Video Collaboration Bar User's and Administrator's Manual

AudioCodes Room Experience (RX) Suite

RXV81 MTRA

Version 3.0

audiocodes

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
RX-PAD Room Controller User's and Administrator's Manual
Pairing RX-PAD with Microsoft Teams Room on Android
RXV81 MTR on Android Video Collaboration Bar with RX-PAD or RCU Quick Installation Guide
RXV81 BYOD User's and Administrator's Manual
Teams Sign-in Implementation for AudioCodes MTRA Devices
One Voice Operation Center (OVOC) User’s Manual
Device Manager Administrator’s Manual

Document Revision Record

LTRT	Description
18267	Update Version 2.8.208 Updated Time Zone
18269	Updated to Version 2.8.574 (M1)
09989	Updated to Version 2.8.855 (M2)
09990	Updated to Version 2.8.917 (M3) 802.1x authentication parameters
09996	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 is a standalone Microsoft Teams Rooms on Android™ (MTRA) video bar that takes advantage of plug-and-play simplicity to deliver a familiar and exceptionally productive Microsoft Teams meeting experience.

Outstanding image clarity and enhanced voice quality ensure that remote participants can see and hear everyone in the room and can also participate in full Teams video and content sharing sessions.

RXV81 stands out with its video and audio capabilities, embedded speaker and a 6-element microphone array, as well as Full HD and ePTZ with 5x zoom. These combine seamlessly to make every meeting interactive and personable.

Stylishly designed and quick to set up, RXV81 is by default a standalone MTRA specifically designed for huddle rooms and small shared rooms, as well as for managers' and executives' personal offices in today's busy hybrid workplaces. When used as a standalone MTRA, video and sharing are displayed on the TV screen and meetings are controlled via AudioCodes' RX-PAD Meeting Room Controller or the Remote Control Unit (RCU).

> ⚠ In addition to standalone mode, RXV81 can be used in ad hoc peripheral mode. In this mode, customers connect RXV81 to a BYOD (Bring Your Own Device) (PC/laptop) running a UC client. The BYOD displays meeting video and content, and meetings are controlled via the BYOD (join, accept, manage participants). Audio/video (camera ePTZ, mic mute) can be controlled via the UC client or the RCU (camera on / off, mute, volume). To learn more about RXV81 with BYOD, refer to the RXV81 BYOD User's and Administrator's Manual.

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

RXV81 is supported by AudioCodes' Device Manager, a plugin of the AudioCodes One Voice Operations Center (OVOC), allowing IT managers to remotely oversee and upgrade all deployed devices with ease from anywhere.

Refer to the AudioCodes website for additional information.

> ⚠ 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:

- **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.

- **Peripheral mode.**

  RXV81 can be used on an ad hoc basis as a USB A/V peripheral for any UC client.

Benefits

- Intuitive meeting experiences with one click to join using the MTRA application
- Easy-to-use mounting element and minimal cable connections for quick and simple deployment
- Audio via a full-room pickup with no need for an additional external USB mic or speaker
- Effortlessly manage meetings using the dedicated Bluetooth remote control or RX-PAD

- Audio notifications triggered by RX-PAD are heard through the RXV81 speaker, including Talkback accessibility, to ensure a streamlined and accessible communication experience during meetings and collaboration sessions
- Optional centralized management with AudioCodes' OVOC / Device Manager (see Management on the next page)

Bundles

The *RXV81* MTRA is available in the bundles listed in the following table:

Name of Bundle	Details
TEAMS-RXV81	■ Executive Offices | Huddle Rooms ■ RXV81 main unit ■ Bluetooth Remote Controller Unit (RCU)
TEAMS-RXV81-B10	■ Huddle Rooms | Small and Medium Meeting Rooms ■ 5-8 participants ■ RX-PAD Meeting Room Controller
TEAMS-RXV81-B15	■ Huddle Rooms | Small and Medium Meeting Rooms ■ 5-8 participants ■ RX-PAD Meeting Room Controller + AudioCodes RX15 Speaker
TEAMS-RXV81-B09	■ RXV81 main unit ■ Touch screen display

Hardware

- RXV81 can be used on an ad hoc basis as a USB A/V peripheral for any UC client
- 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 bundles are managed using AudioCodes' On-prem or Live Platform Device Manager, or Microsoft's Teams admin center (TAC), 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
- Upgrading the MTRA APK

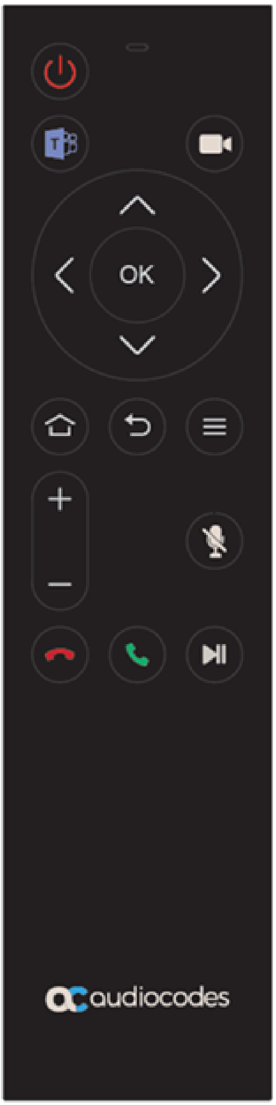
Admins can monitor the status of the device's software modules from the System State screen (see Monitor the System Status on page 63).

⚠

- Firmware downgrade is blocked as of version 2.6.280 to prevent a possible race condition (conflict) between Microsoft Teams admin center (TAC) and AudioCodes' OVOC / Device Manager.
- Downgrading an RXV200 peripheral device to a version older than the built-in release is restricted as of version 2.6.280. Peripheral devices include cameras (RXVCam50, RXVCam360, RXVCam70), audio devices (RX15 or RX40) and RX-PAD.

Remote Controller Unit (RCU)

The AudioCodes RCU is part of the **TEAMS-RXV81** 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 TEAMS-RXV81-B10 and TEAMS-RXV81-B15 Bundles on page 3), see the RX-PAD datasheet.
- For RX15 specifications (included in TEAMS-RXV81-B15 Bundles on page 3), see the RX15 datasheet.

The following table shows RXV81 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

Feature	Details
Network Provisioning	- TCP/IP (IPv4), DHCP/ static IP; Time and date synchronization via 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)
Microsoft Teams Features (Android MTR)	- Calendar integration (with meeting preview) and one click to join Teams meetings - Meet now option - Simple sign-in interface from browser or smartphone with a code - ‘Direct guest join’ to allow joining a third-party meeting - ‘Cast info’ from mobile to the RXV81 screen over Bluetooth - ‘Room remote’ using Teams mobile app allowing controlling RXV81 - Remote sign-out from Microsoft Teams admin center (TAC). - Hide names and meeting titles for individual devices - Meeting stage - Multi-spotlight - Docked meeting controls - Reactions - Control camera/mic for attendees - Live Captions in regular one-on-one calls and in Teams meetings - Whiteboard support when signed in with personal account (short term roadmap for whiteboard support with room account)

Feature	Details
	■ Multi-cloud sign-in support ■ Remote provisioning and sign-in from TAC
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 ■ Shortcut keys for administrators to manually perform recovery operations ■ Ad Hoc Peripheral Mode allows connecting RXV81 via USB to the PC as a peripheral device.

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 consists of:

1. Installingthe RXV81 unit:
   - Reviewing the package contents checklist
   - Positioning
   - Mounting
   - Cabling
   - Powering up

   For details, see the *RXV81 MTR on Android Video Collaboration Bar with RX-PAD or RCU Quick Guide* shipped with the product oravailable from AudioCodes.
2. Pairing and setting up the RXV81 unit with RX-PAD or with the Remote Controller Unit (see Pair RXV81 with RX-PAD below or Pair RXV81 with the RCU on the next page).
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 RX-PAD

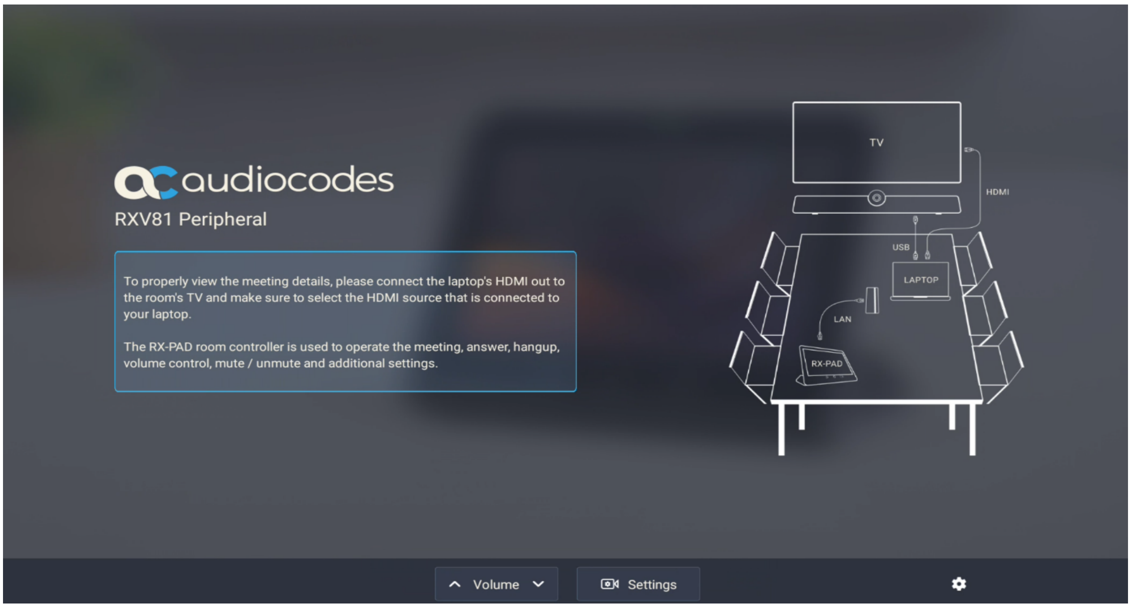
Customers that acquired an RXV81P-B10 bundle (see Bundles on page 3) need to pair the RXV81 with the RX-PAD (which is part of the bundle).

➢ **Before pairing:**

- Make sure both devices are running the latest AudioCodes firmware version.
- Make sure both devices are connected to the same network (subnet).
- Make sure that UDP port 9999 is open in both directions inside the network.
- For Wi-Fi connectivity, you must use a power supply adapter (not supplied but can be ordered separately).
- Make sure that the distance between the pairing devices is close enough for uninterrupted Bluetooth connectivity.

➢ To pair the RXV81 with the RX-PAD:

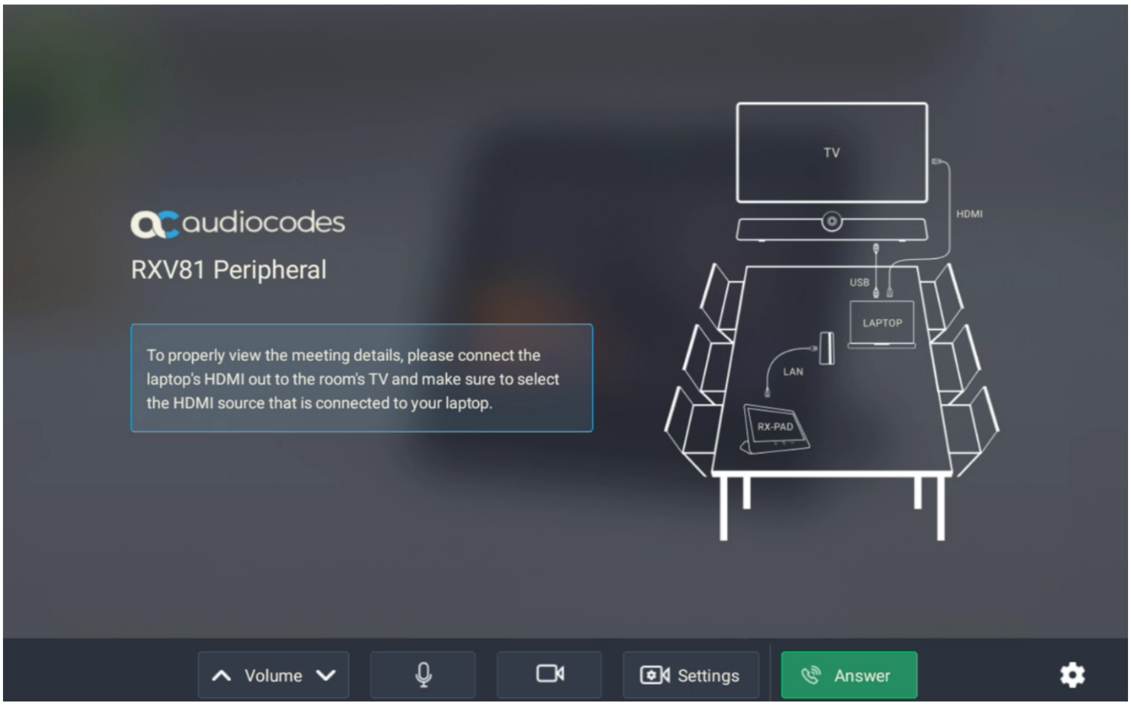
1. After connecting the RX-PAD and RXV81 to the network, the pairing process automatically begins.
2. Once pairing is complete, the RX-PAD displays the following:



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.

The RX-PAD room controller is used to operate the meeting, answer, hangup, volume control, mute / unmute and additional settings.

3. When a call comes in, view the incoming call's functions on the RX-PAD, for example, ANSWER, as shown in the following figure.



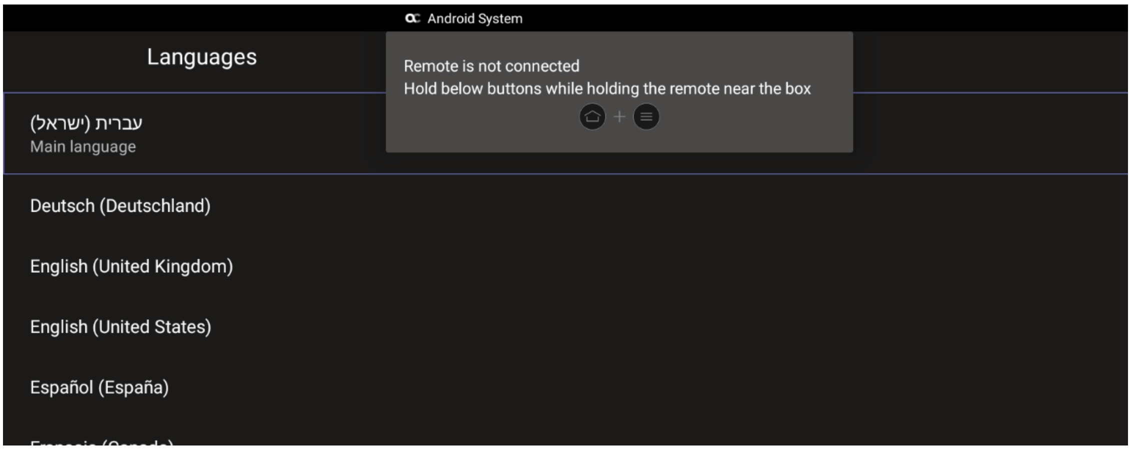
To properly view the meeting details, please connect the laptop's HDMI out to the room's TV and make sure to select the HDMI source that is connected to your laptop.

Pair RXV81 with the RCU

Customers that acquired a **TEAMS-RXV81** bundle (see Bundles on page 3) 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. View in the display the message:
   Remote is not connected. **Hold below buttons while holding the remote near the box**.



Android System

Languages

Remote is not connected
Hold below buttons while holding the remote near the box

עברית (ישראל)
Main language

Deutsch (Deutschland)

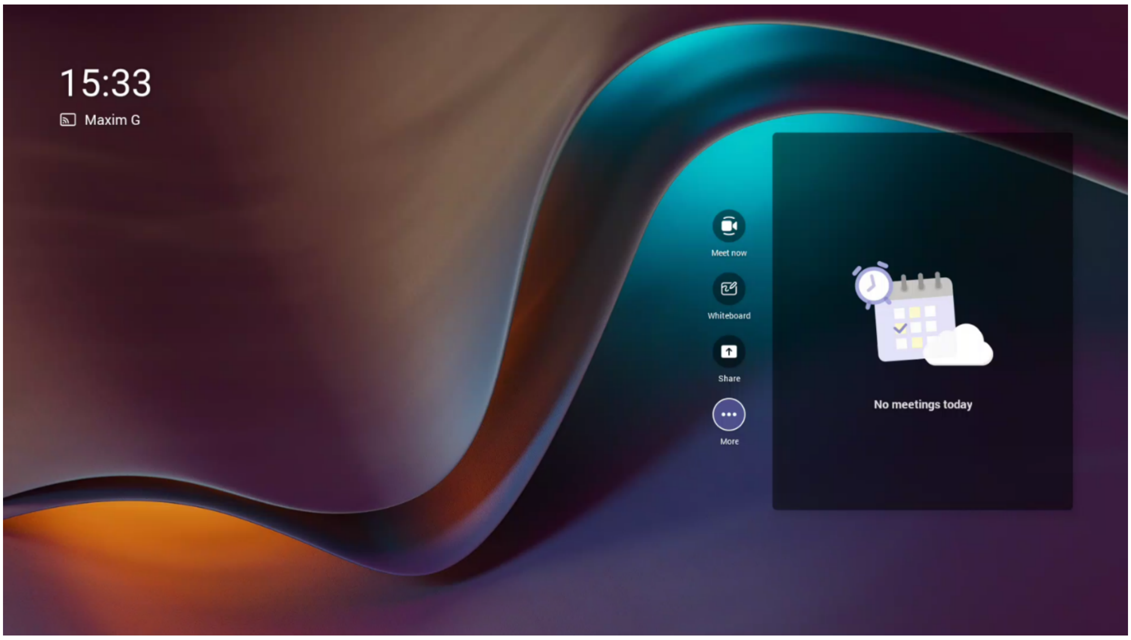
English (United Kingdom)

English (United States)

Español (España)

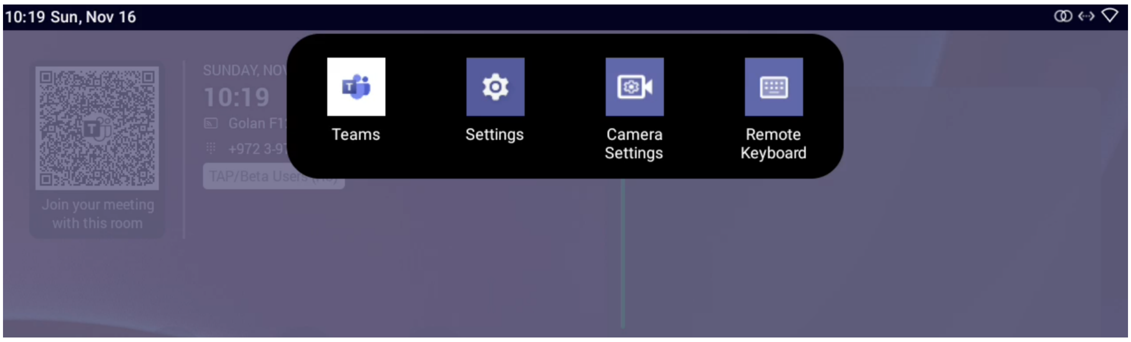
Français (Canada)

3. On the RCU, simultaneously press and hold ■ + ■ until the RCU and the RXV81 are connected and a **Remote connection succeeded** message is displayed.
4. Use the remote control to navigate to and select a language; the Microsoft Teams sign-in screen is displayed.
5. Follow Teams instructions to sign in. The RXV81 home page is displayed.



After Pairing

If you paired a RX-PAD with your RXV81 , scroll down in the RX-PAD to this:



From left to right:

- **Teams** (tap to refresh RX-PAD’s UI)
- **Settings** (tap to enter RX-PAD’s Device Settings)
- **Camera settings** (tap to open the MTRA’s Camera Settings)
- **Remote keyboard** (tap to control the MTRA)

3 Meetings and Calls

This chapter describes how you can use your RXV81 MTRA for conducting value-added meetings. For functions involving Microsoft Teams actions, the description provides a reference to the relevant Microsoft documentation.

- To get the utmost of your meetings, set up camera settings to suit your requirements. For instructions, see MTRA Camera Settings on page 23.
- For detailed instructions on how to operate an RX-PAD, refer to the RX-PAD Room Controller User's and Administrator's Manual.

Schedule Meetings

To schedule a meeting that will use your MTRA meeting room, send out a Teams invitation that includes the MTRA in the list of attendees. The name of the meeting room is displayed on the RX-PAD (if paired) and MTRAhomepages.

If the MTRA is not already booked, it will accept the meeting and display it on the homepage, allowing you to join by tapping the **Join** button. After the meeting is over, it disappears from the homepage.

For instructions on how to send a meeting invitation, refer to the relevant Microsoft Teams documentation.

Ad-hoc Meetings and Calls

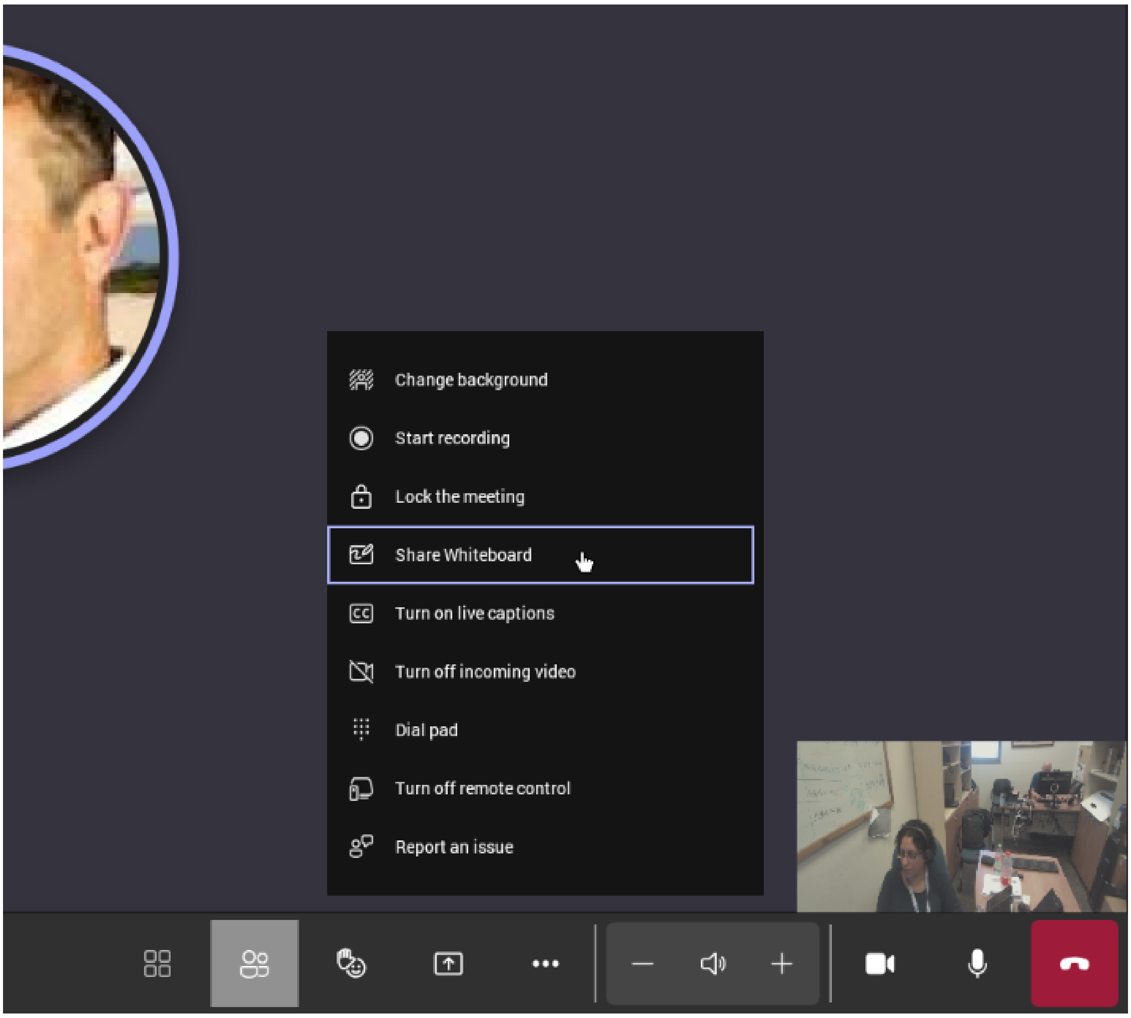
Ad-hoc meetings and calls can be conducted from the RX-PAD homepage in the same way as from a Teams channel. For details, see the relevant Microsoft Teams documentation.

Share a Microsoft Whiteboard

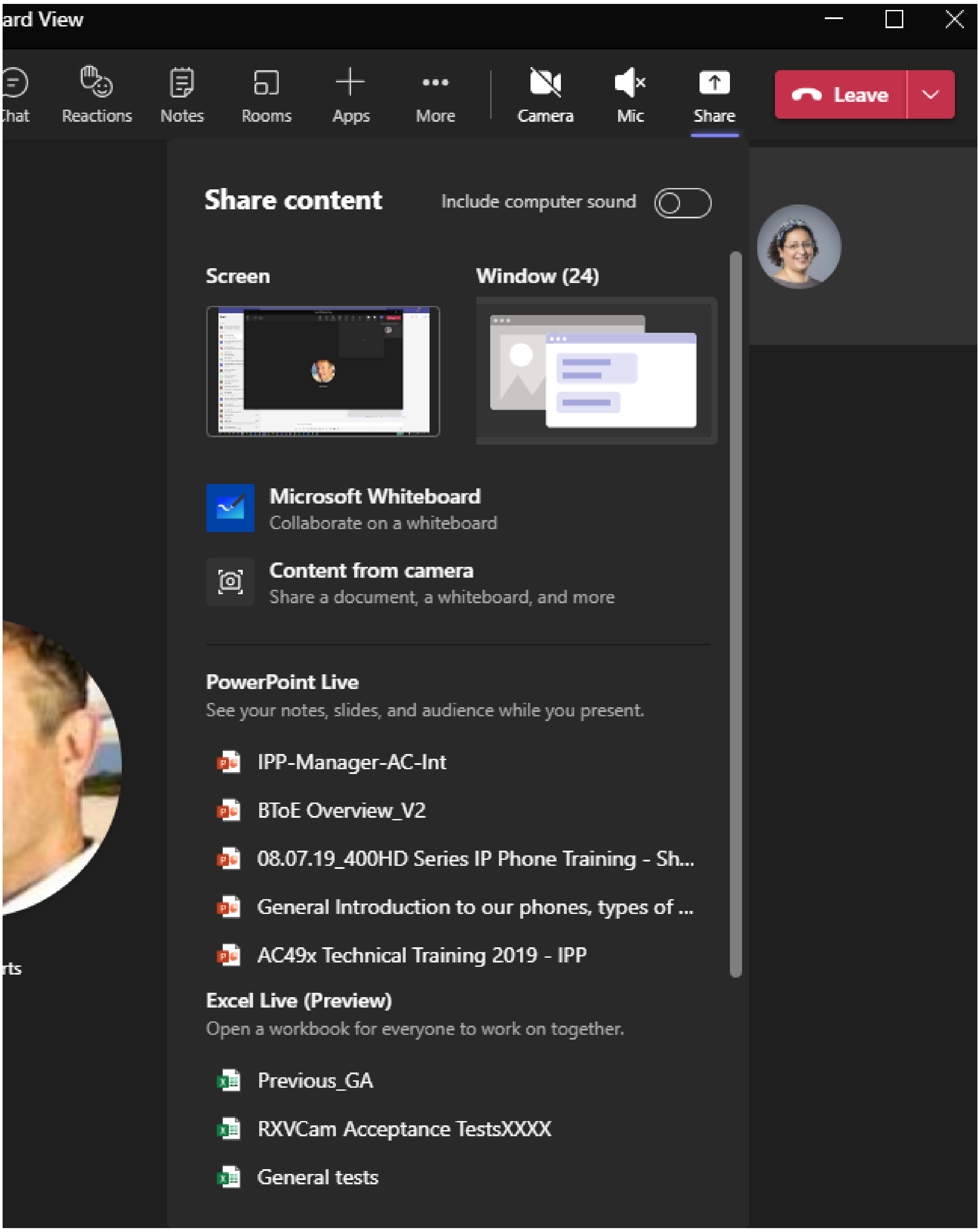
During Teams meetings, participants can open a virtual whiteboard – a digital canvas - on which they can sketch, illustrate, collaborate, brainstorm, plan, and share perspectives with one another in real time. The focus switches away from the presenting participant to the whiteboard. For more details, see the relevant Microsoft documentation.

➢ **To share the Whiteboard:**

- From the **...** menu (in the MTRA GUI), select **Share Whiteboard**.



- Alternatively, access the Whiteboard from **Share content**:



Share content

Include computer sound

Screen

Window (24)

Microsoft Whiteboard
Collaborate on a whiteboard

Content from camera
Share a document, a whiteboard, and more

PowerPoint Live
See your notes, slides, and audience while you present.

- IPP-Manager-AC-Int
- BToE Overview_V2
- 08.07.19_400HD Series IP Phone Training - Sh...
- General Introduction to our phones, types of ...
- AC49x Technical Training 2019 - IPP

Excel Live (Preview)
Open a workbook for everyone to work on together.

- Previous_GA
- RXVCam Acceptance TestsXXXX
- General tests

Edit the Whiteboard; every participant with privileges can edit it.

Screen Sharing

The RXV81 MTRA enables users to share their PC/laptop screen via the RX-PAD HDMI In port, to be shared on the screen in idle mode and peripheral mode.

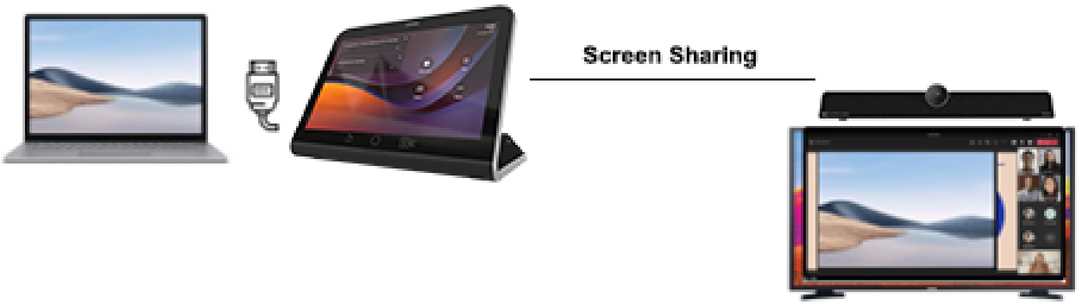
⚠ A short HDMI cable connects the PC/laptop to the RX-PAD HDMI In port. The connection between the RX-PAD and the MTRA is thus 'cableless'.

The feature offers added flexibility by enabling the use of a shorter HDMI cable connected to the center of the meeting room desk, in contrast to a longer (more expensive) cable connected to the MTRA positioned in the front of the room.

- **In-Meeting Mode:** When the MTRA is in a meeting, the presenter can use the Teams app 'Share' key to share their PC screen with in-person attendees who are physically present in the same meeting room, as well as with remote attendees. [Audio sharing is currently unsupported].
- **Idle Mode:** When the MTRA is not in a meeting, the presenter can use the Teams app 'Share' key to share their PC screen only with in-person attendees who are physically present in the same meeting room.

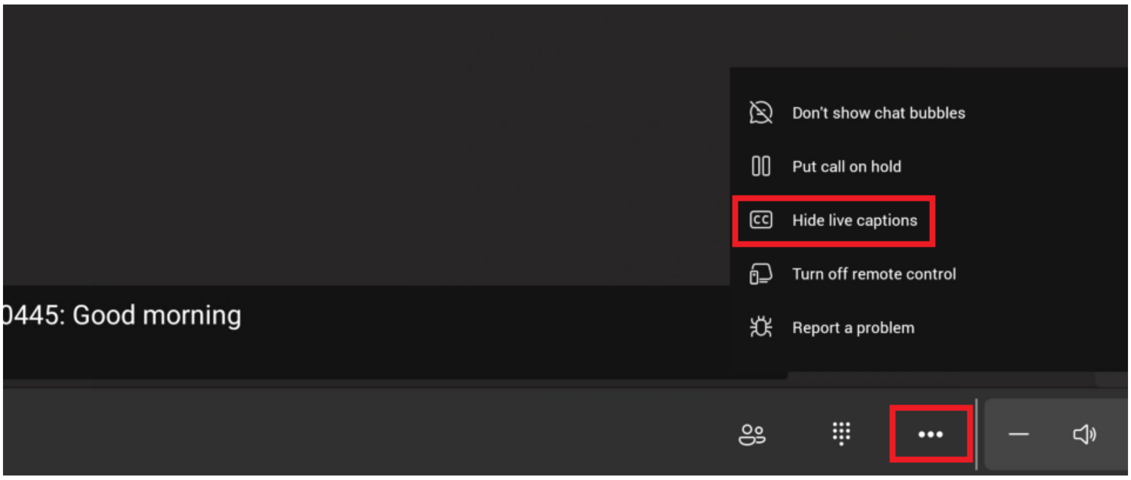
For sharing in either mode, the PC must be connected to the RX-PAD's HDMI In port.

The figure below shows the MTRA connected.



Set Live Captions

Live captions can be set in regular one-on-one calls as well as in Teams meetings. Navigate to the **...** menu at the bottom of the screen and tap the Show /Hide Live Captions toggle option.



0445: Good morning

For more details, refer to the relevant Microsoft Teams documentation.

Dial a Number

You can manually dial someone's phone number.

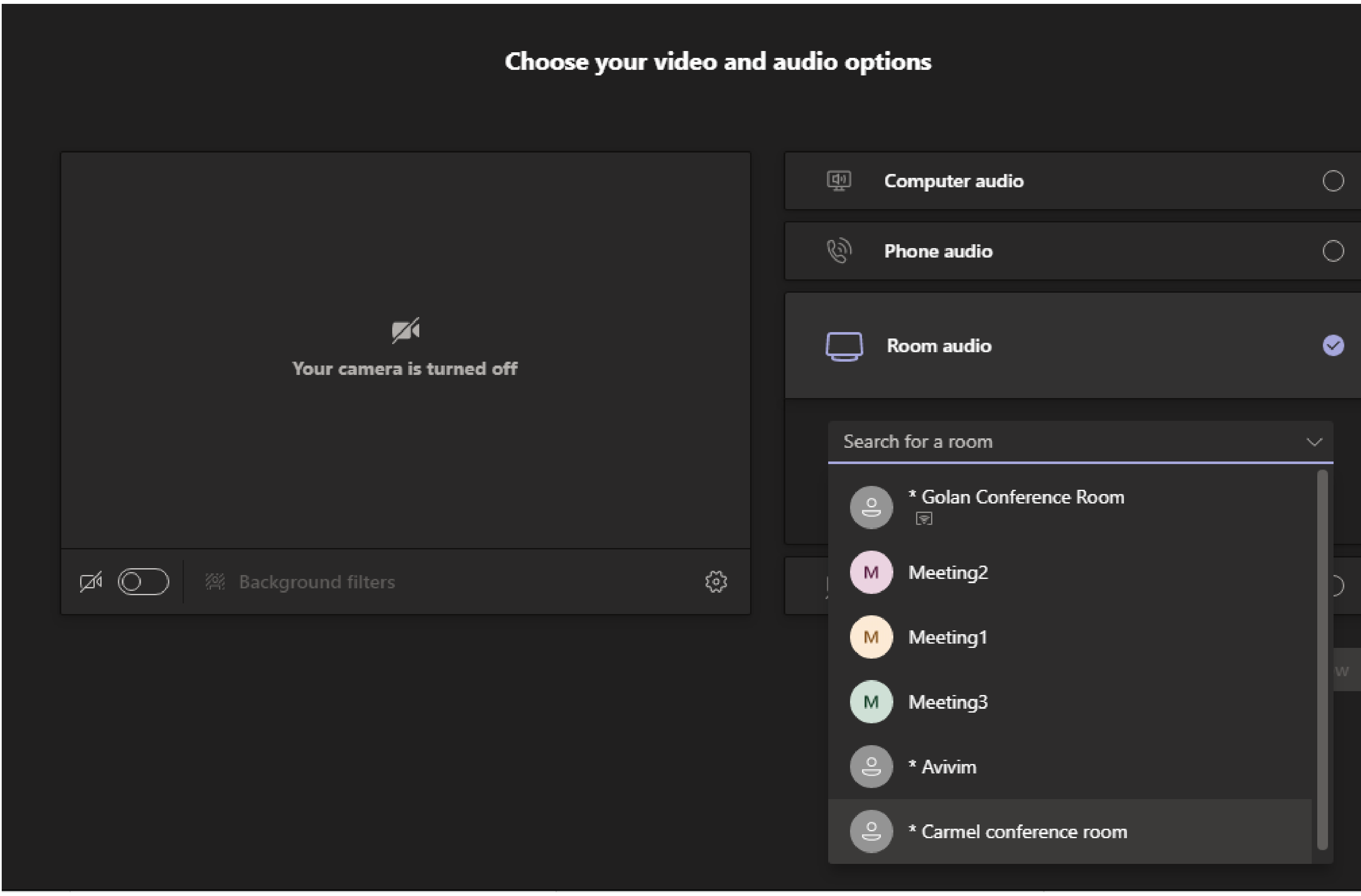
➢ **To dial a phone number:**

1. On the homepage, tap the **Call** option.
2. Enter the digits of the destination to call and select **Call**.

Enable Proximity Join

Proximity Join allows you to discover and add a nearby available MTRA, i.e., the RXV81, to any meeting. It's also possible to accept the incoming meeting on the console of the room.

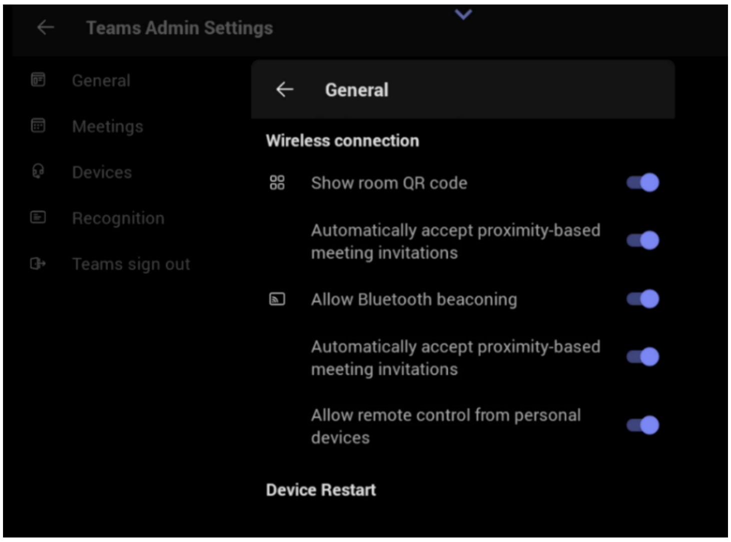
The feature functions in combination with Bluetooth and 'Bluetooth Beaconing', an integral feature in MTRAs. In the case of an RXV81 MTRA, if you bring a laptop or a Teams Mobile Client near the MTRA, it will offer the MTRA as the room audio device. The following figure shows how to select the room audio device.



After you select the room audio device, the meeting is opened without any audio device on your PC client, and then the selected device gets a request to join the meeting.

➢ **To enable 'Proximity join' using the RX-PAD:**

1. This feature requires Admin login. Navigate to 'Device Admin Settings' (see Access Device Admin Settings on page 37).
2. Scroll down and tap **Teams Admin Settings**, then navigate to **Teams Admin Settings > General**.
3. Scroll down to **Wireless connection** and verify that the **Automatically accept proximity-based meeting invitations** toggle options are turned on.



Teams Admin Settings

General

Wireless connection

Show room QR code

Automatically accept proximity-based meeting invitations

Allow Bluetooth beaconing

Automatically accept proximity-based meeting invitations

Allow remote control from personal devices

Device Restart

For more details about proximity joining, refer to the relevant Microsoft Teams documentation.

Hide Meeting Information

You can hide information such as meeting titles or chat bubbles via Teams, or from the RX-PAD as follows:

1. This feature requires Admin login. Navigate to 'Device Admin Settings' (see Access Device Admin Settings on page 37).
2. Scroll down and tap **Teams Admin Settings**, then navigate to **Teams Admin Settings > Meetings**.
3. Tap to show or hide the relevant option.

⚠ You can show and hide meeting information by default or during a specific meeting via Teams. For details, refer to the relevant Microsoft Teams documentation: Hide Attendee Names in Microsoft Teams Meetings and Chat in Microsoft Teams Meetings.

3 RXV81 in Ad Hoc Peripheral Mode

In addition to standalone mode, RXV81 can be used in ad hoc peripheral mode. This mode enables seamless integration of RXV81 with a PC or laptop by utilizing RXV81's audio and camera capabilities as primary audio and camera sources for the PC or laptop.

In this mode, you can connect RXV81 to a BYOD (Bring Your Own Device) PC or laptop running a UC client. The BYOD displays meeting video and content and meetings are controlled via the BYOD (join, accept, manage participants). Audio and video, such as camera ePTZ and mic mute, can be controlled via the UC client.

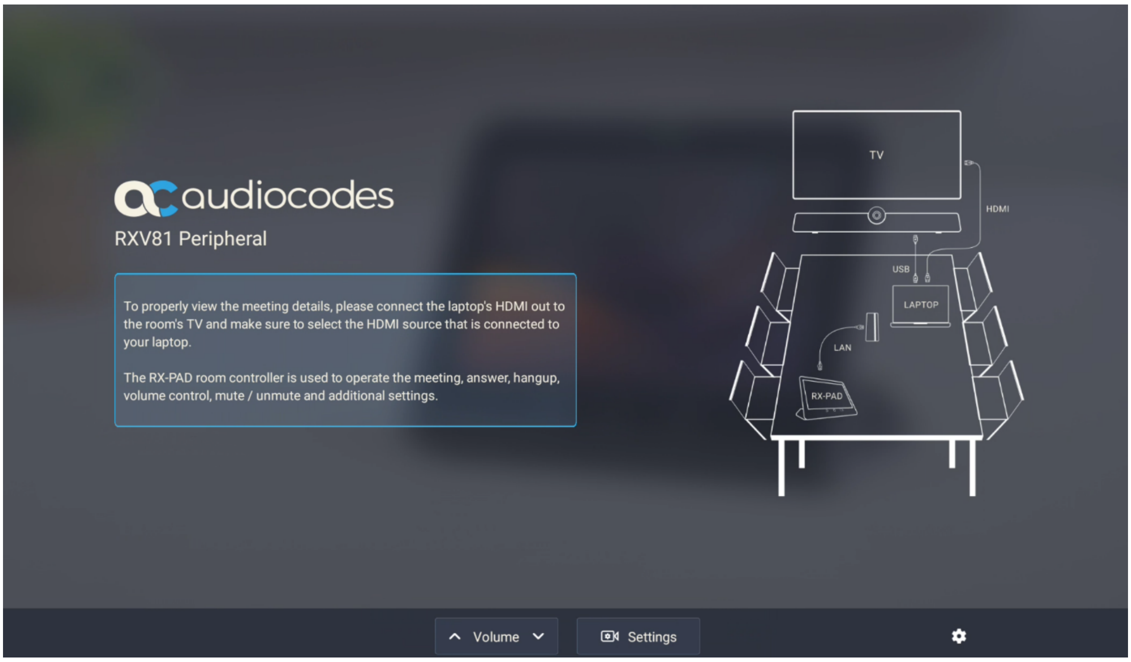
During a video call or meeting, when using the device with the ad hoc USB A/V peripheral , the RCU can be used to:

- Control the volume
- Mute the mic
- Turn the camera on or off

See the RXV81 MTR on Android Video Collaboration Bar with RX-PAD or RCU Quick Guide for detailed information on cabling RXV81.

➢ To use RXV81 in ad hoc peripheral mode:

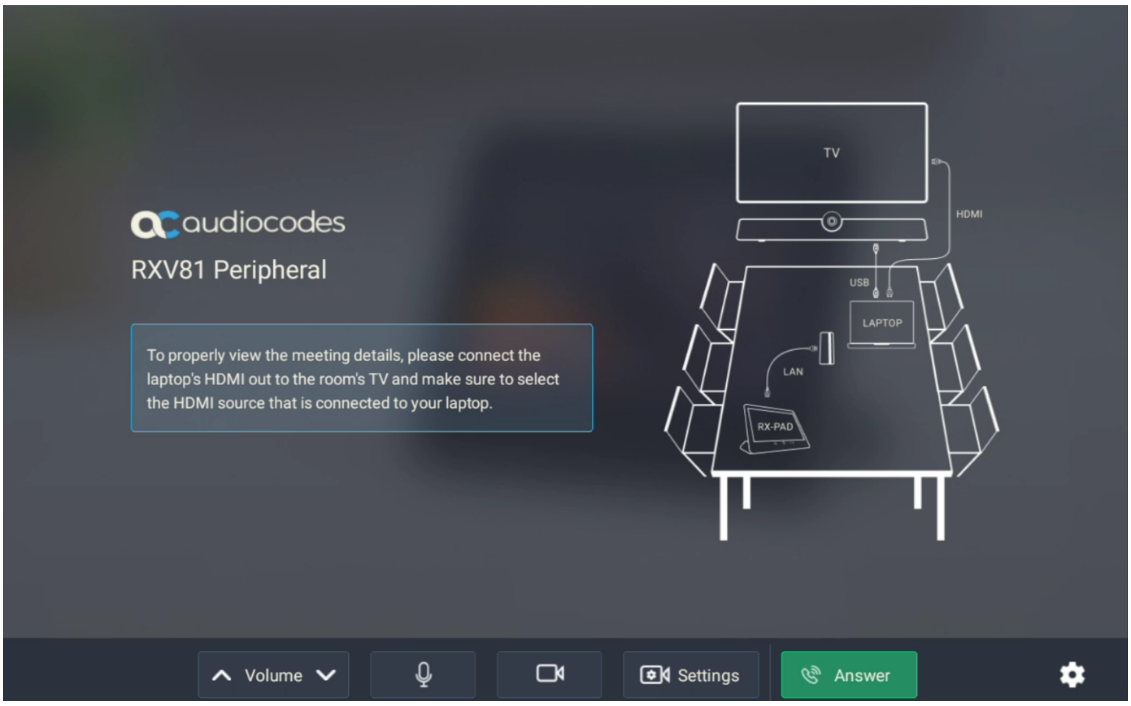
1. Connect the device’s USB Type C port to a PC or laptop running a UC client; the device automatically moves to ad hoc peripheral mode, and the RX-PAD displays the following:



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.

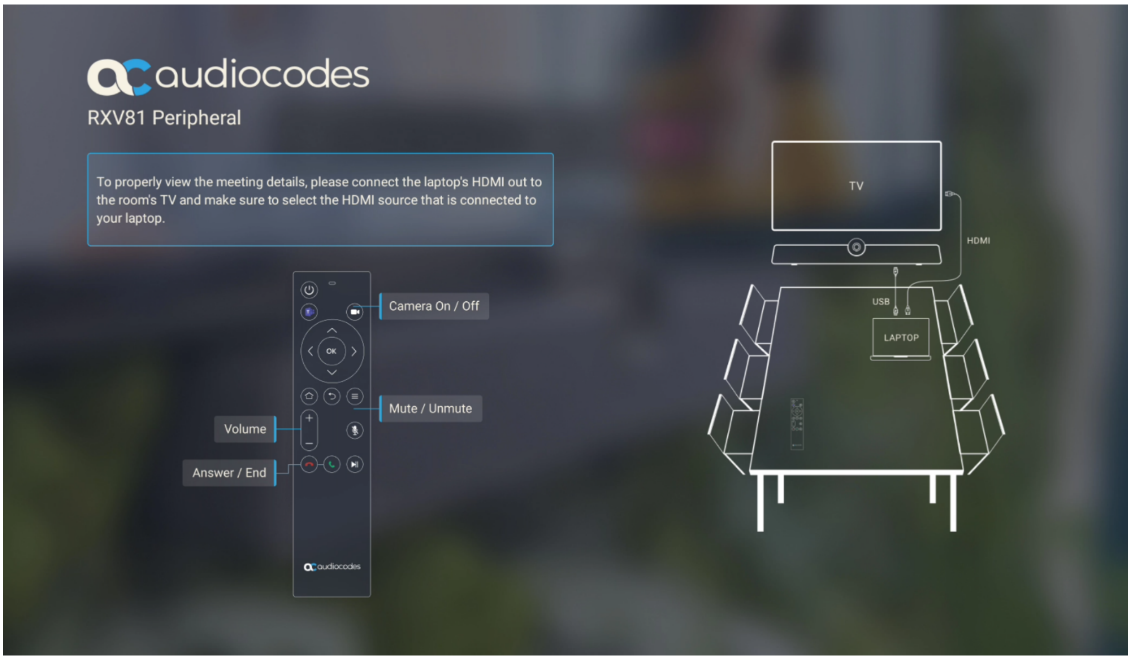
The RX-PAD room controller is used to operate the meeting, answer, hangup, volume control, mute / unmute and additional settings.

2. When a call comes in, view the incoming call’s functions on the RX-PAD, for example, ANSWER, as shown in the following figure.


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. View the ad hoc peripheral mode displayed on RXV81 bundled with the Remote Controller Unit (RCU) as shown in the following figure.


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.

When the device is in ad hoc peripheral mode, it automatically detects the mode when the user connects a USB cable from their BYOD compute, and pops up this message to the user:

> In addition to the USB cable already connected to your laptop, please connect your laptop to the TV using the HDMI cable to properly view meeting details and content sharing.
>
> On your TV, make sure to select the HDMI source that is connected to your laptop.

> Note that you can still use your RXV81 RCU to increase or decrease volume, mute or unmute audio, and switch the camera on or off.

In peripheral mode, the BYOD displays meeting video and content. Meetings actions (join, accept, manage participants) are controlled via the BYOD. Audio/video functions can be controlled via the UC client (camera ePTZ, mic mute) or the RCU (camera on/off, mute, volume).

4 MTRA Camera Settings

You can set up camera settings on the fly during a meeting or use presets to temporarily or permanently configure a combination of settings.

A camera Preset or View contains settings related to the camera or cameras connected to your RXV81 unit. These settings influence the look and feel of conducted meetings and consist of the following:

- Pan-Tilt-Zoom (PTZ) or simple zoom, depending on the camera
- Brightness, contrast, and saturation of colors
- Tracking mode

Temporary and Permanent Settings

➢ Presets

Presets exist only with MTRA bundles that include an RX-PAD. These MTRAs come with an initial preset called “Room”, the preset values being pre-configured depending on the applicable bundle.

- During meetings, any participating user can change the default preset or create or modify presets. If the user has Admin permissions, the changes are permanently saved and remain even after the meeting, while changes made by regular users are temporary and automatically discharged at the end of the meeting.
- When the device is in idle mode, Admins can permanently change preset values or generate additional **permanent** presets. These presets are saved and can be edited as needed. During meetings, they can be selected, thus eliminating the need for re-adjustment during each meeting.

⚠ Admins can create presets when the device is in idle mode (and the presets will be saved). Users cannot.

For more details, see Managing Camera Presets on the next page.

➢ Views

MTRA bundles without RX-PAD do not support presets. Instead, users can modify camera settings and save the current settings in a new view, or override an existing view. An initial view called "Room" is pre-configured with values depending on the applicable bundle. Changes made on views are permanent.

For more details, see Managing Views for RXV81 MTRAs without RX-PAD on page 27.

➢ Camera Settings

Camera Settings can be changed during a meeting without turning off the video to remote parties. They can also be optionally accessed via the Device Settings, though Admin login is necessary (see Access Device Admin Settings on page 37).

> The following sections focus on how to set up camera settings using a paired RX-PAD. If your MTRA bundle uses a touch screen or Remote Controller (RCU) instead, see Configuring Camera Settings for Systems Using Remote Controller.

Managing Camera Presets

> This section is only relevant for MTRA bundles that include an RX-PAD.

You can adjust the default Room preset or create presets to suit your preferences:

- Temporary Presets below
- Permanent Presets on page 26

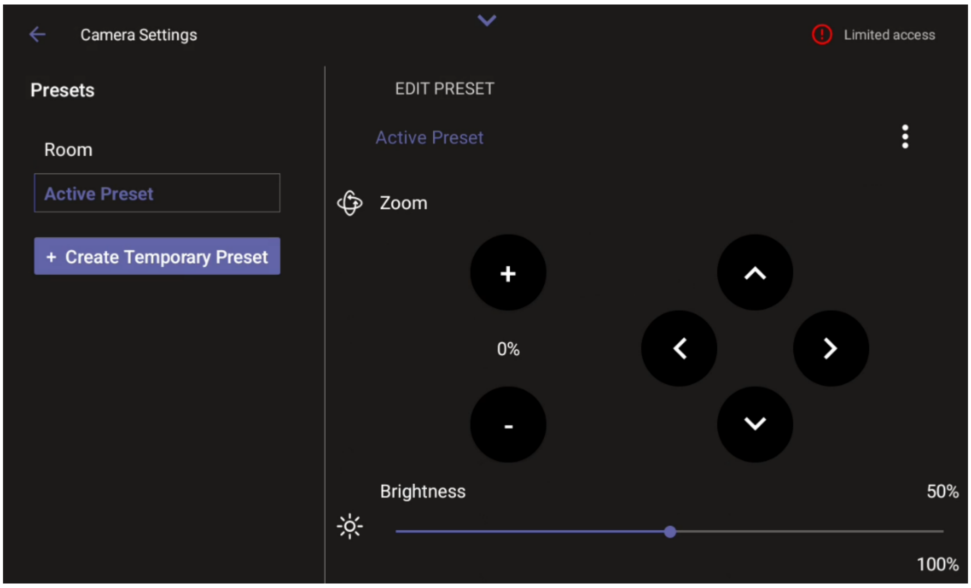
> It is recommended to have permanent presets configured for locations frequently zoomed in and focused on, such as:
>
> - Full room view to capture all participants and action in a meeting room
> - Presenter or single user / desk view to focus on a single user in the room, usually the presenter
> - Whiteboard view if there's a whiteboard in the room
> - Sunlight or dark modes if direct sunlight enters the room at specific times of the day/year

Temporary Presets

> This section is only relevant for MTRA bundles that include an RX-PAD.

➢ To temporarily adjust the Room preset or create a temporary preset during a meeting:

1. Do either of the following on the RX-PAD to access th Camera Settings page:
   - Press the camera button below the screen.
   - Tap the Down arrow on the top of the screen ⌄, then tap **Camera Settings**.



⚠ The default ‘Room’ preset enables you to capture all participants and actions in a meeting room.

2. While in an ongoing meeting, tap the **Create Temporary Preset** button.

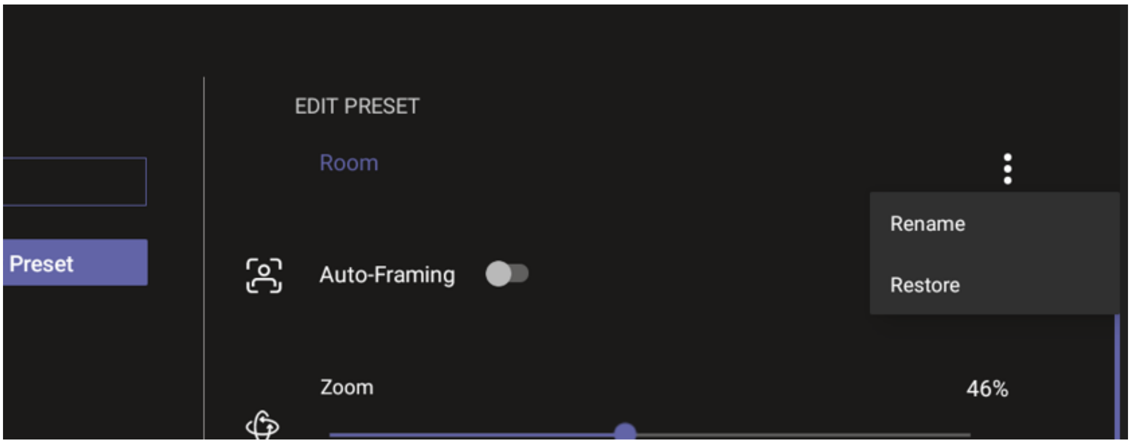
⚠ If the user has Admin permissions, the button is labeled **Create New Preset**. In this case, the generated preset will be permanent.

3. Configure the settings you want.

⚠
- If you configure a preset (for example) to zoom in and focus on a whiteboard in the meeting room, users in a video call-meeting can switch to it and later switch back to the default ‘Room’ preset or any other defined preset.
- Users can easily toggle between presets according to their requirements per call.

4. [Optionally] Edit a preset.

5. [Optionally] To return camera settings to their defaults, tap the vertical ellipsis and then from the pop-up menu select the **Restore** option.



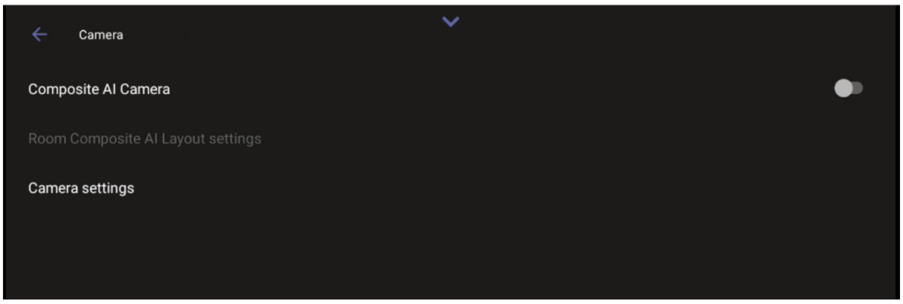
⚠ Camera settings can be changed during a meeting without turning off the video to remote parties.

Permanent Presets

⚠ This section is only relevant for MTRA bundles that include an RX-PAD.

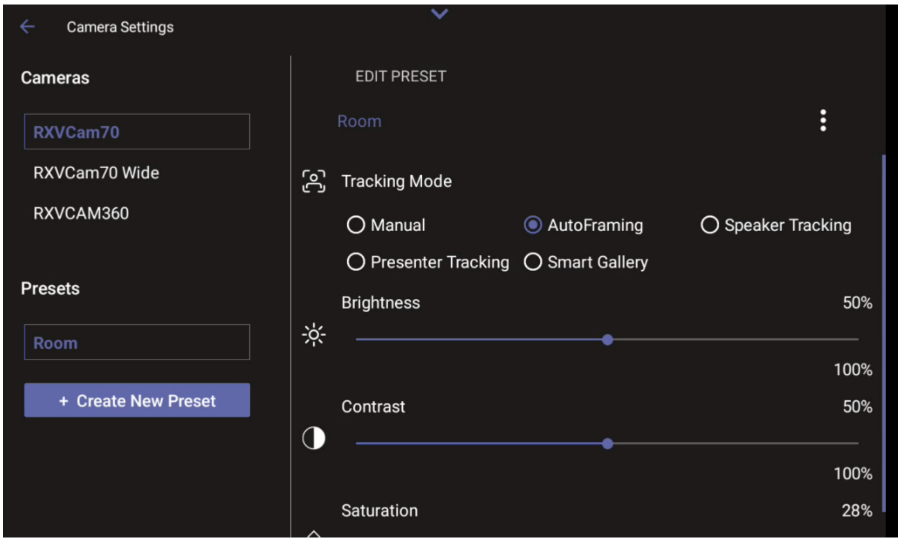
In idle mode, Admins can create new permanent presets and permanently change existing presets:

1. On the RX-PAD, touch the camera hard key below the screen.
2. Log in as administrator if prompted (see Access Device Admin Settings on page 37).
3. Tap **Camera settings**.



⚠ To define presets, Composite AI Camera must be disabled.

4. Edit the ‘Room’ preset or create a new preset. Changes are automatically saved.



Camera Settings

Cameras

RXVCam70

RXVCam70 Wide

RXVCAM360

Presets

Room

EDIT PRESET

Room

Tracking Mode

○ Manual ● AutoFraming ○ Speaker Tracking

○ Presenter Tracking ○ Smart Gallery

Brightness 50%

100%

Contrast 50%

100%

Saturation 28%

5. [Optionally] Tap the vertical ellipsis and then from the pop-up menu select the **Rename** option to change the name of the preset.

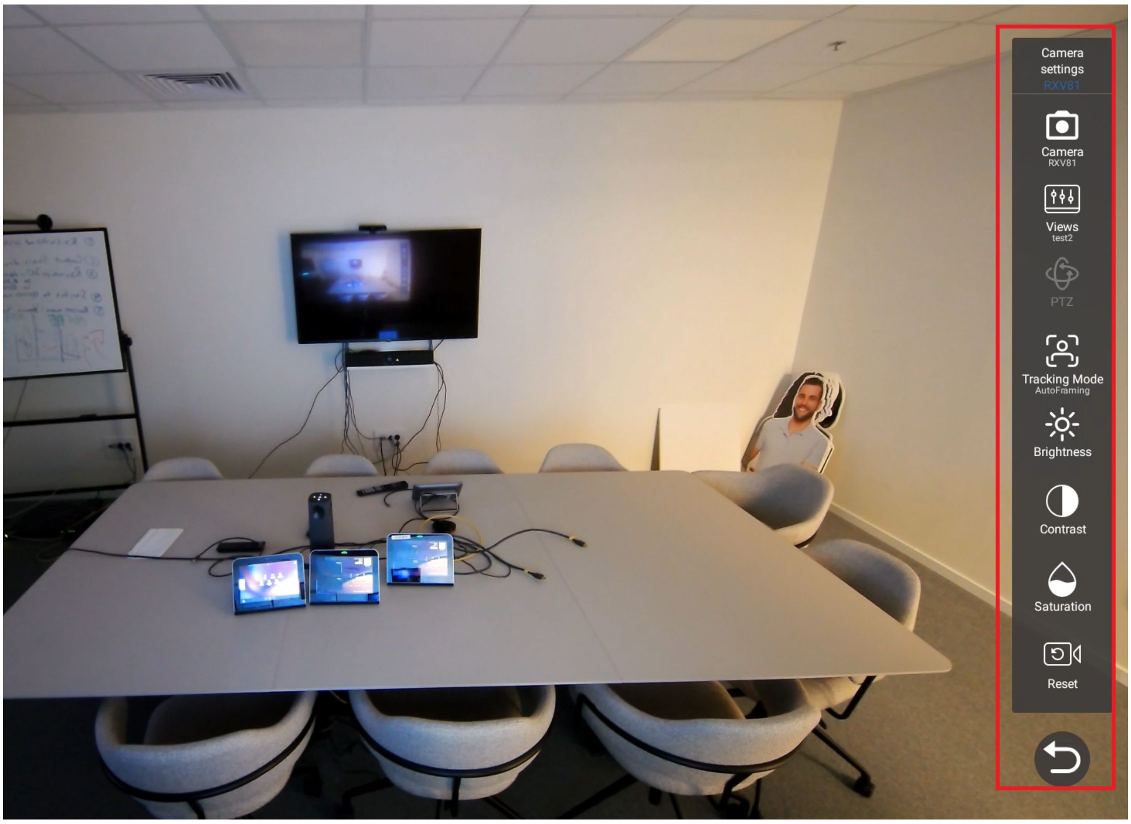
6. [Optionally] Tap the vertical ellipsis and then from the pop-up menu select the **Restore** option to return camera settings to their defaults.

Managing Views for RXV81 MTRAs without RX-PAD

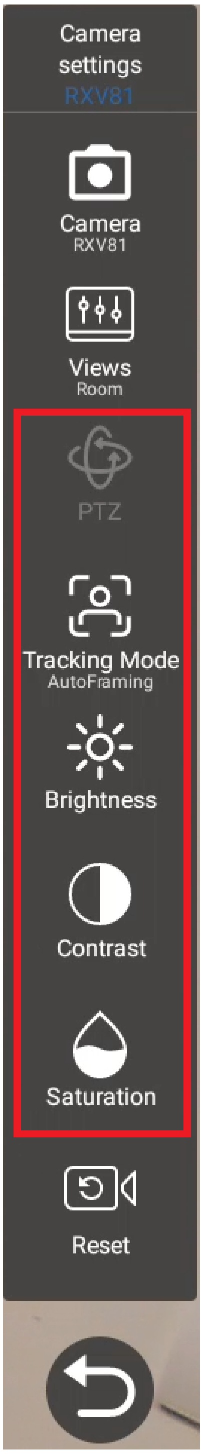
Systems that do not include an RX-PAD do not support presets. Instead, users can create or modify permanent views via the MTRA UI. To do this:

1. On the RCU, long-press the camera icon ■.

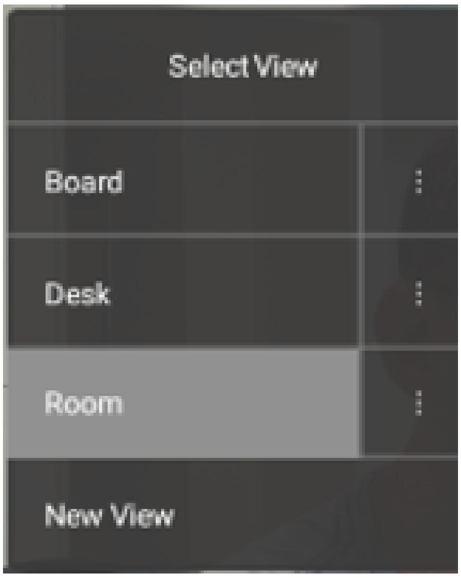
2. The camera output is displayed, with a vertical toolbar in front of it:



3. Change camera settings as required using the options on the vertical toolbar. Pan, Tilt, and Zoom (PTZ) can only be modified if 'Tracking Mode' is **Manual**.



4. Tap the **Views** option on the toolbar. A list of existing views (presets) is displayed.



Select View

Board

Desk

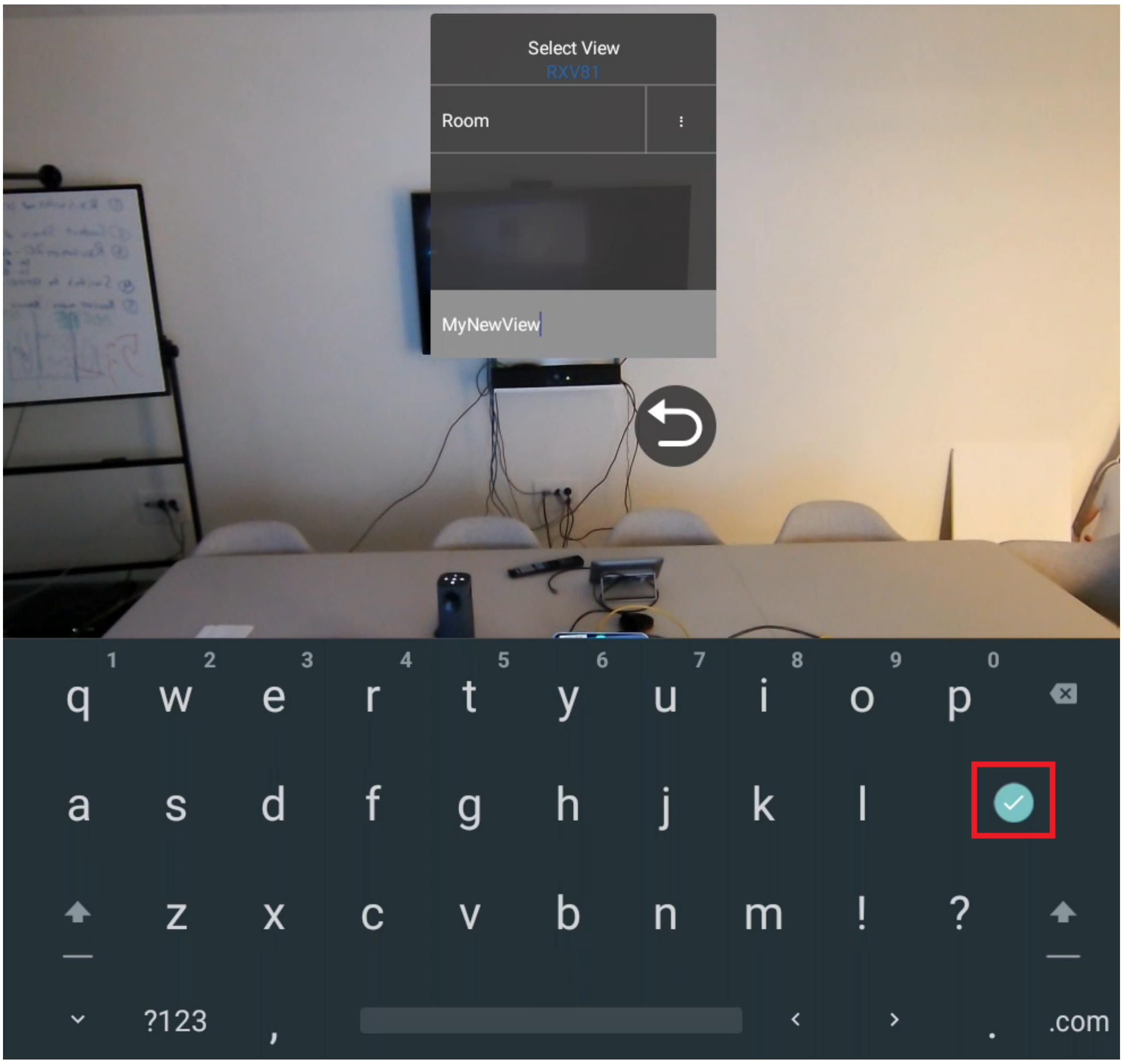
Room

New View

In the 'Select View' list, only the default (i.e., Room) view and up to two additional views are visible. If there are more views, you need to scroll down to see them.

5. Do either of the following:

- To update an existing view with the current camera settings, tap that view.
- To create a new view with the current camera settings, tap **New View**, type a name, and then tap the checkmark key on the virtual keyboard.

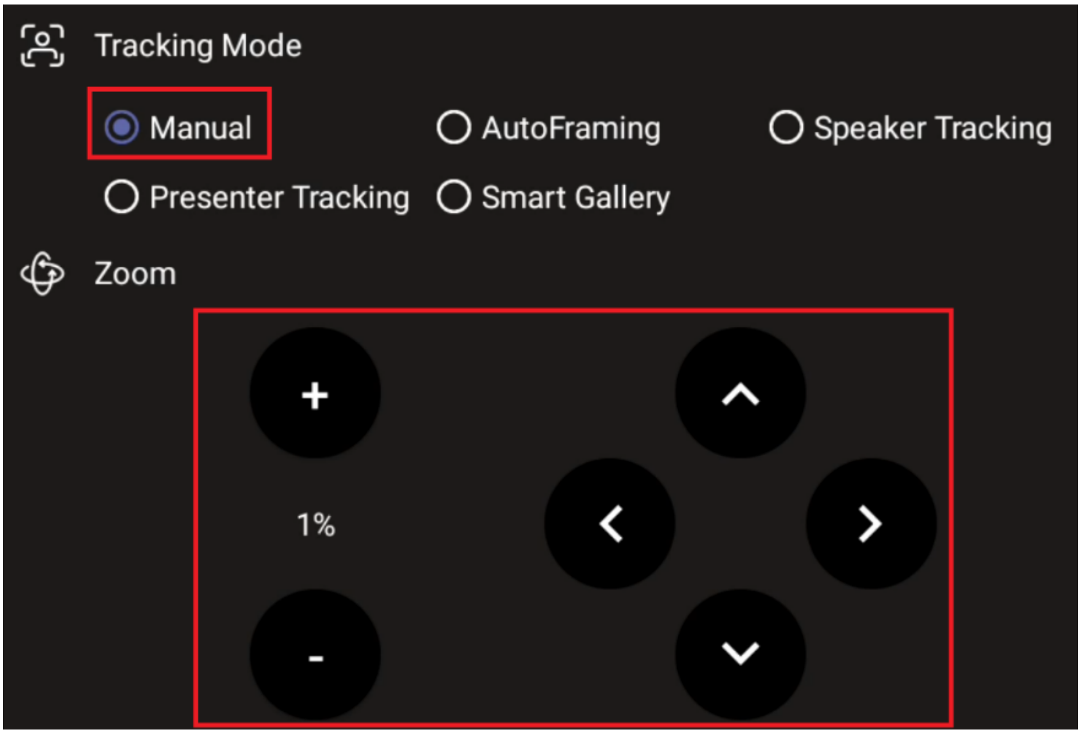


6. To rename or delete a view, tap the vertical ellipsis to the right of its name, and then from the pop-up menu tap the **Rename** or **Delete** option.

Set up Camera Zoom and Color Properties

➢ Zoom

To manually set a camera’s zoom-in and PTZ, set its Tracking Mode to **Manual**. Use the **+** and **-** signs to zoom in and out, and the arrows to set its PTZ.



Tracking Mode

● Manual ○ AutoFraming ○ Speaker Tracking

○ Presenter Tracking ○ Smart Gallery

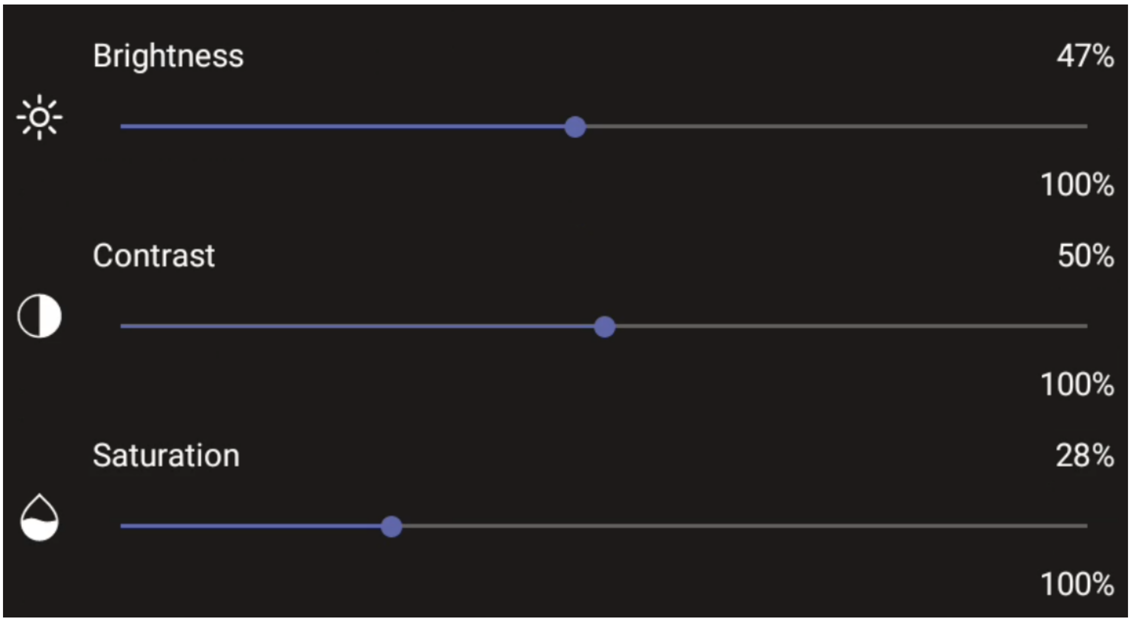
Zoom

1%

- If a Tracking Mode other than Manual is selected, the camera zoom is handled by the MTRA.
- Manual zoom setup is not possible in Composite AI mode.

➢ Color Properties

Each connected camera comes with default Brightness, Contrast, and Saturation properties. You can adjust them as required.



Brightness 47%

100%

Contrast 50%

100%

Saturation 28%

100%

5 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:

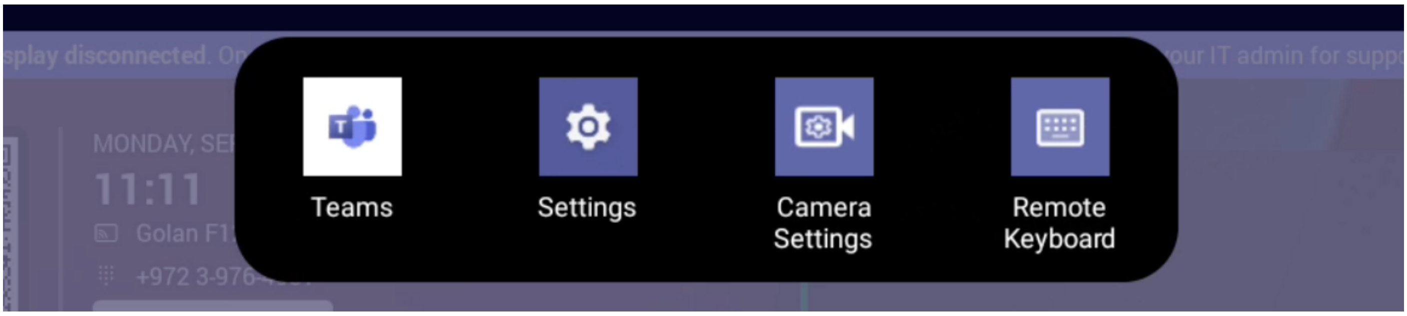
- Adjust the Volume on the next page
- Configure Accessibility Settings on page 35
- View RXV81 Information on page 35
- View Microsoft Teams Information on page 35
- Reboot the Device on page 36

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

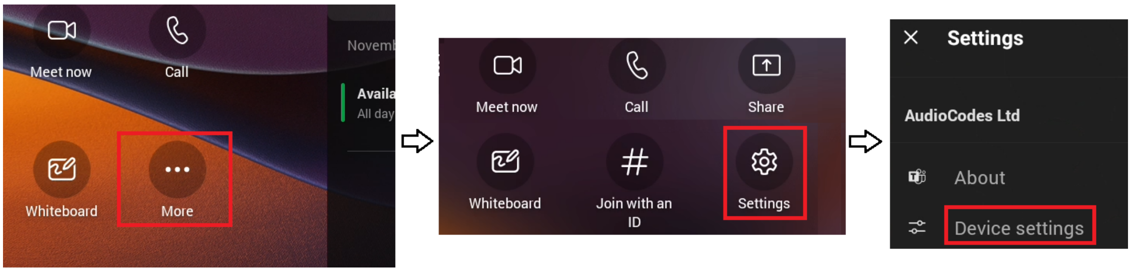
Access User Settings

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

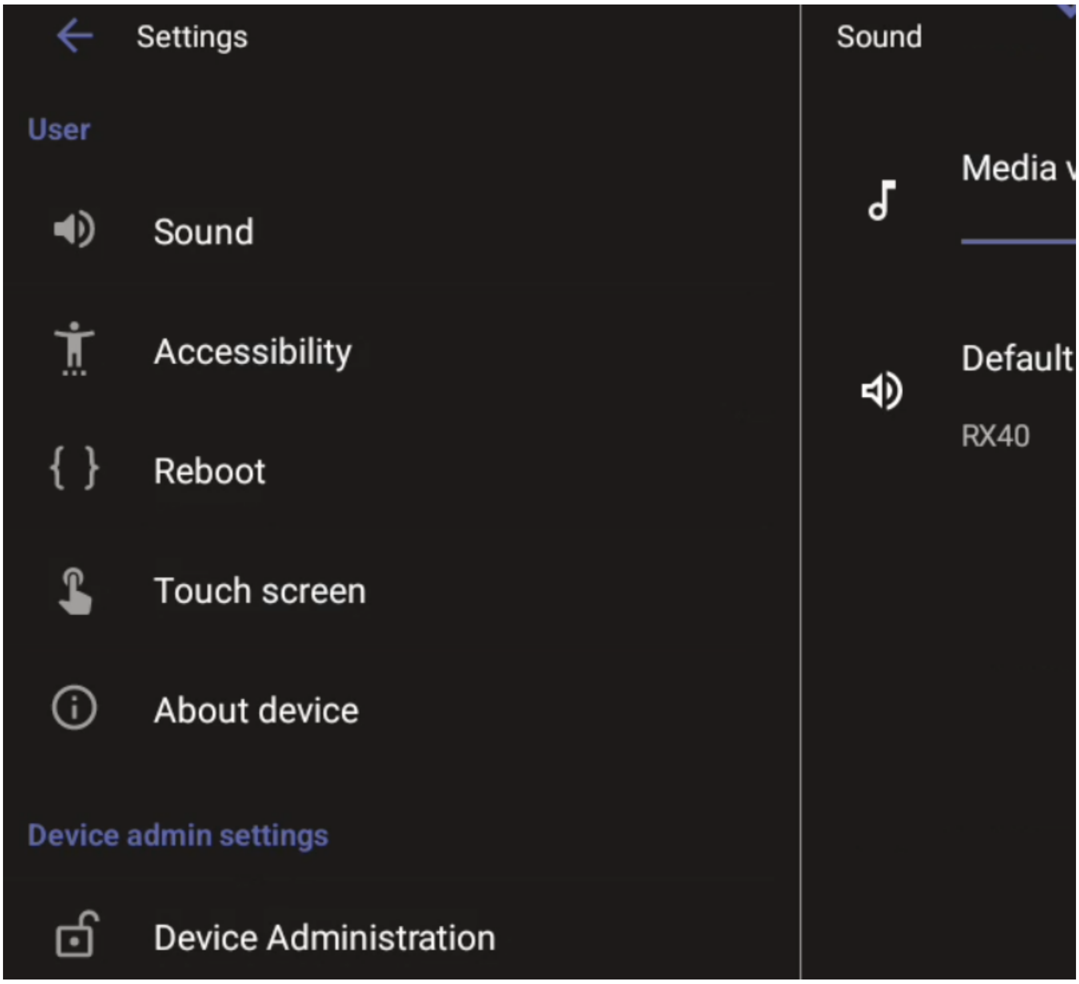
- Swipe down to display the main menu tray, then tap **Settings**.



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



Any user can configure User settings:

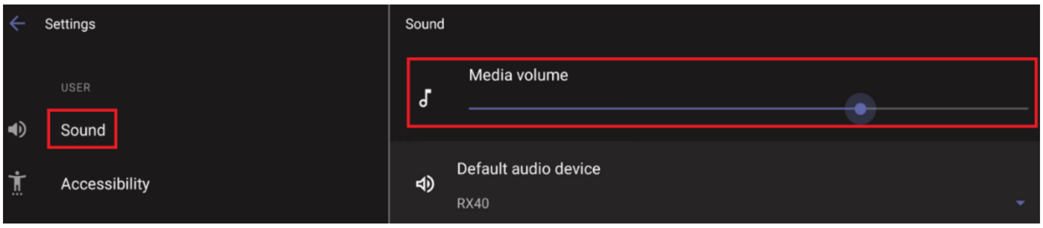


Viewing and configuring Device Admin settings requires Admin login. For details, see Admin Settings on page 37.

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 33).
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 RXV81 Information

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

➢ To access the About page:

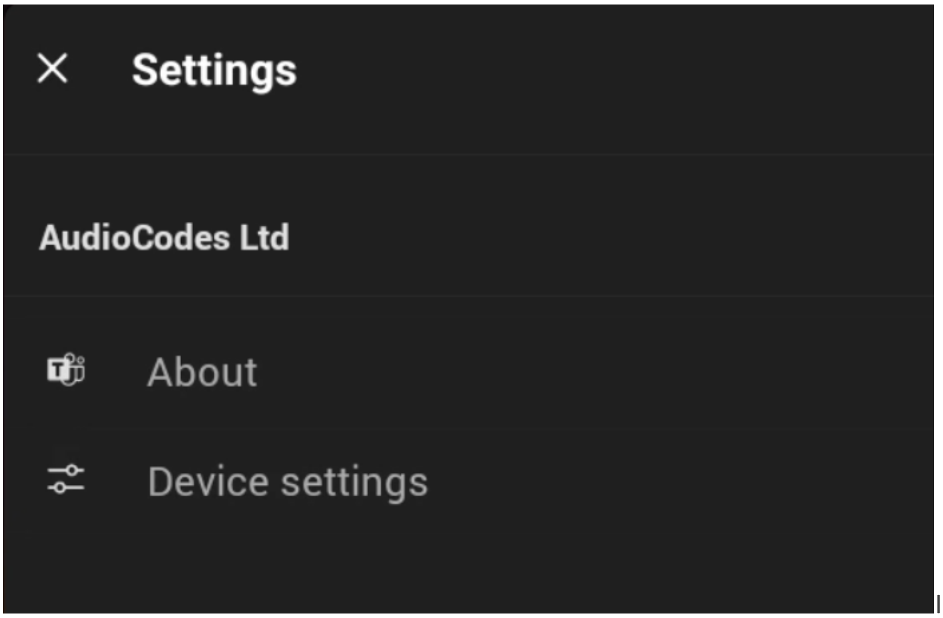
1. Navigate to ‘Settings’ (see Access User Settings on page 33).
2. Under ‘User’, tap **About device**.

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

View Microsoft Teams Information

➢ To view the About Microsoft Teams from the RX-PAD:

1. On the homepage, tap **More**, then tap **Settings**.
2. Press the **About** option.



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 33).
2. Under ‘User’, tap **Reboot**.
3. Tap **Reboot**.
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 69.

6 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 or during initial configuration (see Setting Up the Paired MTRA RXV200 RXV81 using the Initial Configuration Wizard). Admins can view or modify them to suit their enterprise requirements.

- Select the Default Audio Device on page 41
- Configure the Display on page 41
- Set Date and Time on page 41
- Configure Wi-Fi on page 42
- Configure Power Saving on page 46
- Configure UI Language and Input on page 47
- Reconfigure a Bundle on page 47
- Pair RX-PAD with Different MTRA on page 47
- Access the Camera from Admin Settings on page 49
- Modify IP Network Settings on page 49
- Customize the Background on page 53
- Configure Camera Settings with RX-PAD Teams Admin on page 53
- Enroll a Device with Intune Policies on page 54
- Enroll Certificates using SCEP on page 56
- Provision Certificates in .pfx Format on page 58
- Enable Display of Meeting Name using Exchange Online PowerShell on page 58
- Update RXV81 Remotely on page 59

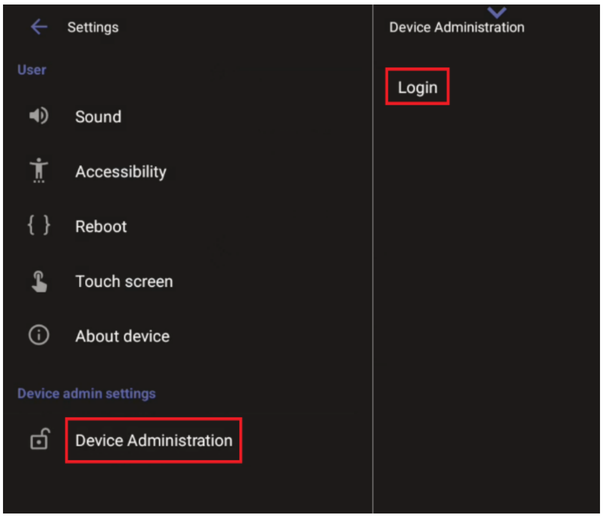
Access Device Admin Settings

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

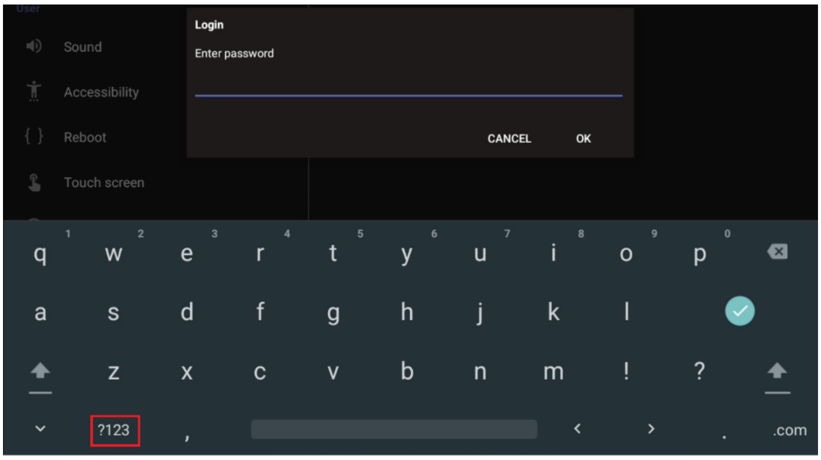
Log in to Device Administration

➢ **To log into Device Administration:**

1. Navigate to the 'Settings' page (see Access User Settings on page 33).
2. Under ‘Device Admin Settings’, tap **Device Administration**, then tap **Login**.



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



⚠ 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:

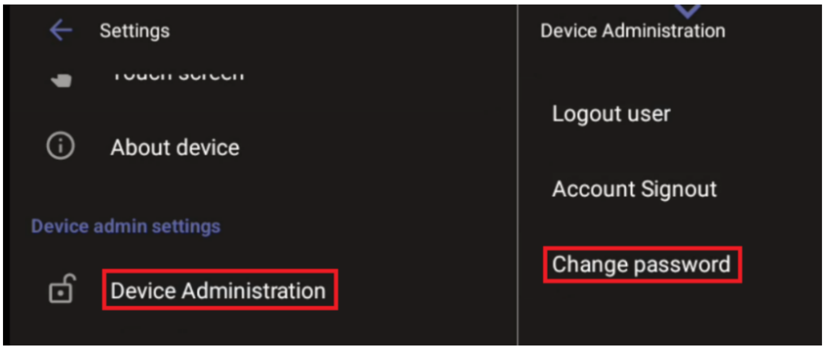
- The password length must be greater than or equal to 8.
- The password must contain one or more uppercase characters.
- The password must contain one or more lowercase characters.
- The password must contain one or more numeric values.
- The password must contain one or more special characters.

> - 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 37).
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 RXV81 (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 RXV81 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 33).
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 37).
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 37).
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:
  - Teams Admin Center, created under configuration profile.
  - 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.

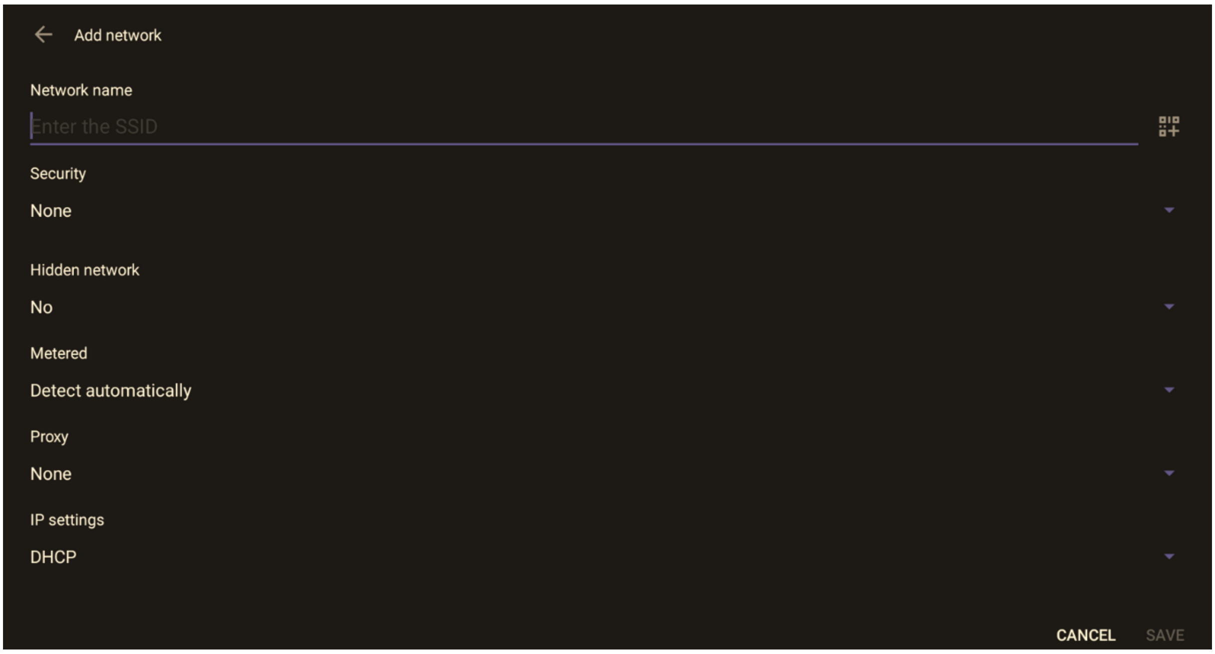
➢ To connect to an available Wi-Fi network:

1. If not already logged in, log in to Device Administration to get admin access (see Log in to Device Administration on page 37).
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 37).
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 45.
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 6-1: Configuration File Wi-Fi Parameters

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

Parameter	Description
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.
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 43).

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 37).
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 37).
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.

Reconfigure a Bundle

Admins can reconfigure a bundle if there has been a change in the MTRA's configuration, for example, if the MTRA peripherals have changed, or to switch a RXV81 from MTR stand-alone mode to peripheral mode and back.

- Switching bundles causes a factory reset.
- See Bundles on page 3 for more information about available bundles.

➢ To reconfigure a bundle:

1. If not already logged in, log in to Device Administration to get admin access (see Log in to Device Administration on page 37).
2. Under 'Device admin settings', scroll down and tap **Bundle**.
3. Select the relevant bundle.

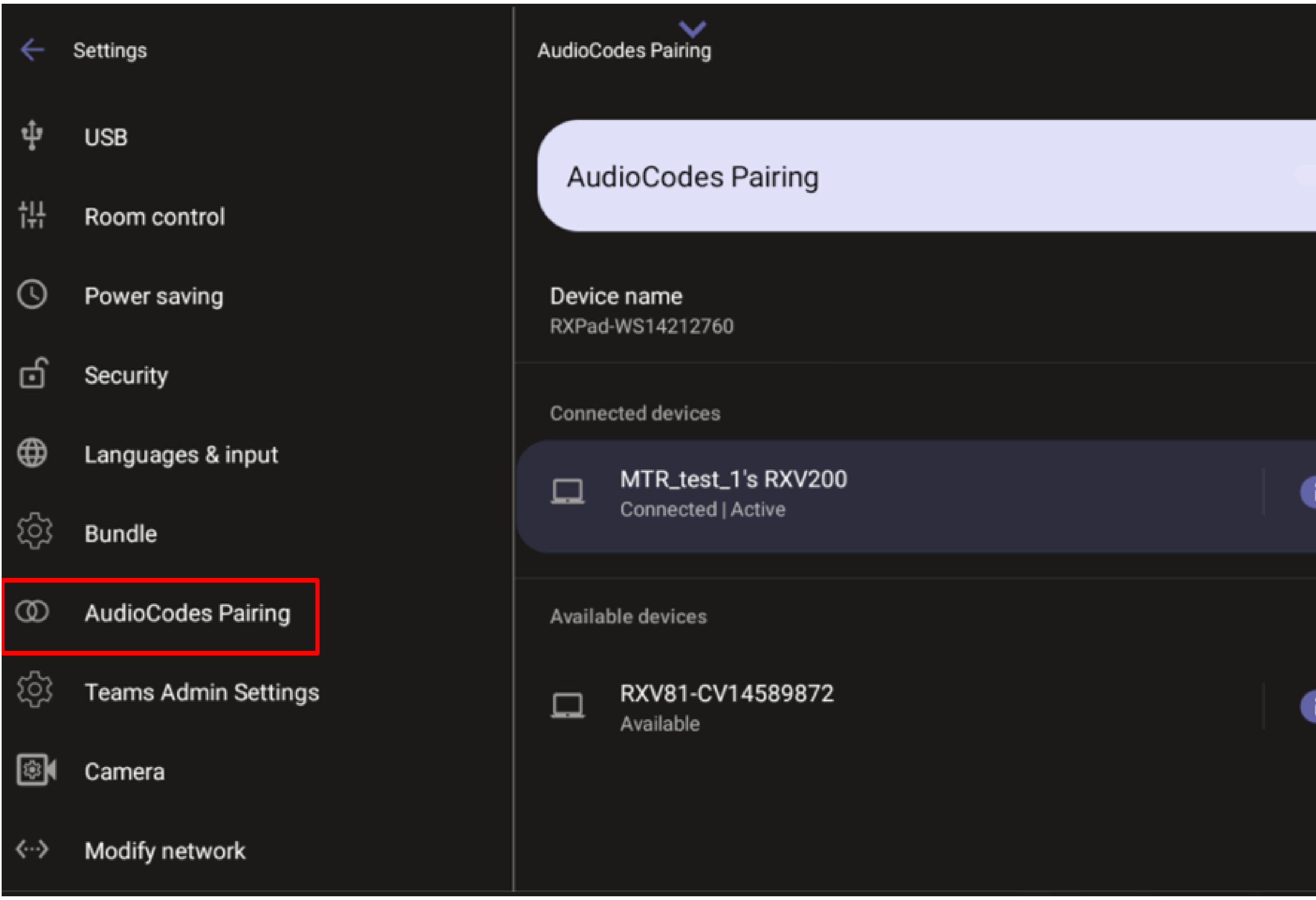
Pair RX-PAD with Different MTRA

You can control your paired MTRA devices with the current RX-PAD and decide which MTRA you wish to pair or unpair with on a current connection.

⚠ Teams unpairing must occur prior to pairing with a new MTRA device.

➢ To pair a device:

1. If not already logged in, log in to Device Administration to get admin access (see Log in to Device Administration on page 37).
2. View details of the currently paired MTRA and other devices available for pairing:
   a. Under 'Device admin settings', scroll down and tap **AudioCodes Pairing**.



Device name
RXPad-WS14212760

Connected devices
MTR_test_1's RXV200
Connected | Active

Available devices
RXV81-CV14589872
Available

   b. Tap ⓘ to view the information of the paired device from the currently paired RX-PAD, for example, the IP address, device model, and MAC address:
3. Unpair the current device at the Teams level: Navigate to **Teams Admin Settings > Devices** menu to break the currently paired set.
4. After unpairing, return to **AudioCodes Pairing** and tap the MTRA you wish to pair with the RX-PAD.

Access the Camera from Admin Settings

Administrators can access camera settings via the Settings page:

1. Navigate to the 'Settings' page and log in as Admin (see Access Device Admin Settings on page 37).
2. Scroll down and tap the **Camera** option, then tap **Camera Settings**.

For details on configuring camera settings, see MTRA Camera Settings on page 23.

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 37).
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 52).

Set up a Proxy Server

Administrators can manually configure the RXV81 with an HTTP proxy server:

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

Configure 802.1x Settings

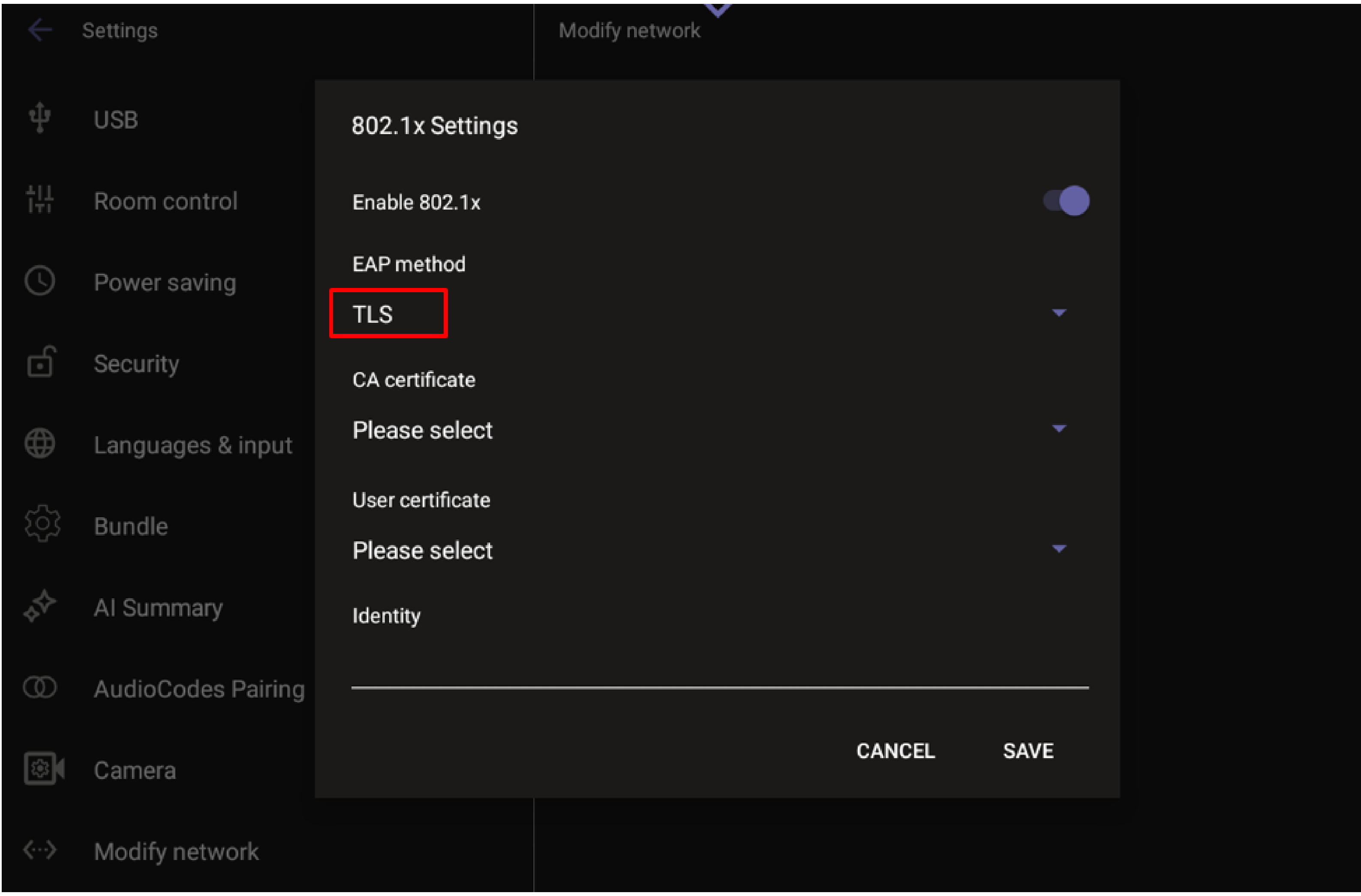
802.1x Authentication is the IEEE Standard for Port-based Network Access Control (PNAC) (refer to https://1.ieee802.org/security/802-1x/ for more information). It is used to enable port-based authentication.

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

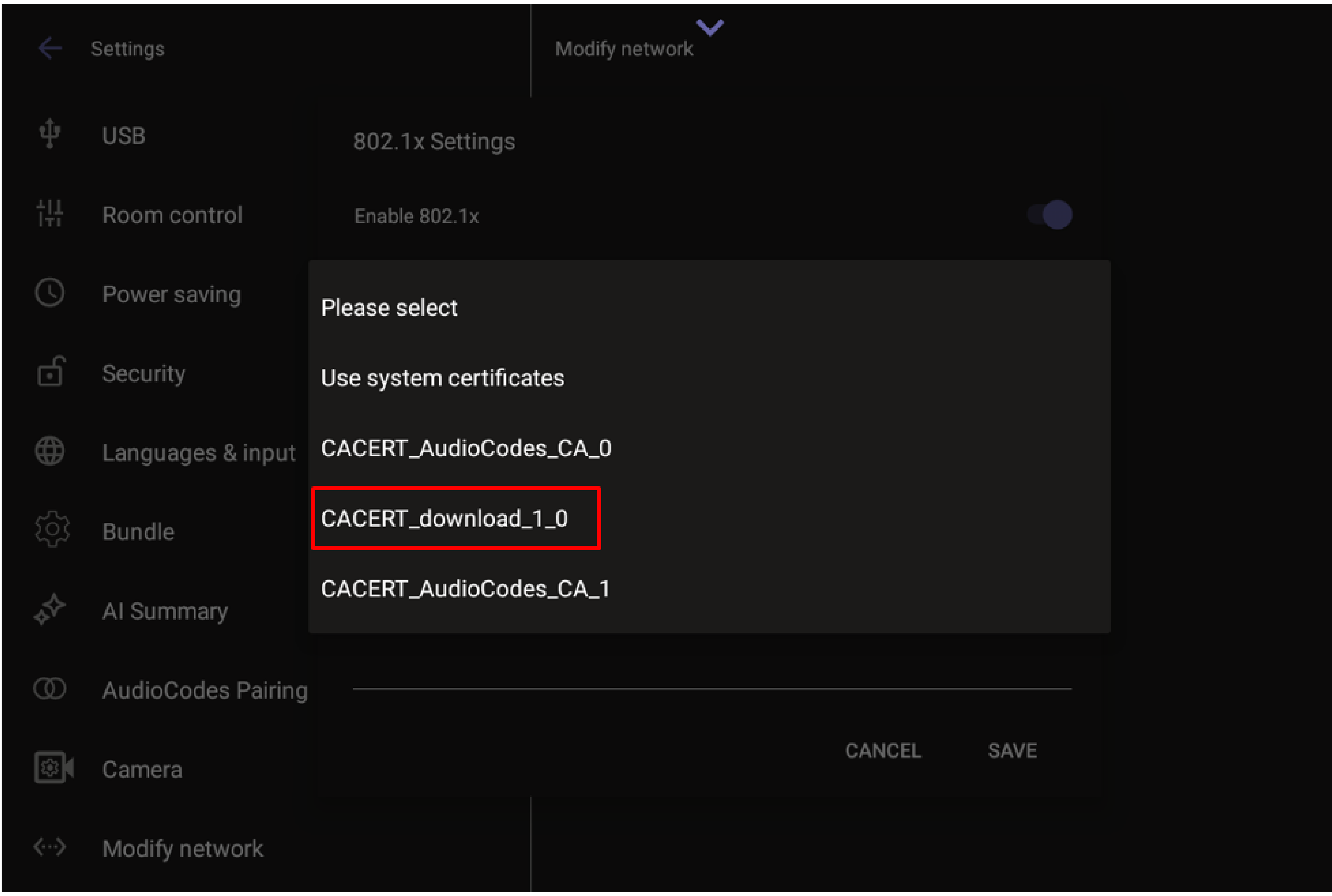
CA certificate
Please select

User certificate
Please select

Identity

CANCEL SAVE

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

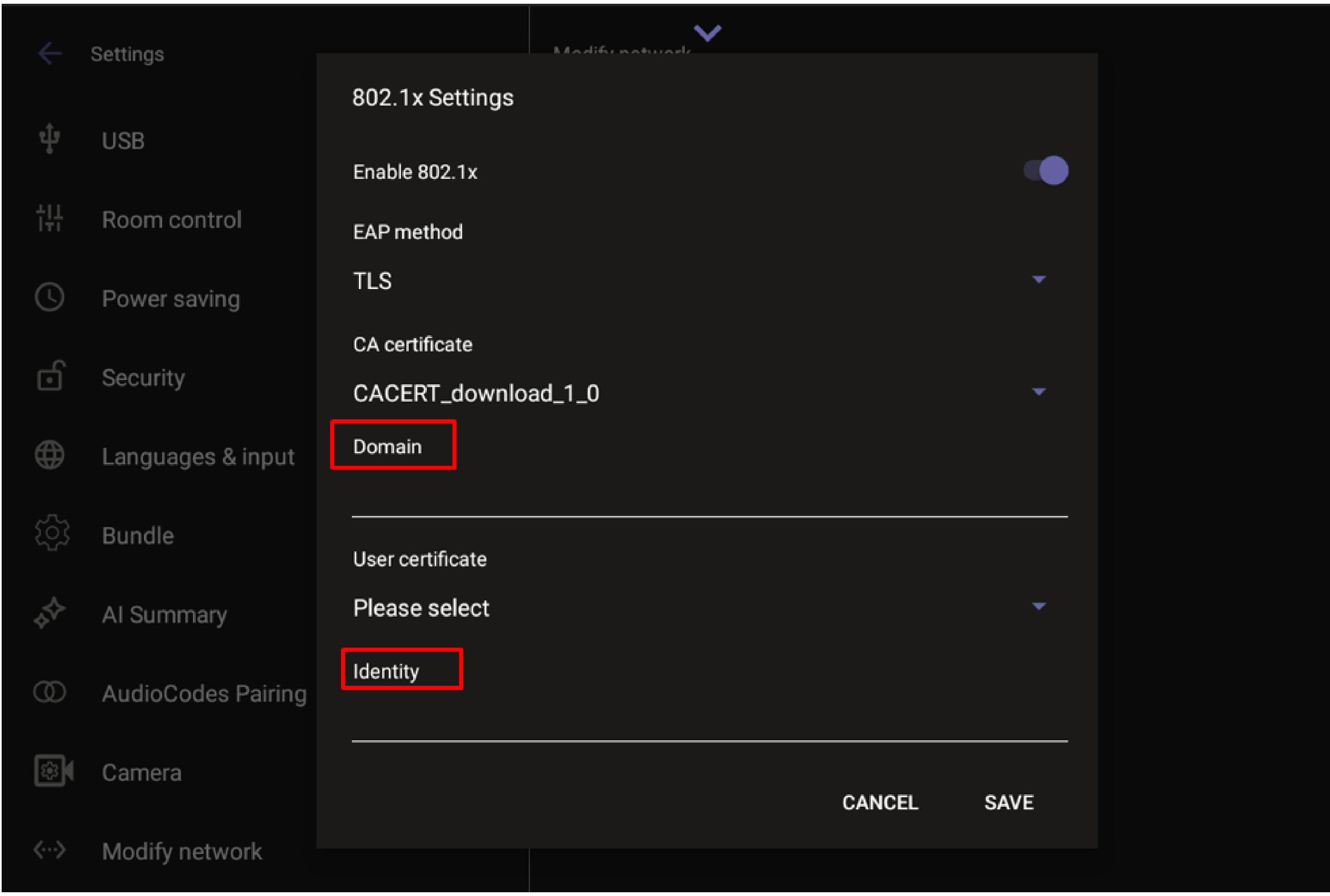
CACERT_AudioCodes_CA_0

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 49) 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**.

Customize the Background

> This feature is only available with the Teams Rooms Pro license.

Admin can upload custom background images on the Teams admin center to reinforce their company brand on their Teams Rooms on Android devices.

The main room display, extended room display, and touch console can each have their own specific background image.

PNG, JPG, and JPEG formats are supported.

See also the relevant Microsoft documentation for more information.

Configure Camera Settings with RX-PAD Teams Admin

AudioCodes camera settings, as reflected in the RX-PAD (or touch screen) UI, are synchronized with Microsoft Teams Room camera settings. This means that users can access them from the RX-PAD, instead of the Teams Admin Center (TAC).

➢ To adjust camera settings through Teams Admin:

1. If not already logged in, log in to Device Administration to get admin access (see Log in to Device Administration on page 37).
2. Under ‘Device admin settings’, scroll down and tap **Teams Admin Settings**.
3. Tap **Teams Admin Settings**, then tap **Devices**.

- To configure room settings for a camera, tap **Room Camera** and configure settings.
- To set up a camera for content sharing, tap **Content Camera**, select a camera, and configure it as required.

Content Camera Framing on a Whiteboard describes how to use the Content Camera option to share a whiteboard using an RXVCam10 camera.

Enroll a Device with Intune Policies

Admins can enroll AudioCodes Teams Android-based devices in Intune in either of the following ways:

- By Create a Dynamic Group below
- By Create an Exclusion Group below

An enrolled device can be removed from Intune (see Remove Devices from Intune Admin Center on the next page).

Create a Dynamic Group

See the AudioCodes Device Enrollment in Microsoft Endpoint Manager to learn how to create dynamic groups in Intune for enrolling AudioCodes Android- based Teams devices.

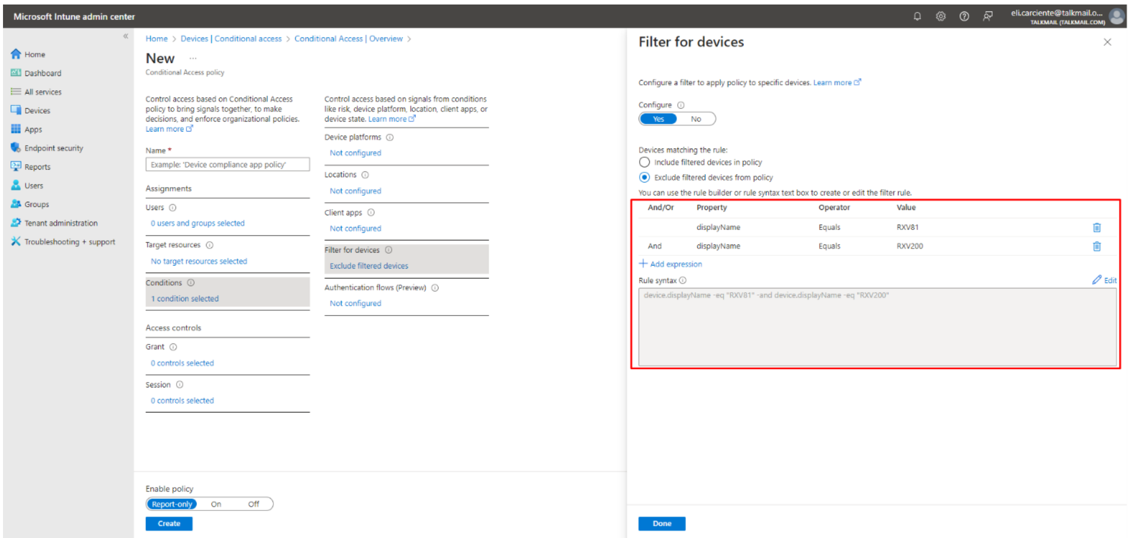
Create an Exclusion Group

The information presented here shows how to exclude AudioCodes Android- based Teams devices from the organization's Intune policies.

➢ To exclude devices from the organization's Intune policies:

Remove all conditions that were previously configured:

1. Access Microsoft Azure Government Portal Home > Conditional Access Policies > Require Hybrid Joined or Intune to Access Cloud Resources Conditional Access policy as shown in the following figure.
2. Exclude the device from Intune policies and replace **displayName -contains RXVxx** where RXVxx is the name of the device model (device.model).


Microsoft Intune admin center
eli.carciente@talkmail.o...
TALKMAIL (TALKMAIL.COM)
Home
Dashboard
All services
Devices
Apps
Endpoint security
Reports
Users
Groups
Tenant administration
Troubleshooting + support
Home > Devices | Conditional access > Conditional Access | Overview >
Create
Done

New ···
Conditional Access policy

Control access based on Conditional Access policy to bring signals together, to make decisions, and enforce organizational policies. Learn more

Name *
Example: 'Device compliance app policy'

Assignments
Users: 0 users and groups selected
Target resources: No target resources selected
Conditions: 1 condition selected

Access controls
Grant: 0 controls selected
Session: 0 controls selected

Control access based on signals from conditions like risk, device platform, location, client apps, or device state. Learn more

Device platforms: Not configured
Locations: Not configured
Client apps: Not configured
Filter for devices: Exclude filtered devices
Authentication flows (Preview): Not configured

Enable policy: [✓ Report-only] On Off

Filter for devices

Configure a filter to apply policy to specific devices. Learn more

Configure: [✓ Yes] No

Devices matching the rule:
○ Include filtered devices in policy
● Exclude filtered devices from policy

You can use the rule builder or rule syntax text box to create or edit the filter rule.

And/Or	Property	Operator	Value
	displayName	Equals	RXV81
And	displayName	Equals	RXV200

+ Add expression

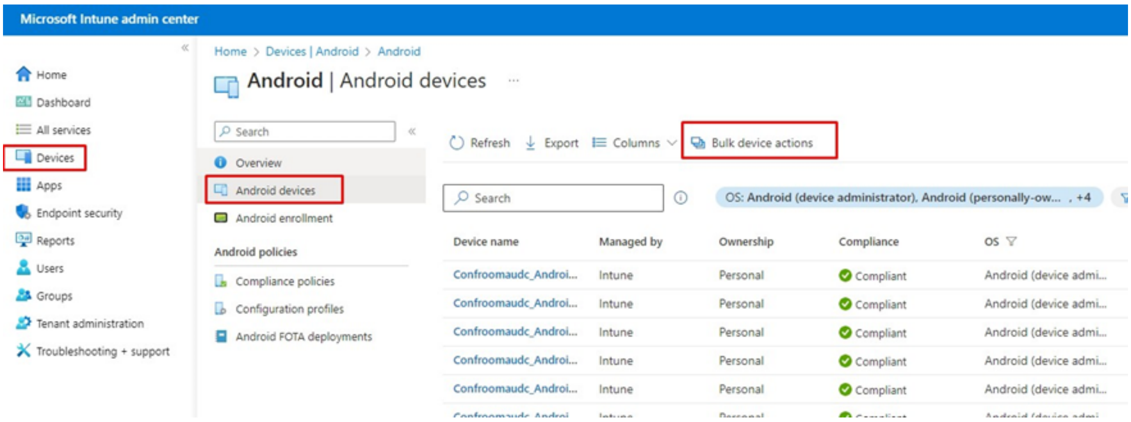
Rule syntax
```
device.displayName -eq "RXV81" -and device.displayName -eq "RXV200"
```

Remove Devices from Intune Admin Center

You can remove devices from Intune admin center when the maximum capacity of signed-in devices is reached.

➢ To remove devices from Intune admin center:

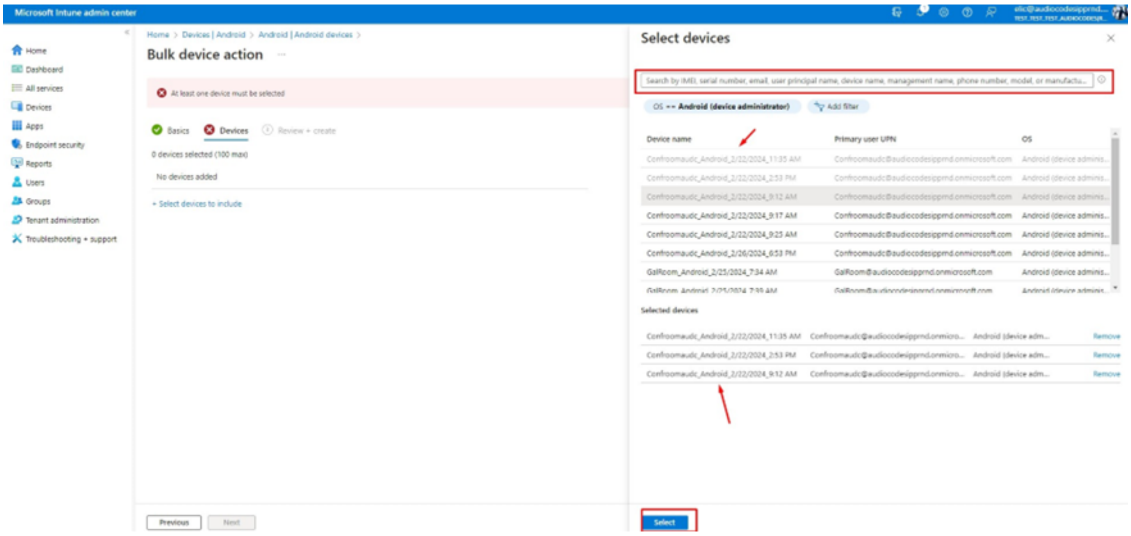
1. Go to Microsoft 365 admin center (portal.office.com) and log in with an Administration account.
2. Navigate to **Devices > Android devices**.



Device name	Managed by	Ownership	Compliance	OS
Confroomaudc_Androi...	Intune	Personal	✓ Compliant	Android (device admi...
Confroomaudc_Androi...	Intune	Personal	✓ Compliant	Android (device admi...
Confroomaudc_Androi...	Intune	Personal	✓ Compliant	Android (device admi...
Confroomaudc_Androi...	Intune	Personal	✓ Compliant	Android (device admi...
Confroomaudc_Androi...	Intune	Personal	✓ Compliant	Android (device admi...

The Intune admin center service is licensed according to the terms of individual licenses so not all network admins will be able to navigate to it. Check if the license you're using includes the service or not.

3. Click **Bulk device actions**.
4. From the 'OS' drop-down under the **Basics** tab, select **Android (device administrator)**. From the 'Device action' drop-down, select **Delete**. Click **Next**.



Microsoft Intune admin center
Home
Dashboard
All services
Devices
Apps
Endpoint security
Reports
Users
Groups
Tenant administration
Troubleshooting + support
Home > Devices | Android > Android | Android devices >
Bulk device action
Basics
Devices
Review + create
+ Select devices to include
Previous
Next
Select devices
Search by IMEI, serial number, email, user principal name, device name, management name, phone number, model, or manufactu...
OS == Android (device administrator)
Add filter
Select

At least one device must be selected

0 devices selected (100 max)

No devices added

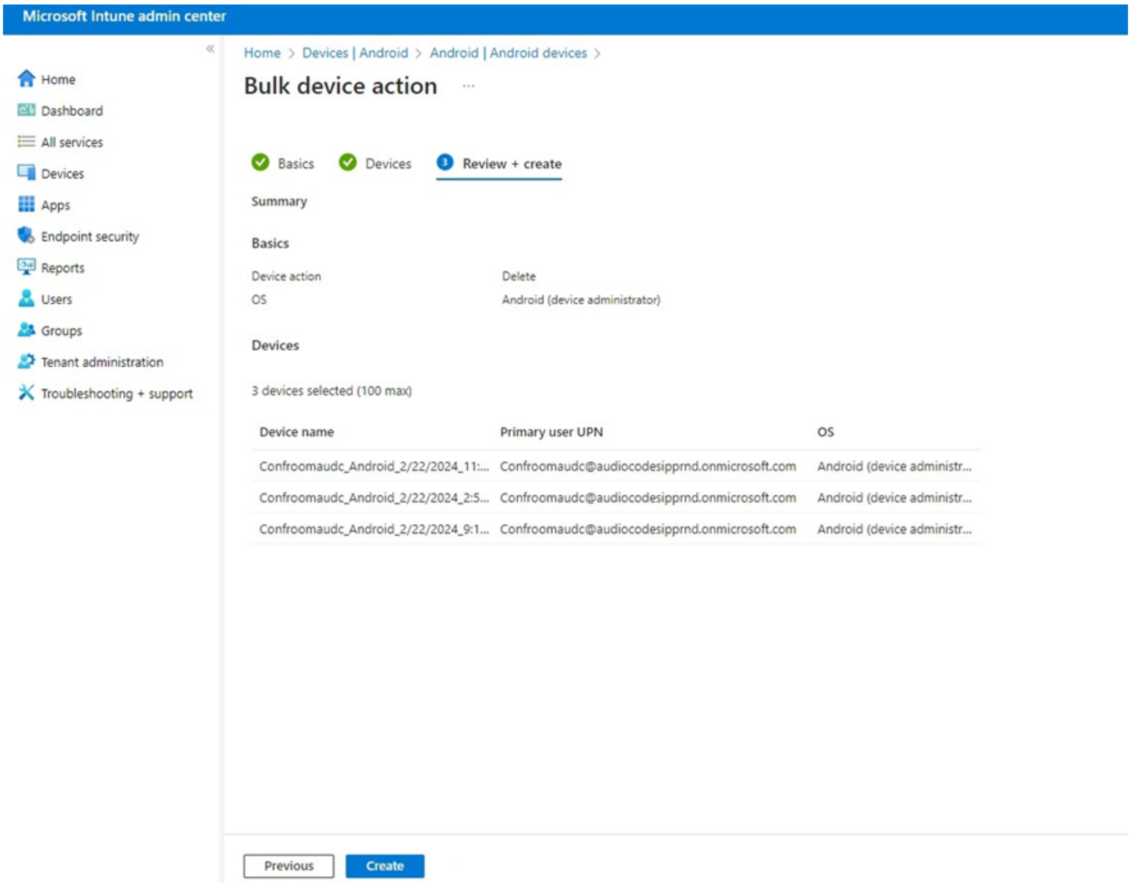
Device name	Primary user UPN	OS
Confroomaudc_Android_2/22/2024_11:35 AM	Confroomaudc@audiocodesipprnd.onmicrosoft.com	Android (device adminis...
Confroomaudc_Android_2/22/2024_2:53 PM	Confroomaudc@audiocodesipprnd.onmicrosoft.com	Android (device adminis...
Confroomaudc_Android_2/22/2024_9:12 AM	Confroomaudc@audiocodesipprnd.onmicrosoft.com	Android (device adminis...
Confroomaudc_Android_2/22/2024_9:17 AM	Confroomaudc@audiocodesipprnd.onmicrosoft.com	Android (device adminis...
Confroomaudc_Android_2/22/2024_9:25 AM	Confroomaudc@audiocodesipprnd.onmicrosoft.com	Android (device adminis...
Confroomaudc_Android_2/26/2024_6:53 PM	Confroomaudc@audiocodesipprnd.onmicrosoft.com	Android (device adminis...
GalRoom_Android_2/25/2024_7:34 AM	GalRoom@audiocodesipprnd.onmicrosoft.com	Android (device adminis...
GalRoom_Android_2/25/2024_7:39 AM	GalRoom@audiocodesipprnd.onmicrosoft.com	Android (device adminis...

Selected devices

Confroomaudc_Android_2/22/2024_11:35 AM	Confroomaudc@audiocodesipprnd.onmicro...	Android (device adm...	Remove
Confroomaudc_Android_2/22/2024_2:53 PM	Confroomaudc@audiocodesipprnd.onmicro...	Android (device adm...	Remove
Confroomaudc_Android_2/22/2024_9:12 AM	Confroomaudc@audiocodesipprnd.onmicro...	Android (device adm...	Remove

5. Select the devices to delete (i.e., to remove from Intune admin center), and then click **Select**.

6. Under the **Devices** tab, click **Next**.
7. Under the **Review + Create** tab, make sure your definitions are correct and then click **Create**.



Summary

Basics

Device action	Delete
OS	Android (device administrator)

Devices

3 devices selected (100 max)

Device name	Primary user UPN	OS
Confroomaudc_Android_2/22/2024_11:...	Confroomaudc@audiocodesipprnd.onmicrosoft.com	Android (device administr...
Confroomaudc_Android_2/22/2024_2:5...	Confroomaudc@audiocodesipprnd.onmicrosoft.com	Android (device administr...
Confroomaudc_Android_2/22/2024_9:1...	Confroomaudc@audiocodesipprnd.onmicrosoft.com	Android (device administr...

8. Admin receives a notification that a delete action from Intune was successfully initiated on all devices and that n devices were removed.

> ⚠ It may take some time to completely sync the devices with the account. After deleting the devices, wait for 30 minutes before signing in.

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` 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:

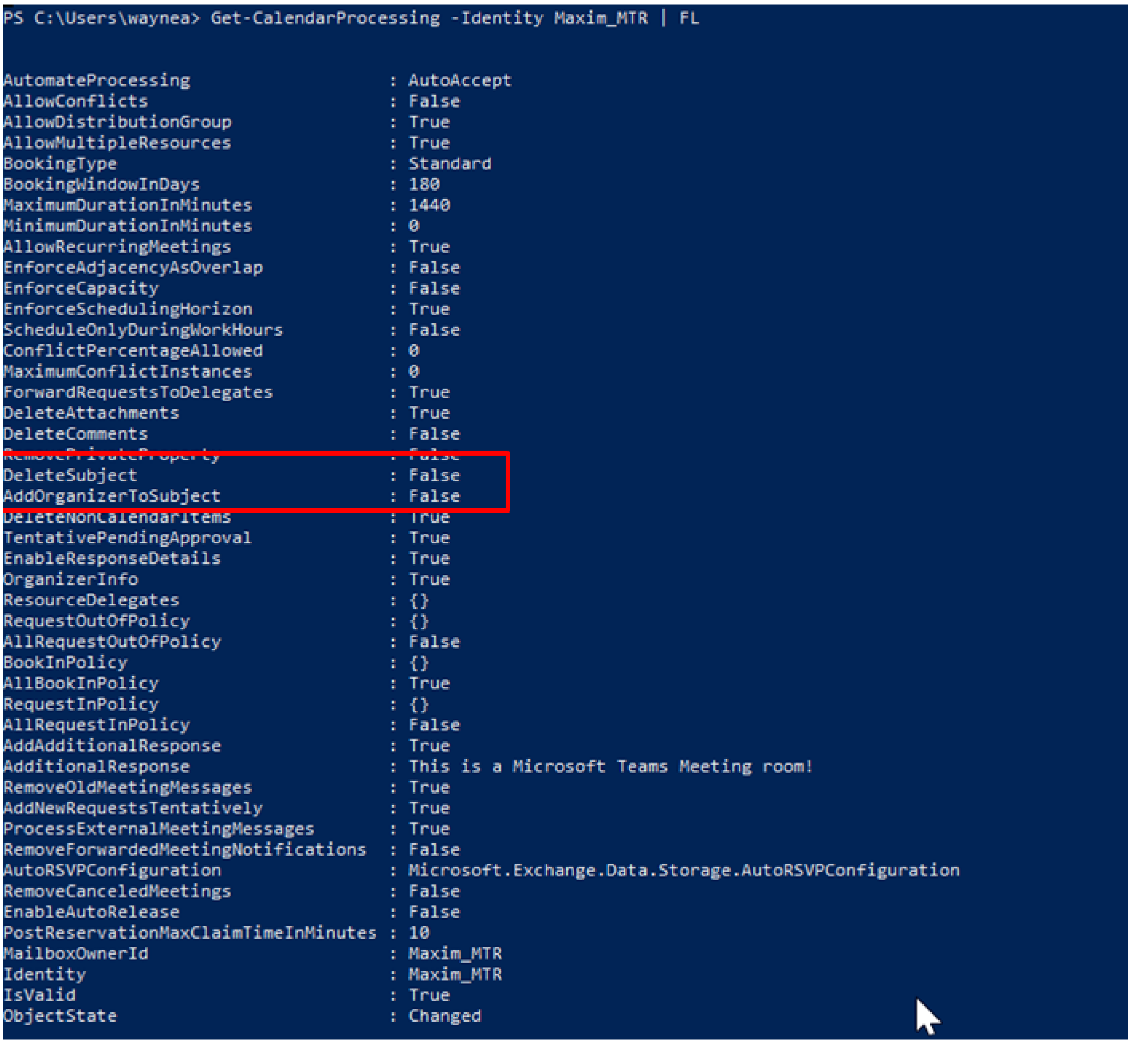
- /security/device_certificate_url = <url>/certificate.pfx
- /security/device_private_key_url = NULL
- security/device_certificate/password=<pfx password>

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.

Enable Display of Meeting Name using Exchange Online PowerShell

See the relevant Microsoft documentation for information about how to access the exchange instance (the tenant). Admin must set the two parameters indicated in the following figure to 'False':



```
PS C:\Users\waynea> Get-CalendarProcessing -Identity Maxim_MTR | FL


AutomateProcessing                      : AutoAccept
AllowConflicts                          : False
AllowDistributionGroup                  : True
AllowMultipleResources                  : True
BookingType                             : Standard
BookingWindowInDays                     : 180
MaximumDurationInMinutes                : 1440
MinimumDurationInMinutes                : 0
AllowRecurringMeetings                  : True
EnforceAdjacencyAsOverlap               : False
EnforceCapacity                         : False
EnforceSchedulingHorizon                : True
ScheduleOnlyDuringWorkHours             : False
ConflictPercentageAllowed               : 0
MaximumConflictInstances                : 0
ForwardRequestsToDelegates              : True
DeleteAttachments                       : True
DeleteComments                          : False
RemovePrivateProperty                   : False
DeleteSubject                           : False
AddOrganizerToSubject                   : False
DeleteNonCalendarItems                  : True
TentativePendingApproval                : True
EnableResponseDetails                   : True
OrganizerInfo                           : True
ResourceDelegates                       : {}
RequestOutOfPolicy                      : {}
AllRequestOutOfPolicy                   : False
BookInPolicy                            : {}
AllBookInPolicy                         : True
RequestInPolicy                         : {}
AllRequestInPolicy                      : False
AddAdditionalResponse                   : True
AdditionalResponse                      : This is a Microsoft Teams Meeting room!
RemoveOldMeetingMessages                : True
AddNewRequestsTentatively               : True
ProcessExternalMeetingMessages          : True
RemoveForwardedMeetingNotifications     : False
AutoRSVPConfiguration                   : Microsoft.Exchange.Data.Storage.AutoRSVPConfiguration
RemoveCanceledMeetings                  : False
EnableAutoRelease                       : False
PostReservationMaxClaimTimeInMinutes    : 10
MailboxOwnerId                          : Maxim_MTR
Identity                                : Maxim_MTR
IsValid                                 : True
ObjectState                             : Changed
```

The admin applies these two settings to the ‘Identity’ account:

- `Set-CalendarProcessing -Identity "Maxim_MTR" -DeleteSubject $false`
- `Set-CalendarProcessing -Identity "Maxim_MTR" -AddOrganizerToSubject $false`

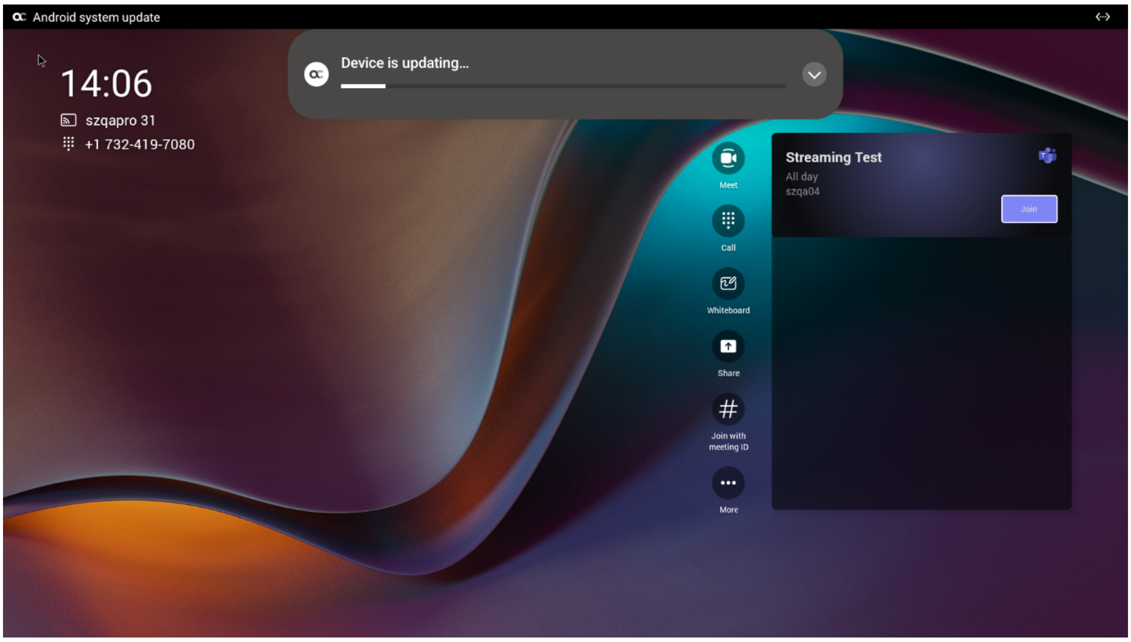
Update RXV81 Remotely

For instructions on how to update the device remotely, refer to https://docs.microsoft.com/en-us/microsoftteams/devices/remote-update.

Before an update is pushed to a device, the firmware detects whether the user is using the device or not. If they are, the user is notified and given an option to delay the update or apply it, nonetheless. The feature avoids disrupting users’ ongoing activities on their devices, such as calls.

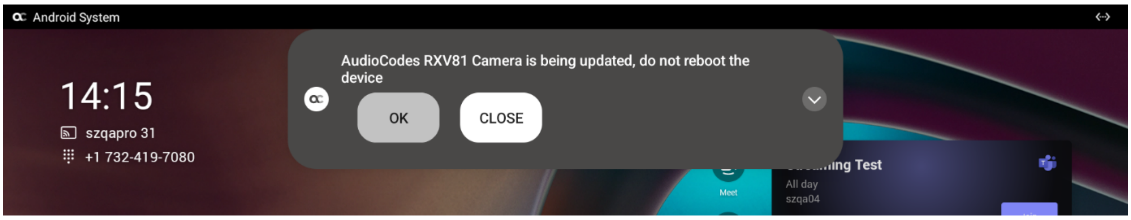
To ensure device integrity, RXV81 audio and camera peripherals firmware is automatically updated at the same time as the RXV81 firmware update.

During the update, notifications are displayed, indicating the device being updated and alerting the user not to reboot. The RXV81 unit is updated first:

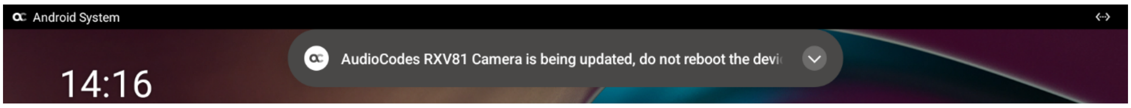


Device is updating...

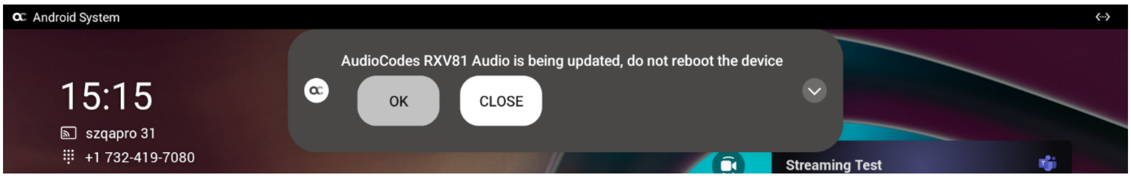
Next, AudioCodes camera and audio peripherals are updated. If prompted, tap **OK** to confirm the alert.



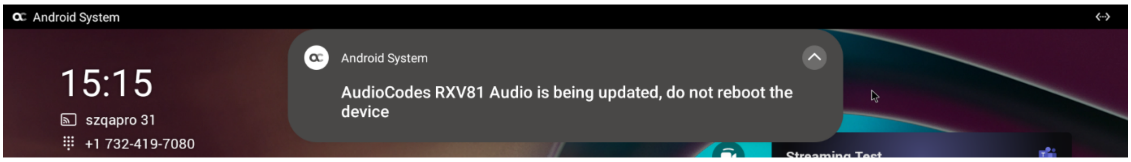
AudioCodes RXV81 Camera is being updated, do not reboot the device



AudioCodes RXV81 Camera is being updated, do not reboot the devi



AudioCodes RXV81 Audio is being updated, do not reboot the device



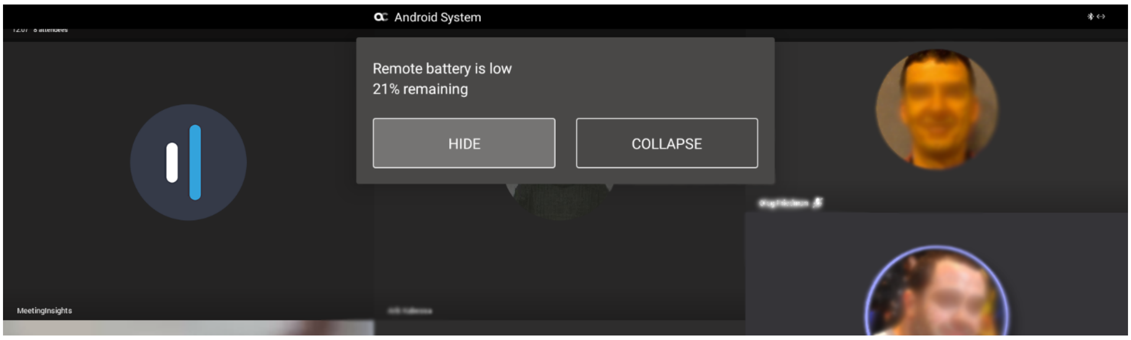
AudioCodes RXV81 Audio is being updated, do not reboot the device

Once all devices have been updated, a "Device restarting" notification is displayed.

View the RCU Battery Level

This section is only relevant for the TEAMS-RXV81 bundle, which includes an AudioCodes RCU.

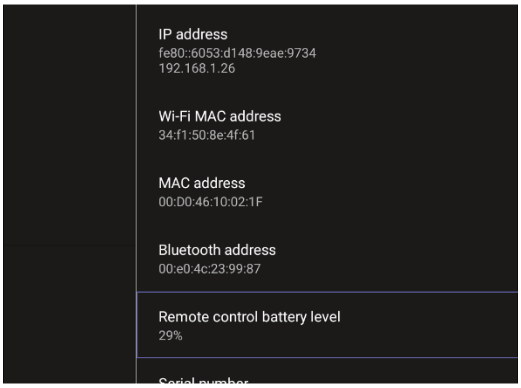
If the RCU batteries run low, the RXV81 application notifies you about the issue. This notification is sent to the screen / TV, as well as to AudioCodes' Device Manager. It indicates that the battery voltage level is low and what percentage level is left. Tap **HIDE** to conceal the notification.



Android System

Remote battery is low
21% remaining

You can also view the RCU battery level anytime on the 'Status' page. To access this page, navigate to the 'About' page (see View RXV81 Information on page 35), then tap **Status**.



IP address
fe80::6053:d148:9eae:9734
192.168.1.26

Wi-Fi MAC address
34:f1:50:8e:4f:61

MAC address
00:D0:46:10:02:1F

Bluetooth address
00:e0:4c:23:99:87

Remote control battery level
29%

Serial number

7 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 37).
2. Navigate to ‘Device Admin Settings’ (see Access Device Admin Settings on page 37).
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
- Configure Log Settings for Collecting Logs on the next page
- Enable Remote Logging on page 64
- Copy Diagnostic Data to SD Card on page 64
- Reset the System Configuration on page 65
- Reset User Data on page 67
- Restart the Teams App on page 67
- Perform Debug Recording on page 67
- Control Screen Capture on page 68
- Control Remote Package Capture on page 68
- Return to Previous Version on page 68

Additional procedures for device monitoring and troubleshooting are:

- Determine Device Status from LED Color Indications on page 68
- Perform Recovery Operations using the Power Button on page 69
- Save Logs while the Device is in Recovery Mode on page 70
- Restore Device Firmware via USB Disk on page 70
- Configure DSCP for QoS on page 71

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).
- You can limit the HDMI resolution and the Frames per Second (FPS) rate for debugging purposes. For details, see Configure the Display on page 41.

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.

Configure Log Settings for Collecting Logs

Device diagnostics (Logcat) can be collected using the Microsoft Admin Portal. For support purposes, general logs can be collected also using the Microsoft Admin Portal. The logs can help debug Teams application issues and issues related to the device.

➢ To configure log settings:

1. Access the 'Debugging' page (see System Monitoring and Debugging on the previous page).
2. Tap **Log settings**.
3. Tap **Log Level** and then select either **Verbose**, **Debug**, **Info**, **Warning**, **Error**, **Assert** or **None**.
4. Tap **Log Package Filter** and enter the filter.
5. Tap **Log Tag Filter** and enter the filter.
6. Tap **Log Buffer Filter**.
7. Tap **Current filter for logs**.

➢ **To collect logs:**

1. Reproduce the issue.
2. Access the Microsoft Admin Portal and under the **Devices** tab click the **Diagnostics** icon.
3. Click the **Diagnostics** icon and click **Proceed** in the upcoming dialog to confirm. The logs are uploaded to the server:
4. Click the **History** tab.
5. Click **Download** to download the logs.

Enable Remote Logging

Remote Logging via Syslog provides the same log level as Device Diagnostics (performed via the Microsoft Admin Portal) with some additional information that may be relevant to device issues (not Teams application issues).

Diagnostics via the Microsoft Admin Portal are saved to the device SD-card and collected after the event. Remote Logging via Syslog is different. The 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 page 62).
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 62).
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:

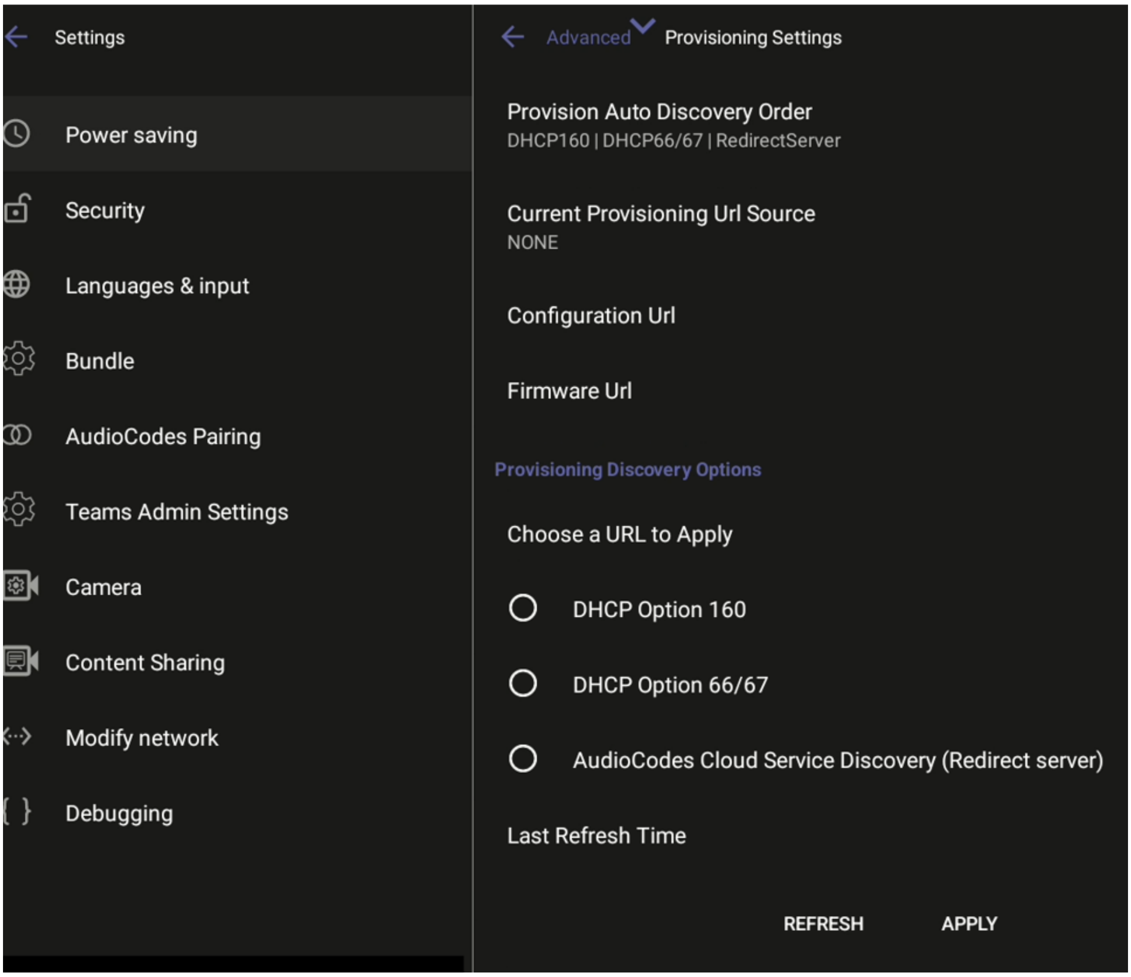
- Configure Provisioning Source Auto Discovery Settings below
- Reset Bundle Settings on the next page
- Reset to Original Configuration on the next page
- Perform a Full Factory Reset on page 67

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 62).
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 Bundle Settings

Admins can reset the current bundle settings using the **Reset Bundle** action. This action removes the current settings. Subsequently, upon rebooting the device, the bundle wizard is displayed (see Reconfigure a Bundle on page 47), where the new bundle type can be selected.

To reset the bundle:

1. Access the 'Debugging' page (see System Monitoring and Debugging on page 62).
2. Tap **Advanced**, then **Reset Bundle**. A confirmation prompt is displayed.
3. Select **OK**.

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 62).
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 62).
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 62).
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 62).
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 62).

2. Scroll down and turn the **Screen Capture** toggle button on or off.

Control Remote Package Capture

If SSH is enabled, admins can capture traffic packages using the ‘rpcapd’ (Remote Packet Capture) network sniffer application, which allows them to analyze and debug Android traffic on their desktop PC using the app's integral SSH server.

By default, Remote Package Capture is disabled. You can enable it to allow capturing of remote packages.

➢ **To enable or disable remote package capture:**

1. Access the 'Debugging' page (see System Monitoring and Debugging on page 62).

2. Scroll down and turn the **Remote Package 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:**

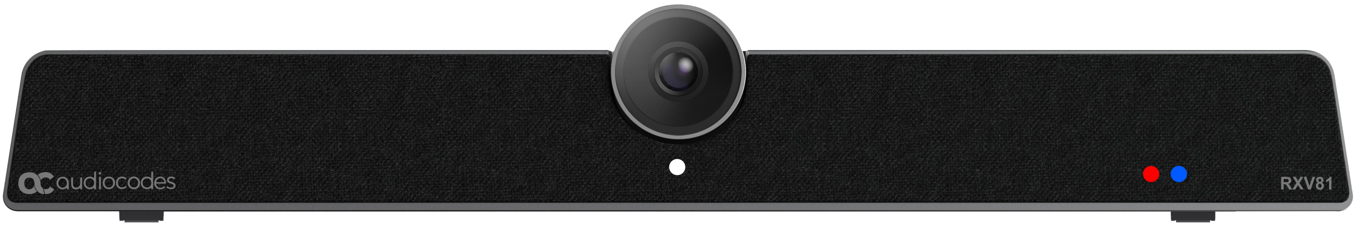
1. Access the 'Debugging' page (see System Monitoring and Debugging on page 62).

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 RXV81 from its LED color indications.

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



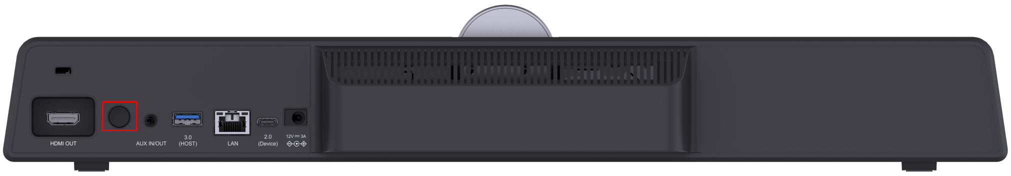
🔴	Red / white / red & white
White on	Device is powered on, signed in to Teams
White flashing	Device is in booting phase
Red on	Device is in mute (highest priority state)
Red flashing	Network connectivity lost / Device is in upgrade mode / RCU connectivity lost
Red + white on	Device is powered on, network 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 7-1: 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.

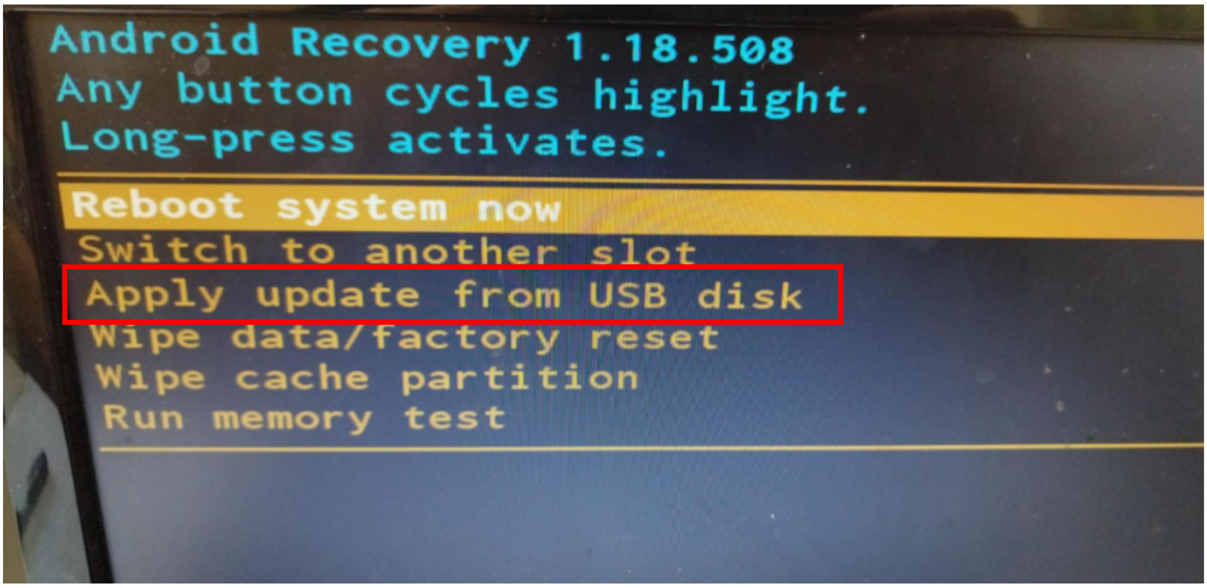
By simply clicking the **Export logs to USB disk** option, all logs are efficiently copied to the USB stick, providing a convenient and reliable method for log management during recovery procedures.

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.



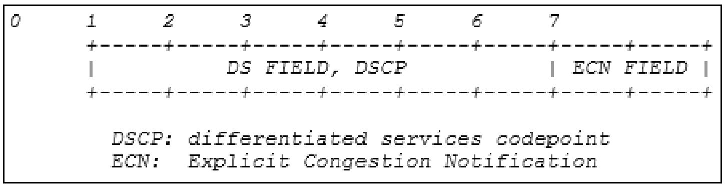
```
Android Recovery 1.18.508
Any button cycles highlight.
Long-press activates.

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

Configure DSCP for QoS

Microsoft Teams supports Differentiated Services (DS) containing a differentiated Services Code Point (DSCP) value and an ECN (Explicit Congestion Notification) value, for monitoring Quality of Service (QoS). The DSCP is part of the IP header that defines the type of routing service to tag outgoing voice packets originated from the device. It informs routers that these packets must receive a specific QoS.

Values can be set in decimal (e.g., 184) or hexadecimal (e.g., 0xb8). The default value is 0xb8 (184).



```
0     1     2     3     4     5     6     7
      +-----+-----+-----+-----+-----+-----+-----+-----+
      |          DS FIELD, DSCP           | ECN FIELD |
      +-----+-----+-----+-----+-----+-----+-----+-----+

        DSCP: differentiated services codepoint
        ECN:  Explicit Congestion Notification
```

- The DSCP value for **audio** is **0x46**.
- The DSCP value for **video** is **0x34** (screen sharing is not supported).

The DSCP value can be adjusted on the server, but not on the client.

The following figure shows the recommended port ranges:

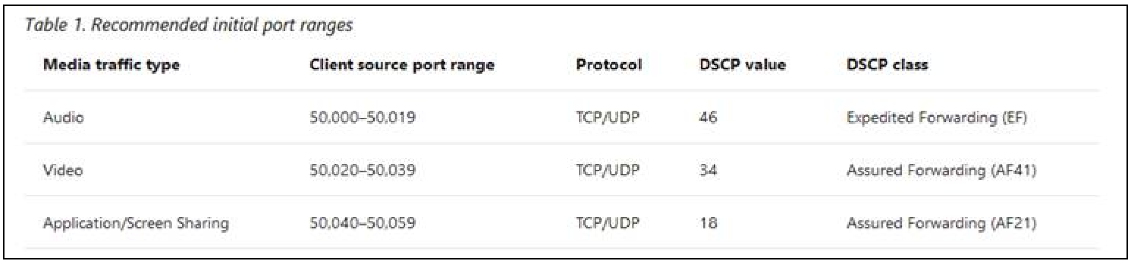
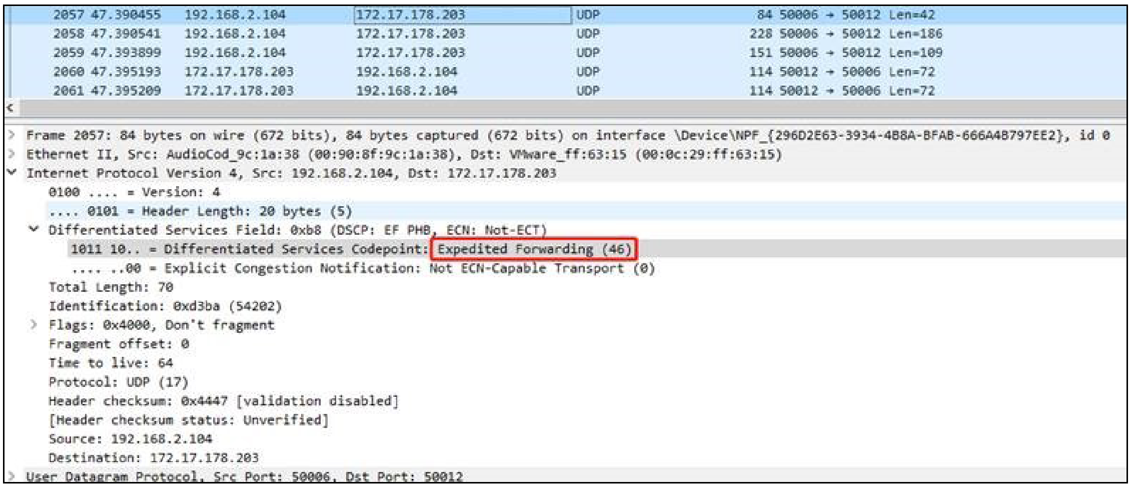


Table 1. Recommended initial port ranges

Media traffic type	Client source port range	Protocol	DSCP value	DSCP class
Audio	50,000–50,019	TCP/UDP	46	Expedited Forwarding (EF)
Video	50,020–50,039	TCP/UDP	34	Assured Forwarding (AF41)
Application/Screen Sharing	50,040–50,059	TCP/UDP	18	Assured Forwarding (AF21)

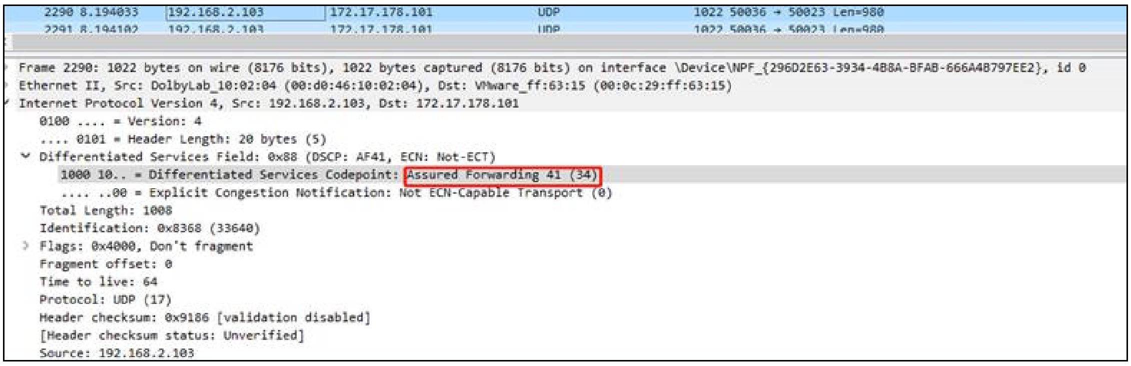
The following figure shows the recommended DSCP setting for Audio:



```
2057 47.390455   192.168.2.104     172.17.178.203     UDP         84 50006 → 50012 Len=42
2058 47.390541   192.168.2.104     172.17.178.203     UDP        228 50006 → 50012 Len=186
2059 47.393899   192.168.2.104     172.17.178.203     UDP        151 50006 → 50012 Len=109
2060 47.395193   172.17.178.203    192.168.2.104      UDP        114 50012 → 50006 Len=72
2061 47.395209   172.17.178.203    192.168.2.104      UDP        114 50012 → 50006 Len=72

> Frame 2057: 84 bytes on wire (672 bits), 84 bytes captured (672 bits) on interface \Device\NPF_{296D2E63-3934-4B8A-BFAB-666A48797EE2}, id 0
> Ethernet II, Src: AudioCod_9c:1a:38 (00:90:8f:9c:1a:38), Dst: VMware_ff:63:15 (00:0c:29:ff:63:15)
v Internet Protocol Version 4, Src: 192.168.2.104, Dst: 172.17.178.203
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  v Differentiated Services Field: 0xb8 (DSCP: EF PHB, ECN: Not-ECT)
      1011 10.. = Differentiated Services Codepoint: Expedited Forwarding (46)
      .... ..00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)
    Total Length: 70
    Identification: 0xd3ba (54202)
  > Flags: 0x4000, Don't fragment
    Fragment offset: 0
    Time to live: 64
    Protocol: UDP (17)
    Header checksum: 0x4447 [validation disabled]
    [Header checksum status: Unverified]
    Source: 192.168.2.104
    Destination: 172.17.178.203
> User Datagram Protocol, Src Port: 50006, Dst Port: 50012
```

The following figure shows the recommended DSCP setting for Video:



```
2290 8.194033    192.168.2.103     172.17.178.101     UDP       1022 50036 → 50023 Len=980
2291 8.194102    192.168.2.103     172.17.178.101     UDP       1022 50036 → 50023 Len=980

Frame 2290: 1022 bytes on wire (8176 bits), 1022 bytes captured (8176 bits) on interface \Device\NPF_{296D2E63-3934-4B8A-BFAB-666A48797EE2}, id 0
Ethernet II, Src: DolbyLab_10:02:04 (00:d0:46:10:02:04), Dst: VMware_ff:63:15 (00:0c:29:ff:63:15)
Internet Protocol Version 4, Src: 192.168.2.103, Dst: 172.17.178.101
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  v Differentiated Services Field: 0x88 (DSCP: AF41, ECN: Not-ECT)
      1000 10.. = Differentiated Services Codepoint: Assured Forwarding 41 (34)
      .... ..00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)
    Total Length: 1008
    Identification: 0x8368 (33640)
  > Flags: 0x4000, Don't fragment
    Fragment offset: 0
    Time to live: 64
    Protocol: UDP (17)
    Header checksum: 0x9186 [validation disabled]
    [Header checksum status: Unverified]
    Source: 192.168.2.103
```

For more information refer to Microsoft's website.

8 Android-based Teams Devices Parameters

The following are the configuration file parameters currently supported by Android-based Teams devices, in AudioCodes' UC version format. These parameters are comprised of Microsoft configuration profile settings and AudioCodes' device-specific parameters.

Parameter	Possible Values	Default Value
general/power_saving	**0** or **1**	0
phone_lock/enabled	**0** or **1**	0
phone_lock/timeout	(Number of seconds)	900
phone_lock/lock_pin	(Pin number)	123456
display/language	(Language)	English
display/screensaver_enabled	**0** or **1**	1
display/screensaver_timeout	(Number of seconds)	1800
display/backlight	(Number between 0 and 100 inclusive)	80
display/high_contrast	**0** or **1**	0
date_time/timezone	(Timezone)	(Retrieved from network)
date_time/time_format	**12** or **24**	24
network/ip_address	Manually defined by customer if needed	
network/subnet_mask		
network/default_gateway		
network/primary_dns		
network/pecondary_dns		
network/pc_port	**0** or **1**	1
office_hours/start	(Time in 24-hour XX:XX format)	08:00
office_hours/end	(Time in 24-hour XX:XX	17:00

Parameter	Possible Values	Default Value
	format)	
logging/enabled	**0** or **1**	0
logging/levels	**Verbose**, **Debug**, **Info**, **Warn**, **Error**, **Assert** or **None**	Verbose
admin/default_password		1234
admin/ssh_enabled	**0** or **1**	0
security/SSLCertificateErrorsMode	**IGNORE**, **NOTIFICATION** or **DISALLOW**	DISALLOW
security/ca_certificate/[0-4]/uri	(URI to download the customer's root CA)	User downloads, left blank by default
provisioning/period/daily/time	(Time in 24-hour XX:XX format)	0:00
provisioning/period/hourly/hours_ interval		24
provisioning/period/type	**HOURLY**, **DAILY**, **WEEKLY**, **POWERUP**, **EVERY5MIN** or **EVERY15MIN**	DAILY
provisioning/period/weekly/day		Sunday
provisioning/period/weekly/time	(Time in 24-hour XX:XX format)	0:00
provisioning/random_provisioning_ time		120

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

Document #: LTRT-09996

audiocodes