User's and Administrator's Manual

AudioCodes Room Experience (RX) Suite

RXV200

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

The RXV200 AV Intelligent Hub does not support using separate microphones and speakers. It only works with audio peripheral devices that combine both a microphone and speaker in a single unit.

Related Documentation

Document Name
RXV81 RXV200 RX-PAD RX-PANEL Release Notes
RXV200 Microsoft Teams Rooms on Android Compute Unit Quick Installation Guide
RX-PAD Room Controller User's and Administrator's Manual
Pairing RX-PAD with Microsoft Teams Room on Android
Teams Sign-in Implementation for AudioCodes MTRA Devices
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
09985	Initial document release for Version 2.8.574 (M1); AlphaSSL certificate; no firewall required for screen sharing; Composite AI individual camera settings and user modifications during meeting; selecting presenter to track; whiteboard sharing; preferred HDMI IN source; return to previous version
09987	Updated to Version 2.8.855 (M2)
09992	Updated to Version 2.8.917 (M3) Full document revision and structural changes 802.1x authentication parameters
09997	Updated to Version 3.0; provisioning source auto discovery; admin password brute force protection; new bundle RXV200-B50 Revised Getting Started section

Table of Contents

1 Introduction

The enterprise workspace and meeting space have changed dramatically over the past decade. Virtually all our communication today is hybrid, involving both on-site participants gathered in one or more meeting rooms and online participants located in their home offices or on the go. Modern meeting devices must be adaptable enough to accommodate any room size or shape, while minimizing the number of table-mounted accessories and devices apart from a microphone and a meeting room controller like the AudioCodes RX-PAD.

To meet this specific need, AudioCodes has created a range of RXV200 bundles which function as Microsoft Teams Rooms on Android™ (MTRA) devices.

The AudioCodes RXV200 MTRA is a robust, dependable and adaptable solution that enables an easy upgrade of any component within the meeting room, thereby facilitating the adoption of new and advanced devices to keep up with latest technology trends without excessive expenditure. Together with the RX-PAD Meeting Room Controller, it provides an easy meeting room experience that significantly boosts productivity.

This RXV200 MTRA unit serves as the meeting room's nerve center and sits at the heart of the RXV200 bundles. It can be connected to a variety of cameras, audio sources and advanced AI applications.

Controlled by AudioCodes' RX-PAD Meeting Room Controller, the RXV200 offers innovative features such as one-click-to-join with an integrated calendar for easy collaboration initiation, smooth content sharing and simple camera adjustments for a complete hybrid experience.

See also 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

RXV200 feature highlights are:

- Multiple device support for mix-and-match adaptability
- Reliable Android compute unit for every room configuration
- Simple deployment and management

- Cost-effective and value for money
- Allows future addition and upgrade of peripherals (mix-and-match of video and audio devices)
- Comprehensive support for Microsoft Teams features is provided for a complete hybrid collaboration
- Intuitive meeting experience with calendar integration and click-to-join or proximity-join experience
- Users can hear audio notifications triggered by RX-PAD through the RXV200 speaker, including Talkback accessibility, ensuring a streamlined and accessible communication experience during meetings and collaboration sessions.
- HDMI Out CEC (Consumer Electronics Control) One-Touch-Play command, triggered by RX-PAD's human sensor, turns on/off the TV screen. For more information, see the AOSP documentation.
  - When RX-PAD (pre-set to 'Screen timeout') enters sleep mode, it automatically triggers RXV200 to enter sleep mode as well, activating the CEC One-Touch-Play command to turn the TV off.
  - When RX-PAD's human sensor wakes up RX-PAD, RXV200 wakes up as well and turns the TV on.

Benefits

- Superb video quality provided by AudioCodes's cameras for any size of meeting room:
  - RXVCam50 AI camera with HD 4K resolution, EPTZ, and auto framing capabilities
  - RXVCam360 video conferencing camera providing a 360° Field of View, ultra-high image and video quality, and powerful speakers
  - RXVCam70 PTZ camera for medium and large meeting rooms, with both close-up and panoramic high-quality lenses, and advanced AI features for optimal audio and video
- Hear and be heard with crystal-clear sound through the RXVCam360 camera's built-in audio, the RX40 sound bar or the RX15 speakerphone
- Human sensor for activating the system and welcoming the user upon proximity
- An optimal solution for small to large meeting spaces
- Fully controllable by the RX-PAD Meeting Room Controller center-of-room intelligent touch controller
- Optional centralized management with AudioCodes' OVOC / Device Manager (see Management on page 11)

Bundles

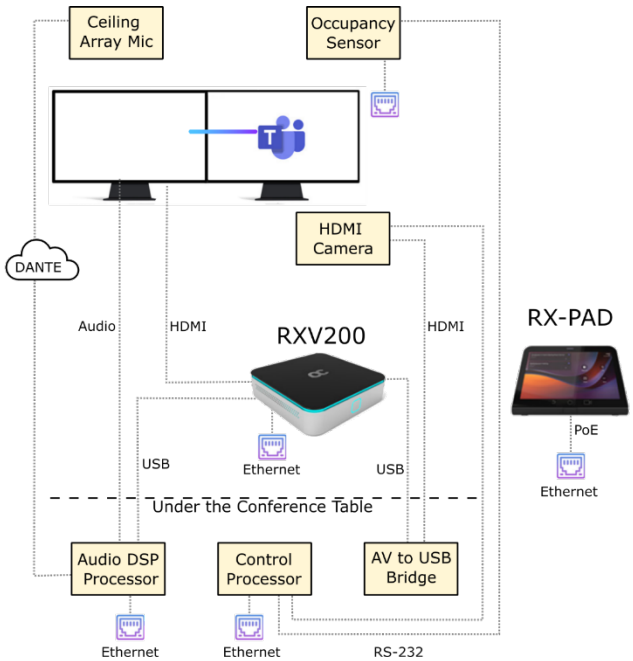
The *RXV200* MTRA supports multiple devices for mix-and-match adaptability and simplified deployment and management. Providing a reliable solution for every room layout and allow easy meeting room component upgrades, RXV200 is available in six main bundles, as listed in the following table:

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 the next page.
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 5.
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 6.
RXV200-B40	■ RX-PAD ■ RXVCam50 ■ RX40 (audio) ■ Medium size rooms of 6-12 participants ■ Productivity: Meeting Insights

Name of Bundle	Description
	See the RXV200-B40 Bundle on page 7.
RXV200-B50	■ RX-PAD ■ RXVCam50 ■ RX-HDL200 sound bar (audio) ■ Medium size rooms of 6-12 participants ■ Productivity: Meeting Insights See the RXV200-B50 Bundle on page 8.
RXV200-B70	■ RX-PAD ■ RXVCam70 ■ RX40 (audio) ■ Large rooms of 10-18 participants ■ Productivity: Meeting Insights See the RXV200-B70 Bundle on page 9.

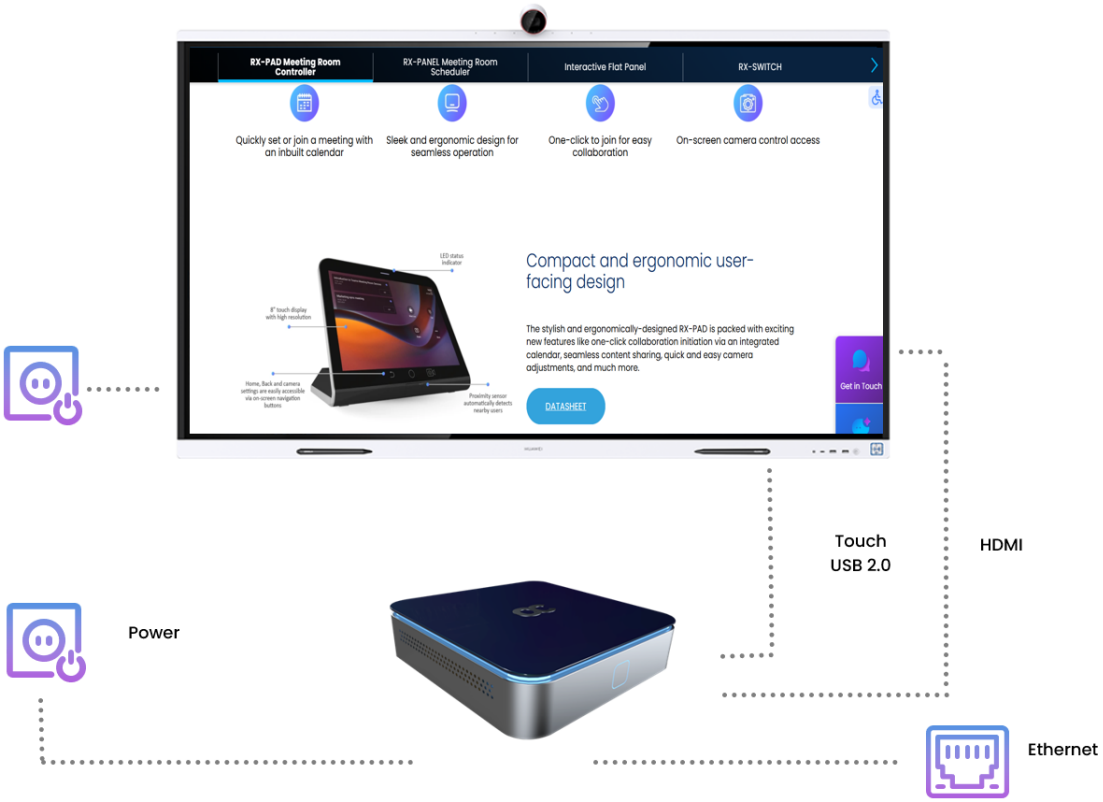
RXV200-BO5 Bundle

The following figure illustrates the RXV200-B05 bundle.



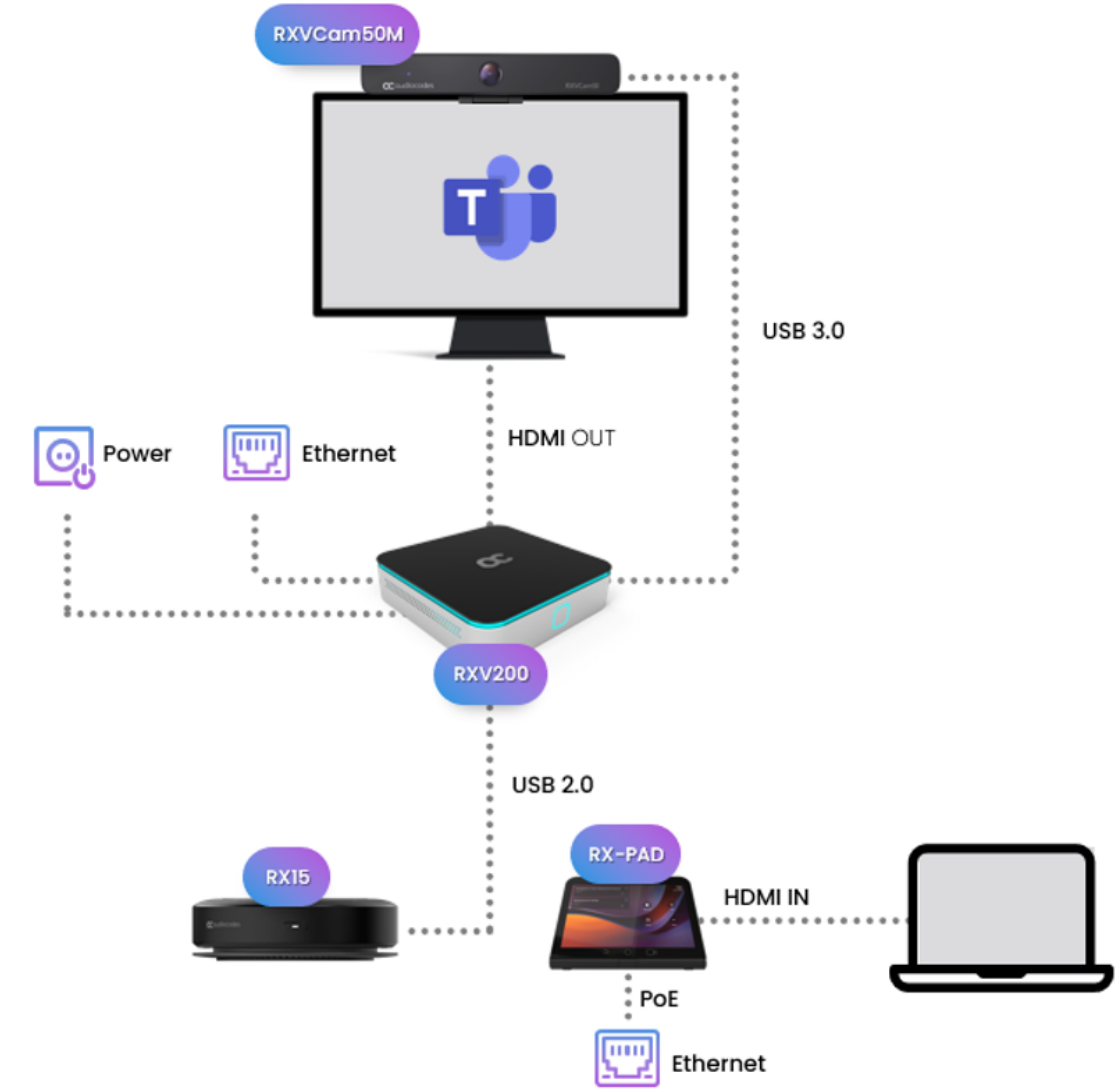
RXV200-B09 Bundle

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



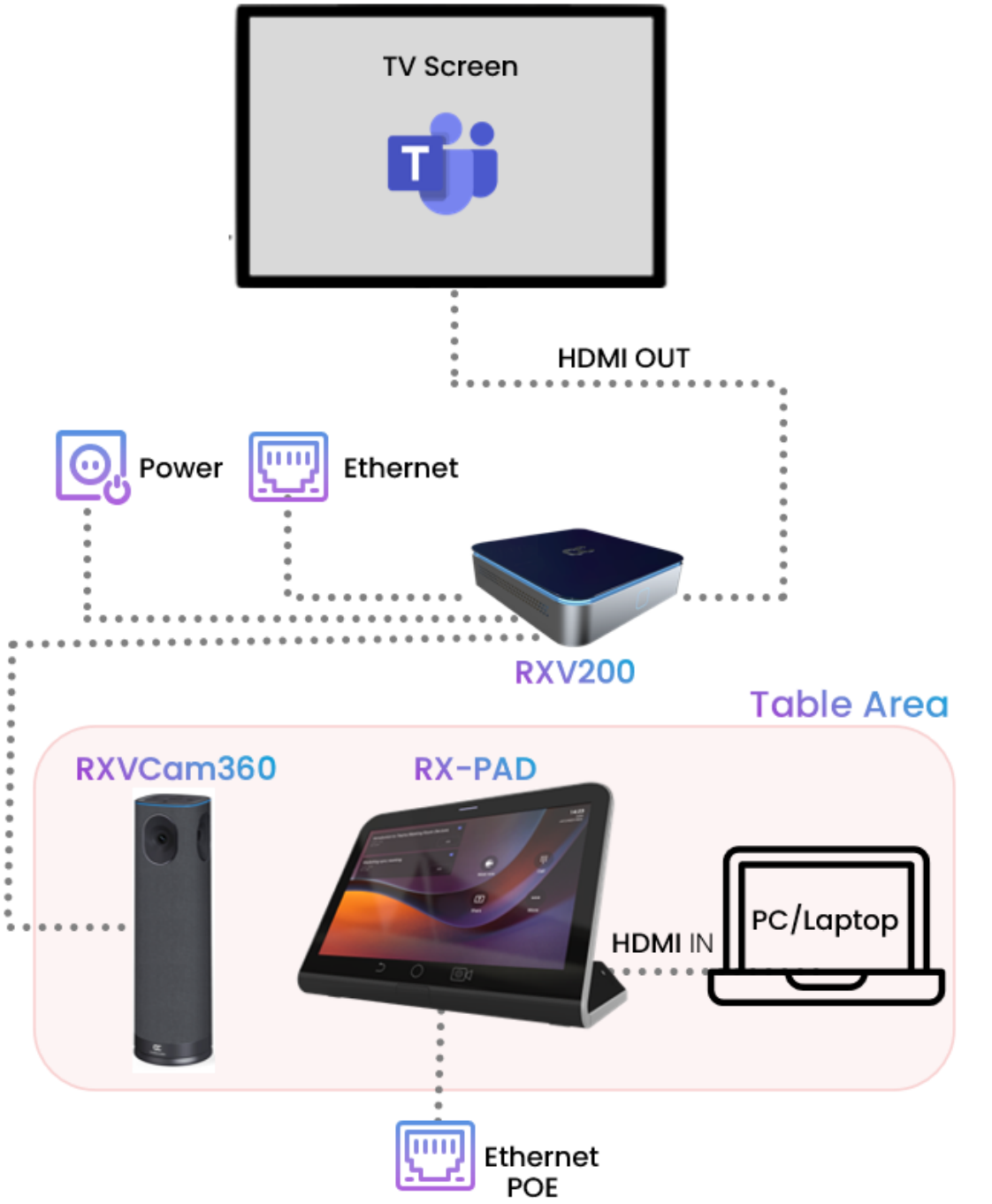
RXV200-B20 Bundle

The following figure illustrates the RXV200-B20 bundle.



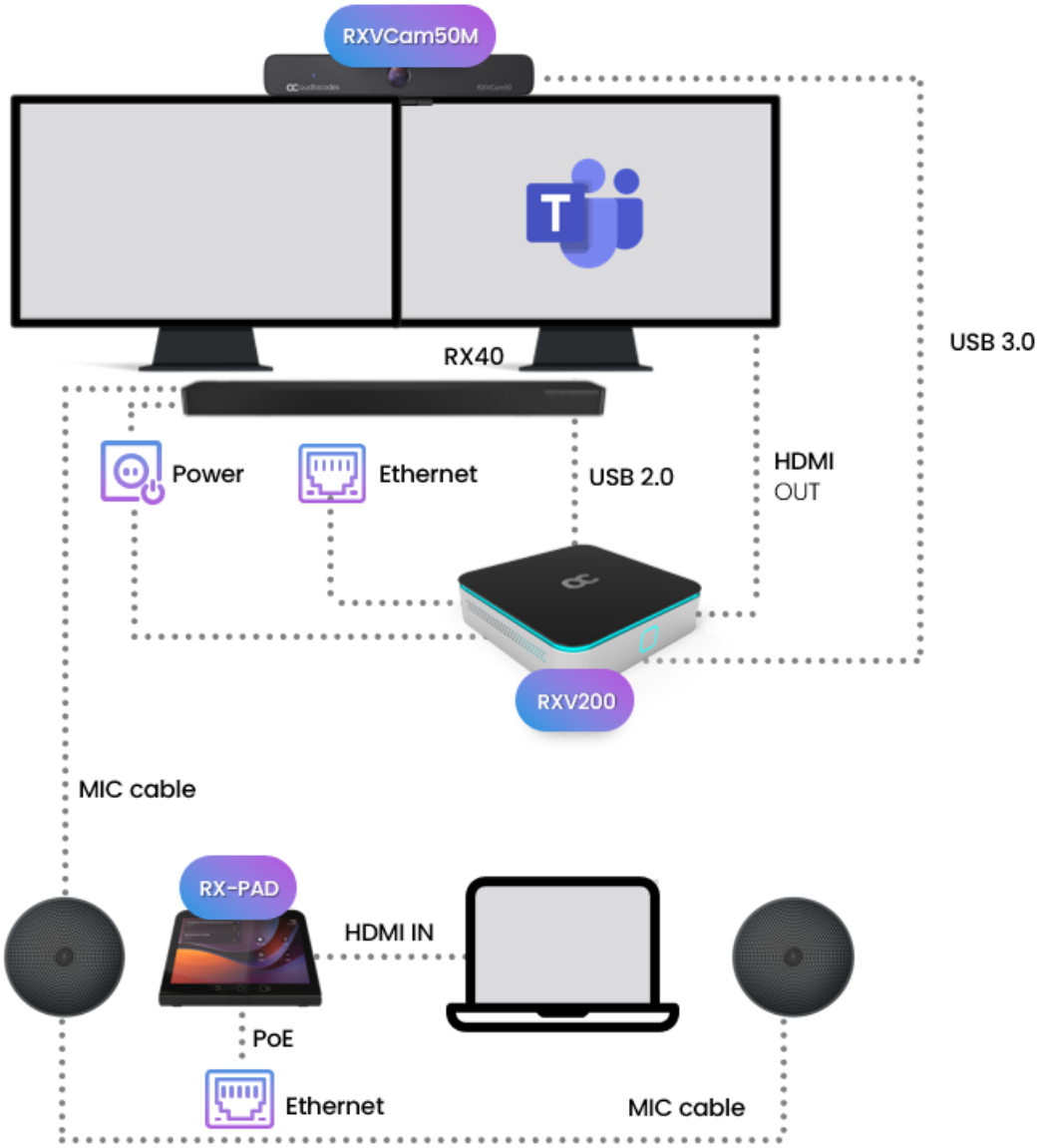
RXV200-B360 Bundle

The following figure illustrates the RXV200-B360 bundle.



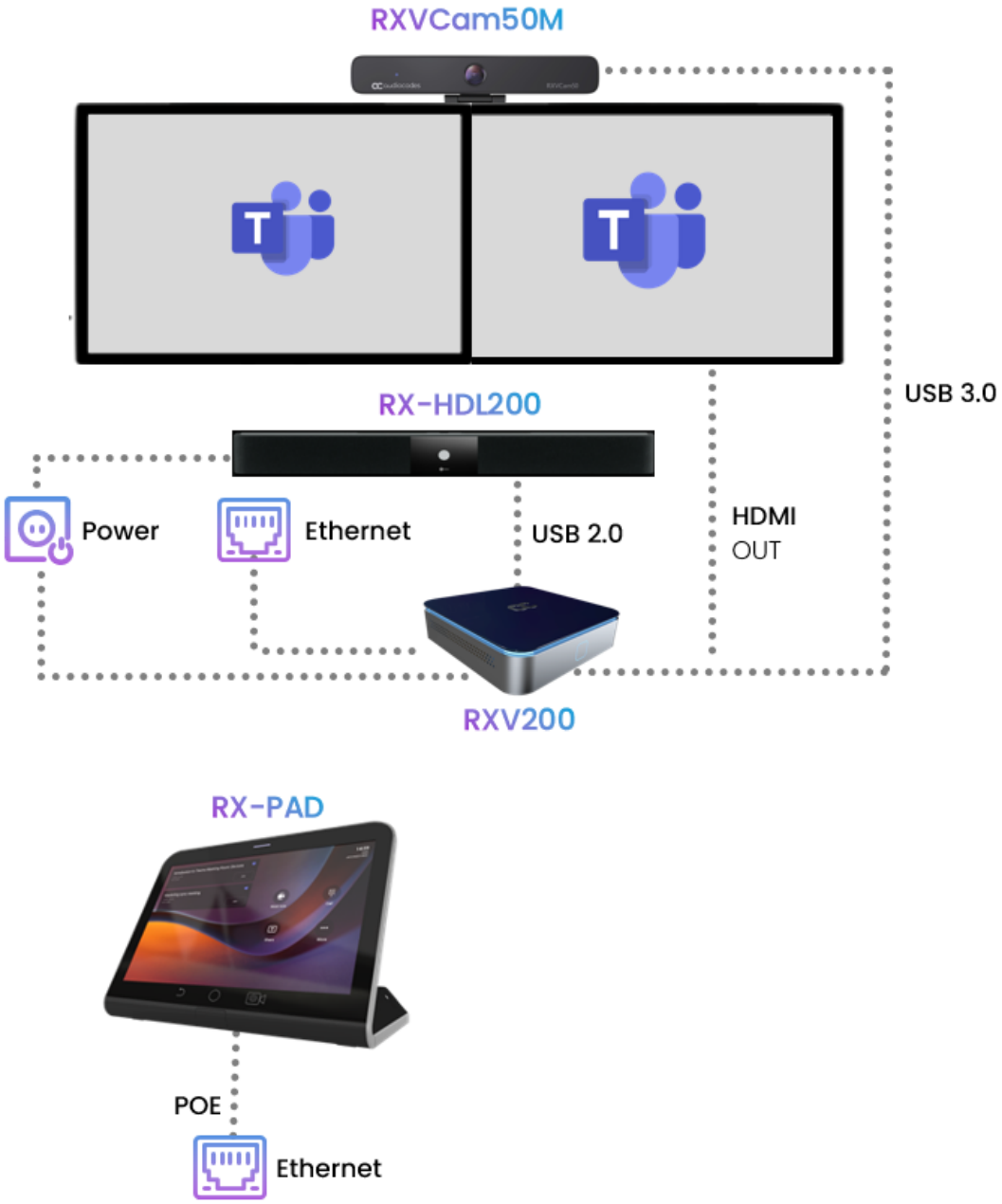
RXV200-B40 Bundle

The following figure illustrates the RXV200-B40 bundle.



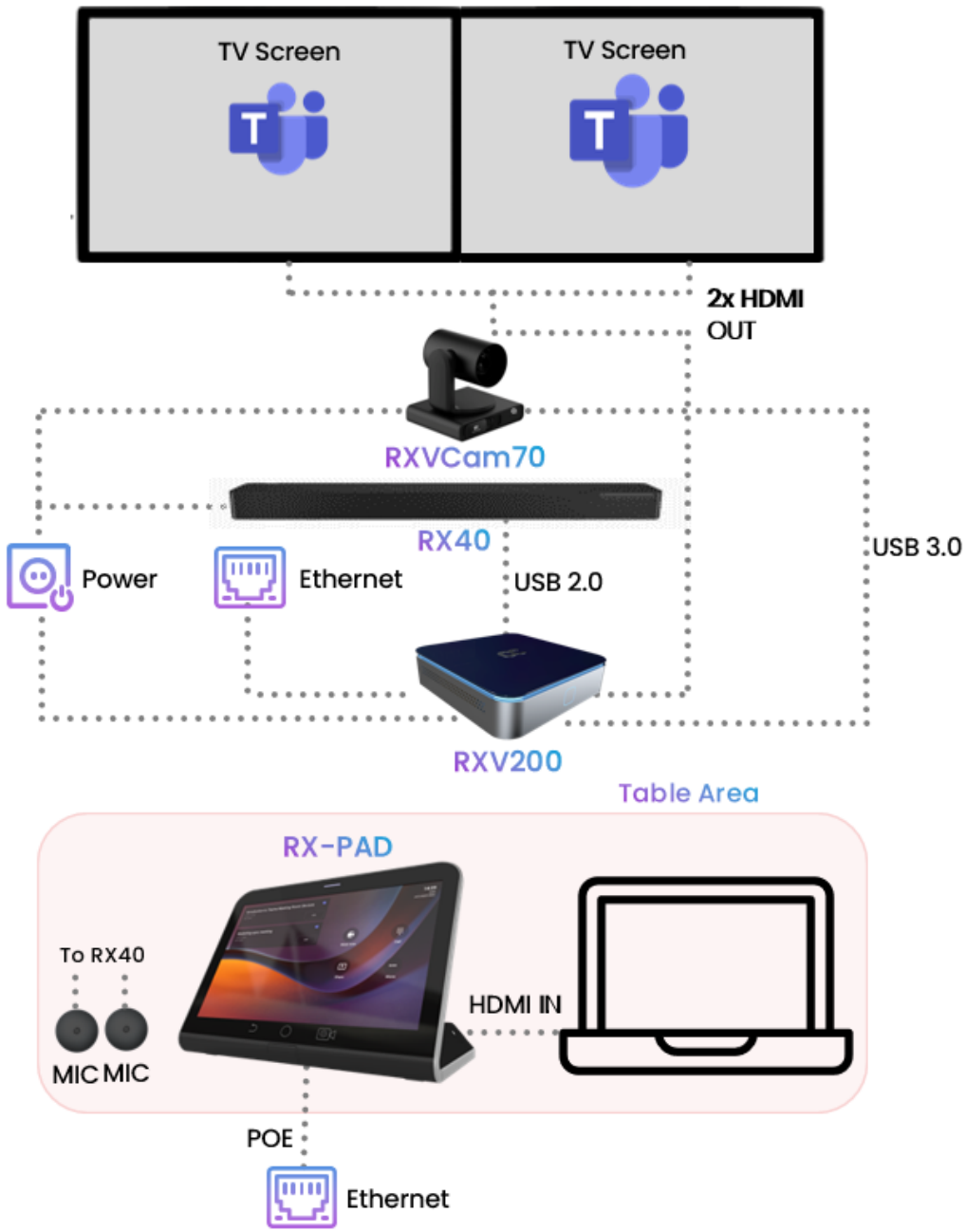
RXV200-B50 Bundle

The following figure illustrates the RXV200-B50 bundle.



RXV200-B70 Bundle

The following figure illustrates the RXV200-B70 bundle.



Hardware

The RXV200's plug-and-play simplicity makes it easy to connect a screen, sound system, and AI camera with auto- framing to simplify Microsoft Teams physical whiteboard sharing, all controlled by a meeting room controller.

- HDMI In enables participants to share their desktop during a meeting via a simple cable connection
- 4K HDMI Out enables users to seamlessly connect and display ultra-high-definition visuals in compatible external displays during Teams meetings, ensuring a visually immersive and crystal-clear collaboration experience. Whether you're presenting a slideshow, streaming

content, or simply extending your display, 4K HDMI Out enhances the overall viewing experience.

- 1x USB C and 2x USB A to connect camera and audio peripherals. The C port can be connected to a touch screen display via a Type C cable.

The HDMI-IN status can be monitored from the System State page (see Monitor the System Status on page 88).

Management

RXV200 bundles are managed using AudioCodes' On-prem or Live Platform Device Manager, or Microsoft's Teams admin center (TAC), enabling IT admins to monitor and upgrade the devices from anywhere. Using Device Manager, IT admins can easily monitor and manage all bundled devices from a centralized location. Management includes:

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

Admins can monitor the status of the device's software modules from the System State screen (see Monitor the System Status on page 88).

- 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 RXV200 specifications, see the RXV200 datasheet.
- For RX-PAD specifications, see the RX-PAD datasheet.
- For RXVCam360 specifications, see the RXVCam360 datasheet.
- For RXVCam70 specifications, see the RXVCam70 datasheet.
- For RXVCam50 specifications, see the RXVCAM50 datasheet.
- For RX15 specifications, see the RX15 datasheet.
- For RX40 specifications, see the RX40 datasheet.

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 RXV200 consists of:

1. Installing the RXV200 unit:
   - Reviewing the package contents checklist
   - Positioning
   - Mounting
   - Cabling
   - Powering up

   For details, see the *RXV200 Microsoft Teams Rooms on Android Compute Unit Quick Installation Guide* shipped with the product oravailable from AudioCodes.
2. Pairing and setting up the RXV200 unit with RX-PAD or with a touch screen (see Set up RXV200 with the Initial Configuration Wizard below).
3. Configuring and operating the RXV200 using the paired RX-PAD, as described in the following sections of this manual.

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

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

Set up RXV200 with the Initial Configuration Wizard

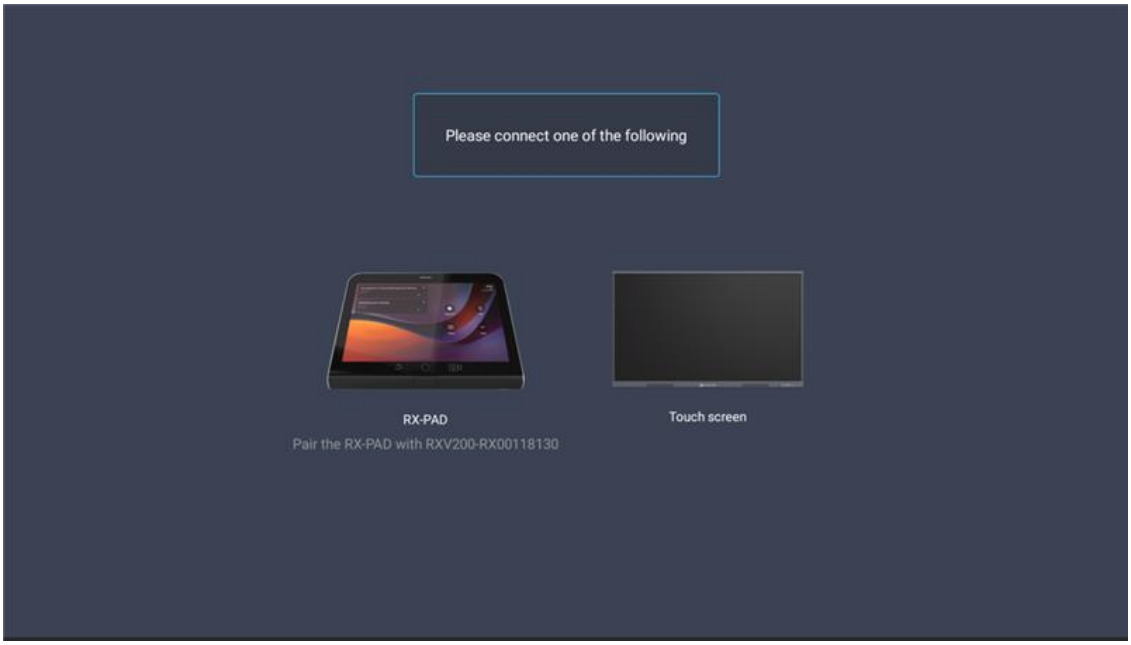
The Initial Configuration Wizard allows you to easily set up your MTRA with *either* of the following input devices:

- For systems with an RX-PAD, from the RX-PAD after pairing (see Setting up MTRA with RX-PAD below)
- For systems with a touch screen (RXV200-B09 Bundle on page 5), from the RXV200 after pairing with the touch screen (see Setting up RXV200 with Touch Screen on page 16)

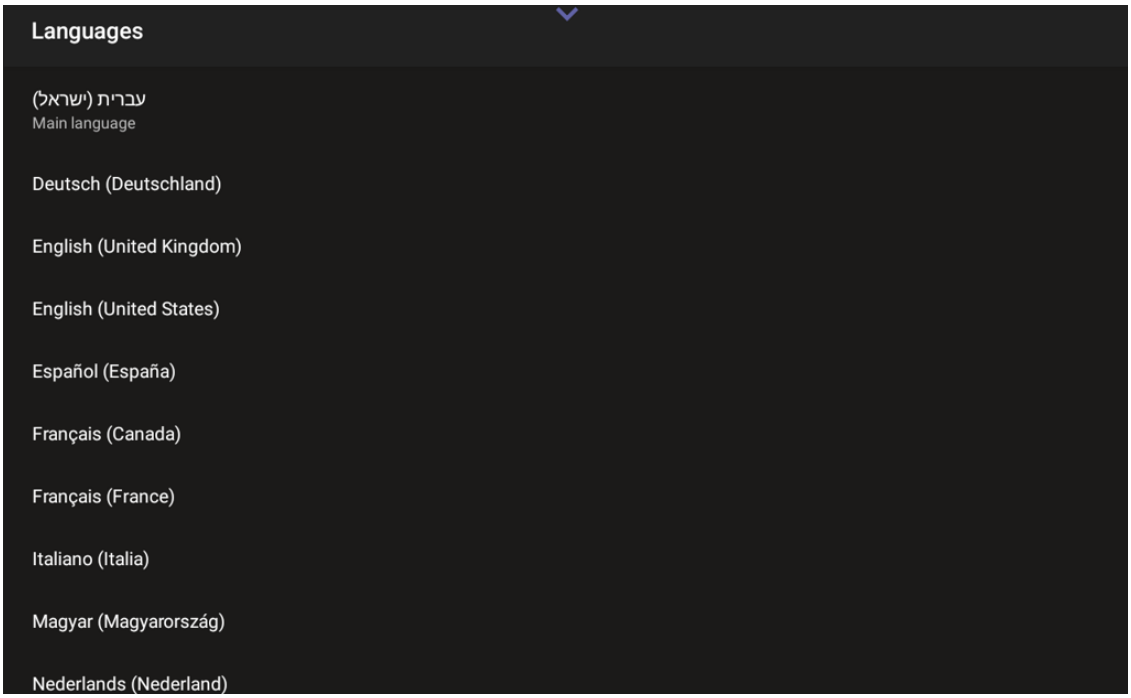
Setting up MTRA with RX-PAD

➢ **To set up your MTRA:**

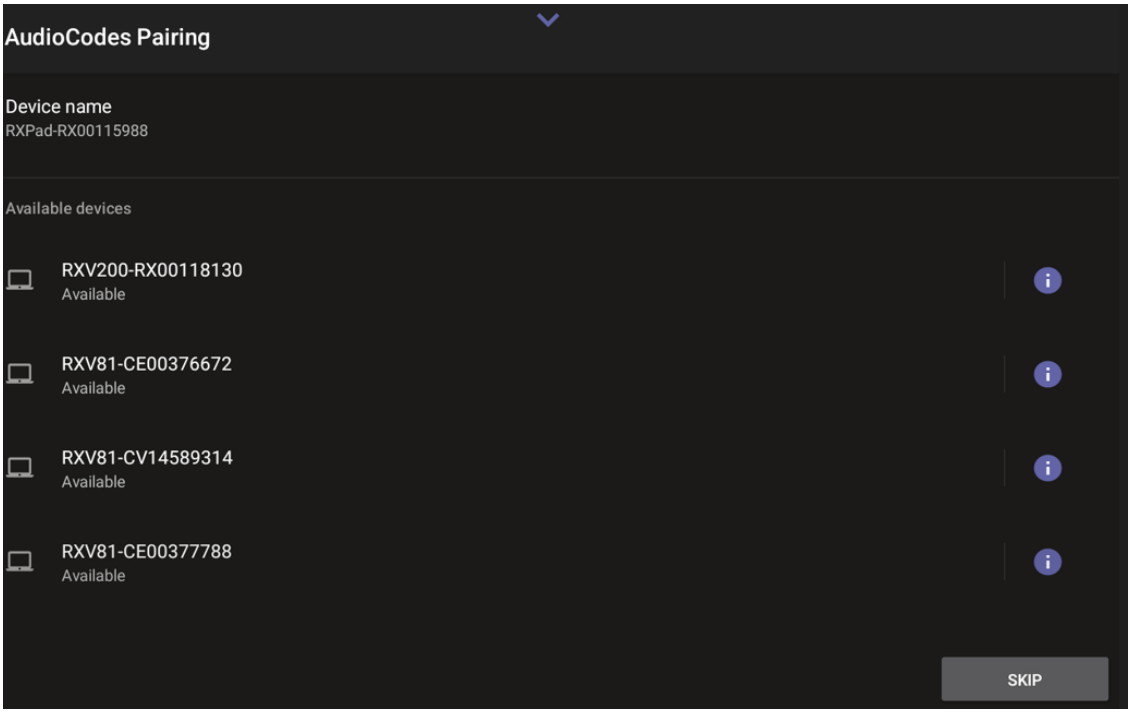
1. Connect the RXV200 and the RX-PAD to the power supply and the same local network.
   - The RXV200 starts up and prompts you to connect an RX-PAD or a touch screen.



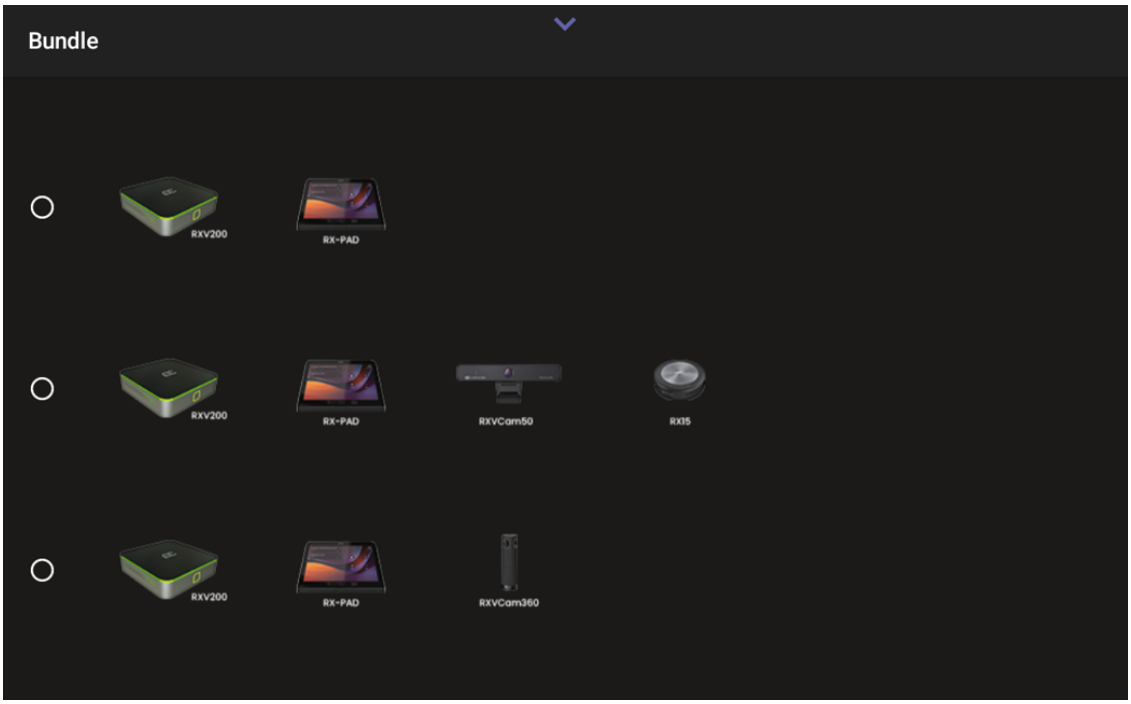
- The RX-PAD starts up and prompts you to select a language for the UI.



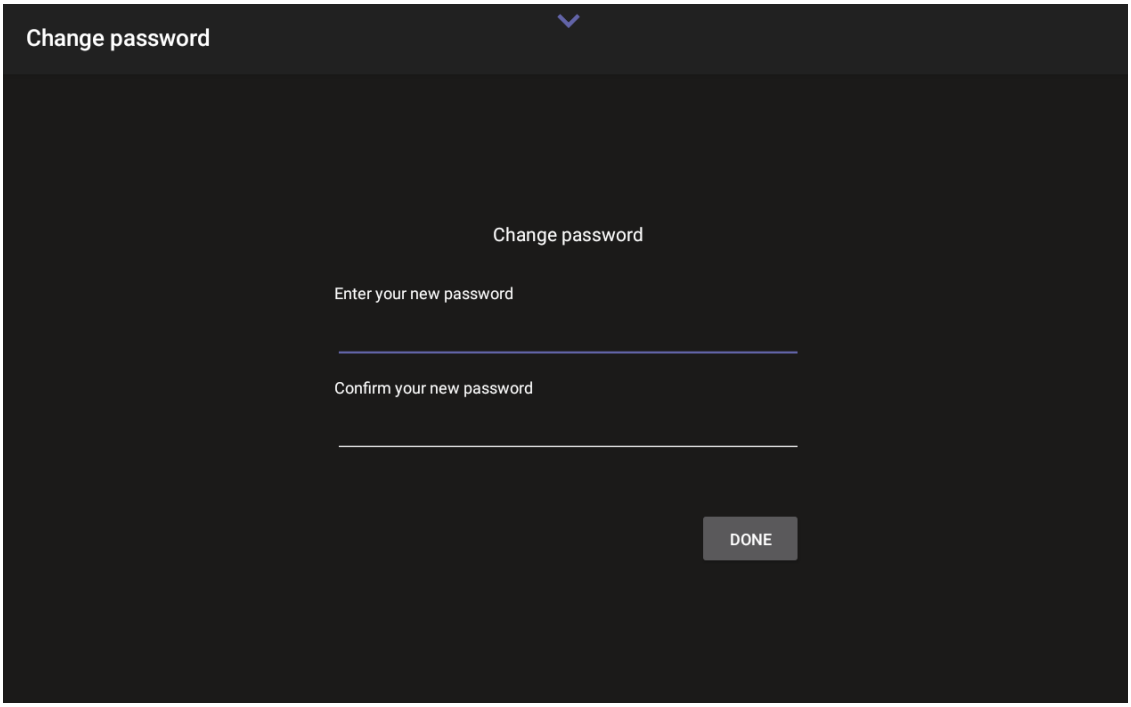
2. On the RX-PAD, select the requested language. The AudioCodes Pairing page is displayed, listing the available MTRAs:



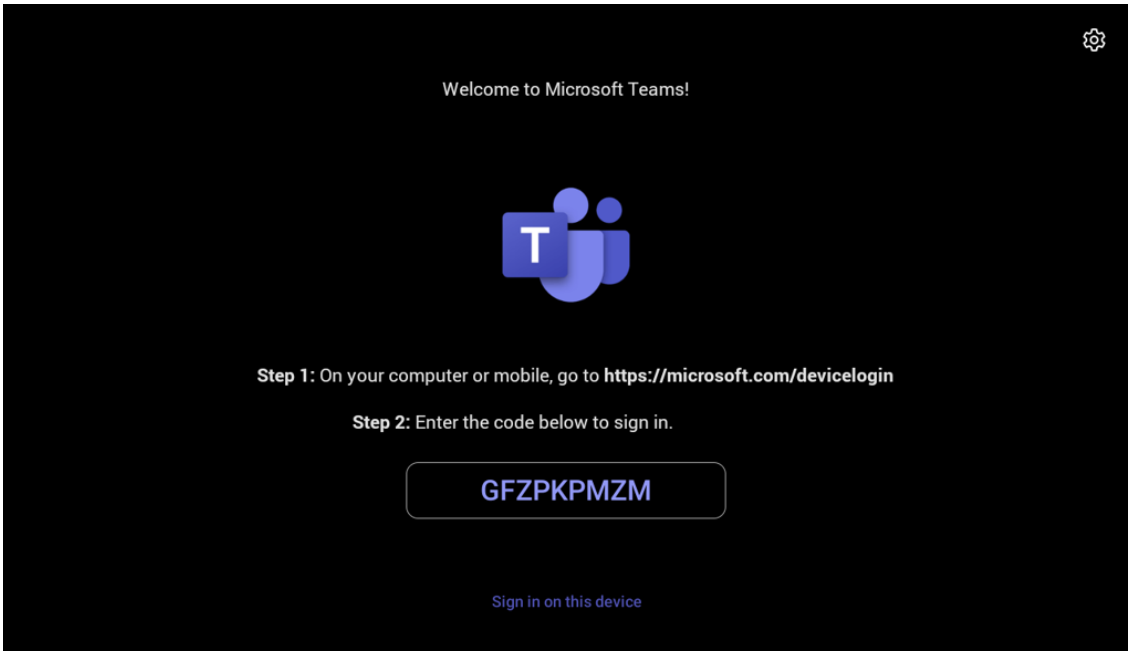
3. Select the relevant RXV200. The RX-PAD finalizes the pairing process and prompts you to select a bundle.



4. Select the bundle (see Bundles on page 3 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.



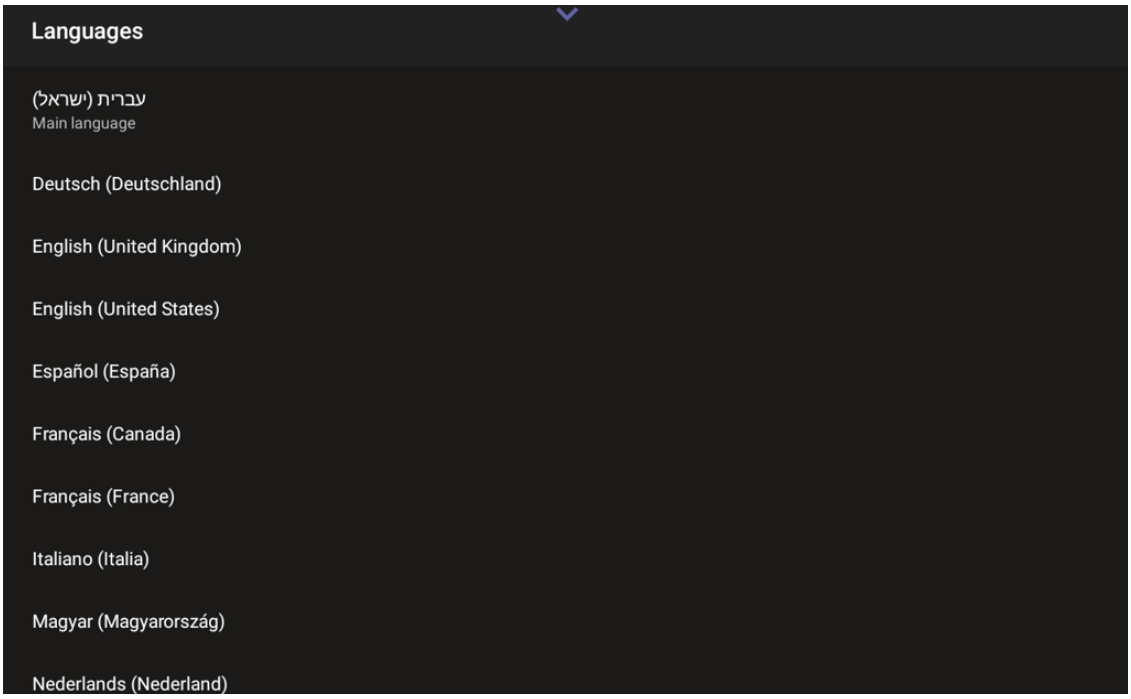
6. On both devices, sign in to your Microsoft account.

Setting up RXV200 with Touch Screen

➢ **To set up your RXV200:**

1. Connect the RXV200 and the touch screen to the power supply and the same local network. The RXV200 automatically identifies and pairs with the touch screen.

2. When the pairing is complete, the RXV200 prompts you to select the language for the UI. Select the requested language.

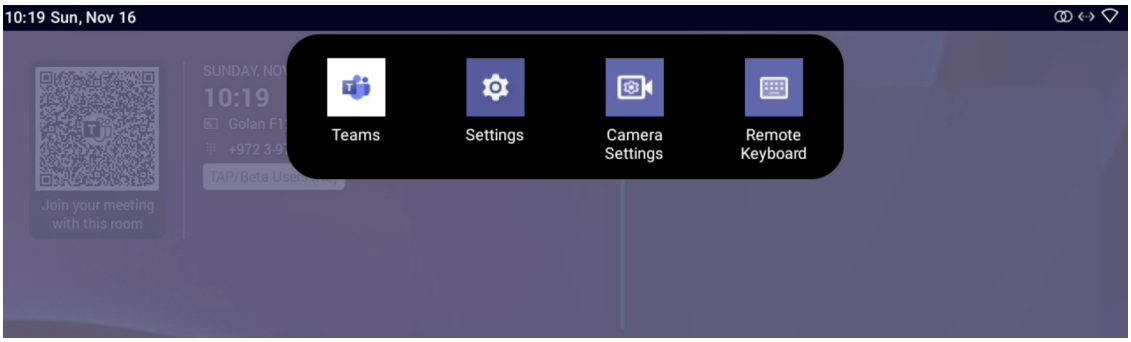


3. Select the requested language. You are prompted to change the (default) admin password.
4. After changing the password, the Microsoft Teams sign-in page is displayed on both devices, showing the code you need to sign into your Microsoft account.
5. Sign in.

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.

After Pairing

If you paired a RX-PAD with your RXV200 , scroll down in the RX-PAD to this:



From left to right:

- **Teams** (tap to refresh RX-PAD's UI)

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

3 Meetings and Calls

This chapter describes how you can use your RXV200 for conducting value-added meetings. It focuses on functions that you perform from the paired RX-PAD (or touch screen). 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 26 and Composite AI Camera on page 45.
- For detailed instructions on how to operate an RX-PAD, refer to the RX-PAD Room Controller User's and Administrator's Manual.

Schedule Meetings

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

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

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

Ad-hoc Meetings and Calls

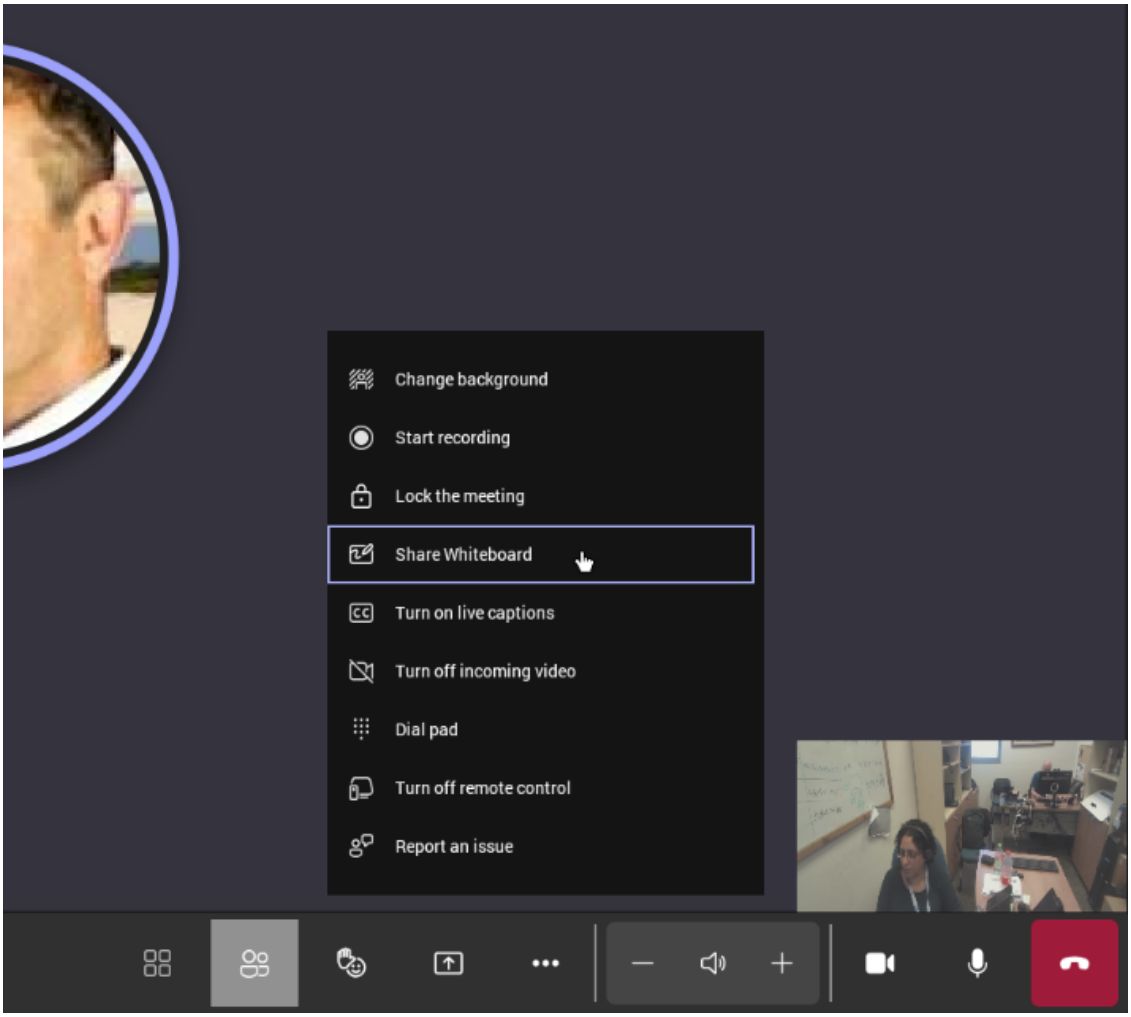
Ad-hoc meetings and calls can be conducted from the RX-PAD homepage in the same way as from a Teams channel. For details, see the relevant Microsoft Teams documentation.

Share a Microsoft Whiteboard

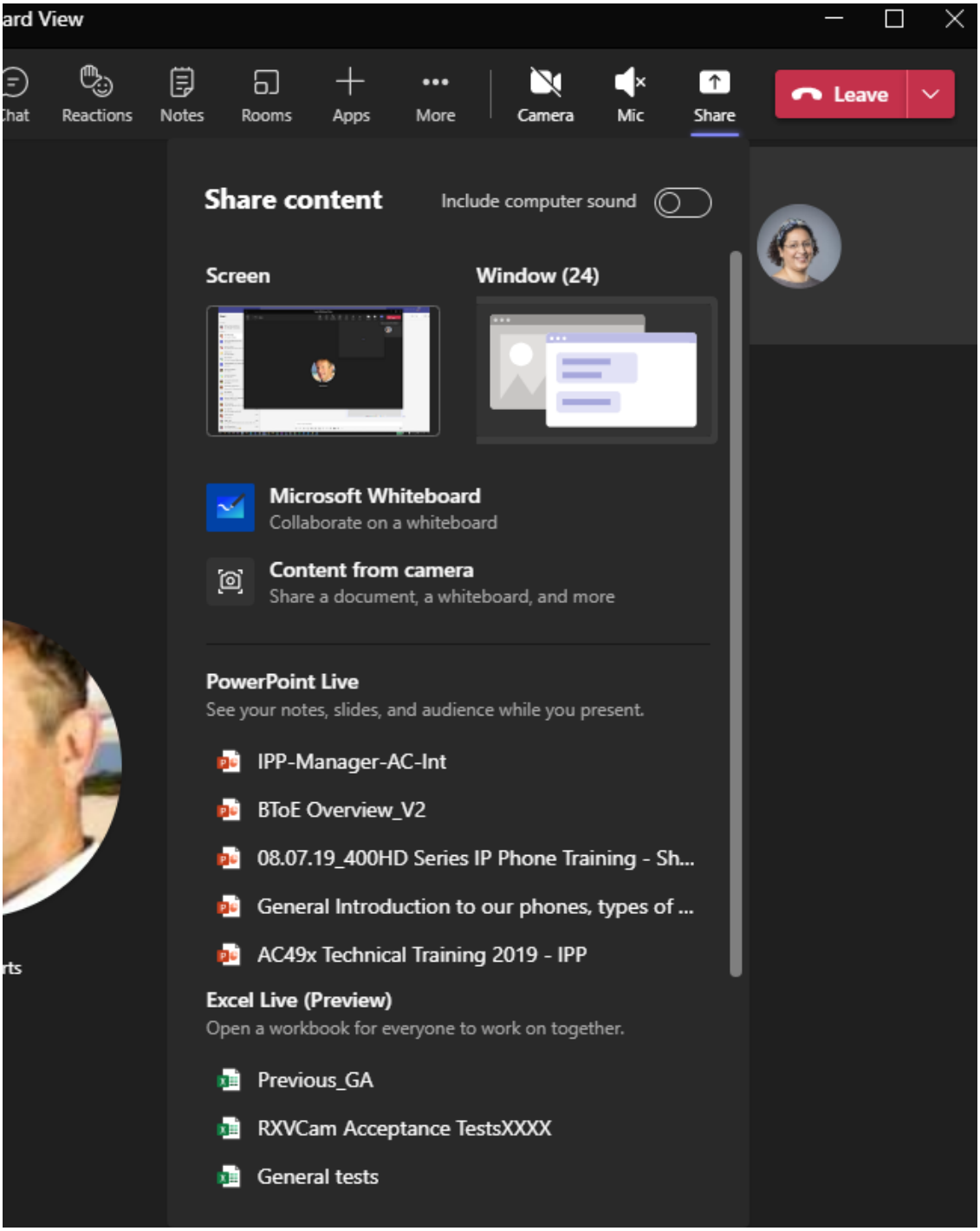
During Teams meetings, participants can open a virtual whiteboard – a digital canvas - on which they can sketch, illustrate, collaborate, brainstorm, plan, and share perspectives with one another in real time. The focus switches away from the presenting participant to the whiteboard. For more details,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

➢ **To share the Whiteboard:**

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



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



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

Screen Sharing

The RXV200 MTRA enables users to share their PC/laptop screen via the RX-PAD HDMI In port, to be shared on the screen in idle mode and peripheral mode.

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

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

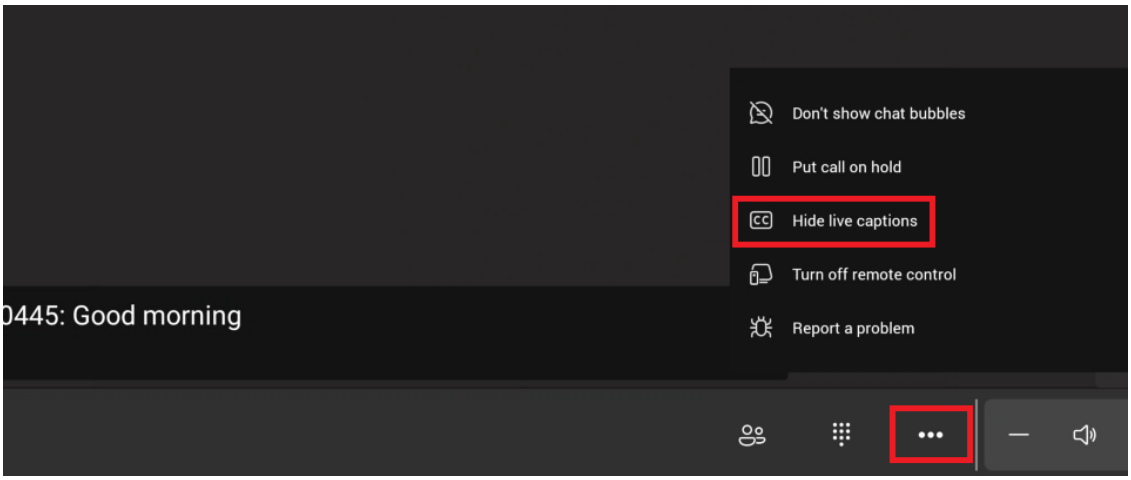
- **In-Meeting Mode:** When the MTRA is in a meeting, the presenter can use the Teams app 'Share' key to share their PC screen with in-person attendees who are physically present in the same meeting room, as well as with remote attendees. [Audio sharing is currently unsupported].
- **Idle Mode:** When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

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

The figure below shows the MTRA connected.

Set Live Captions

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



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

Dial a Number

You can manually dial someone's phone number.

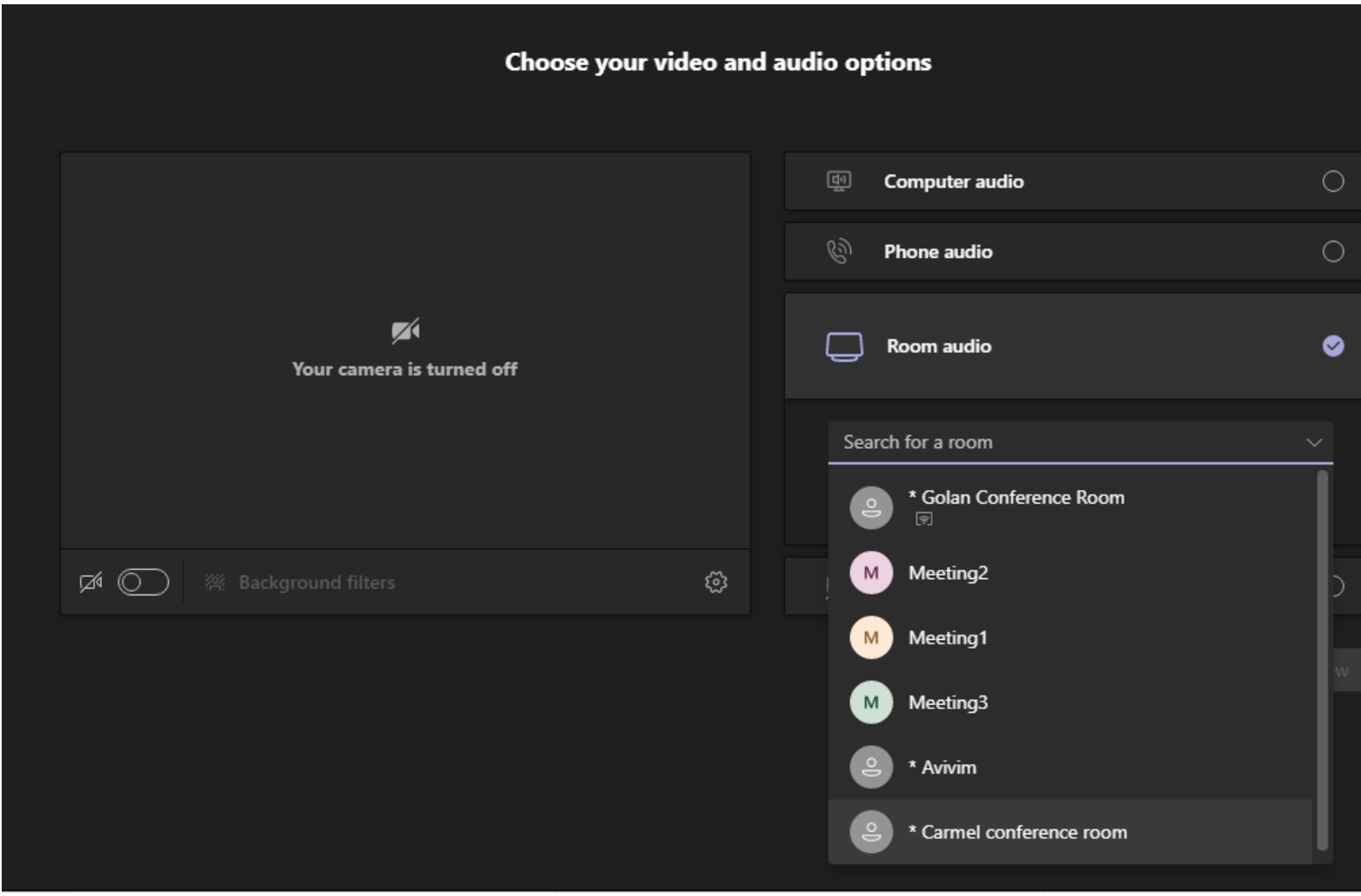
➢ **To dial a phone number:**

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

Enable Proximity Join

Proximity Join allows you to discover and add a nearby available MTRA, i.e., the RXV200, to any meeting. It's also possible to accept the incoming meeting on the console of the room.

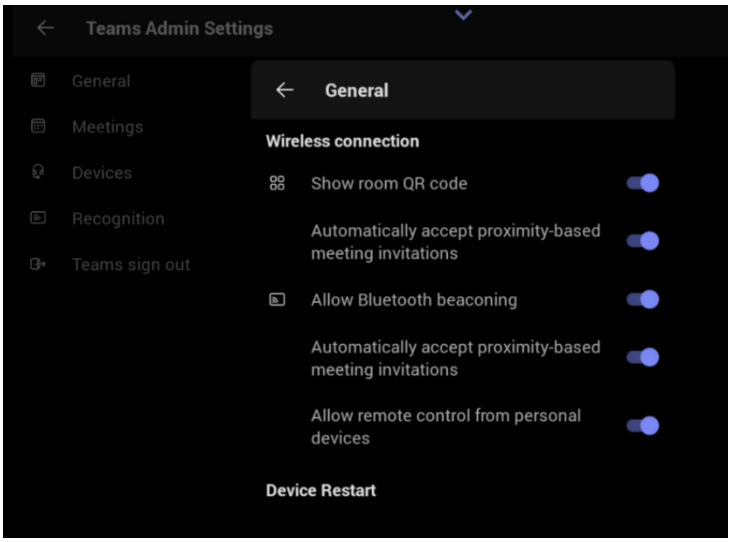
The feature functions in combination with Bluetooth and 'Bluetooth Beaconing', an integral feature in MTRAs. In the case of an RXV200 MTRA, if you bring a laptop or a Teams Mobile Client near the MTRA, it will offer the MTRA as the room audio device. The following figure shows how to select the room audio device.



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

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

1. This feature requires Admin login. Navigate to 'Device Admin Settings' (see Access Device Admin Settings on page 56).
2. Scroll down and tap **Teams Admin Settings**, then navigate to **Teams Admin Settings > General**.
3. Scroll down to **Wireless connection** and verify that the **Automatically accept proximity-based meeting invitations** toggle options are turned on.



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

Hide Meeting Information

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

1. This feature requires Admin login. Navigate to 'Device Admin Settings' (see Access Device Admin Settings on page 56).
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.

4 MTRA Camera Settings

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

A camera Preset or View contains settings related to the camera or cameras connected to your RXV200 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 45).

Temporary and Permanent Settings

➢ Presets

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

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

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

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

➢ Views

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

For more details, see Managing Views for RXV200 MTRAs without RX-PAD on page 30.

➢ **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 56).

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

Managing Camera Presets

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

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

- Temporary Presets below
- Permanent Presets on page 29

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

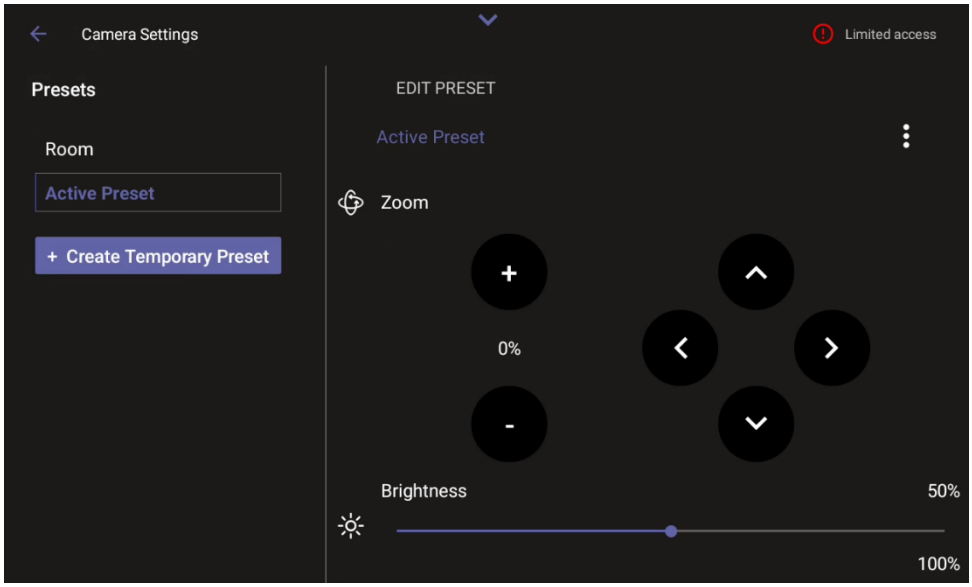
- Full room view to capture all participants and action in a meeting room
- Presenter or single user / desk view to focus on a single user in the room, usually the presenter
- Whiteboard view if there's a whiteboard in the room
- Sunlight or dark modes if direct sunlight enters the room at specific times of the day/year

Temporary Presets

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

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

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



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

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

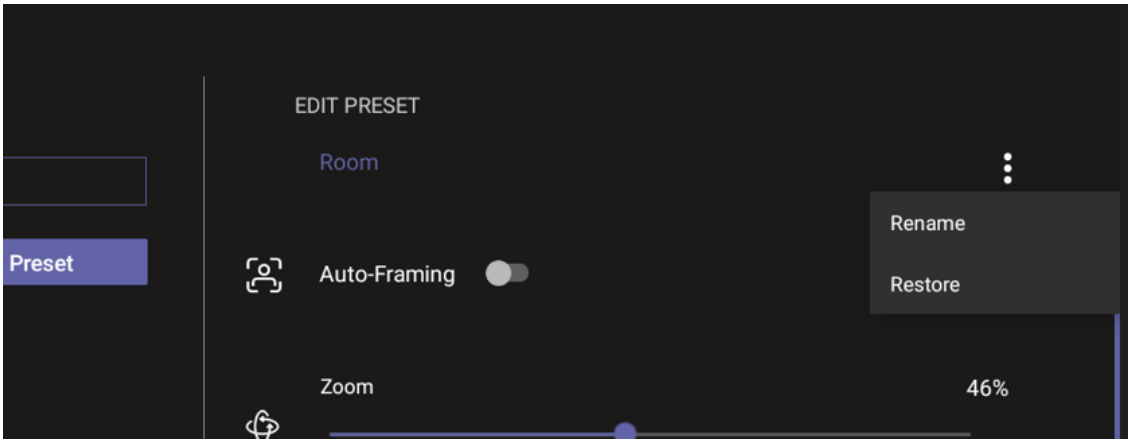
If the user has Admin permissions, the button is labeled **Create New Preset**. In this case, the generated preset will be permanent.

3. Configure the settings you want.

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

4. [Optionally] Edit a preset.

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



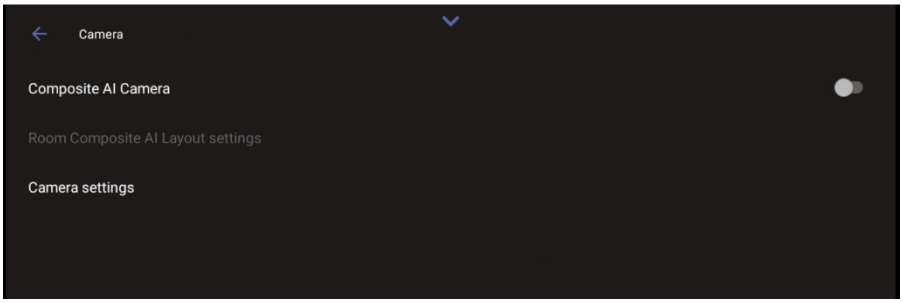
Camera settings can be changed during a meeting without turning off the video to remote parties.

Permanent Presets

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

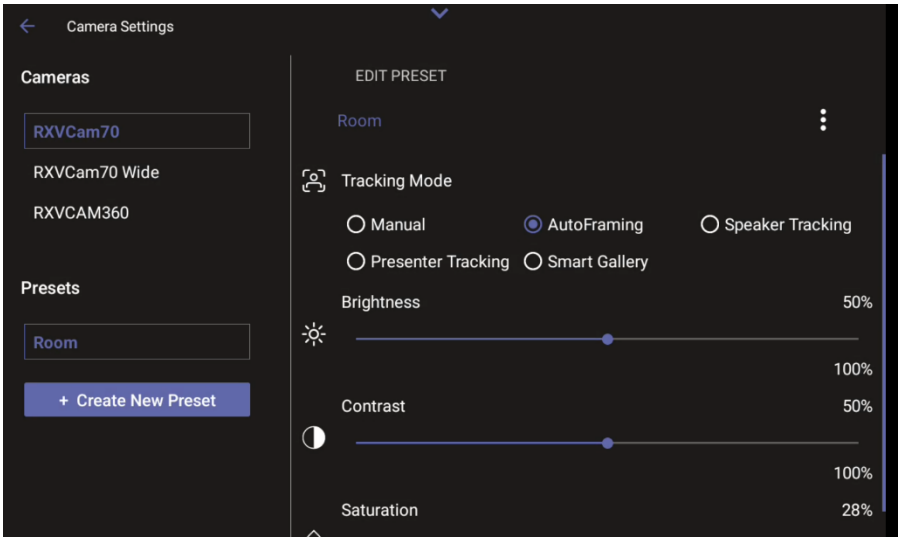
In idle mode, Admins can create new permanent presets and permanently change existing presets:

1. On the RX-PAD, touch the camera hard key below the screen.
2. Log in as administrator if prompted (see Access Device Admin Settings on page 56).
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.

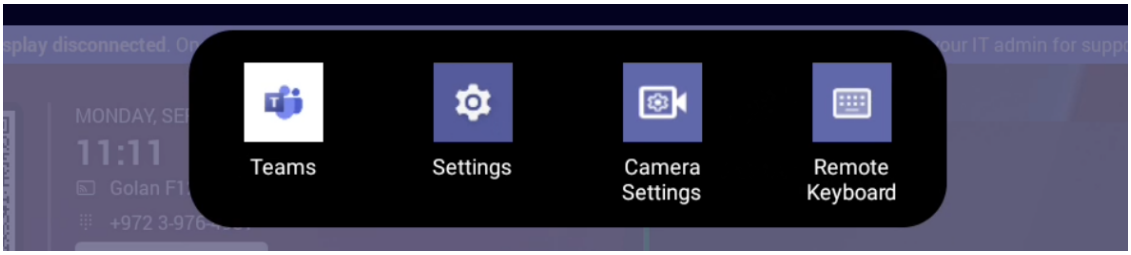


5. [Optionally] Tap the vertical ellipsis and then from the pop-up menu select the **Rename** option to change the name of the preset.
6. [Optionally] Tap the vertical ellipsis and then from the pop-up menu select the **Restore** option to return camera settings to their defaults.

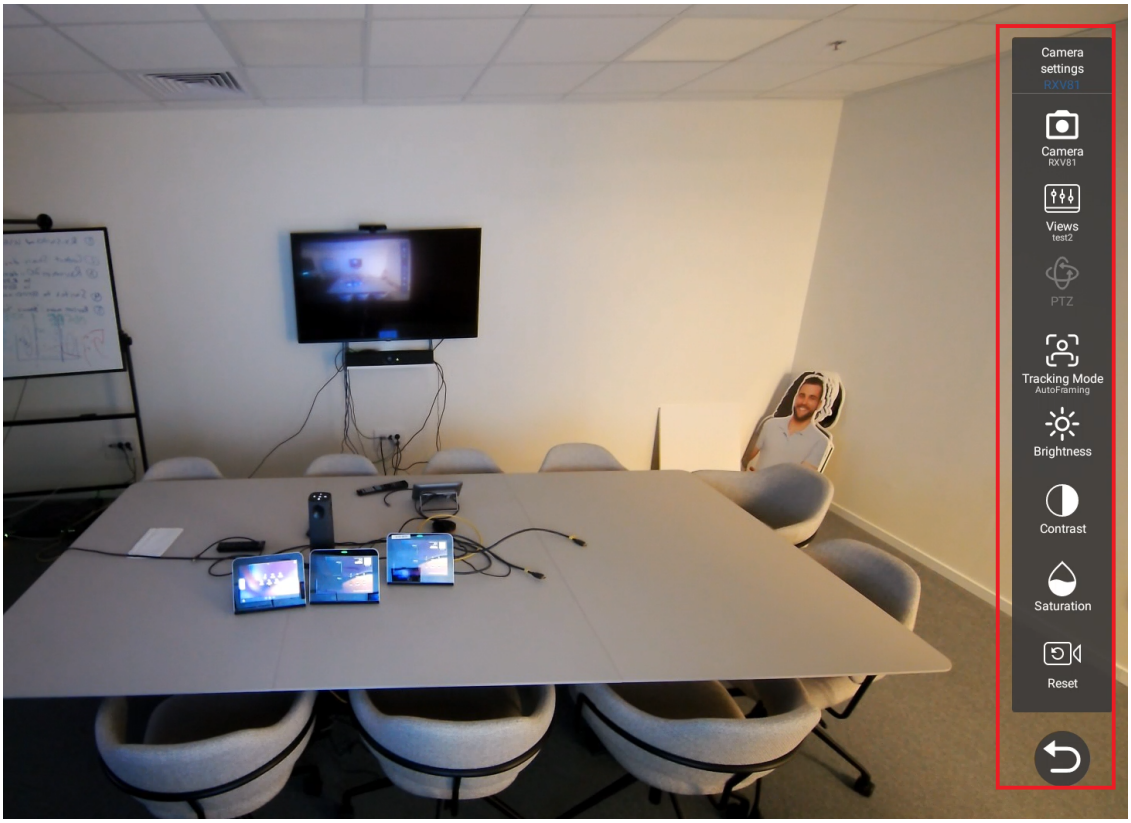
Managing Views for RXV200 MTRAs without RX-PAD

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

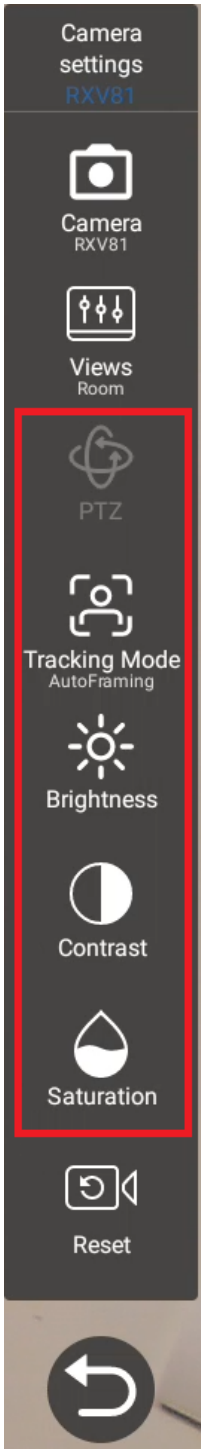
1. On the touch screen, swipe down to display the main menu tray, then tap **Camera Settings**.



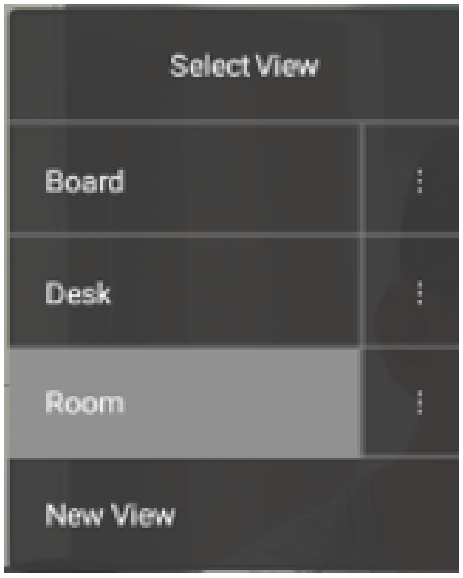
2. The camera output is displayed, with a vertical toolbar in front of it:



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

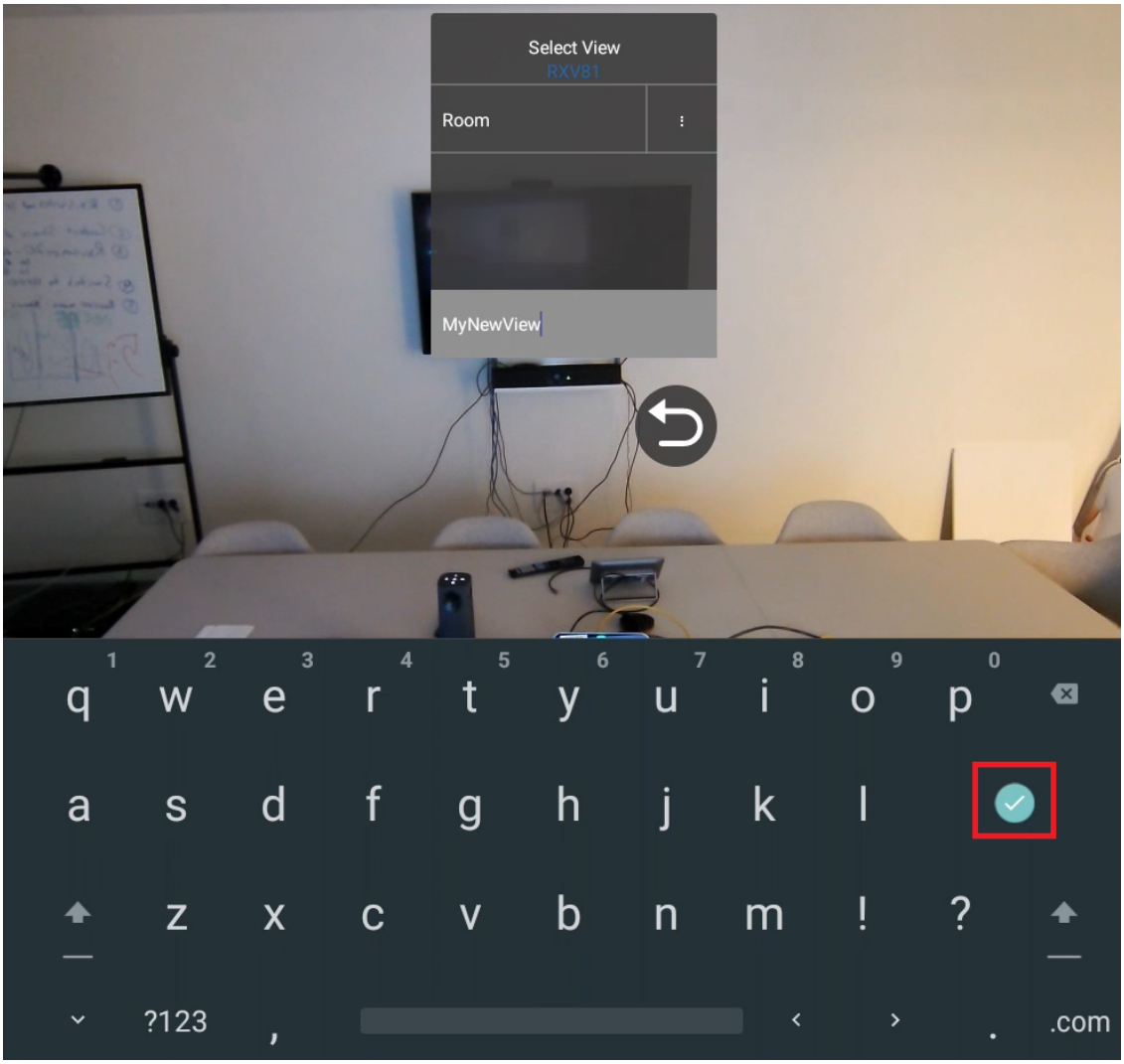


4. Tap the **Views** option on the toolbar. A list of existing views (presets) is displayed.



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

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

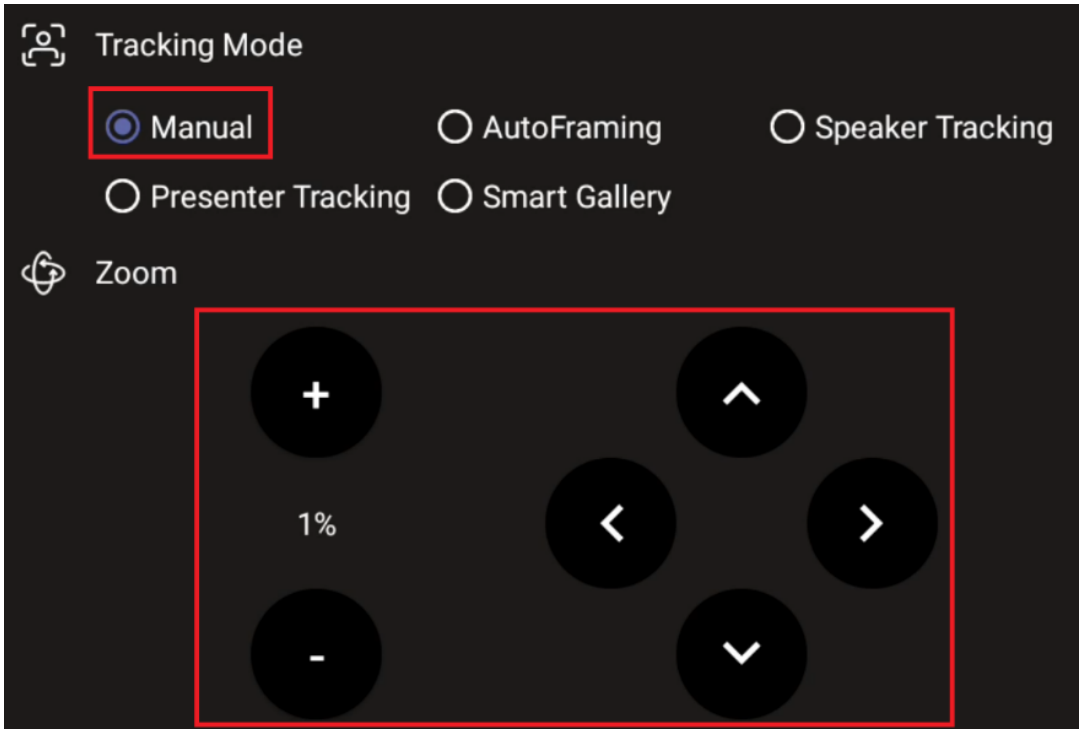


6. To rename or delete a view, tap the vertical ellipsis to the right of its name, and then from the pop-up menu tap the **Rename** or **Delete** option.

Set up Camera Zoom and Color Properties

➢ Zoom

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



- 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

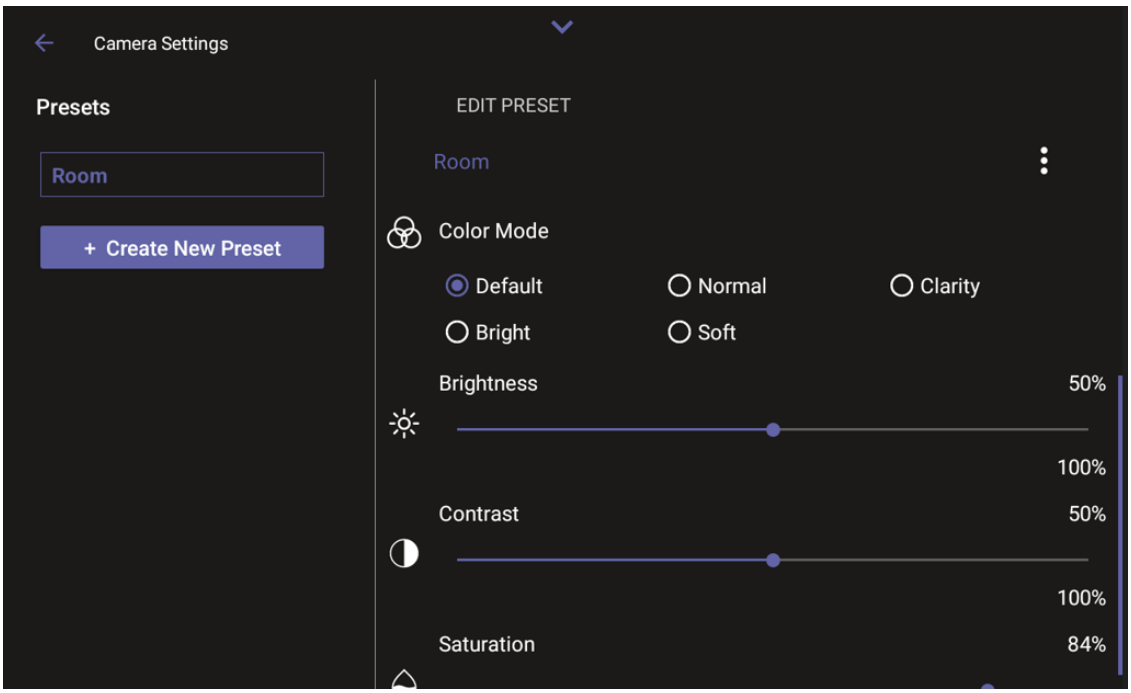
Each connected camera comes with default Brightness, Contrast, and Saturation properties. You can adjust them as required.

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 56).



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

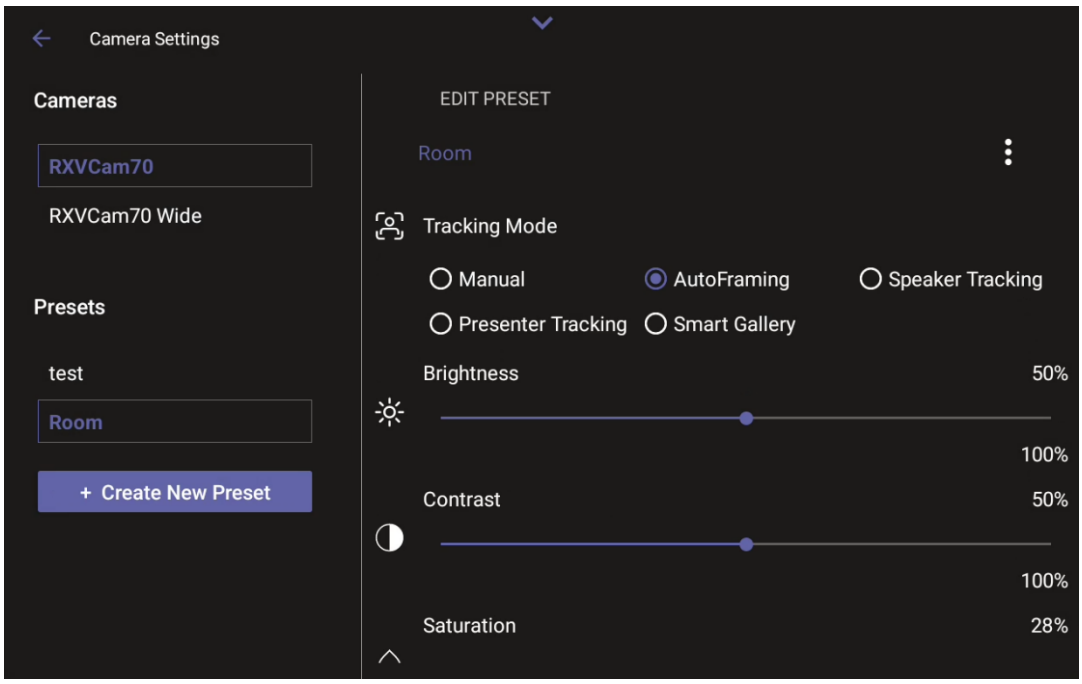
Select RXVCam70 Camera Tracking Mode

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 56).

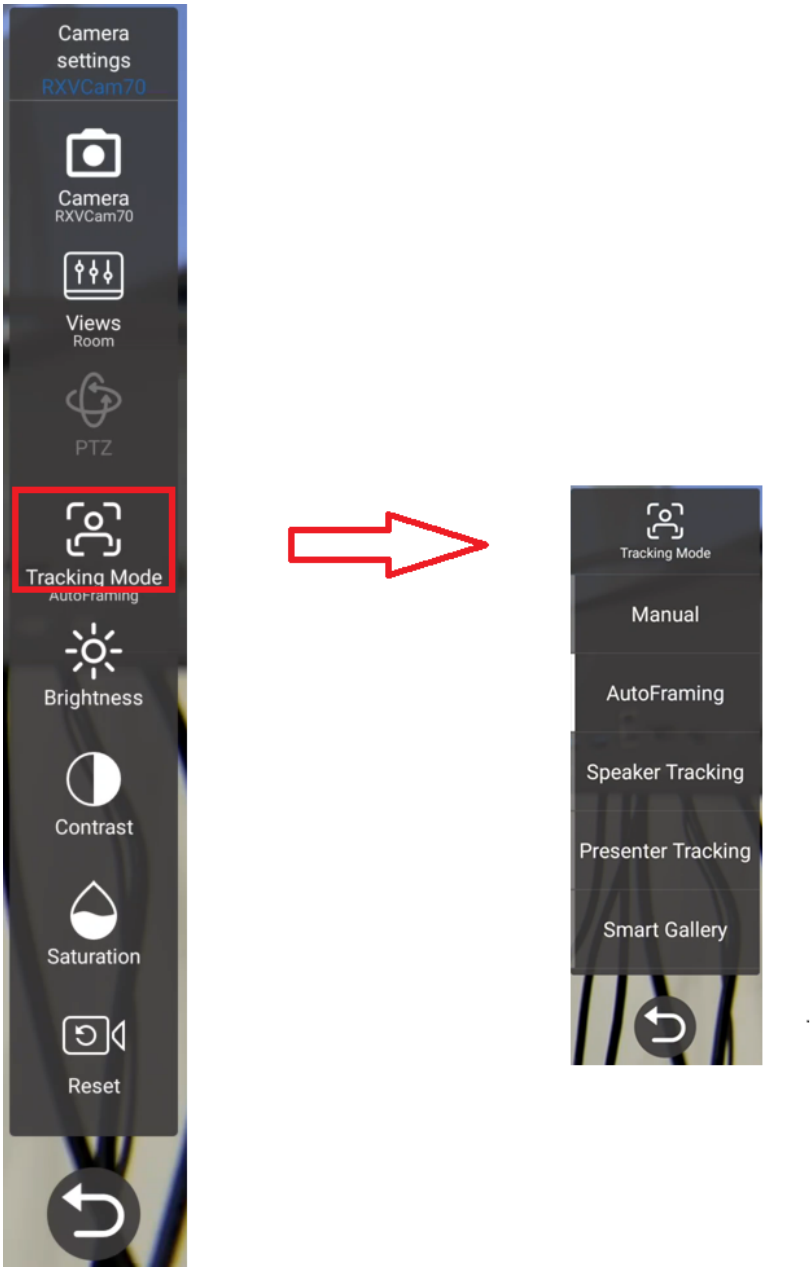
To select a Tracking Mode:

1. Do *either* of the following:

   - From your RX-PAD (if available), 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

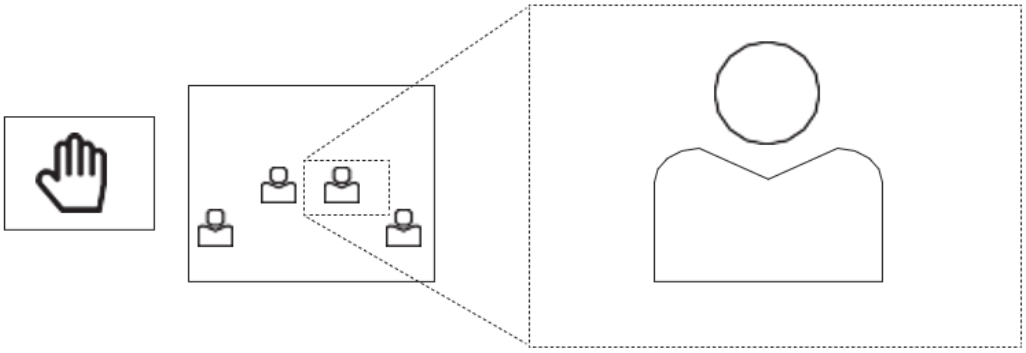
Manual

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.



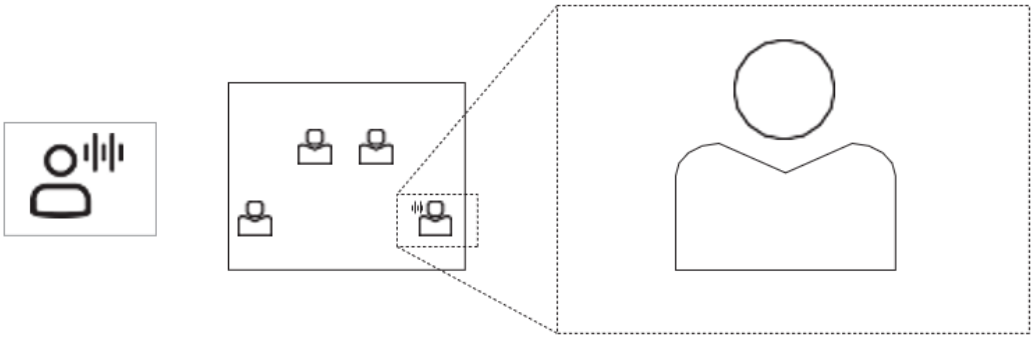
Speaker Tracking

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

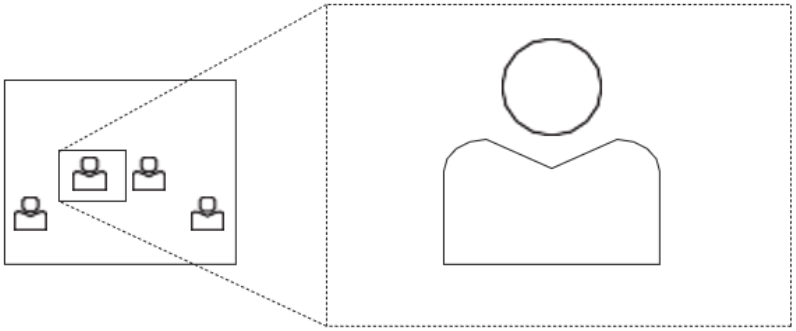


Presenter Tracking

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.



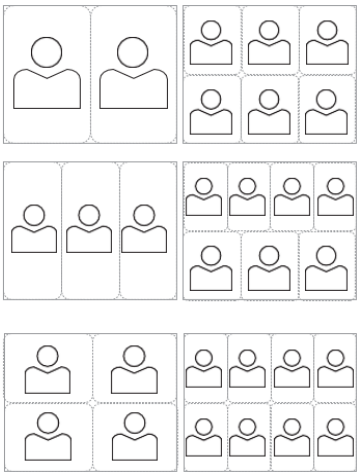
Smart Gallery

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

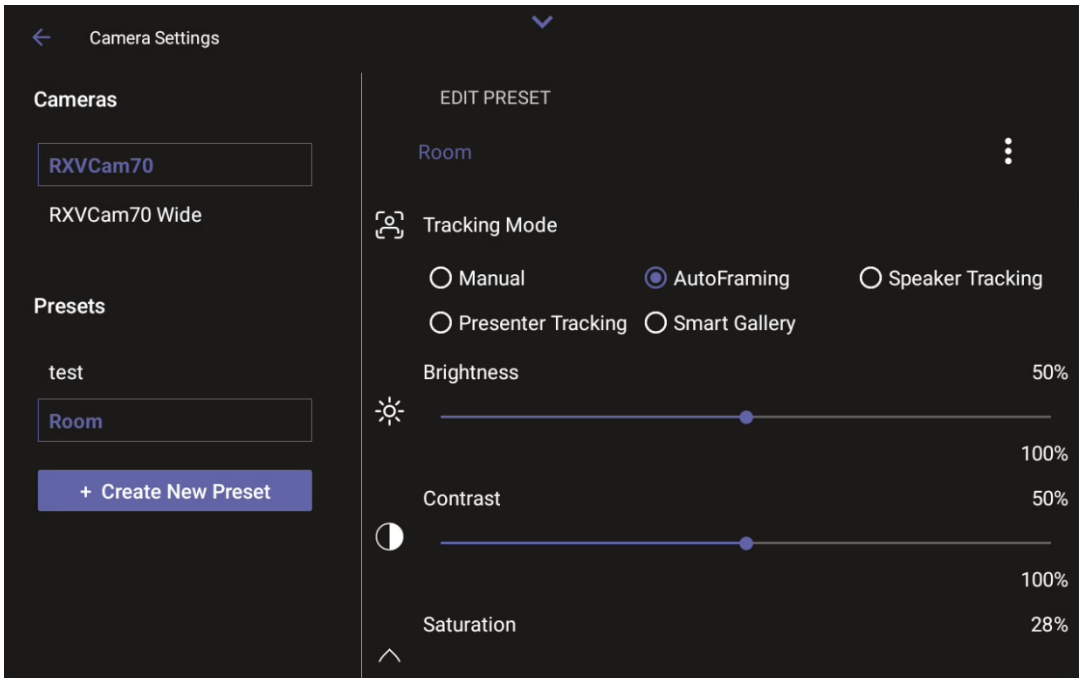
Regular users can only create temporary presets during ongoing meetings. These presets are automatically deleted at the end of the meeting.

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 56).

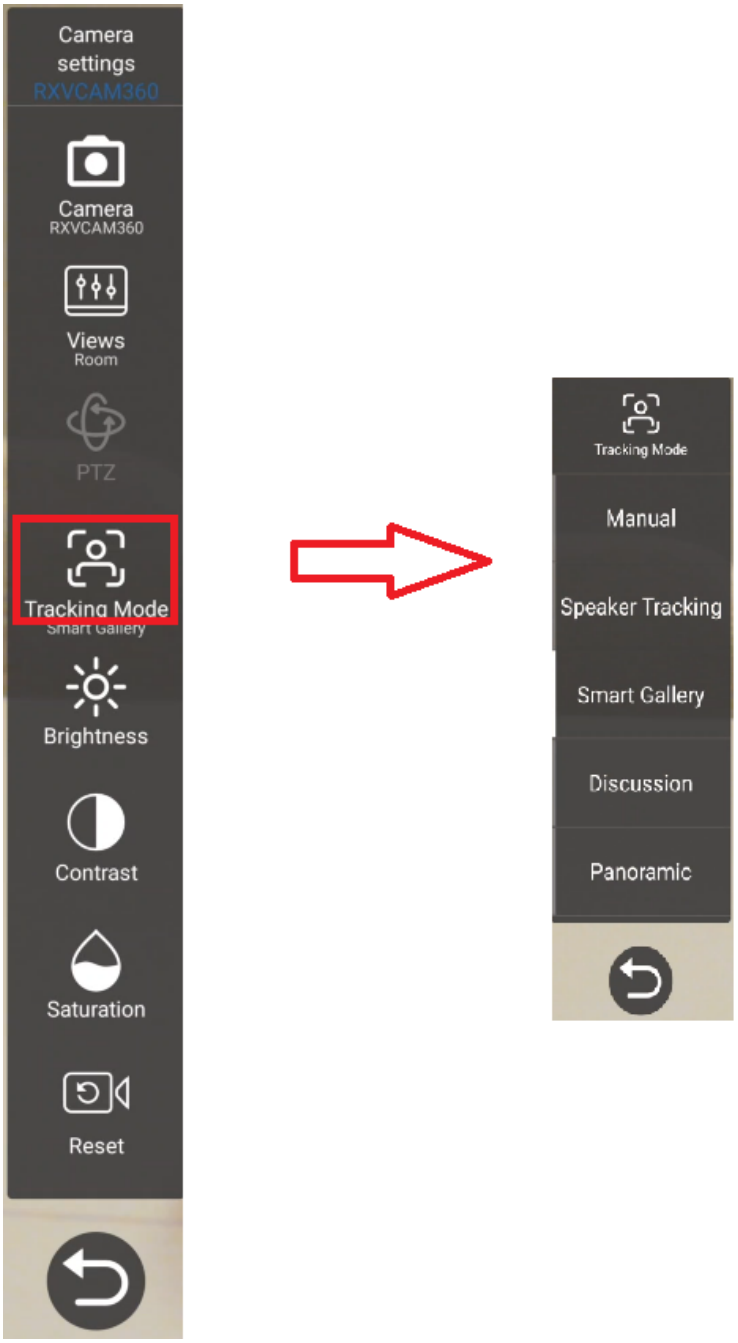
➢ To select a Tracking Mode:

1. Do *either* of the following:

- From your RX-PAD (if available), 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

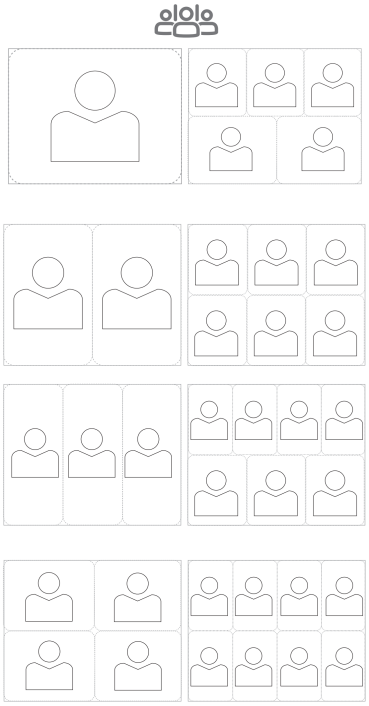
Recommended

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

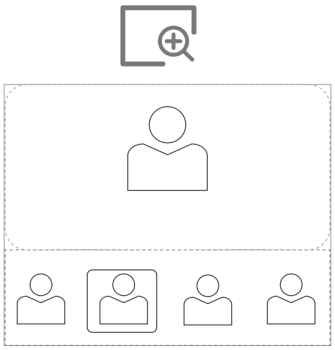
Select an area to focus on

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.

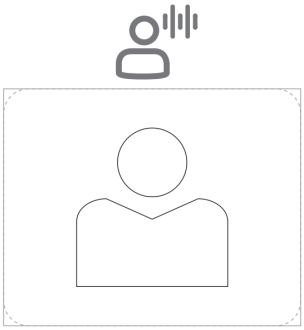
This mode does not have AI functions.

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



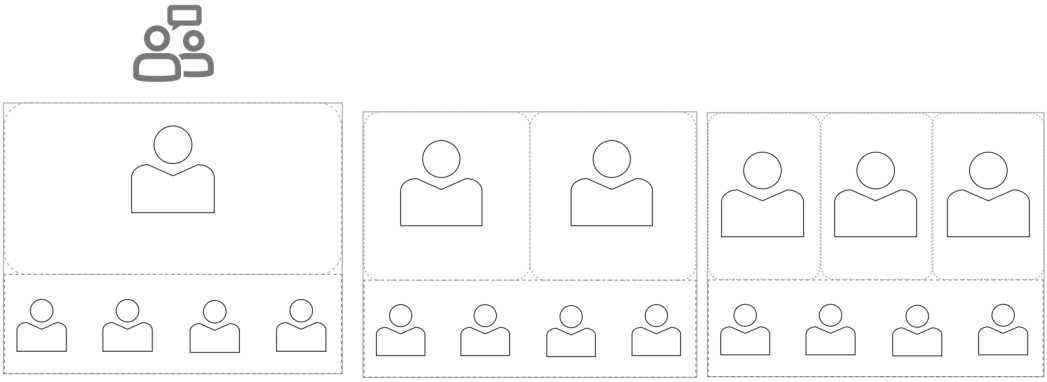
Discussion Mode

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.

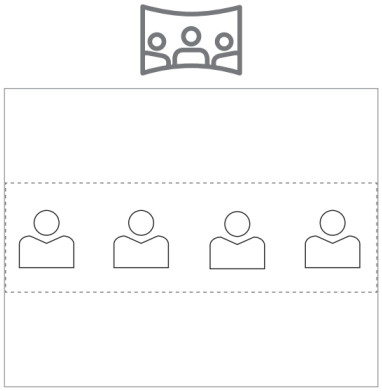
For using this mode with Composite AI, see Enable RXVCam360 Discussion Mode with Composite AI on page 48.



Panoramic Mode

360° panoramic high-definition view

This mode does not have AI functions



5 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.

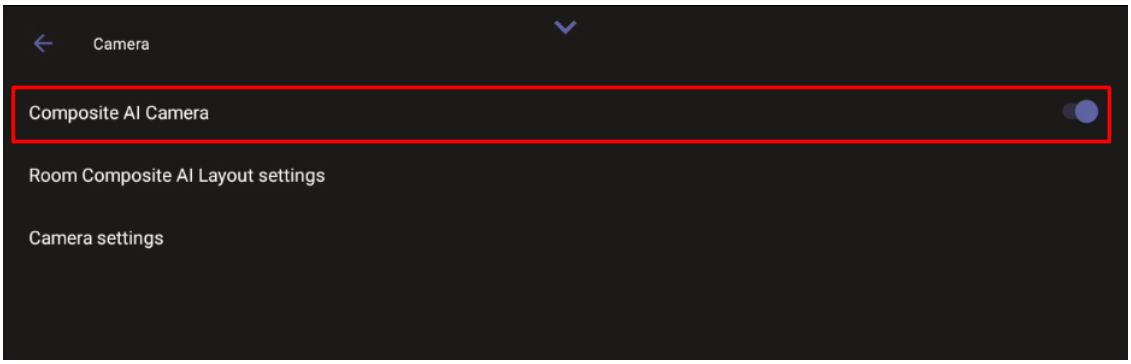
Set up Composite AI

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

1. Do either of the following:

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

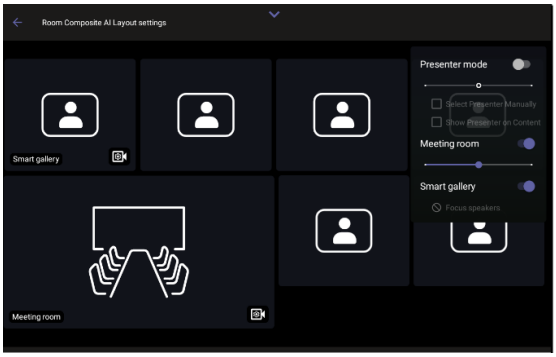
2. Tap the **Composite AI Camera** toggle button so that it is on:

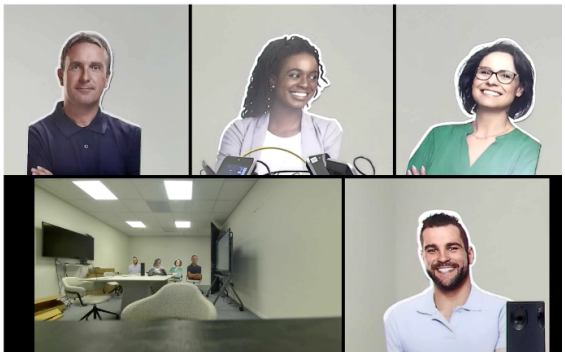


On the screen to which the RXV200 is connected, a pop-up message appears, indicating that the Composite AI camera is connected.

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

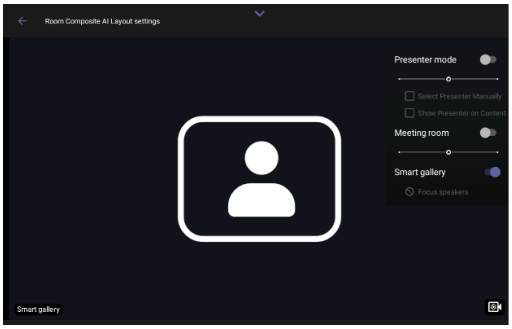
The connected camera stream opens. On RX-PAD, the layouts are displayed as shown in the following figure:



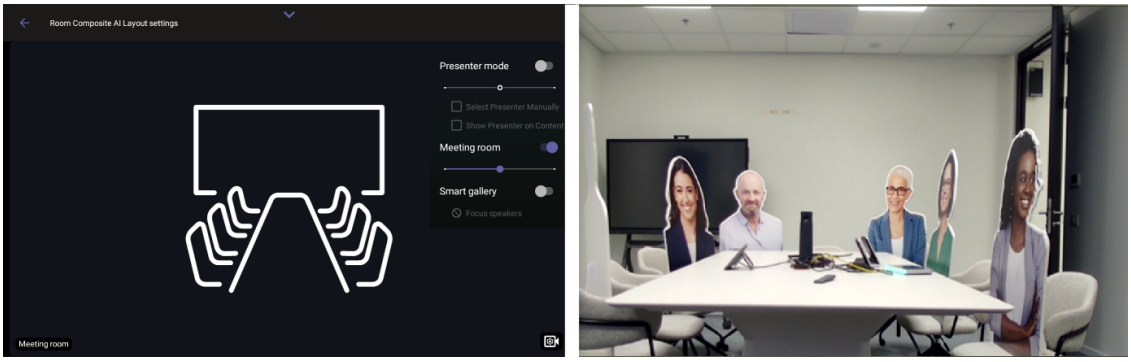


In the RXV200 screen (when RXV200 is connected to RXVCam70), the main camera is in the center of the screen and the wide-angle camera at the lowermost left.

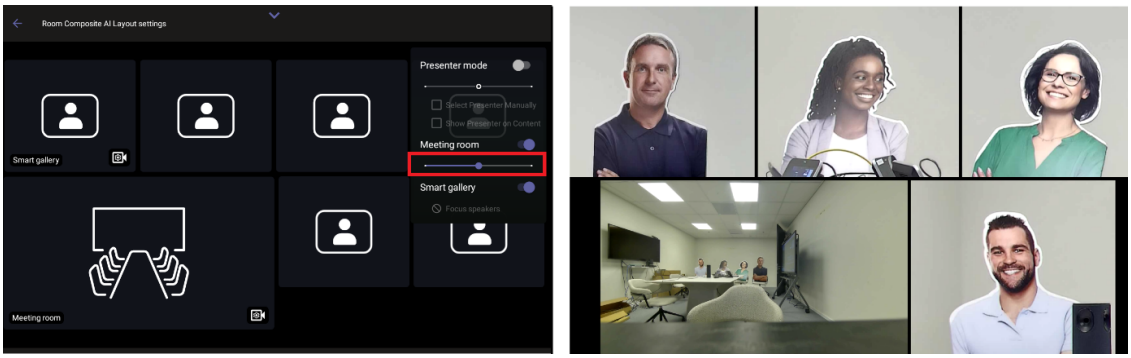
4. Disabling **Meeting room** closes the wide-angle camera and centers the main camera feed in the screen.



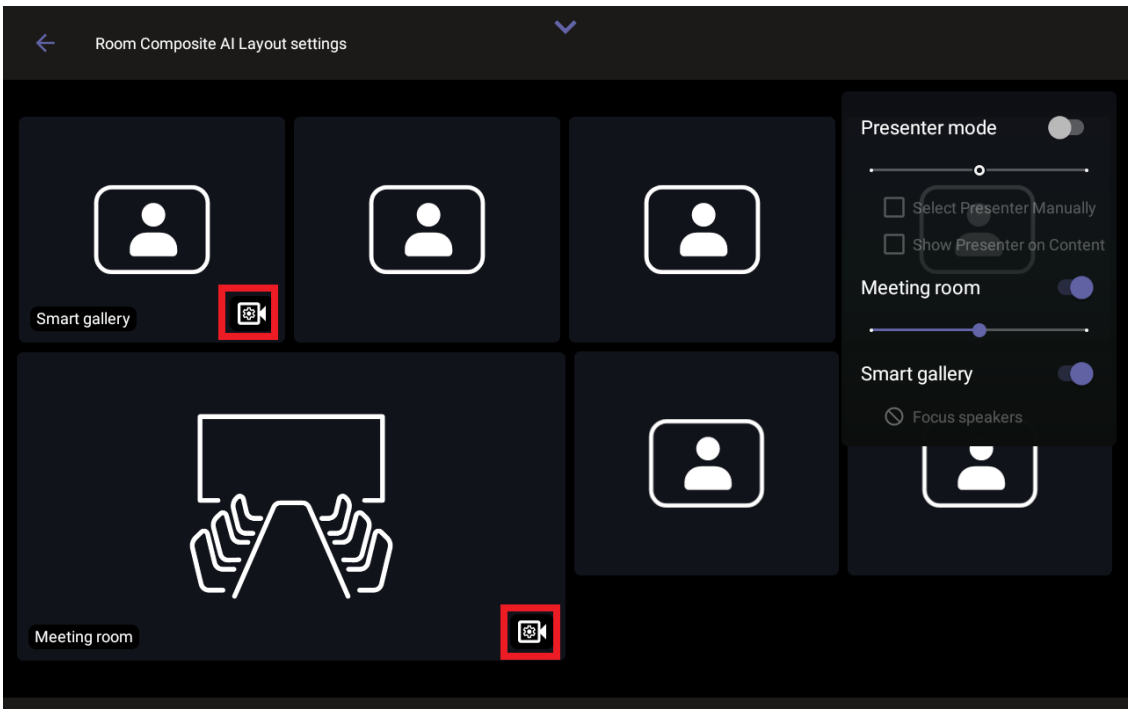
5. To close the main camera and center the wide-angle camera feed in the screen, disable the **Smart gallery**.



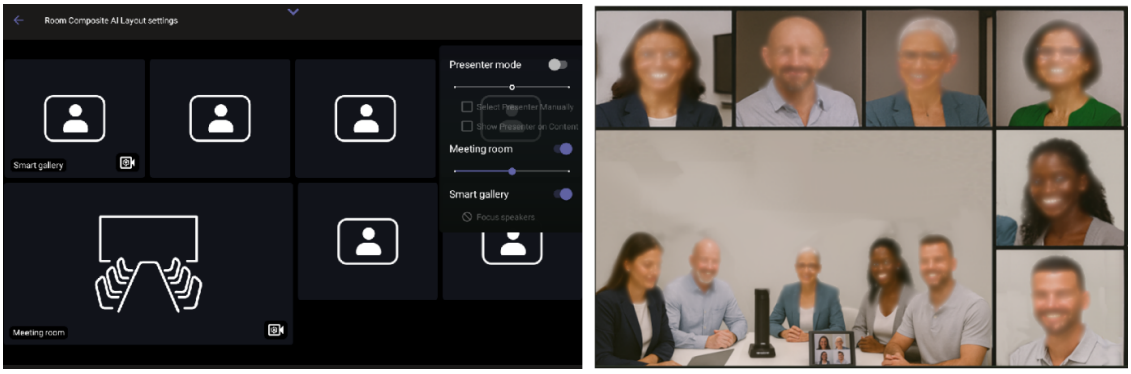
6. Use the scaling bar shown in the following figure to control the ratio between the main camera size and the wide-angle camera size; move the slide bar to adjust the size of the **Meeting room** view accordingly.



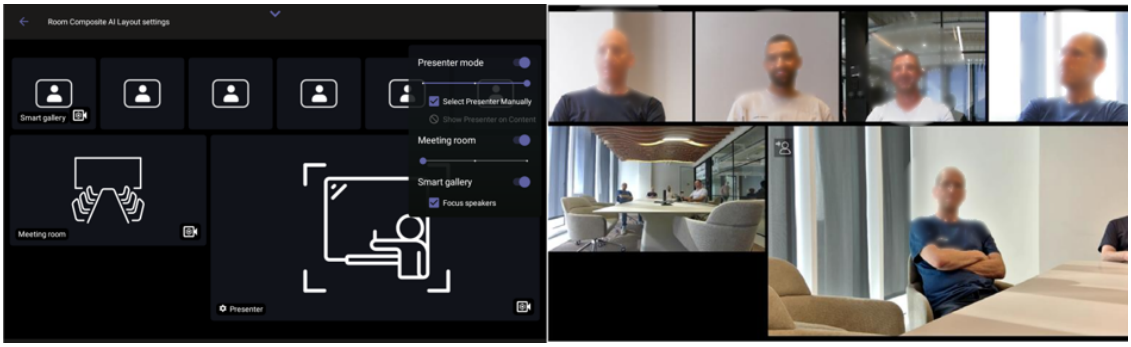
7. To adjust the settings (e.g., brightness and saturation) of a specific camera, click its  icon:



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:



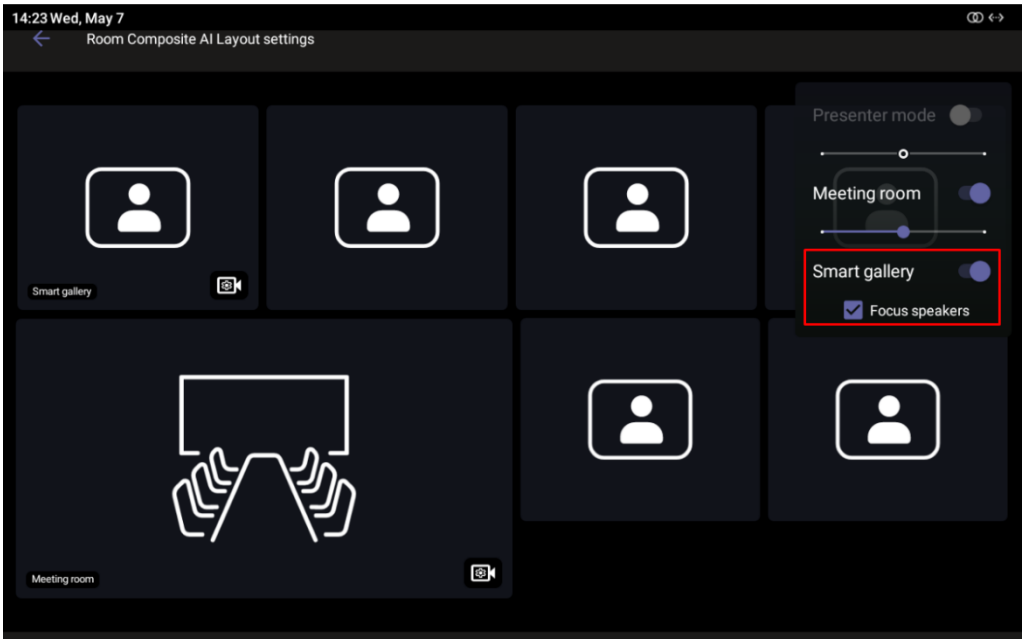
Enable RXVCam360 Discussion Mode with Composite AI

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:**

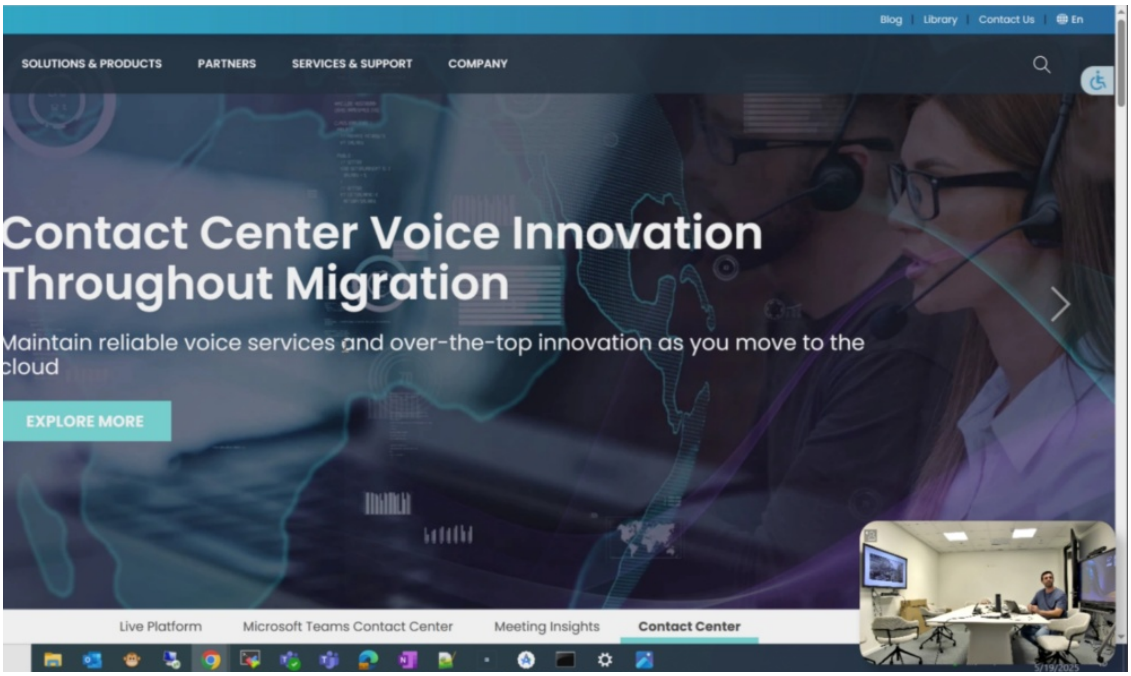
1. Navigate to the Composite AI Layout Settings page (see Set up Composite AI on page 45).
2. Turn on 'Smart gallery' and select the **Focus Speakers** option.

> 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.

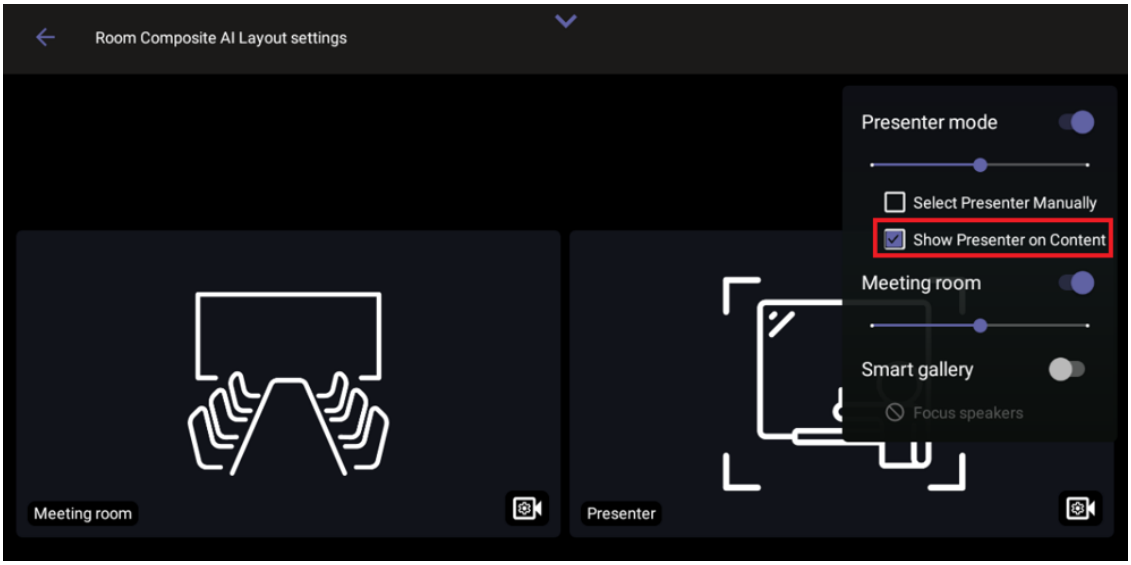


This feature can be toggled on/off via the RX-PAD using the Show Presenter on Content setting under Composite AI mode.

➢ **To enable this:**

1. Navigate to the Composite AI Layout Settings page (see Set up Composite AI on page 45).

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



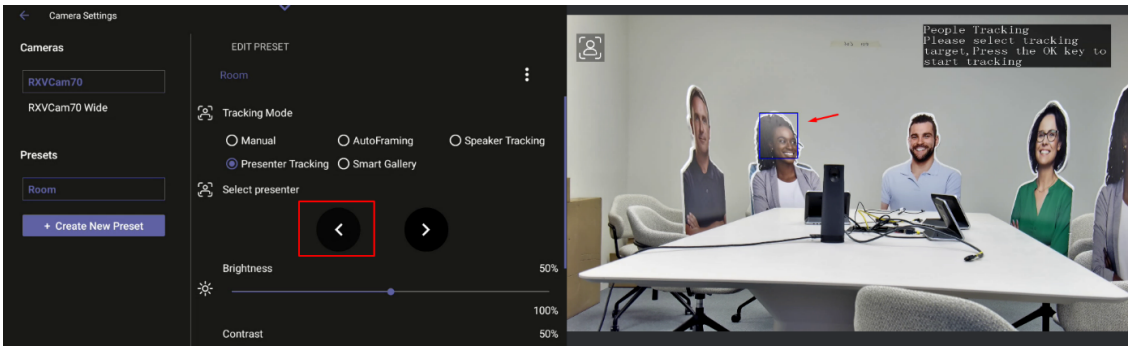
For non-supported cameras (e.g., RXVCam360), the Show Presenter on Content option is grayed out.

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 37) 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 45).
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.



6 User Settings

RXV200s 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:

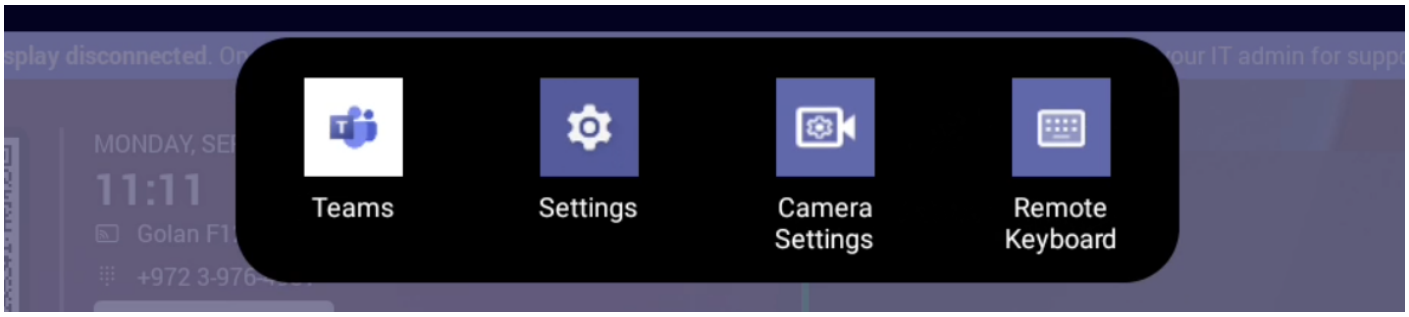
- Adjust the Volume on the next page
- Configure Accessibility Settings on page 53
- View RXV200 Information on page 53
- Approve Firmware Updates of Connected Peripherals on page 53
- View Microsoft Teams Information on page 54
- Reboot the Device on page 55

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

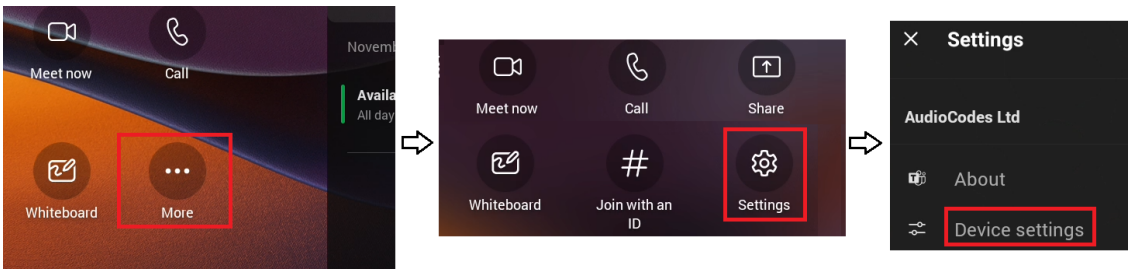
Access User Settings

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

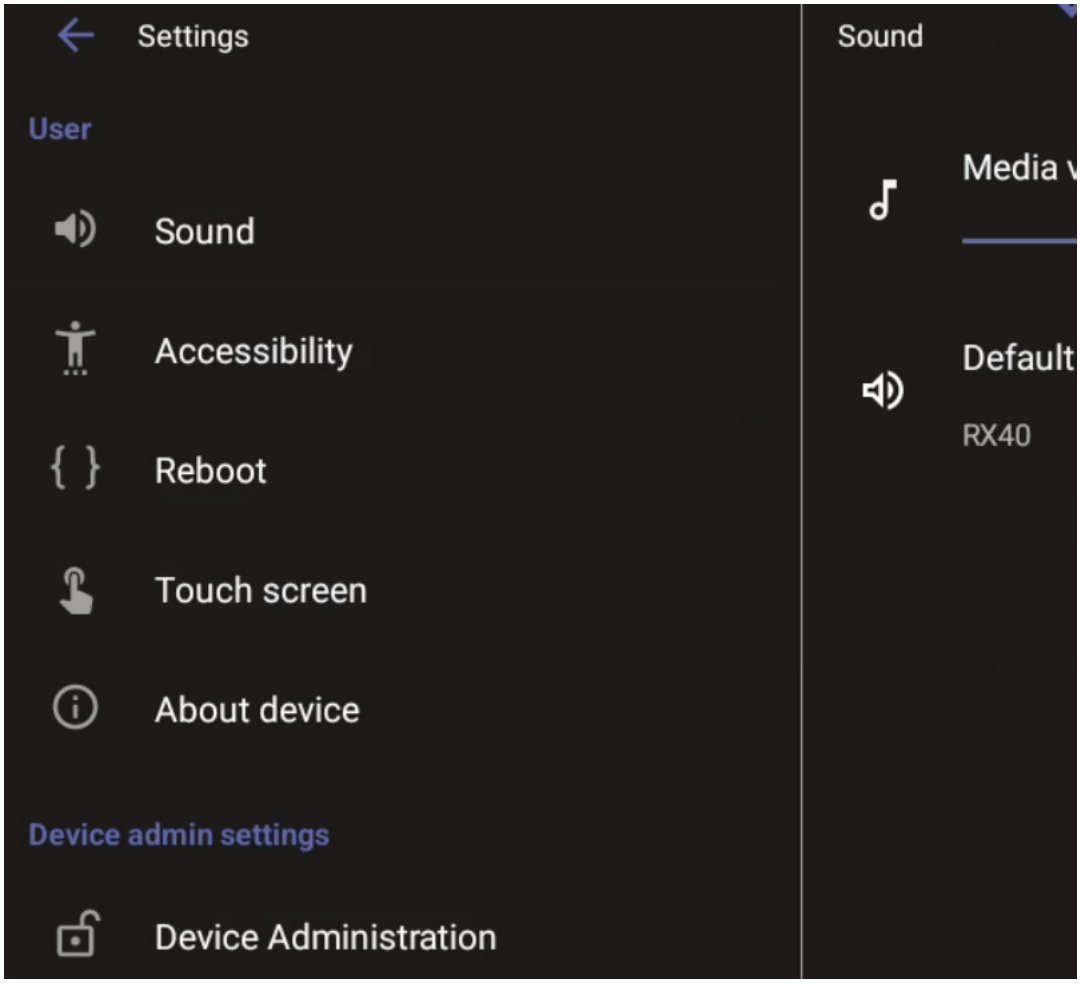
- Swipe down to display the main menu tray, then tap **Settings**.



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



Any user can configure User settings:

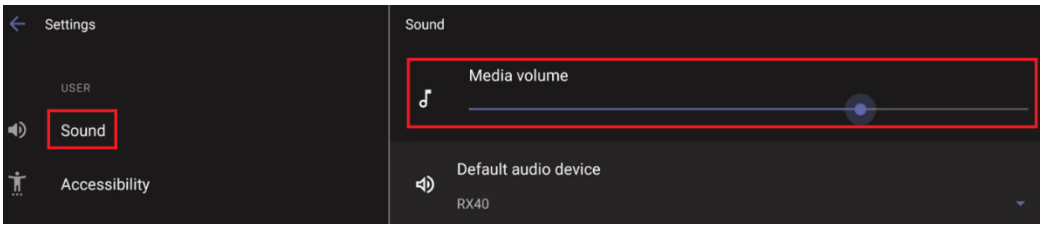


Viewing and configuring Device Admin settings requires Admin login. For details, see Admin Settings on page 56.

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 51).
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 RXV200 Information

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

➢ **To access the About page:**

1. Navigate to 'Settings' (see Access User Settings on page 51).
2. Under 'User', tap **About device**.

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

Approve Firmware Updates of Connected Peripherals

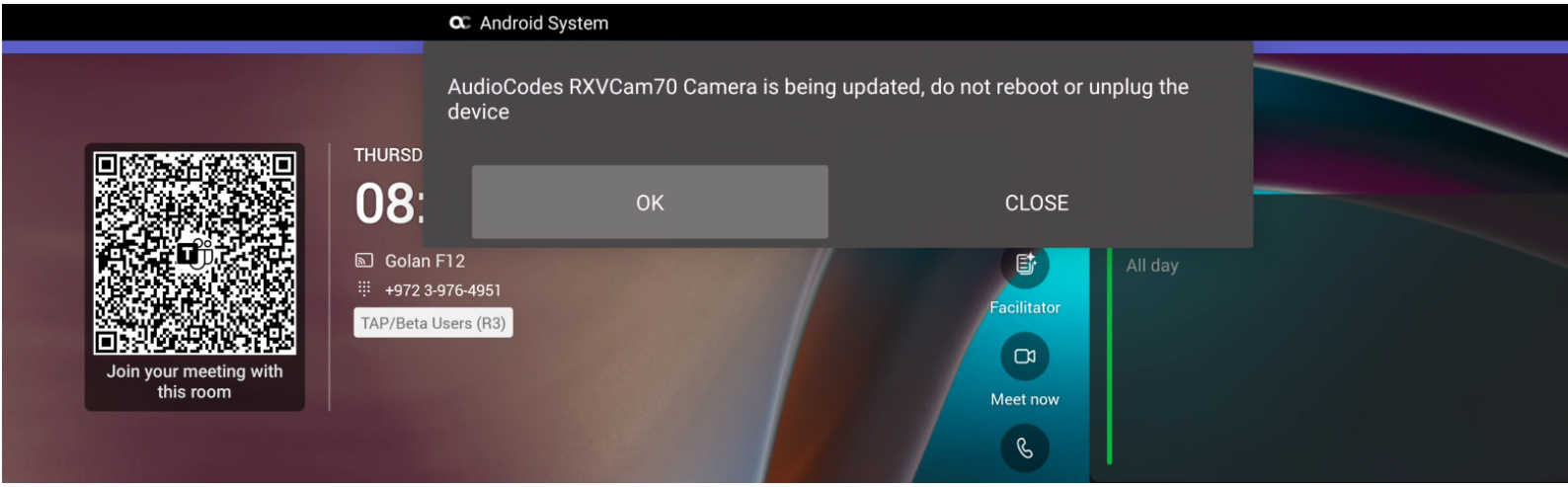
RXV200 firmware update includes upgrading:

- **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**.

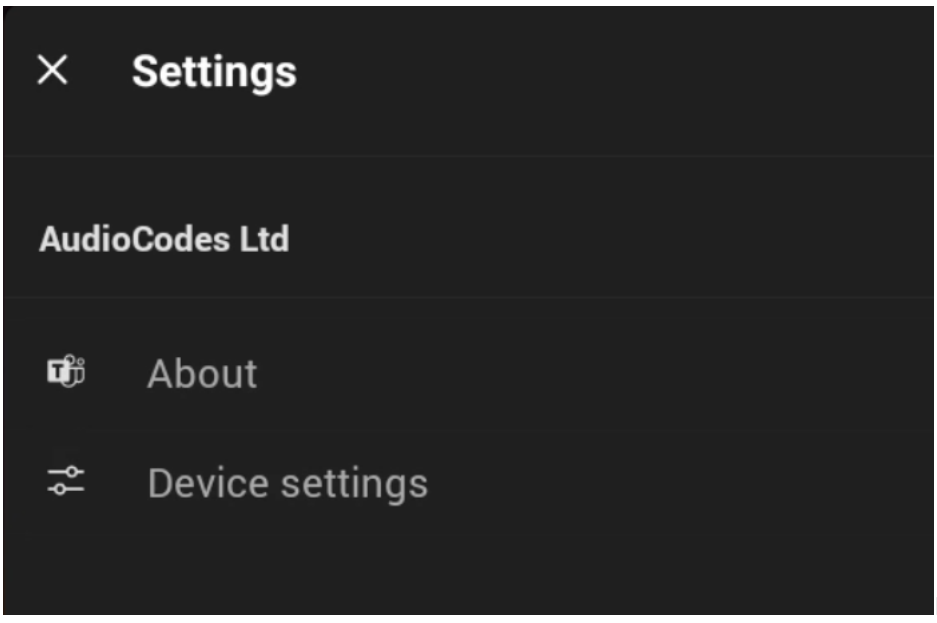


After a peripheral firmware upgrade is completed, the connected device will perform a reboot, and an associated notification will appear at the bottom of the page.

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 51).
2. Under ‘User’, tap **Reboot**.
3. Tap **Reboot**.
4. Confirm the reboot.

For an explanation on how to reboot, shut down, or turn on the device using its Power button, seePerform Recovery Operations using the Power Button on page 94.

7 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.

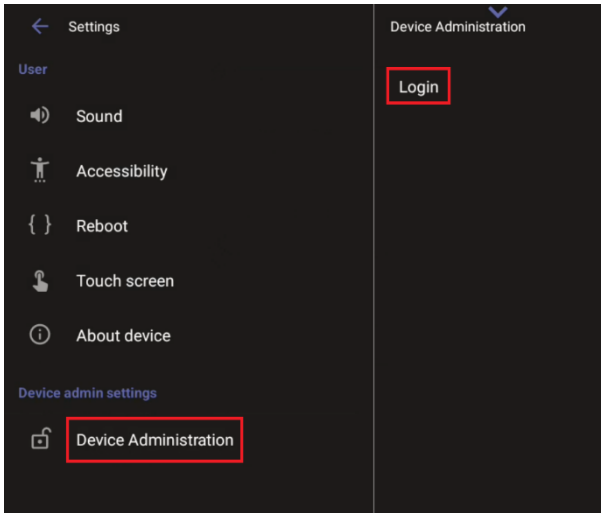
Access Device Admin Settings

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

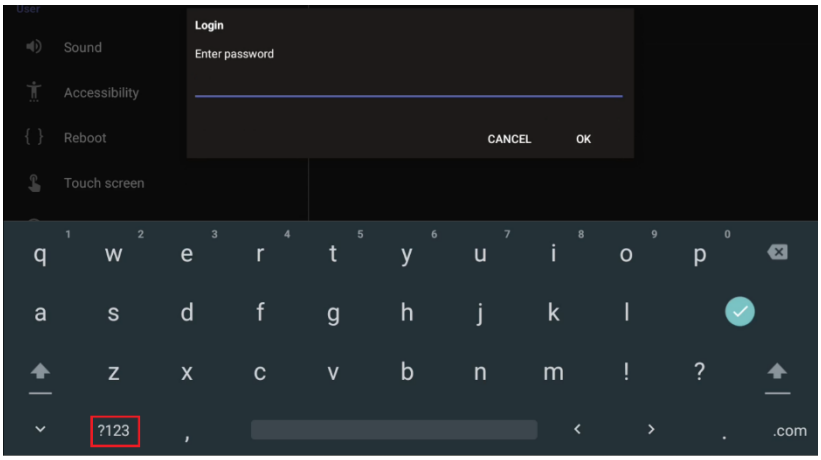
Log in to Device Administration

➢ **To log into Device Administration:**

1. Navigate to the 'Settings' page (see Access User Settings on page 51).
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:

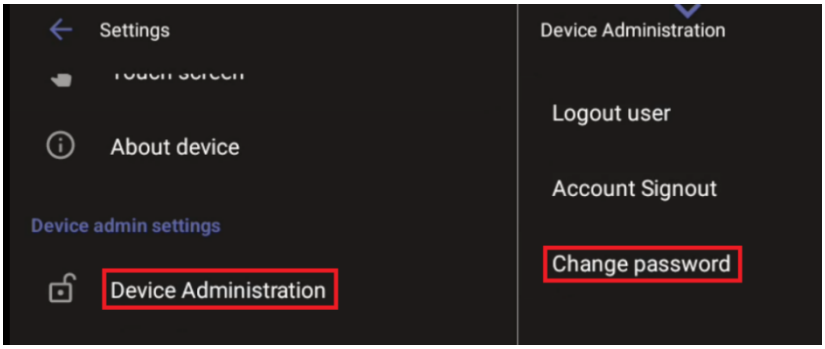
- The password length must be greater than or equal to 8.
- The password must contain one or more uppercase characters.
- The password must contain one or more lowercase characters.
- The password must contain one or more numeric values.
- The password must contain one or more special characters.

- 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 56).
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 RXV200 (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 RXV200 from the TAC, remotely sign in, and sign out.

➢ To sign out of the MTRA using Microsoft TAC:

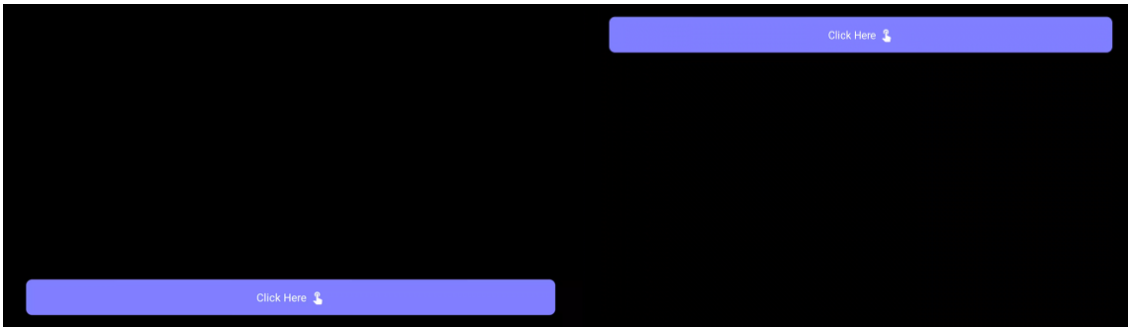
- Navigate to the 'Devices' > 'Teams Rooms' screen. From the **...** menu located in the uppermost right corner of the screen, select **Actions** and then **Sign out**.

Set up Dual Touch Screen Orientation

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

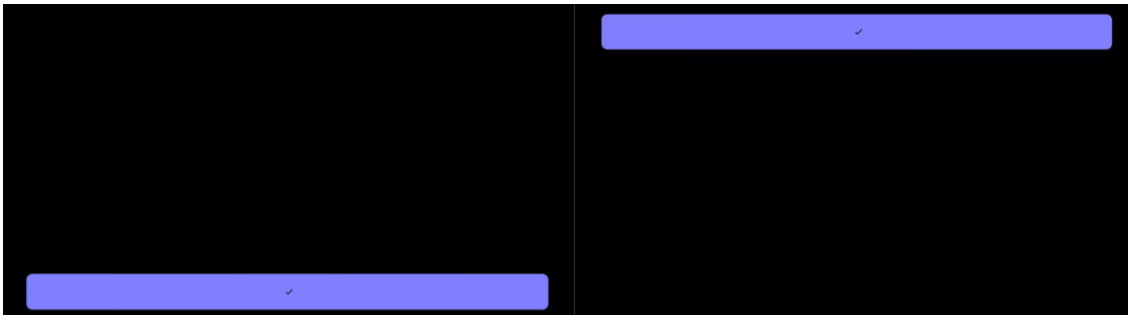
➢ To display two screens:

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

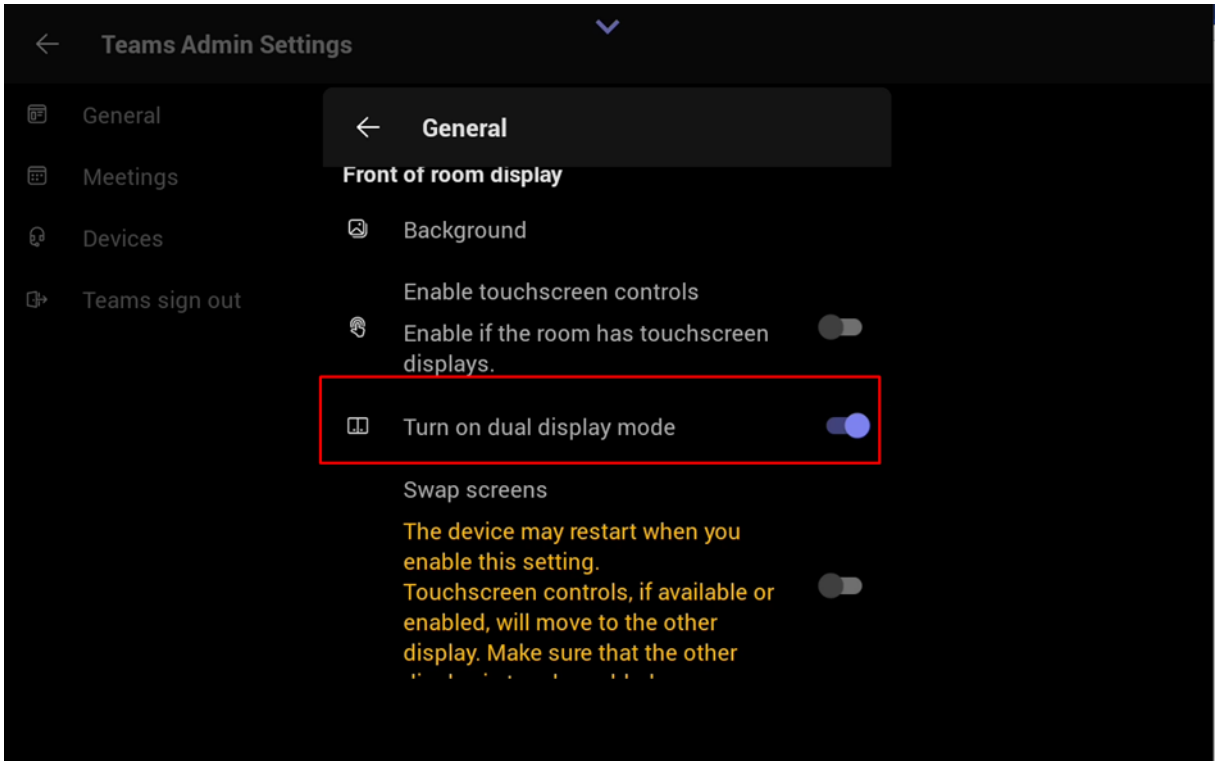
This feature is for RX-PAD paired with RXV200 only, and for a Pro room account, as described below. The devices must run the following Teams app version or later - 1449/1.0.96.2024110701 (November 2024).

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 56).
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 51).
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 56).
2. Under 'Device admin settings', scroll down and tap **Display**.
3. To decrease or increase screen brightness, tap the **Brightness level** scale.
4. To set the screen timeout, tap **Screen timeout**. Tap the option of your choice and then tap ← to go back to the previous screen.
5. To 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 56).
2. Under 'Device admin settings', scroll down and tap **Date & Time**.
3. Adjust according to your preferences.

➢ Configuring time zones on Teams devices

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

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

■ **Geolocation (Default):**

- The default geolocation method uses a device's public IP address to obtain its location. If the devices are behind NAT, they use a STUN server to discover their public IP addresses.

- A common STUN server example is Google's publicly accessible server: stun.l.google.com:19302 (default URL).

- **DHCP Option 100/101 (posix/tzdbx):**
  - Configuration is obtained from DHCP server (once defined as available).
- **Admin Provisioning:**

  Use one of the following:
  - Teams Admin Center, created under configuration profile.
  - Device Manager, created in configuration parameters setup.
  - AudioCodes Device Manager supports provisioning of the device's language, and date and time setting.

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

Configure Wi-Fi

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

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

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

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

Connect to an Available Wi-Fi Network

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

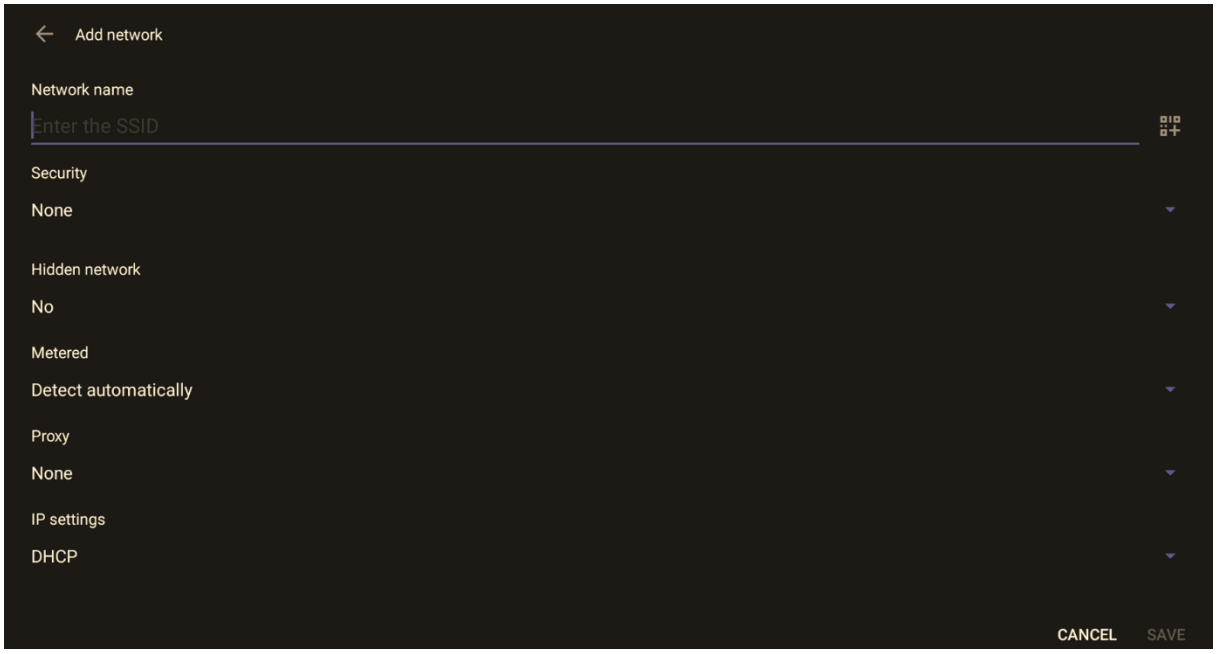
➢ **To connect to an available Wi-Fi network:**

1. If not already logged in, log in to Device Administration to get admin access (see Log in to Device Administration on page 56).
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 56).
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 66.
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 7-1: 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.
network/wireless/client_cert	Defines which client certificate to use.

Parameter	Description
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 64).

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 56).
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 56).
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.

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

➢ **To reconfigure a bundle:**

1. If not already logged in, log in to Device Administration to get admin access (see Log in to Device Administration on page 56).
2. Under 'Device admin settings', scroll down and tap **Bundle**.
3. Select the relevant bundle.

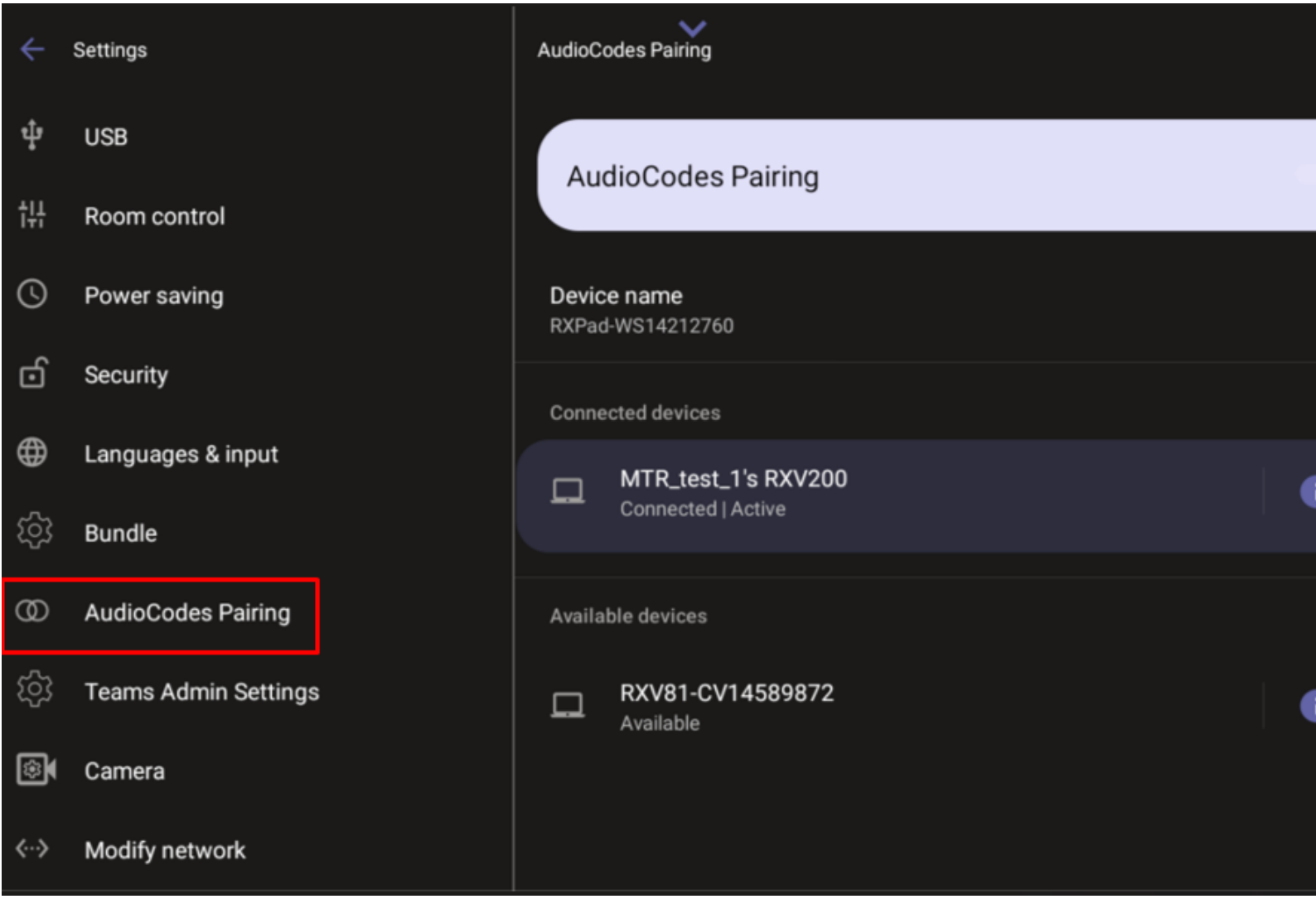
Pair RX-PAD with Different MTRA

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 56).
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 56).
2. Scroll down and tap the **Camera** option, then tap **Camera Settings**.

For details on configuring camera settings, see MTRA Camera Settings on page 26.

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 56).
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 73).

Set up a Proxy Server

Administrators can manually configure the RXV200 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

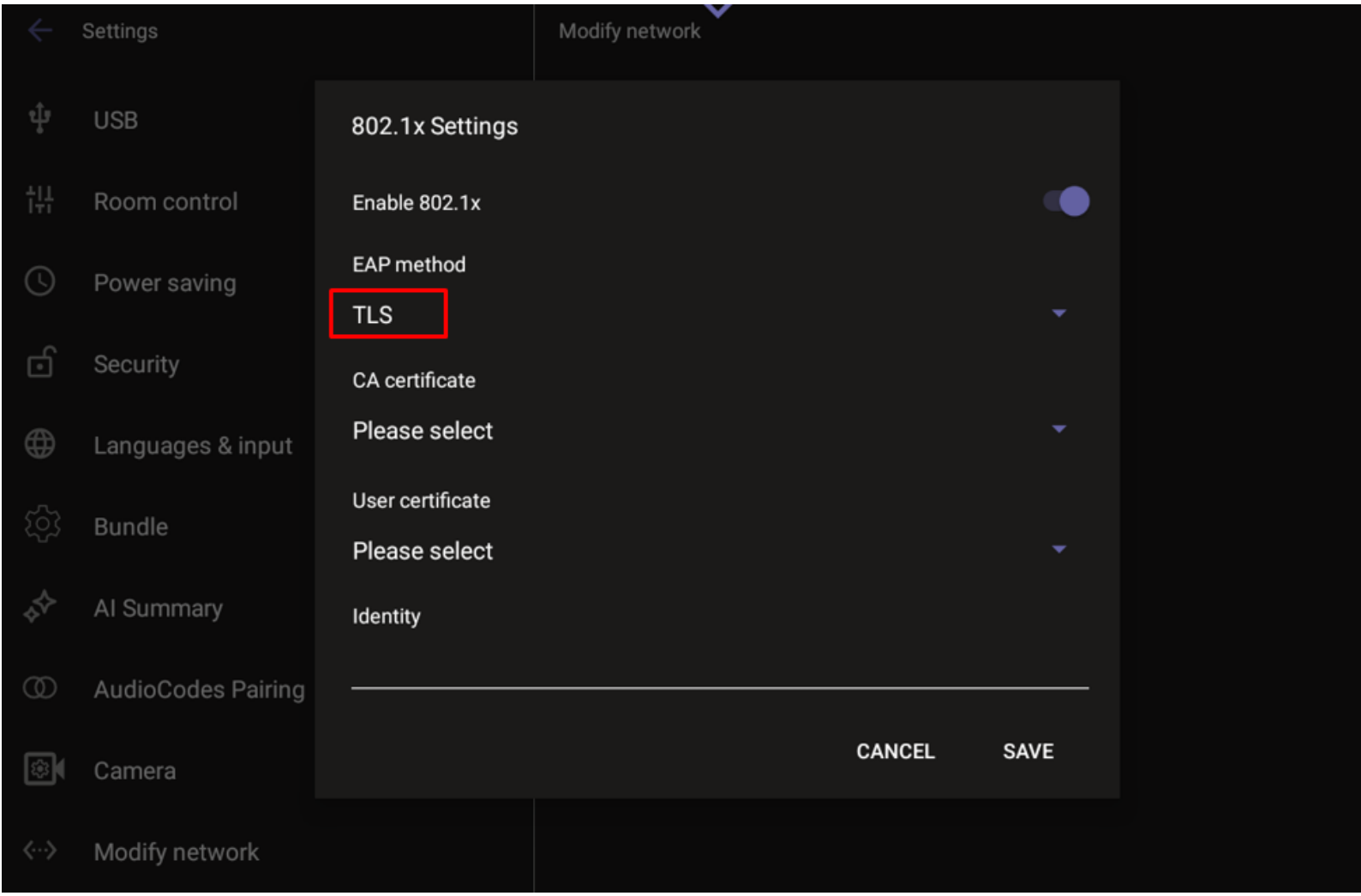
802.1x Authentication is the IEEE Standard for Port-based Network Access Control (PNAC) (refer to https://1.ieee802.org/security/802-1x/ for more information). It is used to enable port-based authentication.

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`

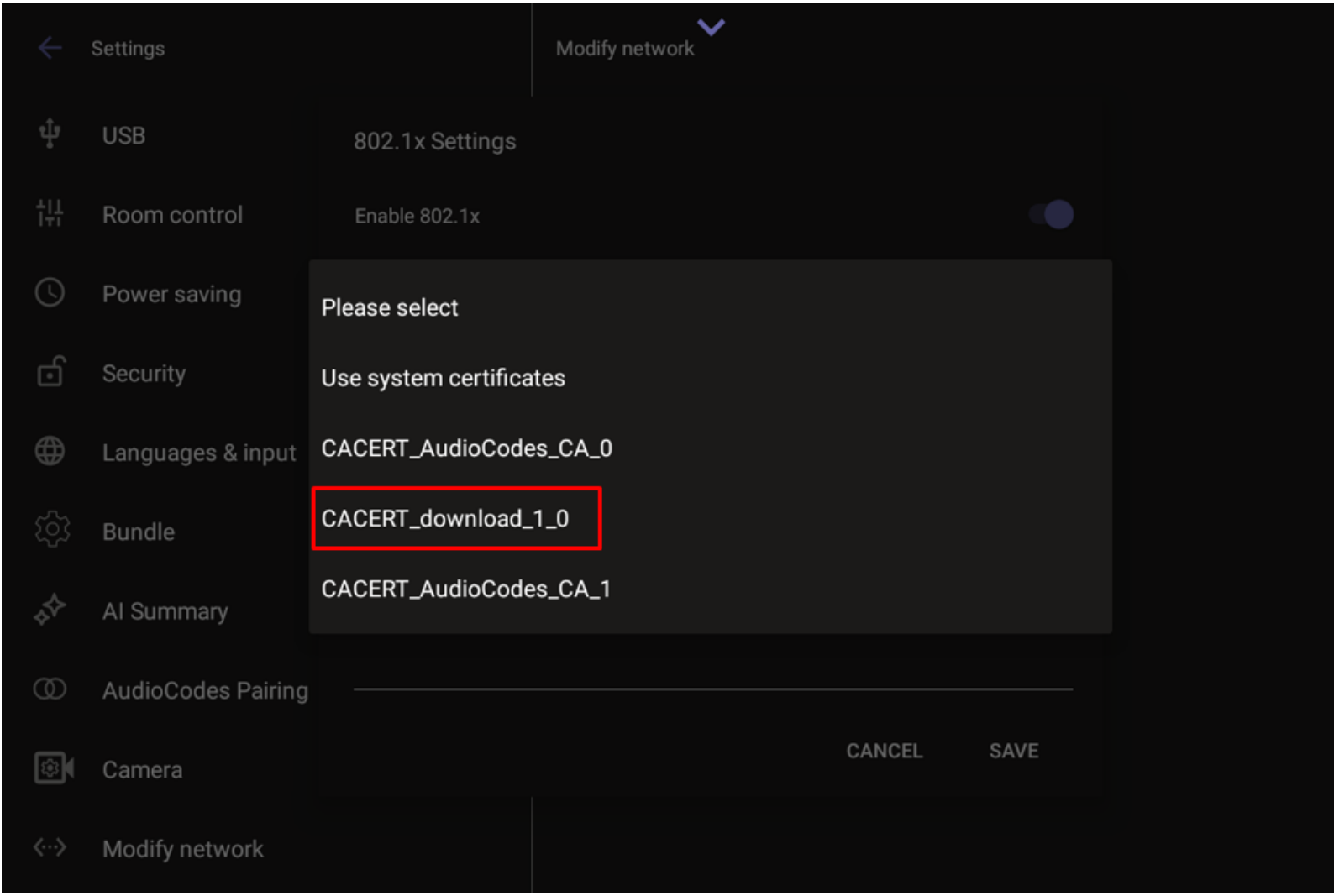
➢ **To configure 802.1x settings:**

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

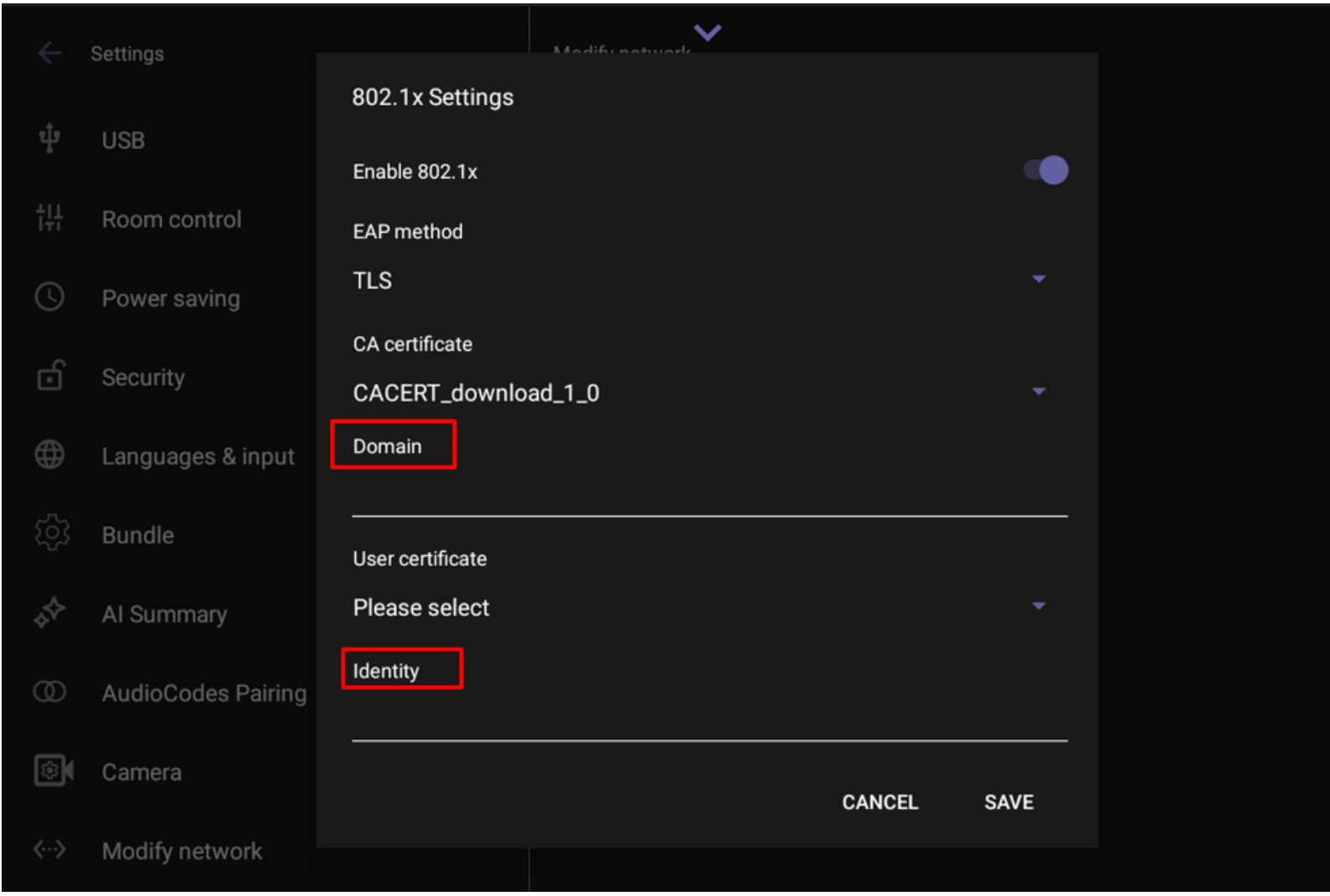
2. Tap **Enable 802.1x** and then tap **Save**.
3. Once 802.1x is enabled, choose the security method and strength. A commonly used option is EAP-TLS.



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 70) 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.

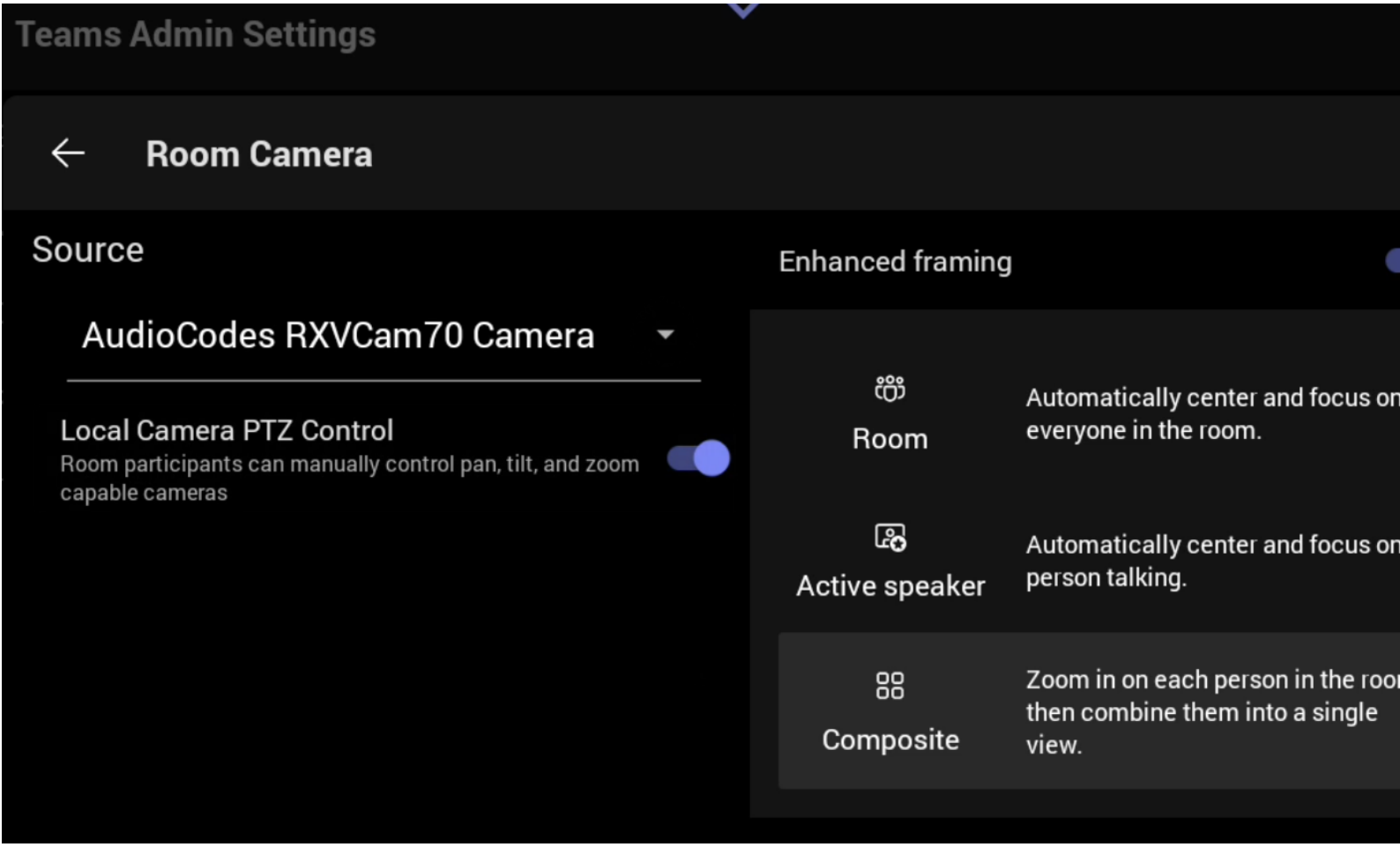
Configure Camera Settings with RX-PAD Teams Admin

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 56).
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.

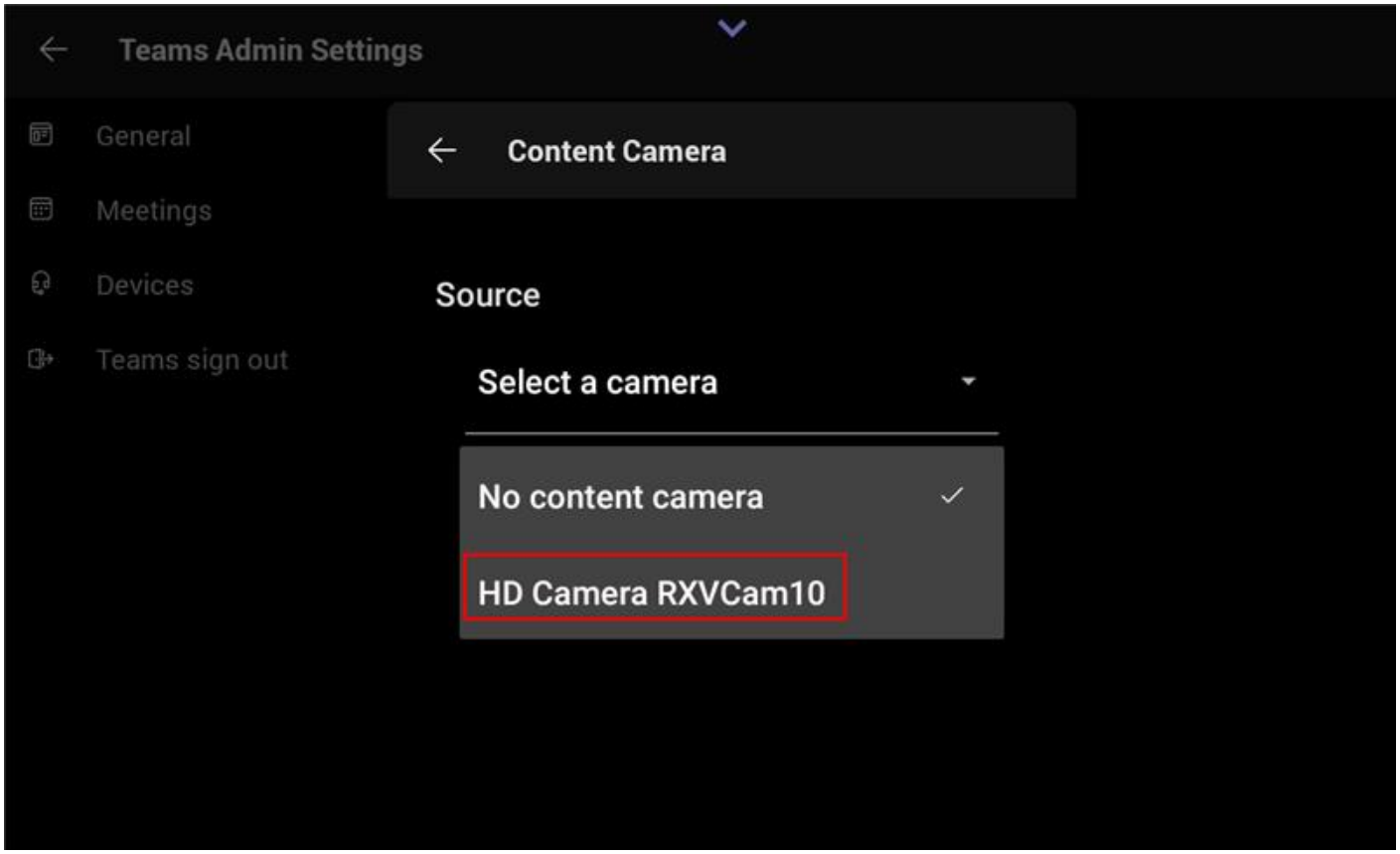
Content Camera Framing on a Whiteboard below describes how to use the Content Camera option to share a whiteboard using an RXVCam10 camera.

Content Camera Framing on a Whiteboard

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

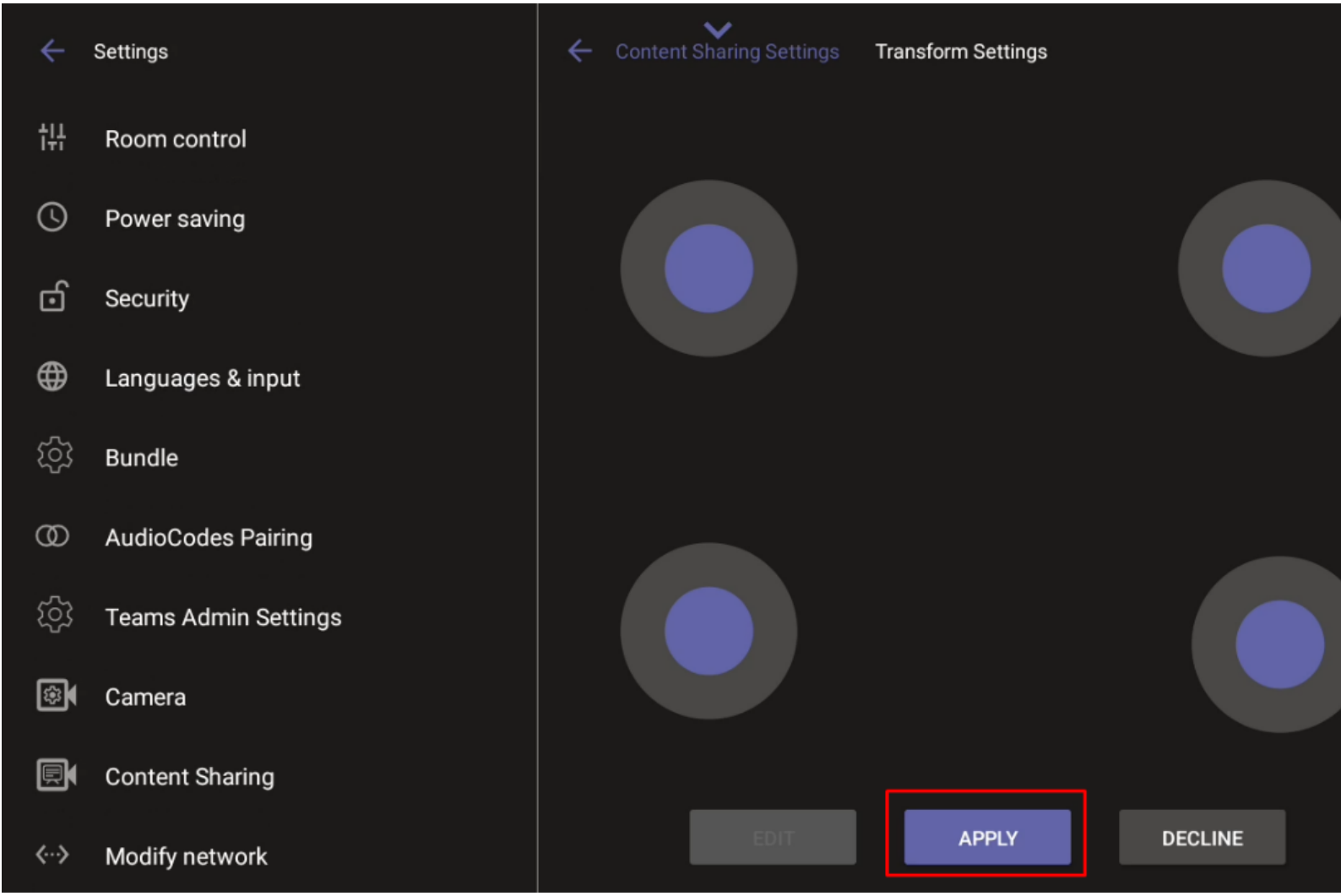
Presenters can share their physical whiteboard with remote participants using the **Content Camera** feature. To optimize the view, use **Transform settings** to define and capture the area precisely, isolating the whiteboard and removing unwanted margins beyond its edges.

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

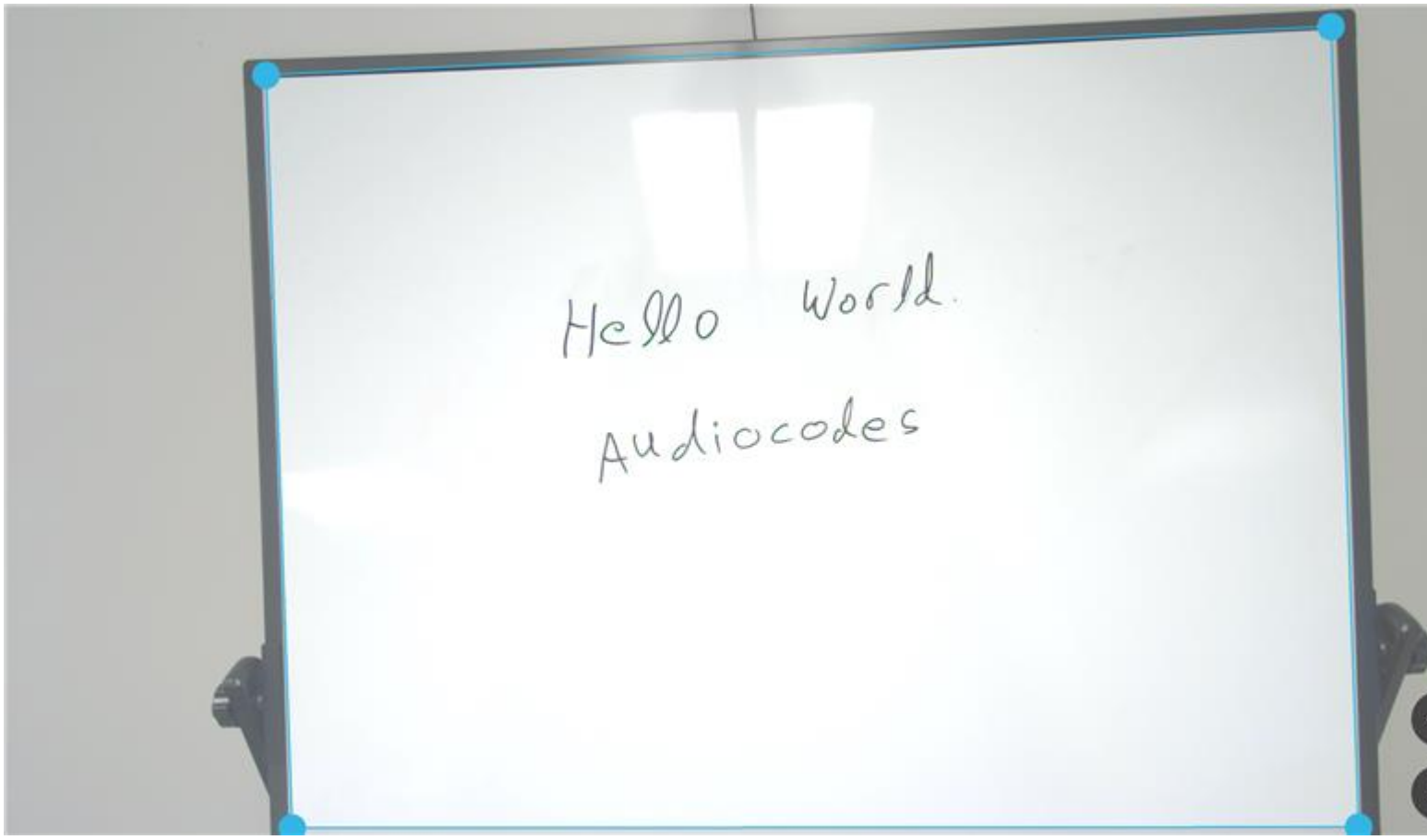


➢ **To share content:**

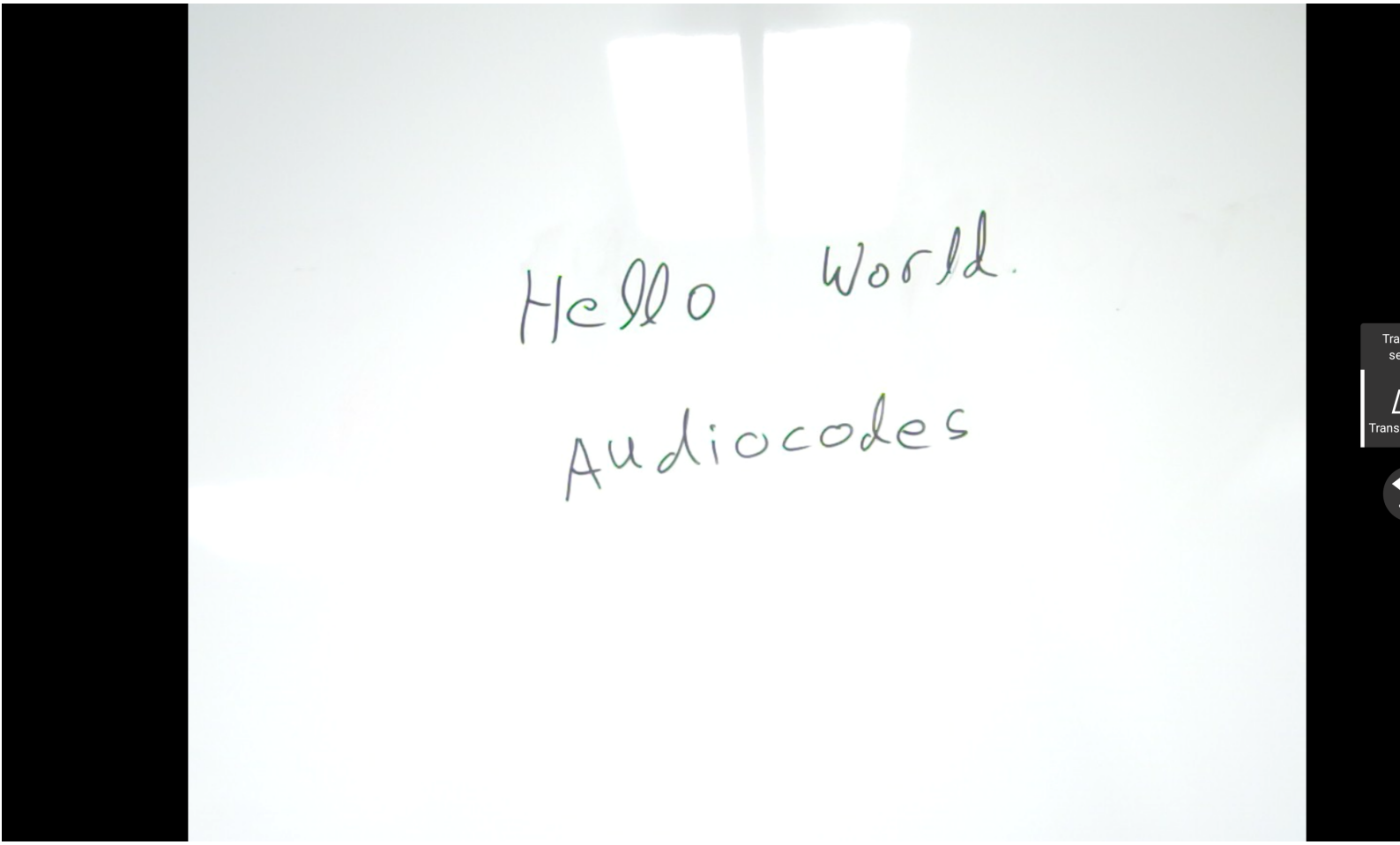
1. If not already logged in, log in to Device Administration (see Log in to Device Administration on page 56).
2. Under 'Device admin settings', scroll down and tap **Content Sharing**, then tap **Transform settings**:
3. Use the four joysticks on the RX-PAD to adjust the boundaries of the content camera's capture area:



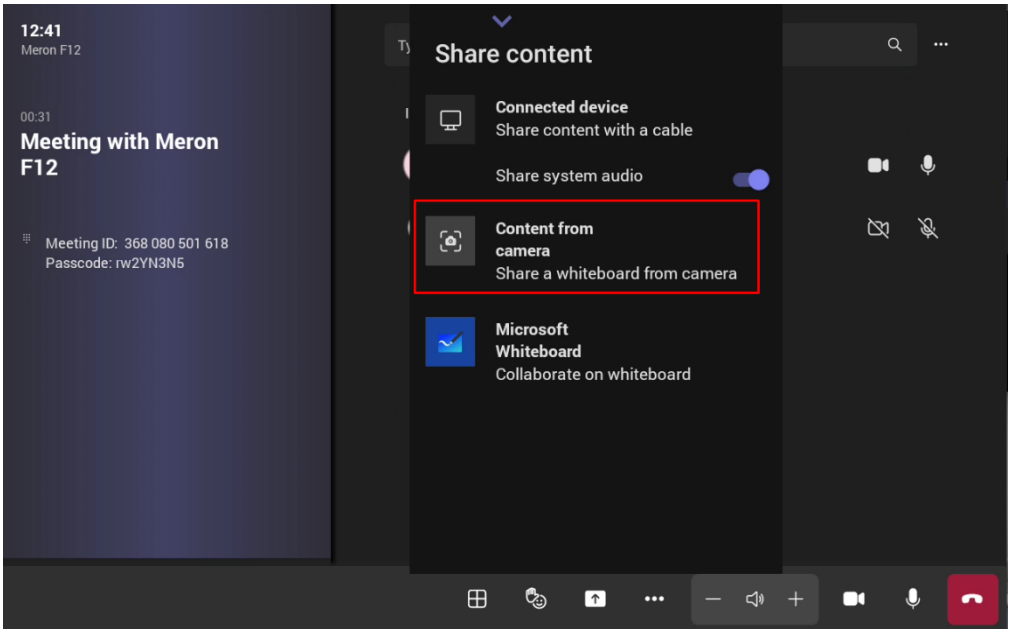
The admin can view the adjustment on the display:



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.

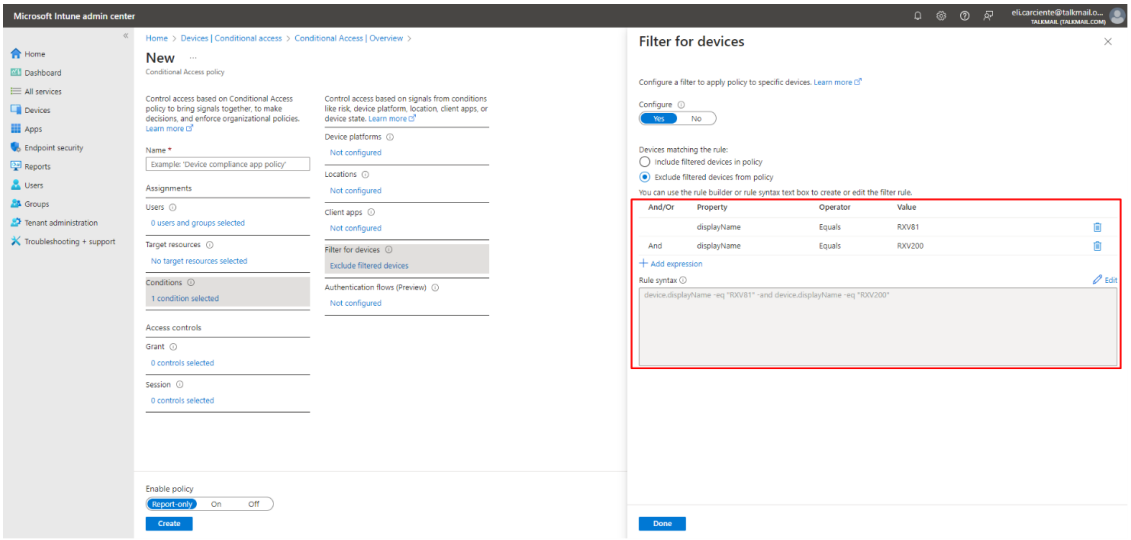
Create an Exclusion Group

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).

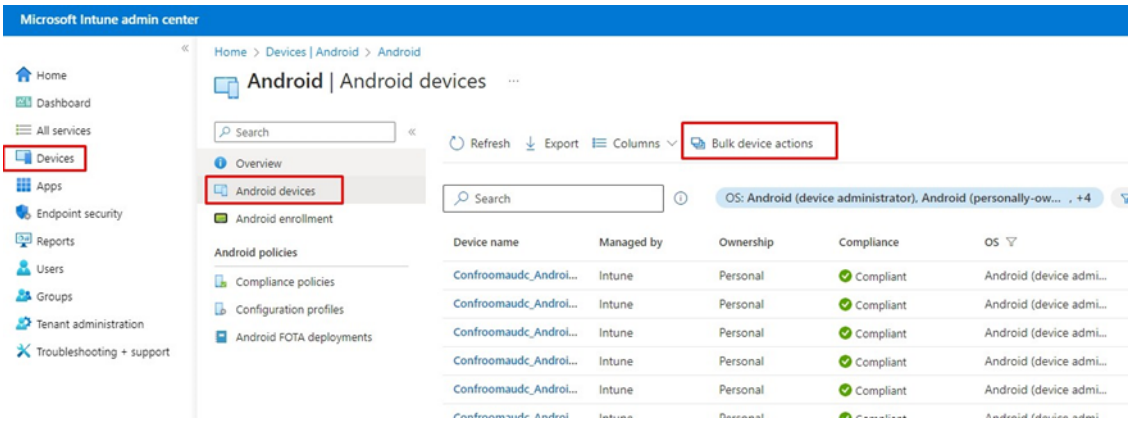


Remove Devices from Intune Admin Center

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

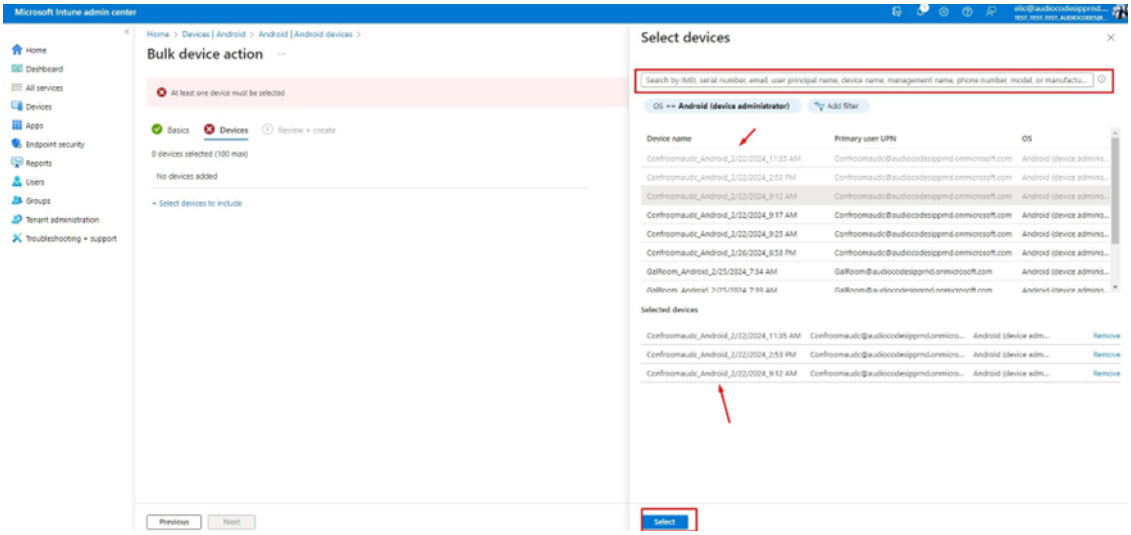
➢ To remove devices from Intune admin center:

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



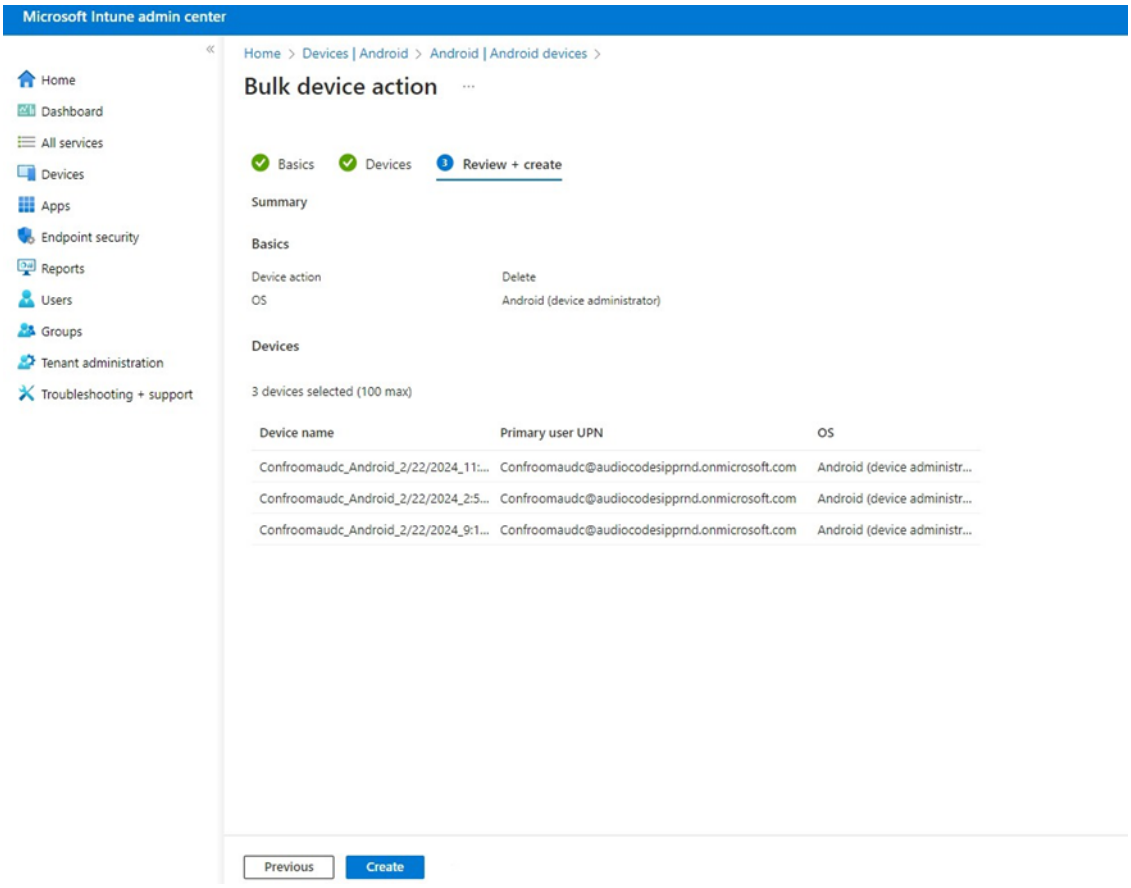
> The Intune admin center service is licensed according to the terms of individual licenses so not all network admins will be able to navigate to it. Check if the license you're using includes the service or not.

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`

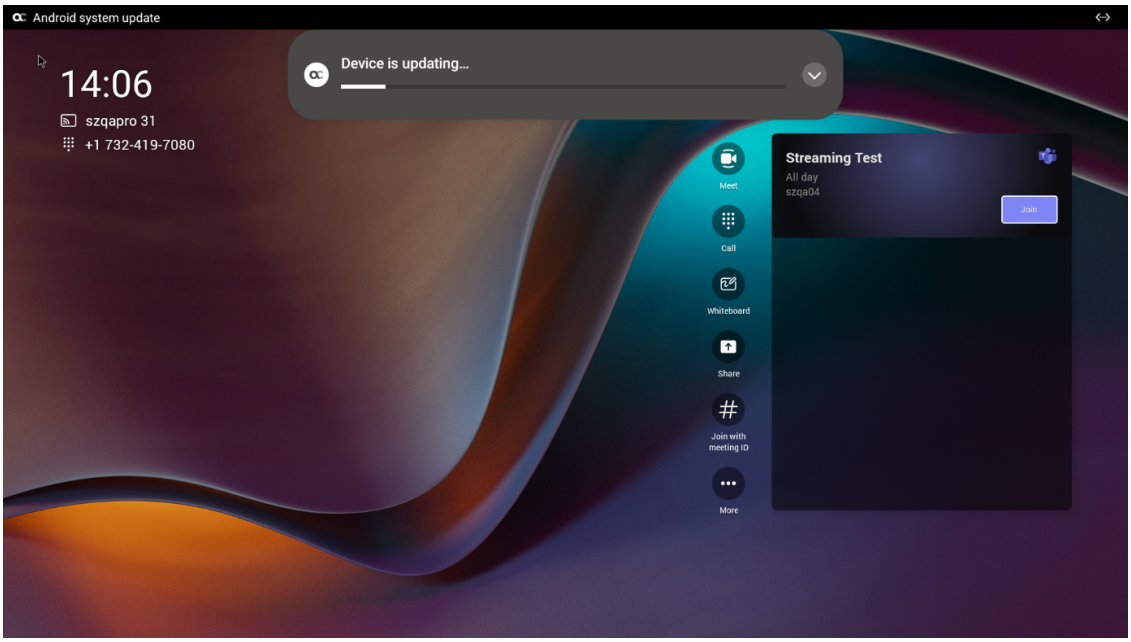
Update RXV200 Remotely

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

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

To ensure device integrity, RXV200 AudioCodes-branded audio and camera peripherals firmware is automatically updated at the same time as the RXV200 firmware update.

During the update, notifications are displayed, indicating the device being updated and alerting the user not to reboot. The RXV200 unit is updated first:



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

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

8 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 56).
2. Navigate to ‘Device Admin Settings’ (see Access Device Admin Settings on page 56).
3. Scroll down and tap **Debugging**.

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

Additional procedures for device monitoring and troubleshooting are:

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 61.

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 87).
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 87).
2. Tap **Diagnostic Data**.
3. Tap **OK** to confirm 'Copy logs to sdcard'; the device creates all necessary logs and copies them to the **SD Card/Logs** folder.
4. Get the logs using SCP notation as follows:

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

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

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

Reset the System Configuration

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

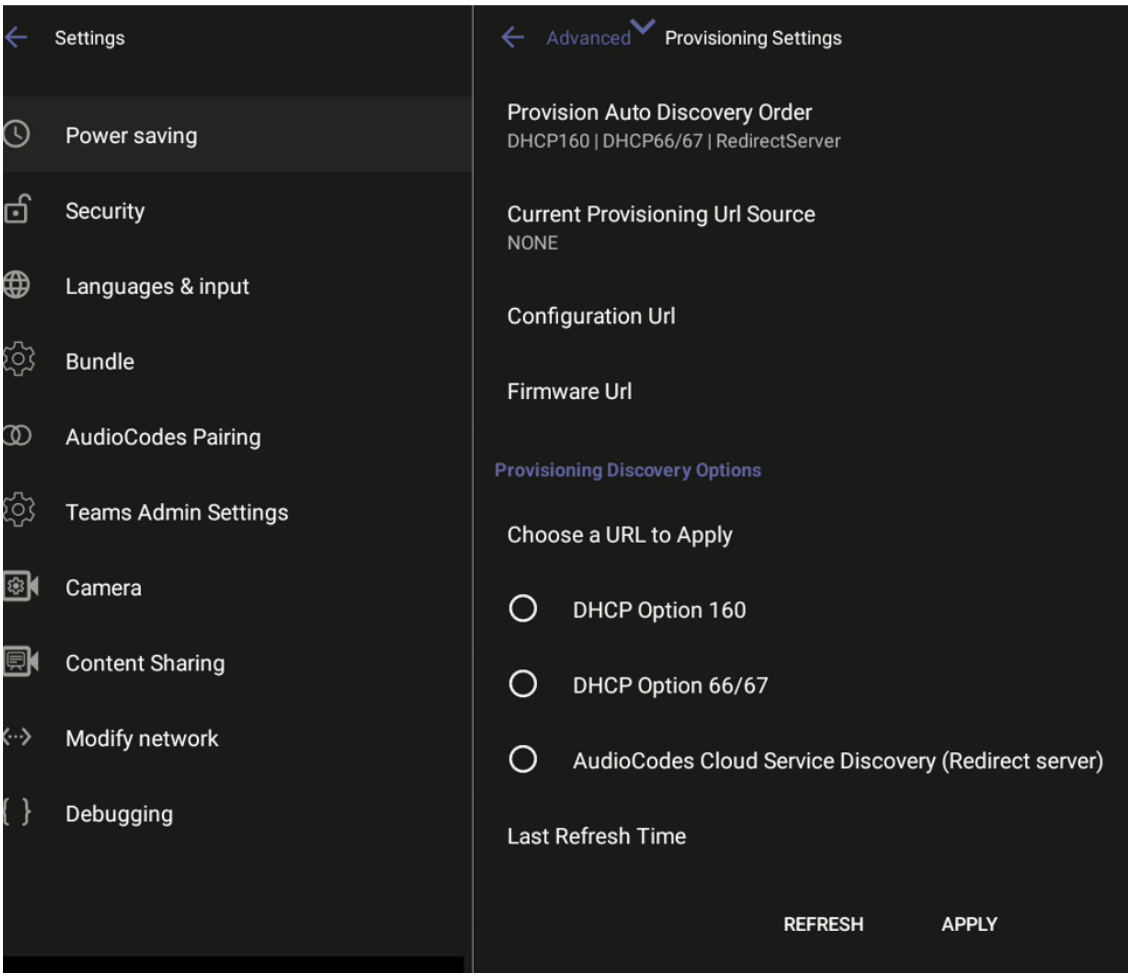
- Configure Provisioning Source Auto Discovery Settings below
- Reset Bundle Settings on the next page
- Reset to Original Configuration on the next page
- Perform a Full Factory Reset on page 92

Configure Provisioning Source Auto Discovery Settings

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

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

1. Access the 'Debugging' page (see System Monitoring and Debugging on page 87).
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 Bundle Settings

Admins can reset the current bundle settings using the **Reset Bundle** action. This action removes the current settings. Subsequently, upon rebooting the device, the bundle wizard is displayed (see Reconfigure a Bundle on page 67), where the new bundle type can be selected.

To reset the bundle:

1. Access the 'Debugging' page (see System Monitoring and Debugging on page 87).
2. Tap **Advanced**, then **Reset Bundle**. A confirmation prompt is displayed.
3. Select **OK**.

Reset to Original Configuration

Admin users can opt to ‘clean up’ their configuration history and return the RXV200 to an Out of Box Experience (OOBE). If the Teams app isn't running well, this might help.

➢ **To perform a factory reset:**

1. Access the 'Debugging' page (see System Monitoring and Debugging on page 87).
2. Tap **Reset configuration**, then tap **OK** to confirm.

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

Perform a Full Factory Reset

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

➢ **To erase all data (factory reset):**

1. Access the 'Debugging' page (see System Monitoring and Debugging on page 87).
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 87).
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 87).
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 87).
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 87).
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 87).
2. Tap **Return to previous version**. The device changes the active firmware slot and undergoes a factory reset.

Determine Device Status from LED Color Indications

Users and admins can determine the status of the RXV200 from its LED color indications.

Use the following table as reference to determine the status.

Color Indication	Status
Blue	Indicates the device is currently booting up
Green	Indicates the device is currently idle
Flashing red	Indicates the device is currently receiving an incoming call/meeting
Red	Indicates the device is currently in a call/ meeting/mute

Perform Recovery Operations using the Power Button

Network administrators can perform recovery operations using the power button on the front panel of the RXV200.

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

The following figure shows the power button.

➢ **To perform recovery operations:**

1. Disconnect the power cord from the RXV200 while long pressing the power button shown in the preceding figure.

2. Reconnect the power cord and continue pressing the power button, as described in the following table.

Press button	Action	Press button for	LED indication after releasing the button
On Uboot	Nothing	<= 4 seconds	
	ENTER_RECOVERY	4 ~ 6 seconds	Red
	SWITCH_AB_SLOT	6 ~ 8 seconds	Green
	ENTER_LOADER	8 ~ 10 seconds	Blue
	RESTORE_DEFAULTS	>= 10 seconds	Yellow

3. In the recovery menu use the power button to navigate between menus in the recovery mode. Long-pressing the button selects the highlighted option.

Save Logs while the Device is in Recovery Mode

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

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

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

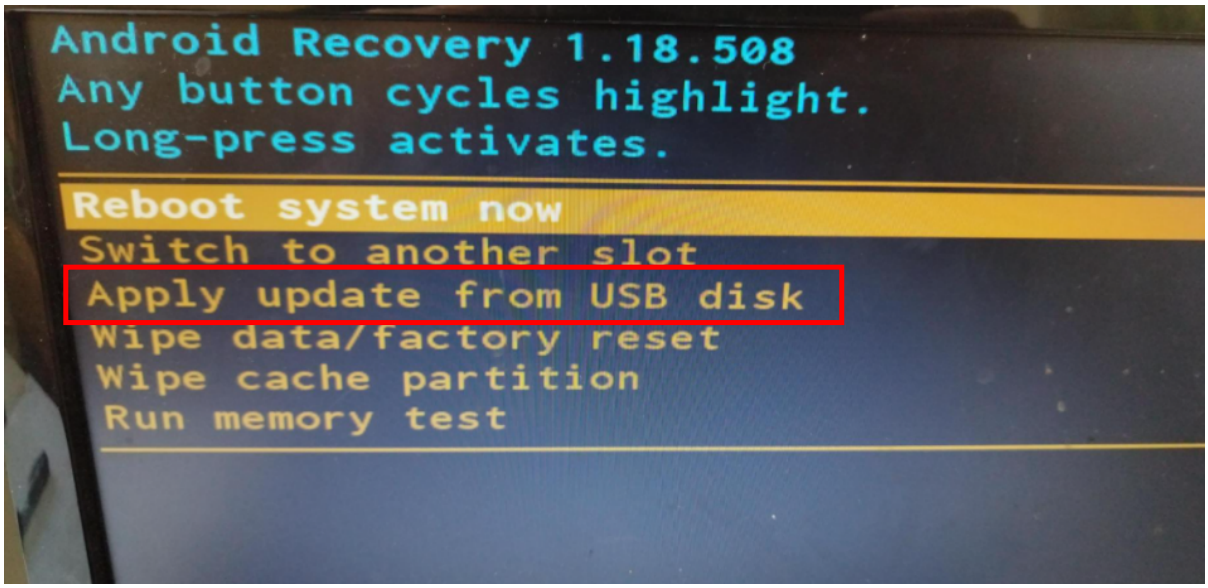
Restore Device Firmware via USB Disk

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

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

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

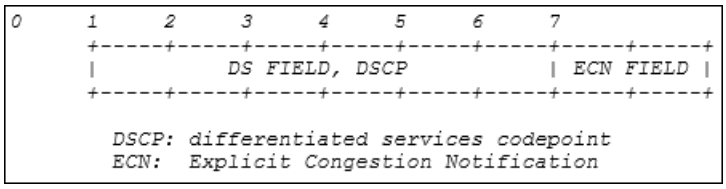
4. Select the **Apply update from USB disk** option and then choose the correct firmware image from the disk.



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).

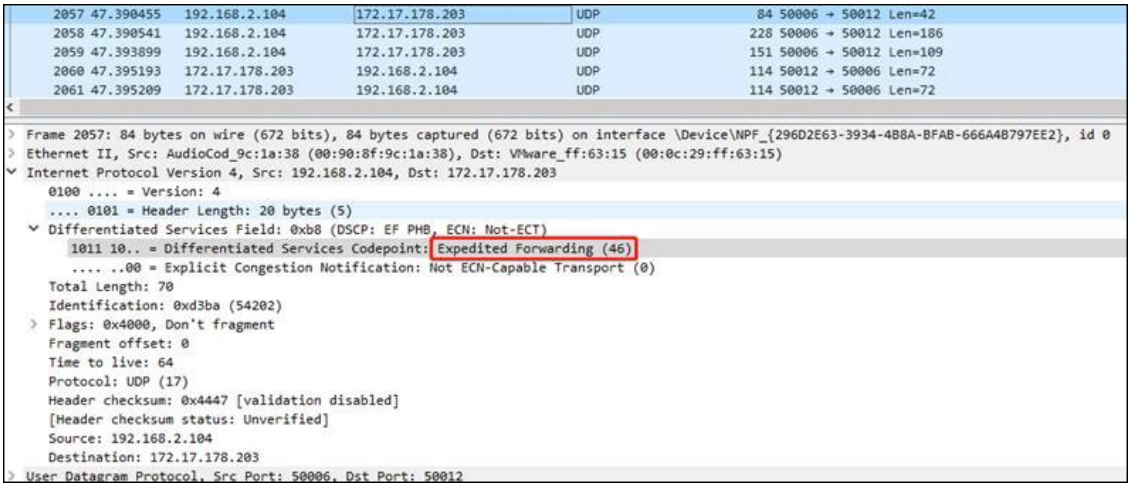
> The DSCP value can be adjusted on the server, but not on the client.

The following figure shows the recommended port ranges:

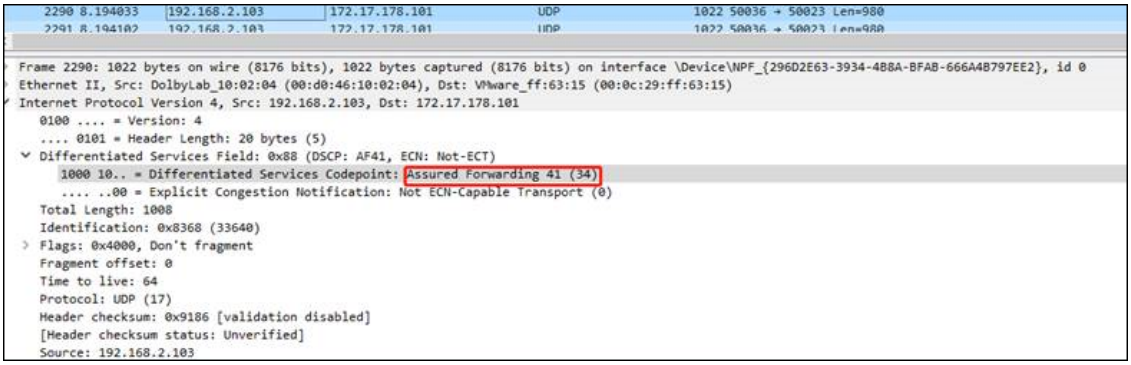
Table 1. Recommended initial port ranges

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.

9 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-09997