Room Experience (RX) Suite

AudioCodes RX-PAD Meeting Room Controller

Version 2.4





Table of Contents

1	Intro	troduction		
	1.1	Highlights	. 7	
	1.2	Specifications		
	1.3	Connectivity		
	1.4	Managing RX-PAD		
	1.4			
		Audio Notifications via MTRA Speakers		
	1.6			
		1.6.1 Microsoft Teams Security Guidelines1.6.2 Android Level Security Hardening		
		1.6.2.1 Google Play Services		
		1.6.2.2 Running Android in Kiosk Mode	9	
		1.6.2.3 Screen Lock.		
		1.6.2.4AudioCodes Private Key1.6.2.5Android Debug Bridge (ADB)		
		1.6.2.6 App Signing		
		1.6.2.7 Web Browser	10	
		1.6.2.8 Remote Configuration Management		
		1.6.2.9AudioCodes Device Manager Validation1.6.2.10Sandboxing		
		1.6.2.11 Keystore		
		1.6.2.12 Device Certificate		
		1.6.2.13Data Protection1.6.2.14Device File System		
		1.6.2.15 Debugging Interface		
		1.6.3 Android Security Updates	11	
		1.6.4 AudioCodes Root CA Certificate	12	
2	Gett	ting Started1	13	
2	Gett 2.1	t ing Started 1 Setting up RX-PAD		
2		-	13	
2	2.1	Setting up RX-PAD	13 13	
2	2.1	Setting up RX-PAD Signing in to RX-PAD	13 13 13	
2	2.1 2.2	Setting up RX-PAD Signing in to RX-PAD	13 13 13 13	
	2.1 2.2 2.3 2.4	Setting up RX-PAD	13 13 13 13 13	
2	2.12.22.32.4Ope	Setting up RX-PAD Signing in to RX-PAD	13 13 13 13 14 14	
	 2.1 2.2 2.3 2.4 Ope 3.1 	Setting up RX-PAD	13 13 13 13 14 15 16	
	2.1 2.2 2.3 2.4 Ope 3.1 3.2	Setting up RX-PAD	13 13 13 13 14 15 16	
	 2.1 2.2 2.3 2.4 Ope 3.1 	Setting up RX-PADSigning in to RX-PADSigning in to RX-PADSigning in to RX-PADSigning Admin Login TimeoutPairing RX-PAD with MTRAfter PairingSetting RX-PADSetting RX-PADSetting RX-PADSetting RX-PADSetting With the Remote KeyboardSetting With the Remote KeyboardSetting Popup MessagesSetting MTR Camera SettingsSetting MTR Camera Setting MTR C	13 13 13 13 14 15 16 16 17	
	 2.1 2.2 2.3 2.4 Ope 3.1 3.2 3.3 	Setting up RX-PADSigning in to RX-PADSigning in to RX-PAD	13 13 13 13 14 15 16 16 17 20	
	 2.1 2.2 2.3 2.4 Ope 3.1 3.2 3.3 3.4 	Setting up RX-PAD. Signing in to RX-PAD. 2.2.1 Configuring Admin Login Timeout. Pairing RX-PAD with MTR. After Pairing. Prating RX-PAD. Operating with the Remote Keyboard. Managing Popup Messages. Adjusting MTR Camera Settings. 3.3.1 Configuring a Color Mode Preset on the RXVCAM50M/L Camera Configuring a Bundle.	13 13 13 13 14 15 16 16 17 20 21	
	2.1 2.2 2.3 2.4 Ope 3.1 3.2 3.3 3.4 3.5	Setting up RX-PAD. Signing in to RX-PAD. 2.2.1 Configuring Admin Login Timeout. Pairing RX-PAD with MTR. After Pairing. Prating RX-PAD. Operating with the Remote Keyboard. Managing Popup Messages. Adjusting MTR Camera Settings. 3.3.1 Configuring a Color Mode Preset on the RXVCAM50M/L Camera . Configuring a Bundle. Configuring Ad Hoc Mode on RXV81 MTRA.	13 13 13 13 14 15 16 16 17 20 21 22	
3	2.1 2.2 2.3 2.4 Ope 3.1 3.2 3.3 3.4 3.5 3.6	Setting up RX-PAD	13 13 13 14 15 16 16 17 20 21 22 23	
	2.1 2.2 2.3 2.4 Ope 3.1 3.2 3.3 3.4 3.5 3.6 Con	Setting up RX-PAD Signing in to RX-PAD 2.2.1 Configuring Admin Login Timeout. Pairing RX-PAD with MTR After Pairing erating RX-PAD	 13 13 13 14 15 16 16 17 20 21 22 23 25 	
3	2.1 2.2 2.3 2.4 Ope 3.1 3.2 3.3 3.4 3.5 3.6 Con 4.1	Setting up RX-PAD. Signing in to RX-PAD. 2.2.1 Configuring Admin Login Timeout. Pairing RX-PAD with MTR. After Pairing. erating RX-PAD Operating with the Remote Keyboard. Managing Popup Messages. Adjusting MTR Camera Settings. 3.3.1 Configuring a Color Mode Preset on the RXVCAM50M/L Camera Configuring a Bundle. Configuring Ad Hoc Mode on RXV81 MTRA. Screen Sharing. Accessibility.	13 13 13 14 15 16 16 17 20 21 22 23 25 25	
3	2.1 2.2 2.3 2.4 Ope 3.1 3.2 3.3 3.4 3.5 3.6 Con 4.1 4.2	Setting up RX-PAD	13 13 13 14 15 16 16 16 17 20 21 22 23 25 25 25	
3	2.1 2.2 2.3 2.4 Ope 3.1 3.2 3.3 3.4 3.5 3.6 Con 4.1 4.2 4.3	Setting up RX-PAD	13 13 13 14 15 16 16 16 17 20 21 22 23 25 25 25 25 25	
3	2.1 2.2 2.3 2.4 Ope 3.1 3.2 3.3 3.4 3.5 3.6 Con 4.1 4.2	Setting up RX-PAD	13 13 13 14 15 16 16 16 17 20 21 22 23 25 25 25 25 25	

5	Enro	olling a Device with Intune Policies	27
	5.1	Creating a Dynamic Group	
	5.2	Creating an Exclusion Group	
	5.3	Removing Devices from Intune admin center	
6	Mon	itoring Device Software Modules Status	33
7	Deb	ugging	35
	7.1	Log Settings Collecting Logs	
	7.2	Remote Logging	
	7.3	Diagnostic Data	
	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	
	7.10	Restoring to Defaults	
	7.11	Erase all data (factory reset)	
	7.12	Screen Capture	43
	7.13	Performing Recovery Operations	
	7.14	Restoring Device Firmware via USB Disk	
8	Savi	ing Logs while Device is in Recovery Mode	45
9	Upd	ating Microsoft Teams Devices Remotely	

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
RX-PAD Meeting Room Controller Quick Guide
Pairing RX-PAD with Teams Rooms on Android
RXV81 MTRA User & Admin Manual
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.



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

:	Human sensor
IJ	Cable compartment
	POE or power enabled
(î;	Dual-band Wi-Fi and Bluetooth support
, militaria de la composición	Android 12

1.2 Specifications

See the <u>RX-PAD Datasheet</u> 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 <u>here</u>.
- 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 <u>here</u>.

1.6.4 AudioCodes Root CA Certificate

Certificate Details for File 'New Text Document.cer'				
Certificate Hierarchy:				
RootCA				
Version:	3			
Subject:	CN=RootCA,O=ACL			
Issuer:	CN=RootCA,O=ACL			
Serial Number:	0×1			
Valid From:	1/1/2000 2:00:00 AM IST			
Valid Until:	1/1/2030 2:00:00 AM IST			
Public Key:	RSA 2048 bits			
Signature Algorithm:	SHA256WITHRSA			
Fingerprint:	MD5 - AD:F7:94:DE:B3:1D:F0:3F:74:3B:C5:42:34:51:19			
	Import <u>Extensions PEM</u> <u>ASN.1</u>			
	ОК			

----BEGIN CERTIFICATE----

MIIDMTCCAhmgAwIBAgIBATANBgkqhkiG9w0BAQsFADAfMQwwCgYDVQQKEwNBQ0wx MB8xDDAKBgNVBAoTA0FDTDEPMA0GA1UEAxMGUm9vdENBMIIBIjANBgkqhkiG9w0B AQEFAAOCAQ8AMIIBCqKCAQEA6GK495KUCXAm/UE17G4/cjnZN4LNaxYEYzbfZL0a EhgSKYt/LQ+iUcDhojsneusNgrcGkpwKklKsGsvGWmSRNULV01CW+TX2VJN73+hh V0uzhyOIYAUhbDaoqNM6Kp5b7sJ1ew4Ig9kfd/ma9Cz15koESLlw/inLj/r+rD96 mUcPElWrKspv7Qy4I14fsK/yMArixRopTL1munVVPpSFM9Jh8IY3JHyr5CQJXKKs EhGAJsnHaRqsR2Su3X/WtslqEF+cvP34pxhlhFL29nMfnaFATSS3rqGaFlSvl1ZS esLMqkWjp9cqGYrvt7K61sYnvMMb+o/KbWqVokXb+Fr7bwIDAQABo3gwdjAMBgNV HRMEBTADAQH/MB0GA1UdDgQWBBQDXySn9hz15lDraZ+iXddZGReB+zBHBgNVHSME QDA+gBQDXySn9hz15lDraZ+iXddZGReB+6EjpCEwHzEMMAoGA1UEChMDQUNMMQ8w DQYDVQQDEwZSb290Q0GCAQEwDQYJKoZIhvcNAQELBQADggEBAI0rUywommWWJnH3 JOfKiS3+VnX5hJITZymvWanMXUz/6FonHccPXEBYTrUYwhiWx3dwELAFXDFKkxMp 0KKWZ4F39cA0LRjqhzya+xUeeJ9HQZCXYAJ6XgvTfN2BtyZk9Ma8WG+H1hNvvTZY QLbWsjQdu4eFniEufeYDke1jQ6800LwMlFlc59hMQCeJTenRx4HdJbJV86k1gBUE A7fJT1ePrRnXNDRz6QtADWoX3OmN7Meqen/roTwvLpEP22nYwvB28dq3JetlQKwu XC4gwI/o8K2wo3pySLU9Y/vanxXCr0/en513RDz1YpYWmQwHA8jJIu8rxdhr+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

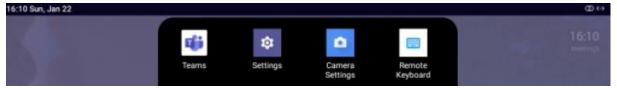
RX-PAD must be paired with the Microsoft Teams Room (MTR) on Android device (RXV81 | RXV200).



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: Solid red indicates in a meeting Solid green indicates the RX-PAD is online and signed in Flashing red indicates incoming invite to join a meeting 			
8	Drop-down menu to make it easy to open the RX-PAD application launcher. The new launcher enables accessing an app <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:
 - 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.

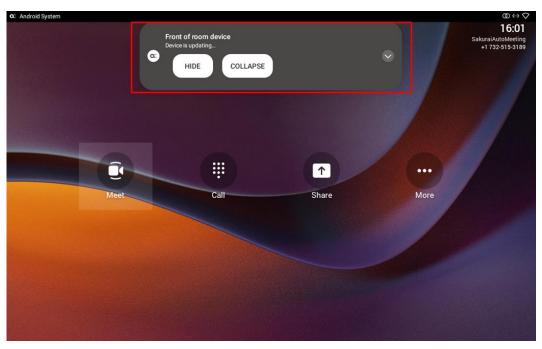
3.2 Managing Popup Messages

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.

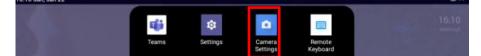


If the alert is an action, you can perform the action using RX-PAD, for example, REBOOT / DO IT LATER / COLLAPSE, as shown in the figure below.

			$\odot \leftrightarrow \bigcirc$
Front of room device Restarting REBOOT DO IT LATER	COLLAPSE		16:09 SakuraiAutoMeeting +1732-515-3189
Call	Share	More	
	Restarting REBOOT DO IT LATER	Restarting REBOOT DO IT LATER COLLAPSE 	Restarting REBOOT DO IT LATER COLLAPSE

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.

Caudiocodes

Presets	EDIT PRESET	
		:
+ Create New Preset	ලි Auto-Framing 🌑	
	Zoom I I I I I I I I I I I I I I I I I I I	0%
	Tilt	50%
	Pan	50% 100%

 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.

← Camera Settings		Limited access
Presets	VIEW PRESET	
Room		
+ Create Temporary Preset	준, Auto-Framing 🌑	
	Zoom G o	0%
		100%
	Tilt	50%
		100%
	Pan	50%
		100%
	Brightness	50%

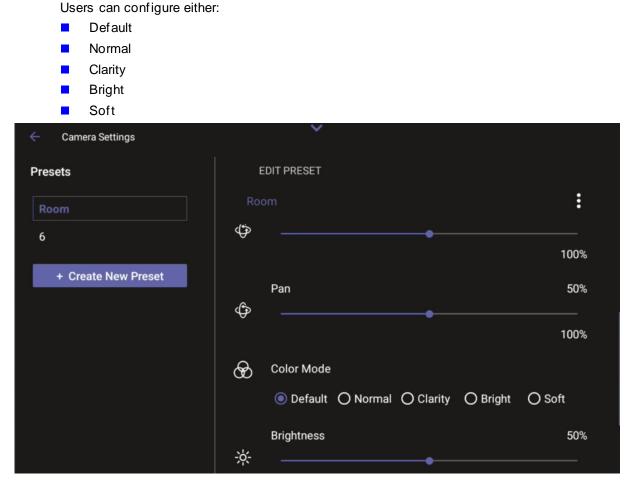


Note: If that user leaves the meeting, the temporary presets will be erased when they later reenter Camera Settings (or another user later enters); temporary presets are only for that meeting they were configured for; new presets can be configured for the new meeting.

← Camera Settings		Uimited access
Presets	EDIT PRESET	
Room test + Create Temporary Preset	test දුටු Auto-Framing 🌒	:
	Zoom	56%
	Tilt	67%
	Pan	66%
	Brightness	60%
← Camera Settings		United access
Presets	VIEW PRESET	
Room		
+ Create Temporary Preset	ညြ Auto-Framing 🕕	
	Zoom © •	0%
		100%
	Tilt	50%
		100%
	Pano	50%
		100%
	Brightness	50%

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.



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

Bluetooth

Security

Bundle Camera

Languages & input

ර

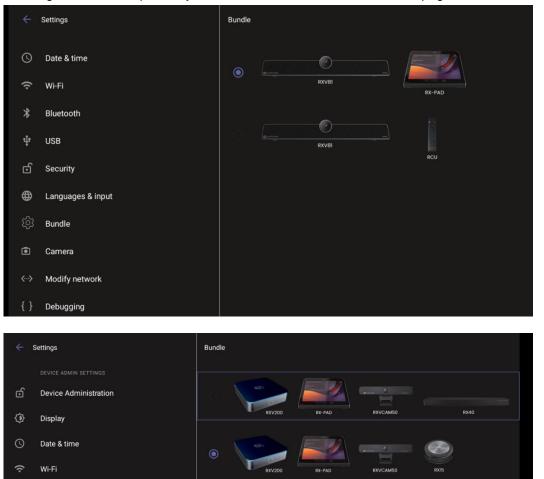
⊕

3.4 Configuring a Bundle

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

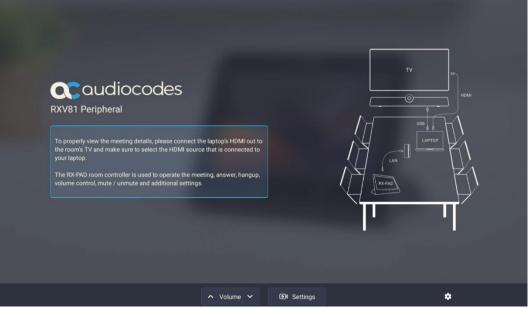
- Navigate to the Bundle setting using RX-PAD's Remote Keyboard that controls the MTR (see also the next section).
- You must be logged in to access the Bundle page.

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

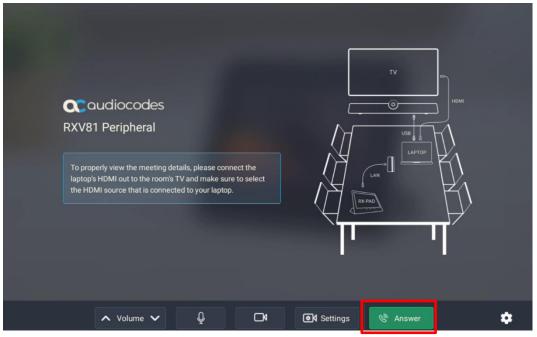


3.5 Configuring Ad Hoc Mode on RXV81 MTRA

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.

÷	Settings	Accessibility
(۵	Sound	Font size Default 당
Ĭ	Accessibility	High contrast text
{ }	Reboot	Color correction
í	About	Off

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.

Reboot	
Are you sure you want to reboot the device?	
CANCEL OK	

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.

Caudiocodes

÷	Settings	About
۹)	Sound	Status
Ţ	Accessibility	Model RXV80
{ }	Reboot	Android version
()	About	9
Device admin settings		Version info

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

÷	Settings	← About Status
•)	Sound	IP address fe80::2980:1cd8:ccd8:c0d3
Ĭ	Accessibility	10.22.13.32
{}	Reboot	Wi-Fi MAC address 34:f1:50:8e:3e:5f
(j)	About	MAC address 00:90:8F:C8:B0:19
Device	admin settings	00.90.07.00.00.19
⋳	Device Administration	Bluetooth address 34:f1:50:8e:3e:60
٩	Display	Serial number DB13152281
©	Date & time	Up time
♥	Wi-Fi	50:46:03
۲	Camera	

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).

×	K Home > Devices Conditional access > Conditional Access Overview >		Filter	r for	devices			
A Home	New							
Dashboard	Conditional Access policy				and a second			
E All services	Control access based on Conditional Access	Control access based on signals from conditions			er to apply policy to specific devic	es. Learn more L3		
Devices	policy to bring signals together, to make decisions, and enforce organizational policies.	like risk, device platform, location, client apps, or device state. Learn more C	Configur		No			
Apps	Learn more C	Device platforms ③	(Tes					
🌏 Endpoint security	Name *	Not configured			ng the rule:			
Reports	Example: 'Device compliance app policy'	Locations ①			ered devices in policy			
🚨 Users	Assignments	Not configured			ered devices from policy rule builder or rule syntax text bi	ov to croate or edit the	filter rule	
A Groups	Users (i)	Client apps ()	And/		Property	Operator	Value	
Tenant administration	0 users and groups selected	Not configured			displayName	Equals	RXV81	Û
🗙 Troubleshooting + support	Target resources ()	Filter for devices	And		displayName	Equals	RXV200	Û
	No target resources selected	Exclude filtered devices	+ Add	expressi	ion			
	Conditions ③	Authentication flows (Preview)	Rule synt	ntax 🛈				🖉 Edit
	1 condition selected	Not configured	device.	display	Name -eq "RXV81" -and device.d	isplayName -eq "RXV2	00"	
	Access controls							
	Grant 💿							
	0 controls selected							
	Session ()							
	0 controls selected							
	Enable policy							
	(Report-only) On Off			_				
	Create		Don	1e				

ali carciente@talkmail.o

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.

Microsoft Intune admin cente	r -					
Home Dashboard	Home > Devices Android > Android	devices				
All services	Search « Overview	🖔 Refresh 🛓 Export	E Columns V	Bulk device action	15	
Apps Endpoint security	Android devices Android enrollment	,O Search	0	OS: Android (d	evice administrator), And	roid (personally-ow, , +4
Reports	Android policies	Device name	Managed by	Ownership	Compliance	os 🛛
Groups	🔓 Compliance policies	Confroomaudc_Androi	Intune	Personal	Compliant	Android (device admi Android (device admi
Tenant administration	 Configuration profiles Android FOTA deployments 	Confroomaudc_Androi	Intune	Personal	Compliant	Android (device admi
X Troubleshooting + support		Confroomaudc_Androi	Intune	Personal	Compliant	Android (device admi
		Confroomaude_Androi	Intune	Personal	Compliant	Android (device admi



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.

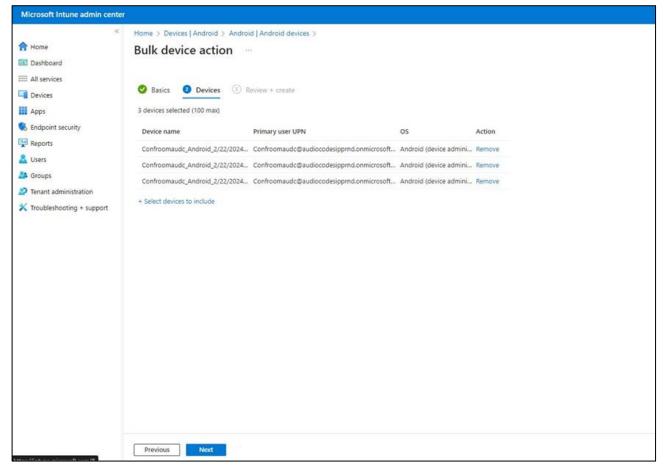
Home > Devices Android > Android	Android devices >
Bulk device action	
built define detion	
1 Basics 2 Devices 3 Rev	iew + create
OS *	Android (device administrator)
Device action *	Delete V
If you delete this device, you will no I	onger be able to view or manage the device from the Intune portal. The device will no
longer be allowed to access your con to check-in after it is deleted.	npany's corporate resources. Company data may be wiped from the device if the device tries
Previous Next	



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

	Home 3 Devices (Android 3 Android (Android devices)	Select devices ×			
A Home	Bulk device action	Select devices			
Cashboard		Search by MRI, serial nundes; email user principal name, device name, management name, phone number; model, or nanotamu			
All services	At least one device must be selected	sandh by Mill, sarar number, emait sair prinopat name, devea name, management name, jindne number, model, or manifactur			
Devices		OS Android (device administrator)			
Apps	Statics Devices ① Review - create	Device name Primary user URN OS			
Endpoint security	0 devices selected (100 max)	Contrastraude JAndreis 2022/2024, 1113 AM Contrastrational Education designed communications - Andreid University			
Reports	No devices added	Conferenced, Annual, 2022/23, 23 PM Conferenced: Read an Annual time and their admin.			
A Croups	+ Select devices to include	Contramavia Antroit, 2020204 (912 AM Contramavia/Bauticoods) gand continuations - Antroid strains administ			
 Process Tenant administration 		Controomaudo, Android, 2/02/2024, 9:17 AM Controomaudo:@audiocodesigpmd.onmicresoft.com Android (Device admins			
X Troubleshooting + support		Confroomaude_Android_2/22/2024_9.25 AM Confroomaude@budiocodesigpmd.ormicrosoft.com Android (device admins			
		Centromaude, Android, 2026/2024, 853 PM Contromaude@sudiccodesigpindionneroeo/f.com Android (Device admins			
		GalRoom, Android, 2/21/2014;7:34.44/ GalRoom@audiocodesippindionmicrosoft.com Android (device adminis			
		Rollecom Anderici 2/25/2021 236 438 Gallocom@ausioncodesinenvicement/comicrosoft.com Anderici Universidations.			
		Selected devices			
		Confromaude Android 2/22/2024 1135 AM Confromaude@auticocolwippind.ormion. Android Edwice adm			
		Confromeutic, Android, 2/22/2024, 2:53 PM Confromeutic@eutiocode/ppmd.ormion. Android plevice edm Remov			
		Confroomwude, Android, 2/12/2024, 9:12 AM Confroomwude@wudiocodevippind.ormicro. Android Edevice edm. Remov			
		Jeinet			

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**.

Microsoft Intune admin center				
×	Home > Devices Android > Android	Android devices >		
A Home	Bulk device action			
2 Dashboard				
All services				
Devices	Sasics OPevices 3 Revi	ew + create		
Apps	Summary			
Endpoint security	Basics			
Reports	Device action	Delete		
🚨 Users	OS	Android (device administrator)		
Sroups	Devices			
Tenant administration	Devices			
X Troubleshooting + support	3 devices selected (100 max)			
	Device name	Primary user UPN	os	
	Confroomaudc_Android_2/22/2024_11:	Confroomaudc@audiocodesipprnd.onmicrosoft.com	Android (device administr	
	Confroomaudc_Android_2/22/2024_2:5	${\tt Confroomaudc} @ {\tt audiocodesipprnd.onmicrosoft.com} \\$	Android (device administr,	
	Confroomaudc_Android_2/22/2024_9:1	Confroomaudc@audiocodesipprnd.onmicrosoft.com	Android (device administr	
	Previous Create			

7. 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 delet- ing 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**).

÷	Settings	← Debugging System State
ර	Device Administration	LLDP CDP Didn't run
۞	Display	IEEE 802 1x
S	Date & time	Didn't run
(¢	Wi-Fi	Network Ran with success result
*	Bluetooth	DHCP Option Ran with success result, IP : 192.168.33.4
ţ	USB	
0	Power saving	DNS Ran once with success result, Server: [192.168.33.1]
ර	Security	NTP Ran with success result, Server: time.android.com/216.239.35.4
	Languages & input	Switch To Voice Vlan Didn't run
<··>	Modify network	Proxy Configuration

÷	Settings	← Debugging System State
ර	Device Administration	Connect To Device Manager Running, connected to https://ippdm.audiocodes.com:443/
✨	Display	Get Certificate By SCEP
S	Date & time	Didn't run
((·	Wi-Fi	Get Certificate By HTTP Ran once with fail result, Reject response. Return code: 600
*	Bluetooth	Firmware Update Didn't run
ţ	USB	
0	Power saving	Configuration Update Didn't run
ර	Security	Redirect Didn't run
⊕	Languages & input	Apps Update Didn't run
< ··>	Modify network	Peripheral Devices Firmware Update

7 Debugging

Admin users can perform debugging for troubleshooting purposes.

To perform Debugging:

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

÷	Settings	Debugging
⋳	Device Administration	Log settings
٩	Display	Remote Logging
C	Date & time	Diagnostic Data
•	Wi-Fi	Reset configuration
۲	Camera	Restart Teams app
*	Bluetooth	Company portal login
⋳	Security	Launch mobile teams
⊕	Languages & input	Debug Recording
<··>	Modify network	Erase all data (factory reset)
Ľ	Calling	ADB

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.

← Debugging Log settings
Log Level
Log Package Filter
Log Tag Filter
Log Buffer Filter
Current filter for logs logcat

- 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.

Log Buffer Filter			
	Radio buffer		
	Events buffer		
	Main buffer		
	System buffer		
	Crash buffer		
	View all buffers		
	Default - main, system and crash buffers		
		CANCEL	ок

- 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.

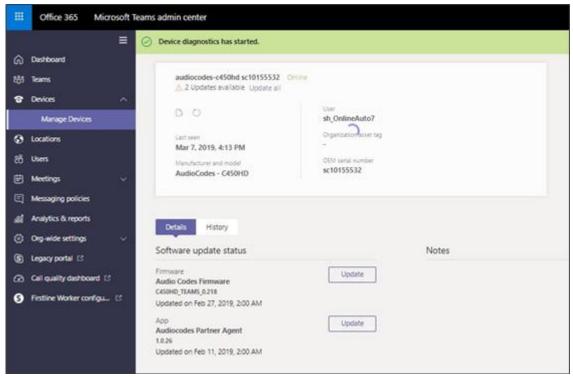
	Office 365 Microsoft T	eams admin center
1	=	Dashboard \ Manage devices \ audiocodes-c450hd sc10155532
ଭ	Dashboard	
885	Teams	audiocodes-c450hd sc10155532 Online
8	Devices ^	
	Manage Devices	D O sh_OnlineAuto7
•	Locations	Last seen Organization asset tag
88	Users	Mar 7, 2019. 4:13 PM Manufacturer and model OEM serial number
Ē	Meetings 🗸 🗸	AudioCodes - C450HD sc10155532
9	Messaging policies	
41	Analytics & reports	
۲	Org-wide settings \sim	Details History
3	Legacy portal 12	Software update status Notes
@	Call quality dashboard	Firmware Update Update
6	Firstline Worker configu (3	C450HD_TEAM5_0218 Updated on Feb 27, 2019, 200 AM
		App Audiocodes Partner Agent 1.0.26 Updated on Feb 11, 2019, 2:00 AM



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.

Device diagnostic	s	×	
Log files will be retrieved from the selected device(s). Would you like to proceed?			
	Proceed	Cancel	



4. Click Proceed; the logs are uploaded to the server.

5. Click the **History** tab.

	Office 365 Microsoft Te	Teams admin center			
	=	Dashboard \ Manage davices \			
ଭ	Deshboard				
885	Teams				
•	Devices 🔍 🗸	D O		User	
۲	Locations	Last seen		Organization scient tag	
88	Users			• CEM serial number	
Ē	Meetings ~	Manufacturer and model		-	
9	Messaging policies				
41	Analytics & reports				
۲	Org-wide settings \sim	Details History			
3	Legacy portal 13				
۵	Cell quality deshboard	History			
9	Firstline Worker configu	Action	Details	Modified on	Diagnostics file
		Device Diagnostics	Completed	Mar 7, 2019, 4:14 PM	Download

6. 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**.

← Debugging Remote Logging	
Remote IP address	
Remote port 514	
Remote Logging Remote logging is now disabled	

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**.

Diagnostic Data			
Copy logs to sdcard?			
	CAN	NCEL	ОК

- 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.
- 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.

Reset configuration	
Are you sure you want to reset to your original configuration?	
CANCEL	ок

2. Navigate to and select **OK**; all data is erased and default factory settings are restored but signin 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

← Device Details	1
alanr_Android_12/1/2020_12:55 PM EXX88 This is the device you're currently using.	
Original Name alanr_Android_12/1/2020_12:55 PM	
Operating System Android	
Ownership Type Personal	
Learn More	
Device Settings Status In Compliance Last checked: December 6, 8:43 AM	
Check device settings	

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:

← Device Details	Settings
alanr_Android_12/1/2020_12:55 PM	About
Device settings meet policy requirements.	
Original Name alanr_Android_12/1/2020_12:55 PM	
Operating System Android	
Ownership Type Personal	
Learn More	
Device Satus In Compliance Last checked: December 6, 08:43	
Check device settings	

L

•	
← Settings	
Usage Data Allow Microsoft to collect performance and usage data to help improve Microsoft products and services. Learn More	()1
Battery Optimization Turn off battery optimization You can turn off battery optimization for the Company Portal and the Microsoft Authenticator app for better performance of work or school apps that sync email or data. Learn More	TURN OFF
Troubleshooting Verbose Logging Allow the Company Portal and intune managed apps to record future actions in greater detail, which may help your company support better identify and solve issues.	(10
Automatically report errors to Microsoft.	
Diagnostic Data Copy logs to SD card.	COPYLOGS
Management Policy Sync your device with the latest policies from AudioCodes Ltd.	SYNC
Enable Browser Access Installs Work Account certificate. You might be prompted for system permissions.	ENABLE

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**.

Debugging Debug Recording	
Remote IP address	
Remote port 50000	
Voice record Voice recording is now disabled	

- 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).

÷	Settings	← Debugging Erase all data (factory reset)
۹)	Sound	This will erase all data from your IP Phone's internal storage, including:
Ĭ	Accessibility	System and app data and settings Downloaded apps
{}	Reboot	• Music • Photos • Other user data
í	About	
Device	e admin settings	You are currently signed into the following accounts:
⋳	Device Administration	alanr@audiocodes.com
✨	Display	
0	Date & time	D ₂
•	Wi-Fi	
٦	Camera	RESET PHONE
. 6		

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 /	Recovery mode (you can restore defaults from there)	~ 4 seconds	Red
Universal Boot Loader)	Switch slots A / B	~ 10 seconds	Green
	Loader	~ 15 seconds	Blue / Yellow
	Restore defaults	~25 seconds	Green + blue / Green + yellow
When successfully booted (on Android)	Reboot	From the Recovery menu	-
	Restore defaults	Long-press the Hold key for ~15 seconds	Flashes yellow once after release

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

