

# AudioCodes RX-PAD Meeting Room Controller

Version 2.4





---

## Table of Contents

---

<b>1</b>	<b>Introduction .....</b>	<b>7</b>
1.1	Highlights .....	7
1.2	Specifications .....	8
1.3	Connectivity .....	8
1.4	Managing RX-PAD .....	8
1.5	Audio Notifications via MTRA Speakers.....	8
1.6	Security Guidelines.....	9
1.6.1	Microsoft Teams Security Guidelines .....	9
1.6.2	Android Level Security Hardening .....	9
1.6.2.1	Google Play Services .....	9
1.6.2.2	Running Android in Kiosk Mode .....	9
1.6.2.3	Screen Lock.....	10
1.6.2.4	AudioCodes Private Key .....	10
1.6.2.5	Android Debug Bridge (ADB) .....	10
1.6.2.6	App Signing .....	10
1.6.2.7	Web Browser .....	10
1.6.2.8	Remote Configuration Management .....	10
1.6.2.9	AudioCodes Device Manager Validation .....	10
1.6.2.10	Sandboxing.....	11
1.6.2.11	Keystore.....	11
1.6.2.12	Device Certificate.....	11
1.6.2.13	Data Protection.....	11
1.6.2.14	Device File System.....	11
1.6.2.15	Debugging Interface .....	11
1.6.3	Android Security Updates.....	11
1.6.4	AudioCodes Root CA Certificate.....	12
<b>2</b>	<b>Getting Started .....</b>	<b>13</b>
2.1	Setting up RX-PAD.....	13
2.2	Signing in to RX-PAD .....	13
2.2.1	Configuring Admin Login Timeout .....	13
2.3	Pairing RX-PAD with MTR .....	13
2.4	After Pairing.....	14
<b>3</b>	<b>Operating RX-PAD .....</b>	<b>15</b>
3.1	Operating with the Remote Keyboard.....	16
3.2	Managing Popup Messages.....	16
3.3	Adjusting MTR Camera Settings.....	17
3.3.1	Configuring a Color Mode Preset on the RXVCAM50M/L Camera .....	20
3.4	Configuring a Bundle .....	21
3.5	Configuring Ad Hoc Mode on RXV81 MTRA.....	22
3.6	Screen Sharing.....	23
<b>4</b>	<b>Configuring User Settings .....</b>	<b>25</b>
4.1	Accessibility .....	25
4.2	Setting Live Captions .....	25
4.3	Hiding Names and Meeting Titles .....	25
4.4	Reboot .....	25
4.5	About.....	25

<b>5</b>	<b>Enrolling a Device with Intune Policies .....</b>	<b>27</b>
5.1	Creating a Dynamic Group.....	27
5.2	Creating an Exclusion Group .....	27
5.3	Removing Devices from Intune admin center.....	28
<b>6</b>	<b>Monitoring Device Software Modules Status .....</b>	<b>33</b>
<b>7</b>	<b>Debugging.....</b>	<b>35</b>
7.1	Log Settings   Collecting Logs.....	36
7.2	Remote Logging .....	38
7.3	Diagnostic Data .....	39
7.4	Reset configuration.....	40
7.5	Restart Teams app .....	40
7.6	Company Portal Login.....	40
7.7	Getting Company Portal Logs .....	40
7.8	Launch Mobile Teams .....	41
7.9	Debug Recording.....	41
7.10	Restoring to Defaults .....	42
7.11	Erase all data (factory reset).....	42
7.12	Screen Capture .....	43
7.13	Performing Recovery Operations.....	43
7.14	Restoring Device Firmware via USB Disk .....	44
<b>8</b>	<b>Saving Logs while Device is in Recovery Mode.....</b>	<b>45</b>
<b>9</b>	<b>Updating Microsoft Teams Devices Remotely .....</b>	<b>47</b>

## Notice

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

This document is subject to change without notice.

Date Published: May-15-2024

## 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.

## 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>.

## Stay in the Loop with AudioCodes



## Abbreviations and Terminology

Each abbreviation, unless widely used, is spelled out in full when first used.

## 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 Web site at <http://online.audiocodes.com/documentation-feedback>.

## Related Documentation

Document Name
RXV81 RXV200 RX-PAD RX-PANEL Release Notes
<a href="#">RX-PAD Meeting Room Controller Quick Guide</a>
<a href="#">Pairing RX-PAD with Teams Rooms on Android</a>
<a href="#">RXV81 MTRA User &amp; Admin Manual</a>
RXV200 MTRA Compute User & Admin Manual
RXV200 Microsoft Teams Rooms on Android Compute Unit Quick Installation Guide
Device Manager User & Admin Manual

## Document Revision Record

LTRT	Description
18320	Initial document release.
18321	Reset pinhole button
18322	HDMI In   MTRA screen sharing   Audio Notifications via MTRA Speakers
18323	Application launcher. Enrolling with Intune Policies. System State page.

# 1 Introduction

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

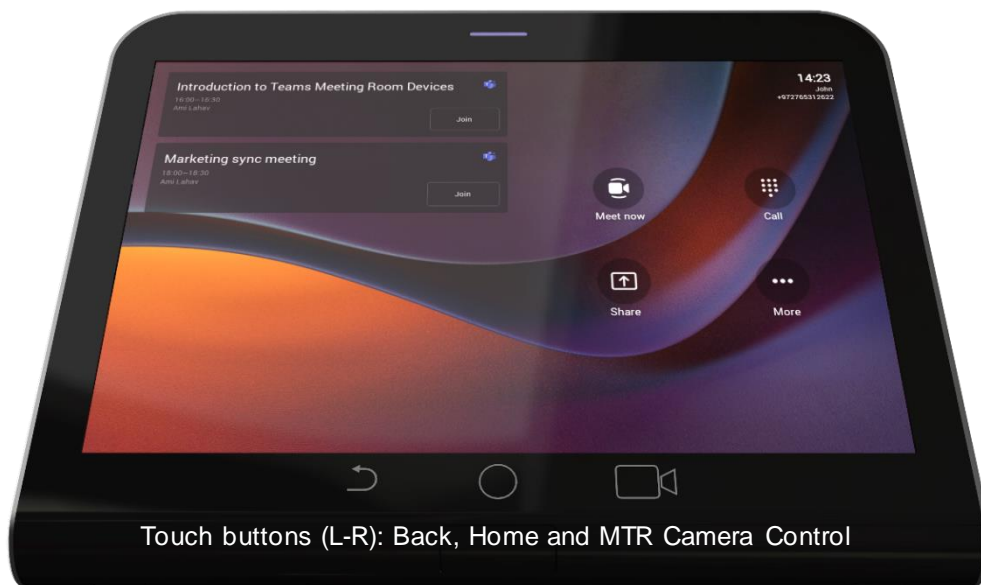
With its proximity sensor, ergonomic design and 8-inch high-resolution display, this high-quality controller enables simple and intuitive operation with extensive customization options.

RX-PAD Meeting Room Controller offers innovative features such as one-click-to-join with an integrated calendar for simple collaboration initiation, smooth content sharing and easy camera adjustments, among others.






Part number: TEAMS-RX-PAD – MSRP

## 1.1 Highlights

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



	Speedy collaboration initiation. One-click-to-join for easy collaboration.
	An inbuilt calendar to quickly set or join meetings
	A single cable connection keeps your desk clean and tidy
	Innovative ergonomic design for seamless operation
	High-resolution, eight-inch touch LCD

	Human sensor
	Cable compartment
	POE or power enabled
	Dual-band Wi-Fi and Bluetooth support
	Android 12

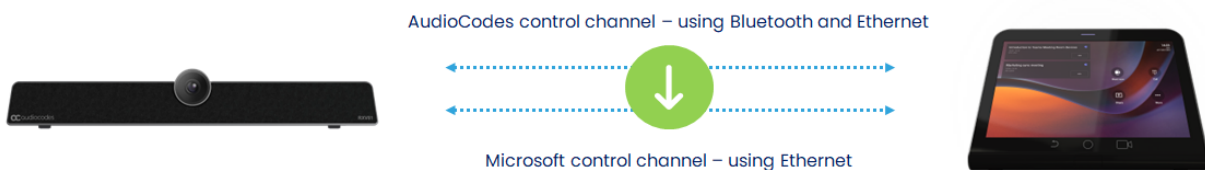
## 1.2 Specifications

See the [RX-PAD Datasheet](#) for more information.

## 1.3 Connectivity

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

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



## 1.4 Managing RX-PAD

Admins can use AudioCodes Device Manager to manage RX-PAD. Management includes:

- Monitoring
- Firmware management / upgrade
- Alarm management



**Note:** For more information, see the *Device Manager User & Admin Manual*.

## 1.5 Audio Notifications via MTRA Speakers

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



## 1.6 Security Guidelines

The RX-PAD is an AudioCodes Native Teams Android-based device purpose-built and customized for Teams calling and meeting and designed to enhance security as part of the default use.

Though customers might see Android-based systems as prone to security issues, security is much less a concern on devices that are purpose-built for Teams meeting and calling.

When analyzing the security of the device there are two levels that should be addressed:

- Authentication and security with regards to Teams connectivity and use
- Android level / system of the device

### 1.6.1 Microsoft Teams Security Guidelines

- Following are AudioCodes' recommendations with regards to device security:
  - Use "sign-in with other device option" – using this mode the user does not type the password on the device, instead obtains a code to be used to sign-in on his PC/laptop; the device obtains a private token that enables it to access Teams cloud; this token, unlike a password, allows only that device which obtained it to reuse it. The token is stored on the secured file system.
  - Leverage Multi-Factor-authentication (MFA) to improve the security of the sign in.
  - IT can consider reducing the expiration time of the sign in for devices which are connected remotely (outside the organization network) vs devices in the organization premise.
- Visit Microsoft technical pages and learn more on security guidelines and policies for Microsoft Teams adoption:
  - [Overview of security and compliance - Microsoft Teams | Microsoft Docs](#)
  - [Identity models and authentication for Microsoft Teams - Microsoft Teams | Microsoft Docs](#)
  - [Sign in to Microsoft Teams - Microsoft Teams | Microsoft Docs](#)

### 1.6.2 Android Level Security Hardening

This section describes the major changes performed on the system/Android level that were incorporated into the device to improve its security.

#### 1.6.2.1 Google Play Services

Goggle Play services were removed from the device software – no access is allowed to any Google store or Play services.

- The device update of the Android software and application is done via special software components that either connect into Teams Admin Center or to AudioCodes Device Manager over secured channel.

#### 1.6.2.2 Running Android in Kiosk Mode

Android Kiosk Lockdown software is the software that locks down the Android devices to just allow the essential apps by disabling access to the Home/Launcher. Using Android Kiosk Lockdown software, the Android devices can be converted into public kiosk terminals or secured work devices.

- Only specific Microsoft apps and AudioCodes signed apps that were certified and approved in the certification process can run under the Kiosk mode; even if a malicious user managed to install a new un-authorized app on the file system – the launcher on the device will only run those specific approved apps and this cannot be changed in run time (only with new software code that is provided by AudioCodes).

### 1.6.2.3 Screen Lock

AudioCodes Native Teams devices use a screen lock mechanism to prevent any malicious user/users from gaining access to Calendar information and / or Active Directory list of employees and / or triggering unauthorized Teams calls from the device. After enabling screen lock, the device automatically locks after a preconfigured period; a code is required to unlock the device and resume full operation.

### 1.6.2.4 AudioCodes Private Key

The system software on the device is signed with AudioCodes private key – users can replace the complete software only with new software that is also signed by the AudioCodes private key. This prevents the user from replacing the complete OTA package of the device with any new system software unless this software has been fully signed by AudioCodes.

### 1.6.2.5 Android Debug Bridge (ADB)

AudioCodes disables the Android Debug Bridge (ADB) application and keeps the Teams app running in the front all the time, which means there is no way to install other Apps from unknown sources and sideloading.

### 1.6.2.6 App Signing

Android requires that all apps are digitally-signed with a developer key before installation; currently the device verifies that the apps are signed by Microsoft. App signing prevents malicious user/users from replacing a Microsoft-signed app with an app that "pretends" to be Microsoft but which lacks the private key that is known only to Microsoft.

### 1.6.2.7 Web Browser

The device does not include a Web browser – users cannot browse to the public internet or internal intranet– all Web services are customized to connect to O365 services and AudioCodes managed services such as One Voice Operations Center (OVOC).

Without a web browser, malicious user/users will not be able to access the device and browse from it as a trusted device into the customer network.

### 1.6.2.8 Remote Configuration Management

The Native Teams device does not have an embedded WEB server – configuration and management is performed using one of the following remote interfaces:

- Microsoft Teams Admin Center (for Native Teams devices) over HTTPS protocols – this is enabled after successful sign-in authentication process.
- AudioCodes Device Manager (part of AudioCodes OVOC suite) over HTTPS.
- Debugging interface over SSH. Note that SSH MUST be disabled by default and enabled only per specific case for debugging-purposes only.

### 1.6.2.9 AudioCodes Device Manager Validation

The device validates the AudioCodes Device Manager identity using known root CA:

- The device is shipped with known Root CAs installed. See [here](#).
- For the initial connection phase, the AudioCodes Device Manager should access the device using a known CA.
- Once a successful secured connection has been established between the device and the Device Manager, the user can replace the root CA on the Device Manager and on the device and re-establish the connection leveraging any private root CA.

### 1.6.2.10 Sandboxing

AudioCodes Native Teams devices use Android Application Sandbox so that each application can access its own data and is isolated from other applications. This prevents a malicious app from accessing the code or the data of other applications in the system.

### 1.6.2.11 Keystore

With AudioCodes Native Teams devices, the certificate keys are encrypted on the device file system.

### 1.6.2.12 Device Certificate

AudioCodes Native Teams devices are shipped with a unique certificate which is signed by AudioCodes Root CA.

### 1.6.2.13 Data Protection

AudioCodes Native Teams devices run Android which has integral procedures for protecting and securing user data.

### 1.6.2.14 Device File System

The device file system is encrypted on the device – customers may enforce a policy of device encryption via Microsoft Intune.

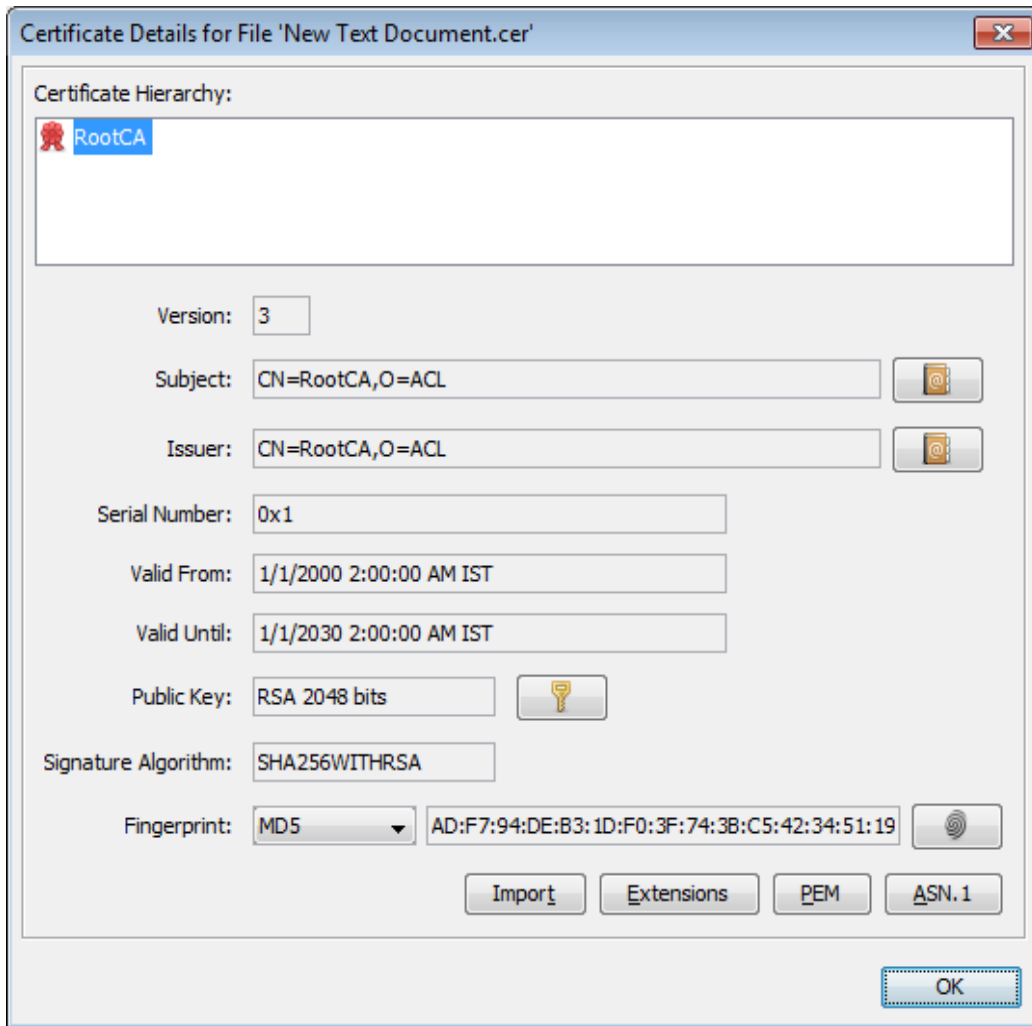
### 1.6.2.15 Debugging Interface

- The device leverages SSH as a debugging interface.
- AudioCodes recommends that customers disable SSH on the device – this can be done via the AudioCodes Device Manager (OVOC).
- AudioCodes recommends changing the Admin password from the default, which can be done via Teams Admin Center or AudioCodes Device Manager (OVOC).
- When debugging of a specific device is required, the user can enable SSH on specific device/s, access SSH with the new Admin password for debugging phase and disable SSH once debugging has been completed.

## 1.6.3 Android Security Updates

In addition to all the above, AudioCodes regularly adopts and integrates the Android security updates. For reference see [here](#).

### 1.6.4 AudioCodes Root CA Certificate



```

-----BEGIN CERTIFICATE-----
MIIDMTCCAhmGAWIBAgIBATANBgkqhkiG9w0BAQsFADAfMQwwCgYDVQQKEwNBQ0wx
DzANBgNVBAMTB1Jvb3RDQTAeFw0wMDAxMDEwMDAwMDBaFw0zMDAxMDEwMDAwMDBa
MB8xDDAKBgNVBAoTAA0FDTDEPMA0GA1UEAxMGUm9vdENBMIIBIjANBgkqhkiG9w0B
AQEFAAOCAQ8AMIIBCgKCAQEAE6GK495KUCXAm/UE17G4/cjnZN4LNaxYFYzbfZL0a
EhgSKYt/LQ+iUcDhojsneusNgrcGkpwKk1KsGsvGwMSRNULV01CW+TX2VJN73+hh
V0uzhyOIYAUhbdAoqNM6Kp5b7sJ1ew4I9kfd/ma9Cz15koESLlW/inLj/r+rD96
mUcPElWrKspv7Qy4I14fsK/yMArixRopTL1munVVPpSFM9Jh8IY3JHyr5CQJXKks
EhGAJsnHaRqsR2Su3X/WtslgEF+cvP34pxhlhFL29nMfnaFATSS3rgGaFlSv11ZS
esLMqkWj9c9qGYrvt7K61sYnvMMb+o/KbWqVokXb+Fr7bwIDAQABo3gwdjAMBgNV
HRMEBTADAQH/MB0GA1UdDgQWBBDQXySn9hz151DraZ+iXddZGRb+zBHBgNVHSME
QDA+gBQDXySn9hz151DraZ+iXddZGRb+6EjpcEwHzEMMAoGA1UEChMDQUNMMQ8w
DQYDVQQDEwZSb290Q0GCAQEwDQYJKoZIhvcNAQELBQADggEBAI0rUywowmWWJnH3
JOfKiS3+VnX5hJITZymvWanMXUz/6FonHccPXEBYTrUYwhiWx3dweLAFXDFKkxMp
0KKWZ4F39cAOLRjqhzya+xUeeJ9HQZCXyAJ6XgvTfn2BtyZk9Ma8WG+H1hNvvTZY
QLbWsjQdu4eFniEufeYDke1jQ6800LwM1Flc59hMQCeJTENrx4HdJbJV86k1gBUE
A7fJT1ePrRnXNDRz6QtADWoX3OmN7Meqen/roTwwLpEP22nYwvB28dq3JetlQKwu
XC4gwI/o8K2wo3pySLU9Y/vanXXCr0/en513RDz1YpYwWqWHA8jJIu8rxdhr+VNQ
Zv6R/Ys=
-----END CERTIFICATE-----

```

## 2 Getting Started

### 2.1 Setting up RX-PAD



**Note:** See *RX-PAD Meeting Room Controller Quick Guide* for information about shipped RX-PAD items, positioning, cabling, and powering up.

### 2.2 Signing in to RX-PAD



**Note:** See the *Pairing RX-PAD with Teams Rooms on Android AudioCodes Devices* for information about how to sign in to your Microsoft Teams Account.

#### 2.2.1 Configuring Admin Login Timeout

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)



**Note:**

- 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.

### 2.3 Pairing RX-PAD with MTR

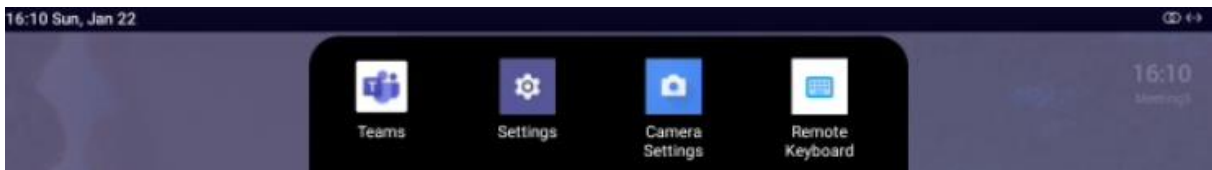
RX-PAD must be paired with the Microsoft Teams Room (MTR) on Android device (RXV81 | RXV200).



**Note:** See the *Pairing RX-PAD with Teams Rooms on Android AudioCodes Devices* for information about how to pair RX-PAD with RXV81 | RXV200.

## 2.4 After Pairing

After pairing RX-PAD with the MTR, scroll down in 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 MTR's 'Camera Settings')
- **Remote keyboard** (tap to control the MTR)

## 3 Operating RX-PAD

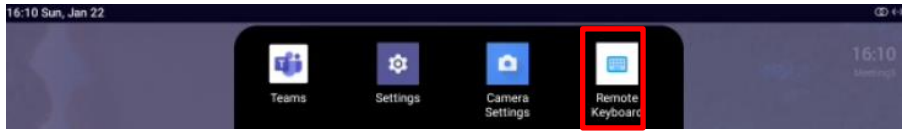
The following summarizes how to operate RX-PAD.



L-R	Description
1	Touch the back button to return to the previous screen.
2	Touch to return to the home screen or long-press to open the Device Settings page.
3	Touch to access the MTR's Camera Settings page.
4	Touch to open Microsoft Teams and the Device Settings menu.
5	Click to join a scheduled meeting.
6	Passive Infrared (PIR) motion sensor (hidden). When sensing motion, it wakes up RX-PAD from screensaver mode, automatically lighting up the screen to greet the user.
7	LED: <ul style="list-style-type: none"> <li>▪ Solid red indicates in a meeting</li> <li>▪ Solid green indicates the RX-PAD is online and signed in</li> <li>▪ Flashing red indicates incoming invite to join a meeting</li> </ul>
8	Drop-down menu to make it easy to open the RX-PAD application launcher. The new launcher enables accessing an app <i>with a single click</i> .

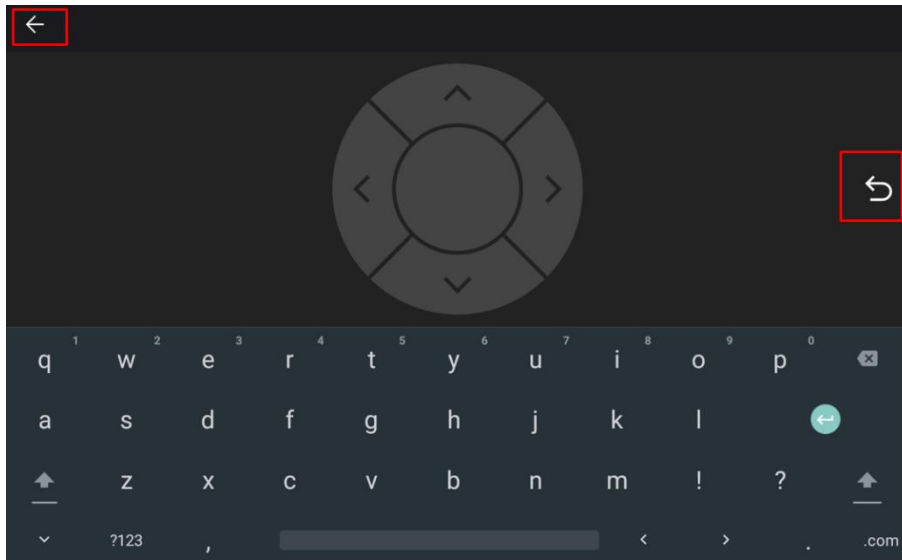
### 3.1 Operating with the Remote Keyboard

After pairing RX-PAD with the MTR, scroll down in RX-PAD to the Remote Keyboard menu:



➤ To operate with the remote keyboard:

1. Tap the menu indicated in the figure above.



2. Enable touchscreen controls for remote control of the MTR.
3. Use RX-PAD's remote keyboard to to:
  - Sign in to an MTR (RXV81 | RXV200)
  - Toggle between the MTR's Teams menus and device menus
  - Navigate to MTR settings for adjustment of relevant features (such as Bundle selection, etc.)
4. Tap the right arrow indicated in the figure above to go back to the previous menu in the MTR.
5. Tap the uppermost left arrow indicated in the figure above to exit Remote Keyboard mode.

### 3.2 Managing Popup Messages

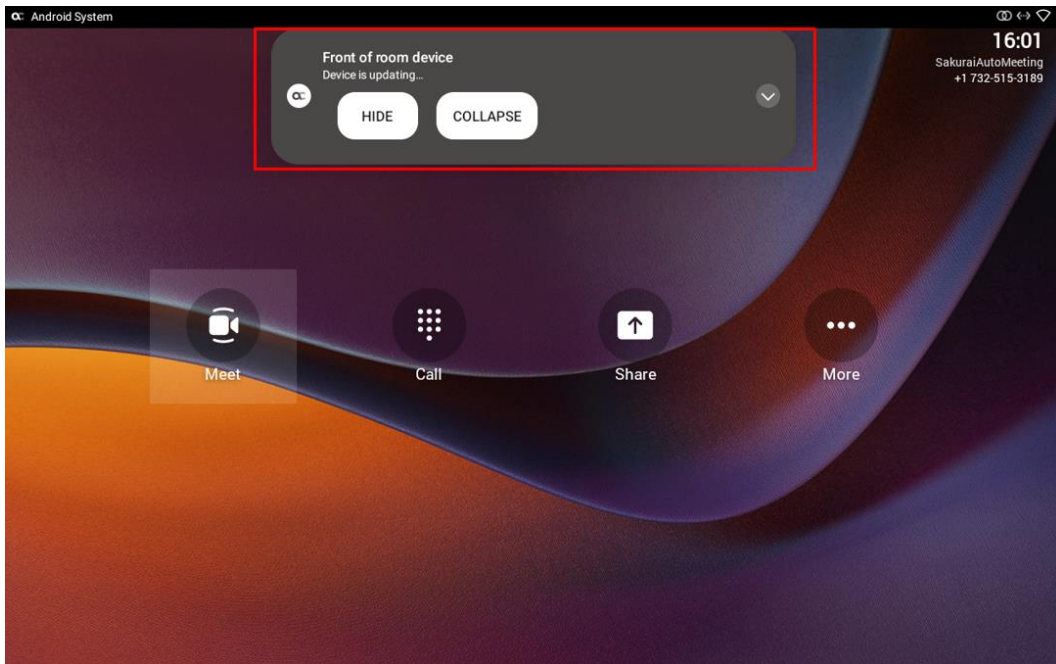
Popup messages displayed on the MTR device (RXV81 | RXV200) are seamlessly mirrored in the bundled RX-PAD to enhance user interaction.

When a message pops up in the MTR GUI, the same is displayed in RX-PAD.

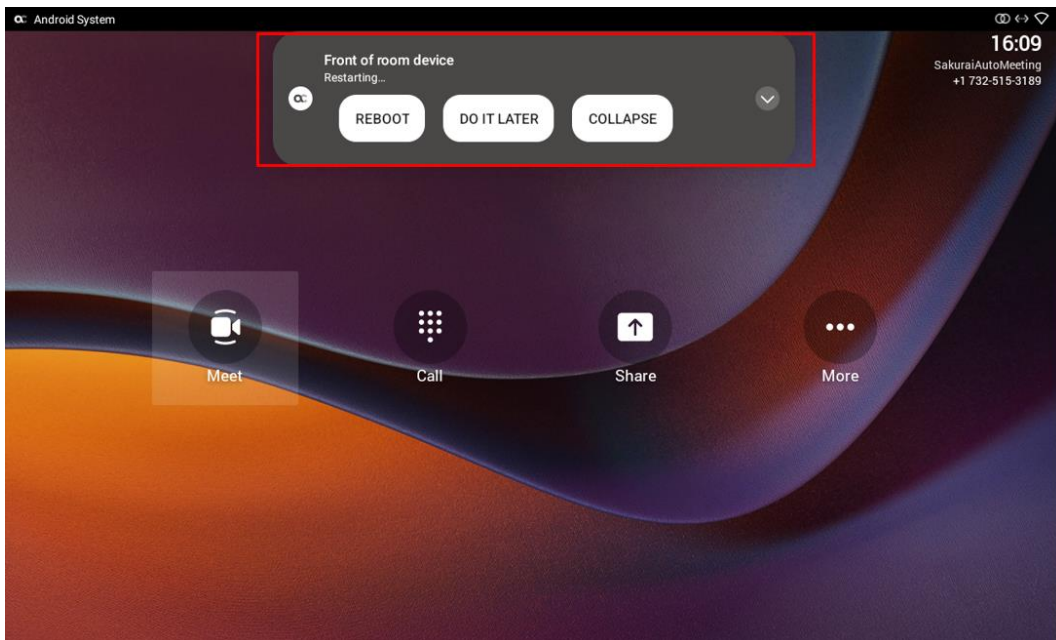
The feature streamlines user experience, allowing users to conveniently confirm messages directly from RX-PAD and manage notifications intuitively and efficiently.

The figure below shows the popup message **Device is updating** on RX-PAD.



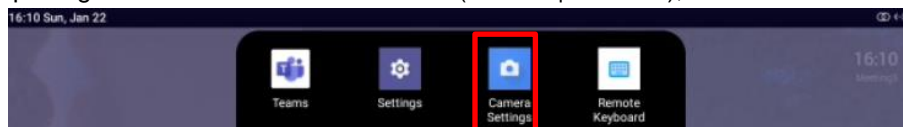


If the alert is an action, you can perform the action using RX-PAD, for example, REBOOT / DO IT LATER / COLLAPSE, as shown in the figure below.



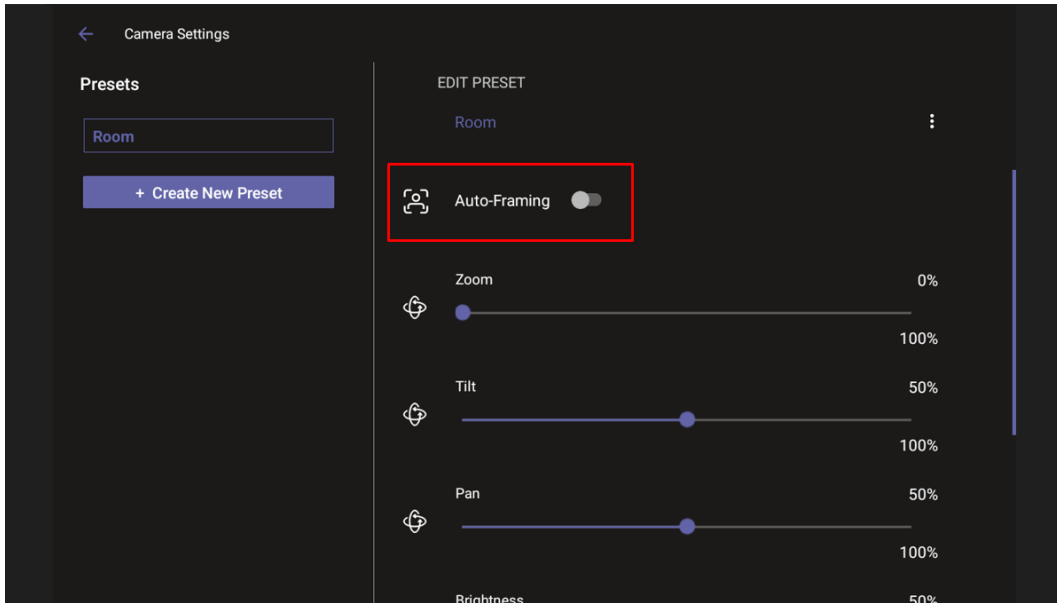
### 3.3 Adjusting MTR Camera Settings

After pairing RX-PAD with the MTR device (RXV81 | RXV200), scroll down in RX-PAD to this:



➤ **To adjust MTR camera settings:**

1. Tap the menu indicated in the figure above to enter the MTR's Camera Settings page -or- use the camera hard key to access the Camera Settings page.



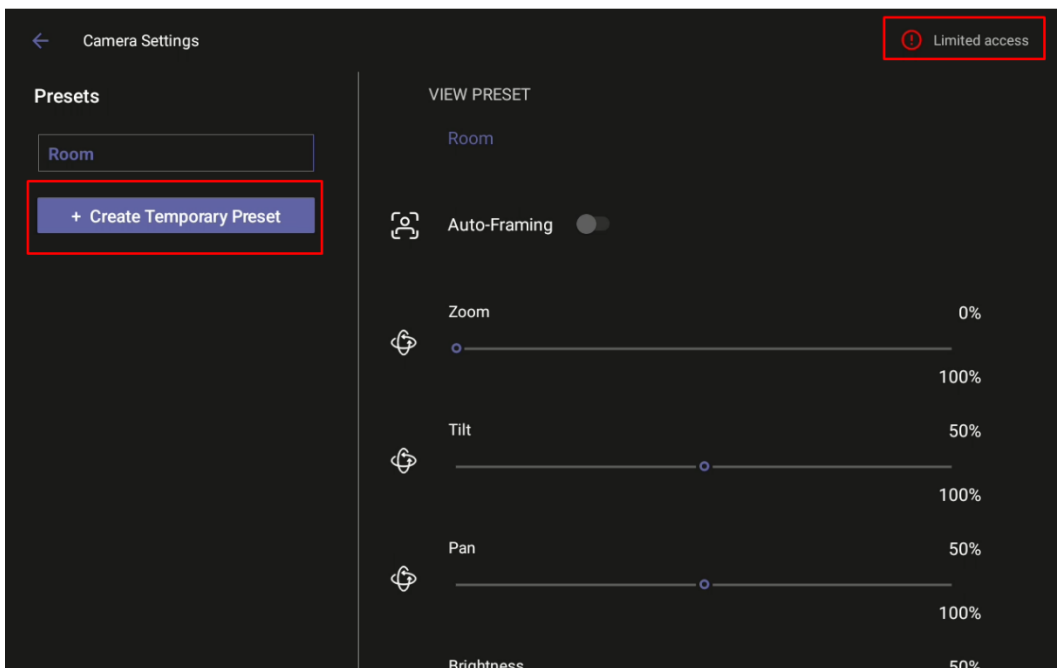
2. In the Camera Settings page shown in the figure above, view an Auto Framing switch available when RX-PAD is used to control RXV81 MTR. In addition to RXV81, the feature is also available on RXVCam50L/M connected to RXV200.

**Note:**



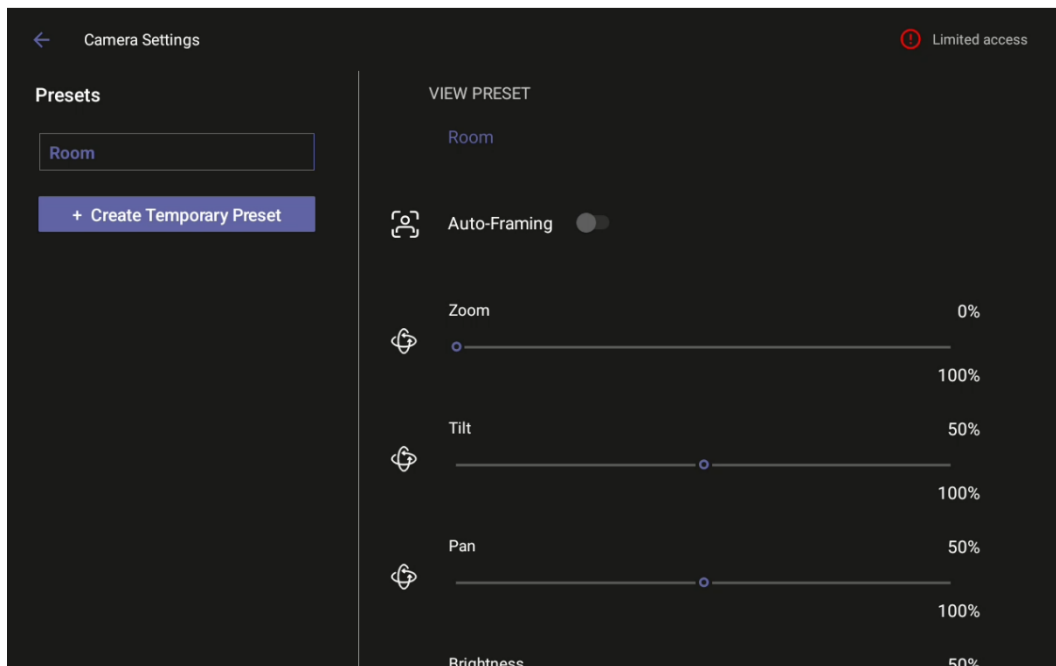
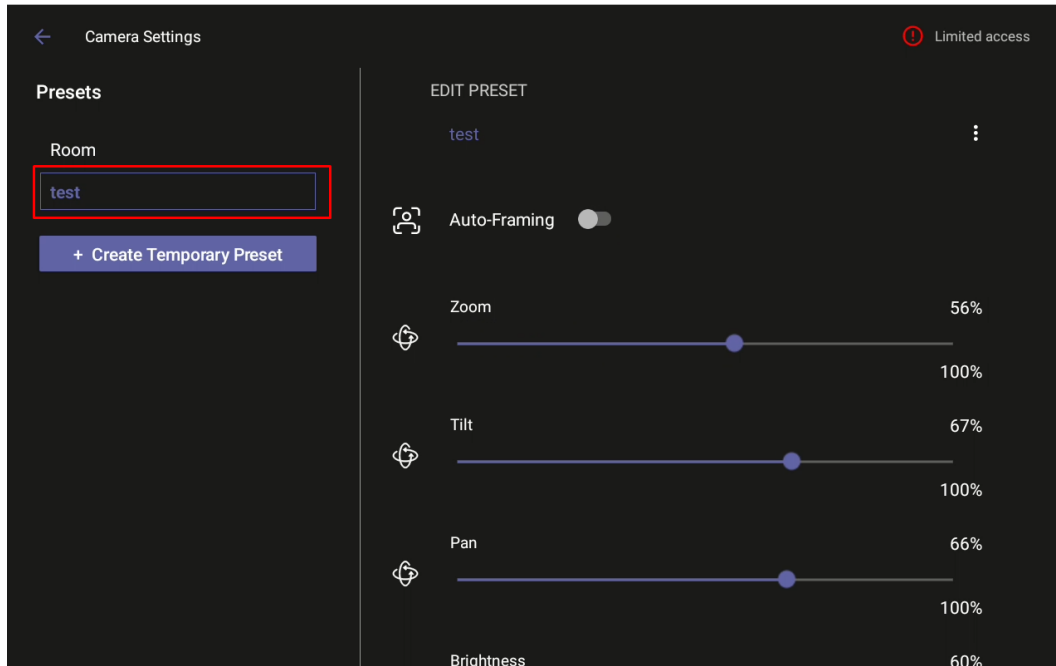
- Admin users can create a permanent camera settings preset including enable / disable of Auto Framing.
- End users can either select a preconfigured preset which includes enable / disable of Auto Framing or create a temporary preset *during a meeting* (which will be deleted at the end of the meeting) and can enable / disable Auto Framing.

3. Enable Auto Framing if required; PTZ (Pan Tilt Zoom) functions are then disabled; temporary presets are available for users without admin permissions; users without administrator permissions can create temporary presets.





**Note:** If that user leaves the meeting, the temporary presets will be erased when they later reenter Camera Settings (or another user later enters); temporary presets are only for that meeting they were configured for; new presets can be configured for the new meeting.

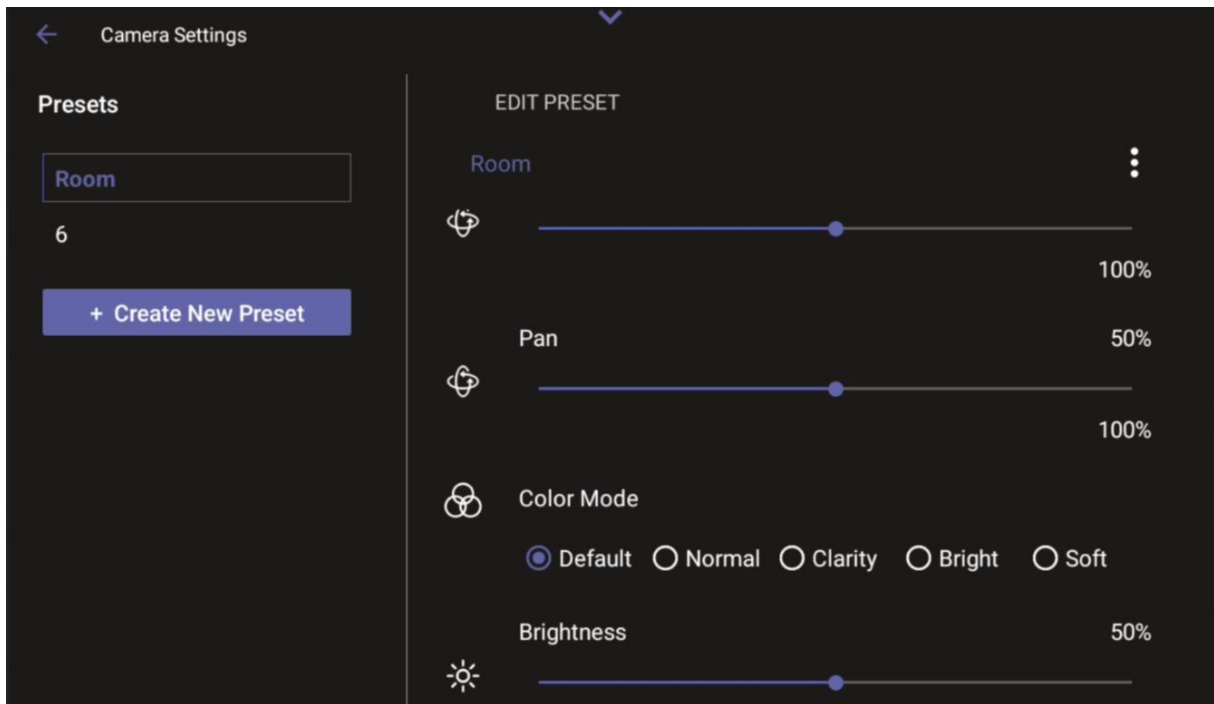


### 3.3.1 Configuring a Color Mode Preset on the RXVCAM50M/L Camera

Users can configure a Color Mode preset from RX-PAD when RXV200 is connected to the AudioCodes RXVCAM50M/L camera.

Users can configure either:

- Default
- Normal
- Clarity
- Bright
- Soft



Each Color Mode preset incorporates the following attributes:

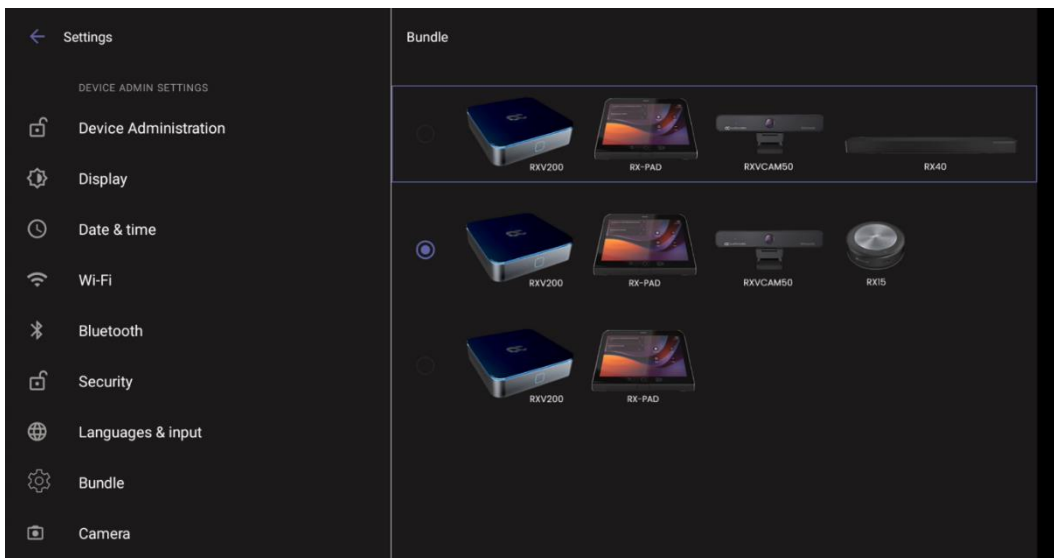
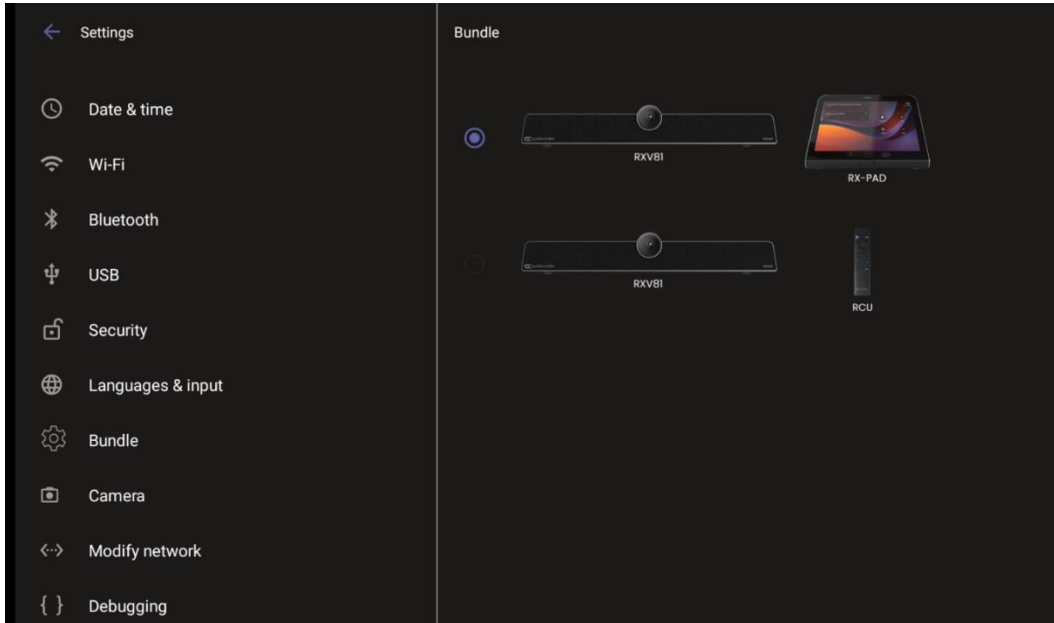
- **Default:** Brightness - 50, Contrast - 50, Saturation - 70
- **Normal:** Brightness - 50, Contrast - 50, Saturation - 70
- **Clarity:** Brightness - 60, Contrast - 50, Saturation - 60
- **Bright:** Brightness - 50, Contrast - 50, Saturation - 70
- **Soft:** Brightness - 50, Contrast - 50, Saturation - 60

### 3.4 Configuring a Bundle

Admins can configure an MTR bundle in the MTR device's GUI (RXV81 | RXV200).

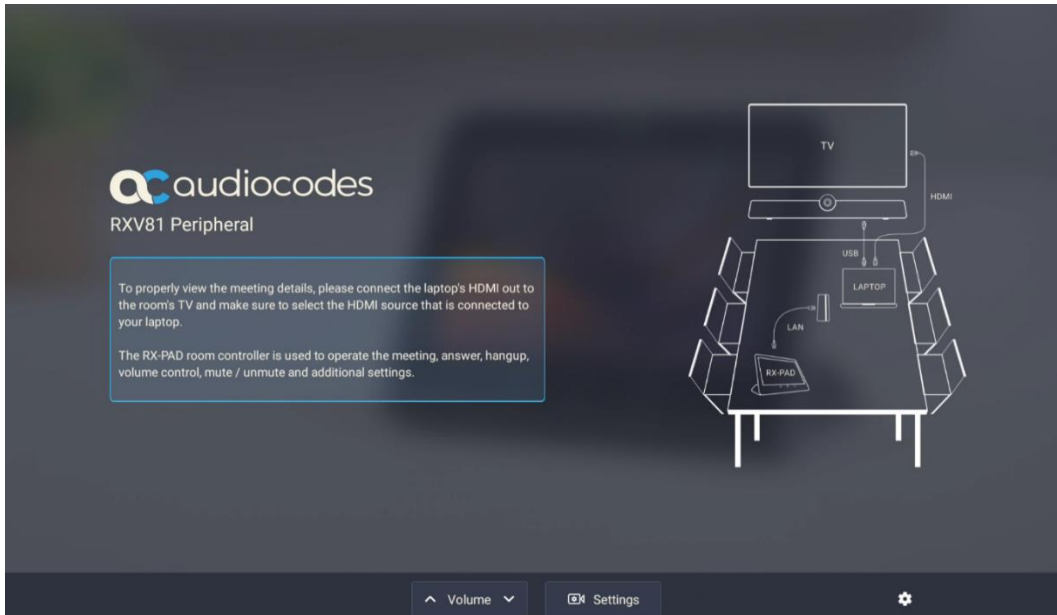
- Navigate to the Bundle setting using RX-PAD's Remote Keyboard that controls the MTR (see also the next section).
- You must be logged in to access the Bundle page.

The figures below respectively show the RXV81 and RXV200 Bundle pages.

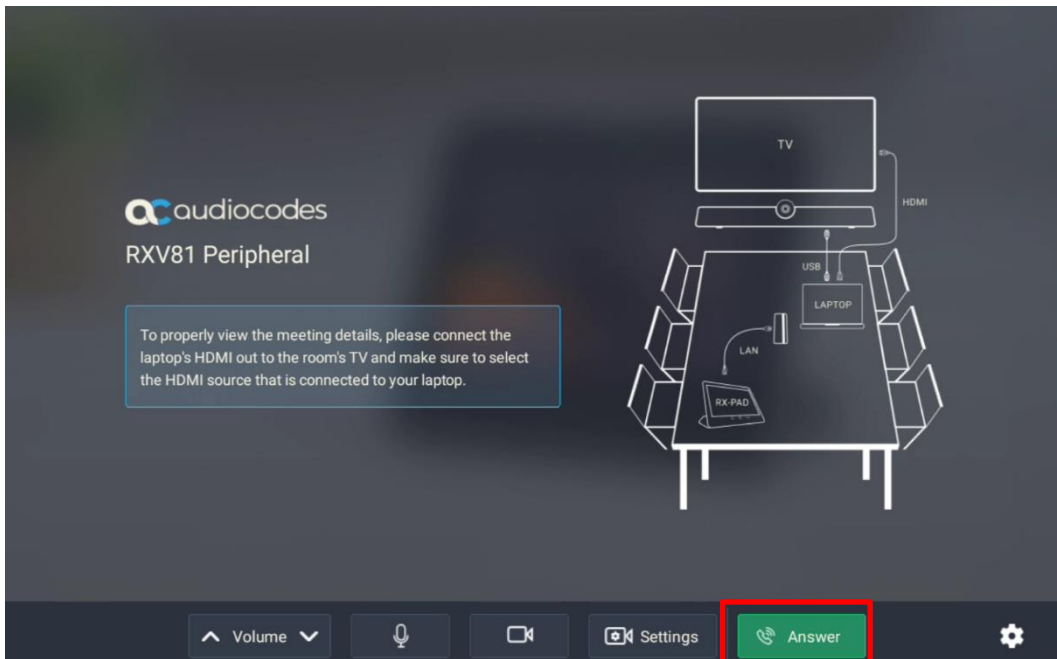


### 3.5 Configuring Ad Hoc Mode on RXV81 MTRA

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



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



## 3.6 Screen Sharing

RXV81 and/or RXV200 enable users to share their PC/laptop screen via the RX-PAD HDMI In port, to be shared on the screen in IDLE mode and peripheral mode.



**Note:**

- A short HDMI cable connects the PC/laptop to the RX-PAD HDMI In port.
- The connection between RX-PAD and RXV81 | RXV200 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 MTR positioned in the front of the room.

- **Teams Meeting Mode:** When the MTR is in a meeting, the presenter can use the Teams app 'Share' key to share their PC screen (when their PC is connected to RX-PAD's HDMI In port) with in-person attendees who are physically present in the same meeting room, as well as with remote attendees. [Audio sharing is currently unsupported].
- **Standby Mode:** When the MTR is not in a meeting, the presenter can use the Teams app 'Share' key to share their PC screen (when their PC is connected to RX-PAD's HDMI In port) only with in-person attendees who are physically present in the same meeting room.

The figure below shows RXV200 connected.



The figure below shows the RXV81 connections.



To enable utilization of this feature, make sure the following is permitted in the organization's firewall settings:

- Hostname: `jitsi-meet-ipp.eastus.cloudapp.azure.com`
- IP Address: `20.115.49.175`
- Allow incoming connections on the following ports:
  - `80/tcp`
  - `443/tcp`
  - `3478/udp`
  - `5349/tcp`
  - `10000/udp`

See also:

- RXV81 MTRA User's and Administrator's Manual
- RXV200 MTRA Compute User's and Administrator's Manual

This page is intentionally left blank.



## 4 Configuring User Settings

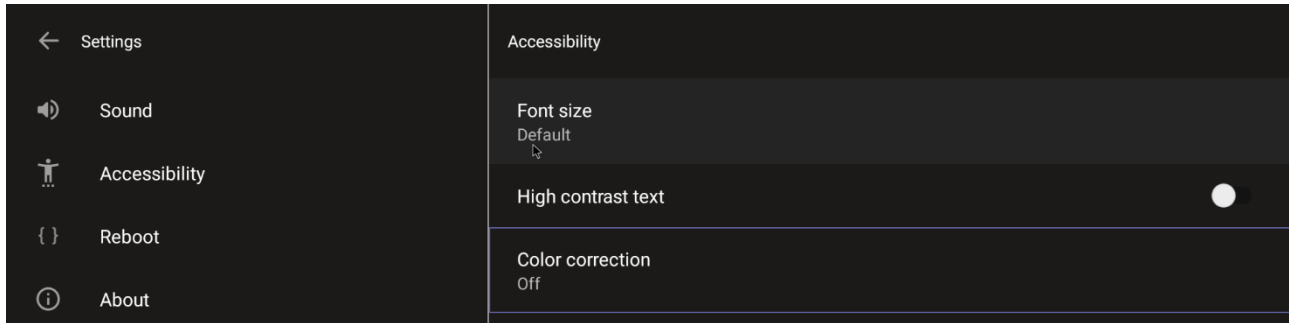
In the 'Settings' screen you can optionally configure the following User settings: Sound, Accessibility, Reboot and About (read-only).

### 4.1 Accessibility

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

➤ **To configure the Accessibility setting:**

1. Under 'User', navigate to and select **Accessibility**.



2. Adjust the settings to suit personal requirements.

### 4.2 Setting Live Captions

Live Captions can be set in regular one-on-one calls as well as in Teams meetings.

### 4.3 Hiding Names and Meeting Titles

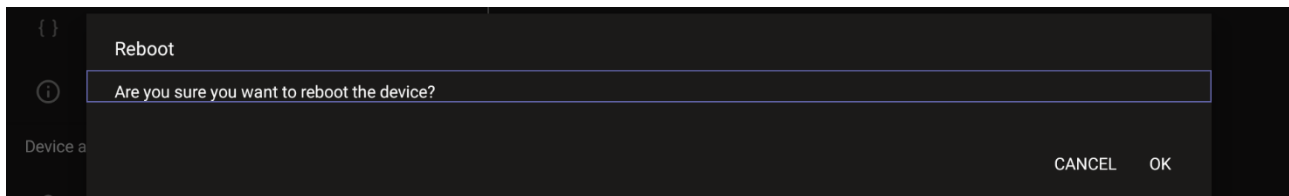
Users can hide information such as names and meeting titles for individual devices via the Meetings page (**More > Settings > Meetings**).

### 4.4 Reboot

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

➤ **To reboot:**

- Under 'User', navigate to and select **Reboot**.

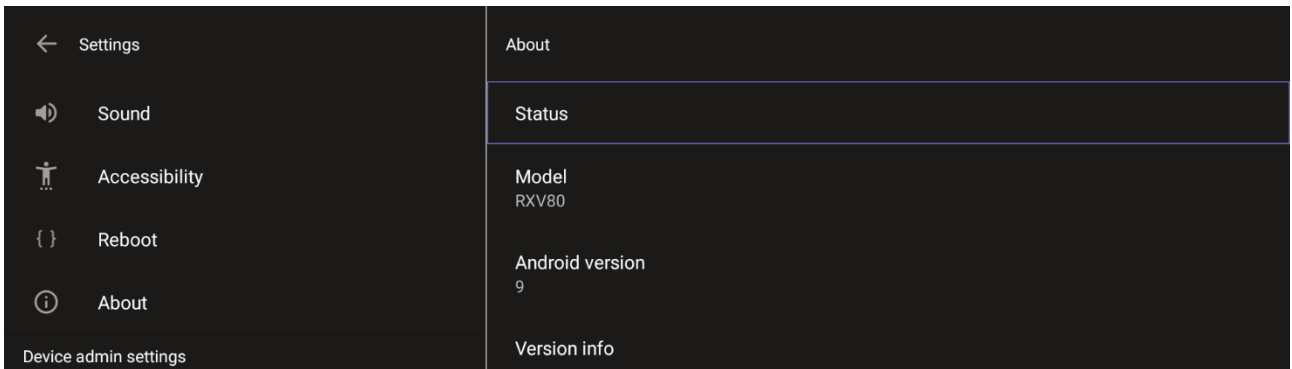


### 4.5 About

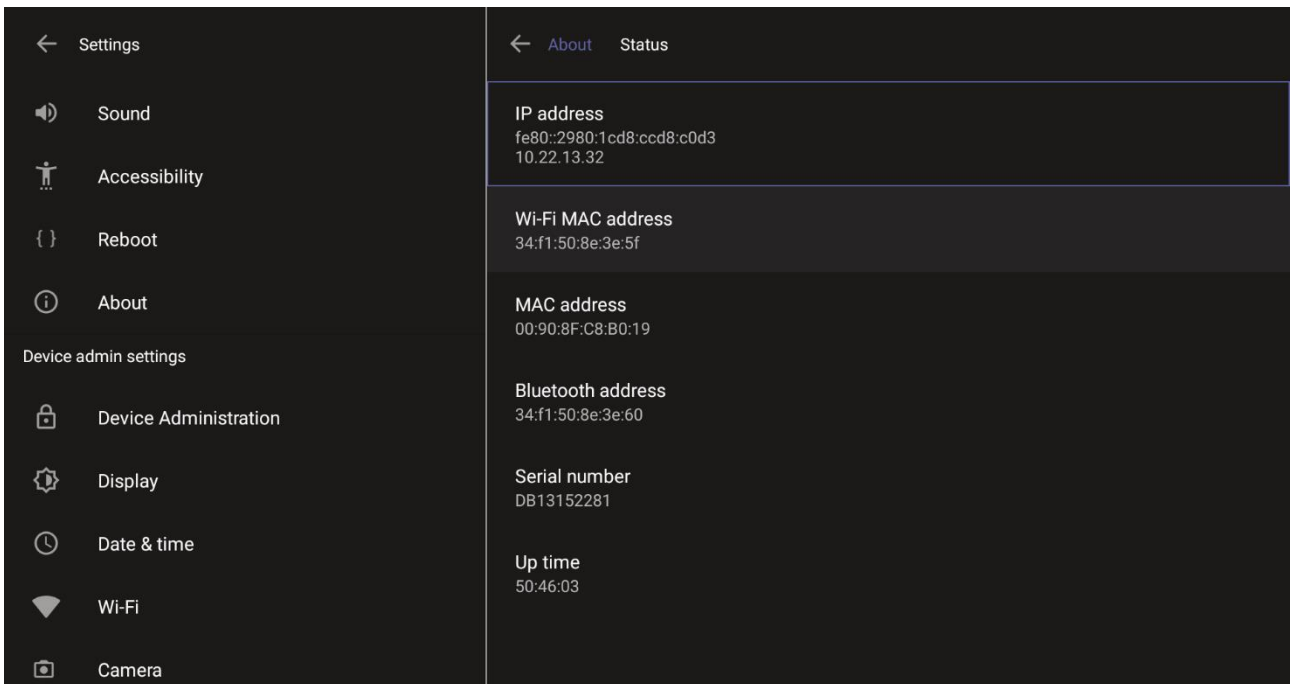
The 'About' screen gives you quick access to information about the deployment.

➤ **To access the About screen:**

1. Under 'User', navigate to and select **About**.



2. Navigate to and select **Status**.



3. View the firmware information.

## 5 Enrolling a Device with Intune Policies

Two ways are available to enroll an AudioCodes Teams Android-based device in Intune:

- Create a dynamic group - see [here](#)
- Create an exclusion group - see [here](#)

### 5.1 Creating a Dynamic Group

See [here](#) how to create dynamic groups in Intune for enrolling AudioCodes Android-based Teams devices.

### 5.2 Creating 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 previous configured:
  - 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 figure below.
  - Exclude the device from Intune policies and replace **displayName -contains RX-PAD** where **RX-PAD** is the name of the device model (**device.model**).

The screenshot shows the Microsoft Intune admin center interface. The main content area is titled "Filter for devices" and is used to configure a filter to apply policy to specific devices. The "Configure" toggle is set to "Yes". Below this, there are two radio buttons: "Include filtered devices in policy" (unselected) and "Exclude filtered devices from policy" (selected). A table below shows the filter rules:

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

Below the table, there is a "Rule syntax" text box containing the following expression:

```
device.displayName -eq 'RXV81' -and device.displayName -eq 'RXV200'
```

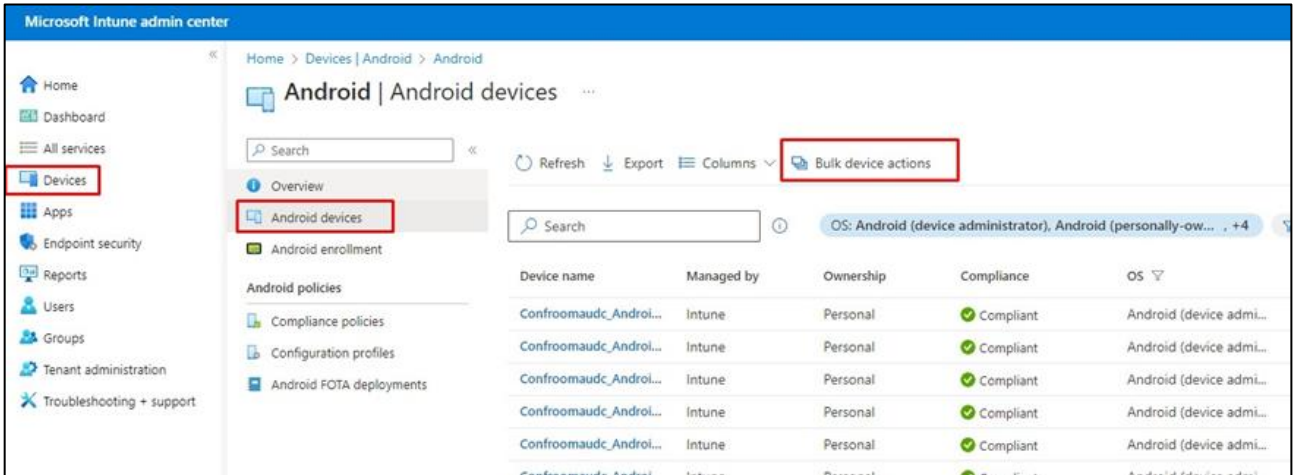
The "Done" button is located at the bottom right of the configuration window.

### 5.3 Removing 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**.



**Note:** 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**.

Home > Devices | Android > Android | Android devices >

## Bulk device action ...

1 Basics 2 Devices 3 Review + create

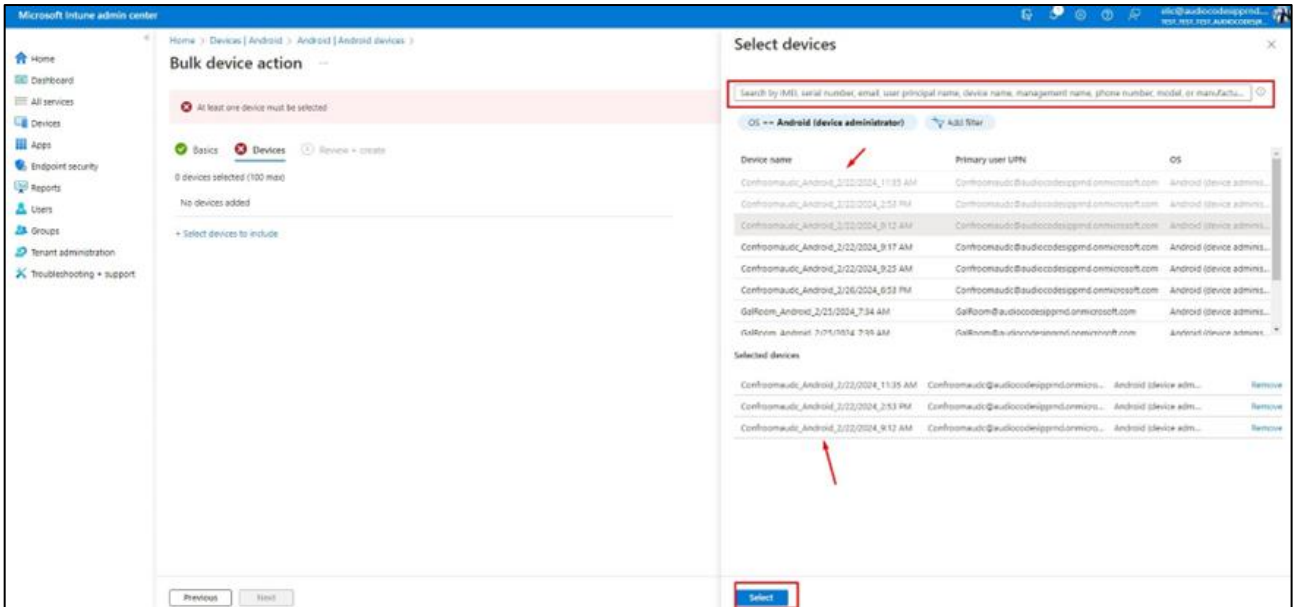
OS \* → Android (device administrator) ▾

Device action \* → Delete ▾

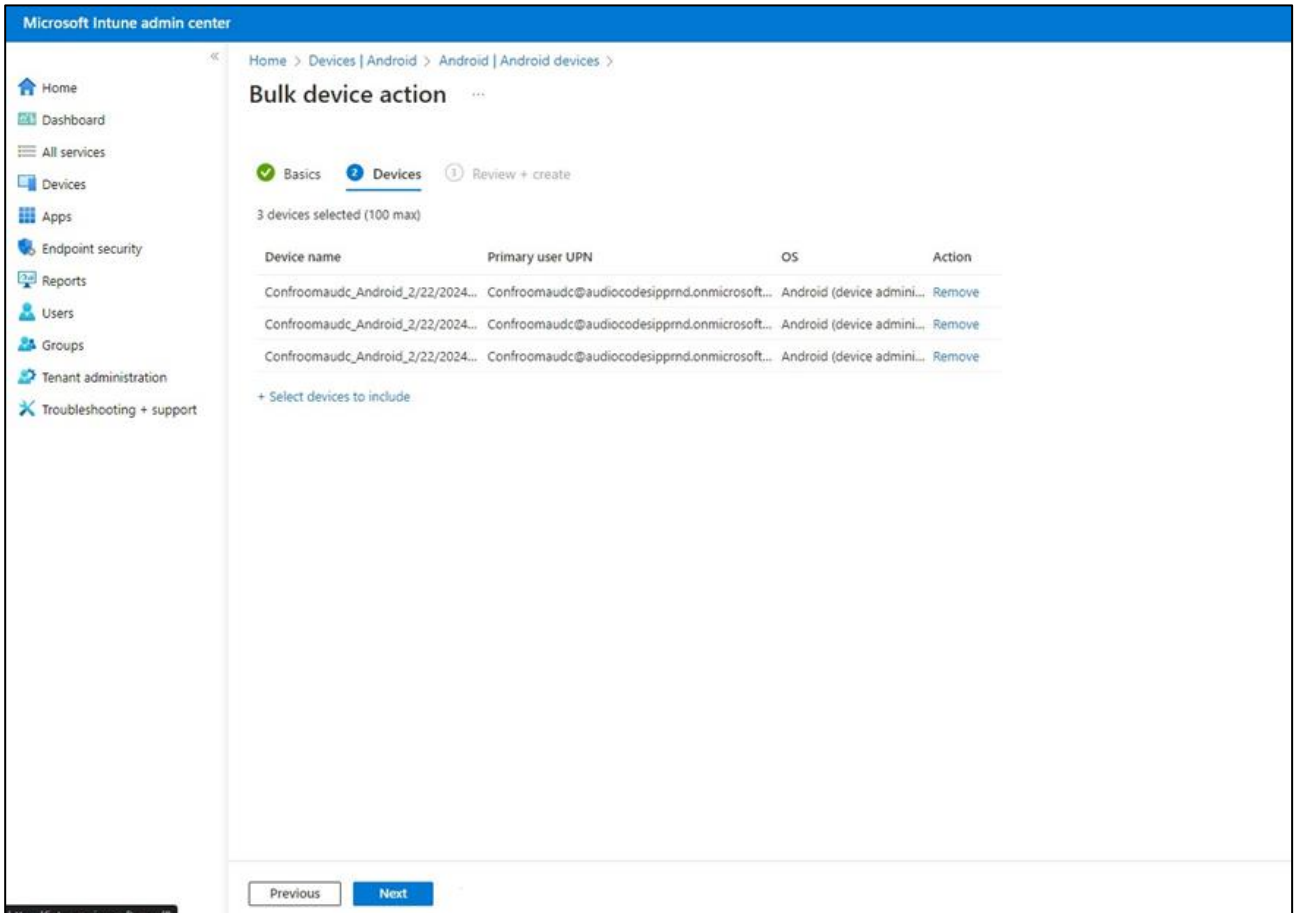
**i** If you delete this device, you will no longer be able to view or manage the device from the Intune portal. The device will no longer be allowed to access your company's corporate resources. Company data may be wiped from the device if the device tries to check-in after it is deleted.

Previous Next

- 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**.



- Under the **Devices** tab, click **Next**.

Microsoft Intune admin center

Home > Devices | Android > Android | Android devices >

### Bulk device action

Basics Devices **Review + create**

Summary

Basics

Device action Delete  
OS Android (device administrator)

Devices

3 devices selected (100 max)

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

Previous Create

- Under the **Review + Create** tab, make sure your definitions are correct and then click **Create**; admin receives a notification that a delete action from Intune was successfully initiated on all devices and that *n* devices were removed.



**Note:** It may take some time to completely sync the devices with the account so after deleting the devices wait for 30 minutes before signing in.



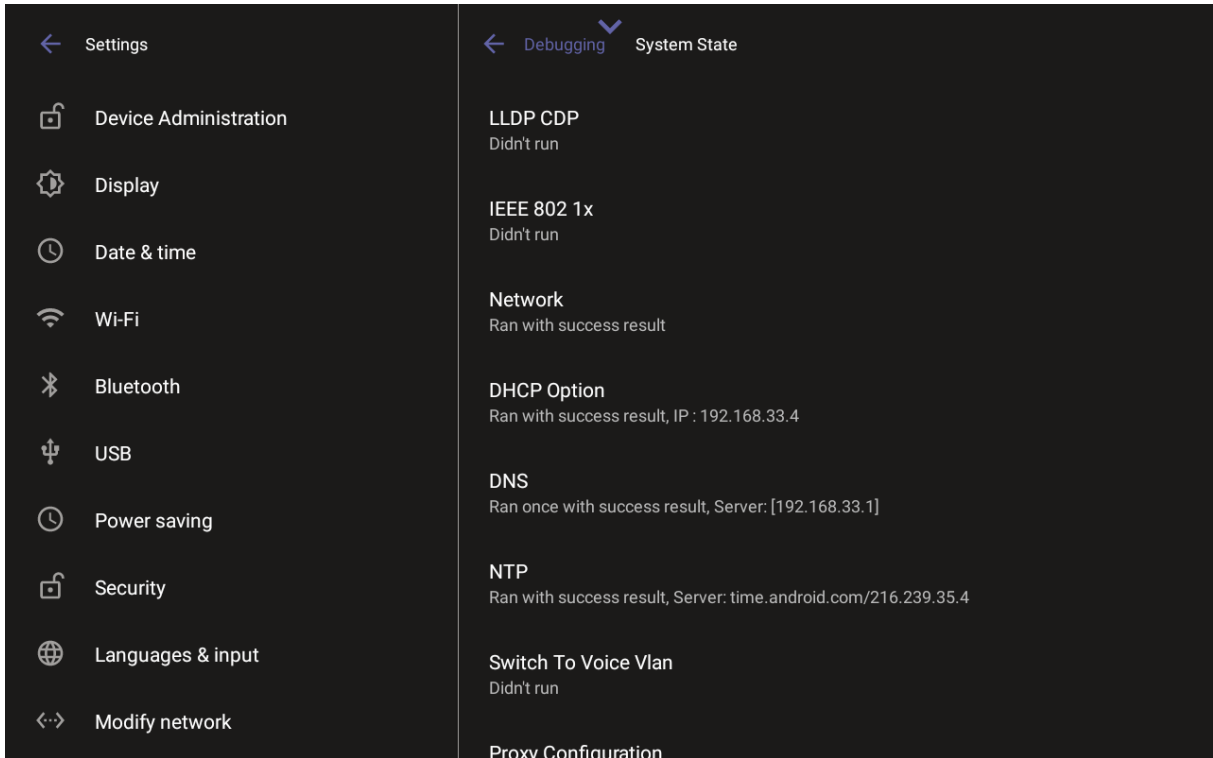
# 6 Monitoring Device Software Modules Status

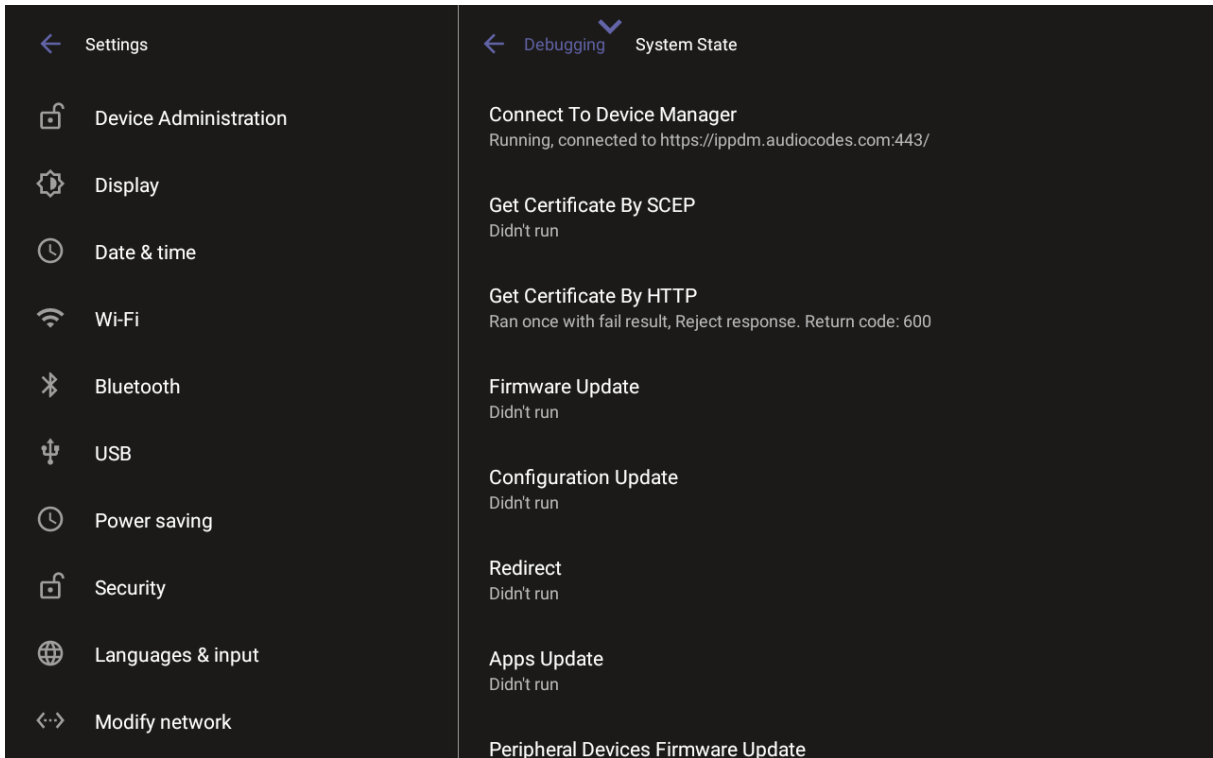
AudioCodes provides out-of-the-box troubleshooting capability: Admins can monitor the status of the device's various software modules from the System State page. If initial provisioning is unsuccessful or if admin encounters an issue related to the network / connection to Device Manager, the feature gives admin an indication as to why.

The feature enables debugging via the device's screen *without requiring external systems*. Admin can check connectivity *independently of external apps*.

➤ **To monitor the device's software modules status:**

- Open the System State page (**Settings > Debugging > System State**).



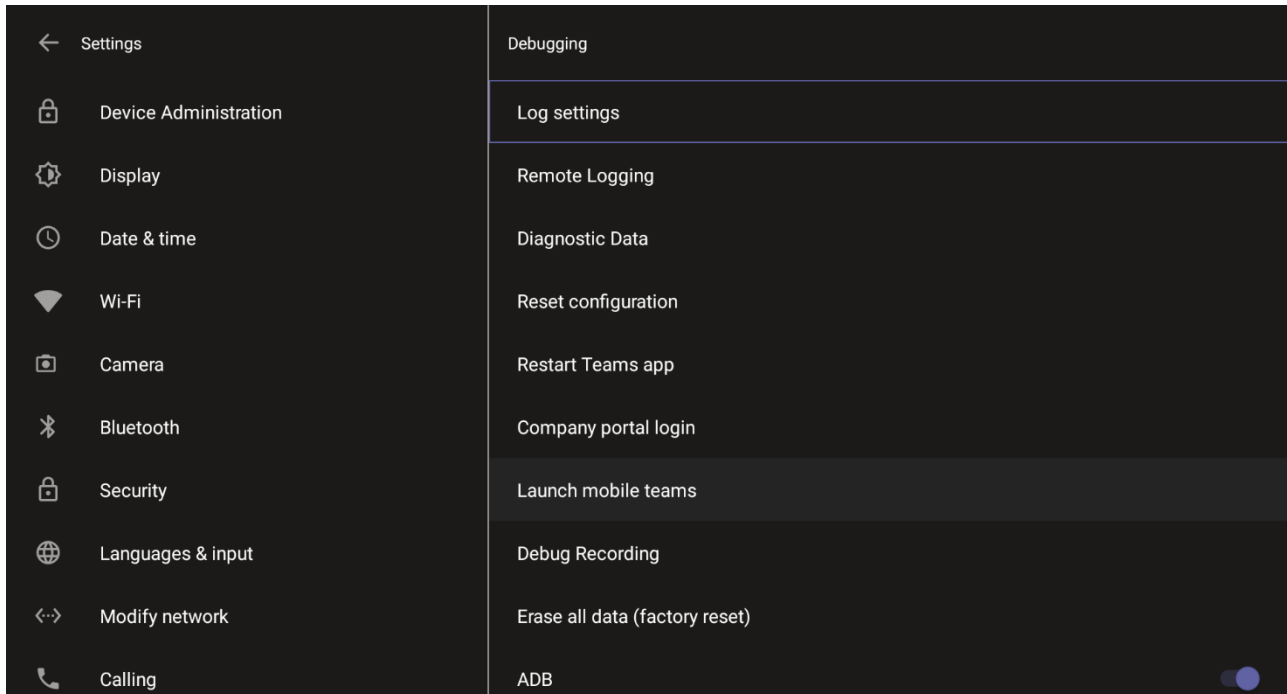


## 7 Debugging

Admin users can perform debugging for troubleshooting purposes.

➤ **To perform Debugging:**

1. In the Settings screen under 'Device administration', select **Debugging**.



2. Use the following debugging features available to Admin users:

- Log settings (see [Log Settings](#))
- Remote Logging (see under [Remote Logging](#))
- Diagnostic Data (see under [Diagnostic Data](#))
- Reset configuration (see under [Reset configuration](#))
- Restart Teams app (see under [Restart Teams app](#))
- Company portal login (see under [Company Portal Login](#))
- Launch mobile teams (see under [Launch Mobile Teams](#))
- Debug Recording (see under [Debug Recording](#))
- Erase all data (see under [Erase all data \(factory reset\)](#))
- Screen Capture (see under [Screen Capture](#))
- Performing Recovery Operations (see under [Performing Recovery Operations](#))
- Restoring Device Firmware via USB Disk (see under [Restoring Device Firmware via USB Disk](#))



**Note:**

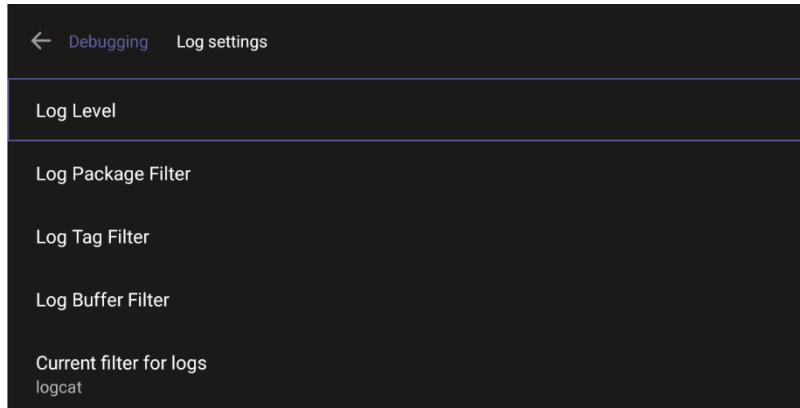
- An enhanced bug report is available for efficient debugging.
- Information such as pack up time, ps, top, meminfo and df commands (information about file system disk space usage) is reflected in it.

## 7.1 Log Settings | 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 also for issues related to the device.

➤ **To configure log settings:**

1. In the Debugging screen, select **Log settings**.



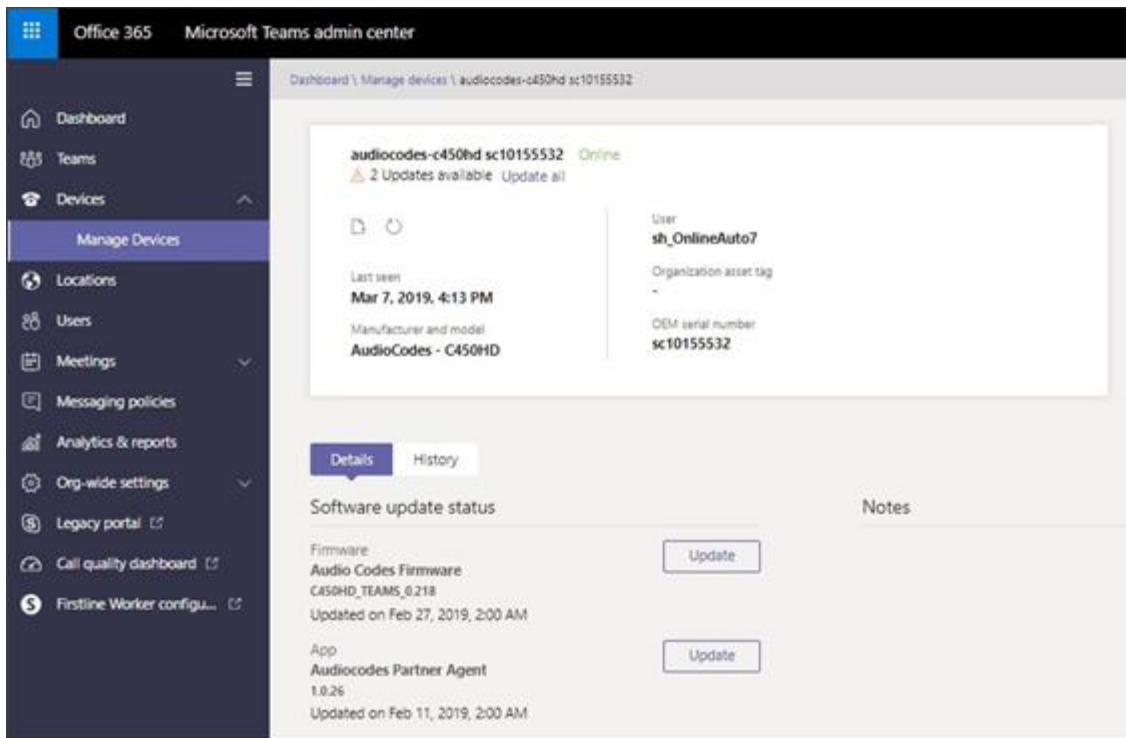
2. Navigate to and select **Log Level** and then select either
  - Verbose, Debug, Info, Warning, Error, Assert -or-None
3. Navigate to and select **Log Package Filter** and enter the filter.
4. Navigate to and select **Log Tag Filter** and enter the filter.
5. Navigate to and select **Log Buffer Filter**.



6. Navigate to and select **Current filter for logs**.

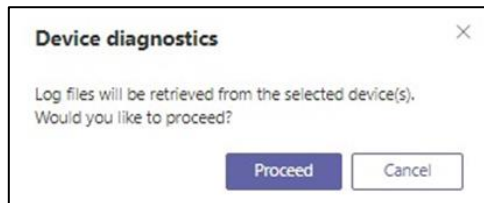
➤ **To collect logs:**

1. Reproduce the issue
2. Access Microsoft Admin Portal and under the **Devices** tab click the **Diagnostics** icon.

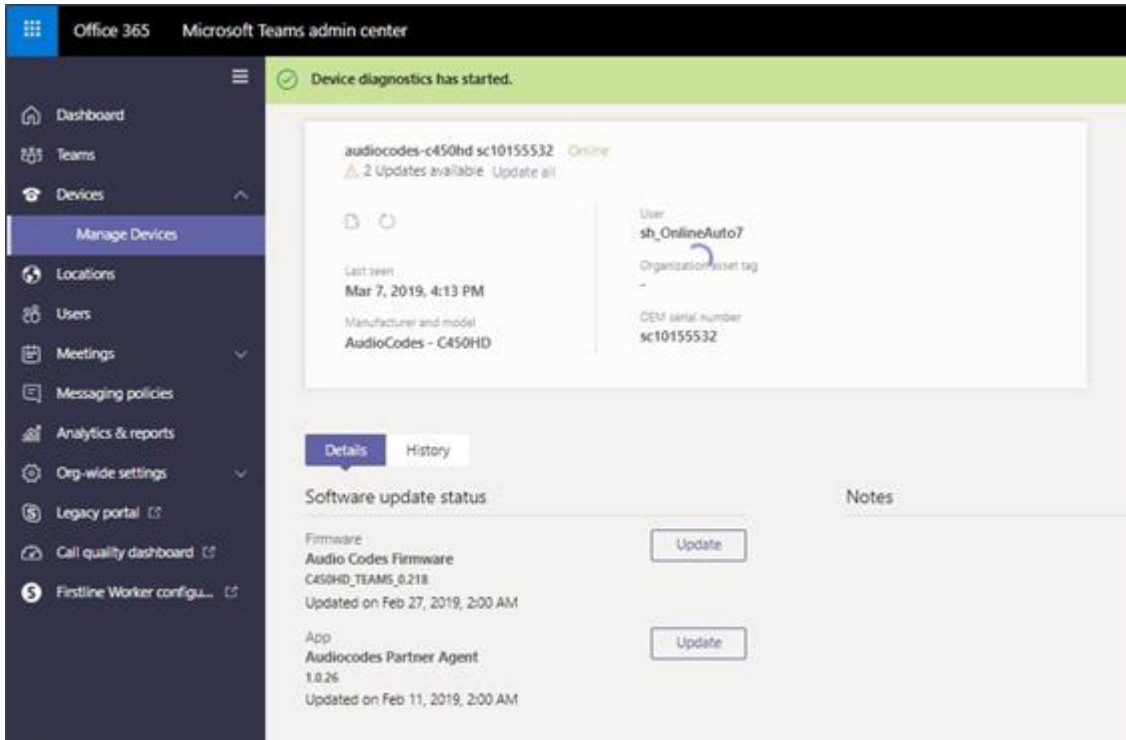


**Note:** The preceding figure is for illustrative purposes. It shows an AudioCodes phone. The same screen is displayed for the MTR.

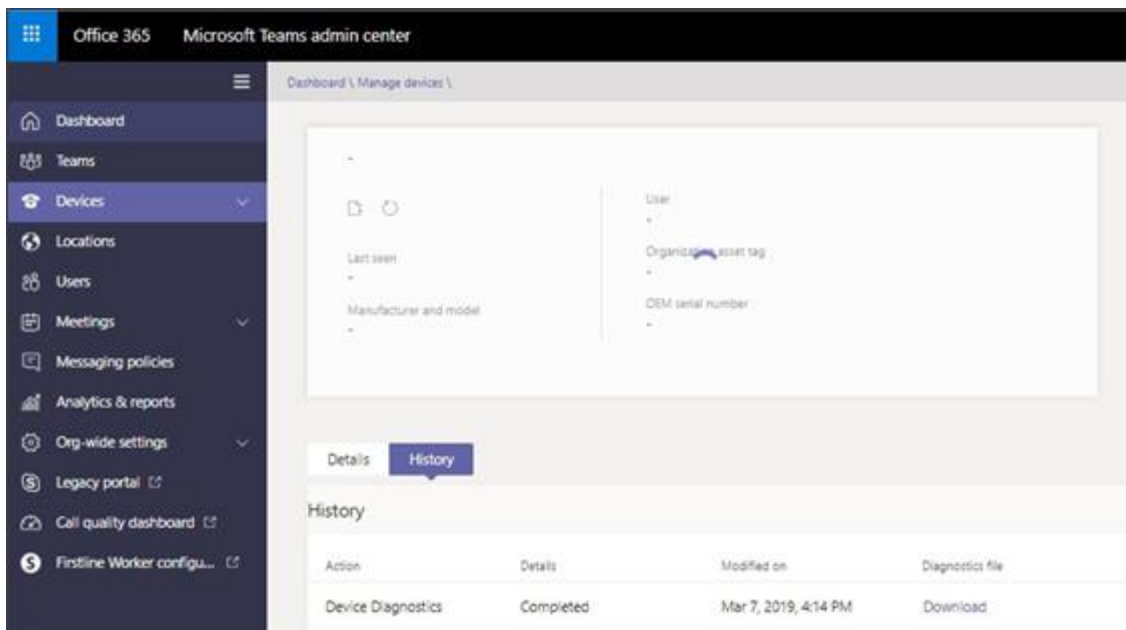
3. Click the **Diagnostics** icon.



- Click **Proceed**; the logs are uploaded to the server.



- Click the **History** tab.



- Click **Download** to download the logs.

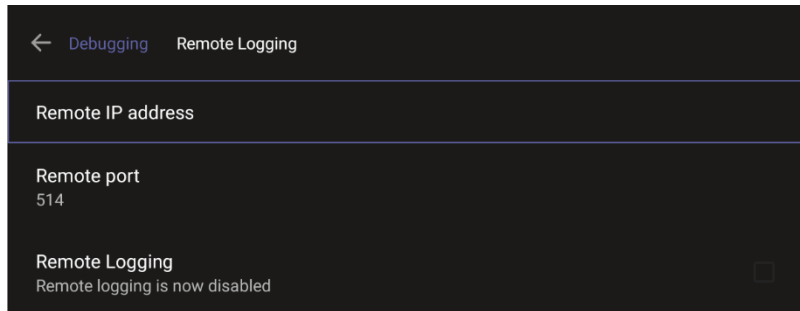
## 7.2 Remote Logging

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 sdcard and collected after the event. Remote Logging via Syslog is different. The logs are collected in real time.

➤ **To enable Remote Logging via Syslog:**

1. Navigate to and select **Remote logging**.



2. Configure the 'Remote IP address' and 'Remote port' and enable 'Remote Logging'; the device starts sending logs to the Syslog server.



**Note:** Network administrators can also enable Syslog using Secure Shell (SSH) protocol.

➤ **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:**

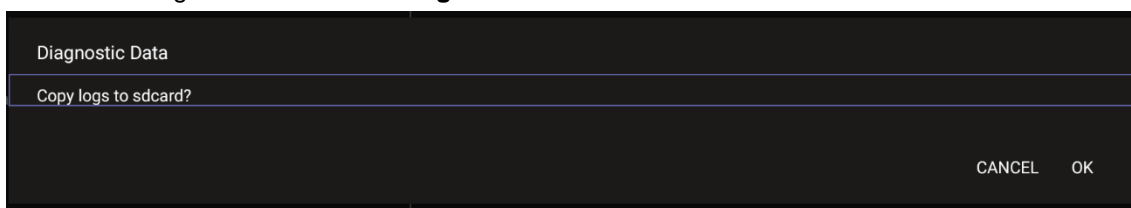
```
setprop persist.ac.rl_address ""
```

## 7.3 Diagnostic Data

Admin users who need to get logs from the device can dump the logs to the device'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. Navigate to and select **Diagnostic Data**.



2. Navigate to and select **OK** to confirm 'Copy logs to sdcard'; the MTR creates all necessary logs and copies them to the its SD Card / Logs folder.
3. 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):

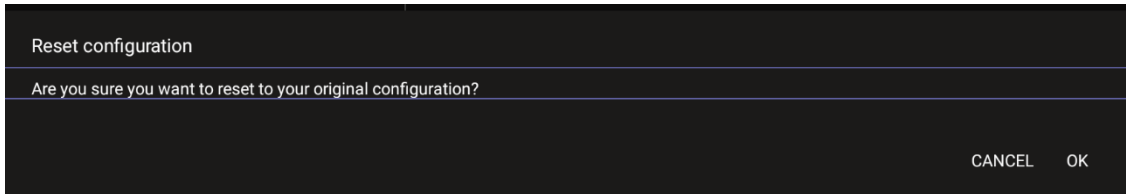
- dmesg.log
- dumpstate-TEAMS\_1.3.16-undated.txt
- dumpstate\_log-undated-2569.txt
- logcat.log

## 7.4 Reset configuration

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

➤ **To reset the configuration:**

1. Navigate to and select **Reset configuration**.



2. Navigate to and select **OK**; all data is erased and default factory settings are restored but sign-in is retained.

See also [here](#).

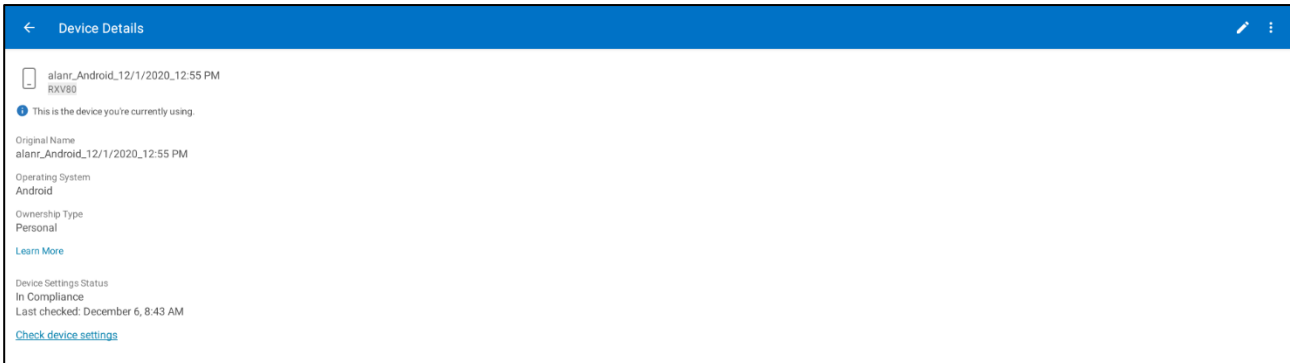
## 7.5 Restart Teams app

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

➤ **To restart the Teams app:**

- Navigate to and select **Restart Teams app**; only the Teams app is restarted.

## 7.6 Company Portal Login



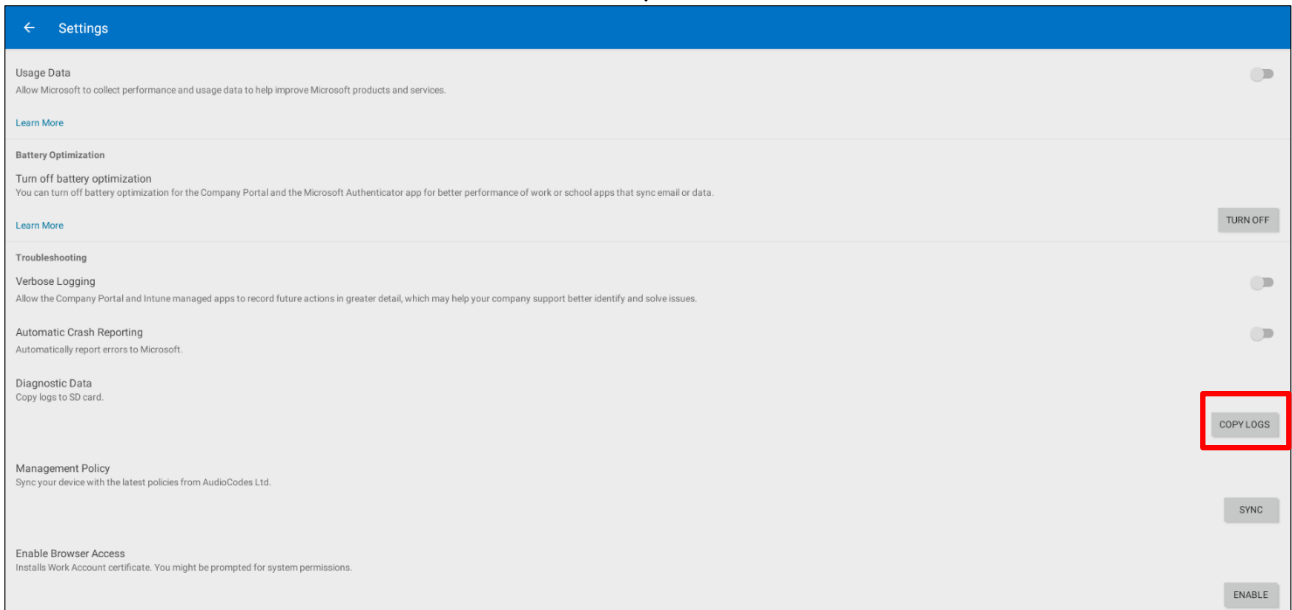
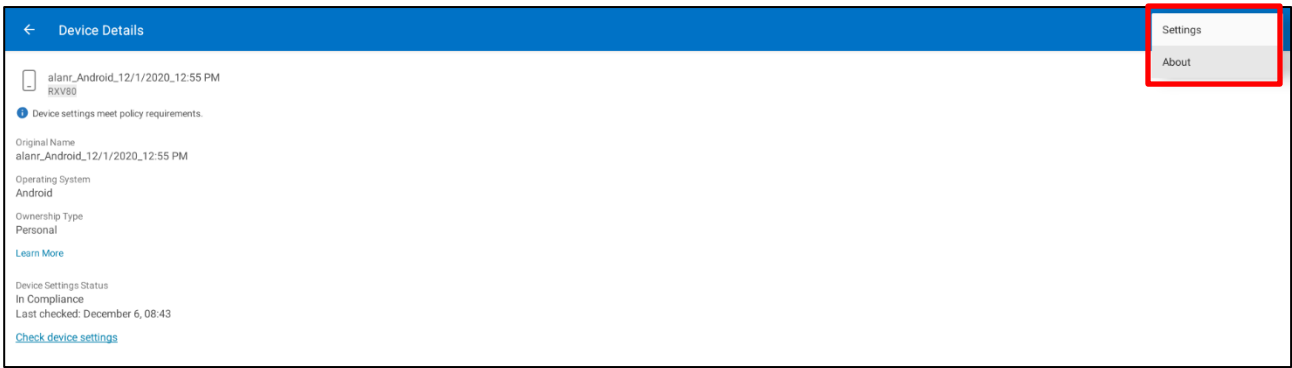
## 7.7 Getting Company Portal Logs

Company Portal logs can be helpful to network administrators when there are issues with signing in to Teams from the device.

➤ **To get Company Portal logs:**

1. Reproduce the issue (logs are saved to the device so you first need to reproduce the issue and then get the logs).
2. Log in to the device as Administrator and then go back.
3. Navigate to and select the **Debugging** option.
4. Navigate to and select **Company Portal login**.
5. In the Device Details screen that opens, navigate to and select **Settings**:





**6. Navigate to and select Copy Logs.**

Company portal logs are copied to:

```
sdcard/Android/data/com.microsoft.windowsintune.companyportal/files/
```

**7. To pull the logs, use ssh:**

```
scp -r admin@hosp_ip:/sdcard/android/data/com.microsoft.windowsintune.companyportal/files/
```

Files are quite heavy so you may need to pull them one by one.

## 7.8 Launch Mobile Teams

'App not found'. N/A in this release.

## 7.9 Debug Recording

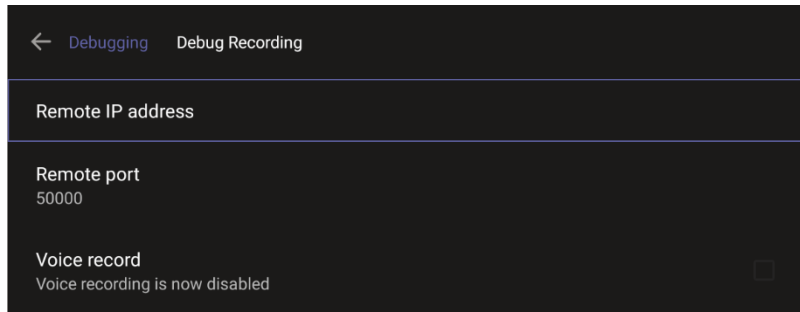
This feature enables Admin users to perform media/DSP debugging.



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

➤ **To reset the configuration:**

- 1. Navigate to and select Debug Recording.**



2. Navigate to and select **Voice record** to enable the feature.
3. Navigate to and select **Remote IP address** to input the IP address of the device whose traffic you want to record.
4. Navigate to and select **Remote port** and input it (Default: 5000).
5. Start Wireshark on your PC to capture audio traffic.

## 7.10 Restoring to Defaults

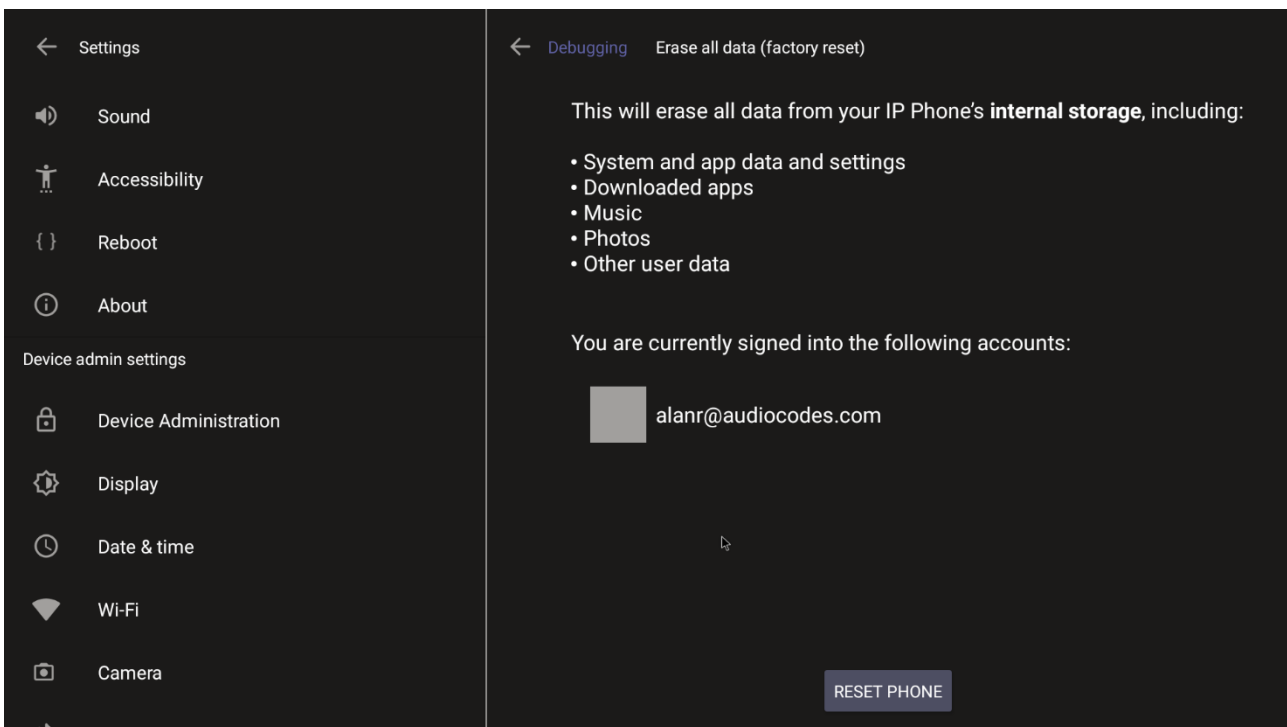
RX-PAD can be restored to defaults by pressing 15 seconds on the bottom key (dedicated button on RX-PAD).

## 7.11 Erase all data (factory reset)

This option is the equivalent of restoring to defaults shown in the preceding section; including logout and device reboot.

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

1. Navigate to and select Erase all data (factory reset).



2. Navigate to and select **RESET PHONE**.

## 7.12 Screen Capture

By default, this setting is enabled. If disabled, the device won't allow its screens to be captured.

## 7.13 Performing Recovery Operations

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



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



**Note:**

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

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

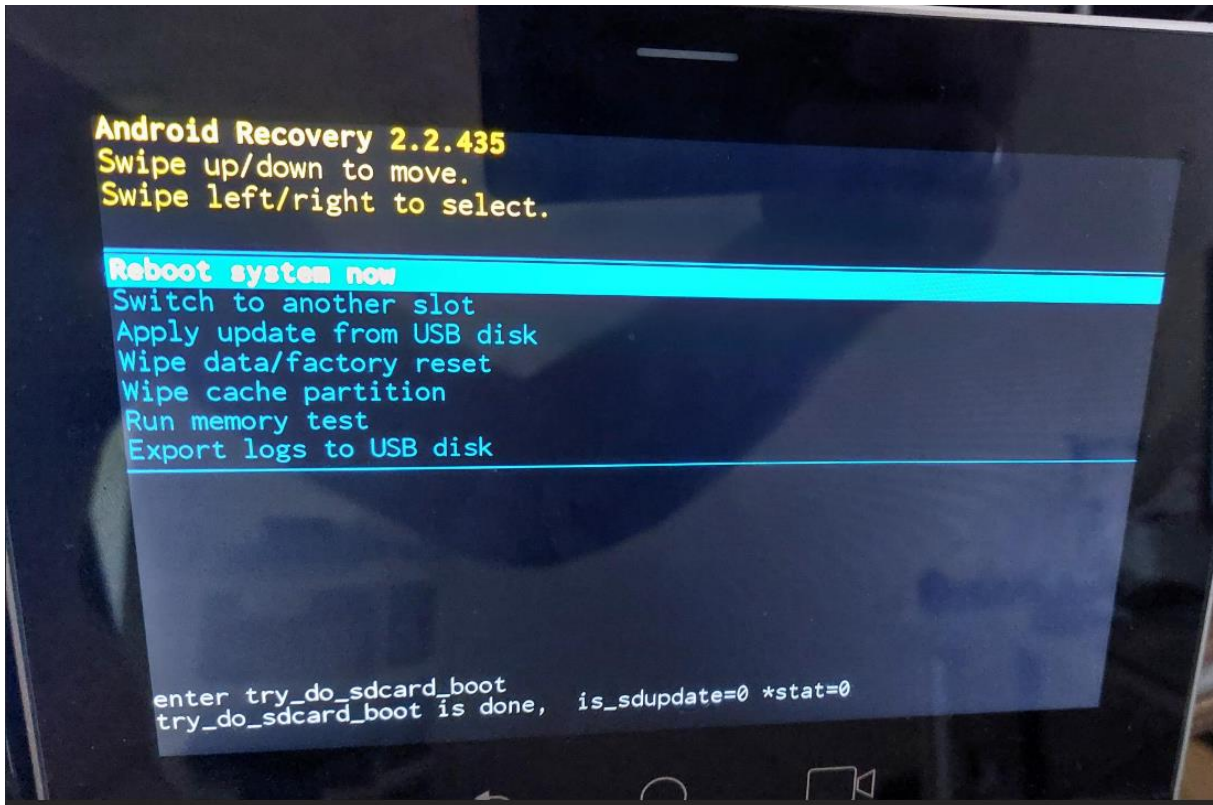
When?	Action	Press for how long?	LED flashes 3x after release
Start pressing immediately after power up (on U-Boot / Universal Boot Loader)	Recovery mode (you can restore defaults from there)	~ 4 seconds	Red
	Switch slots A / B	~ 10 seconds	Green
	Loader	~ 15 seconds	Blue / Yellow
	Restore defaults	~25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

## 7.14 Restoring Device Firmware via USB Disk

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

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

1. Enter recovery mode by pressing for 2-4 seconds the power button as shown in the preceding table (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.

## 8 Saving Logs while 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.

This page is intentionally left blank.

## 9 Updating Microsoft Teams Devices Remotely

For instructions on how to update Microsoft Teams devices remotely, see [here](#).



**Note:** 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.

This page is intentionally left blank.



### **International Headquarters**

Naimi Park  
6 Ofra Haza Street  
Or Yehuda, 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/>

©2024 AudioCodes Ltd. All rights reserved. AudioCodes, AC, HD VoIP, HD VoIP Sounds Better, IPmedia, Mediant, MediaPack, What's Inside Matters, OSN, SmartTAP, User Management Pack, VMAS, VoIPerfect, VoIPerfectHD, Your Gateway To VoIP, 3GX, VocaNom, AudioCodes One Voice, AudioCodes Meeting Insights, AudioCodes Room Experience are trademarks or registered trademarks of AudioCodes Limited. All other products or trademarks are property of their respective owners. Product specifications are subject to change without notice.

Document #: LTRT-18323

