:

```
network/wireless/eap_method=TLS
network/wireless/ca_cert=
network/wireless/client_cert=
```

➢ Example Configuration

The following is an example of the Wi-Fi configuration using EAP-TLS:

```
network/wireless/ssid=RAX10-2.4G-5G
network/wireless/security=802.1x_EAP
network/wireless/eap_method=TLS
network/wireless/phase2_method=NONE
network/wireless/ca_cert=SYSTEM
network/wireless/domain=Cisco
network/wireless/client_cert=USRPKEY_device_crt
network/wireless/identity=ipp
```

Configure Power Saving

You can configure the device to turn off its LED during off-work hours, thereby consuming minimum power.

➢ **To configure Power Saving:**

1. If not already logged in, log in to Device Administration to get admin access (see Log in to Device Administration on page 15).
2. Under 'Device admin settings', scroll down and tap **Power Saving**.
3. Enable power saving and then specify work start and end times.

   During work time, the device LED will be on (no power saving).
   Before the **Start Time** and *after* the **End Time**, its LED will be turned off.

Configure UI Language and Input

This setting allows admins to customize inputting to suit personal requirements.

➢ **To set language and input:**

1. If not already logged in, log in to Device Administration to get admin access (see Log in to Device Administration on page 15).
2. Under 'Device admin settings', scroll down and tap **Languages & input**.
3. Adjust as required:
   - Tap **Languages** to change the UI language.
   - Tap **On-screen keyboard** to adjust the default Android Keyboard or add an on-screen keyboard. To adjust the keyboard, click it and configure settings under 'Preferences' and 'Advanced' as required.
   - Tap **Physical keyboard** to connect a physical keyboard. You can specify whether the physical keyboard should connect in addition to the physical keyboard or replace it.
   - Tap **Text-to-speech output** to adjust its speech rate and pitch.

Modify IP Network Settings

This setting enables the Admin user to determine IP network information and to modify IP network settings.

➢ **To modify network settings:**

1. If not already logged in, log in to Device Administration to get admin access (see Log in to Device Administration on page 15).
2. Under 'Device admin settings', scroll down and tap **Modify network**.

3. Perform the required action or actions:
   - View **IP address** and **Network state** (read-only).
   - Click **IP settings** to set to **DHCP** or **Static**.
   - Set up a proxy (see Set up a Proxy Server below).
   - Configure 802.1x settings (see Configure 802.1x Settings below).
   - Configure VLAN settings (see Configure VLAN Settings on page 28).

Set up a Proxy Server

Administrators can manually configure the with an HTTP proxy server:

1. Navigate to ‘Modify network’ (see Modify IP Network Settings on the previous page) and tap **Proxy**.
2. Fill in the **Proxy hostname**, **Proxy port**, and optionally the bypass IP address.
3. Select **DONE**.

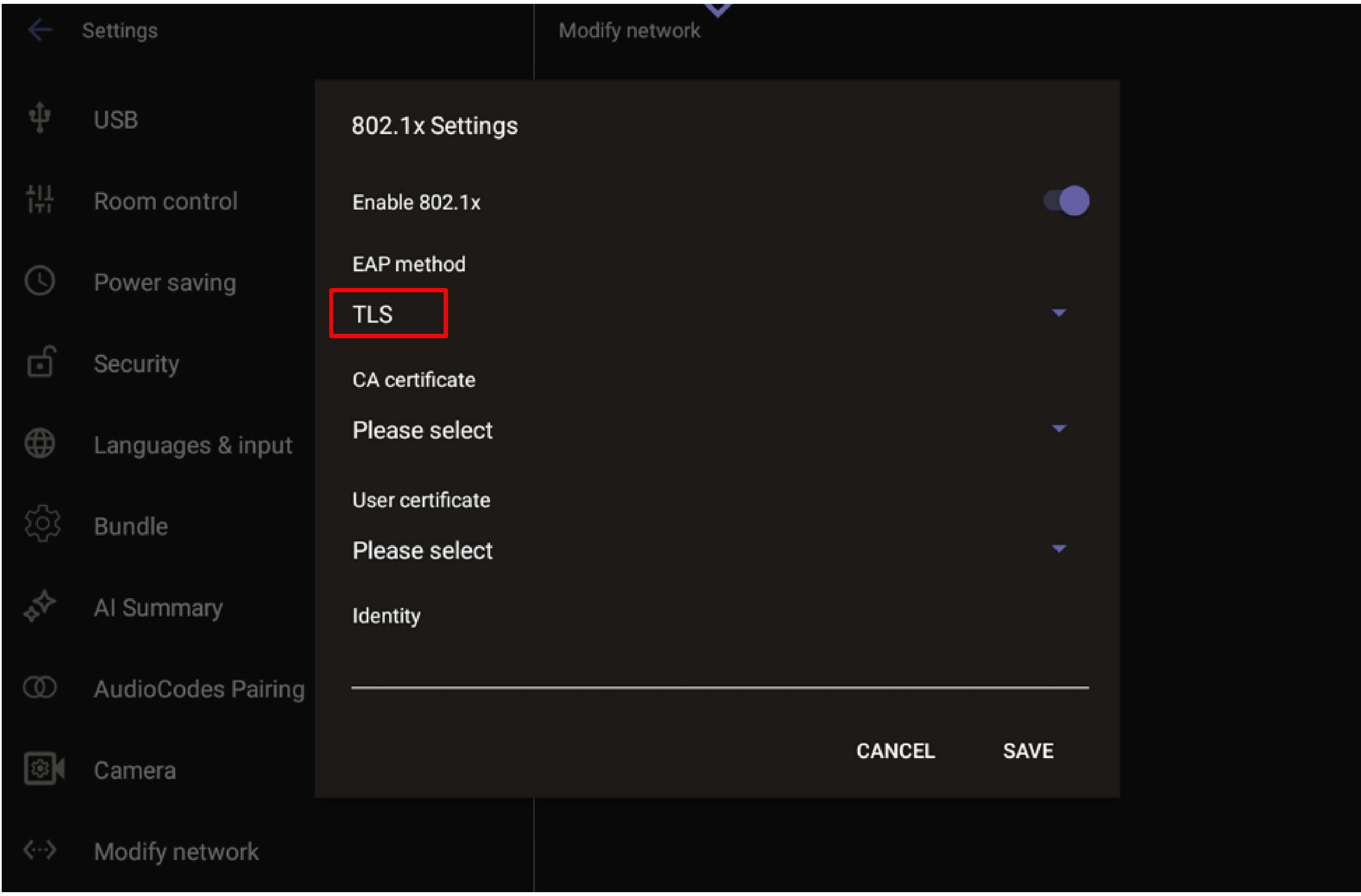
Configure 802.1x Settings

802.1x Authentication is the IEEE Standard for Port-based Network Access Control (PNAC) (refer to https://1.ieee802.org/security/802-1x/ for more information). It is used to enable port-based authentication.

> ⚠ Instead of performing the following steps, 802.1x Authentication can be enabled and predefined via provisioning, by setting the following parameters:
>
> ```
> network/lan/_802_1x/status=true or false
> network/lan/_802_1x/eap_tls/ca_cert=<CA FILE NAME>
> network/lan/_802_1x/eap_tls/client_cert=<Client certificate file name>
> network/lan/_802_1x/eap_tls/identity=<identity name>
> network/lan/_802_1x/eap_type=eap_tls
> ```

➢ To configure 802.1x settings:

1. Navigate to ‘Modify network’ (see Modify IP Network Settings on the previous page) and select **802.1x Settings**.
2. Tap **Enable 802.1x** and then tap **Save**.
3. Once 802.1x is enabled, choose the security method and strength. A commonly used option is EAP-TLS.



802.1x Settings

Enable 802.1x

EAP method

TLS

CA certificate

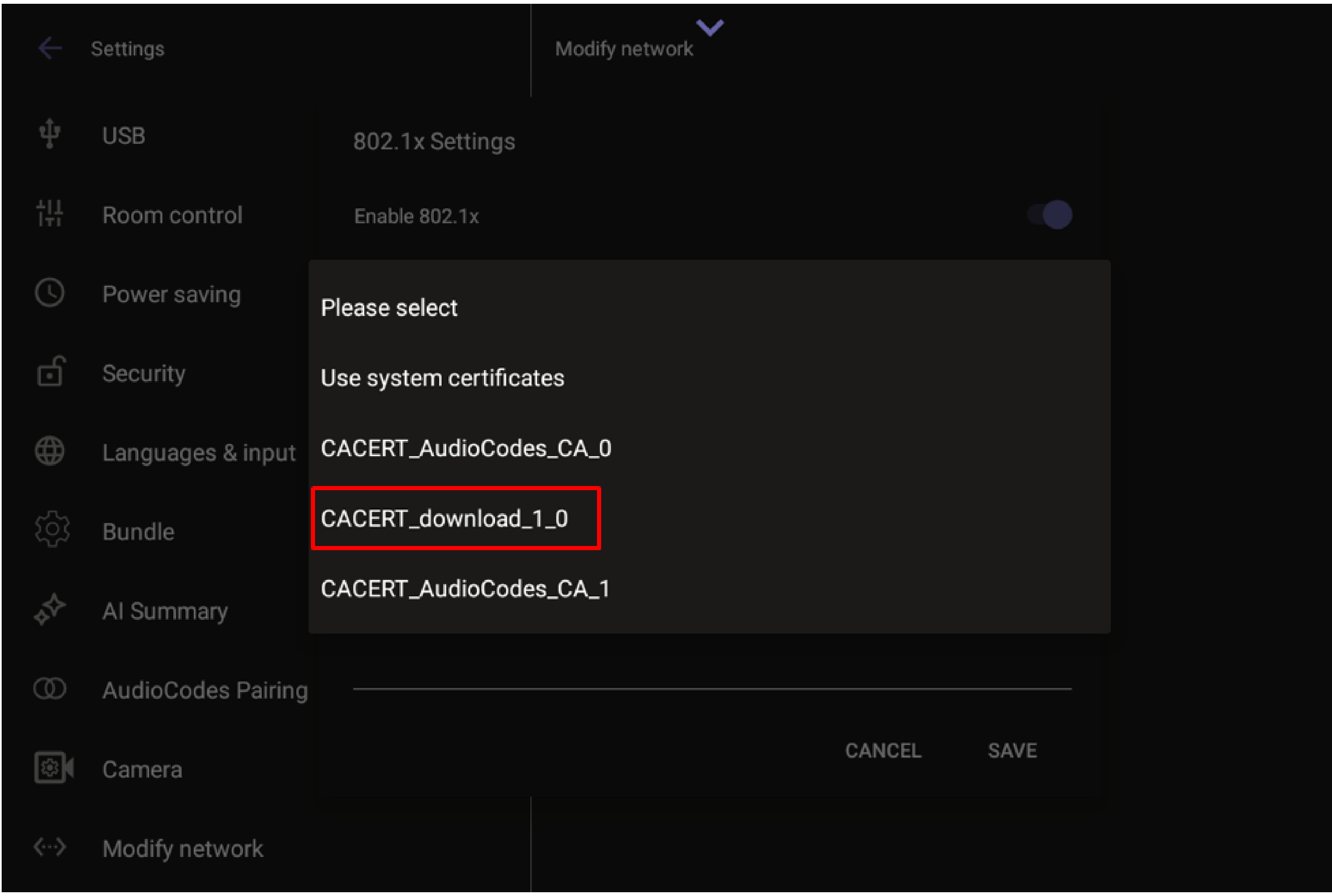
Please select

User certificate

Please select

Identity

4. Next, select the certificate source. The device can use either system certificates or certificates previously uploaded by an administrator, which will appear in the certificate list.



Please select

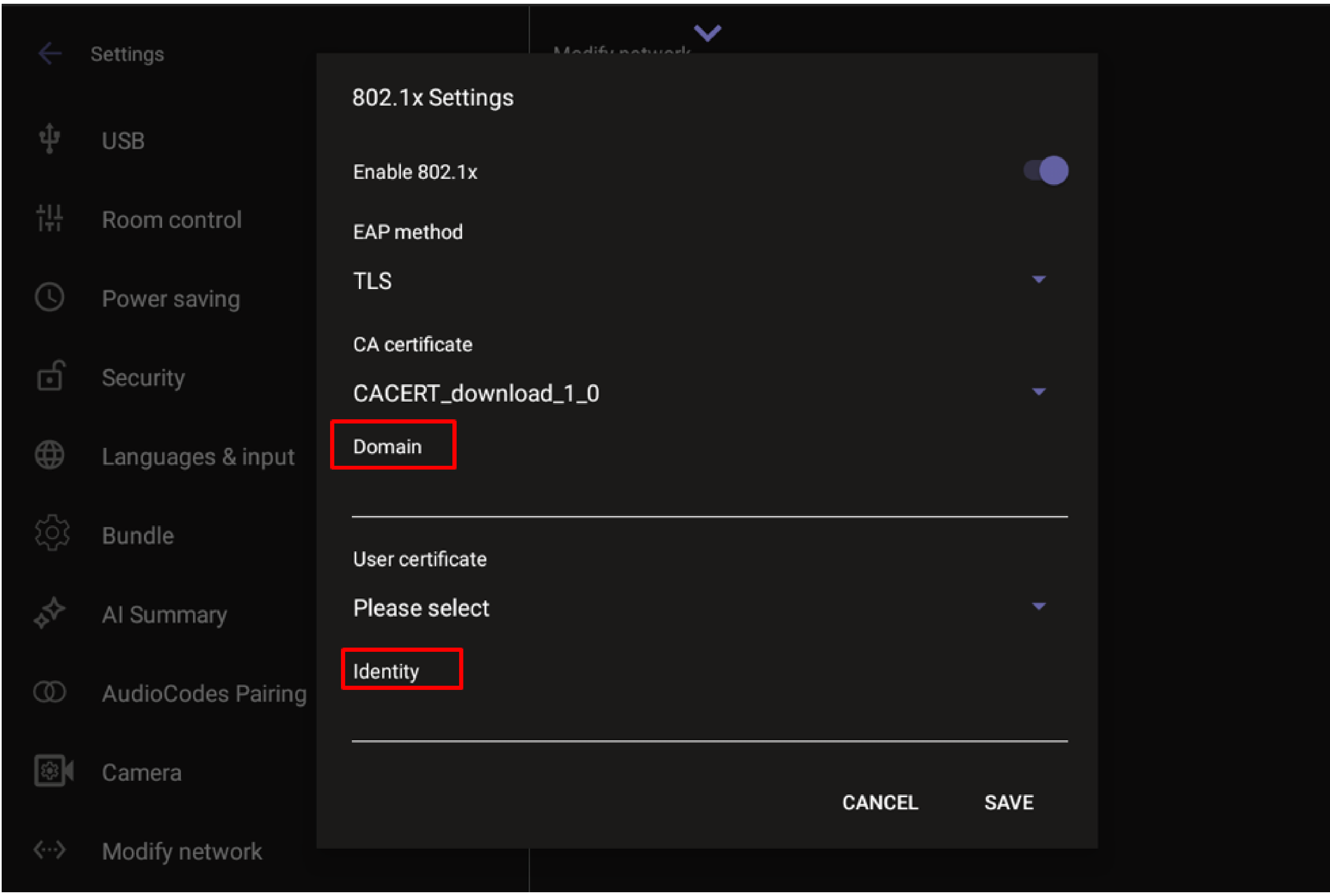
Use system certificates

CACERT_AudioCodes_CA_0

CACERT_download_1_0

CACERT_AudioCodes_CA_1

5. After selecting the appropriate certificate file, set the following:
   - **Identity** – the device identity used during authentication.
   - **Domain** – the domain the device is intended to join.



802.1x Settings

Enable 802.1x

EAP method

TLS

CA certificate

CACERT_download_1_0

Domain

User certificate

Please select

Identity

6. Click **Save** once all fields have been defined.

Configure VLAN Settings

Administrators can configure the VLAN discovery mode. If the mode is automatic, a time interval for running VLAN must be set.

➢ To configure VLAN:

1. Navigate to ‘Modify network’ (see Modify IP Network Settings on page 24) and select **VLAN Settings**.
2. Select the requested VLAN Discovery mode, then tap **OK**:
   - Disabled (no VLAN)
   - Manual configuration
   - Automatic configuration through:
     - CDP (Cisco Discovery Protocol), which is a proprietary Data Link Layer protocol
     - LLDP (Link Layer Discovery Protocol), which is a standard layer 2 discovery protocol

- Both CDP and LLDP

3. If you selected an automatic configuration, set the requested periodic **VLAN Interval** between CDP/LLDP advertisements. Default is 30 seconds.

You can increase or decrease the intervals between the CDP/LLDP packets that are sent, based on network traffic and topology.

> ⚠ In versions before 1.19, if network VLAN mode /network/lan/vlan/mode was set to **LLDP**, the device retrieved the VLAN and LLDP switch information (for location purposes) from LLDP.
> Starting from version 1.19, this VLAN and LLDP switch information is retrieved when the parameter network/lan/lldp/enabled=**1**. This is true even if VLAN is retrieved from **CDP**, or if VLAN is disabled or **Manual**.

Enroll Certificates using SCEP

The device supports certificate enrollment using Simple Certificate Enrollment Protocol (SCEP) using Microsoft's Network Device Enrollment Service (NDES) server without using AudioCodes' OVOC, thereby allowing device certificates and CA certificate provisioning to be scaled to multiple devices.

After devices are provisioned with a SCEP-related configuration, they receive a CA certificate from the NDES (via the parameter 'security/ca_certificate/0/uri'). They then issue a Certificate Signing Request (CSR) to the NDES and receive a device certificate signed by the received CA certificate.

Network administrators must configure the following three parameters:

- security/SCEPEnroll/ca_fingerprint
- security/SCEPEnroll/password_challenge
- security/SCEPServerURL

The following table shows the SCEP parameter descriptions.

Parameter	Description
security/SCEPEnroll/ca_fingerprint	Define the thumbprint (hash value) for the CA certificate. Default value: `NULL` Network admins must set its value as in the following example: `3EBE50003ABF1DF5E6B5A3230B02B856`
security/SCEPEnroll/password_challenge	Define the enrollment challenge password. Default value: `NULL`

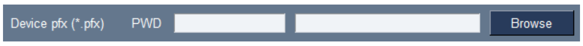
Parameter	Description
	Network admins must set its value as in the following example: 7A7F9FC4BB7625F0935E67EA6D6322ED
security/SCEPServerURL	Define the NDES server’s URL. Default: NULL Network admins must set its value as in the following example: https://ndes_derver
security/SCEPEnroll/renewal/advancethreshold	Define the renewal advance threshold of the device certificate. Configure between 50 and 100 (in units of percentage). Default: 80 The default value indicates that a renewal of the certificate (device.crt) will be initiated when 80 percent of its validity is reached.
security/SCEPEnroll/rollover/advancethreshold	Specify the threshold of the CA Root certificate’s validity at which to initiate a renewal. Configure between 50 and 100 (in units of percentage). Default: 90 The default value indicates a renewal of the certificate (CAROOT.crt.) will be initiated when 90 percent of its validity is reached.

Provision Certificates in .pfx Format

Device certificates can be provisioned in .pfx format (combining .crt and key). The following parameter values can consequently be configured in the devices’ Configuration File:

- /security/device_certificate_url = <url>/certificate.pfx
- /security/device_private_key_url = NULL
- security/device_certificate/password=<pfx password>

The feature is also supported by AudioCodes’ Android Phone Utility.



- Certificate loading is performed using HTTP; prior to version 1.19, it was performed using SCP.
- The HTTP port is 8000.
- Make sure the port is not blocked by the organization’s firewall.

6 System Monitoring and Debugging

From the 'Debugging' page on the RX-PAD, Admin users can perform system monitoring and debugging for troubleshooting purposes.

➢ To access the 'Debugging' page:

1. If not already logged in, log in to Device Administration to get admin access (see Log in to Device Administration on page 15).
2. Navigate to ‘Device Admin Settings’ (see Access Device Admin Settings on page 15).
3. Scroll down and tap **Debugging**.

The 'Debugging' page gives you various options for monitoring performance and debugging issues:

- Monitor the System Status on the next page
- Enable Remote Logging on the next page
- Copy Diagnostic Data to SD Card on page 34
- Reset the System Configuration on page 34
- Reset User Data on page 36
- Perform Debug Recording on page 36
- Control Screen Capture on page 36
- Return to Previous Version on page 37

Additional procedures for device monitoring and troubleshooting are:

- Determine Device Status from LED Color Indications on page 37
- Perform Recovery Operations using the Power Button on page 38
- Restore Device Firmware via USB Disk on page 39

⚠ Additionally:

- An enhanced bug report is available for efficient debugging. This report, which can be extracted via the Device Manager or manually from the device, contains information such as pack up time metrics and output of `ps`, `top`, `meminfo`, and `df` commands. (The `df` commands retrieve information about file system disk space usage).

Monitor the System Status

Admins can monitor the state of the device's modules from the System State screen. This screen can indicate the reason for unsuccessful initial provisioning, network related issues, or Device Manager connection issues.

System State monitoring enables debugging via the device's screen *without requiring external systems*. The admin can check connectivity *independently of external apps*.

> For some states, the reason for failure will be displayed as well.
> Each state displays its operational result: Successful or Failed.

➢ To monitor the device's module states:

1. Access the 'Debugging' page (see System Monitoring and Debugging on the previous page).
2. Scroll down and tap **System State**, then scroll down to the requested information.

Enable Remote Logging

Remote Logging via Syslog provides log-level diagnostics with information relevant to device issues. With Remote Logging via Syslog, logs are collected in real time.

> Network administrators can also enable Syslog using Secure Shell (SSH) protocol.

➢ To enable Remote Logging via Syslog:

1. Access the 'Debugging' page (see System Monitoring and Debugging on the previous page).
2. Tap **Remote logging**.
3. Configure the **Remote IP address** and **Remote port** and enable **Remote Logging**; the device starts sending logs to the Syslog server.

➢ To enable Syslog using SSH protocol, type the following command at the shell prompt:

```
setprop persist.ac.rl_address <syslog_server_ip>:<port>.
```

➢ To disable Syslog using SSH, type the following command at the shell prompt:

```
setprop persist.ac.rl_address ""
```

Copy Diagnostic Data to SD Card

Admin users who need to get logs from the device can dump the logs to the phone’s Secure Digital (SD) Card and then later collect them using Secure Copy Protocol (SCP) based on Secure Shell (SSH) protocol. Whenever an issue occurs, the Admin can dump the logs into the SD Card.

➢ **To use the tool:**

1. Access the 'Debugging' page (see System Monitoring and Debugging on page 32).
2. Tap **Diagnostic Data**.
3. Tap **OK** to confirm ‘Copy logs to sdcard’; the device creates all necessary logs and copies them to the **SD Card/Logs** folder.
4. Get the logs using SCP notation as follows:

```
scp -r admin@host_IP:/sdcard/logs/ .
```

Following are the relevant logs (version and ID may be different to those shown here):

- dmesg.log
- dumpstate-TEAMS_1.3.16-undated.txt
- dumpstate_log-undated-2569.txt
- logcat.log

Reset the System Configuration

Administrators can use one of the following reset methods depending on the issue:

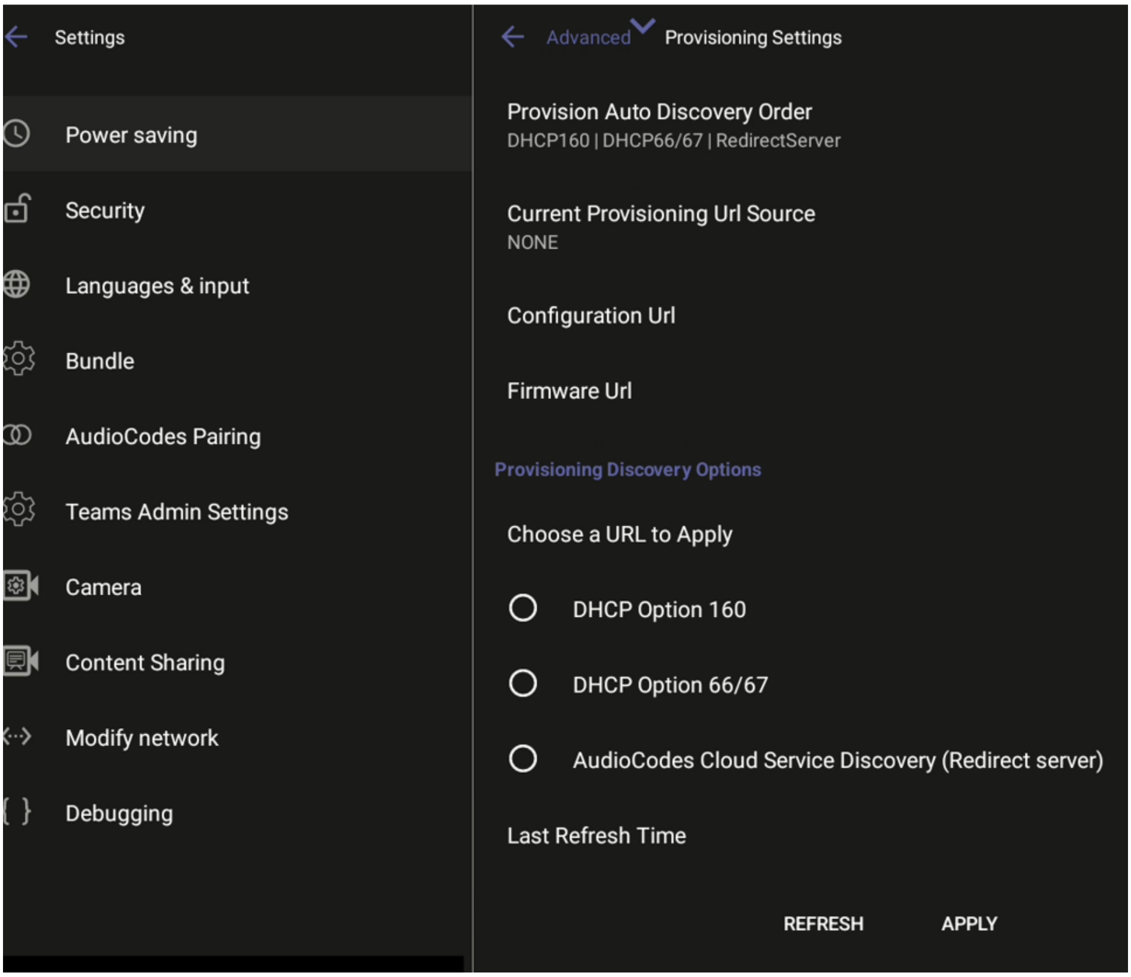
- Configure Provisioning Source Auto Discovery Settings below
- Perform a Full Factory Reset on the next page

Configure Provisioning Source Auto Discovery Settings

Admins can select the preferred discovery option for the MTRA without affecting other devices in the network. This action restarts the device but does *not* perform a factory reset.

➢ **To set up provisioning source discovery:**

1. Access the 'Debugging' page (see System Monitoring and Debugging on page 32).
2. Tap **Advanced**, then **Provisioning Settings**. The page displays the current order for provisioning auto discovery, as well as the URL locations of the provisioning, configuration, and firmware sources.



Provision Auto Discovery Order
DHCP160 | DHCP66/67 | RedirectServer

Current Provisioning Url Source
NONE

Configuration Url

Firmware Url

Provisioning Discovery Options

Choose a URL to Apply

○ DHCP Option 160

○ DHCP Option 66/67

○ AudioCodes Cloud Service Discovery (Redirect server)

Last Refresh Time

3. Select the desired discovery option for the device and click **APPLY**. After restarting, the device will use the selected option for provisioning. If no provisioning source is discovered, the system will use an alternate discovery option based on the Discovery Order setting.
4. To update the page with the latest changes and locations, click **REFRESH**.

Reset to Original Configuration

Admin users can opt to ‘clean up’ their configuration history and return the RXV81 to an Out of Box Experience (OOBE). If the Teams app isn't running well, this might help.

➢ **To perform a factory reset:**

1. Access the 'Debugging' page (see System Monitoring and Debugging on page 32).
2. Tap **Reset configuration**, then tap **OK** to confirm.

All data is erased and default factory settings are restored, but sign-in is retained.

Perform a Full Factory Reset

This option is the equivalent of restoring to defaults, including logout and device reboot.

➢ To erase all data (factory reset):

1. Access the 'Debugging' page (see System Monitoring and Debugging on page 32).
2. Tap **Erase all data (factory reset)**, then tap **OK** to confirm.

Reset User Data

This function resets all user-defined settings that are not admin settings, such as brightness, contrast, fonts, etc.

The user is signed out after performing this operation.

Restart the Teams App

If the Teams application freezes or malfunctions, a good way to resolve this is to restart the app.

➢ To restart the Teams app:

1. Access the 'Debugging' page (see System Monitoring and Debugging on page 32).
2. Tap **Restart Teams App**; only the Teams app is restarted.

Perform Debug Recording

This feature enables Admin users to perform media/DSP debugging.

⚠ DSP recording can be activated on the fly without requiring the network administrator to reset the device.

➢ To set up recording:

1. Access the 'Debugging' page (see System Monitoring and Debugging on page 32).
2. Tap **Debug Recording**, then tap **Voice record** to enable the feature.
3. Tap **Remote IP address** to input the IP address of the device whose traffic you want to record.
4. Tap **Remote port** and input it (Default: 50000).
5. Start Wireshark on your PC to capture audio traffic.

Control Screen Capture

By default, Screen Capture is enabled (using AudioCodes' SSH protocol based Android Device Utility or the Device Manager). If disabled, the phone won't allow its screens to be captured.

➢ To enable or disable screen capture:

1. Access the 'Debugging' page (see System Monitoring and Debugging on page 32).
2. Scroll down and turn the **Screen Capture** toggle button on or off.

Return to Previous Version

When a customer receives a build for testing and completes the testing, they must switch back to the previous firmware version. This version is the General Availability build running on the device.

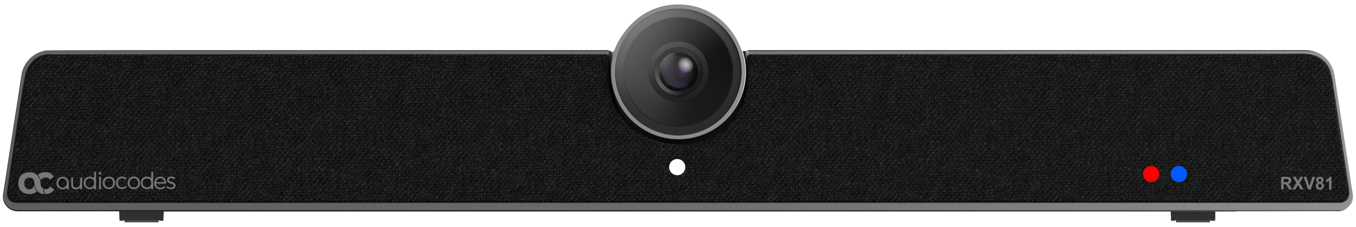
➢ To return to the previous version:

1. Access the 'Debugging' page (see System Monitoring and Debugging on page 32).
2. Tap **Return to previous version**. The device changes the active firmware slot and undergoes a factory reset.

Determine Device Status from LED Color Indications

Users and admins can determine the status of the from its LED color indications.

Use the following figure and table as reference to determine RXV81 status when viewing LEDs:



🔴	**Red / white / red & white**
White on	Device is powered on, signed in to Teams
White flashing	Device is in booting phase
Red on	Device is in mute (highest priority state)
Red flashing	Network connectivity lost / Device is in upgrade mode / RCU connectivity lost
Red + white on	Device is powered on, network is connected, but not signed into Teams
🔵	**Blue**

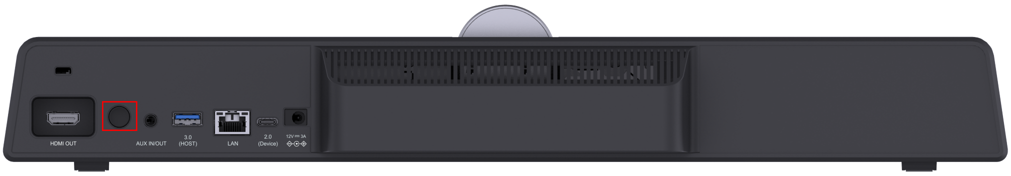
Blue on	In a call (active call or meeting)
Blue flashing	Incoming call
	Camera on/off
White on	Camera on
White off	Camera off

Perform Recovery Operations using the Power Button

Network administrators can perform recovery operations using the power button on the rear panel of RXV81.

> Besides this recovery option, Android devices also feature an independent, automatic problem detection and recovery attempt capability that can culminate in recovery mode or in switching image slots.

The following figure shows the power button.



➢ To perform recovery operations:

1. 1. Disconnect the power cord from RXV81 while long-pressing the power button for as long as is required for the action (see the 'Action' and 'Long press for' columns in the following table).

Table 6-1: Recovery Operation Options using RXV81’s Power Button

Stage	Action	Long-press for	LED Flashes 3x
On Uboot	NOTHING	< = 2 seconds	
	ENTER_RECOVERY	2-4 seconds	RED
	SWITCH_AB_SLOT	4-6 seconds	WHITE
	ENTER LOADER	6-8 seconds	BLUE
	RESTORE_DEFAULT	8-10 seconds	BLUE + WHITE
	SHUTDOWN	> = 10 seconds	

3. 2. Reconnect the power cord and continue pressing the power button for however long is necessary.

4. 3. In the recovery menu use the power button to navigate between menus in the recovery mode. A long press selects the highlighted option.

Save Logs while the Device is in Recovery Mode

The device features USB log export while in recovery mode. This feature enables users to seamlessly save logs while their device is in recovery mode.

In Android recovery mode, the system automatically mounts a partition, enabling users to connect a USB stick.

By simply clicking the **Export logs to USB disk** option, all logs are efficiently copied to the USB stick, providing a convenient and reliable method for log management during recovery procedures.

Restore Device Firmware via USB Disk

For recovery purposes, firmware can be applied to the MTRA from a USB disk.

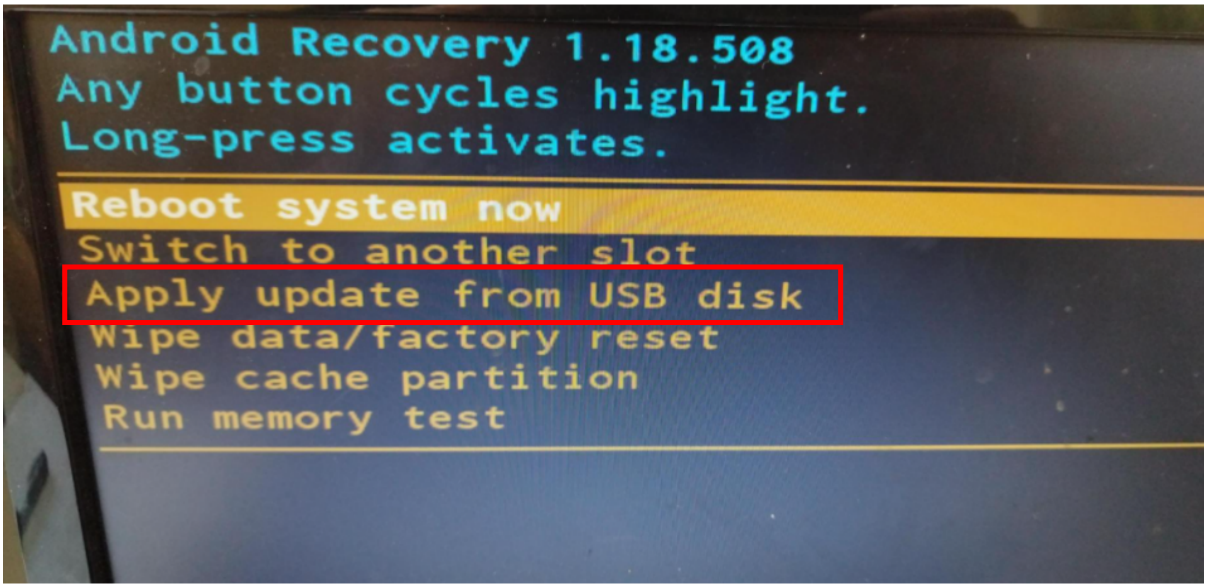
➢ To apply the firmware from the USB disk:

1. Enter recovery mode by pressing for 2-4 seconds the power button (Action: ENTER_ RECOVERY); the device's LED lights up red.

2. Short-press the power button to move down the menu options, and long-press to select an option.

3. Insert the USB disk with the target firmware.

4. Select the **Apply update from USB disk** option and then choose the correct firmware image from the disk.



```
Android Recovery 1.18.508
Any button cycles highlight.
Long-press activates.

Reboot system now
Switch to another slot
Apply update from USB disk
Wipe data/factory reset
Wipe cache partition
Run memory test
```

This page is intentionally left blank.

International Headquarters

6 Ofra Haza Street
Naimi Park
Or Yehuda, 6032303, Israel
Tel: +972-3-976-4000
Fax: +972-3-976-4040

AudioCodes Inc.

80 Kingsbridge Rd
Piscataway, NJ 08854, USA
Tel: +1-732-469-0880
Fax: +1-732-469-2298

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

Website: https://www.audiocodes.com/

Documentation Feedback: https://online.audiocodes.com/documentation-feedback

©2026 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, AudioCodes One Voice, AudioCodes Meeting Insights, and AudioCodes Room Experience 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-09995