User's and Administrator's Manual

AudioCodes Room Experience (RX) Suite

RX-PAD

Version 3.0

audiocodes

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

Notes and Warnings

Canada Warning

This device contains licence-exempt transmitter(s)/receiver(s) that comply with Innovation,

Science and Economic Development Canada's licence-exempt RSS(s). Operation is subject to the following two conditions:

- This device may not cause interference.
- This device must accept any interference, including interference that may cause undesired operation of the device.

Le présent appareil est conforme aux CNR d'ISED applicables aux appareils radio exempts de licence. L'exploitation est autorisée aux deux conditions suivantes :

- l'appareil ne doit pas produire de brouillage;
- l'utilisateur de l'appareil doit accepter tout brouillage radioélectrique subi, même si le brouillage est susceptible d'en compromettre le fonctionnement.

Radio apparatus containing digital circuitry which can function separately from the operation of a transmitter or an associated transmitter, shall comply with ICES-003. In such cases, the labelling requirements of the applicable RSS apply, rather than the labelling requirements in ICES-003. This Class B digital apparatus complies with Canadian ICES-003.

Cet appareil numérique de la classe B est conforme à la norme NMB-003 du Canada.

IC SAR Warning:

This equipment should be installed and operated with minimum distance 20 cm between the radiator and your body.

Lors de l' installation et de l' exploitation de ce dispositif, la distance entre le radiateur et le corps est d 'au moins 20 cm.

Operation of 5150-5250 MHz is restricted to indoor use only.

Le fonctionnement de 5150-5250 MHz est limité à une utilisation en intérieur uniquement.

Related Documentation

Document Name
RXV81 RXV200 RX-PAD RX-PANEL Release Notes
RXV200 MTRA Compute User's and Administrator's Manual
RX-PAD Meeting Room Controller Quick Guide

Document Name
Pairing RX-PAD with Microsoft Teams Room on Android
RXVCAM70 PTZ Camera Quick Guide
RXVCam360 Video Conferencing Camera Quick Guide
One Voice Operation Center (OVOC) User's Manual
Device Manager Administrator's Manual

Document Revision Record

LTRT	Description
18320	Initial document release
18321	Reset pinhole button
18322	HDMI In | MTRA screen sharing | Audio Notifications via MTRA Speakers
18323	Application launcher. Enrolling with Intune Policies. System State page.
18324	2.6. Wall mount installation
18325	Camera Settings. PTZ adjusters. Downgrade block. Tracking Mode. Configuring Display.
18326	Updated to Version 2.8.208
18327	Updated to Version 2.8.574 (M1); Canada warnings
18328	Updated to Version 2.8.855 (M2)
18329	Room Control icon when URL configured
18330	Updated to Version 2.8.917 (M3); clarification in Configuring Room Control section; added Modifying IP Network Settings section
18331	Added Configuring Wi-Fi section
18332	Added AI Summary section; document restructure
18333	Updated to Version 3.0; provisioning source auto discovery; customizable room control icon; admin password brute force

LTRT	Description
	protection; new bundle RXV200-B50 Revised Getting Started section

Table of Contents

1 Introduction

The AudioCodes RX-PAD Meeting Room Controller is a center-of-room intuitive touch controller that provides complete and straightforward access to AudioCodes meeting room solutions.

With its proximity sensor, ergonomic design and 8-inch high-resolution display, this high-quality controller enables simple and intuitive operation with extensive customization options.

The RX-PAD Meeting Room Controller offers innovative features, such as:

- One-click-to join with an integrated calendar for simple collaboration initiation
- Smooth content sharing
- Easily configurable camera adjustments and views; in addition, Composite AI camera view if paired with RXV200
- Room control option from local web page of Customer's room control app
- AI summary option to create and send out meeting summaries

Part number: TEAMS-RX-PAD – MSRP

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.

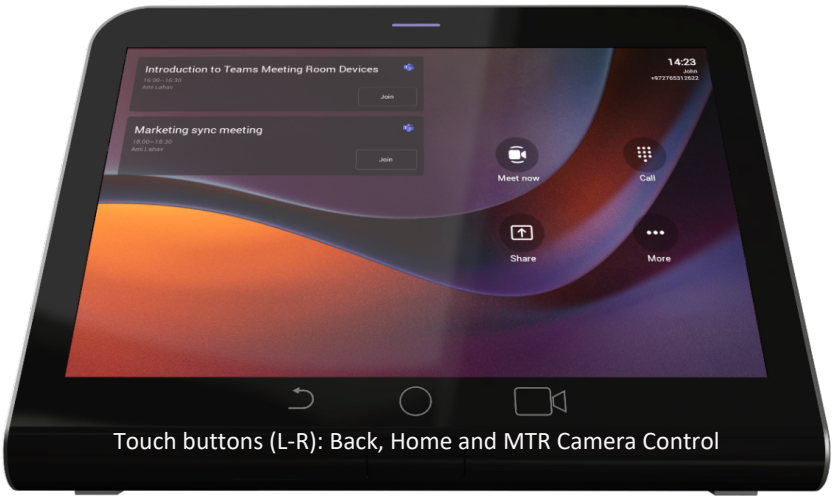
For detailed information on the AOSP migration process, please refer to the relevant Microsoft documentation.

Highlights

RX-PAD feature highlights are:

- Leverages plug-and-play simplicity to deliver a productive and familiar Microsoft Teams meeting experience requiring connection with just a PoE cable.
- Features functions that are readily accessible to all participants with easy access to camera settings via onscreen navigation buttons that put all AudioCodes meeting room solutions at your fingertips.
- Paired with the main MTR unit which runs the Teams Room application on Android
- Compatible with the AudioCodes RXV81 MTR on Android and RXV200 MTR on Android
- High-resolution 8-inch touch LCD

- Supported by OVOC Device Manager, enabling monitoring/upgrading from anywhere.



Touch buttons (L-R): Back, Home and MTR Camera Control

	Speedy collaboration initiation. One-click-to-join for easy collaboration.
	An inbuilt calendar to quickly set or join meetings
	A single cable connection keeps your desk clean and tidy
	Innovative ergonomic design for seamless operation
	High-resolution, eight-inch touch LCD
	Human sensor
	Cable compartment
	POE or power enabled
	Dual-band Wi-Fi and Bluetooth support
	Android 12

Bundles

The *RXV200* MTRA supports multiple devices for mix-and-match adaptability and simplified deployment and management. Providing a reliable solution for every room layout and allow easy meeting room component upgrades, RXV200 is available in six main bundles, as listed in the following table:

Name of Bundle	Description
RXV200-B05	■ Leverages RX-PAD to enable integration of an existing conference room AV system with Microsoft Teams. Connects to an existing audiovideo conference system. ■ Any room size ■ Any number of participants See the RXV200-BO5 Bundle on page 5.
RXV200-B09	■ RXV200 ■ Touch screen See the RXV200-B09 Bundle on page 5.
RXV200-B20	■ RX-PAD ■ RXVCam50 ■ RX15 (audio) ■ Small rooms of up to 10 participants See the RXV200-B20 Bundle on page 6.
RXV200-B360	■ RX-PAD ■ RXVCam360 (video | audio) ■ Small-medium size rooms of 2-8 participants ■ Productivity: Meeting Insights See the RXV200-B360 Bundle on page 7.
RXV200-B40	■ RX-PAD ■ RXVCam50 ■ RX40 (audio) ■ Medium size rooms of 6-12 participants ■ Productivity: Meeting Insights See the RXV200-B40 Bundle on page 8.
RXV200-B50	■ RX-PAD ■ RXVCam50 ■ RX-HDL200 sound bar (audio)

Name of Bundle	Description
	■ Medium size rooms of 6-12 participants ■ Productivity: Meeting Insights See the RXV200-B50 Bundle on page 9.
RXV200-B70	■ RX-PAD ■ RXVCam70 ■ RX40 (audio) ■ Large rooms of 10-18 participants ■ Productivity: Meeting Insights See the RXV200-B70 Bundle on page 10.

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

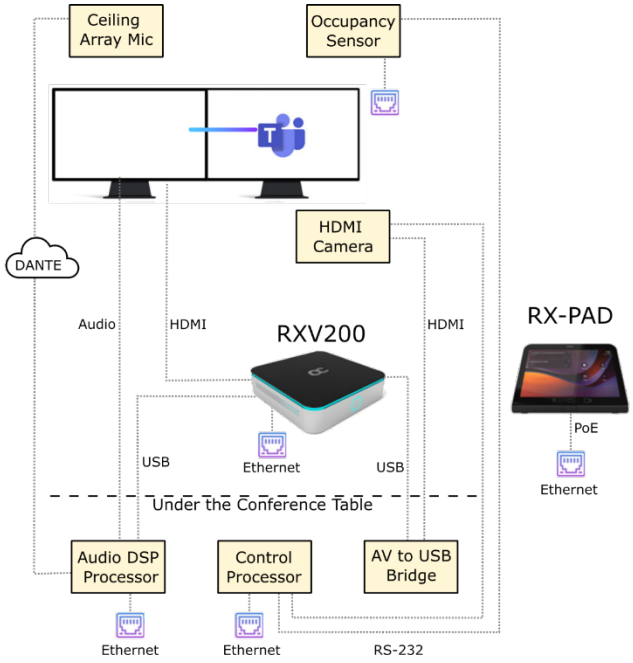
RXV81 BYOD is available in the bundles listed in the following table:

Name of Bundle	Details
RXV81P	■ Executive Offices | Huddle Rooms ■ RXV81 main unit

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

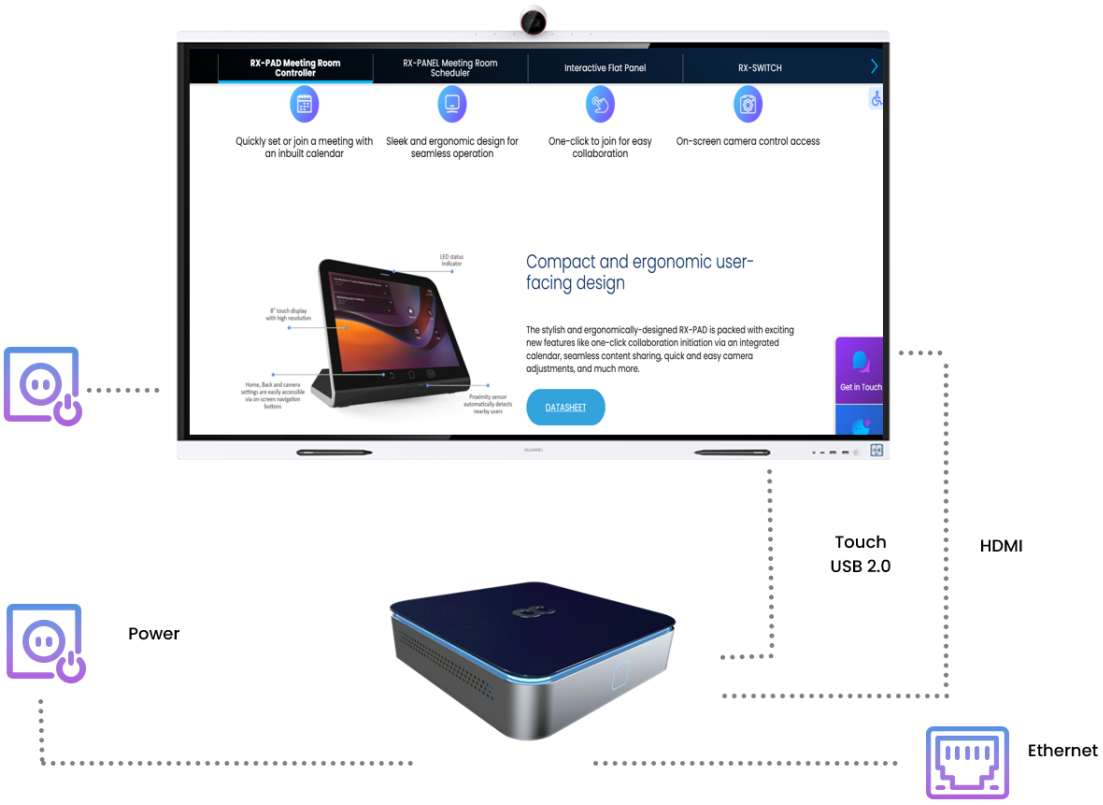
RXV200-BO5 Bundle

The following figure illustrates the RXV200-B05 bundle.



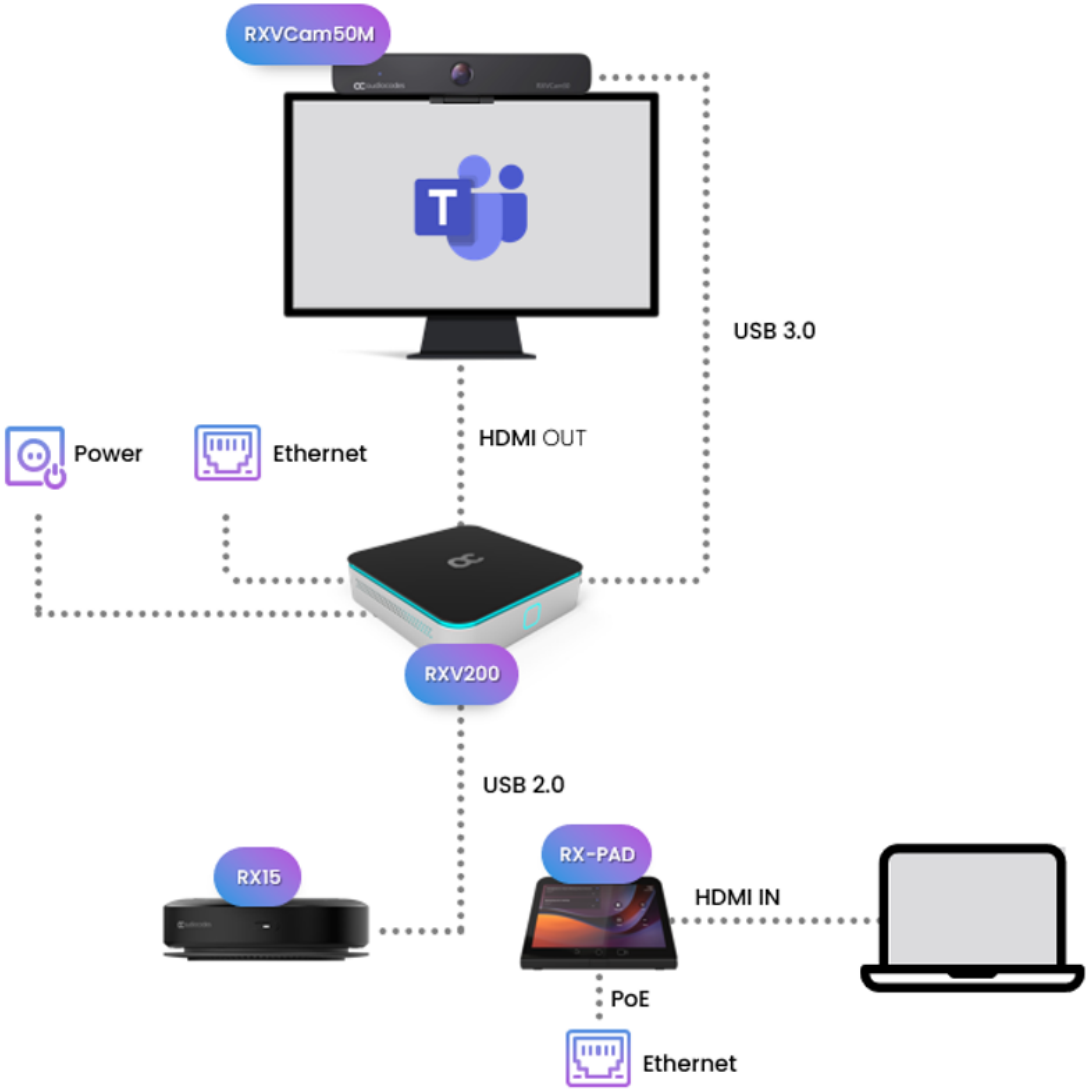
RXV200-B09 Bundle

The RXV200 AV compute unit integrates with the client’s touch screens without the need for an RX-PAD.



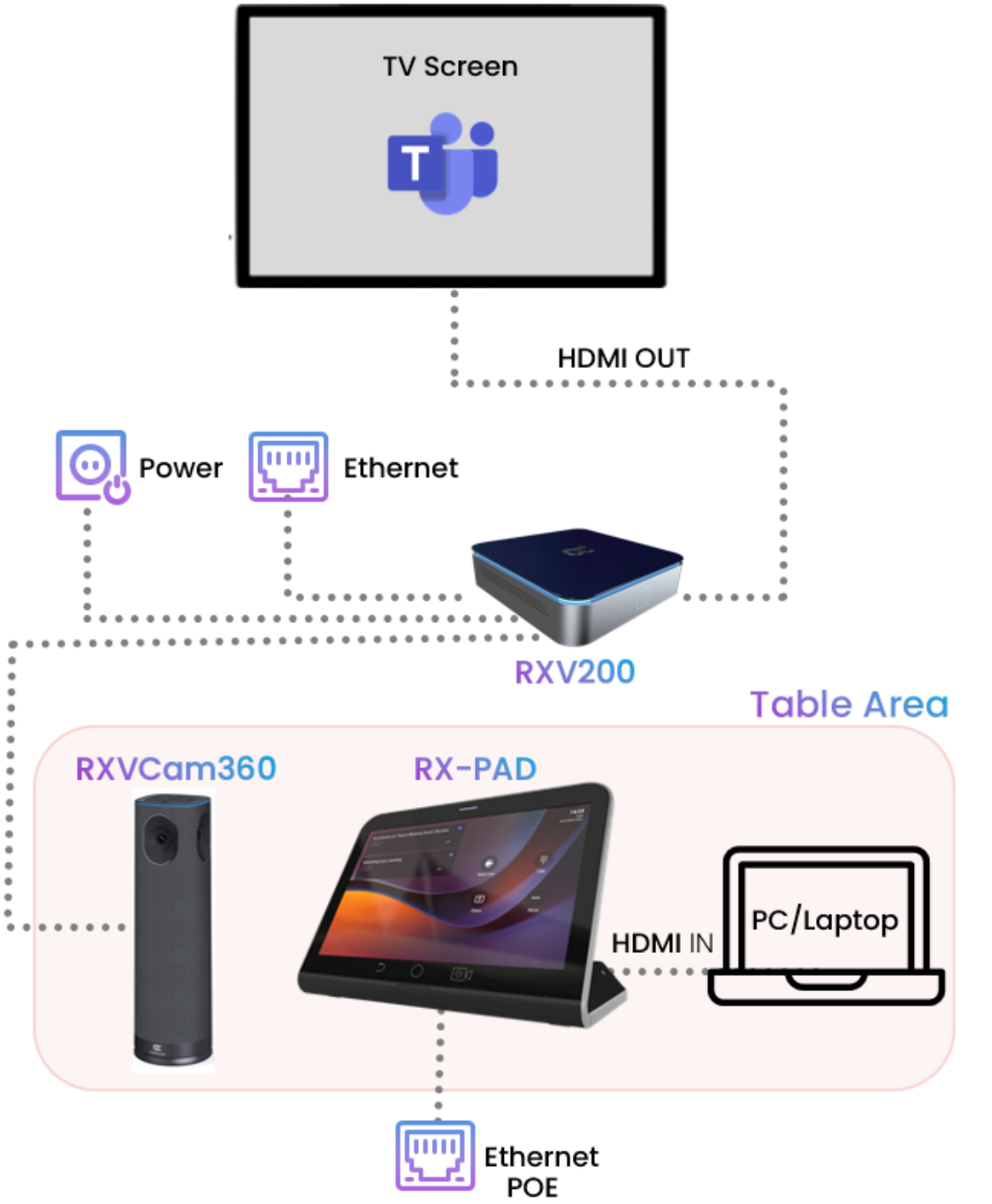
RXV200-B20 Bundle

The following figure illustrates the RXV200-B20 bundle.



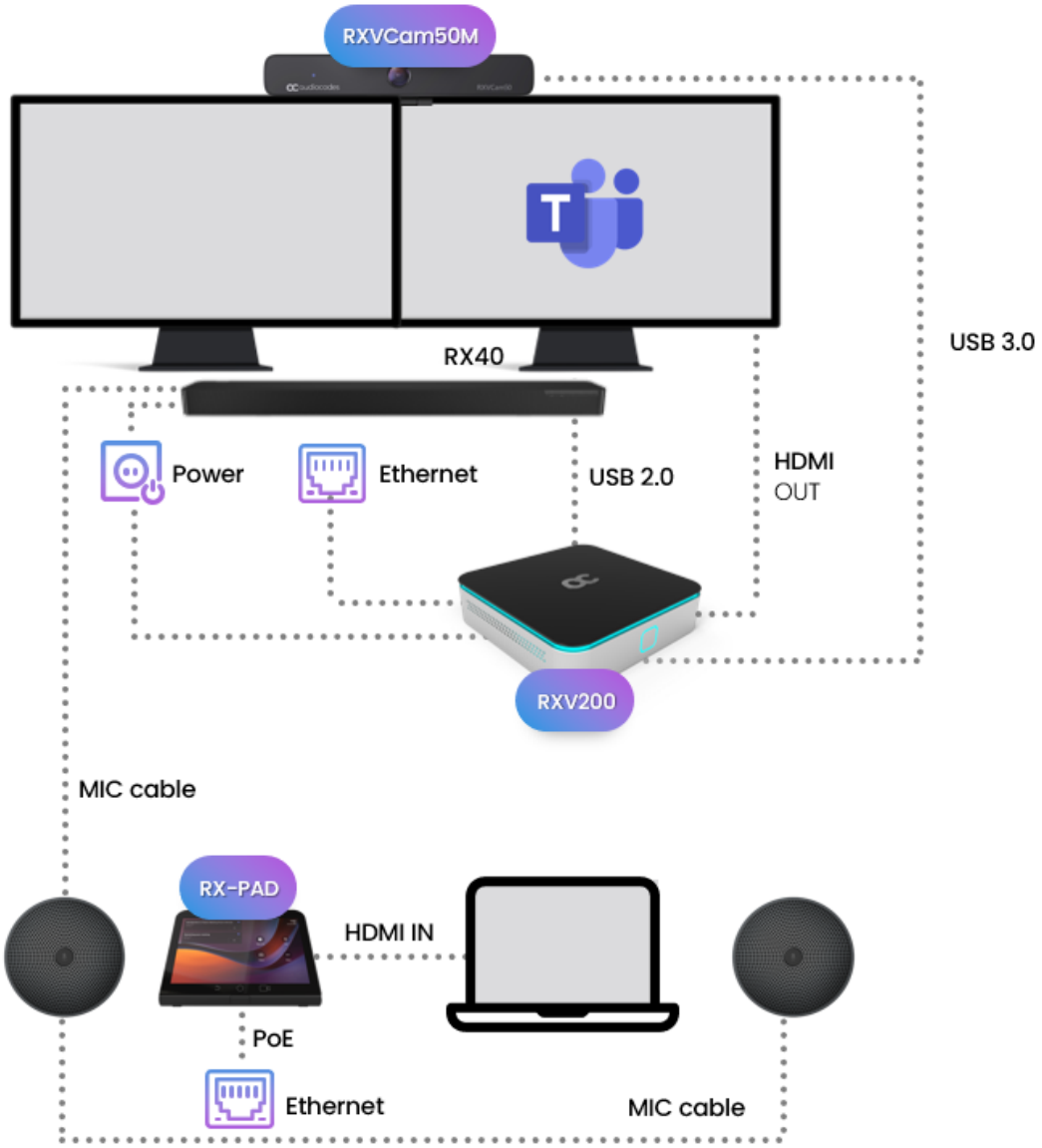
RXV200-B360 Bundle

The following figure illustrates the RXV200-B360 bundle.



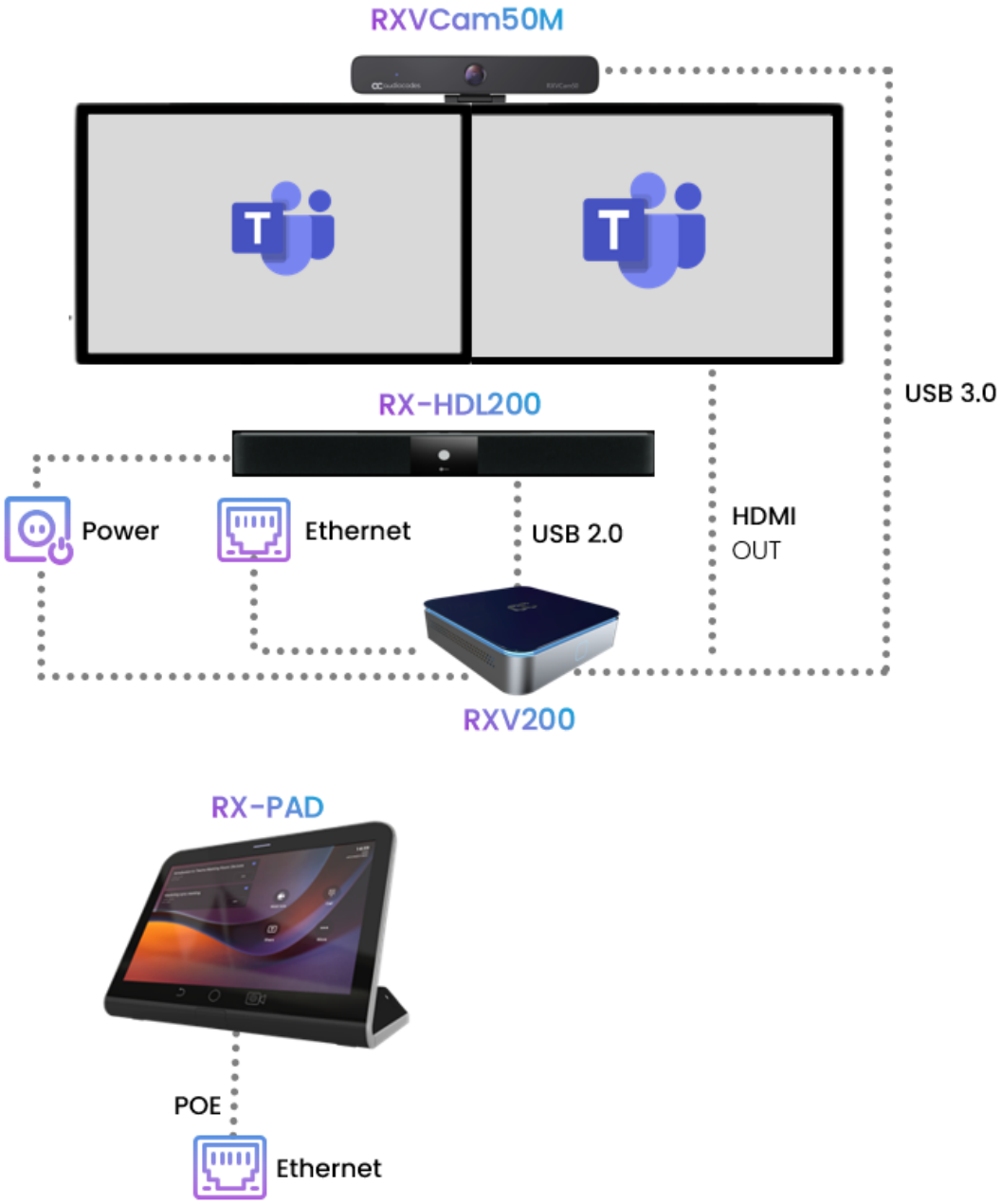
RXV200-B40 Bundle

The following figure illustrates the RXV200-B40 bundle.



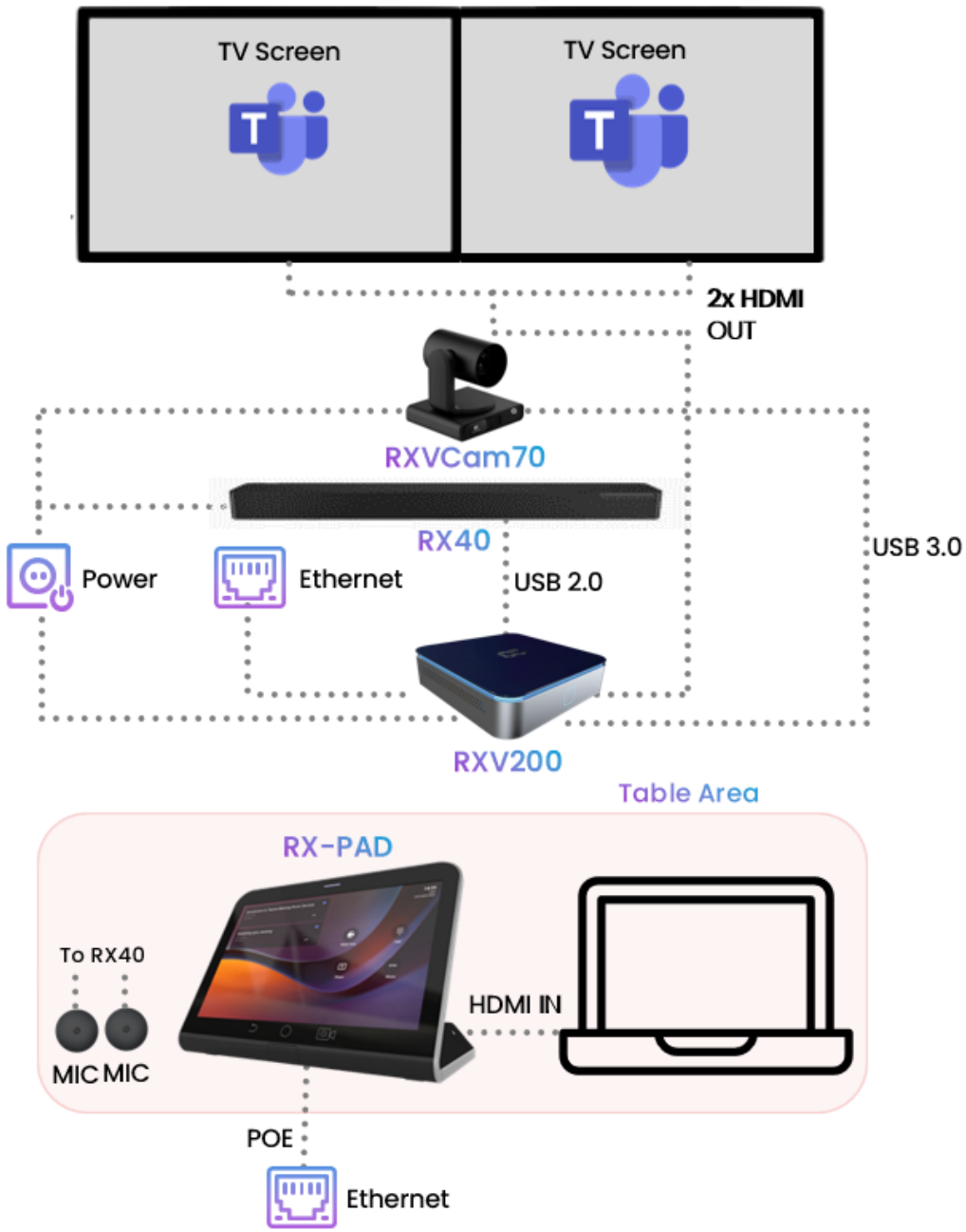
RXV200-B50 Bundle

The following figure illustrates the RXV200-B50 bundle.



RXV200-B70 Bundle

The following figure illustrates the RXV200-B70 bundle.



HDMI Input Source Features

When multiple HDMI-IN inputs are used, typically involving both a physical HDMI-IN input and a wireless HDMI-IN from an RX-PAD:

- When a new HDMI-IN input is connected during a sharing session, it automatically becomes the current active source.
- When an HDMI-IN input is unplugged, the remaining connected HDMI-IN source automatically becomes the active source.

The HDMI-IN status can be monitored from the System State page (see Monitor the System Status on page 101).

Management

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

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

Admins can monitor the status of the device's software modules from the System State screen (see Monitor the System Status on page 101).

- 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.

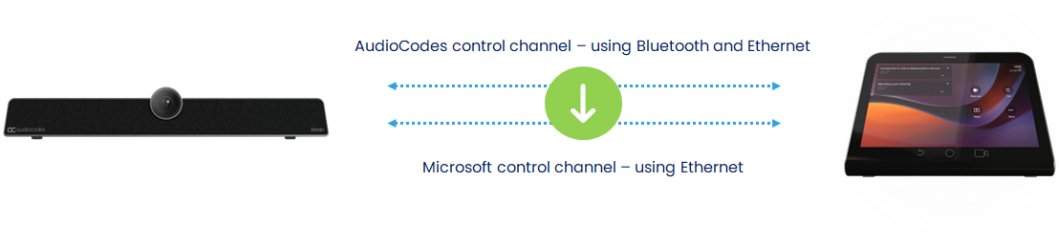
Specifications

- For RX-PAD specifications, see the RX-PAD datasheet.

Connectivity

The RX-PAD must be paired with the 'main MTR unit', for example, RXV81 or RXV200, to be active. RXV81 | RXV200 is the Front of the Room MTR main unit.

- The RX-PAD runs the main client and MTR processing (audio, video, sharing)
- The main unit (RXV81 | RXV200) can run as a standalone (using remote / keyboard / mouse) or paired with the controller
- Both RX-PAD and RXV81 | RXV200 share the same MTR license and account
- The user signs in on both RX-PAD and RXV81 | RXV200, to the same account
- Configuration is 'shared' between the Room Controller and the main unit



Audio Notifications via MTRA Speakers

RX-PAD triggers audio notifications via RXV81 and RXV200 MTRA speakers. Users hear audio notifications produced by the RX-PAD directly through the MTRA. Crucial features such as Talkback accessibility, ensuring a more streamlined and accessible communication experience during meetings and collaboration sessions, are included. The capability leverages Front of Room devices (RXV81 | RXV200) to serve as the audio source for the RX-PAD, enabling the utilization of accessibility features it.

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 RX-PAD consists of:

1. Installing RX-PAD:
   - Reviewing the shipped RX-PAD items
   - Positioning
   - Mounting
   - Cabling
   - Powering up

   For details, see the *RX-PAD Meeting Room Controller Quick Guide* shipped with the product oravailable from AudioCodes.
2. Pairing or setting up the RXV200 or RXV81 unit with RX-PAD (see Set up RXV200 with the Initial Configuration Wizard below or Pair RXV81 with RX-PAD on page 18).
3. Operating RX-PAD and configuring the paired RXV200 or RXV81, as described in the following sections of this manual.

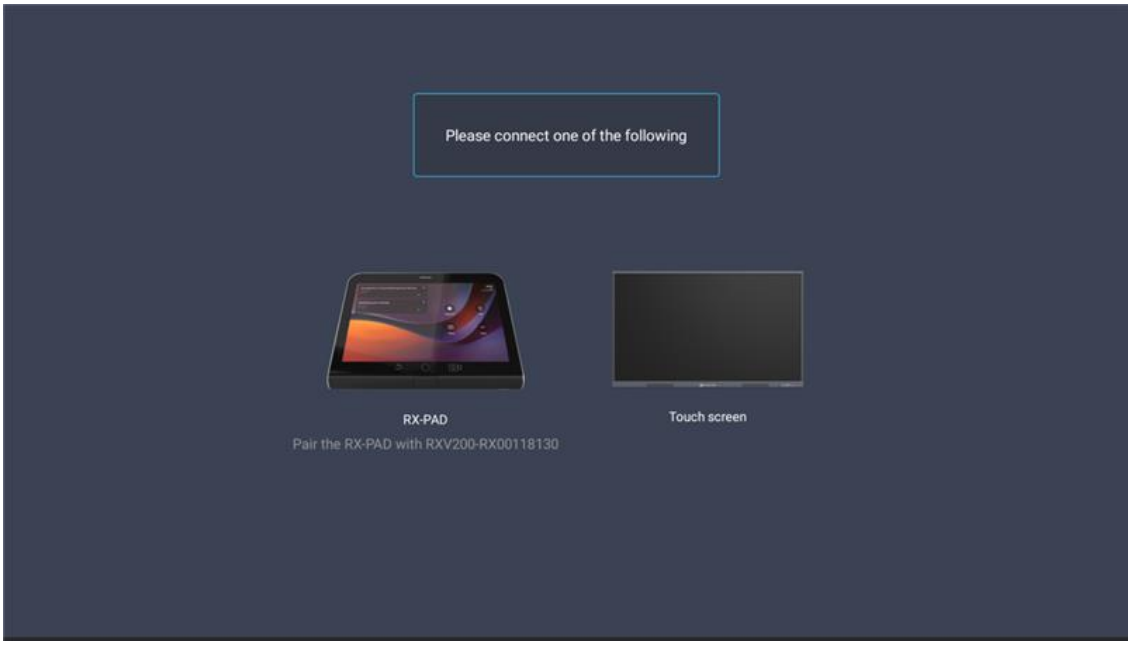
You can remotely sign-in and provision Android Teams devices via the Microsoft Teams Admin Center. For details, refer to the relevant Microsoft documentation.

Set up RXV200 with the Initial Configuration Wizard

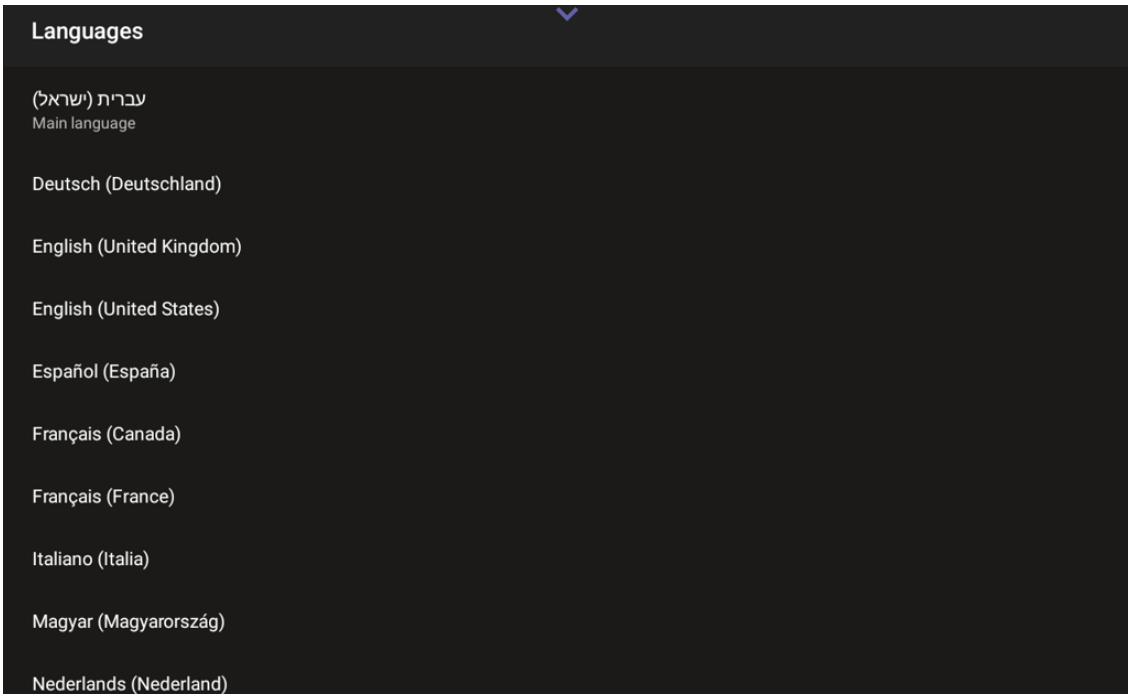
The Initial Configuration Wizard allows you to easily set up your MTRA with RX-PAD.

➢ **To set up your MTRA:**

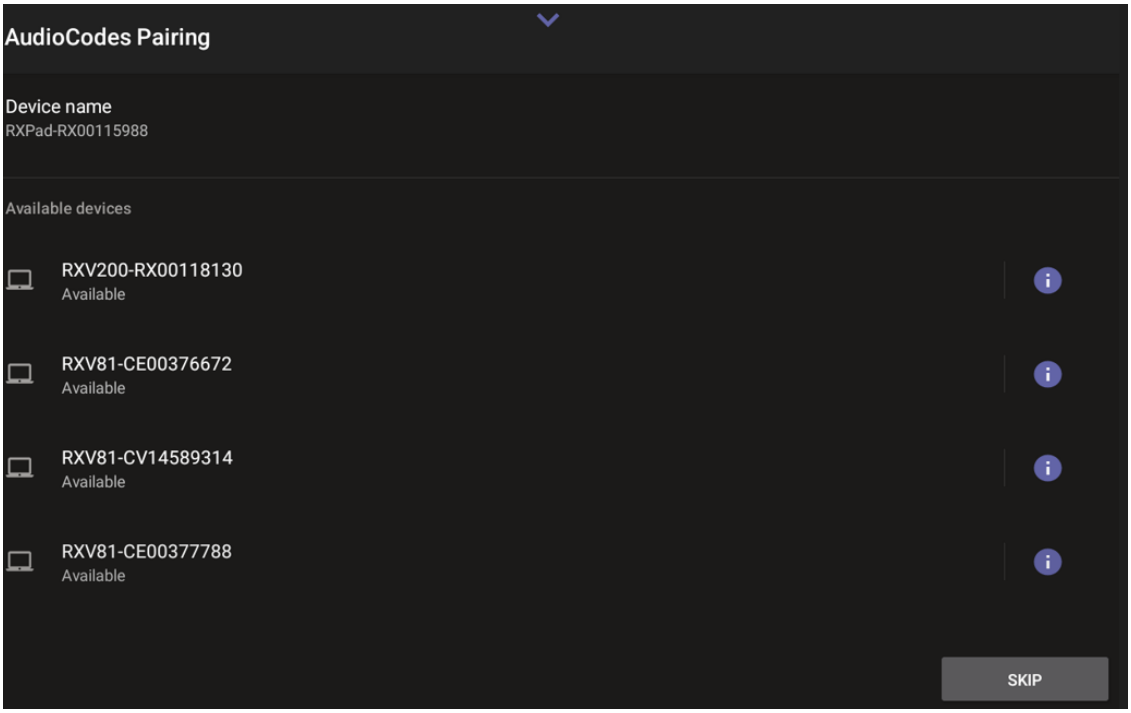
1. Connect the RXV200 and the RX-PAD to the power supply and the same local network.
   - The RXV200 starts up and prompts you to connect an RX-PAD or a touch screen.



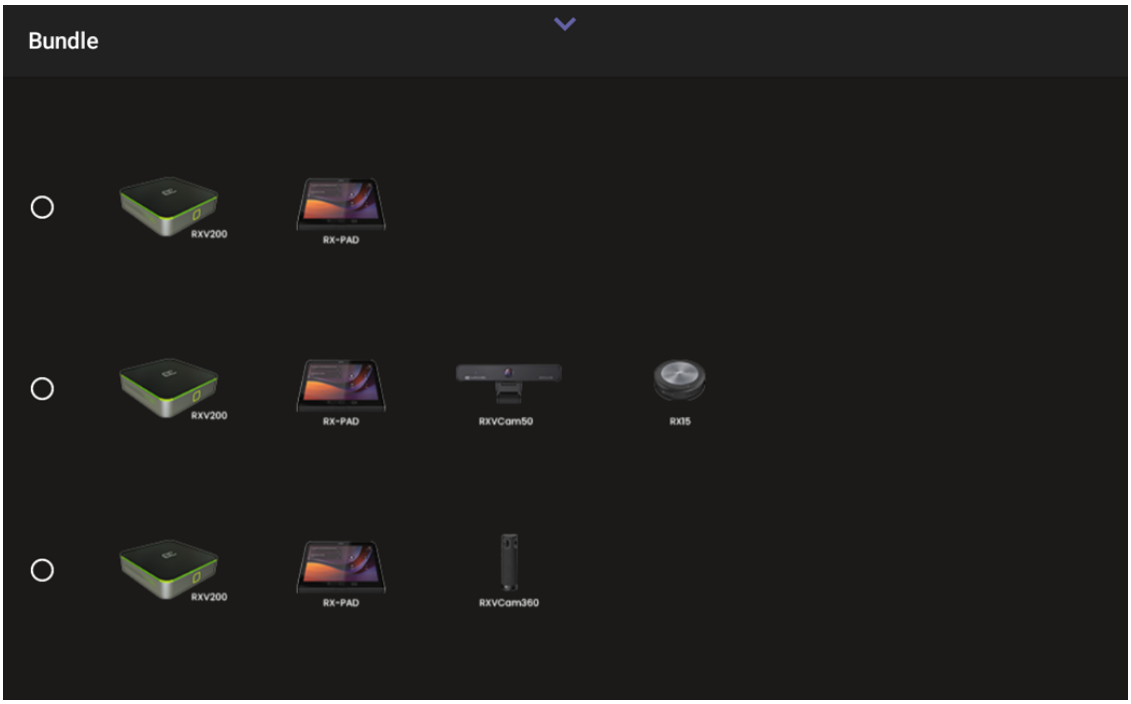
- The RX-PAD starts up and prompts you to select a language for the UI.



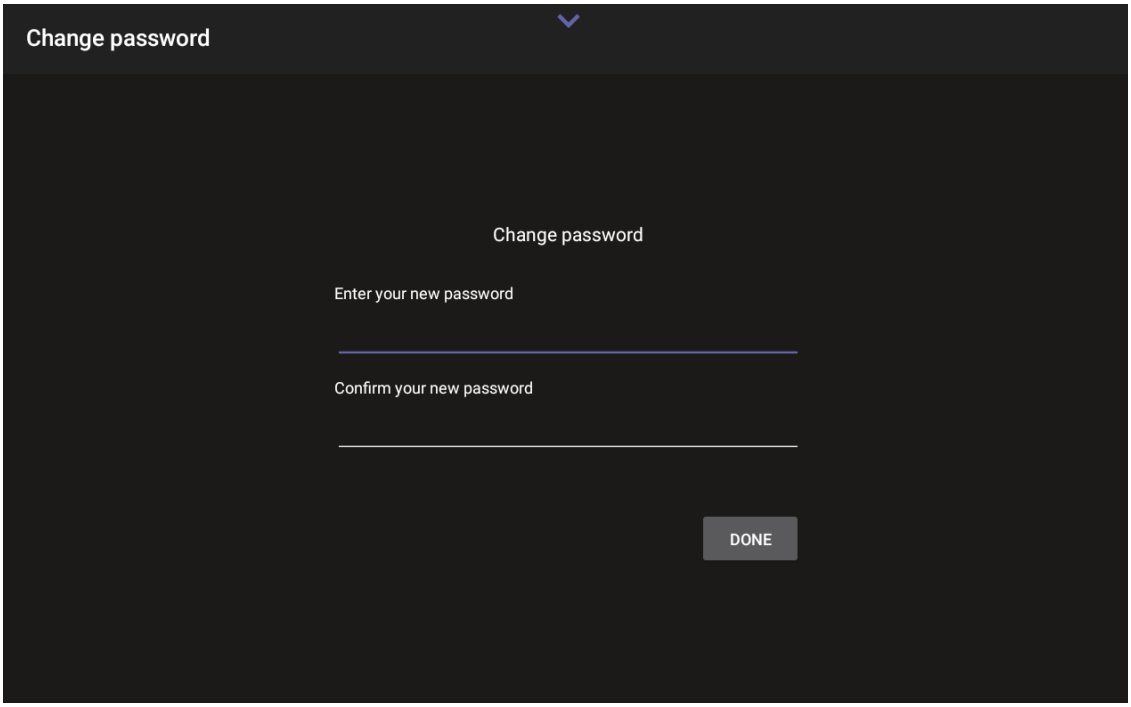
2. On the RX-PAD, select the requested language. The AudioCodes Pairing page is displayed, listing the available MTRAs:



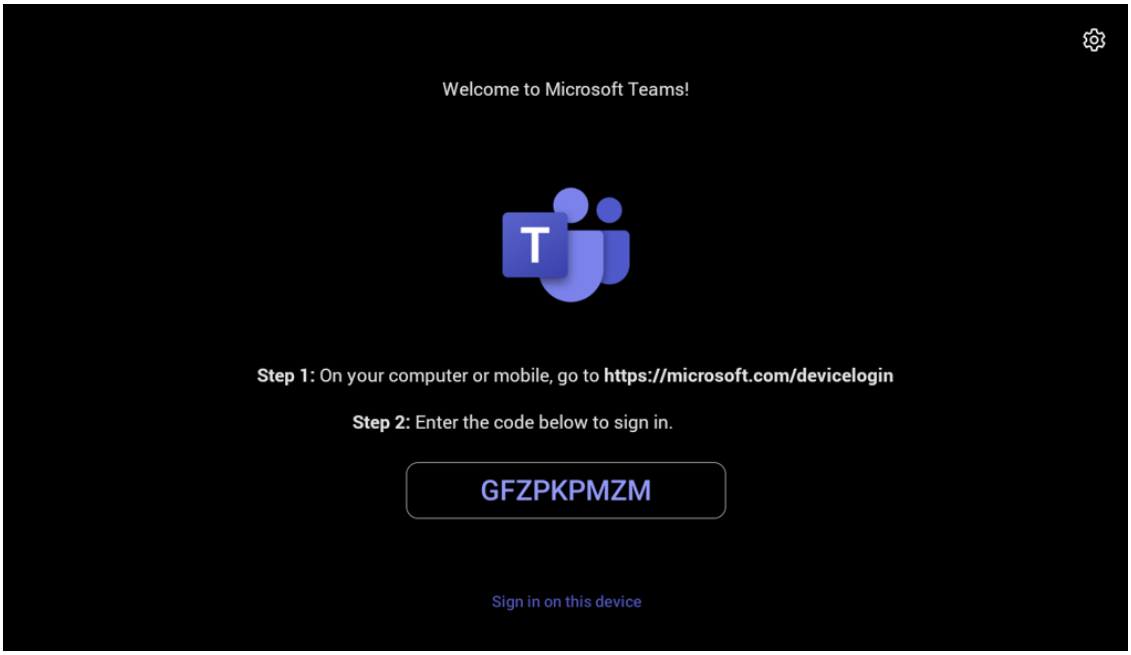
3. Select the relevant RXV200. The RX-PAD finalizes the pairing process and prompts you to select a bundle.



4. Select the bundle (see Bundles on page 2 for an explanation). The RX-PAD assigns the bundle with the RXV200 and prompts you to change the (default) admin password.



5. After this process is completed, the Microsoft Teams sign-in page is displayed on both devices, showing the code you need to sign into your Microsoft account.



6. On both devices, sign in to your Microsoft account.

If the device is not connected to a network during setup, a Network Configuration page is displayed after selecting the language, prompting you to set up the network before continuing with the wizard.

Pair RXV81 with RX-PAD

Customers that acquired an RXV81P-B10 bundle (see Bundles on page 2) need to pair the RXV81 with the RX-PAD (which is part of the bundle).

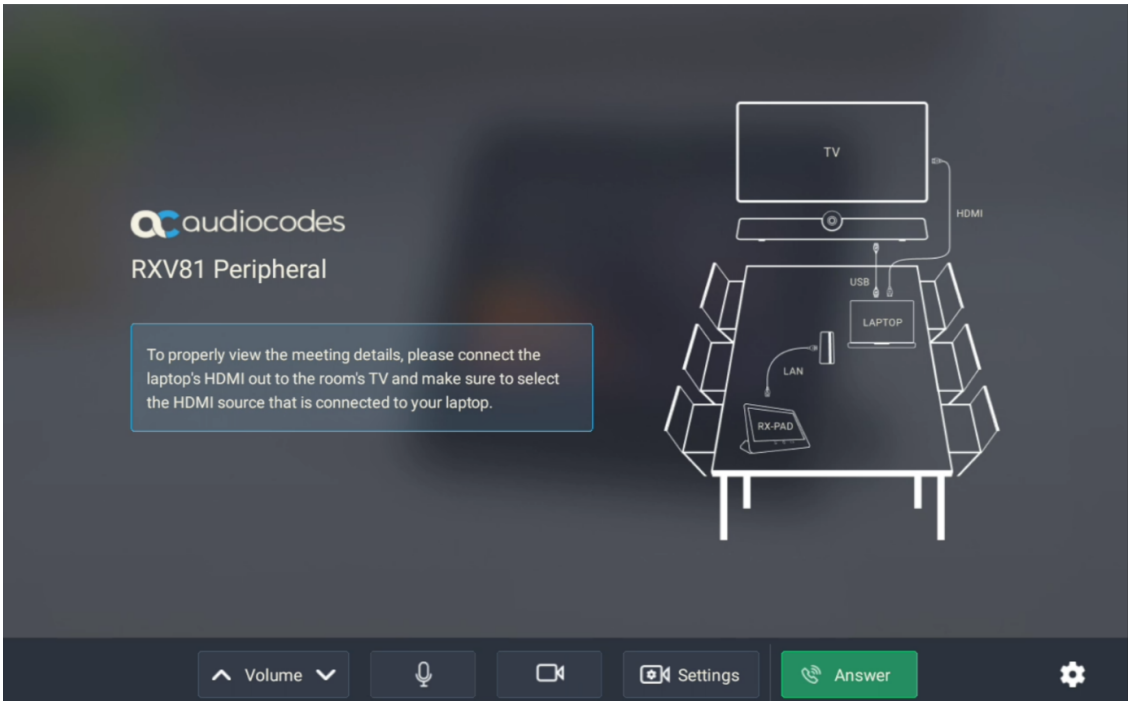
➢ Before pairing:

- 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:

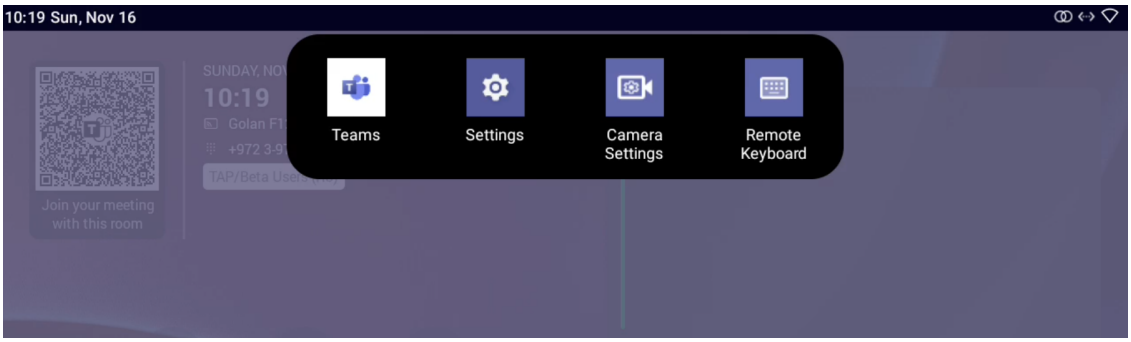
1. After connecting the RX-PAD and RXV81 to the network, the pairing process automatically begins.
2. Once pairing is complete, the RX-PAD displays the following:

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.



After Pairing

After pairing your RX-PAD with an RXV200 or RXV81 MTRA, 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 RX-PAD Operation

The following summarizes how to operate your RX-PAD.

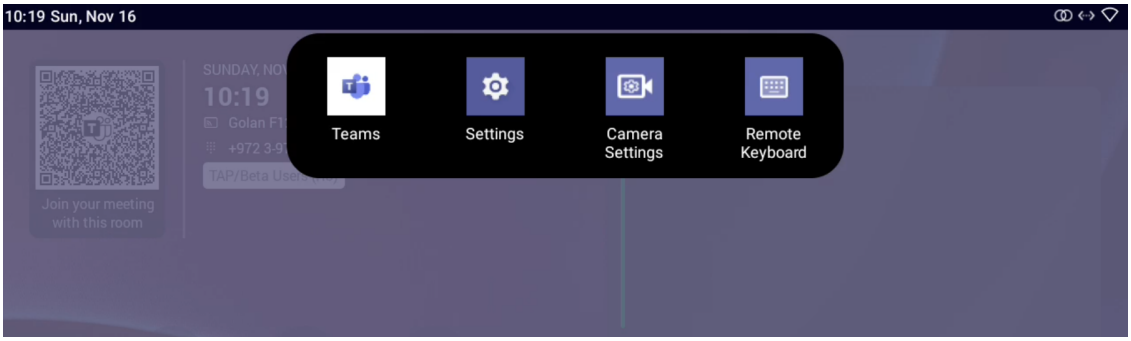
L-R	Description
1	Touch the back button to return to the previous screen.
2	Touch to return to the home screen or long-press to open the Device Settings page.
3	Touch to access the MTR's Camera Settings page.
4	Touch to open Microsoft Teams and the Device Settings menu.
5	Click to join a scheduled meeting.
6	Passive Infrared (PIR) motion sensor (hidden). When sensing motion, it wakes up RX-PAD from screensaver mode, automatically lighting up the screen to greet the user.
7	LED: ■ Solid red indicates in a meeting ■ Solid green indicates the RX-PAD is online and signed in

L-R	Description
	■ Flashing red indicates incoming invite to join a meeting
8	Drop-down menu to make it easy to open the RX-PAD application launcher. The new launcher enables accessing an app *with a single click*.

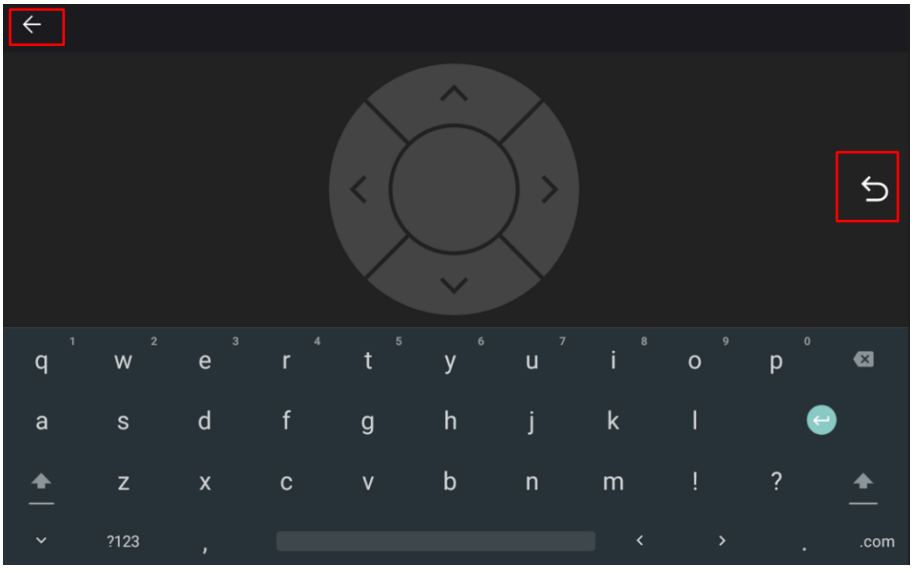
Operate RX-PAD with Remote Keyboard

➢ **To operate with the remote keyboard:**

1. After pairing your RX-PAD with the MTRA, scroll down in the RX-PAD to the menu tray:



2. Tap the **Remote Keyboard** option.



3. Enable touchscreen controls for remote control of the MTRA.
4. Use the RX-PAD's remote keyboard to:
   - Sign in to an MTRA
   - Toggle between the MTRA's Teams menus and device menus

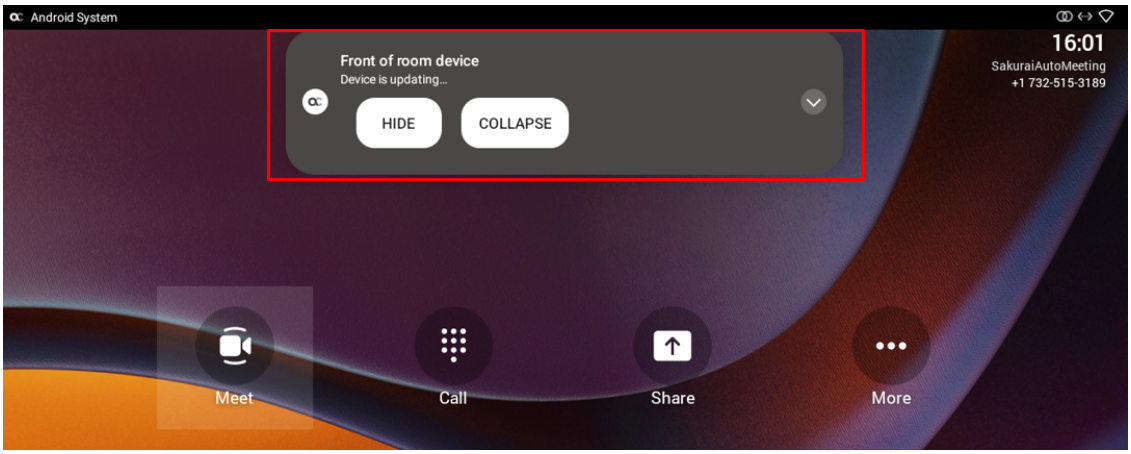
- Navigate to MTRA settings for adjustment of relevant features (such as Bundle selection, etc.)

5. Tap the right arrow indicated in the preceding picture to go back to the previous menu in the MTRA.
6. Tap the uppermost left arrow indicated in the preceding picture to exit Remote Keyboard mode.

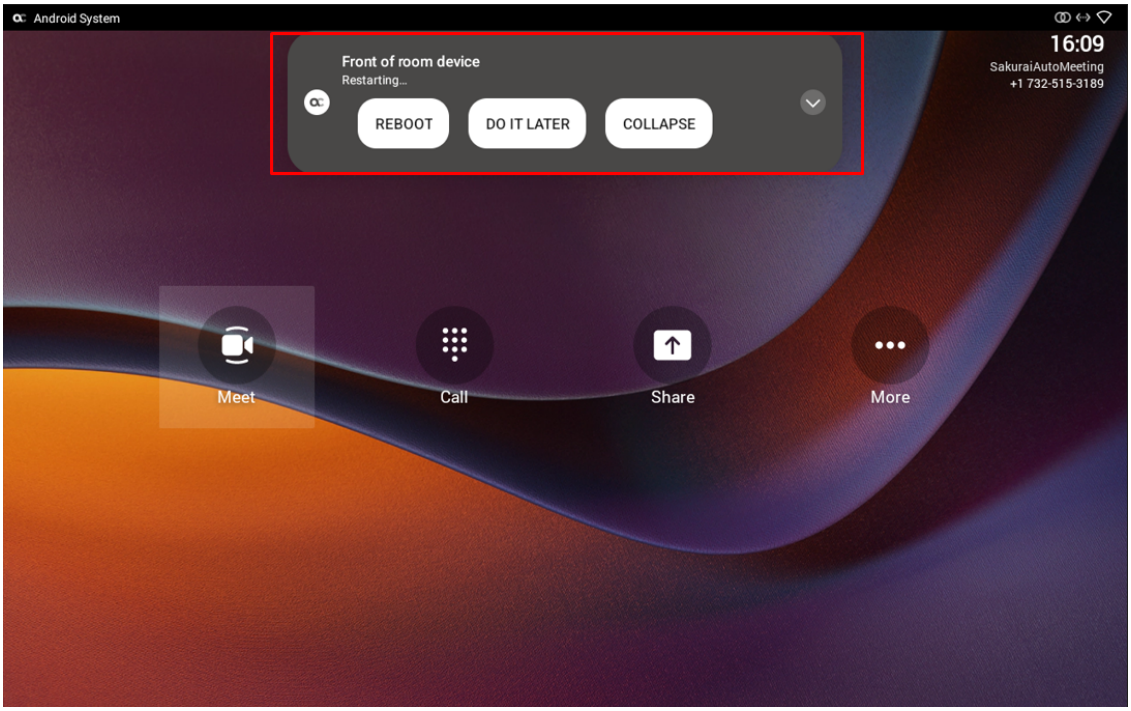
Manage Popup Messages

Popup messages displayed on the MTRA device are seamlessly mirrored in the bundled RX-PAD to enhance user interaction. When a message pops up in the MTRA GUI, the same is displayed in the RX-PAD. The feature streamlines user experience, allowing users to conveniently confirm messages directly from the RX-PAD and manage notifications intuitively and efficiently.

The following picture shows the popup message **Device is updating** on the RX-PAD.



If the alert is an action, you can perform the action using the RX-PAD, for example, **REBOOT** / **DO IT LATER** / **COLLAPSE**, as shown in the following picture.


Android System
16:09
SakuraiAutoMeeting
+1 732-515-3189
Front of room device
Restarting...
REBOOT
DO IT LATER
COLLAPSE
Meet
Call
Share
More

4 Meetings and Calls

This chapter describes how you can use your RX-PAD 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 30 and Composite AI Camera on page 46.

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 homepage.

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

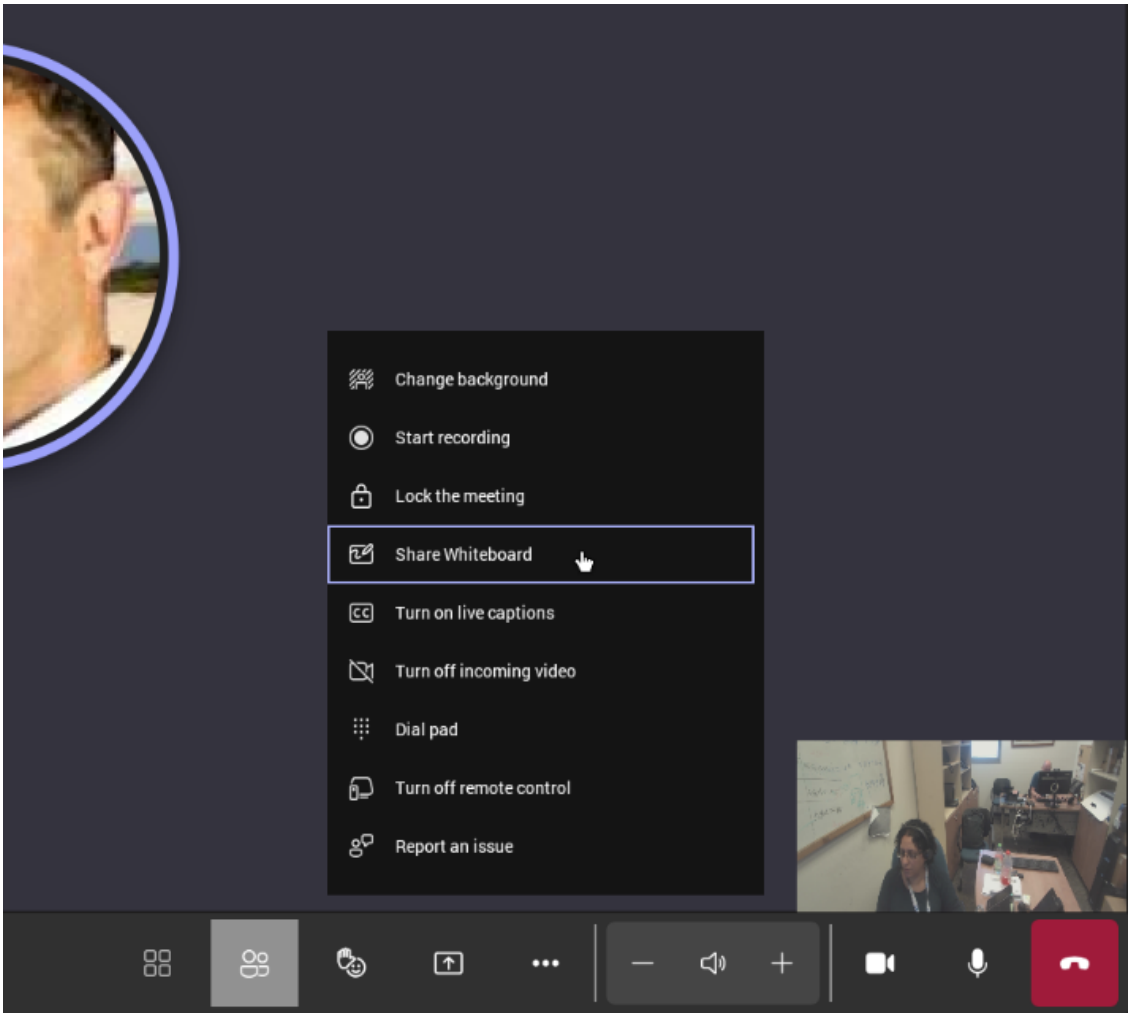
Ad-hoc meetings and calls can be conducted from the RX-PAD homepage in the same way as from a Teams channel. For details, see the relevant Microsoft Teams documentation.

Share a Microsoft Whiteboard

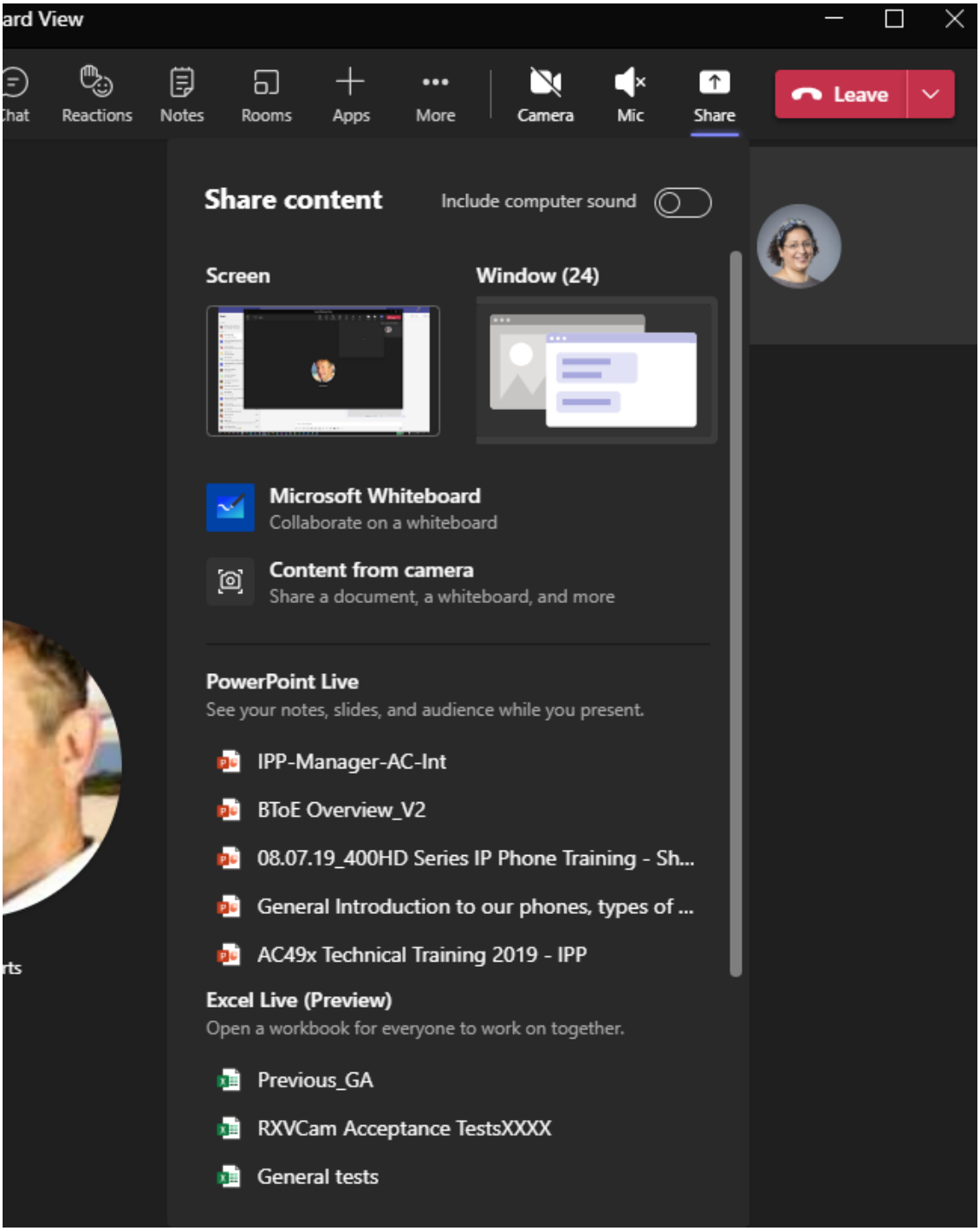
During Teams meetings, participants can open a virtual whiteboard – a digital canvas - on which they can sketch, illustrate, collaborate, brainstorm, plan, and share perspectives with one another in real time. The focus switches away from the presenting participant to the whiteboard. For more details,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



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

Screen Sharing

The RXV200 and RXV81 MTRAs enable 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.

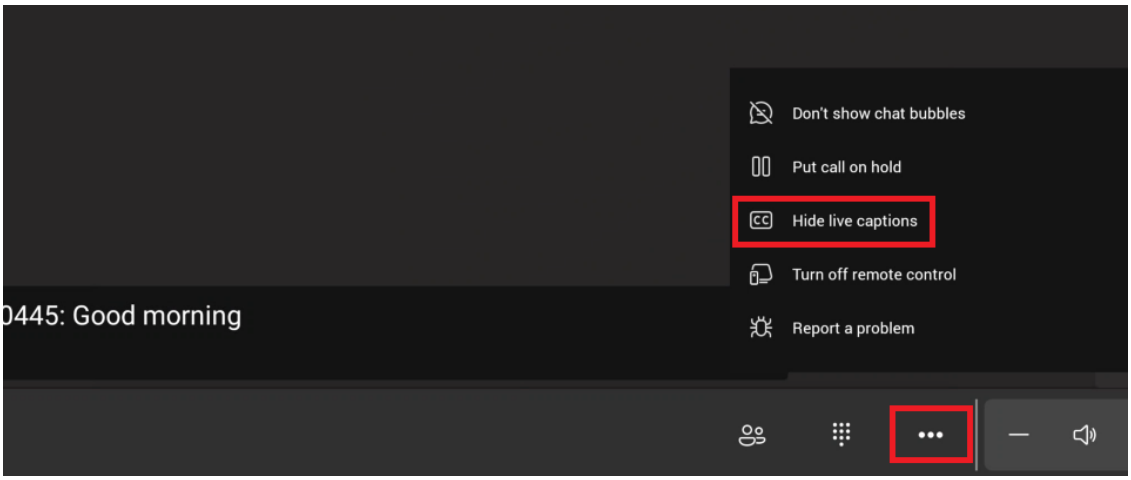
- **In-Meeting Mode:** When the MTRA is in a meeting, the presenter can use the Teams app 'Share' key to share their PC screen with in-person attendees who are physically present in the same meeting room, as well as with remote attendees. [Audio sharing is currently unsupported].
- **Idle Mode:** When 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 RX-PAD 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.



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**.

Hide Meeting Information

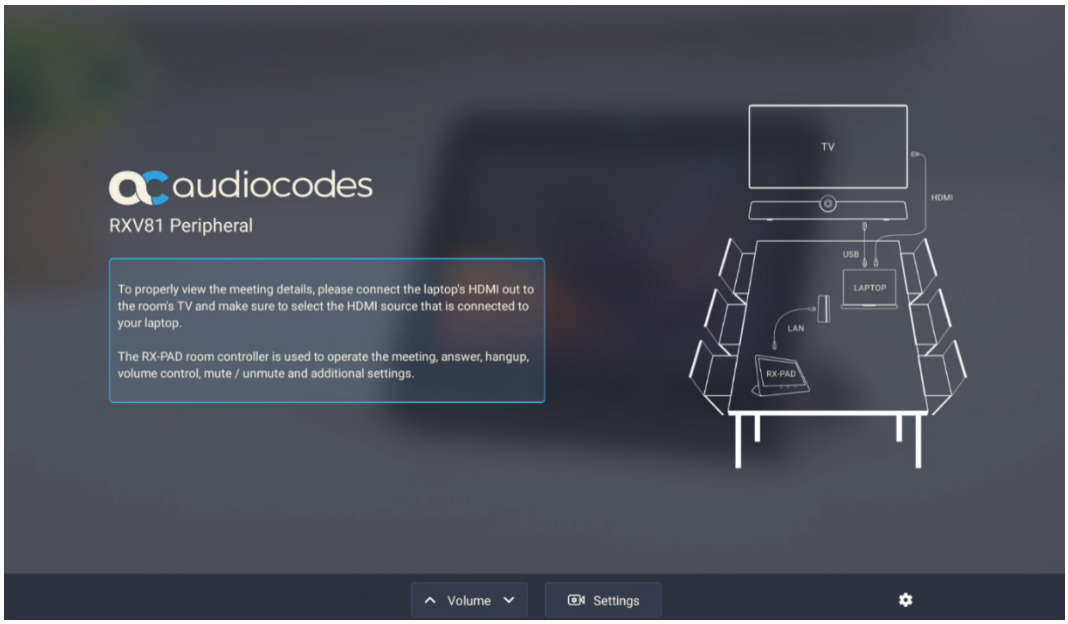
You can hide information such as meeting titles or chat bubbles via Teams, or from the RX-PAD as follows:

1. This feature requires Admin login. Navigate to 'Device Admin Settings' (see Access Device Admin Settings on page 69).
2. Scroll down and tap **Teams Admin Settings**, then navigate to **Teams Admin Settings > Meetings**.
3. Tap to show or hide the relevant option.

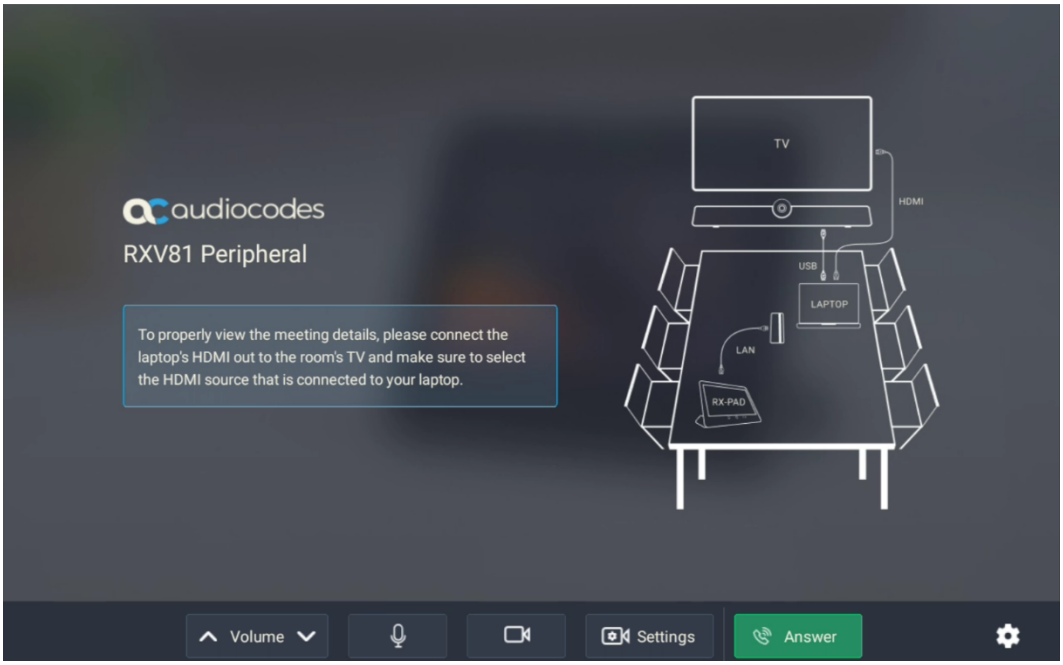
You can show and hide meeting information by default or during a specific meeting via Teams. For details, refer to the relevant Microsoft Teams documentation: Hide Attendee Names in Microsoft Teams Meetings and Chat in Microsoft Teams Meetings.

5 Ad Hoc Mode on RXV81 MTRA

RXV81 MTRA and RX-PAD Controller support ad hoc peripheral mode. When RXV81 MTRA is connected via USB to a PC/laptop, it automatically moves to ad hoc peripheral mode and the following is displayed on the RX-PAD:



When a call comes in, the RX-PAD displays the incoming call's functions as follows:



6 MTRA Camera Settings

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

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 contains settings related to the camera or cameras connected to your RXV200 or 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

If your MTRA uses a combination of cameras, settings are set up independently for each camera. To set up a display integrating these cameras for most efficient use, specify a *Composite AI* layout (see Composite AI Camera on page 46).

Temporary and Permanent Settings

➢ Presets

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.

➢ 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 69).

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

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

- Temporary Presets below
- Permanent Presets on page 33

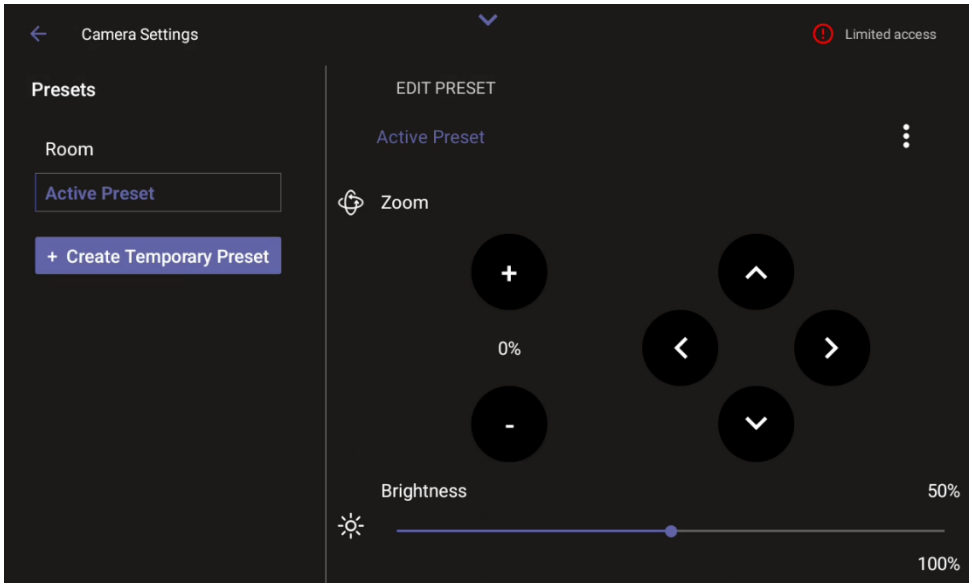
It is recommended to have permanent presets configured for locations frequently zoomed in and focused on, such as:

- 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

➢ 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.

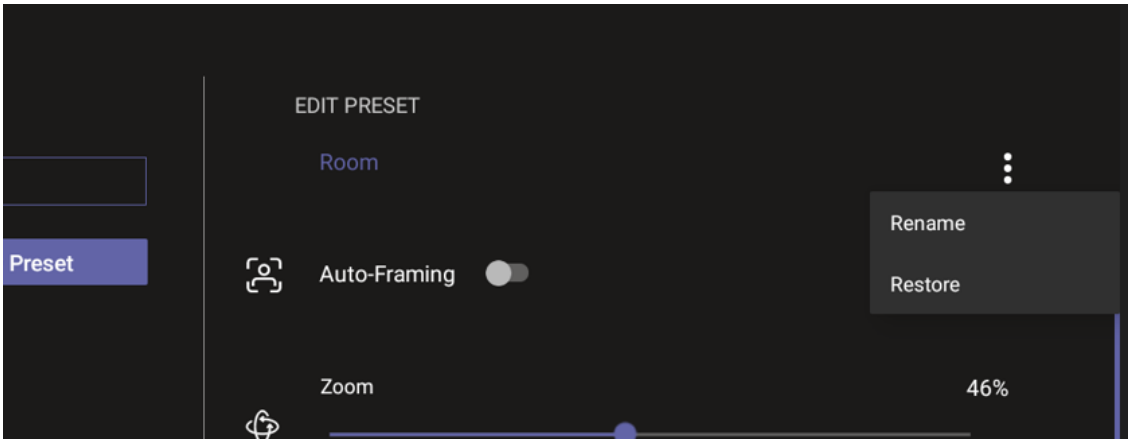
If the user has Admin permissions, the button is labeled **Create New Preset**. In this case, the generated preset will be permanent.

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.

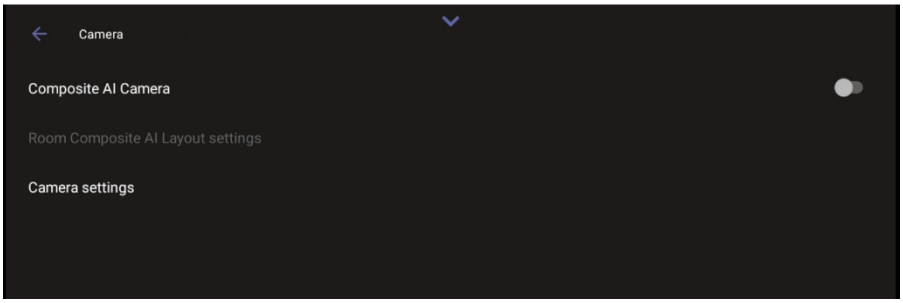


Camera settings can be changed during a meeting without turning off the video to remote parties.

Permanent Presets

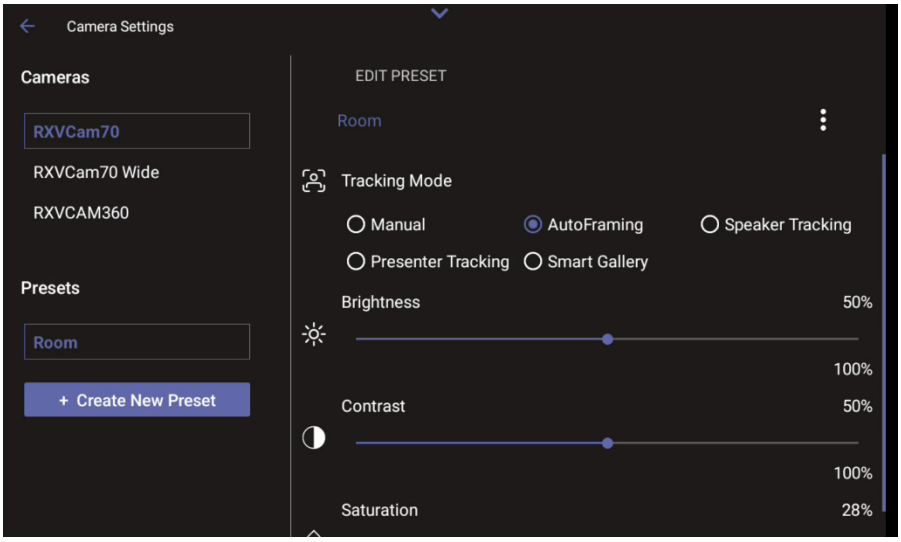
In idle mode, Admins can create new permanent presets and permanently change existing presets:

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 69).
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.

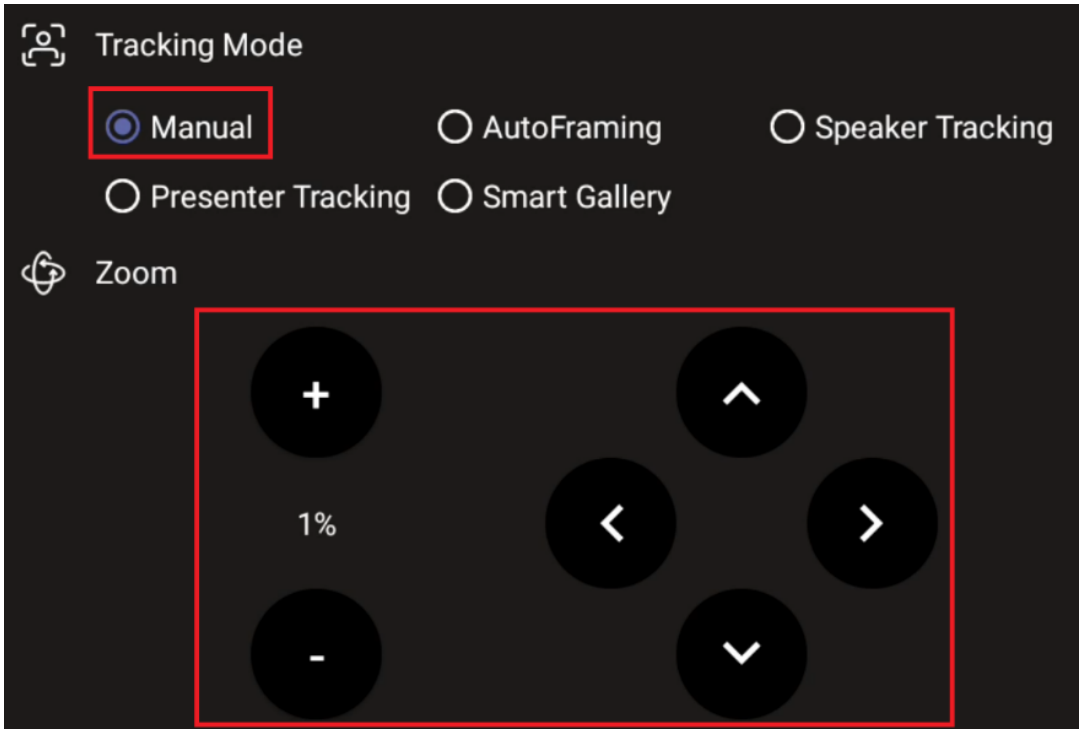


5. [Optionally] Tap the vertical ellipsis and then from the pop-up menu select the **Rename** option to change the name of the preset.
6. [Optionally] Tap the vertical ellipsis and then from the pop-up menu select the **Restore** option to return camera settings to their defaults.

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.



- 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

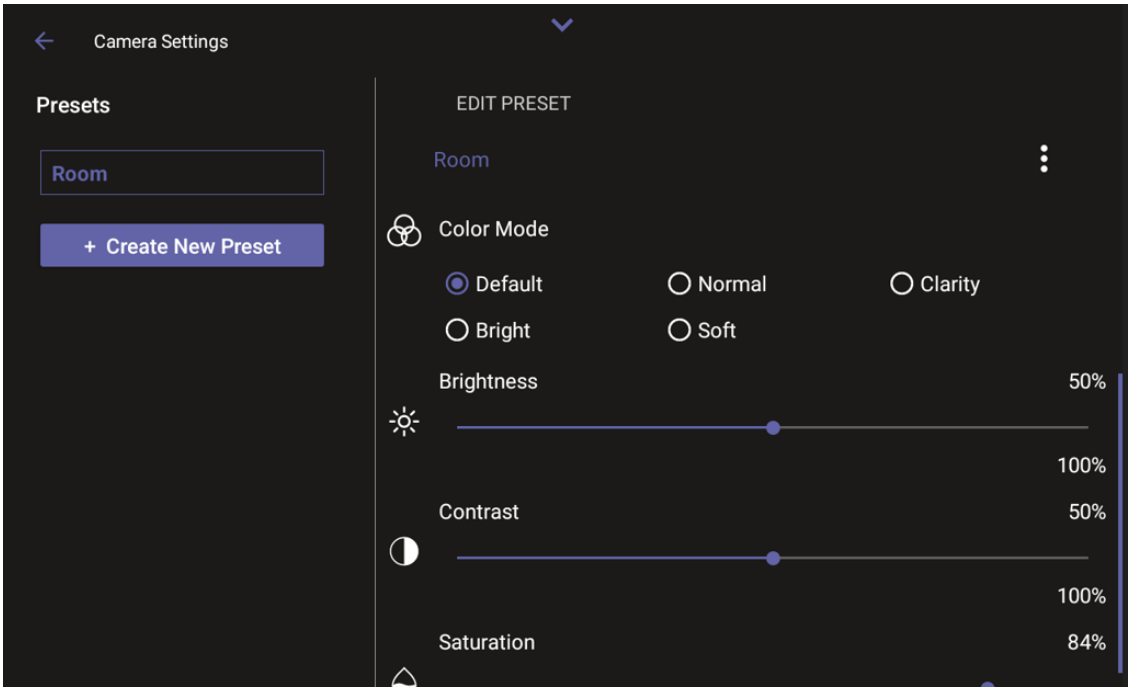
Each connected camera comes with default Brightness, Contrast, and Saturation properties. You can adjust them as required.

With an RXVCAM50 camera, you can also select a Color Mode (see Configure a Color Mode Preset on the RXVCAM50 Camera below).

Configure a Color Mode Preset on the RXVCAM50 Camera

When RXV200 is connected to the AudioCodes RXVCAM50 camera, you can configure a Color Mode preset from RX-PAD.

Regular users can only create temporary presets during ongoing meetings. These presets are automatically deleted at the end of the meeting.
To permanently configure the default Room preset or create permanent presets, you need to be logged in as admin (see Access Device Admin Settings on page 69).



Users can configure either of the following options:

Color Mode	Attributes
Default	Brightness - 50, Contrast - 50, Saturation - 70
Normal	Brightness - 50, Contrast - 50, Saturation - 70
Clarity	Brightness - 60, Contrast - 50, Saturation - 60
Bright	Brightness - 50, Contrast - 50, Saturation - 70
Soft	Brightness - 50, Contrast - 50, Saturation - 60

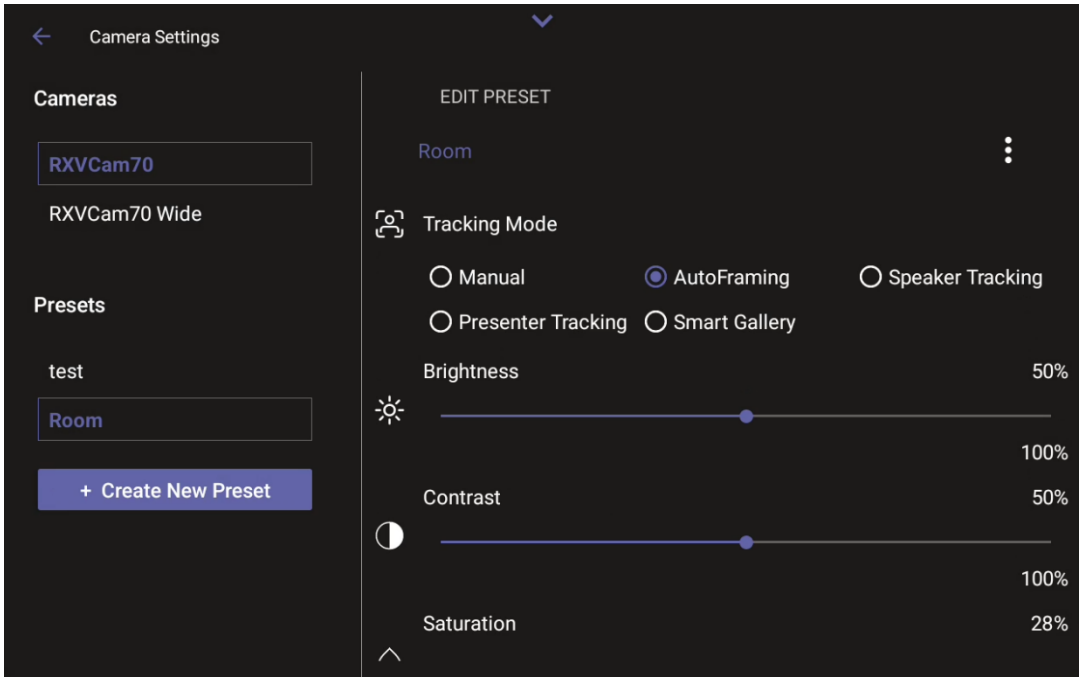
Select RXVCam70 Camera Tracking Mode

Regular users can only create temporary presets during ongoing meetings. These presets are automatically deleted at the end of the meeting.
To permanently configure the default Room preset or create permanent presets, you need to be logged in as admin (see Access Device Admin Settings on page 69).

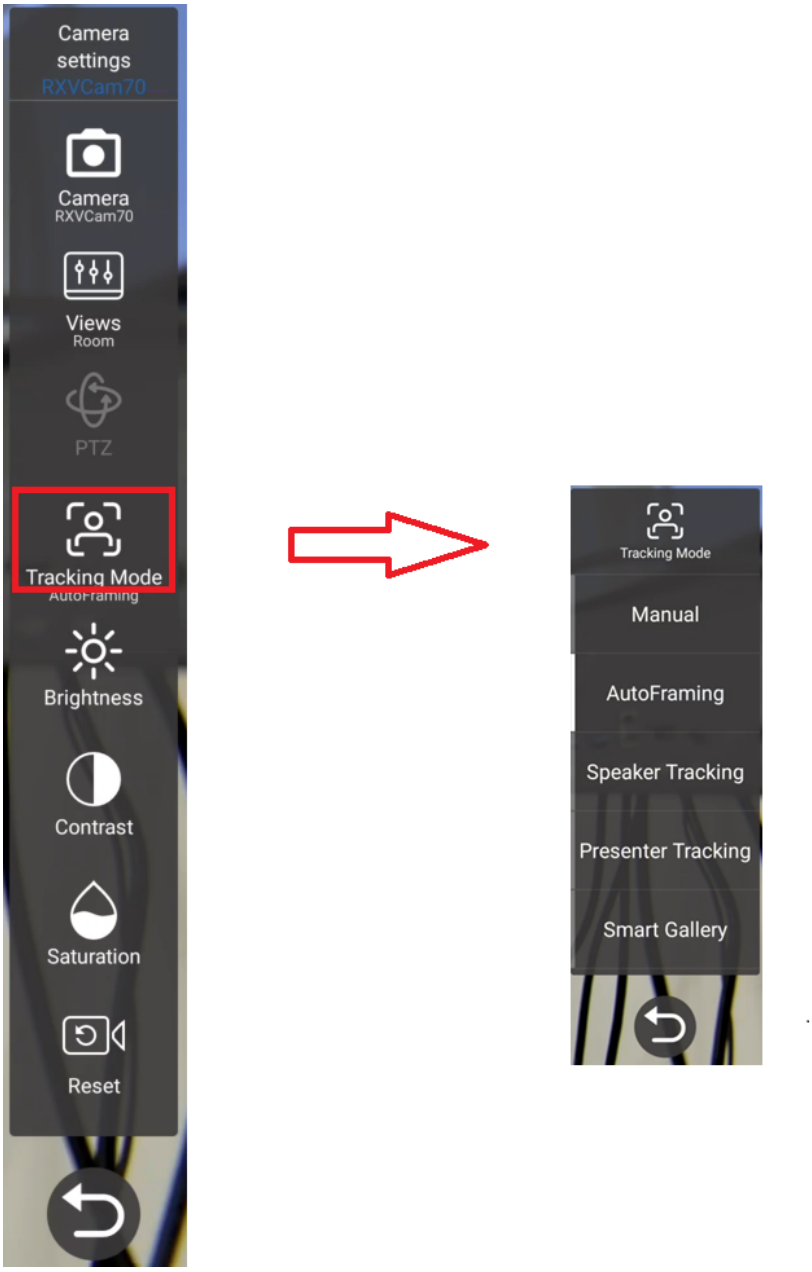
➢ To select a Tracking Mode:

1. Do *either* of the following:

   - From your RX-PAD, open the Edit Preset page (**Camera Settings > Room > Edit Preset**).



   - From your RXV200, navigate to the camera display (via Camera Settings) and tap the **Tracking Mode** option on the vertical toolbar.



2. Select one of the following RXVCam70 camera tracking mode options:
   - Auto Framing (default), also known as Group Framing
   - Manual
   - Speaker Tracking
   - Presenter Tracking
   - Smart Gallery

   See the next step for a description of each tracking mode.
3. Use the following descriptions as a reference when configuring a tracking mode:

Group Framing (Auto Framing)

[Supported by RX-PAD Camera Settings]

Default mode

Automatically detects and frames all the participants in the room.

Effective distance: 8m

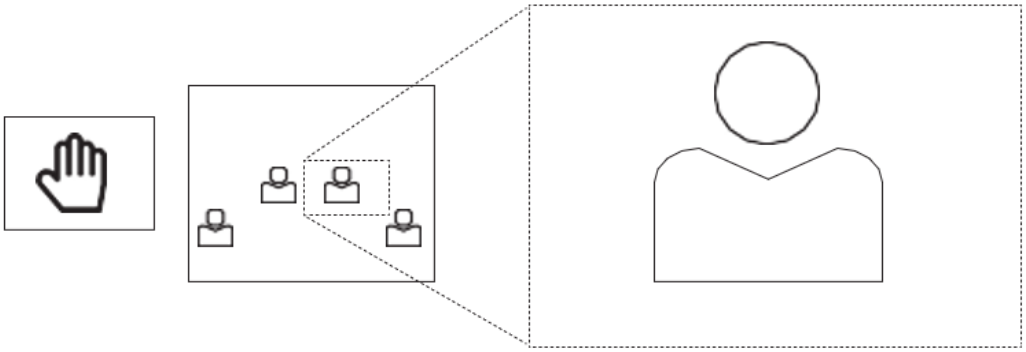
Manual

Select this option to manually adjust the Zoom, Tilt or Pan.

In RX-PAD's 'Camera Settings' page, use the sliders to set Zoom, Tilt or Pan.

Using the RCU, after selecting an area to display, zoom in | out, move up | down, and move left | right.

This mode does not have AI functions.



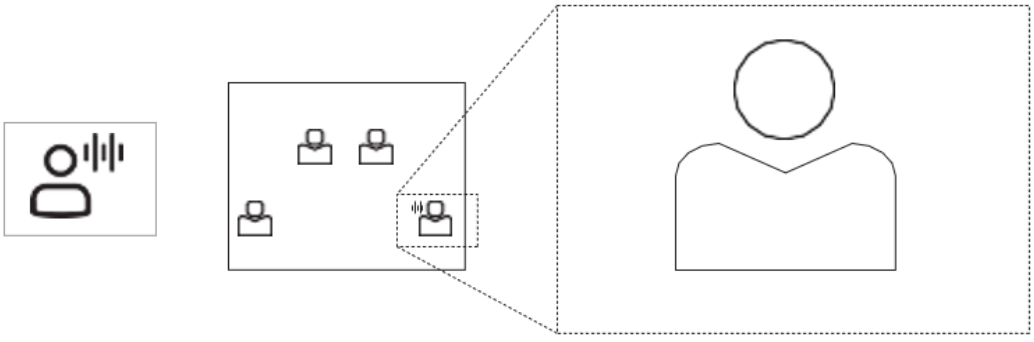
Speaker Tracking

Select this option to manually adjust the Zoom, Tilt or Pan.

Automatically tracks speakers who speak continuously for 3-5 seconds

Focuses on the speaker (displays them close-up allowing participants to focus more)

Effective distance: 6m

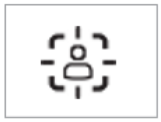


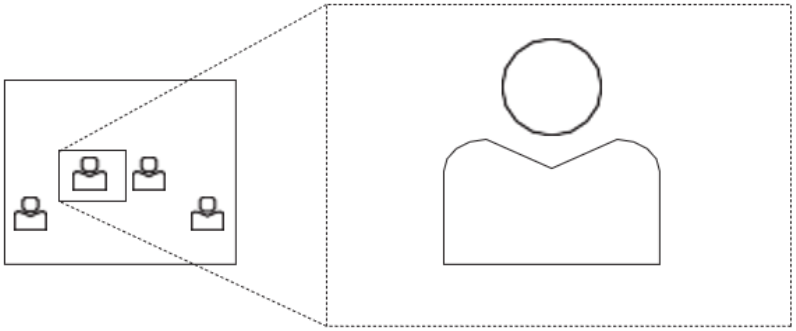
Presenter Tracking

Automatically identifies and tracks the position of the presenter to ensure that that person remains centered.

Press the left and right keys to select the target to track.

Press **OK** to choose the target.





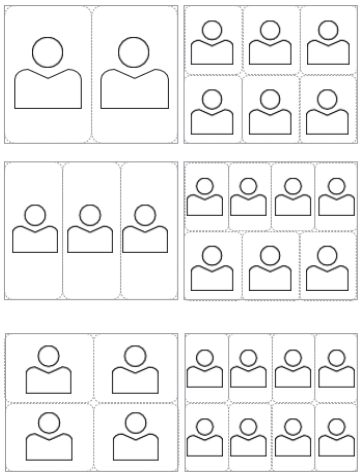
Smart Gallery

Automatically identifies up to 18 people

Automatically lays out the display

When a person moves, the camera automatically tracks them and keeps them centered

Switching from one person to another is accompanied by dynamic effects of entry and exit



Select RXVCam360 Camera Tracking Mode

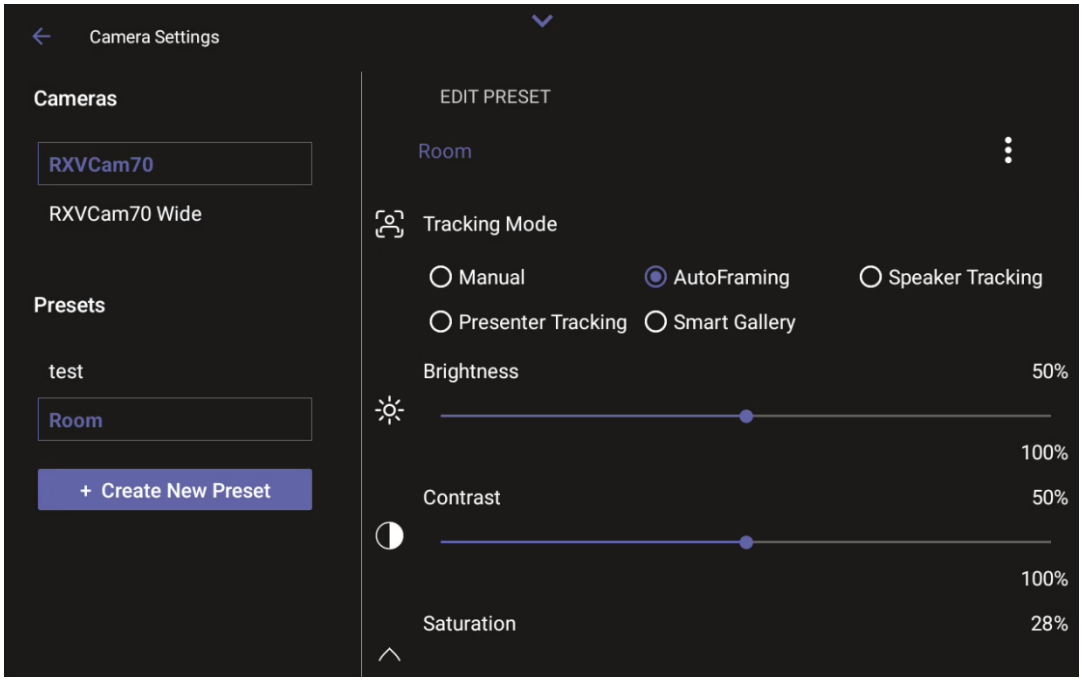
Regular users can only create temporary presets during ongoing meetings. These presets are automatically deleted at the end of the meeting.

To permanently configure the default Room preset or create permanent presets, you need to be logged in as admin (see Access Device Admin Settings on page 69).

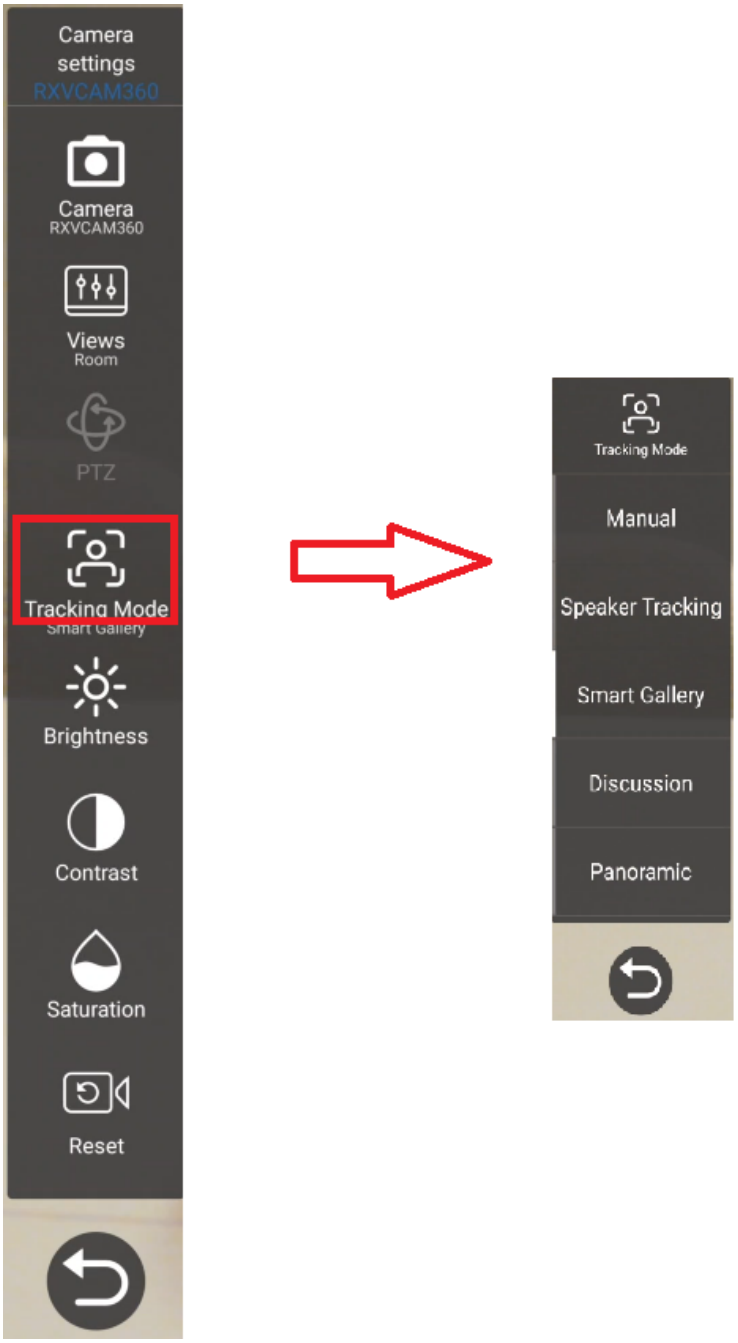
➢ **To select a Tracking Mode:**

1. Do *either* of the following:

- From your RX-PAD, open the Edit Preset page (**Camera Settings > Room > Edit Preset**).



- From your RXV200, navigate to the camera display (via Camera Settings) and tap the **Tracking Mode** option on the vertical toolbar.



2. Select one of the following RXVCam360 camera tracking mode options:
   - Smart Gallery (default)
   - Manual
   - Speaker tracking
   - Discussion
   - Panoramic
3. Use the following descriptions as a reference when configuring a tracking mode:

Smart Gallery

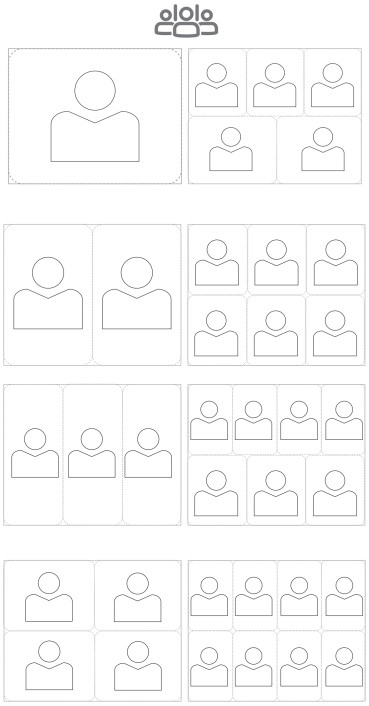
Recommended

Automatically identifies up to 18 people

Puts each in a dedicated frame

Maximum: 8 frames

When a person moves, the camera automatically tracks and keeps their head centered



Manual

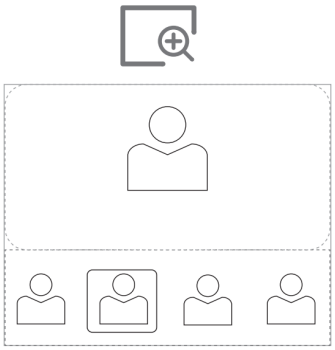
Select an area to focus on

Use the remote controller to zoom in and out (five levels) and move up, down, left and right to select a focused area.

The selected area has a fixed 16:9 aspect ratio.

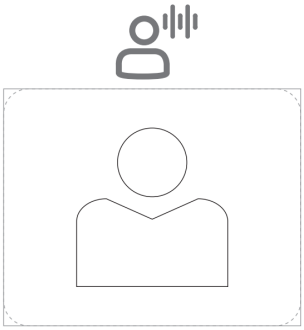
This mode does not have AI functions.

This mode is currently available only when using the PC.



RXVCam360 follows the active speaker and automatically switches from the previous speaker to the next speaker within three seconds.

Speaker Tracking



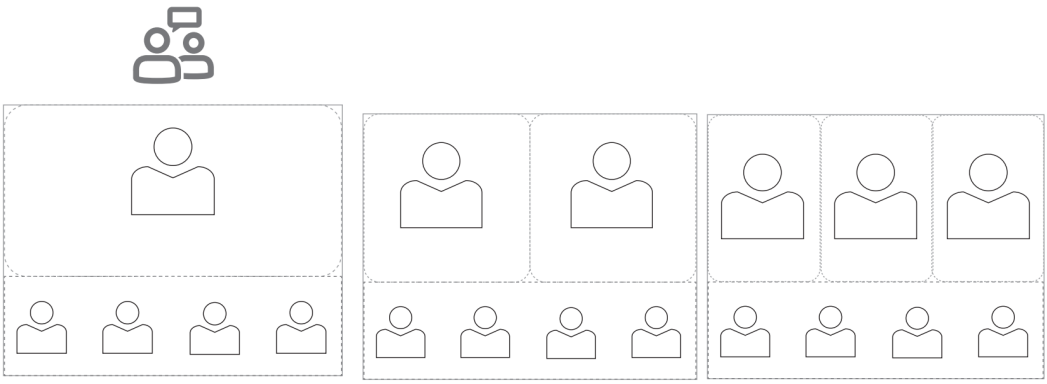
Discussion Mode

The lowermost panel displays a 360° panoramic view.

The second level displays an automatic layout of 1-3 speakers.

- Only the person speaking is displayed.
- Those not speaking are not displayed.

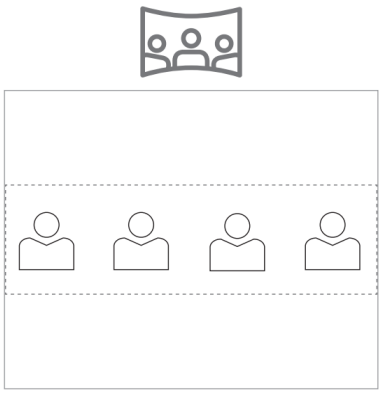
For using this mode with Composite AI, see Enable RXVCam360 Discussion Mode with Composite AI on page 49.



Panoramic Mode

360° panoramic high-definition view

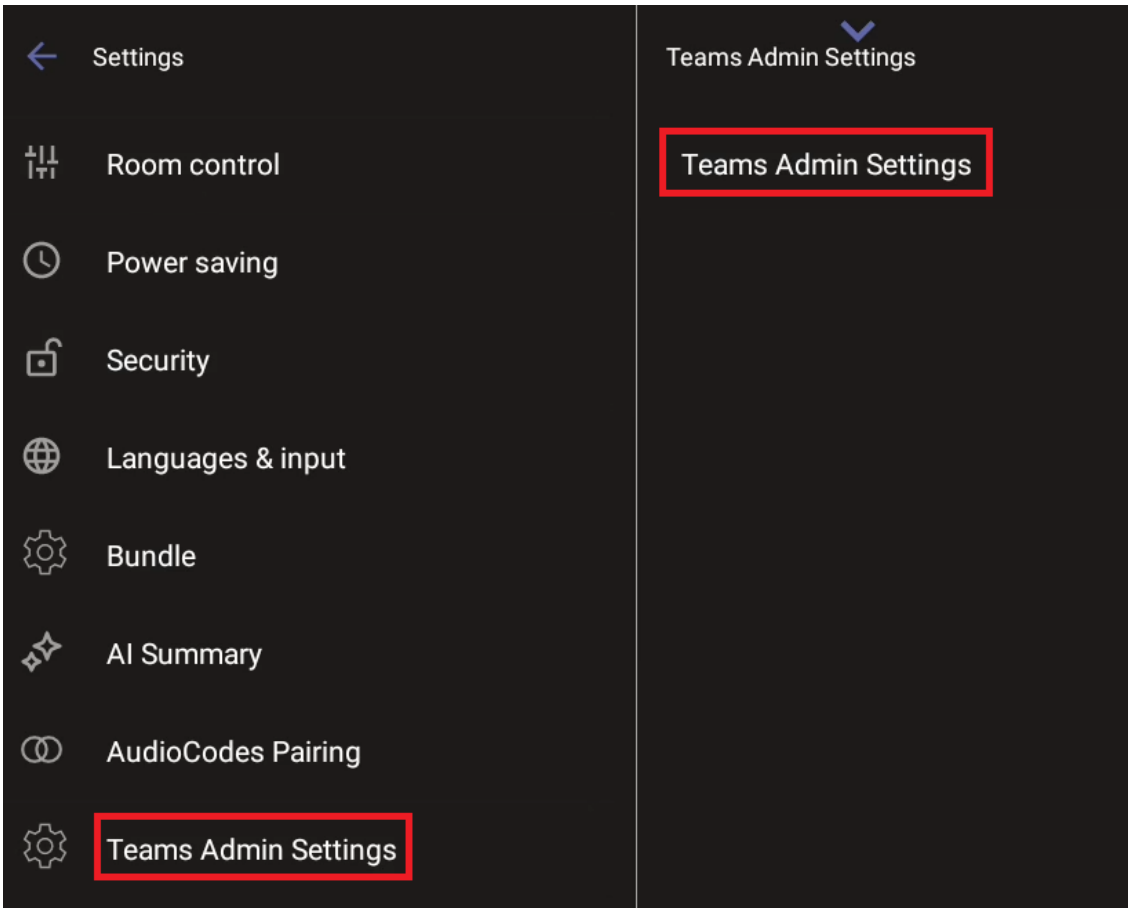
This mode does not have AI functions



Configure Camera Teams Settings from the RX-PAD

Admins can set up a camera's Teams- related settings from the RX-PAD. To do this:

1. If not already logged in, log in to Device Administration to get admin access (see Log in to Device Administration on page 69).
2. Under 'Device admin settings', scroll down and tap **Teams Admin Settings**.



3. Tap **Teams Admin Settings** and configure camera settings as required.

Alternatively, you can access these settings from the Teams Admin Center (TAC). For details, see the Microsoft Teams documentation.

The 'Teams Admin Settings' option is only available in the RX-PAD Device Admin Settings if you access settings if its navigation is Teams originated. Consequently:

- If you access Settings by tapping **More** on the RX-PAD homepage and then tapping **Settings > Device Settings**, the 'Teams Admin Settings' option will appear in the Settings sidebar menu.
- If you access Settings via the pull-down menu tray, the 'Teams Admin Settings' option will not appear.

7 Composite AI Camera

The RXV200 supports composite AI camera technology. **Composite AI** enhances video conferencing by intelligently combining streams from two cameras into a single, seamless layout. This innovation ensures remote participants gain an optimized and immersive view of the meeting room and its participants.

This feature applies to the following setups:

- **RXV200 with RXVCam70:** Utilizes the dual cameras of the RXVCam70: the wide-angle camera (full-room view) and the mechanical camera (Smart Gallery mode).
- **RXV200 with RXVCam360 and RXVCam50:** Combines streams from the RXVCam50 (full-room view) and RXVCam360 (Smart Gallery mode).
- **RXV200 with RXVCam360, RXVCam70 wide-angle camera, and RXVCam70 PTZ camera:** Combines the RXVCam360 (Smart Gallery) and the RXVCam70 wide-angle camera (full-room view) streams with the RXVCam70 PTZ stream to support speaker tracking.

Key capabilities:

- **Enhanced room visibility:** Provides a comprehensive view of the meeting room capturing all participants clearly.
- **Intelligent Layout:** Automatically arranges the combined streams into a cohesive and intuitive layout.
- **Manual Layout adjustment:** Allows users to resize room view and enable or disable room view or smart gallery.
- **Adjustment of Individual Camera Settings:** Allows users to adjust each individual camera, for example, brightness and saturation, without leaving the Room Composite AI Layouts.
- **Speaker tracking and presenter tracking:** The camera automatically tracks the speaker or presenter if the person moves. The presenter is either identified by the system as the first speaker or manually selected.

Composite AI is disabled by default.
Changing the Composite AI settings (layout, enabling/disabling Smart Gallery, or Room View) in idle state (no active meeting) can only be done by the Admin. During an active Teams meeting, both admin and non-admin users can change the Composite AI settings. Once the meeting ends, these settings automatically revert to the system's pre-configured defaults.
During a meeting, only the admin can disable the Composite AI mode.

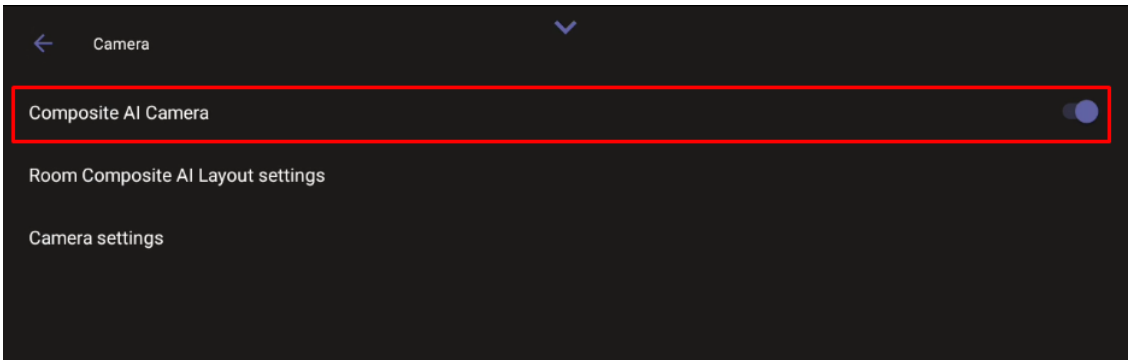
Set up Composite AI

➢ **To enable and set up composite AI:**

1. Do either of the following:

- On the RX-PAD, touch the camera hard key below the screen.
- Swipe down to display the main menu tray, then tap the **Camera Settings** option.

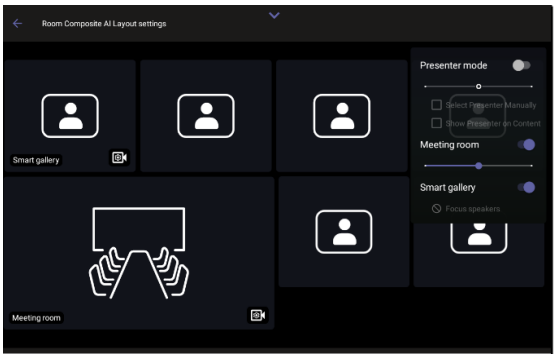
2. Tap the **Composite AI Camera** toggle button so that it is on:



On the screen to which the RXV200 is connected, a pop-up message appears, indicating that the Composite AI camera is connected.

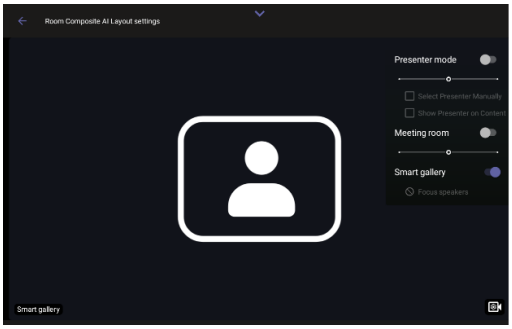
3. Tap **Room Composite AI Layout Settings** to choose the layout.

The connected camera stream opens. On RX-PAD, the layouts are displayed as shown in the following figure:

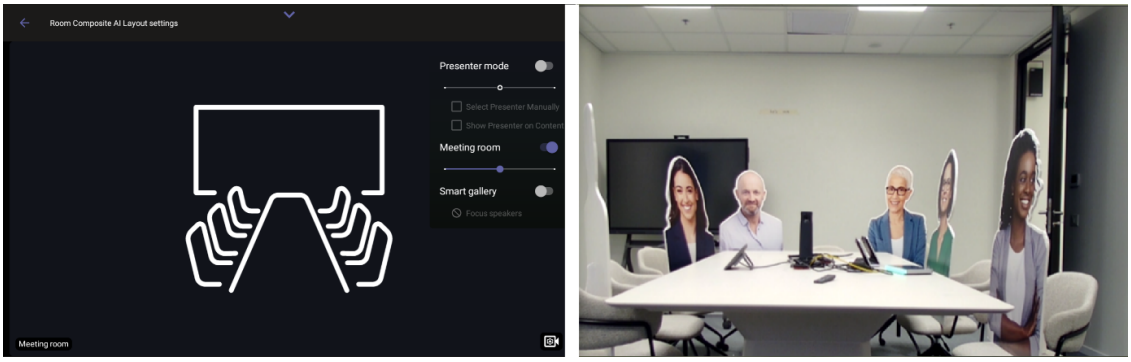


In the RXV200 screen (when RXV200 is connected to RXVCam70), the main camera is in the center of the screen and the wide-angle camera at the lowermost left.

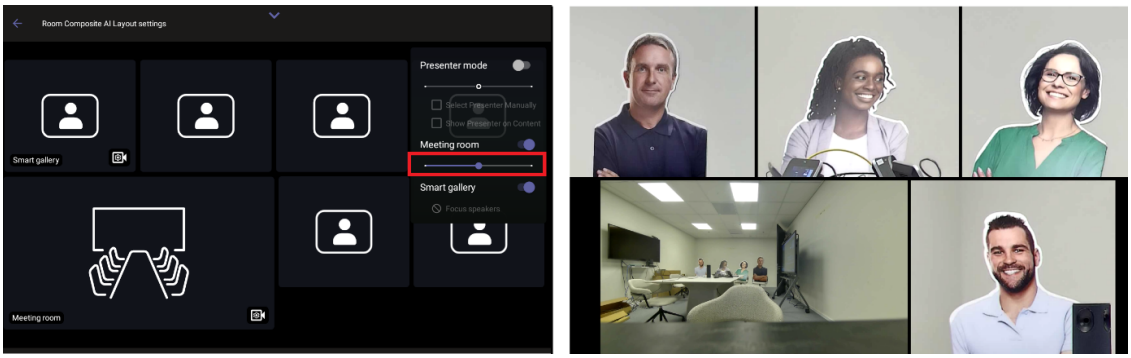
4. Disabling **Meeting room** closes the wide-angle camera and centers the main camera feed in the screen.



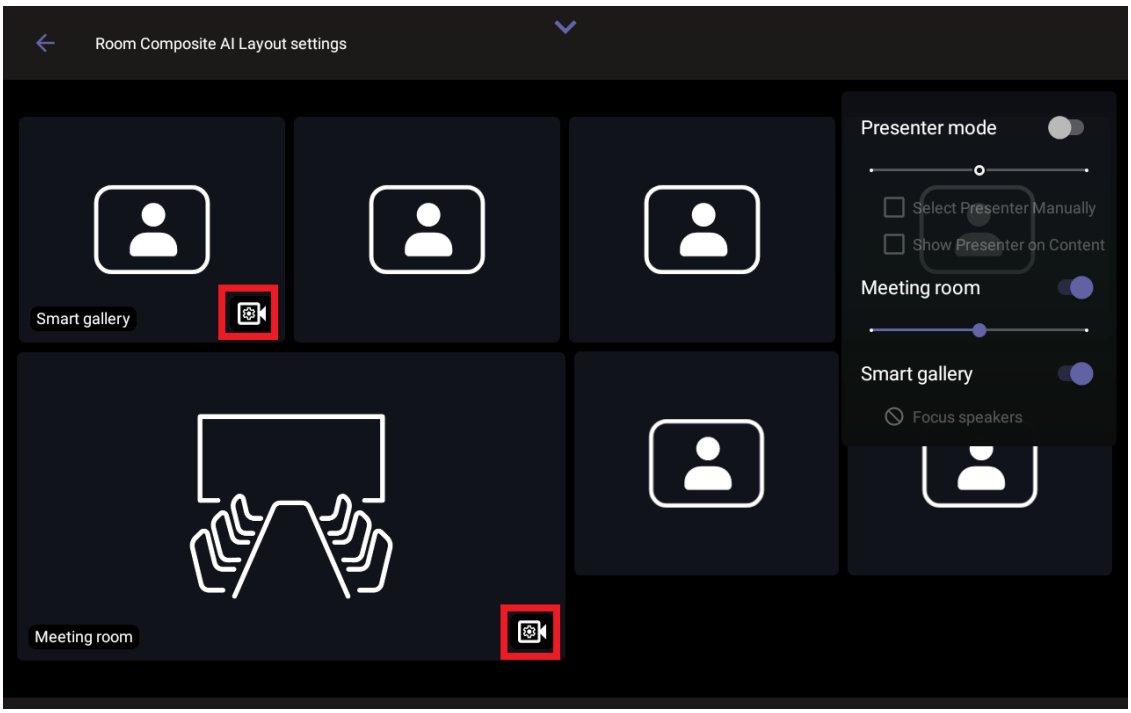
5. To close the main camera and center the wide-angle camera feed in the screen, disable the **Smart gallery**.



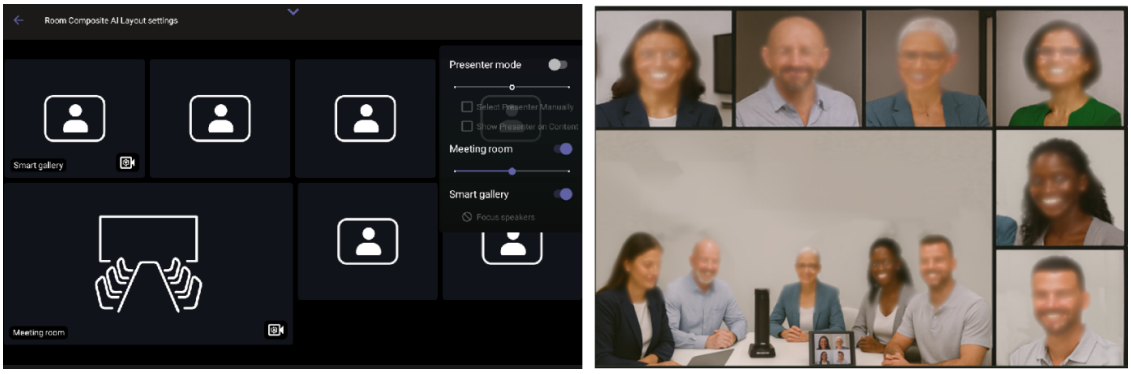
6. Use the scaling bar shown in the following figure to control the ratio between the main camera size and the wide-angle camera size; move the slide bar to adjust the size of the **Meeting room** view accordingly.



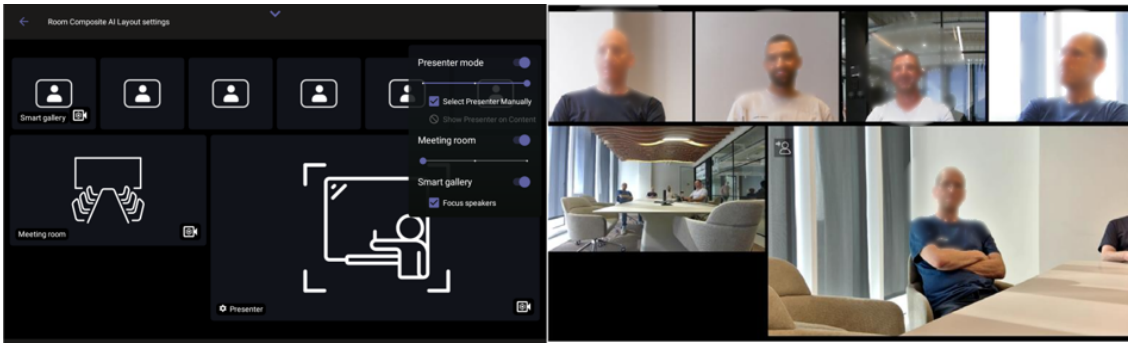
7. To adjust the settings (e.g., brightness and saturation) of a specific camera, click its  icon:



When connected to the RXVCam360 and RXVCam50 cameras, the following screen displays:



When connected to the RXVCam360 and RXVCam70 (RXVCam70 combining both wide-angle camera and PTZ camera), the following screen is displayed:



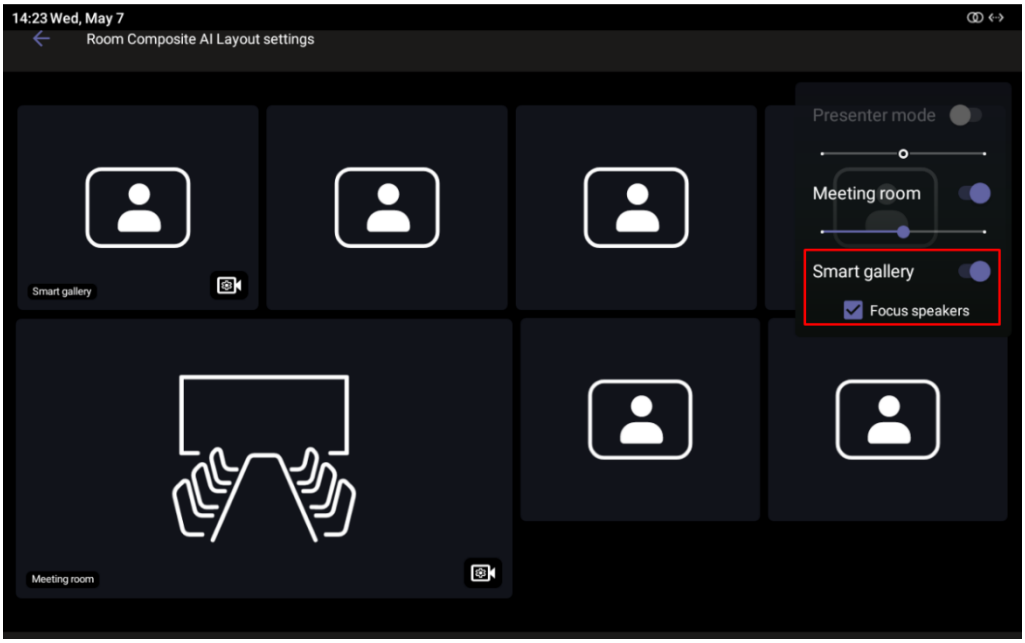
Enable RXVCam360 Discussion Mode with Composite AI

This feature enhances the Smart Gallery view in Composite AI rooms by prioritizing active speakers, displaying them in larger tiles instead of equal-sized frames for all participants.

➢ **To enable this:**

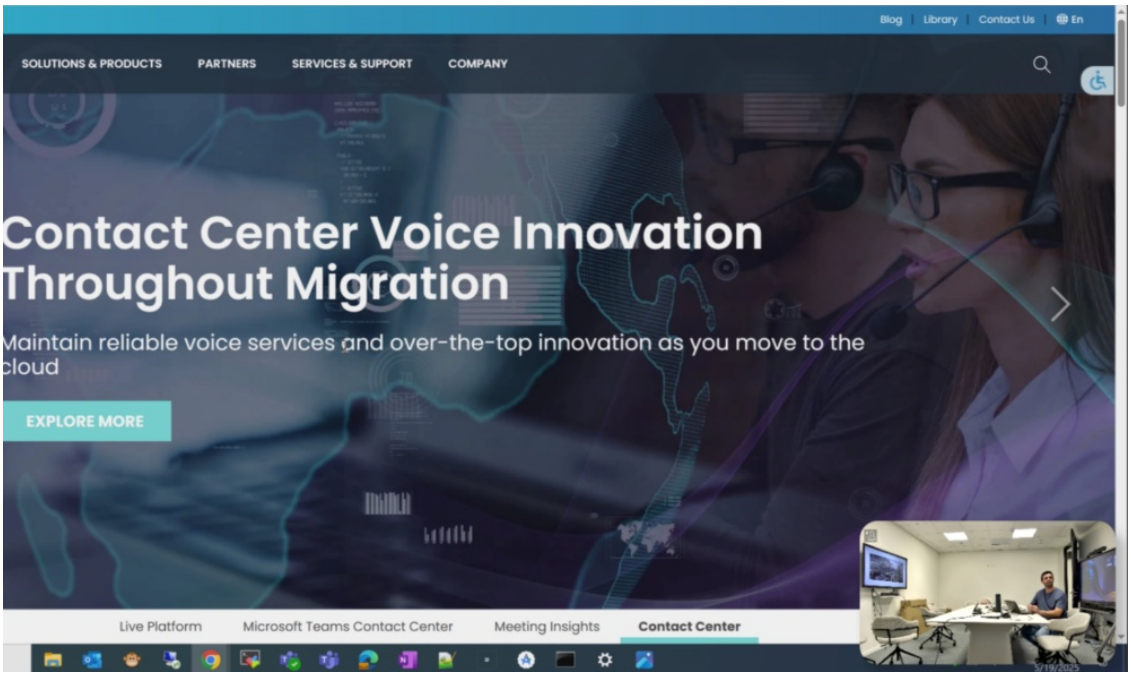
1. Navigate to the Composite AI Layout Settings page (see Set up Composite AI on page 46).
2. Turn on 'Smart gallery' and select the **Focus Speakers** option.

> For non-supported cameras (e.g., RXVCam70), the Focus Speakers option is grayed out.



Show Presenter on Content (Supported with RXVCam70)

This feature allows presenters to be the focus during content sharing. It uses the RXVCam70 PTZ camera's **Speaker Tracking** to keep the presenter in focus and overlays their video feed in the bottom-right corner of the screen during presentations.

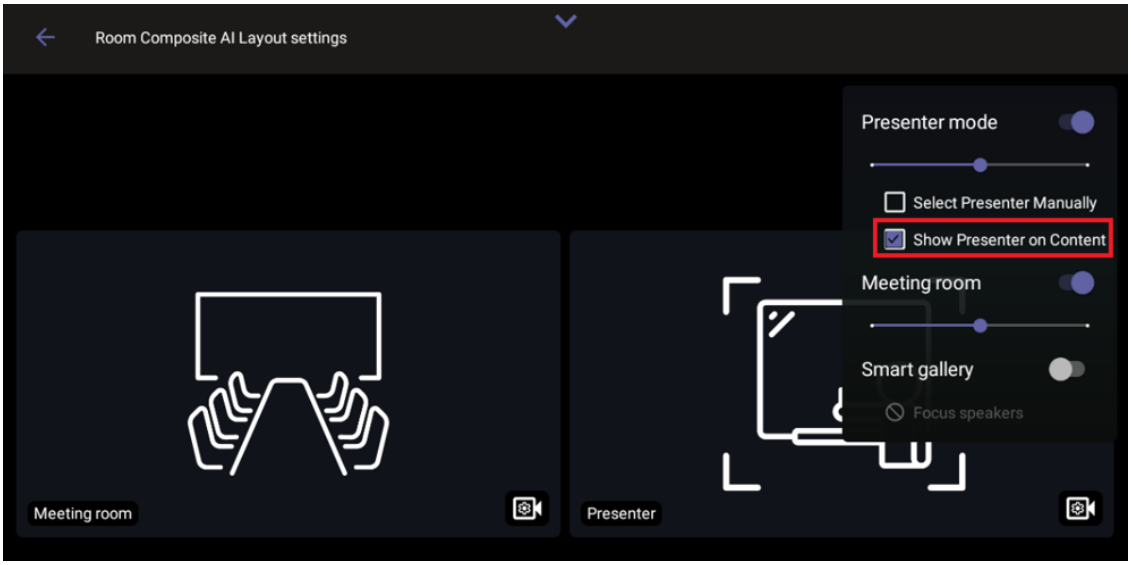


This feature can be toggled on/off via the RX-PAD using the Show Presenter on Content setting under Composite AI mode.

➢ **To enable this:**

1. Navigate to the Composite AI Layout Settings page (see Set up Composite AI on page 46).

2. Turn on 'Presenter mode' and select **Show Presenter on Content**.



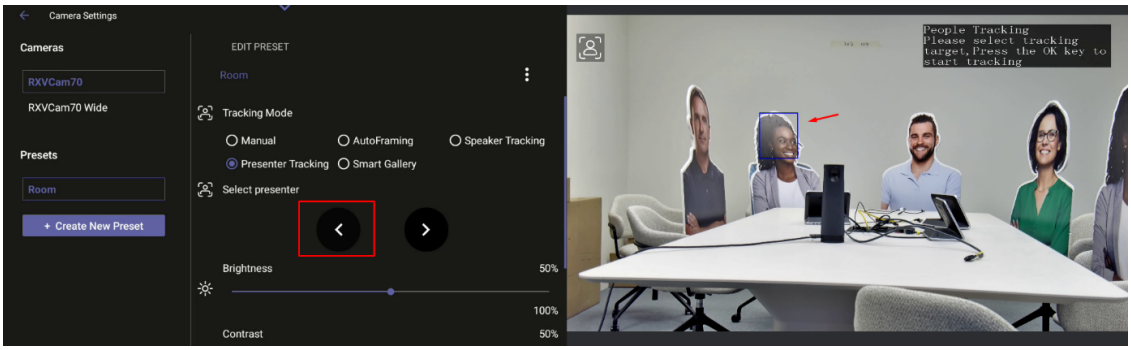
For non-supported cameras (e.g., RXVCam360), the Show Presenter on Content option is grayed out.

Select Presenter in Tracking Mode with Composite AI

If your RXV200 is connected to an RXVCam70 camera, you can select the presenter you want the camera to track. This can be done in non-composite AI mode (see Select RXVCam70 Camera Tracking Mode on page 36) or with Composite AI, as described below.

➢ To select a presenter to track in Camera Settings:

1. Navigate to the Composite AI Layout Settings page (see Set up Composite AI on page 46).
2. Turn on 'Presenter Mode' and tap **Select Presenter Manually**.
3. Under 'Select presenter', use the right-left arrows to choose the presenter. The presenter is accepted after a timeout of a few seconds, following the marking of the person in the room.



8 AI Summary

The AudioCodes AI Summary feature uses generative AI to automatically create and share meeting summaries among meeting participants and beyond. In-room participants can focus their attention on the ongoing discussions rather than taking notes manually. To ensure privacy and data integrity, the meeting summary emails are sent without transcription or recording to a database.

AI Summary is set up in the Device Manager. For details, refer to the AI Summary Configuration Guide for the AudioCodes RX Suite.

Before AI Summary can be used, it must be enabled on the RX-PAD (see Enable AI Summary below).

Using AI Summary consists of:

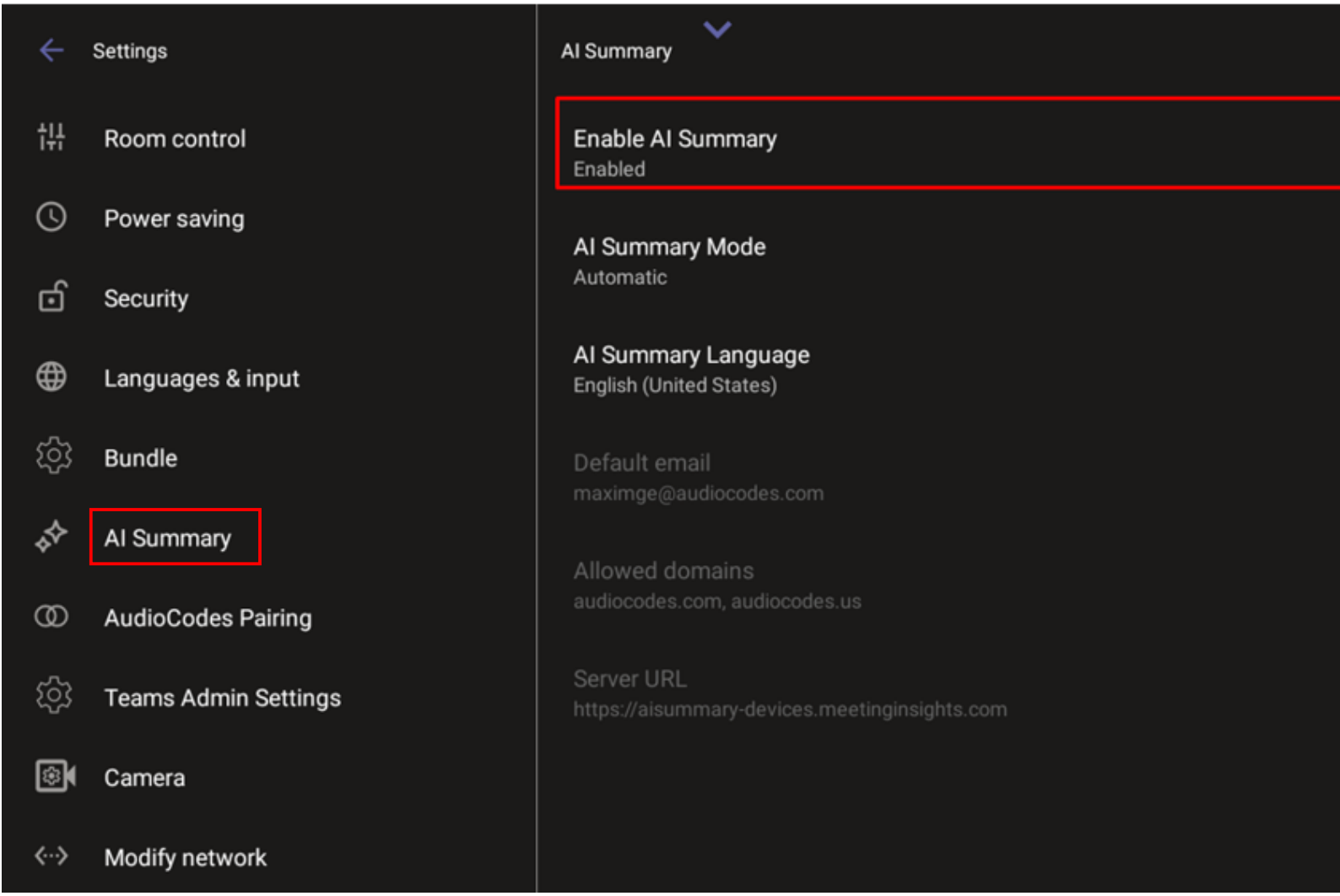
- Admitting the AI Summary Bot to a meetings (see Add the AI Summary Bot to a Meeting on the next page)
- Adding AI Summary mail recipients and changing the summary language (see Set AI Summary Mail Recipients and Summary Language on page 56)
- Removing AI Summary from a meeting (if requested) (see Remove AI Summary from a Meeting on page 56)
- Receiving AI Summary emails (see Receive AI Summary Emails on page 57)

Enable AI Summary

For the AI Summary feature to work, it must be enabled locally on the RX-PAD. This manual activation confirms that an authorized administrator has access to the MTRA hardware.

➢ **To enable AI Summary:**

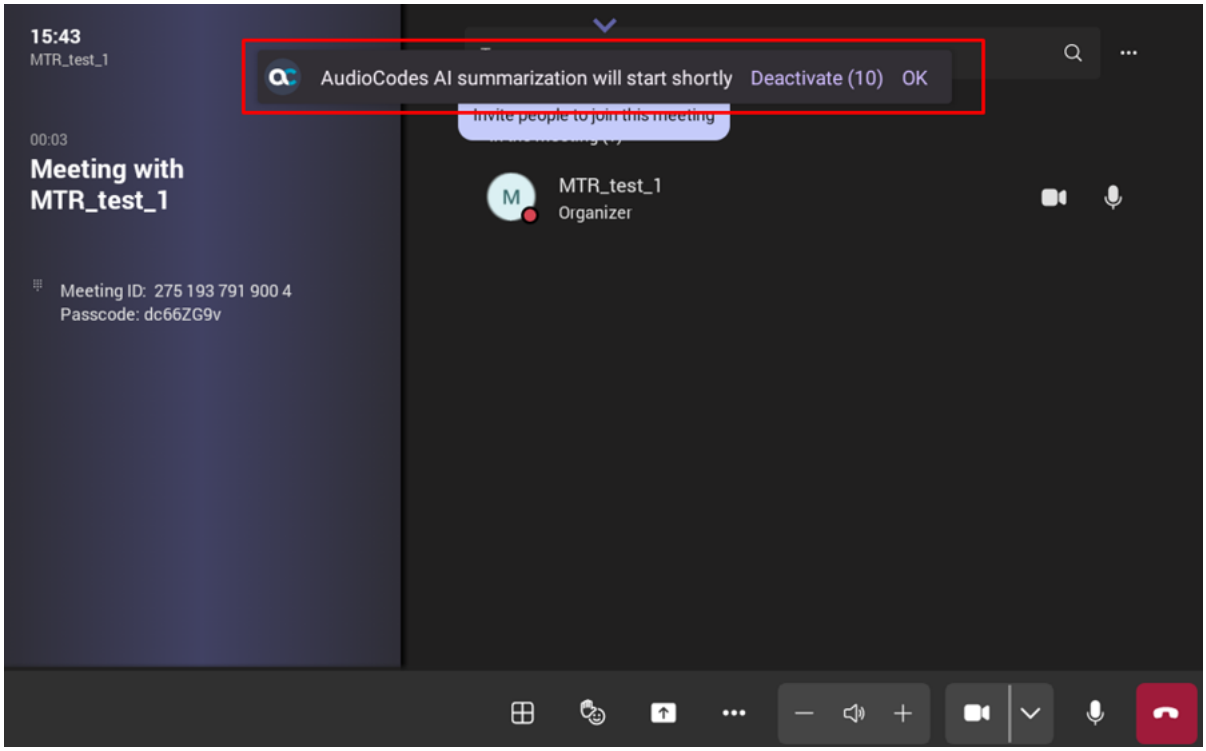
1. If not already logged in, log in to Device Administration to get admin access (see Log in to Device Administration on page 69).
2. Under 'Device admin settings', scroll down and tap **AI Summary**, then tap **Enable AI Summary**.



3. If prompted to approve, verify that the 'Default email', 'Allowed domains', and 'Server URL' values in the grayed out fields are correct, then tap **OK**.
4. Optionally modify the default values in the 'AI Summary Mode' and 'AI Summary Language' fields.

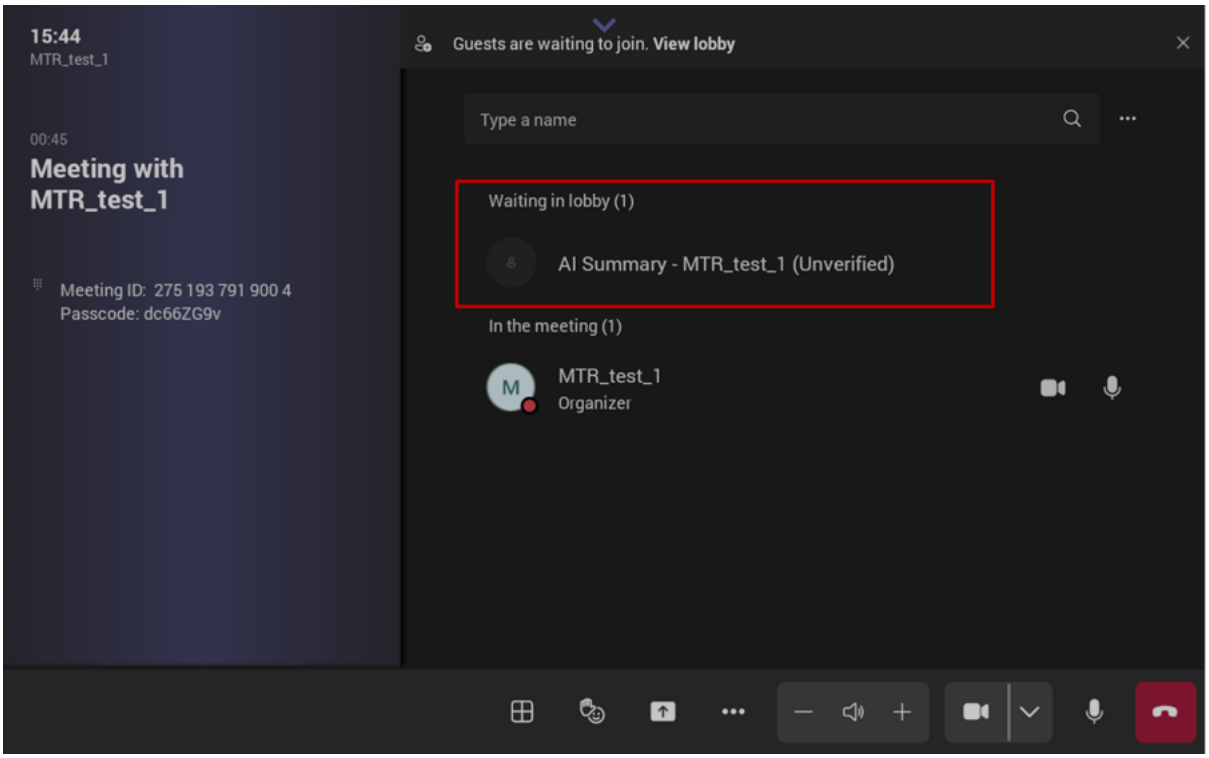
Add the AI Summary Bot to a Meeting

AI Summary is implemented through a bot developed by AudioCodes. Upon the start of a meeting (scheduled or Ad-hoc), the user is prompted that the bot is about to start.

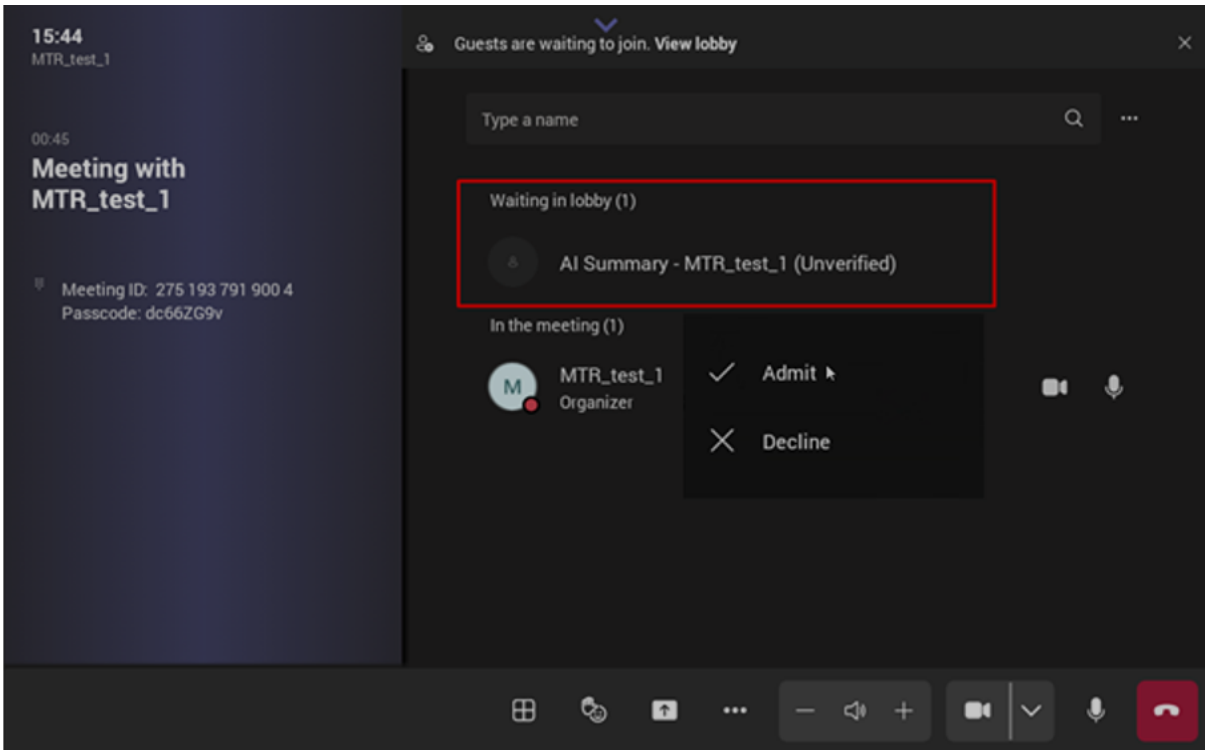


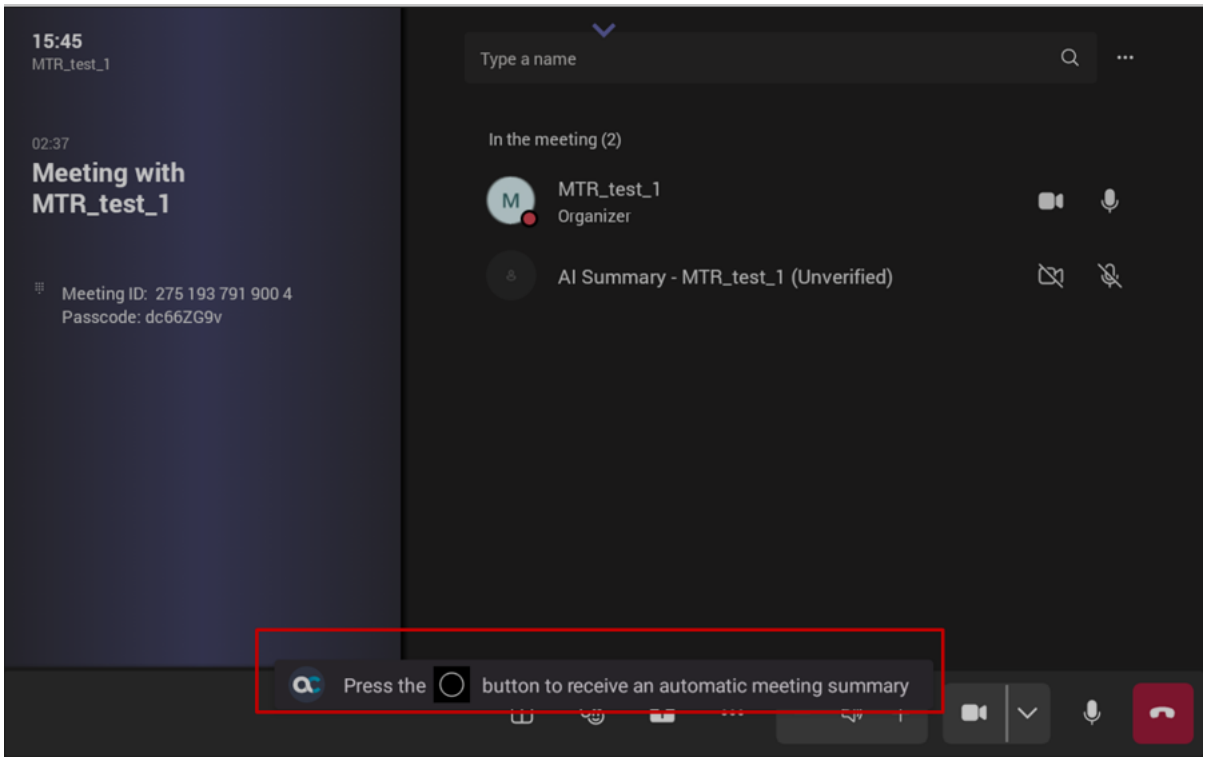
- Due to privacy concerns, the Bot enters the Meeting Room lobby pending admittance by the user who is already in the meeting.

> In Calendar meetings with the 'Bypass lobby' option set to **Everyone**, the AI Summary Bot joins automatically, *without awaiting admittance*.



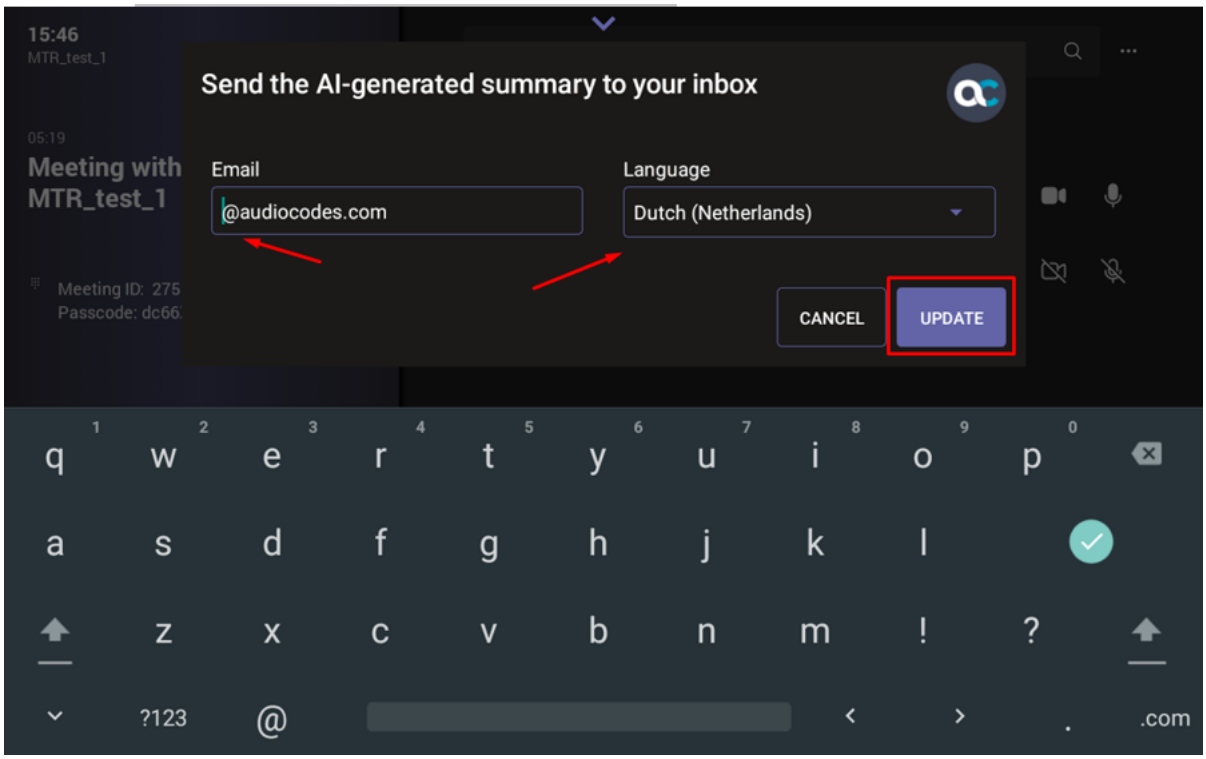
- Once admitted, the AI Summary Bot is successfully joined to the meeting and the recording starts.





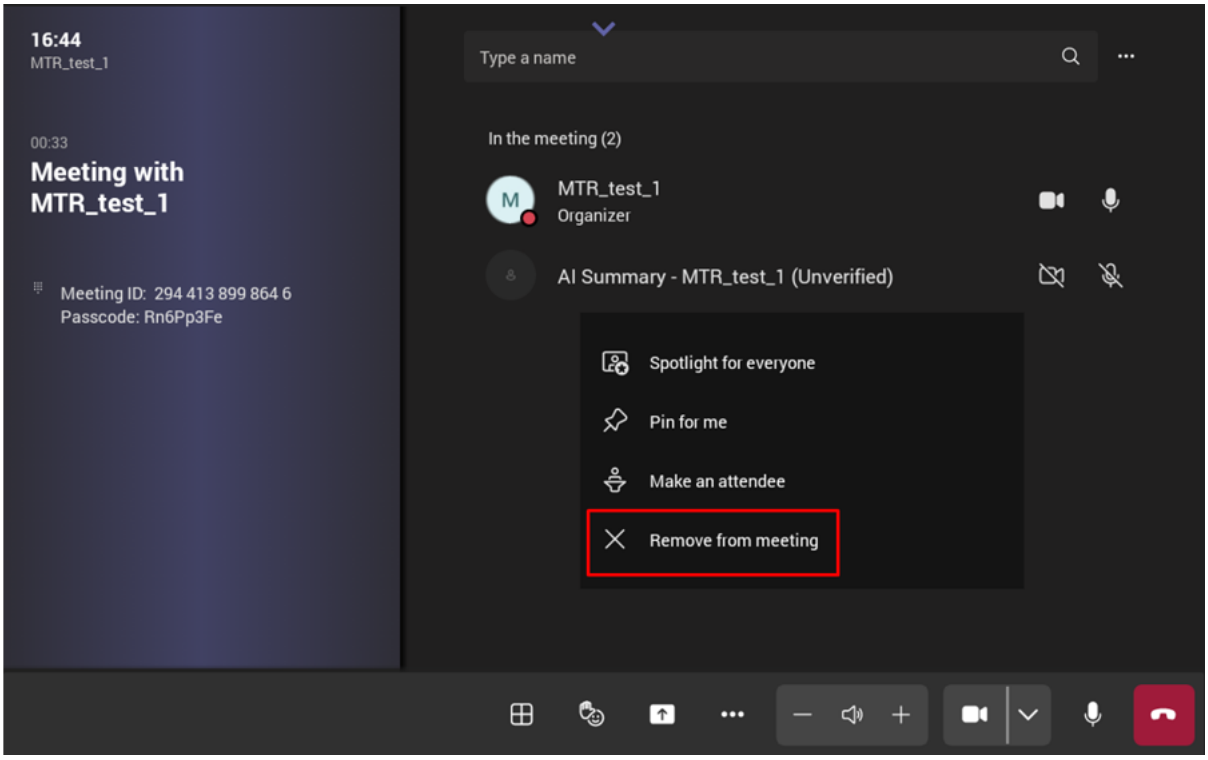
Set AI Summary Mail Recipients and Summary Language

During any stage of the meeting, press the **Home** hard key on the RX-PAD to add a recipient's email for the AI summary. Here you can also select the language of the summary. The last selected language will be used for all recipients.



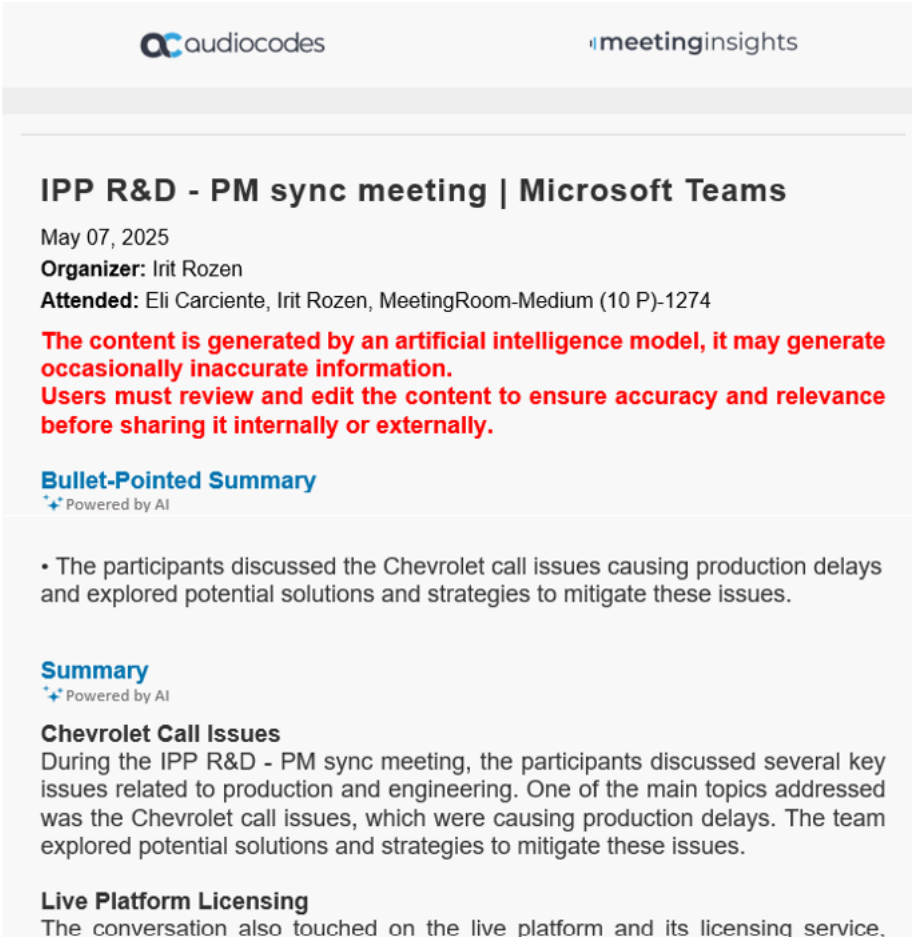
Remove AI Summary from a Meeting

Once the AI Summary bot is active, you can always tap **Remove from meeting** and remove the AI Summary feature from the meeting.



Receive AI Summary Emails

A couple of minutes after the meeting has ended, the AI Summary mail is sent to the recipients.



audiocodes meetinginsights

IPP R&D - PM sync meeting | Microsoft Teams

May 07, 2025

Organizer: Irit Rozen

Attended: Eli Carciente, Irit Rozen, MeetingRoom-Medium (10 P)-1274

The content is generated by an artificial intelligence model, it may generate occasionally inaccurate information.
Users must review and edit the content to ensure accuracy and relevance before sharing it internally or externally.

Bullet-Pointed Summary

Powered by AI

• The participants discussed the Chevrolet call issues causing production delays and explored potential solutions and strategies to mitigate these issues.

Summary

Powered by AI

Chevrolet Call Issues

During the IPP R&D - PM sync meeting, the participants discussed several key issues related to production and engineering. One of the main topics addressed was the Chevrolet call issues, which were causing production delays. The team explored potential solutions and strategies to mitigate these issues.

Live Platform Licensing

The conversation also touched on the live platform and its licensing service.

9 Room Control

The RX-PAD can run a web page of a Room Control system that is being placed in the same location as the RX-PAD and resides on the local network. The web page URL can be specified either as an FQDN or an IP address.

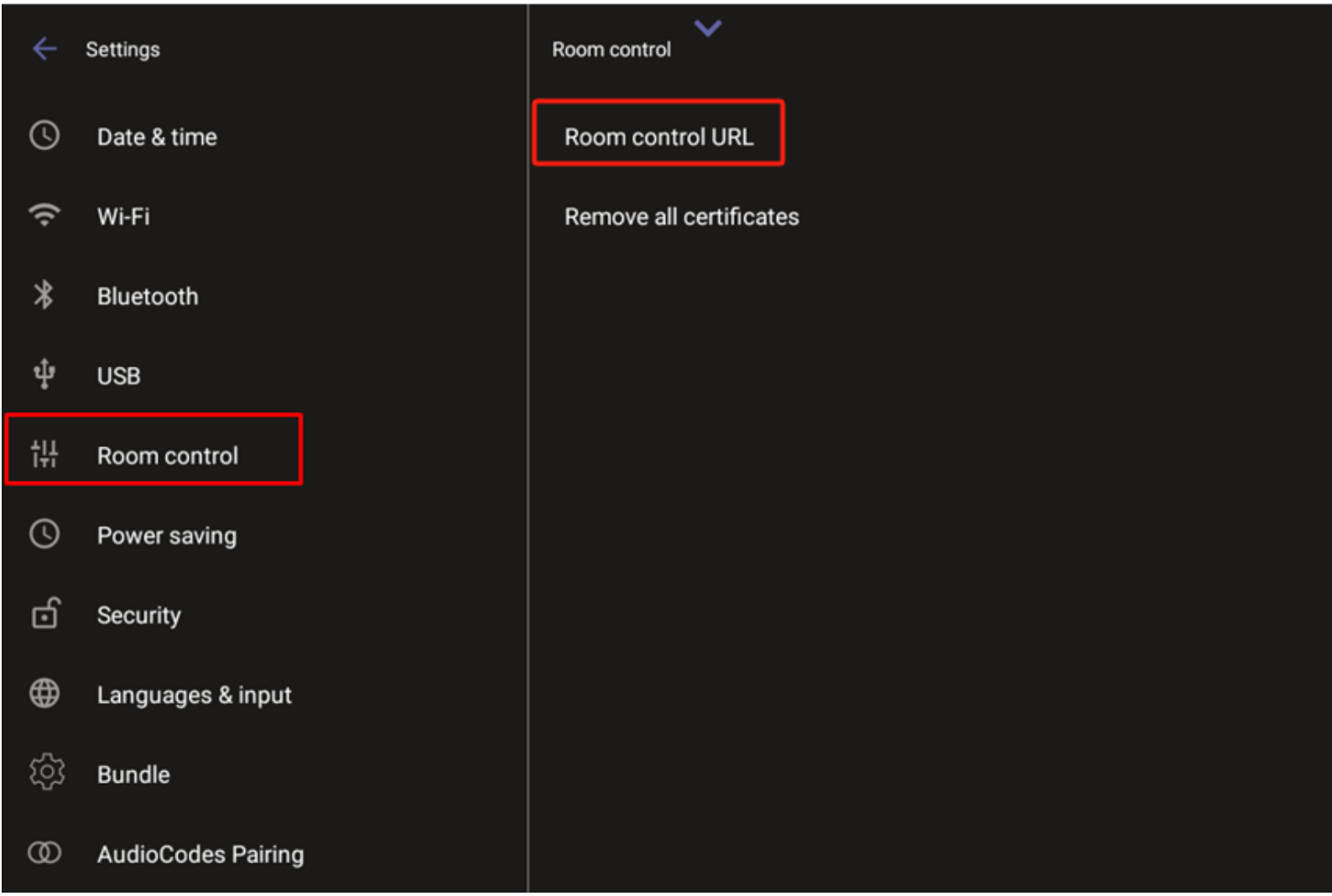
RX-PAD control URL restricted to local network

The RX-PAD will not communicate with the Room Controller if the Room Controller has a public IP address. Both devices must be on the same local network, using local IP addresses, for communication to work.

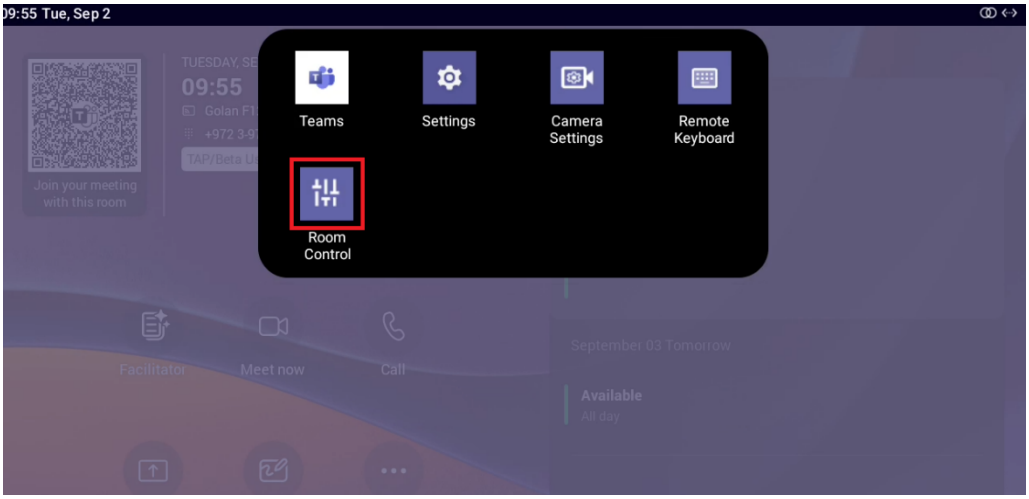
Ports 443 and 80 are blocked. If you try to enter a URL to a public destination, a “Can’t access public internet” message is displayed, and the entered value is not saved.

➢ **To specify the page URL of the Room Control system:**

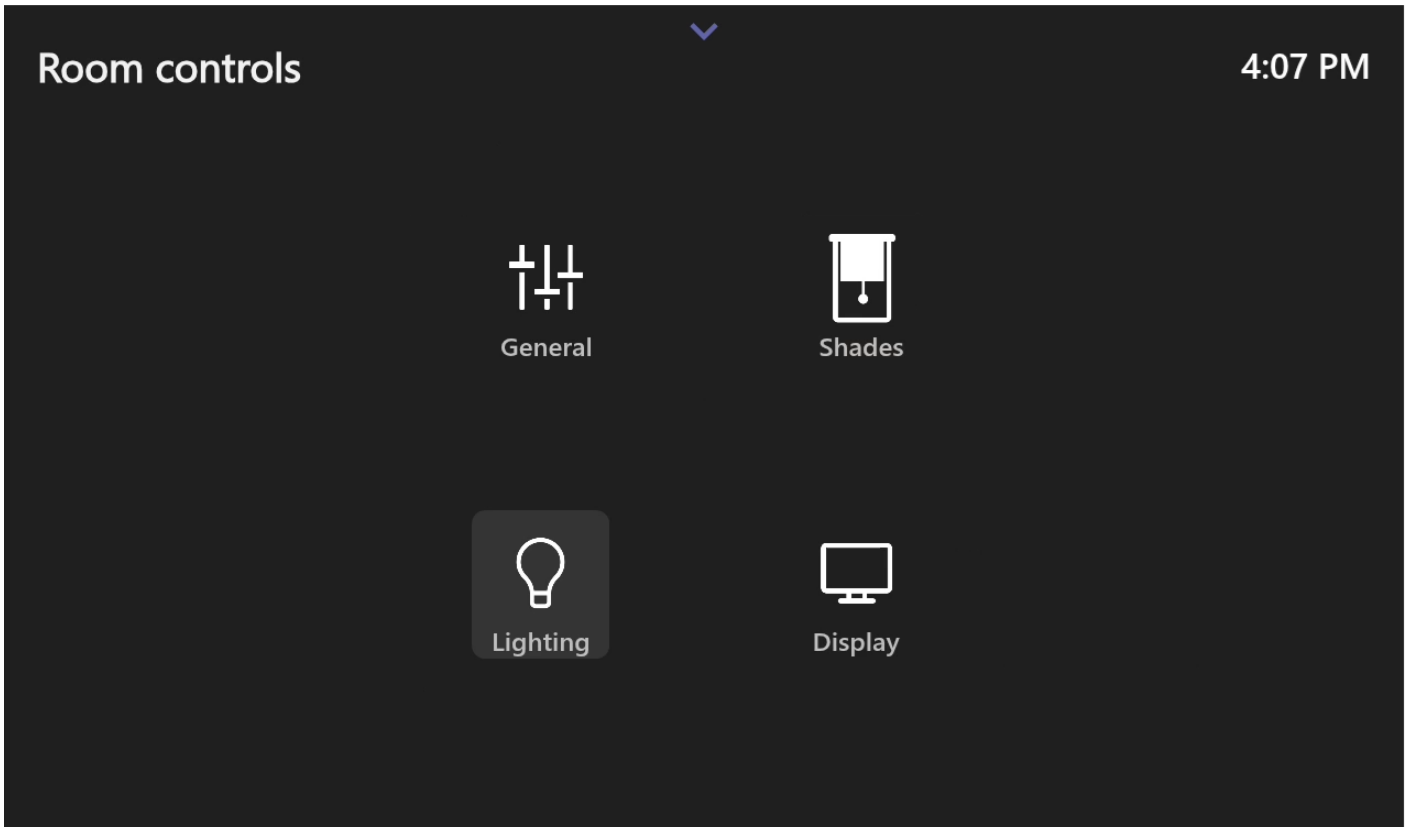
1. If not already logged in, log in to Device Administration to get admin access (see Log in to Device Administration on page 69).
2. Under ‘Device admin settings’, scroll down and tap **Room control**.
3. Tap **Room control URL** and enter the FQDN or IP address.



Once the Room Control URL has been set, the Room Control icon is created in the notification tray.

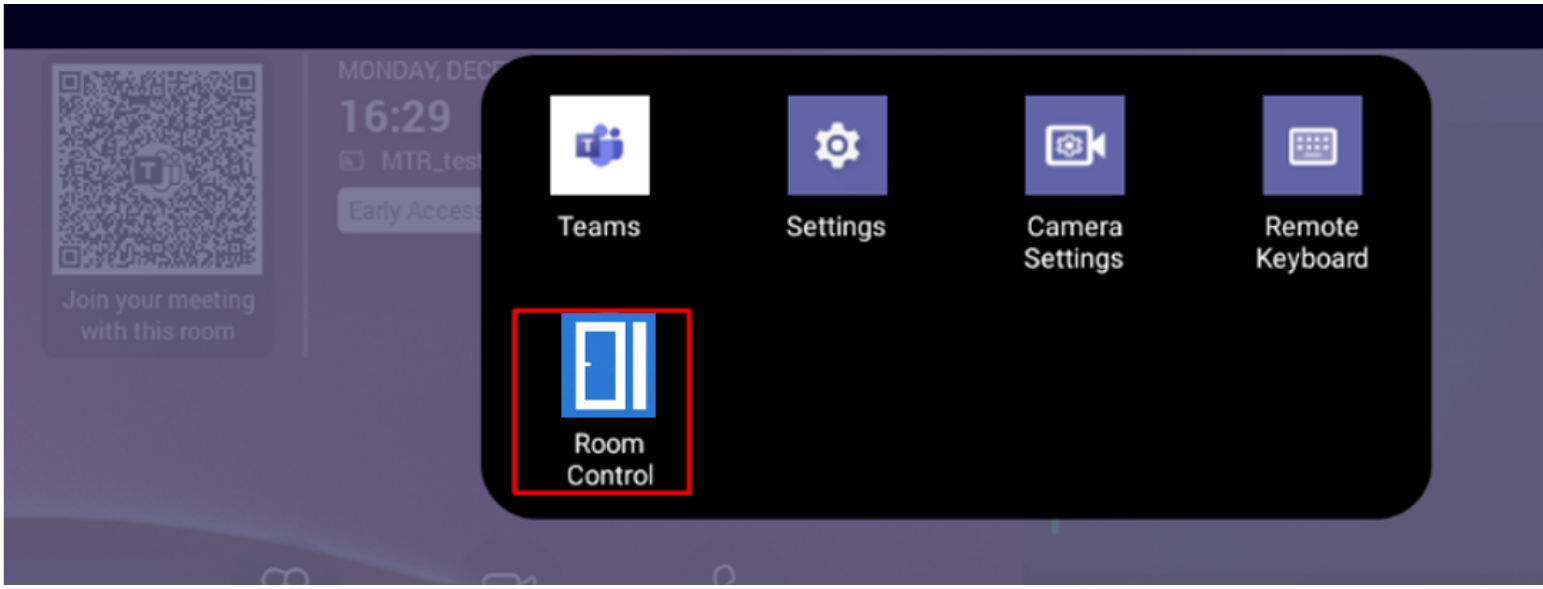


The following is an example of a Room Control app running and operated from the RX-PAD:



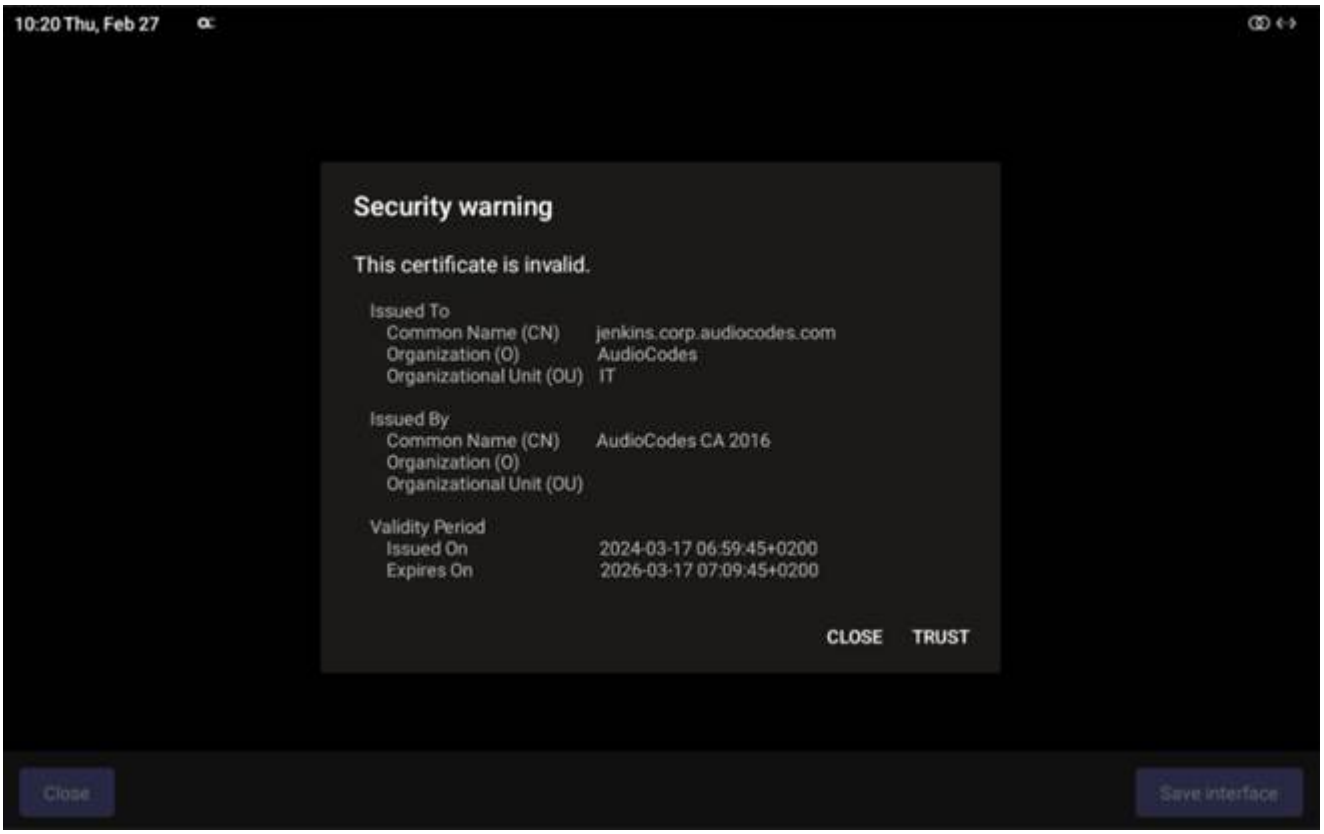
You can replace the Room Control icon with an image of your choice. To do this, execute the following command to the RX-PAD via an SSH connection:

```
param_tool scp system/room_control/icon_url
"URLtoIconLocation"
```



Handle Certificates

Some third-party Room Control systems use certificates that are either self-signed or not issued by a well-known Certificate Authority (CA). If the connected Room Control system presents a non-standard certificate, a prompt is displayed asking you if you want to trust this certificate. You have the option to manually trust these certificates during setup. However, it's important to understand that doing so involves accepting potential security risk. As a certificate's authenticity cannot be verified through standard procedures, you should exercise caution and be aware of the implications. If you trust the certificate, tap **Trust**.



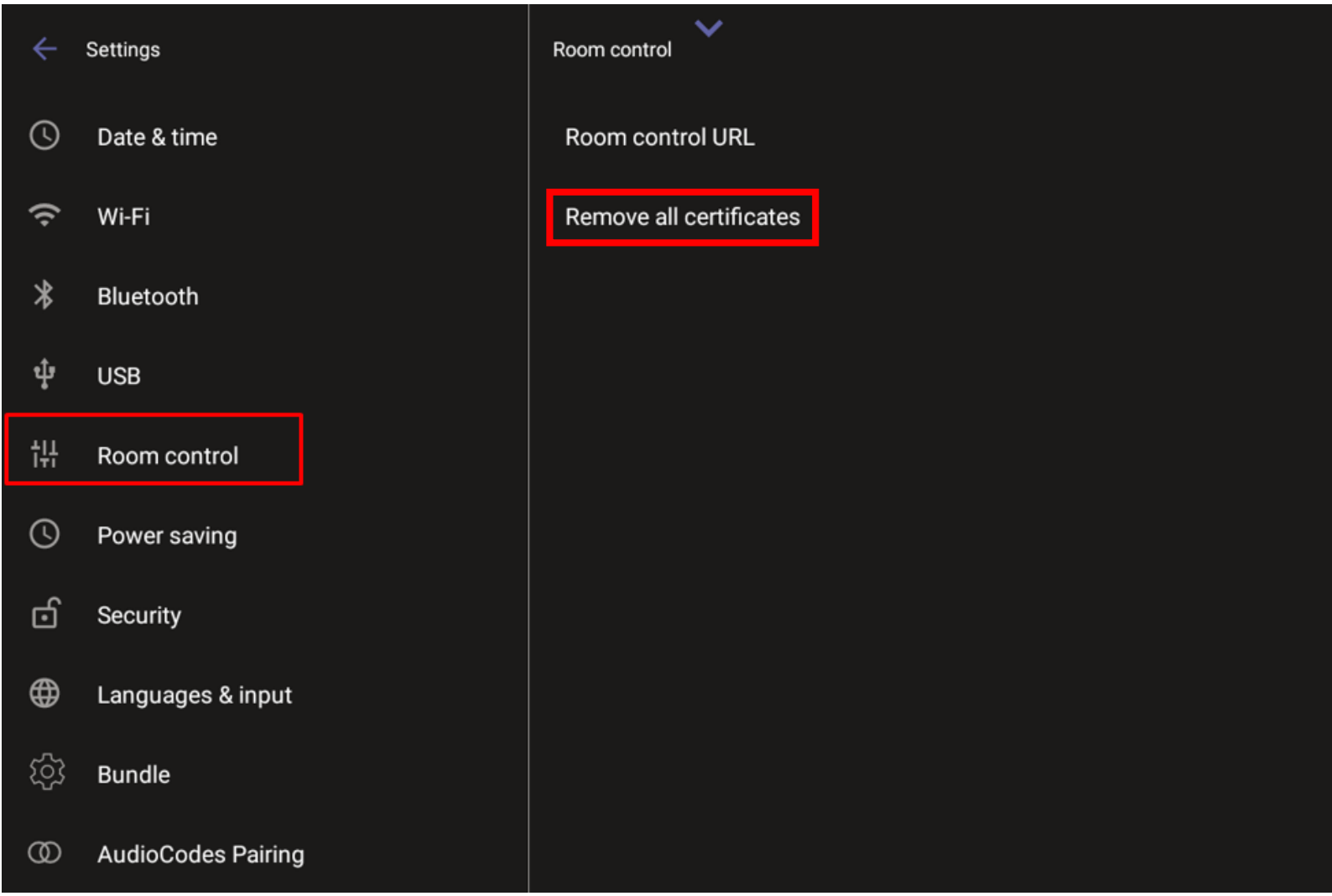
- The option is supported even though IP address may be a rare case since the server certificate's CN must include it.
- There is also a settings option to download the CA certificate.

Remove All Certificates

Admins can remove certificates trusted by the RX-PAD when necessary to update the Room control URL. This prevents the control URL from being exploited to access websites like CNN or Netflix. To achieve this, ports 443 and 80 are blocked. Controllers use different ports for communication.

➢ **To remove certificates:**

1. If not already logged in, log in to Device Administration to get admin access (see Log in to Device Administration on page 69).
2. Under 'Device admin settings', scroll down and tap **Room control**, then tap **Remove all certificates**.



.

10 User Settings

RXV200 and RXV81 MTRAs 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:

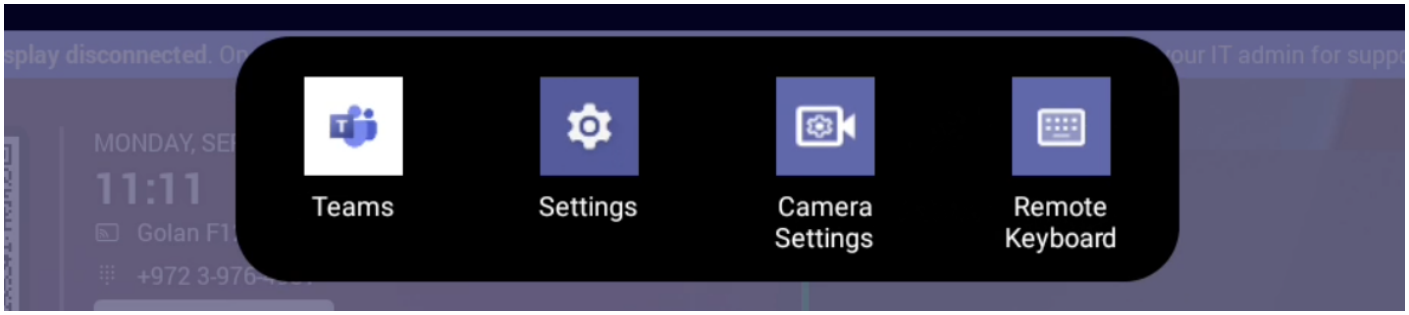
- Adjust the Volume on the next page
- Configure Accessibility Settings on page 66
- View the RXV200 or RXV81 Information on page 66
- Approve Firmware Updates of Connected Peripherals on page 67
- View Microsoft Teams Information on page 67
- Reboot the Device on page 68

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

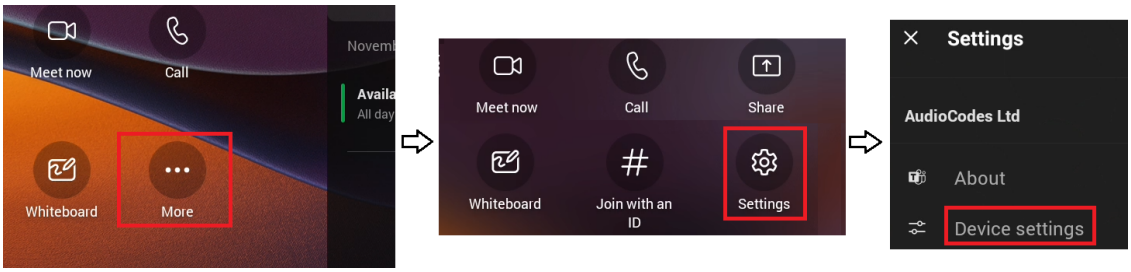
Access User Settings

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

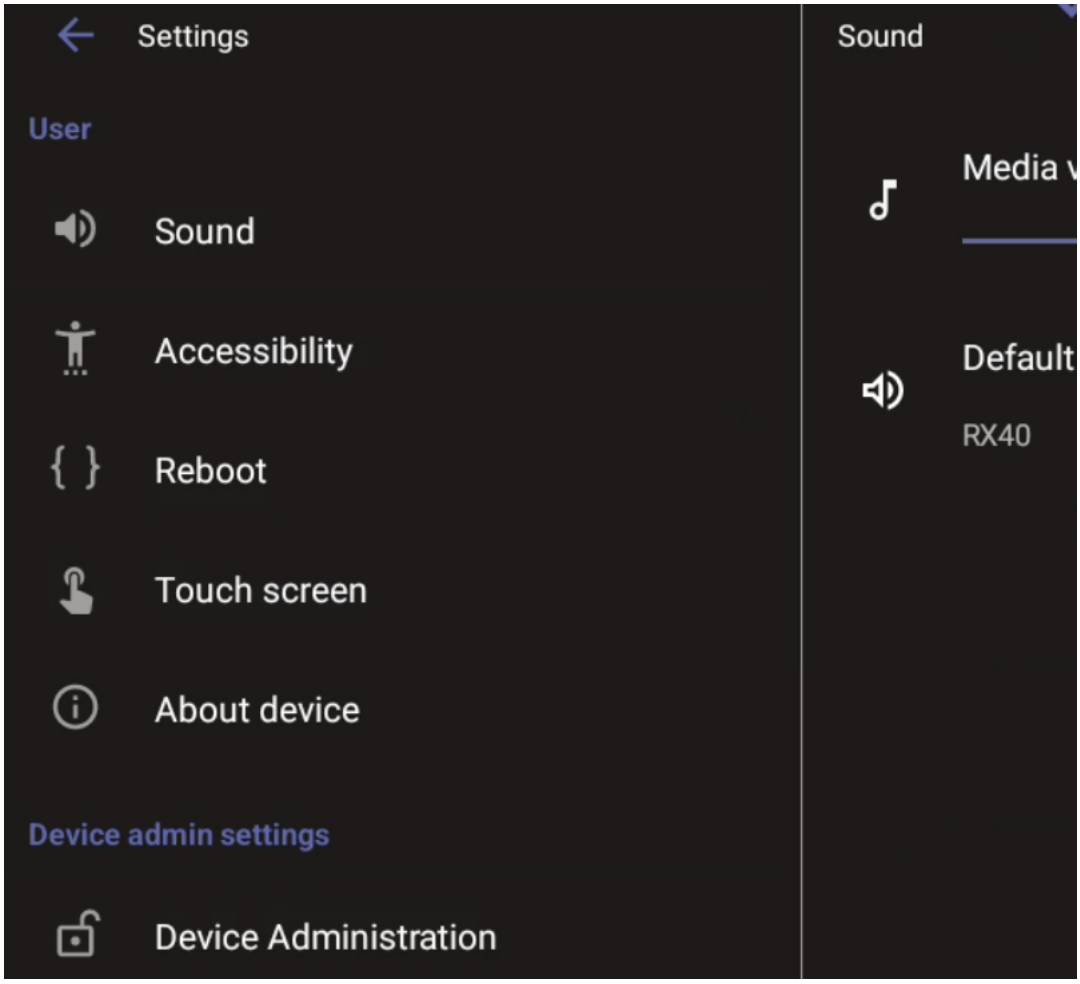
- Swipe down to display the main menu tray, then tap **Settings**.



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



Any user can configure User settings:

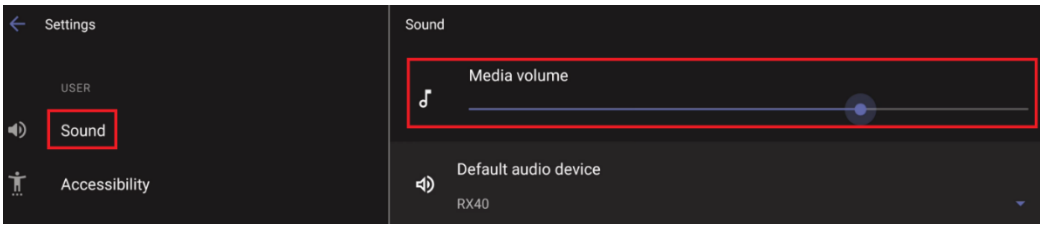


Viewing and configuring Device Admin settings requires Admin login. For details, see Admin Settings on page 69.

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 64).
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 the RXV200 or RXV81 Information

The 'About' screen gives you quick access to information about the RXV200 / deployment.

➢ **To access the About page:**

1. Navigate to 'Settings' (see Access User Settings on page 64).
2. Under 'User', tap **About device**.

   If you are accessing the page from the RX-PAD, the RX-PAD device information is displayed. To view the RXV device info, tap **About Front of Room device**.

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

Approve Firmware Updates of Connected Peripherals

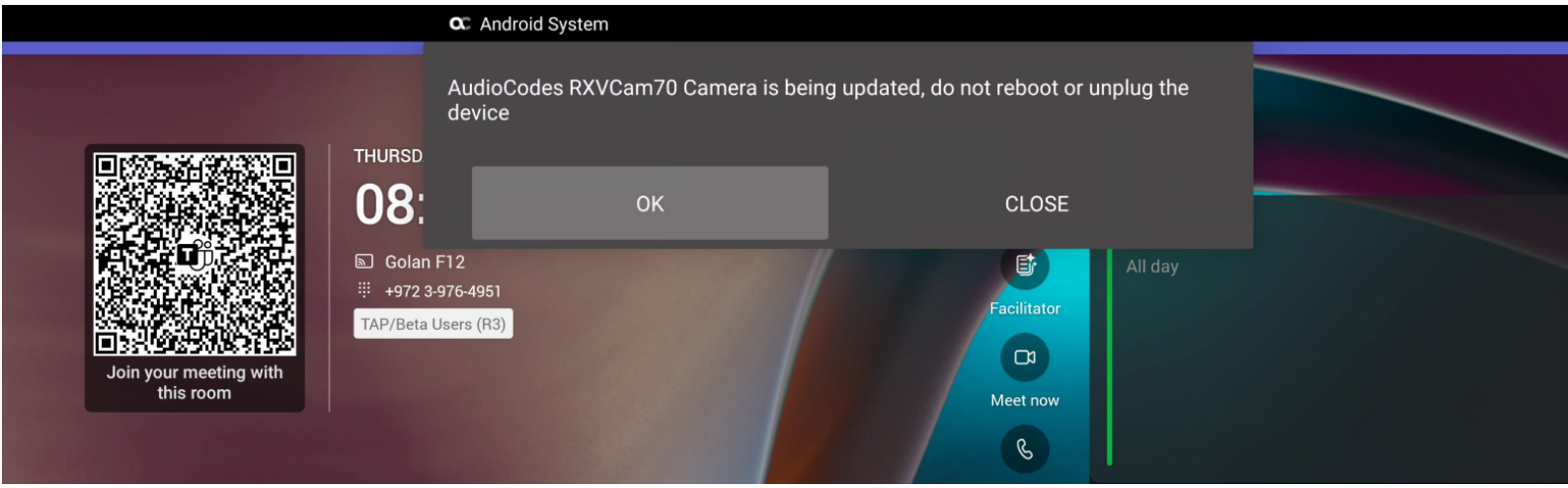
RXV200 firmware update includes upgrading:

- **RXVCam360** camera and speaker firmware
- **RXVCam70** camera firmware
- **RXVCam50** camera firmware
- **RX15** speaker firmware

Updating RXV200 audio and camera peripherals firmware is a safe and streamlined process. Peripherals' update packages are included in the RXV200 firmware update and executed according to the currently connected peripheral.

You may get a popup message prompting you to accept an upgrade to the firmware of a peripheral connected to the RXV200.

When upgrading, you might get notifications not to reboot the device. Tap **OK**.

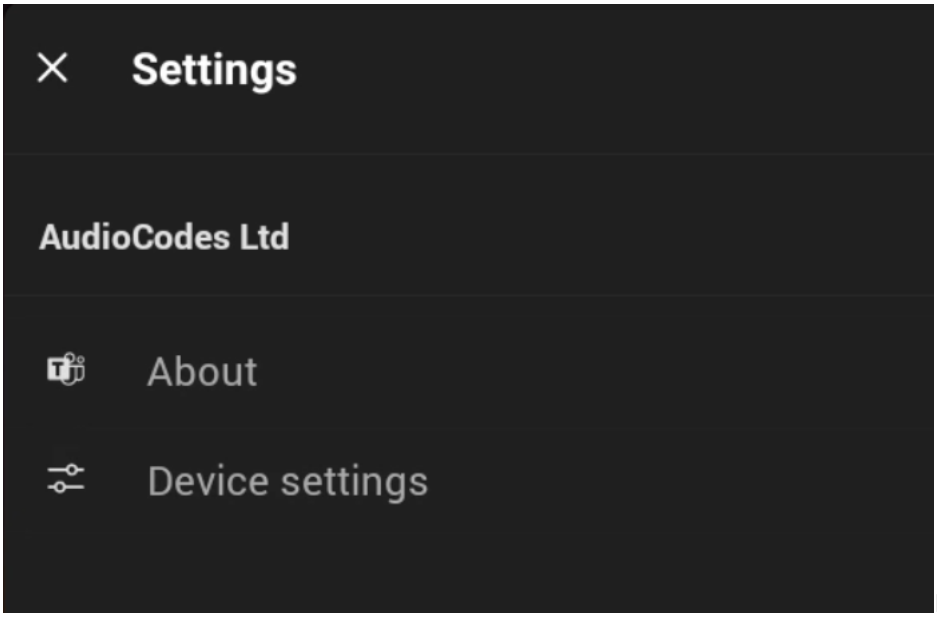


After a peripheral firmware upgrade is completed, the connected device will perform a reboot, and an associated notification will appear at the bottom of the page.

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.

➢ **To reboot:**

1. Navigate to 'Settings' (see Access User Settings on page 64).
2. Under 'User', tap **Reboot**. You can reboot the RX-PAD, the RXV200 / RXV81 unit, or both.
3. Tap the appropriate Reboot option .
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 106.

11 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.

Access Device Admin Settings

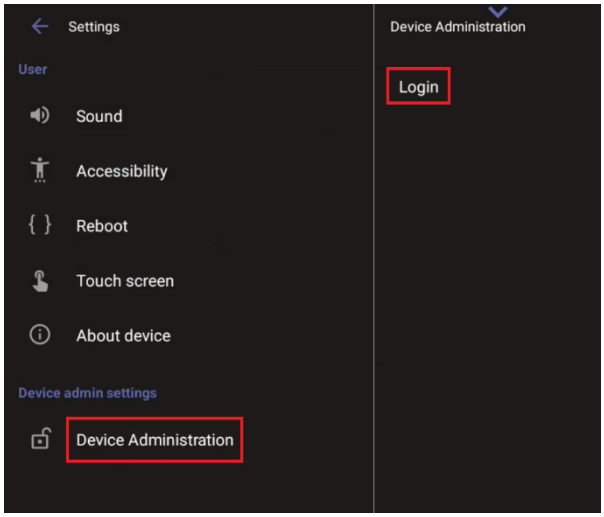
To view and access Device Admin settings, you need to be logged into Device Administration (see Log in to Device Administration below).

Log in to Device Administration

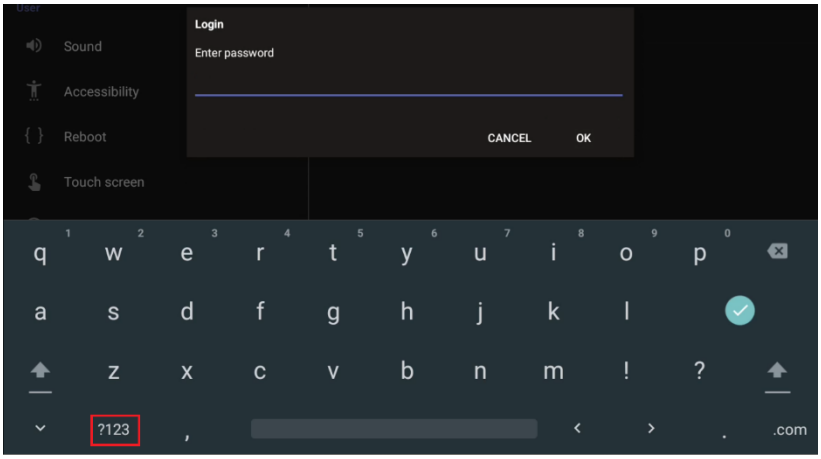
➢ **To log into Device Administration:**

1. Navigate to the 'Settings' page (see Access User Settings on page 64).

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:

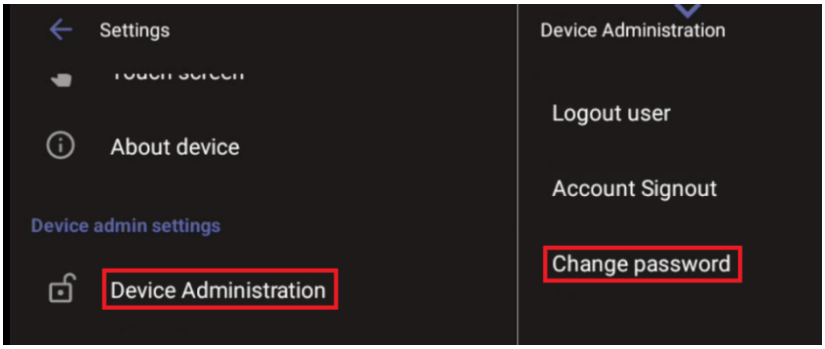
- The password length must be greater than or equal to 8.
- The password must contain one or more uppercase characters.
- The password must contain one or more lowercase characters.
- The password must contain one or more numeric values.
- The password must contain one or more special characters.

- 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 69).
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 MTRA (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 MTRA from the TAC, remotely sign in, and sign out.

➢ To sign out of the MTRA using Microsoft TAC:

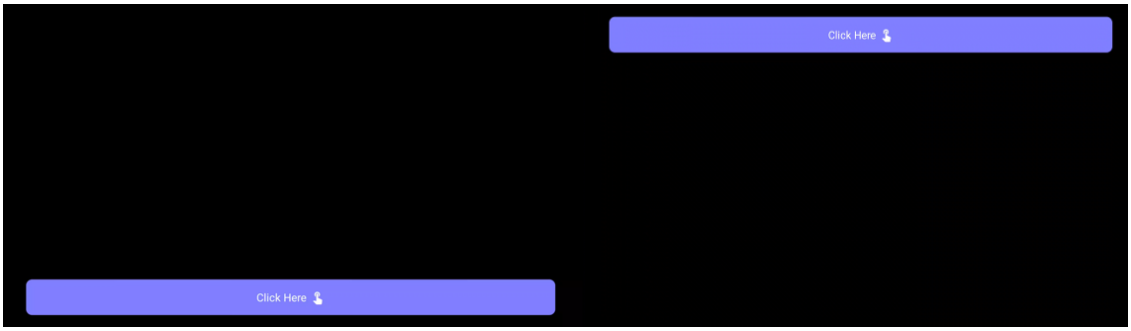
- Navigate to the 'Devices' > 'Teams Rooms' screen. From the **...** menu located in the uppermost right corner of the screen, select **Actions** and then **Sign out**.

Set up Dual Touch Screen Orientation

When two touch screens connect to the RXV200 they can simultaneously display.

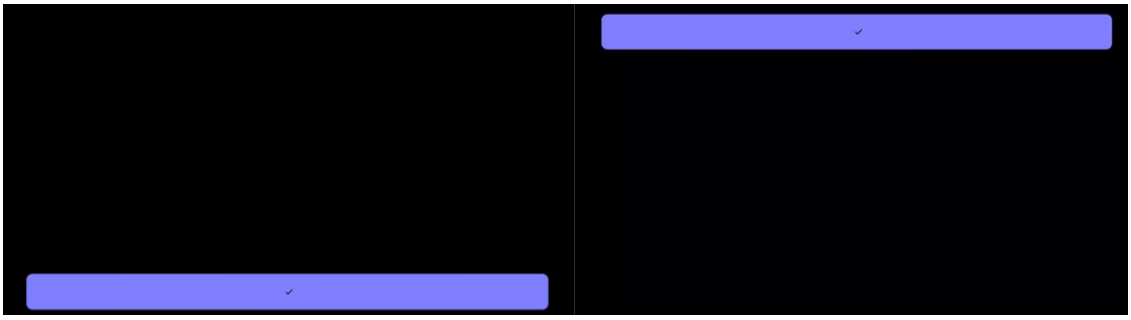
➢ To display two screens:

1. In the Out-of-Box phase, connect both screens and their USB cables to the RXV200 before the device is booted. The following screen is displayed:



> The screens display before every other phase only when the touch screens are connected.

2. Tap each **Click Here** button: a tick is displayed on each button:



The UI now displays the language phase options.

> For a new installation, the dual touch GUI pops up when the setup has two screens, also for a single touch (to know to which screen this touch belongs).

Dual Display Mode and Swap Screens Admin Controls

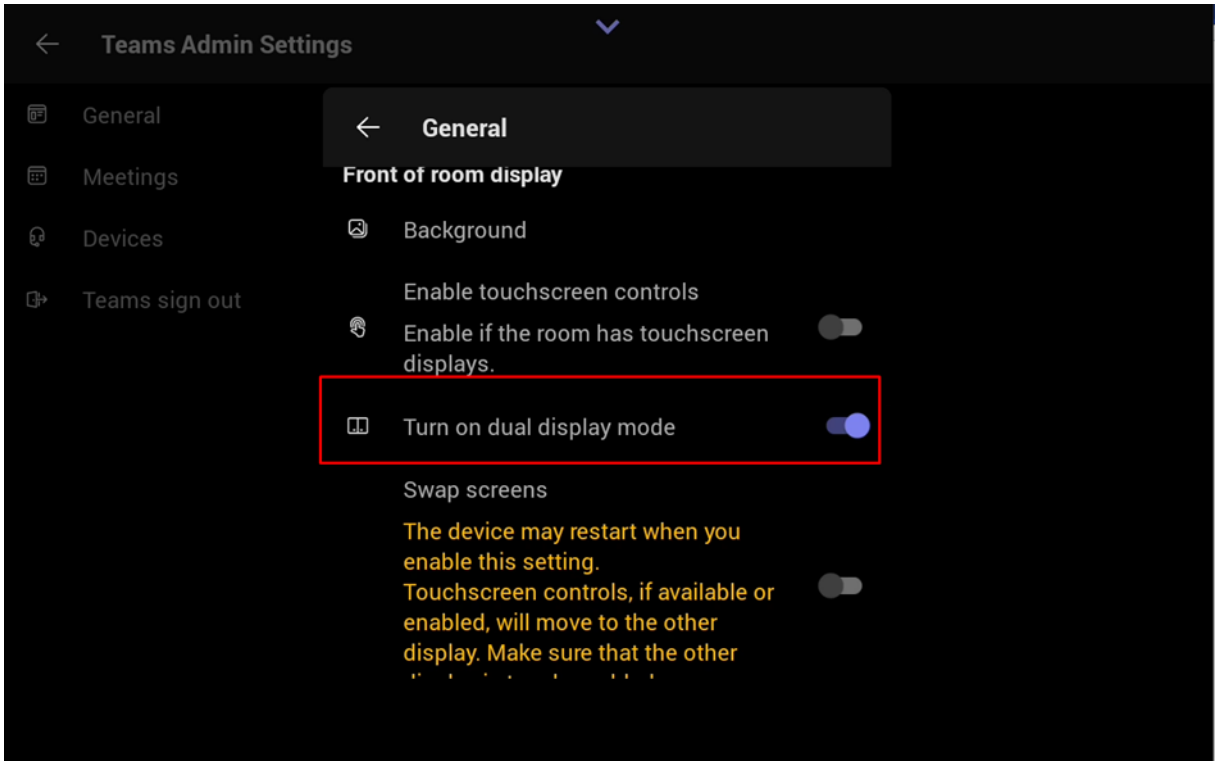
> This feature is for RX-PAD paired with RXV200 only, and for a Pro room account, as described below. The devices must run the following Teams app version or later - 1449/1.0.96.2024110701 (November 2024).

Admins can configure Teams Rooms on Android devices to run in dual display mode and to switch the screens in these rooms when set up invertedly as front-of-room display. This can be

done without physically disconnecting and reconnecting the HDMI OUT cables from the RXV200.

➢ **To disable dual display mode or switch screens:**

1. If not already logged in, log into Device Administration (see Access Device Admin Settings on page 69).
2. Under 'Device Admin Settings', scroll down and tap **Teams Admin Settings**.
3. Navigate to **Teams Admin Settings > General**, then turn on dual display mode.



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 64).
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 69).
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.

It's recommended not to enable the 'No IR Power off' option which exists in known TV brands such as LG and Samsung, and to allow RX-PAD to put the system to sleep while it is not in use.

5. To limit the HDMI resolution and Frames per Second (FPS) (usually for debugging purposes), tap **Resolution** and select the required option.
6. 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 69).
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 MTRA (or) 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 69).
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 69).
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 79.
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.

- '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 11-1: 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.
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.

Parameter	Description
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 77).

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 69).
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 69).
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 2 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 69).
2. Under 'Device admin settings', scroll down and tap **Bundle**.
3. Select the relevant bundle.

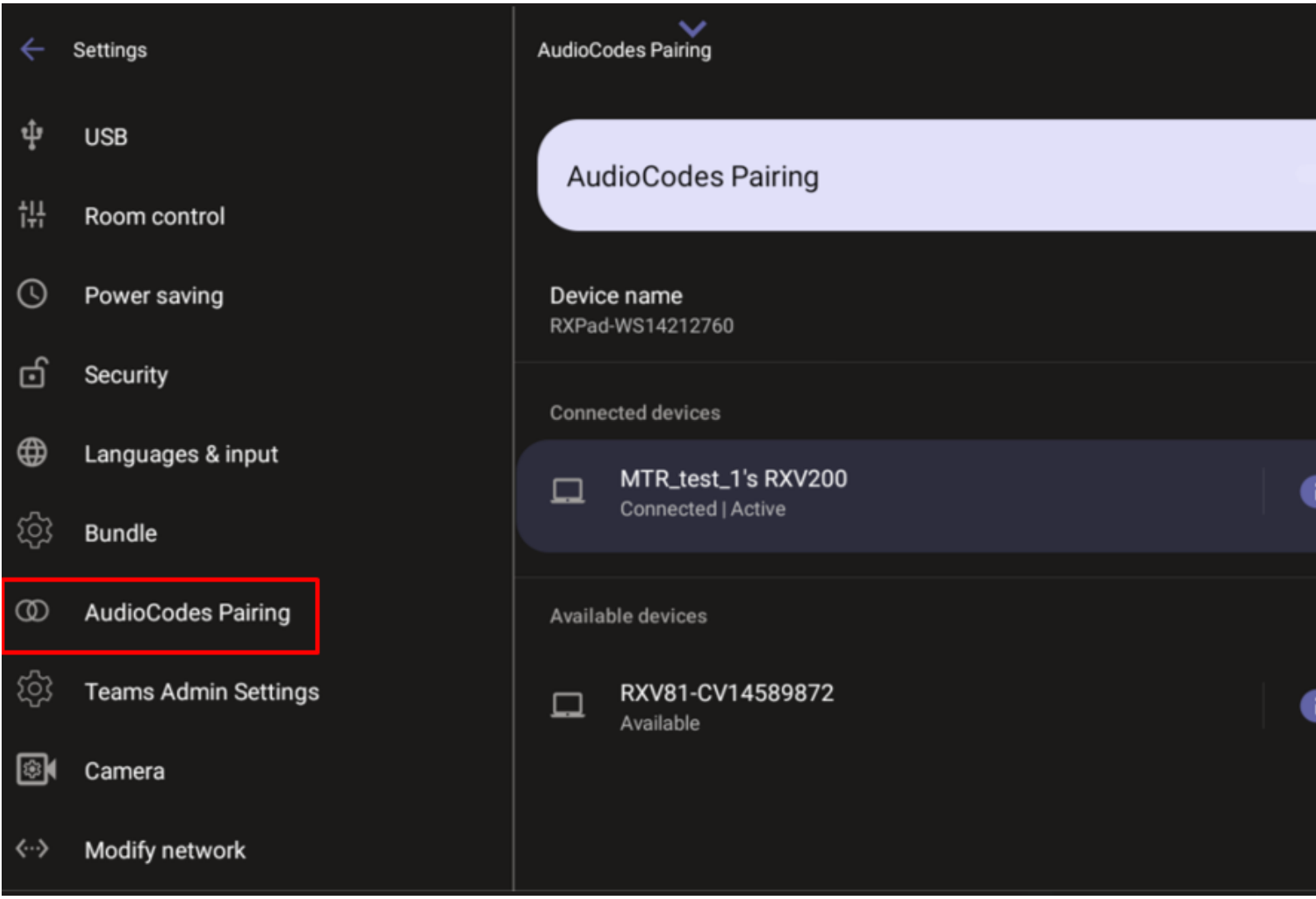
Pair RX-PAD with Different MTRA

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 69).
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**.



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 69).
2. Scroll down and tap the **Camera** option, then tap **Camera Settings**.

For details on configuring camera settings, see MTRA Camera Settings on page 30.

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 69).
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 86).

Set up a Proxy Server

Administrators can manually configure the MTRA 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

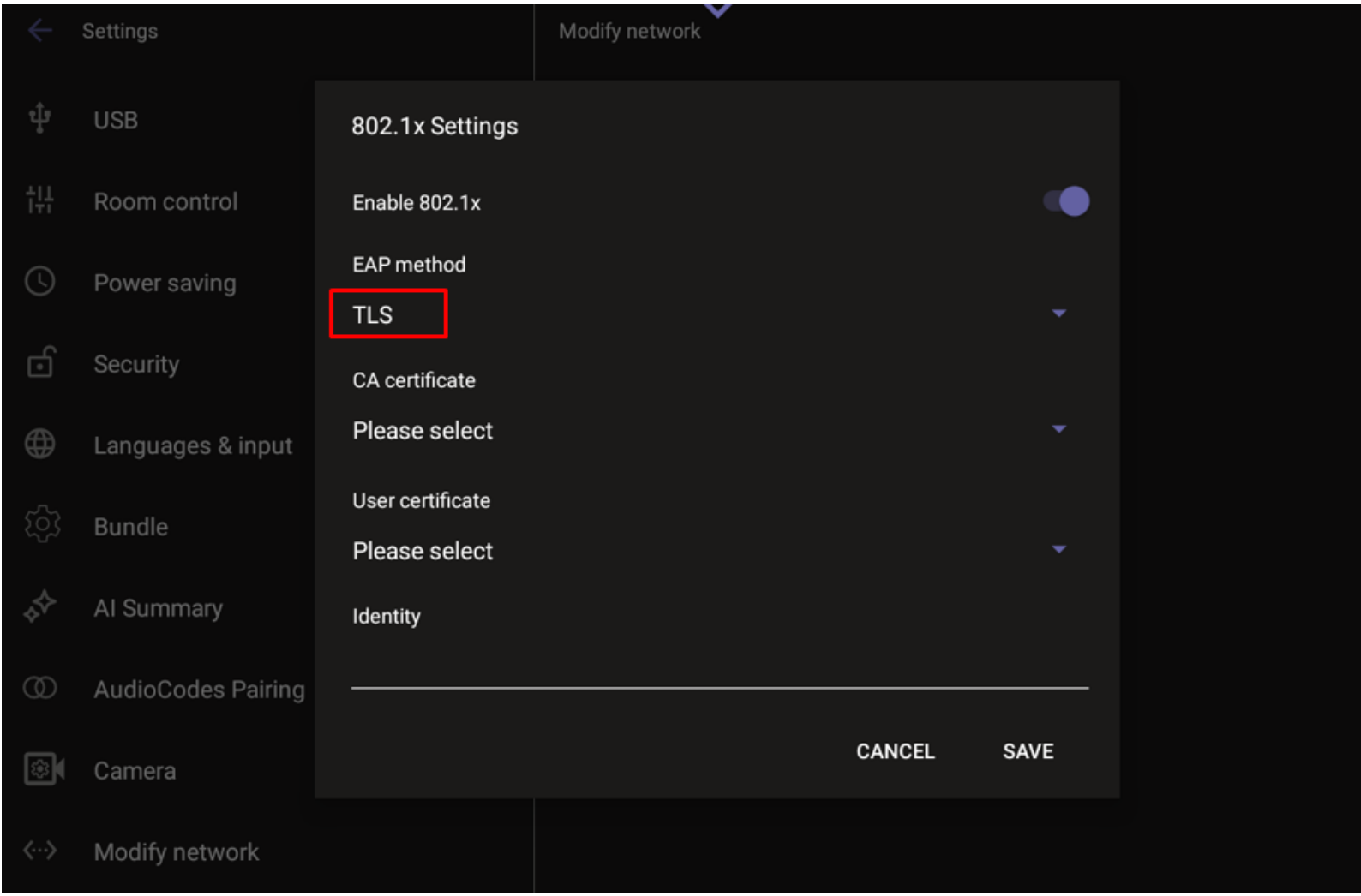
802.1x Authentication is the IEEE Standard for Port-based Network Access Control (PNAC) (refer to https://1.ieee802.org/security/802-1x/ for more information). It is used to enable port-based authentication.

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`

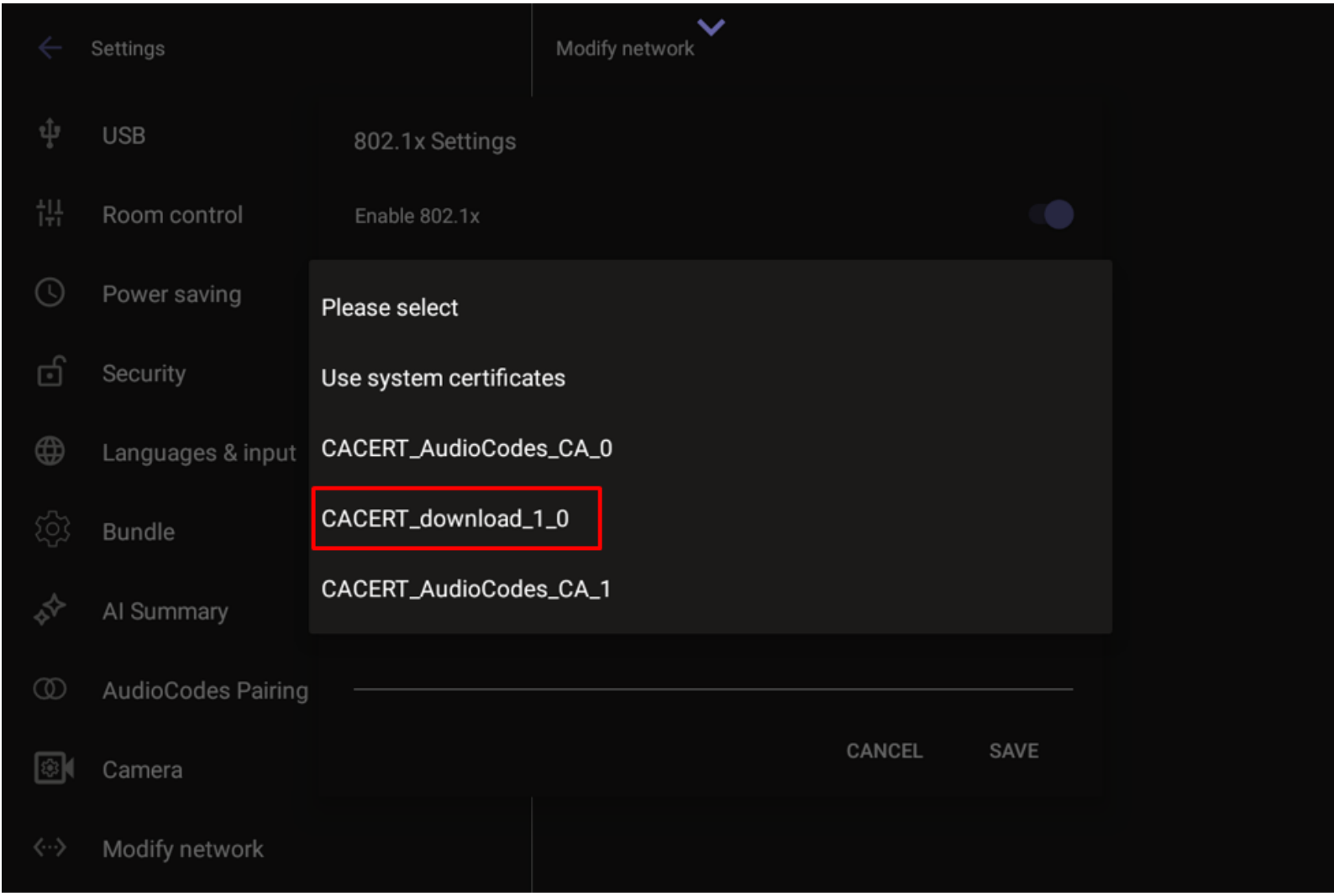
➢ **To configure 802.1x settings:**

1. Navigate to 'Modify network' (see Modify IP Network Settings above) and select **802.1x Settings**.

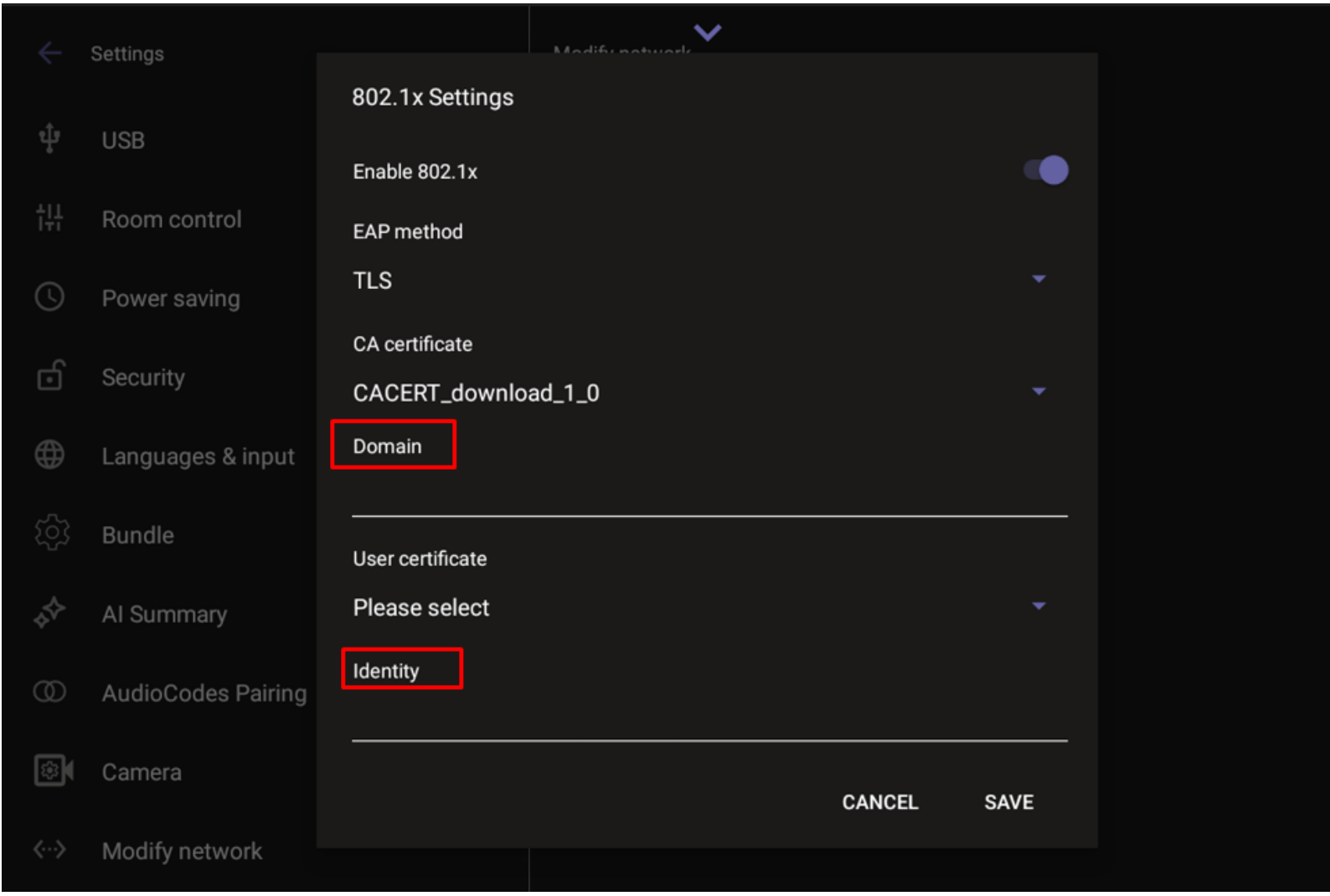
2. Tap **Enable 802.1x** and then tap **Save**.
3. Once 802.1x is enabled, choose the security method and strength. A commonly used option is EAP-TLS.



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.



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.



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 83) 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.

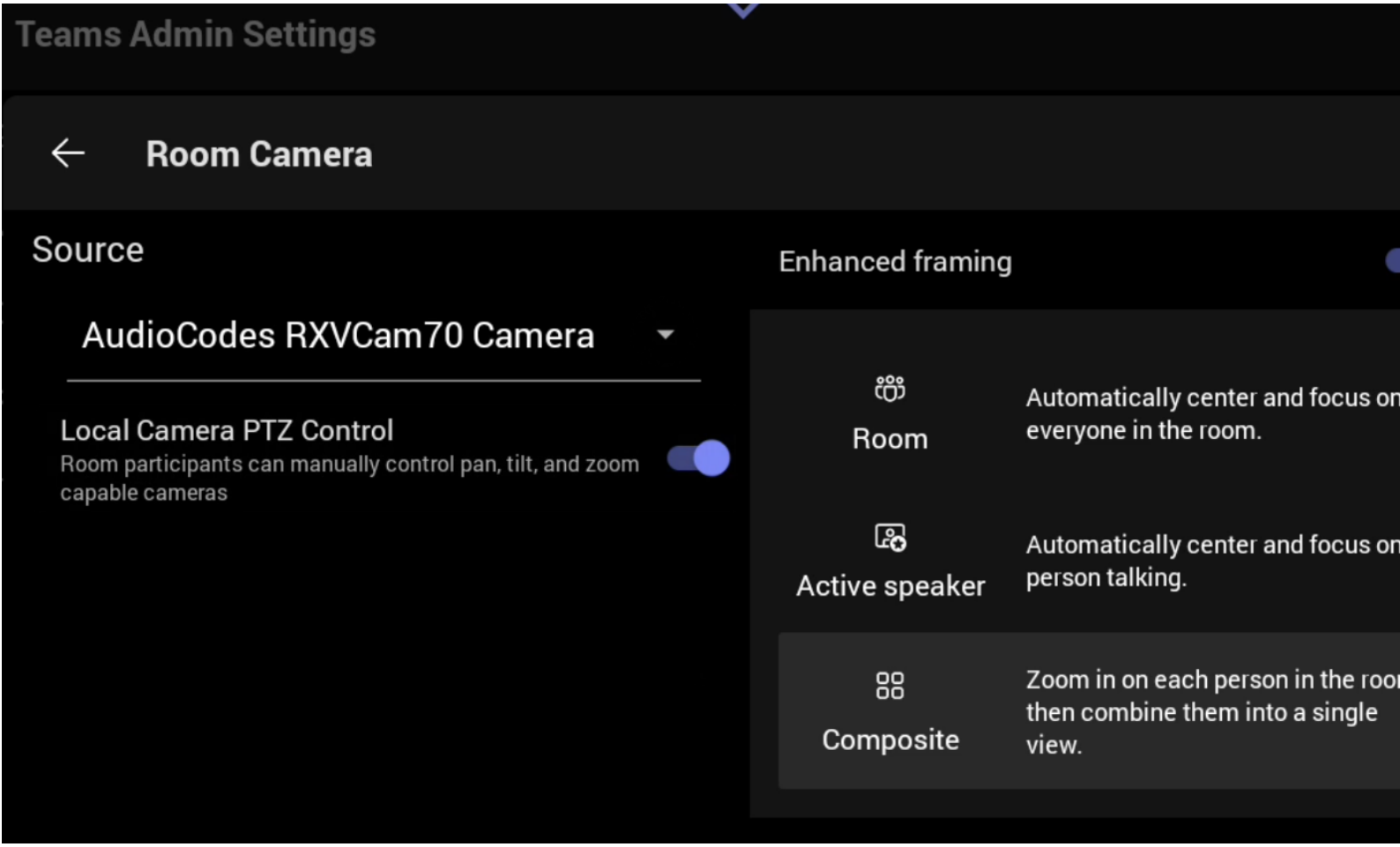
Configure Camera Settings with RX-PAD Teams Admin

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 69).
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**, select the relevant camera, and configure settings.



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

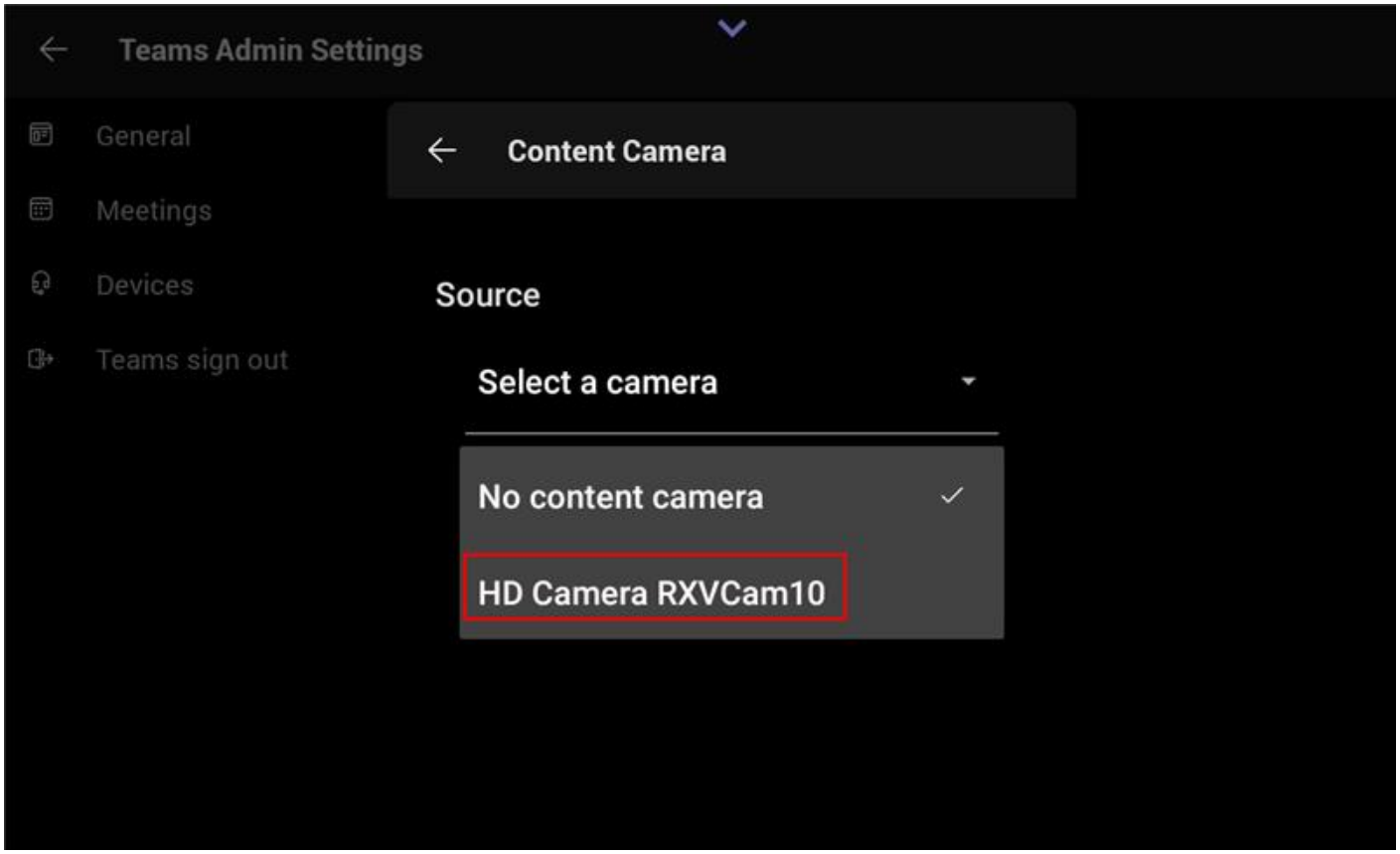
Content Camera Framing on a Whiteboard below describes how to use the Content Camera option to share a whiteboard using an RXVCam10 camera.

Content Camera Framing on a Whiteboard

> ⚠ For this function to work, the MTRA must be equipped with an RXVCam10 camera.

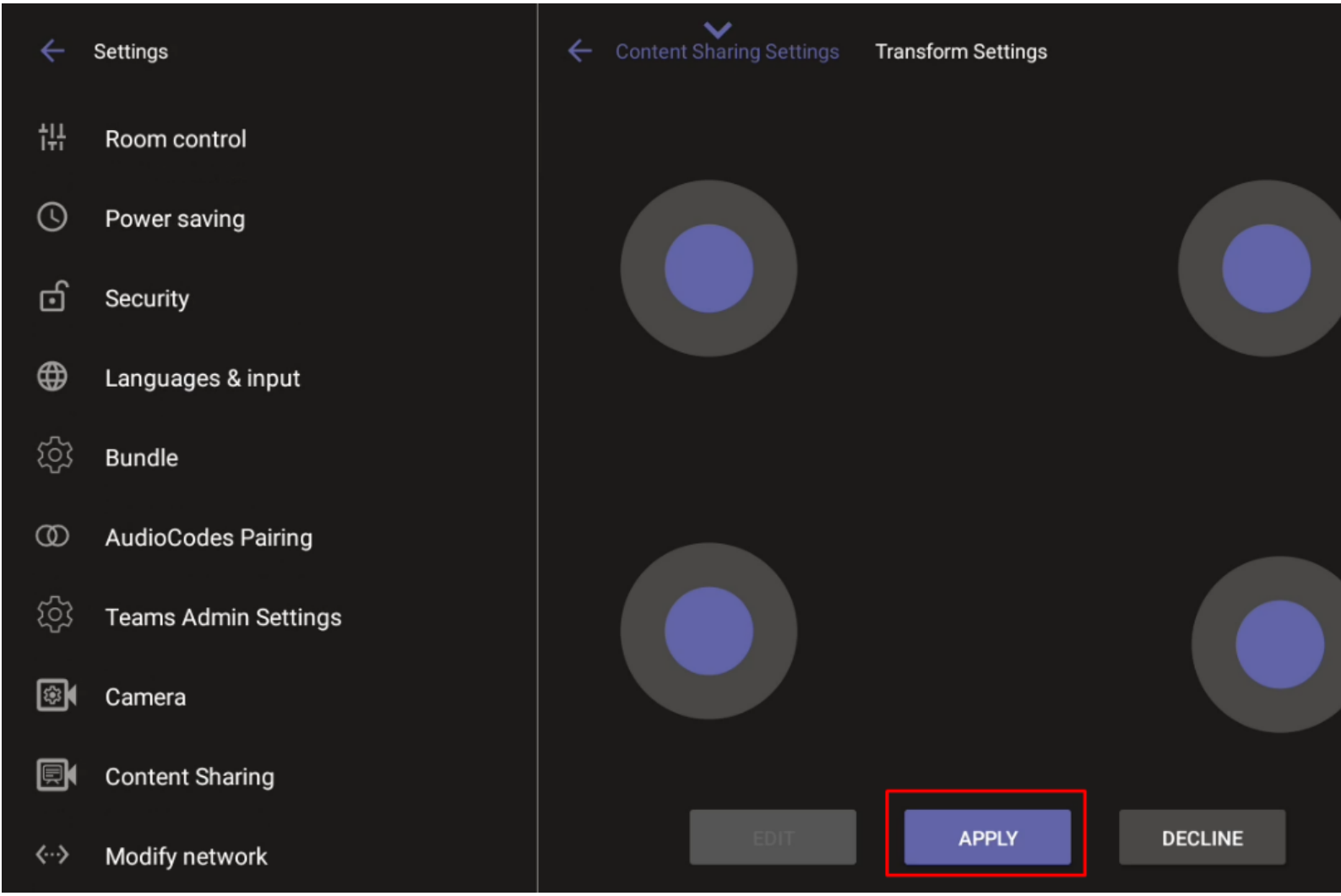
Presenters can share their physical whiteboard with remote participants using the **Content Camera** feature. To optimize the view, use **Transform settings** to define and capture the area precisely, isolating the whiteboard and removing unwanted margins beyond its edges.

Before starting, the admin must confirm the RXVCam10-CC is set as the content camera in **Teams Admin Settings > Devices**:

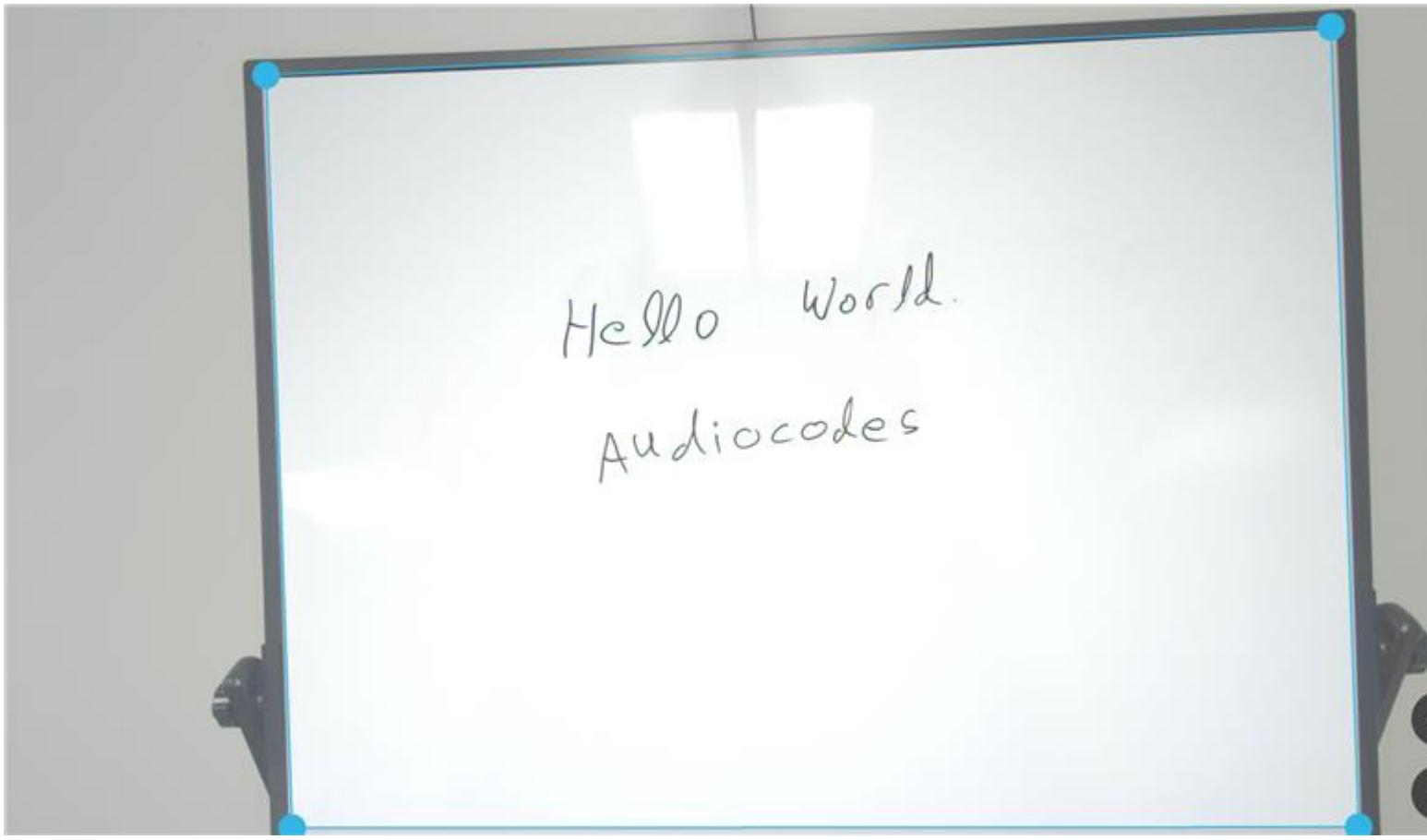


➢ **To share content:**

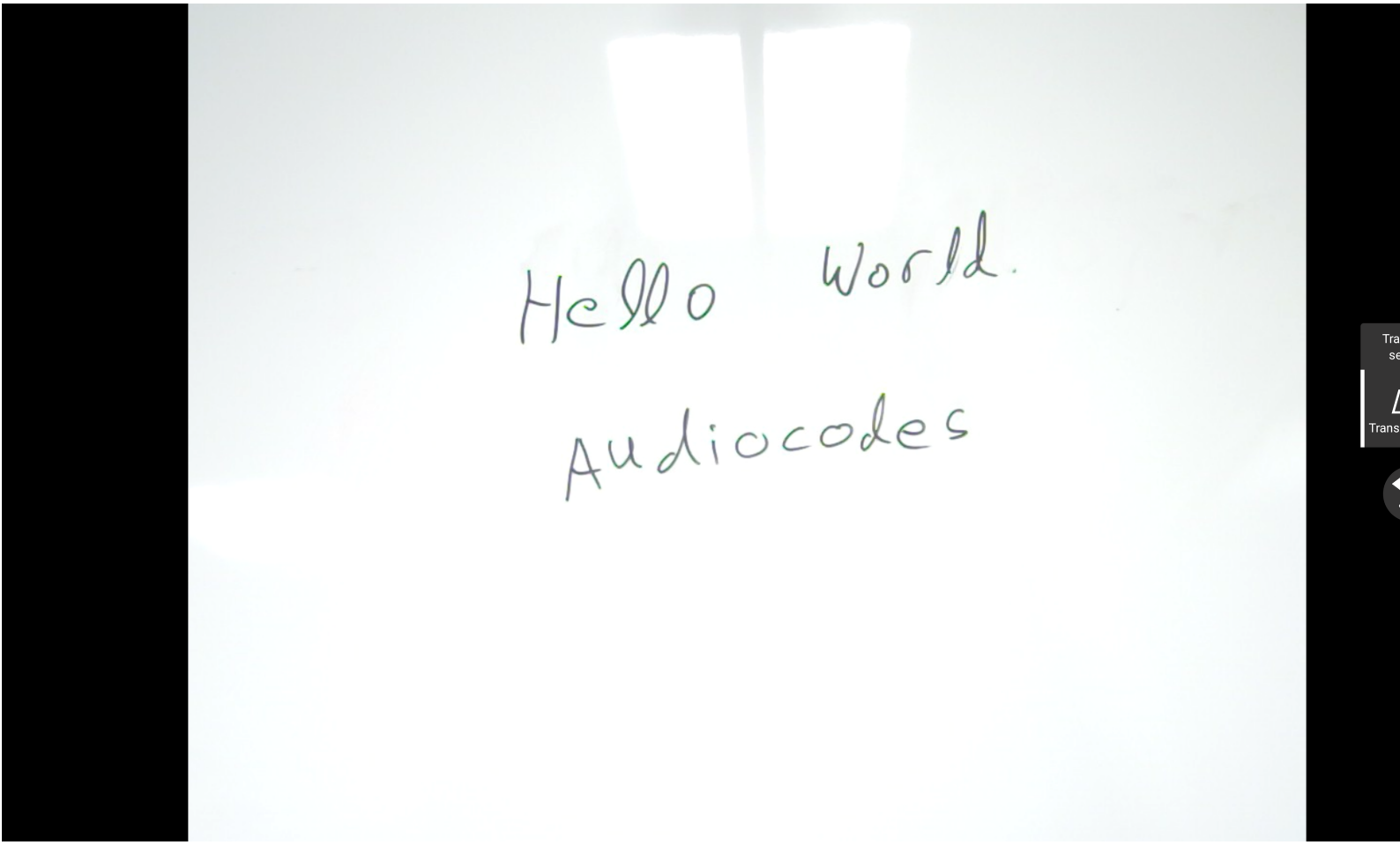
1. If not already logged in, log in to Device Administration (see Log in to Device Administration on page 69).
2. Under 'Device admin settings', scroll down and tap **Content Sharing**, then tap **Transform settings**:
3. Use the four joysticks on the RX-PAD to adjust the boundaries of the content camera's capture area:



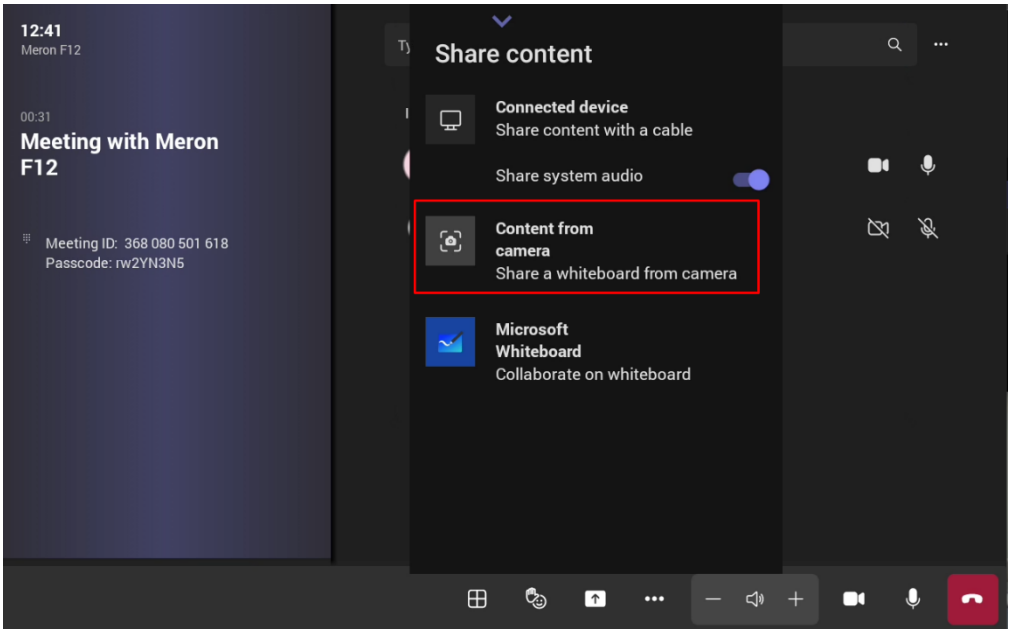
The admin can view the adjustment on the display:



4. When the desired shape is chosen, tap **Apply** to confirm. The shape can now be cut out and displayed on the screen:



5. To edit or delete the shape, return to the **Transform settings** screen.
6. In the Teams meeting, the user can share content from the connected 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.

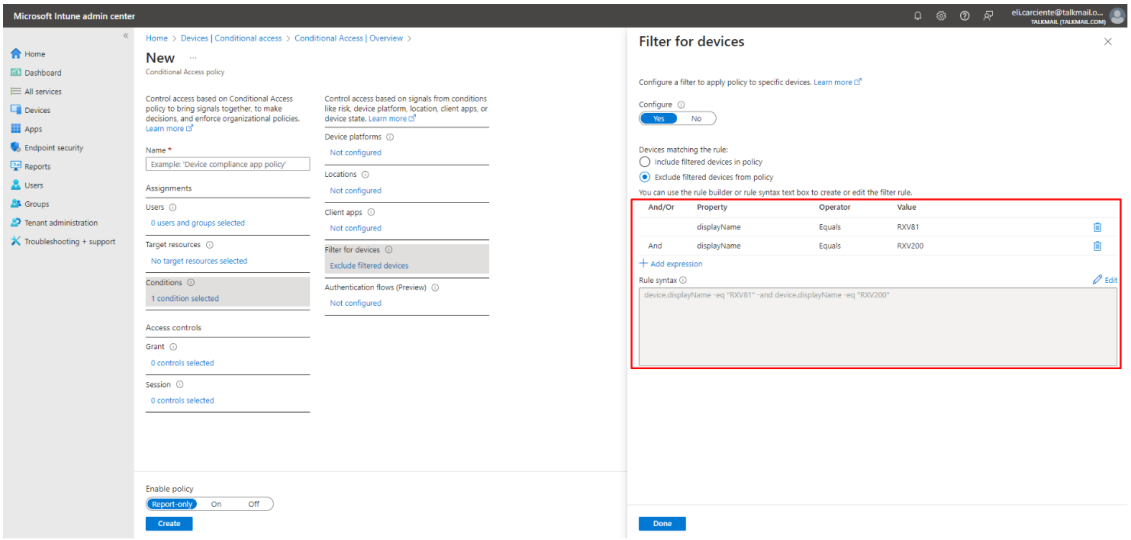
Create an Exclusion Group

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).

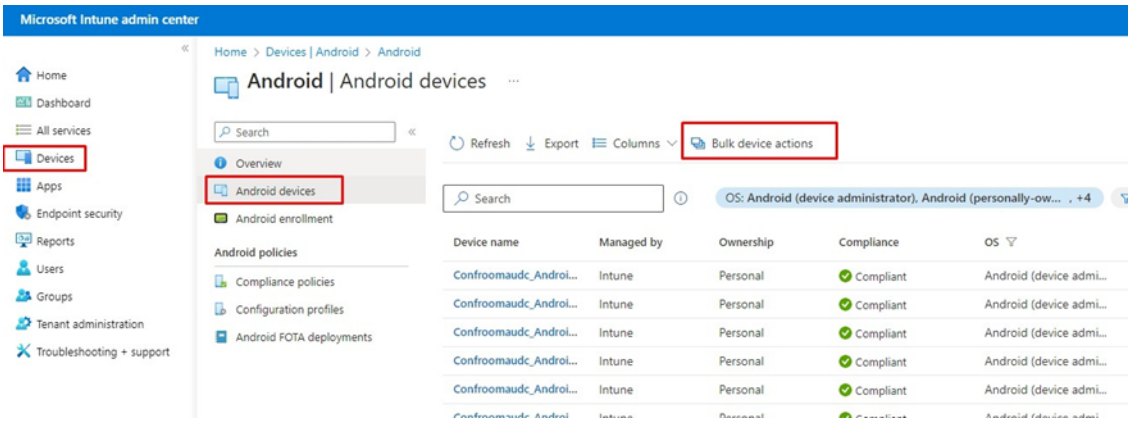


Remove Devices from Intune Admin Center

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

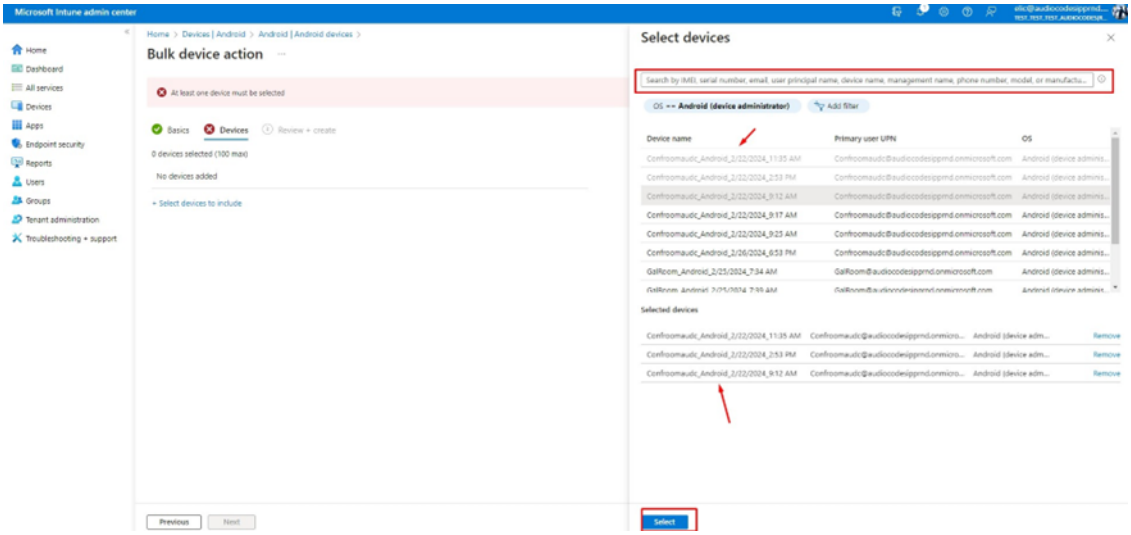
➢ **To remove devices from Intune admin center:**

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



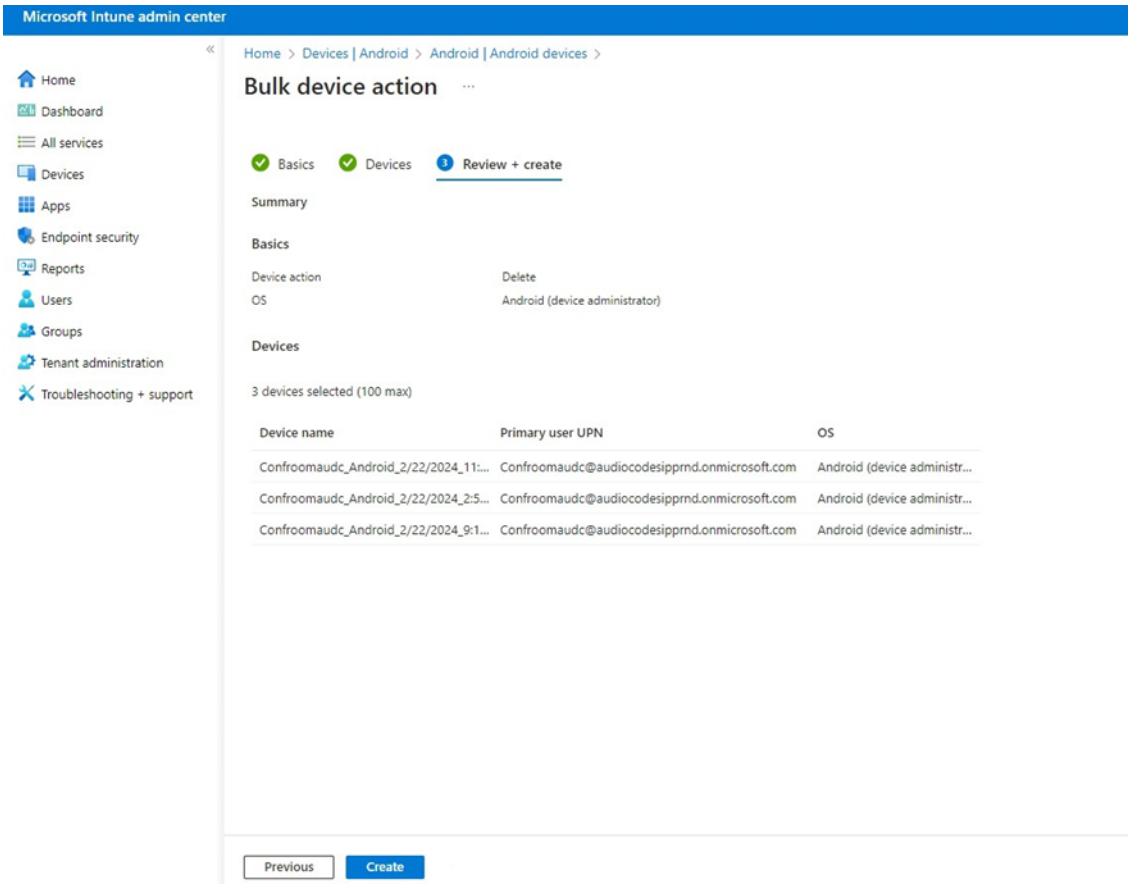
> The Intune admin center service is licensed according to the terms of individual licenses so not all network admins will be able to navigate to it. Check if the license you're using includes the service or not.

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**.



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**.



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:

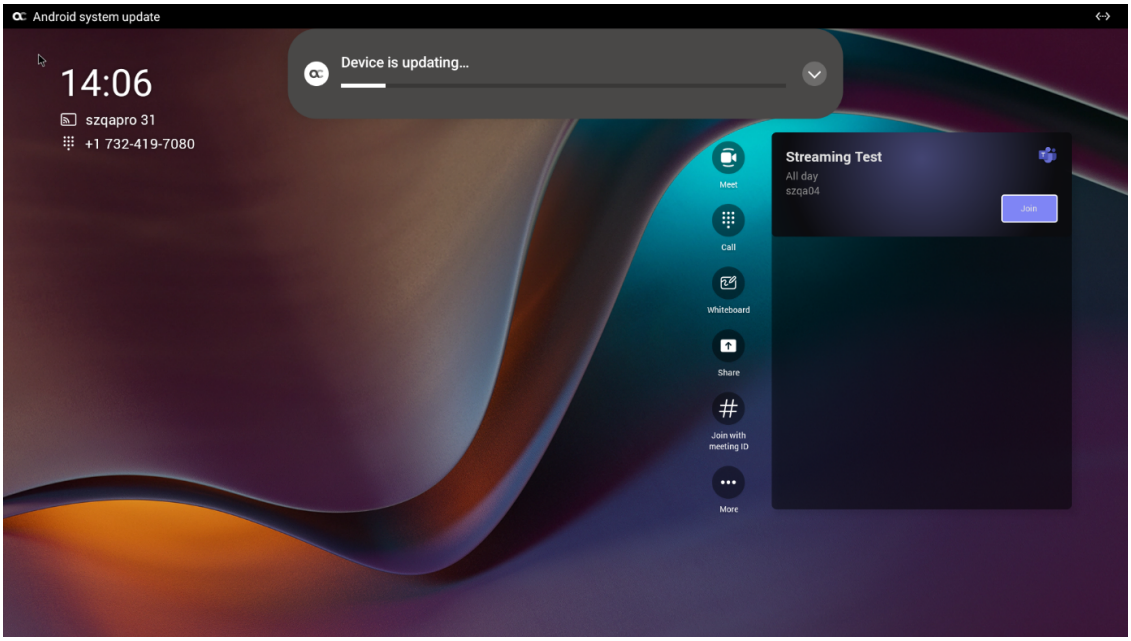
- `Set-CalendarProcessing -Identity "Maxim_MTR" -DeleteSubject $false`
- `Set-CalendarProcessing -Identity "Maxim_MTR" -AddOrganizerToSubject $false`

Update RX-PAD 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.

During the update, notifications are displayed, indicating the device being updated and alerting the user not to reboot.



If prompted, tap **OK** to confirm the alert.

12 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 69).
2. Navigate to ‘Device Admin Settings’ (see Access Device Admin Settings on page 69).
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 102
- Copy Diagnostic Data to SD Card on page 102
- Reset the System Configuration on page 103
- Reset User Data on page 105
- Restart the Teams App on page 105
- Perform Debug Recording on page 105
- Control Screen Capture on page 105
- Control Remote Package Capture on page 106
- Return to Previous Version on page 106

Additional procedures for device monitoring and troubleshooting are:

- Perform Recovery Operations using the Power Button on page 106
- Save Logs while the Device is in Recovery Mode on page 108
- Restore Device Firmware via USB Disk on page 108
- Configure DSCP for QoS on page 109

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 74.

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 100).
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 100).
2. Tap **Diagnostic Data**.
3. Tap **OK** to confirm 'Copy logs to sdcard'; the device creates all necessary logs and copies them to the **SD Card/Logs** folder.
4. Get the logs using SCP notation as follows:

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

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

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

Reset the System Configuration

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

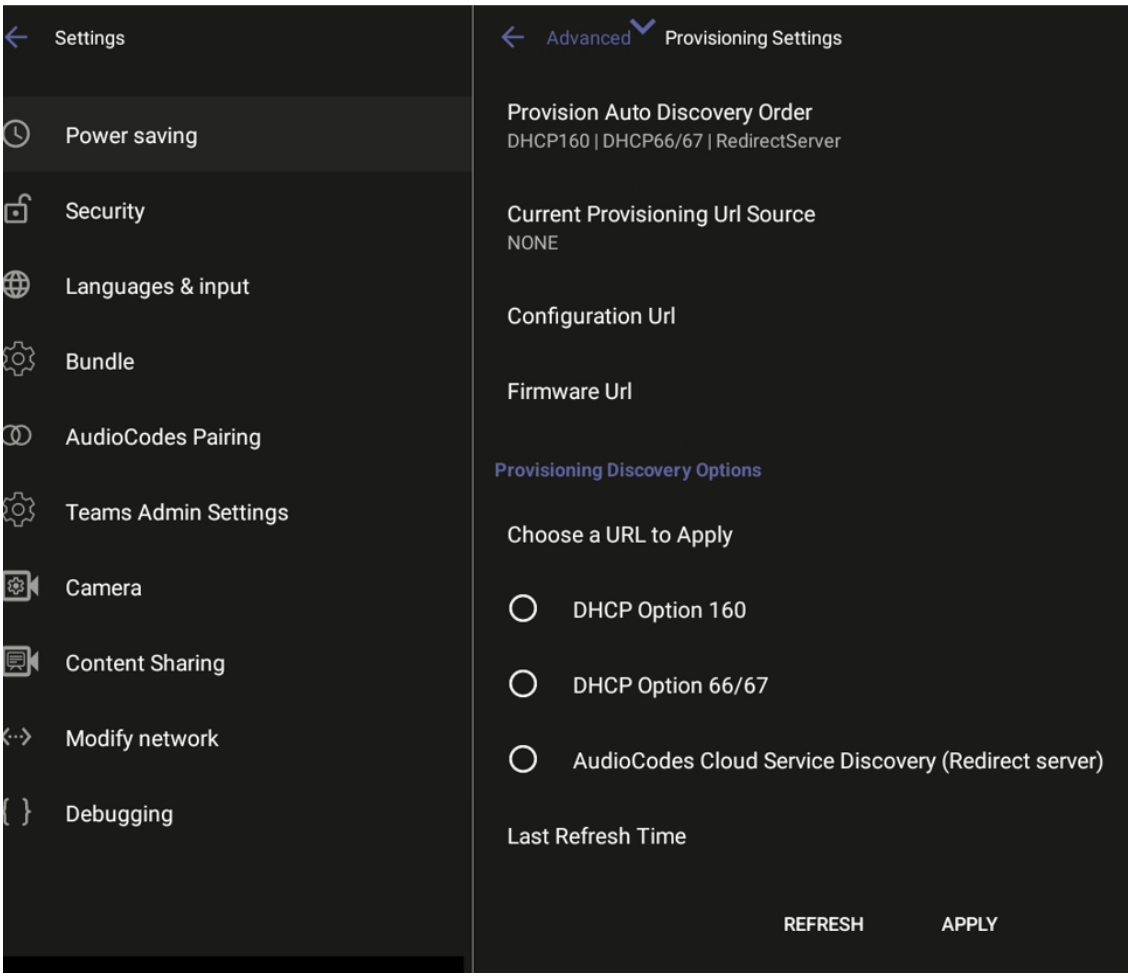
- Configure Provisioning Source Auto Discovery Settings below
- Perform a Full Factory Reset on the next page

Configure Provisioning Source Auto Discovery Settings

Admins can select the preferred discovery option for the RX-PAD 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 100).
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.



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

Reset to Original Configuration

The RX-PAD can be restored to default settings by pressing 15 seconds on a dedicated key/button on the bottom of the device.

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 100).
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 100).
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 100).
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 100).
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 100).
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 100).
2. Tap **Return to previous version**. The device changes the active firmware slot and undergoes a factory reset.

Perform Recovery Operations using the Power Button

While RX-PAD is powering up, admin can perform recovery operations by inserting a sharp pointed object, for example, a paper clip or pin, into the pinhole button shown below and pressing for the length of time shown in the following table.

When pressing the pinhole button, the device's main LED changes color after every n seconds; each color is aligned with a recovery operation option.

- Besides manual recovery options, Android devices also feature an independent, automatic problem detection and recovery attempt capability that can culminate in recovery mode or in switching image slots.
- Android devices also feature a 'hardware watchdog'. This feature resets the device if Android is stacked and doesn't respond (though Android stacking is unlikely); there's no recovery process; the device is only reset.

Use this as reference as to how to use the pinhole button to perform recovery operations.

When?	Action	Press for how long?	LED flashes 3x after release
Start pressing immediately after power up (on U-Boot / Universal Boot Loader)	Recovery mode (you can restore defaults from there)	~ 4 seconds	Red
	Switch slots A / B	~ 10 seconds	Green
	Loader	~ 15 seconds	Blue / Yellow
	Restore defaults	~25 seconds	Green + blue / Green + yellow
When successfully booted (on Android)	Reboot	From the Recovery menu	-
	Restore defaults	Long-press the Hold key for ~15 seconds	Flashes yellow once after release

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.

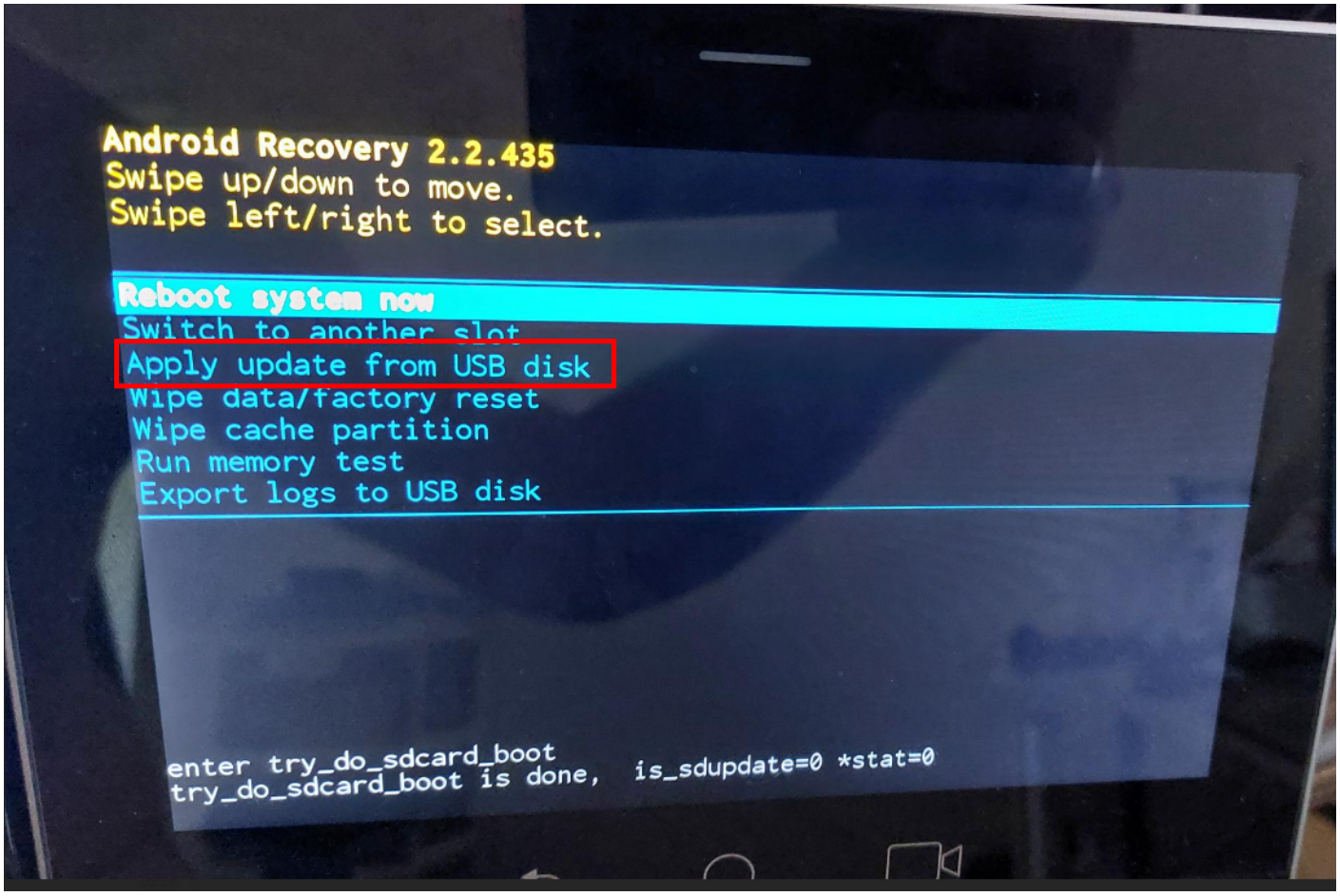
By simply clicking the **Export logs to USB disk** option, all logs are efficiently copied to the USB stick, providing a convenient and reliable method for log management during recovery procedures.

Restore Device Firmware via USB Disk

For recovery purposes, firmware can be applied to the RX-PAD from a USB disk.

➢ **To apply the firmware from the USB disk:**

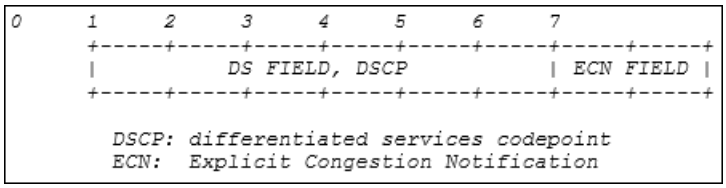
1. Enter recovery mode by pressing for 2-4 seconds the power button (Action: ENTER_ RECOVERY); the device's LED lights up red.
2. Short-press the power button to move down the menu options, and long-press to select an option.
3. Insert the USB disk with the target firmware.
4. Select the **Apply update from USB disk** option and then choose the correct firmware image from the disk.



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).



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

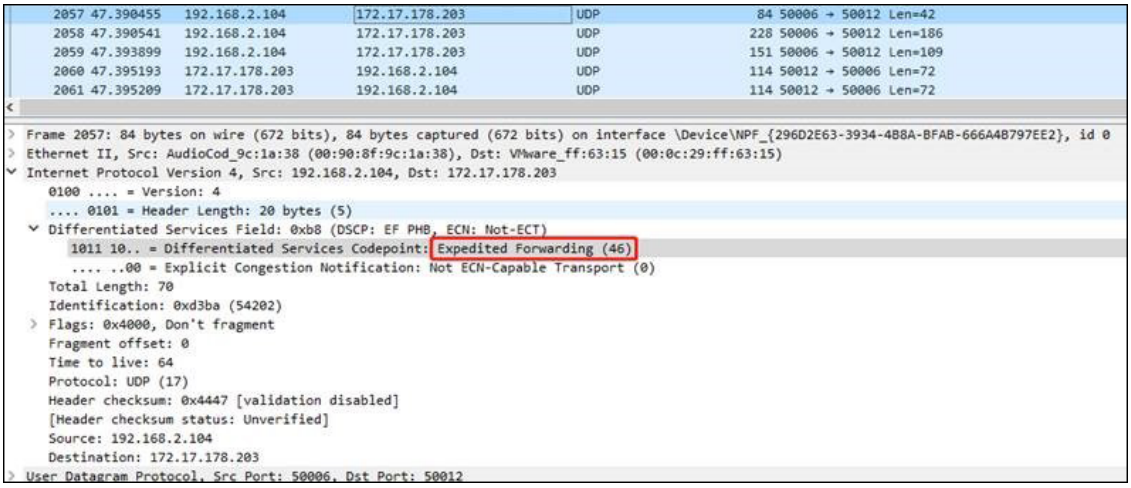
The DSCP value can be adjusted on the server, but not on the client.

The following figure shows the recommended port ranges:

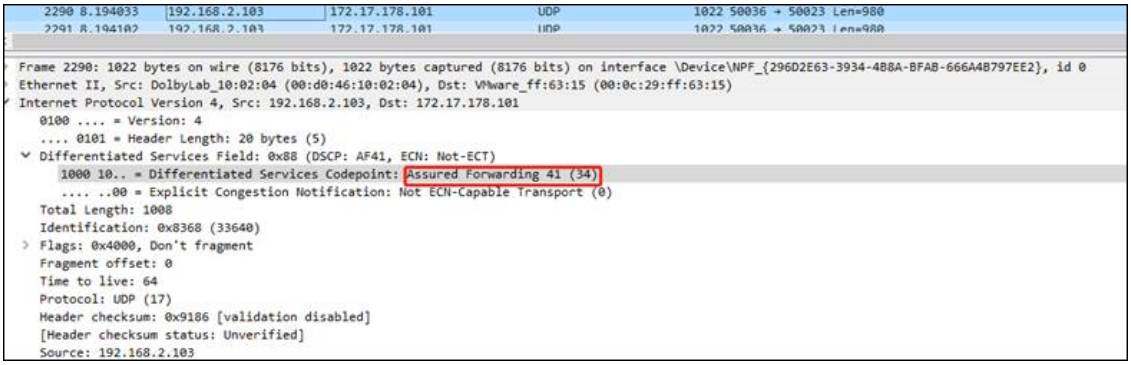
Table 1. Recommended initial port ranges

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:



The following figure shows the recommended DSCP setting for Video:



For more information refer to Microsoft's website.

13 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-18333