User's & Administrator's Manual

Room Experience (RX) Suite

RXV81 MTR on Android™ Video Collaboration Bar with RX-PAD Meeting Room Controller

Version 2.4

Microsoft Solutions Partner

Modern Work

audiocodes

Table of Contents

1 Introduction 7
1.1 Highlights 7
1.2 Benefits 8
1.3 Hardware Features 8
1.4 Bundles 8
1.5 Management 8
1.6 Specifications 9
1.7 Security Guidelines 11
1.7.1 Microsoft Teams Security Guidelines 11
1.7.2 Android Level Security Hardening 11
1.7.2.1 Google Play Services 11
1.7.2.2 Running Android in Kiosk Mode 11
1.7.2.3 Screen Lock 12
1.7.2.4 AudioCodes Private Key 12
1.7.2.5 Android Debug Bridge (ADB) 12
1.7.2.6 App Signing 12
1.7.2.7 Web Browser 12
1.7.2.8 Remote Configuration Management 12
1.7.2.9 AudioCodes Device Manager Validation 12
1.7.2.10 Sandboxing 13
1.7.2.11 Keystore 13
1.7.2.12 Device Certificate 13
1.7.2.13 Data Protection 13
1.7.2.14 Device File System 13
1.7.2.15 Debugging Interface 13
1.7.3 Android Security Updates 13
1.7.4 AudioCodes Root CA Certificate 14
1.8 Certificate Enrollment using SCEP 15
1.9 Provisioning Certificates in .pfx Format 16
2 Connecting to RXV81 17
2.1 Pairing with the RC 17
2.2 Signing in 19
2.2.1 Multi-Cloud Sign-in 19
2.2.2 Remote Provisioning and Sign in from Teams Admin Center 19
3 Using General RXV81 Functions 23
3.1 Managing Notification Messages 23
3.2 Configuring a Bundle 24
3.3 Modifying RXV81 Camera Settings 25
3.4 Starting a New Meeting 28
3.5 Dialing a Number 31
3.6 Enabling Proximity Join 32
3.7 Sharing a Whiteboard 33
3.8 Screen Sharing 35
3.9 About Microsoft Teams 37
3.10 Signing out 37
4 Configuring RXV81 Settings 39
4.1 Device Admin Settings 42
4.1.1 Configuring Display 42
4.1.2 Configuring Date & Time 44

4.1.3 Configuring Wi-Fi 45
4.1.3.1 Connecting to an Available Wi-Fi Network 45
4.1.3.2 Manually Connecting to a Wi-Fi Network 46
4.1.4 Configuring Camera Settings 49
4.1.4.1 Configuring Camera Frequency 50
4.1.5 Auto Framing 50
4.1.6 Pairing RC with RXV81 via Bluetooth 53
4.1.7 Configuring UI Language & Input 53
4.1.8 Modifying IP Network Settings 55
4.1.9 Configuring Call Settings 58
4.1.10 Configuring DSCP for QoS 59
4.1.11 Debugging 61
4.1.11.1 Log Settings | Collecting Logs 62
4.1.11.2 Remote Logging 64
4.1.11.3 Diagnostic Data 65
4.1.11.4 Reset configuration 65
4.1.11.5 Restart Teams app 66
4.1.11.6 Company Portal Login 66
4.1.11.7 Getting Company Portal Logs 66
4.1.11.8 Launch Mobile Teams 67
4.1.11.9 Debug Recording 67
4.1.11.10 Erase all data (factory reset) 68
4.1.11.11 Screen Capture 68
4.2 Performing Recovery Operations using Power Button 69
4.3 Restoring RXV81 Firmware via USB Disk 70
4.4 User Settings 71
4.4.1 Setting the Volume 71
4.4.2 Configuring Accessibility Settings 71
4.4.3 Setting Live Captions 71
4.4.4 Enabling Display of Meeting Name using Exchange Online PowerShell 72
4.4.5 Hiding Names and Meeting Titles 73
4.4.6 Rebooting RXV81 73
4.4.7 Viewing About RXV81 73
4.5 Enrolling a Device with Intune Policies 75
4.5.1 Creating a Dynamic Group 75
4.5.2 Creating an Exclusion Group 75
4.6 Removing Devices from Intune admin center 76
5 Viewing RXV81 Status LEDs 81
6 Monitoring Device Modules States 83
7 Using RXV81 in Ad Hoc Peripheral Mode 85
8 Updating the RXV81 MTR Remotely 89
8.1 Updating RXV81 Audio and Camera Peripherals Firmware 89
9 Replacing RC Batteries 93
9.1 Assessing RC Battery Level 93
9.2 Restarting / Rebooting RXV81 94
9.3 Powering Down/Up RXV81 94
10 RX-PAD Meeting Room Controller 95
10.1 Using RX-PAD 95
10.2 Using RX-PAD to Adjust RXV81 Camera Settings 96
11 Remote Controller (RC) 99
12 Android-based Teams Devices Parameters 101

List of Figures

Figure 3-1: Home Page 23
Figure 3-2: RXV81 Camera Settings when using RCU (not RX-PAD) 25
Figure 3-3: Camera settings 26
Figure 3-4: New meeting – Invite someone 28
Figure 3-5: New meeting – Enter the name of a person 28
Figure 3-6: New meeting – Select the name of a person 29
Figure 3-7: Dial pad 31

List of Tables

Table 1-1: RXV81 Bundles 8
Table 1-2: Specifications 9
Table 1-3: SCEP Parameters 15
Table 4-1: Configuration File Wi-Fi Parameters 47
Table 4-2: Recovery Operation Options using RXV81's Power Button 69
Table 5-1: Viewing RXV81 LEDs to Determine Status 81
Table 10-1: Reference to Using RX-PAD 96

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: June-05-2024

Security Vulnerabilities

All security vulnerabilities should be reported to vulnerability@audiocodes.com.

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 Web site 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 MTR on Android Video Collaboration Bar Deployment Guide
RXV81 MTR on Android Video Collaboration Bar Release Notes
RX-PAD Meeting Room Controller Pairing Guide
One Voice Operation Center (OVOC) Release Notes
One Voice Operation Center (OVOC) User's Manual
Device Manager Administrator's Manual

1 Introduction

AudioCodes' RXV81 is a standalone Microsoft Teams Rooms on Android ™ (MTR) video bar that takes advantage of plug-and-play simplicity to deliver a familiar and exceptionally productive Microsoft Teams meeting experience.

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

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

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

In addition to standalone mode, RXV81 can be used in ad hoc peripheral mode. In this mode, customers connect RXV81 to a BYOD (Bring Your Own Device) (PC/laptop) running a UC client; the BYOD displays meeting video and content and meetings are controlled via the BYOD (join, accept, manage participants). Audio/video (camera ePTZ, mic mute) can be controlled via the UC client or the RC (camera on / off, mute, volume).

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

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

See also AudioCodes' website here for information about the RXV-81.

1.1 Highlights

RXV81 feature highlights:

- **Plug-and-Play Simplicity for Fast Setup.**

  An easy-to-use mounting element and minimal cable connections enable quick and simple deployment.

- **[Optional] RX-PAD Meeting Room Controller**
- **[Optional] Bluetooth Remote Controller**

  Leverages Bluetooth for full control and bi-directional communication. Intuitive. Illuminated 'Mute' and 'Teams' buttons.

- **Intuitive Meeting Experience.**

  Fast access to meetings with one click to join using Microsoft Teams Room Android.

- **High Quality Video and Audio**.

  Outstanding Full HD image clarity and superb surround sound ensures that everyone in the meeting room is seen and heard.

- **Wide-angle 4K Camera**

  Covers a 110° viewing angle capturing every seat in the room even in tight spaces with challenging lighting conditions. D: 120º/ H: 110º/ V: 75º

- **Easy to Manage from Anywhere**.

  Enhance the meeting experience with centralized device management and monitoring from any location.

- **Peripheral Mode**.

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

1.2 Benefits

- Intuitive meeting experiences with one click to join using the Microsoft Teams Rooms on Android application.
- An easy-to-use mounting element and minimal cable connections enable quick and simple deployment.
- Superior audio via a full-room pickup with no need for an additional external USB microphone or speaker.
- Effortlessly manage meetings using the dedicated Bluetooth remote control or RX-PAD Meeting Room Controller.
- Audio notifications triggered by RX-PAD are heard through the RXV81 speaker, including Talkback accessibility, to ensure a streamlined and accessible communication experience during meetings and collaboration sessions.

1.3 Hardware Features

- RXV81 can be used on an ad hoc basis as a USB A/V peripheral for any UC client
- Wide-angle lens with 110° field of view (FoV) covers every seat in the meeting room. D: 120º/ H: 110º/ V: 75º
- Adjustable camera position with ePTZ support - 5x zoom - digital 5x zoom in. Manually vertically (up/down) adjustable ±15º.
- 6-element microphone array with 4.5 m pickup range for mid-size rooms and a 10W speaker for superb sound
- Stylish design and finish.
- Built-in dual band Wi-Fi and Bluetooth.
- High Dynamic Range (HDR) automatically ON - Wide Dynamic Range (WDR).

1.4 Bundles

RXV81 is available in three bundles.

Table 1-1: RXV81 Bundles

Name of Bundle	Details
TEAMS-RXV81	▪ Executive Offices | Huddle Rooms ▪ RXV81 main unit ▪ Bluetooth Remote Controller
TEAMS-RXV81-B10	▪ Huddle Rooms | Small and Medium Meeting Rooms ▪ 5-8 participants ▪ RX-PAD Meeting Room Controller
TEAMS-RXV81-B15	▪ Huddle Rooms | Small and Medium Meeting Rooms ▪ 5-8 participants ▪ RX-PAD Meeting Room Controller + AudioCodes RX15 Speaker

1.5 Management

RXV81 bundles are managed using AudioCodes' One Voice Operations Center (OVOC) Device Manager or Microsoft's Teams admin center (TAC), enabling IT admins to monitor and upgrade the devices from anywhere. Using OVOC, IT admins can easily monitor and manage all bundled devices from a centralized location. Management includes:

- Firmware management / upgrade
- Alarm management
- Upgrade the MTR APK

Admins can monitor the status of the device's modules from the System State page as shown here.

1.6 Specifications

The following table shows RXV81 specifications.

Table 1-2: Specifications

Feature	Details
Video capabilities	▪ Ultra HD 4k image sensor ▪ Super-wide angle horizontal field of view: 110° ▪ Lens: Fixed focus ▪ ePTZ capable, digital 5x zoom in ▪ Output resolution: 1080p ▪ Frame rate: 30 fps ▪ Manually adjustable, vertically (up/down) ±15º ▪ High Dynamic Range (HDR) automatically ON - Wide Dynamic Range (WDR).
Audio	▪ Full duplex, noise suppression, acoustic Echo Cancellation, voice separation ▪ 6x beamforming microphone array ▪ Voice pickup range: 4.5m (15ft) ▪ 10W speaker
Device Interfaces	▪ HDMI Output to TV ▪ Power/reset button ▪ USB 3.0 Type A (host) marked 1 to allow touch LCD or connectivity to wireless KB via BT USB dongle. Do not connect to power! ▪ Ethernet: 10/100 Mbps (RJ-45) network interface ▪ USB2.0 Type-C (device) marked 2 to connect to PC/MAC BYOD device (peripheral mode) ▪ 3 status LEDs indicating camera on/off, mute on, call state, device health ▪ Wi-Fi (dual band support) ▪ Bluetooth 5.0 ▪ 12V/3A DC power input ▪ Remote Controller (Bluetooth managed) ▪ RX-PAD Meeting Room Controller
Design	▪ DIMENSIONS (W X D X H) 462 x 93 x 76 mm ▪ WEIGHT 1.464 kg
Network Provisioning	▪ TCP/IP (IPv4), DHCP/ static IP; Time and date synchronization via SNTP; VLAN support; QoS support: IEEE 802.1p/Q tagging (VLAN) ▪ Layer 3 TOS and DSCP RTCP support: (RFC 1889) ▪ IP address configuration: TCP/IP (IPv4), DHCP/static IP Time and date synchronization: SNTP ▪ QoS support: IEEE 802.1p/Q tagging (VLAN), Layer 3 TOS and DSCP RTCP support: (RFC 1889)
OS	▪ Android 12
Security	▪ Encryption: TLS (Transport Layer Security), SRTP encryption for media, AES256 ▪ Network Access Control: IEEE 802.1x ▪ Built-in certificate
Management	▪ AudioCodes Device Manager, a plugin of AudioCodes One Voice Operations Center (OVOC)
Microsoft Teams Features (Android MTR)	✓ Calendar integration (with meeting preview) and one click to join Teams meetings ✓ Meet now option

Feature	Details
	✓ Simple sign-in interface from browser or smartphone with a code ✓ 'Direct guest join' to allow joining a third-party meeting ✓ 'Cast info' from mobile to the RXV81 screen over Bluetooth ✓ 'Room remote' using Teams mobile app allowing controlling RXV81 ✓ Remote sign-out from Microsoft Teams admin center (TAC). ✓ Hide names and meeting titles for individual devices ✓ Meeting stage ✓ Multi-spotlight ✓ Docked meeting controls ✓ Reactions ✓ Control camera/mic for attendees ✓ Live Captions in regular one-on-one calls and in Teams meetings ✓ Whiteboard support when signed in with personal account (short term roadmap for whiteboard support with room account) ✓ Multi-cloud sign-in support ▪ Remote provisioning and sign-in from TAC
RXV81 Device Feature Set	▪ Camera settings with different privileges for user and Admin ▪ In idle (Admin) and during a call/meeting (all users), long-pressing the camera button on the RC allows: ✓ Defining/editing a new preset ✓ Moving to different presets ✓ Changing all settings options ▪ Video quality: Resolution of 1080p on the decoder side and 720p on the encoding side ▪ RXV81 integration with AudioCodes OVOC-DM ▪ RXV81 Alerts to AudioCodes OVOC-Device Manager: ✓ Notification sent to screen/TV and to Device Manager if Remote Control is disconnected or if it's malfunctioning ✓ Notification sent to screen/TV and to Device Manager if Remote Control battery voltage level falls low, indicating what percentage level remains unused ✓ Remote Control flashes if the connection to RXV81 fails. ▪ Camera frequency set per power supply: ✓ 110V – 60Hz ✓ 220V – 50Hz ▪ Shortcut keys for administrators to manually perform recovery operations ▪ Ad Hoc Peripheral Mode allows connecting RXV81 via USB to the PC as a peripheral device.

1.7 Security Guidelines

RXV81 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

1.7.1 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

1.7.2 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.

1.7.2.1 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.

1.7.2.2 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).

1.7.2.3 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.

1.7.2.4 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.

1.7.2.5 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.

1.7.2.6 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.

1.7.2.7 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.

1.7.2.8 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.

1.7.2.9 AudioCodes Device Manager Validation

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

- The device is shipped with known Root CAs installed. See AudioCodes Root CA Certificate.
- 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 phone and re-establish the connection leveraging any private root CA.

1.7.2.10 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.

1.7.2.11 Keystore

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

1.7.2.12 Device Certificate

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

1.7.2.13 Data Protection

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

1.7.2.14 Device File System

The device file system is encrypted on the RXV81 device – customers may enforce a policy of device encryption via Microsoft Intune.

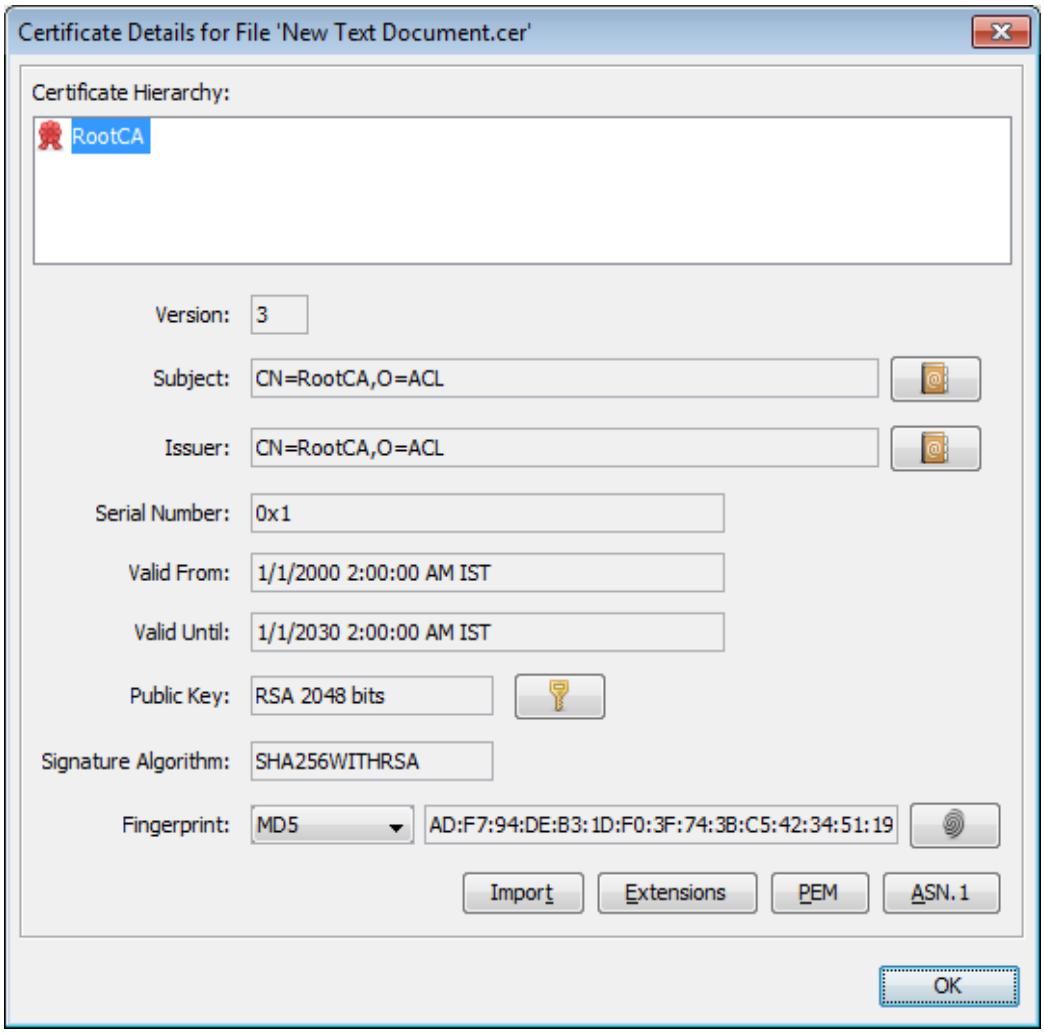
1.7.2.15 Debugging Interface

- 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.

1.7.3 Android Security Updates

In addition to all the above, AudioCodes regularly adopts and integrates the Android security updates. For reference see https://source.android.com/security/bulletin/2019-10-01).

1.7.4 AudioCodes Root CA Certificate




```
-----BEGIN CERTIFICATE-----
MIIDMTCCAhmgAwIBAgIBATANBgkqhkiG9w0BAQsFADAfMQwwCgYDVQQKEwNBQ0wx
DzANBgNVBAMTBlJvb3RDQTAeFw0wMDAxMDEwMDAwMDBaFw0zMDAxMDEwMDAwMDBa
MB8xDDAKBgNVBAoTA0FDTDEPMA0GA1UEAxMGUm9vdENBMIIBIjANBgkqhkiG9w0B
AQEFAAOCAQ8AMIIBCgKCAQEA6GK495KUCXAm/UE17G4/cjnZN4LNaxYEYzbfZL0a
EhgSKYt/LQ+iUcDhojsneusNgrcGkpwKklKsGsvGWmSRNULV01CW+TX2VJN73+hh
V0uzhyOIYAUhbDaoqNM6Kp5b7sJ1ew4Ig9kfd/ma9Czl5koESLlw/inLj/r+rD96
mUcPElWrKspv7Qy4I14fsK/yMArixRopTL1munVVPpSFM9Jh8IY3JHyr5CQJXKKs
EhGAJsnHaRqsR2Su3X/WtslgEF+cvP34pxhlhFL29nMfnaFATSS3rgGaFlSvl1ZS
esLMqkWjp9cqGYrvt7K61sYnvMMb+o/KbWqVokXb+Fr7bwIDAQABo3gwdjAMBgNV
HRMEBTADAQH/MB0GA1UdDgQWBBQDXySn9hz15lDraZ+iXddZGReB+zBHBgNVHSME
QDA+gBQDXySn9hz15lDraZ+iXddZGReB+6EjpCEwHzEMMAoGA1UEChMDQUNMMQ8w
DQYDVQQDEwZSb290Q0GCAQEwDQYJKoZIhvcNAQELBQADggEBAI0rUywommWWJnH3
JOfKiS3+VnX5hJITZymvWanMXUz/6FonHccPXEBYTrUYwhiWx3dwELAFXDFKkxMp
0KKWZ4F39cAOLRjqhzya+xUeeJ9HQZCXYAJ6XgvTfN2BtyZk9Ma8WG+H1hNvvTZY
QLbWsjQdu4eFniEufeYDke1jQ6800LwMlFlc59hMQCeJTenRx4HdJbJV86k1gBUE
A7fJT1ePrRnXNDRz6QtADWoX3OmN7Meqen/roTwvLpEP22nYwvB28dq3JetlQKwu
XC4gwI/o8K2wo3pySLU9Y/vanxXCr0/en5l3RDz1YpYWmQwHA8jJIu8rxdhr+VNQ
Zv6R/Ys=
-----END CERTIFICATE----
```

1.8 Certificate Enrollment using SCEP

The device supports certificate enrollment using Simple Certificate Enrollment Protocol (SCEP) using Microsoft's Network Device Enrollment Service (NDES) server without using AudioCodes' OVOC, thereby allowing device certificates and CA certificate provisioning to be scaled to multiple devices.

After devices are provisioned with a SCEP-related configuration, they receive a CA certificate from the NDES (via parameter 'security/ca_certificate/0/uri'), issue a Certificate Signing Request (CSR) to the NDES and receive a device certificate signed by the CA certificate (the one that the device received from NDES).

Network administrators must configure the following three parameters:

- security/SCEPEnroll/ca_fingerprint
- security/SCEPEnroll/password_challenge
- security/SCEPServerURL

The next table shows the parameter descriptions.

Table 1-3: SCEP Parameters

Parameter	Description
security/SCEPEnroll/ca_fingerprint	Define the thumbprint (hash value) for the CA certificate. Default value: NULL. Network admins must set its value to (for example): **3EBE50003ABF1DF5E6B5A3230B02B856**
security/SCEPEnroll/password_challenge	Define the enrollment challenge password. Default value: NULL. Network admins must set its value to (for example): **7A7F9FC4BB7625F0935E67EA6D6322ED**
security/SCEPServerURL	Define the NDES server's URL. Default: NULL. Network admins must set its value to (for example): **https://ndes_derver**
security/SCEPEnroll/renewal/advancethreshold	Define the renewal advance threshold of the device certificate. Configure between 50 and 100 (in units of percentage) Default: 80 This indicates that a renewal of the certificate (device.crt) will be initiated when 80 percent of its validity is reached.
security/SCEPEnroll/rollover/advancethreshold	Specify the threshold of the CA Root certificate's validity at which to initiate a renewal. Configure between 50 and 100 (in units of percentage). Default: 90 This indicates a renewal of the certificate (CAROOT.crt.) will be initiated when 90 percent of its validity is reached.

1.9 Provisioning Certificates in .pfx Format

Device certificates can be provisioned in .pfx format (combining .crt and key). The following parameter values can consequently be configured in the devices' Configuration File:

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

The feature is also supported by AudioCodes' Android Phone Utility.

Note:

- Certificate loading is performed using HTTP; prior to version 1.19, it was performed using SCP.
- The HTTP port is 8000.
- Make sure the port is not blocked by the organization's firewall.

2 Connecting to RXV81

Note: See the *RXV81 MTR on Android Video Collaboration Bar with RX-PAD or RCU Quick Guide* shipped with the product or available from AudioCodes for information about the hardware of RXV81, including:

- Package contents
- Mounting
- Cabling

After mounting and cabling the RXV81 device as shown in the *Deployment Guide*, pair it with the

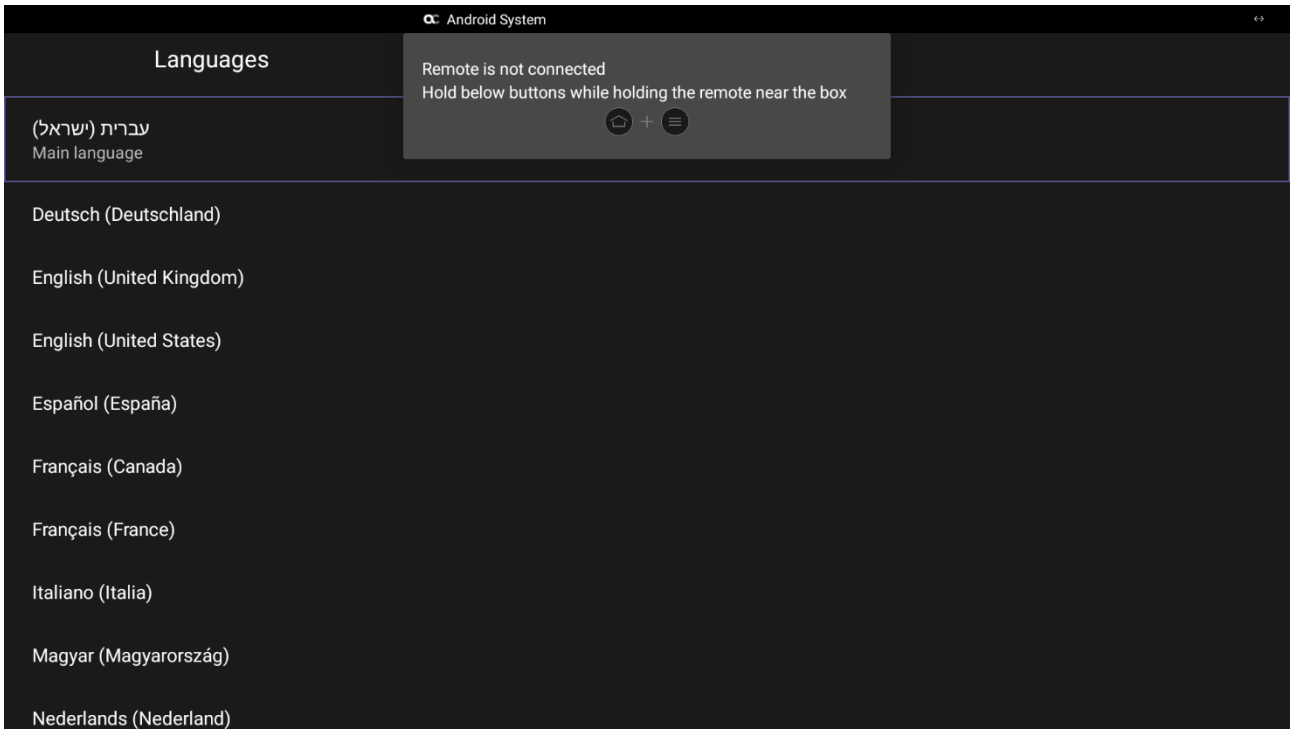
- Remote Controller (see the next section)
- RX-PAD (see *Pairing RX-PAD with Teams Rooms on Android AudioCodes Devices*)

2.1 Pairing with the RC

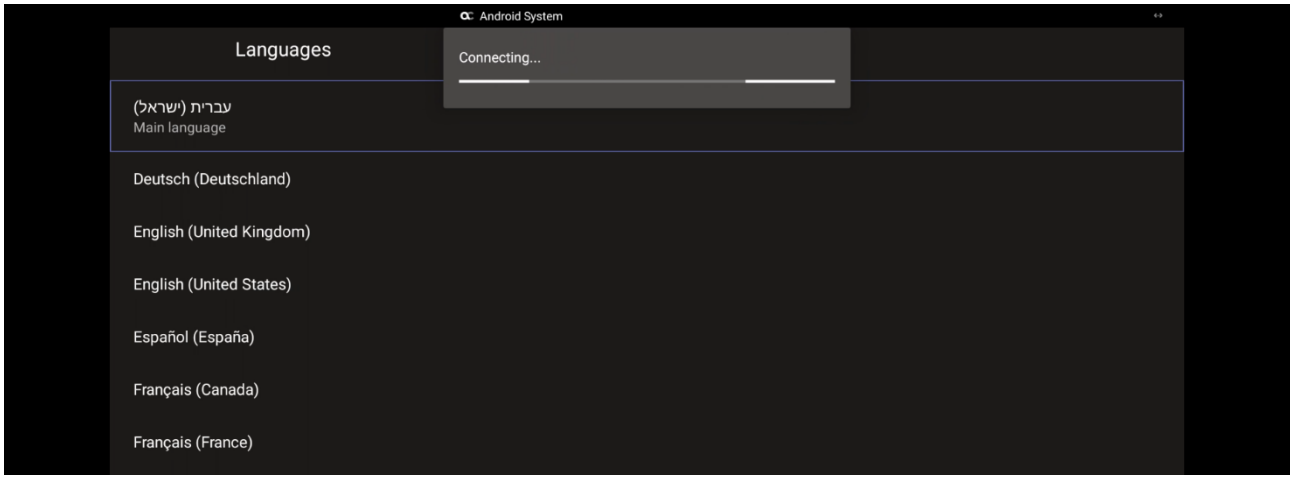
The instructions here show how to pair RXV81 with the RC. Applies to users who acquired the **TEAMS-RXV81** bundle.

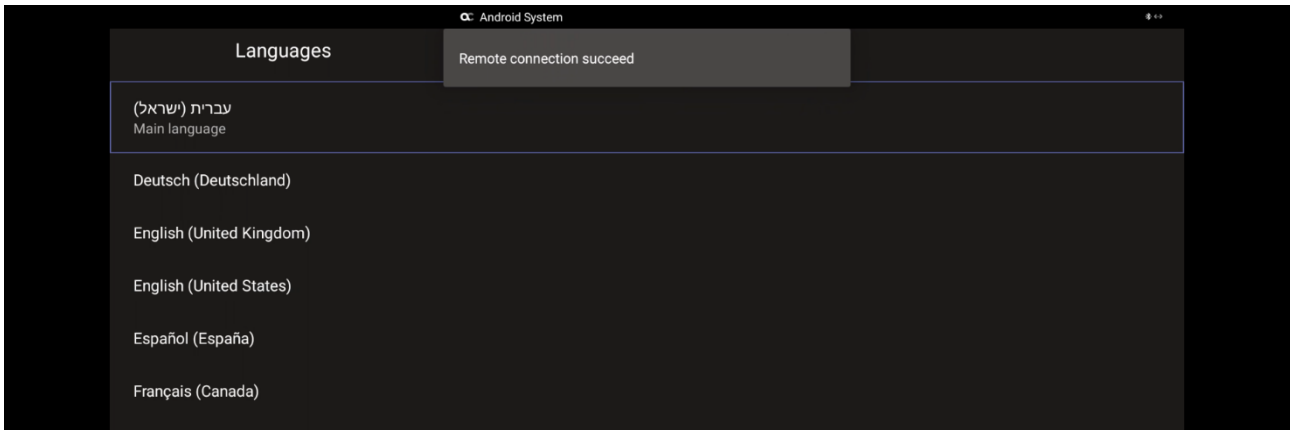
➢ **To pair RXV81 with the RC:**

1. After cabling, remove the RC from its packaging and insert the batteries supplied into it.
2. View in the display the message:
   Remote is not connected. **Hold below buttons while holding the remote near the box**.

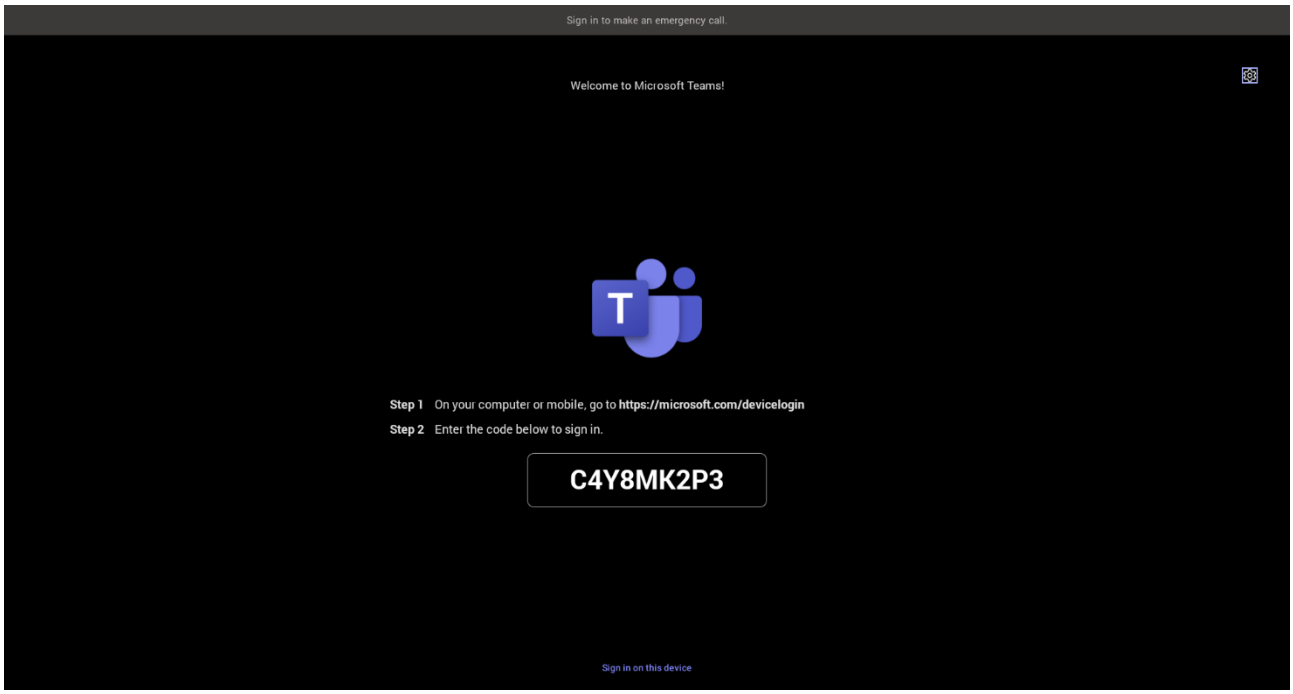


3. On the RC, simultaneously press and hold + until RC and RXV81 are connected.





4. Use the remote control to navigate to and select a language; the sign-in screen is displayed.

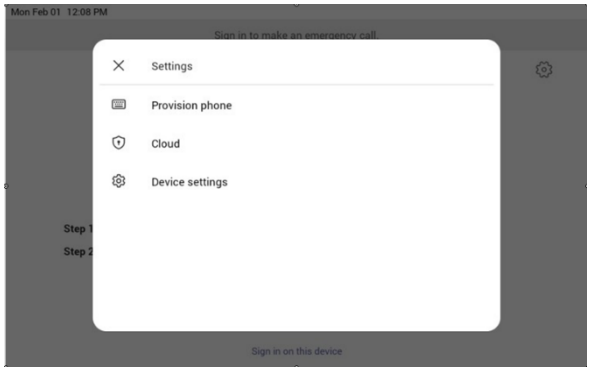


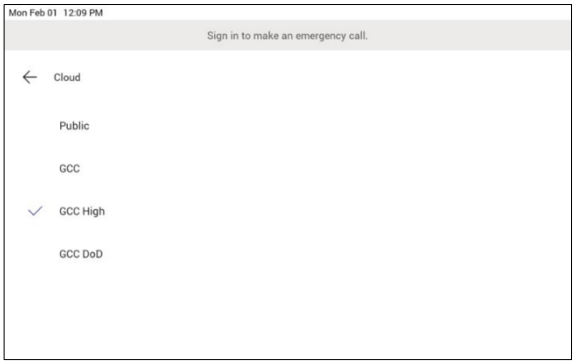
2.2 Signing in

Users are provided by default with the option to sign in from any browser or smartphone with a prominent device code. If you choose to sign in from the device, you can enter your username and password on-screen via the device keyboard.

2.2.1 Multi-Cloud Sign-in

For authentication into specialized clouds, the network administrator can choose the Settings gear on the sign-in page to see the options that are applicable to their tenant.





2.2.2 Remote Provisioning and Sign in from Teams Admin Center

See Remote provisioning and sign in for Teams Android devices - Microsoft Teams | Microsoft Docs for more information.

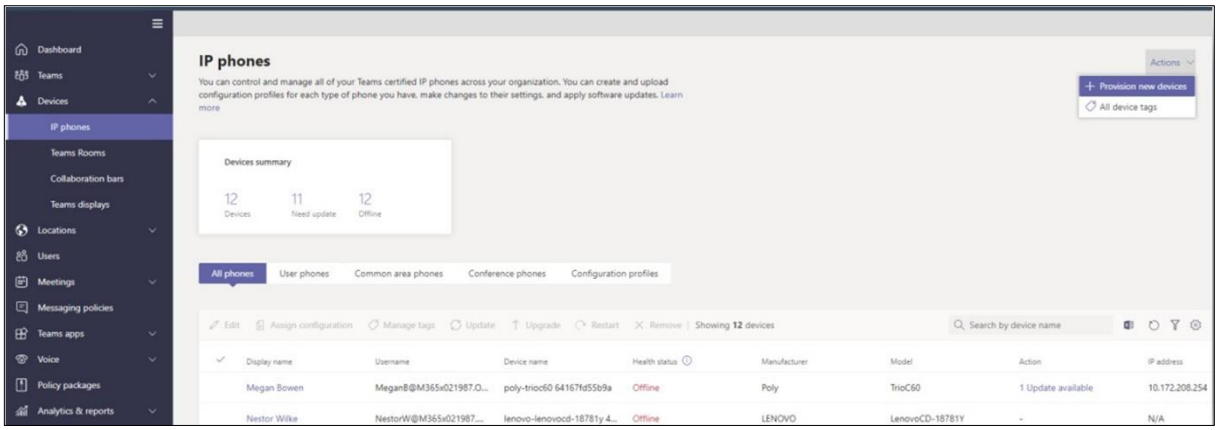
IT admins can remotely provision and sign in to a Teams device.

To provision a device remotely, the network administrator needs to upload the MAC IDs of the devices being provisioned and create a verification code. The entire process can be completed remotely from the Teams admin center.

Step 1: Add a device MAC address

Provision the device by imprinting a MAC address on it.

1. Sign in to the Teams admin center.
2. Expand **Devices**.
3. Select **Provision new device** from the **Actions** tab.



In the 'Provision new devices' window, you can either add the MAC address manually or upload a file.

Manually add a device MAC address

1. From the **Awaiting Activation** tab, select **Add MAC ID**.
2. Enter the MAC ID.
3. Enter a location, which helps technicians identify where to install the devices.
4. Select **Apply** when finished.

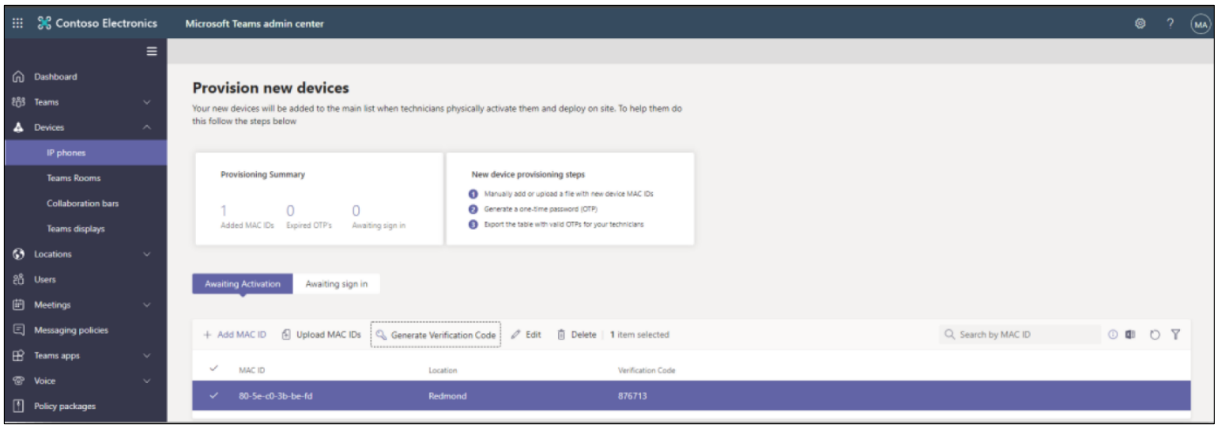
Upload a file to add a device MAC address

1. From the **Awaiting Activation** tab, select **Upload MAC IDs**.
2. Download the file template.
3. Enter the MAC ID and location, and then save the file.
4. Select the file, and then select **Upload**.

Step 2: Generate a verification code

You need to generate a verification code for the devices. The verification code is generated in bulk or at the device level and is valid for 24 hours.

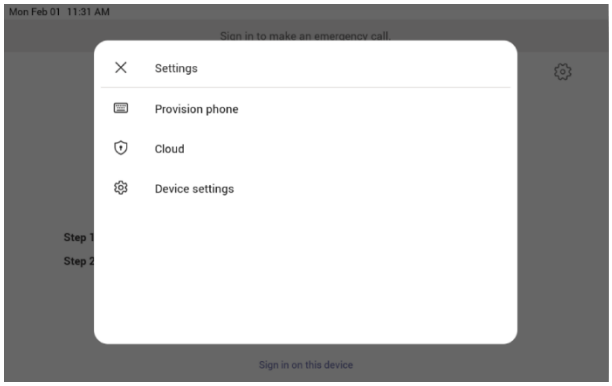
- From the **Awaiting Activation** tab, select an existing MAC ID. A password is created for the MAC address and is shown in the **Verification Code** column.



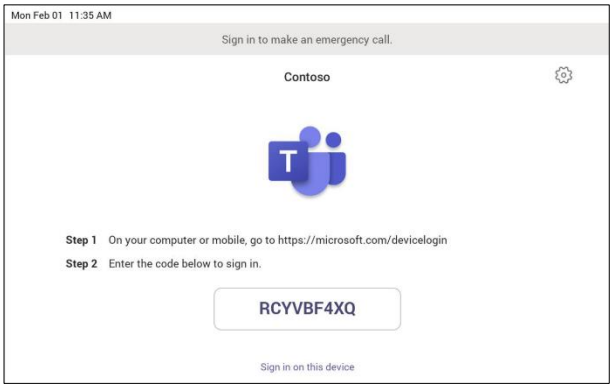
You'll need to provide the list of MAC IDs and verification codes to the field technicians. You can export the detail directly in a file and share the file with the technician who is doing the actual installation work.

Step 3: Provisioning on the device

Once the device is powered up and connected to the network, the technician provisions the device by choosing the 'Settings' gear on the top right of the new 'Sign in' page and selecting **Provision phone**.



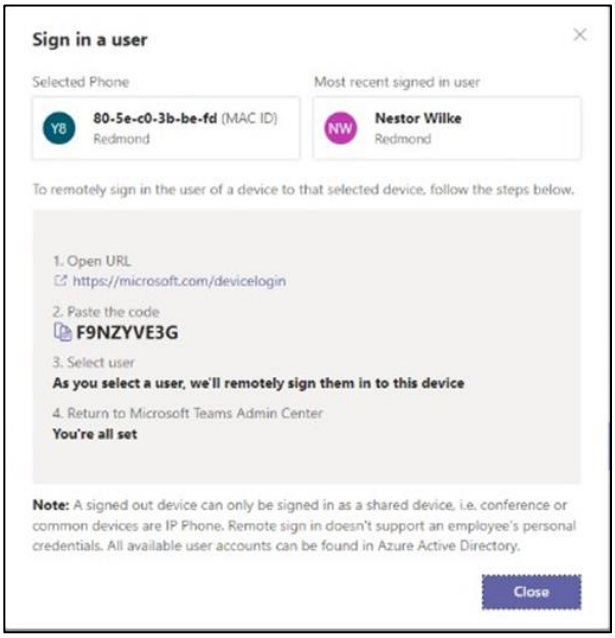
The technician is then expected to enter the device-specific Verification code that was provided in the Teams admin center on the phone's user interface. Once the device is provisioned successfully, the tenant name will be available on the sign in page.



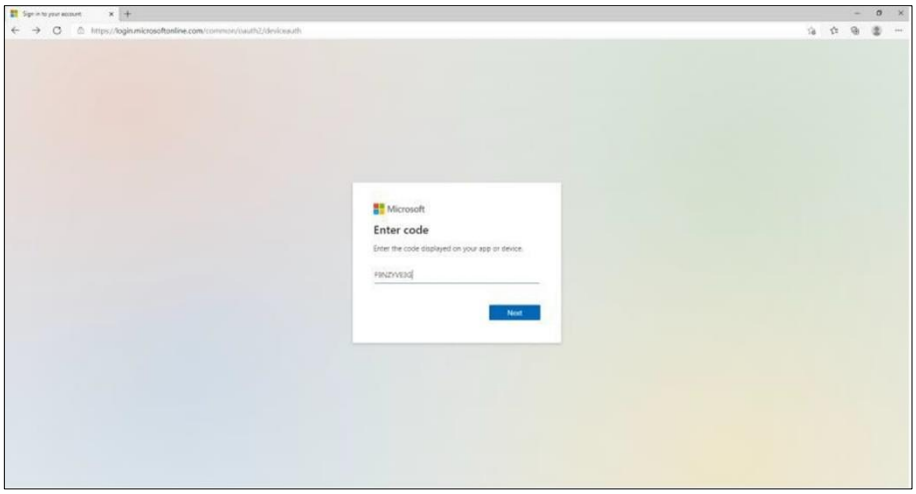
Step 4: Sign in remotely

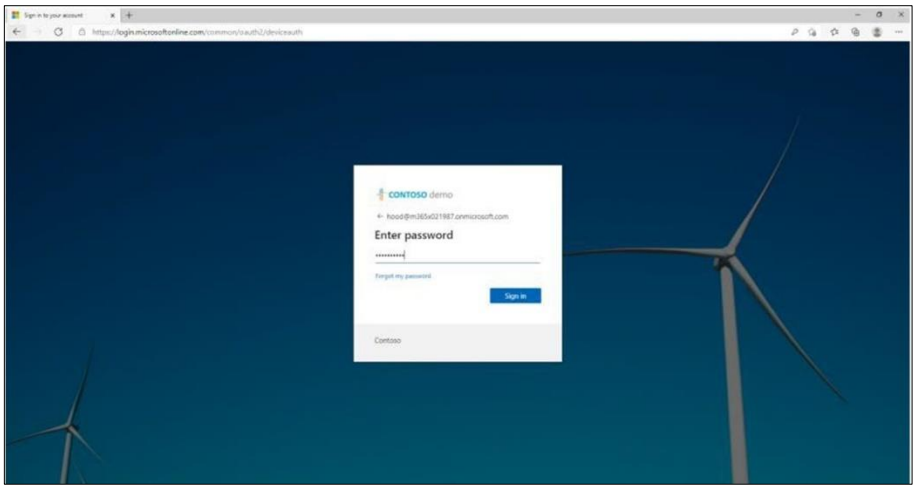
The provisioned device appears in the Awaiting sign in tab. Initiate the remote sign-in process by selecting the individual device.

1. Select a device from the **Awaiting sign in** tab.
2. Follow the instructions in **Sign in a user**, and then select **Close**.

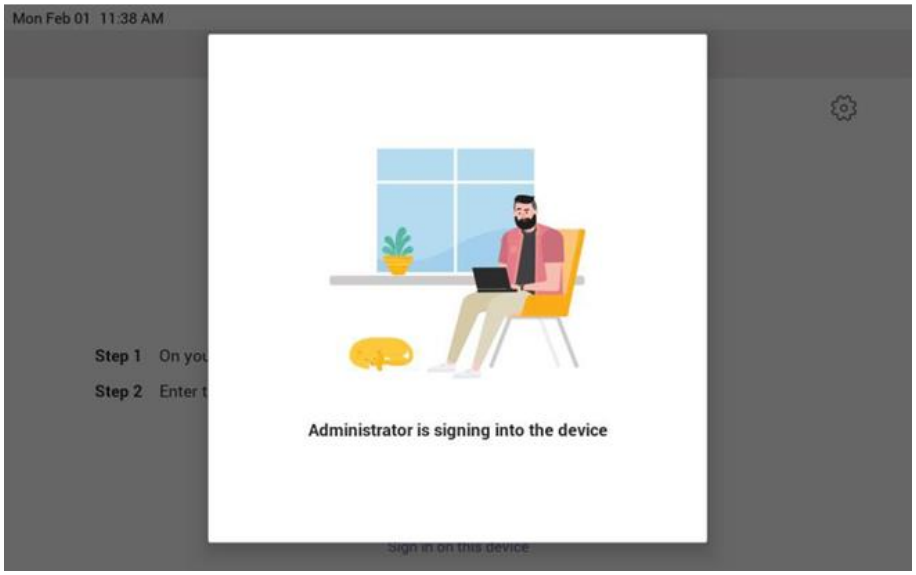


The tenant admin is expected to complete authentication on the device from any browser or smartphone.





When the tenant admin is signing in from Teams Admin Center, the user interface on the device is blocked to prevent other actions on the phone.



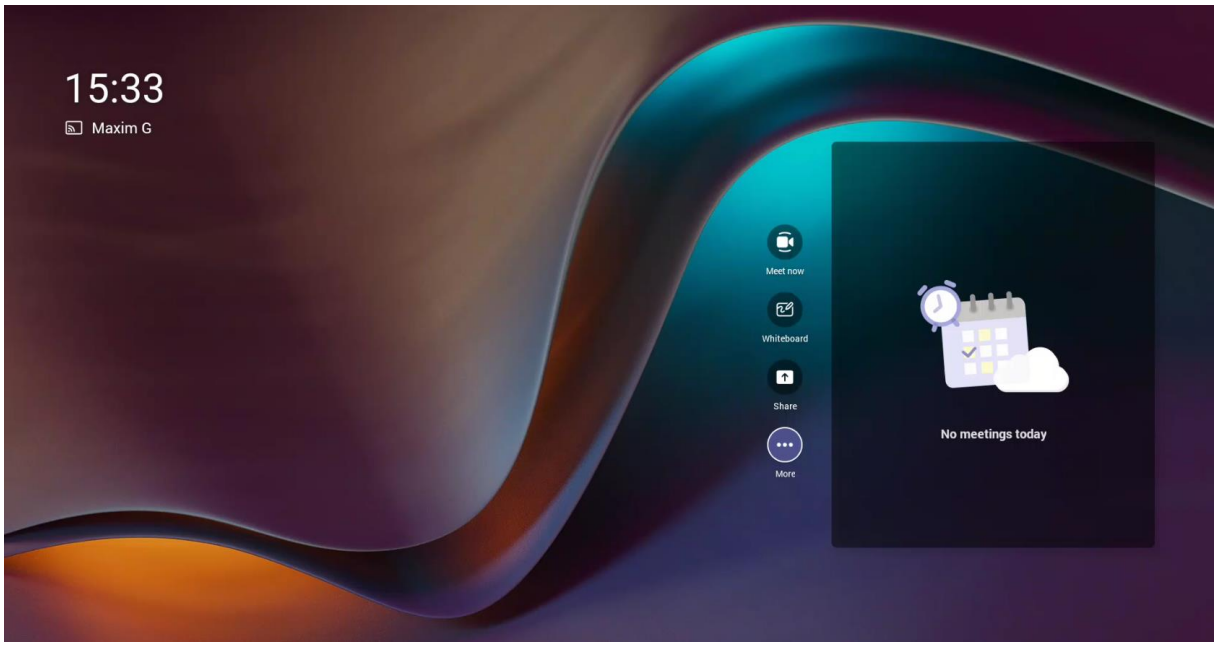
3 Using General RXV81 Functions

This section shows how to use general RXV81 functions.

➢ **To get started:**

1. After signing in, view the RXV81 home page.

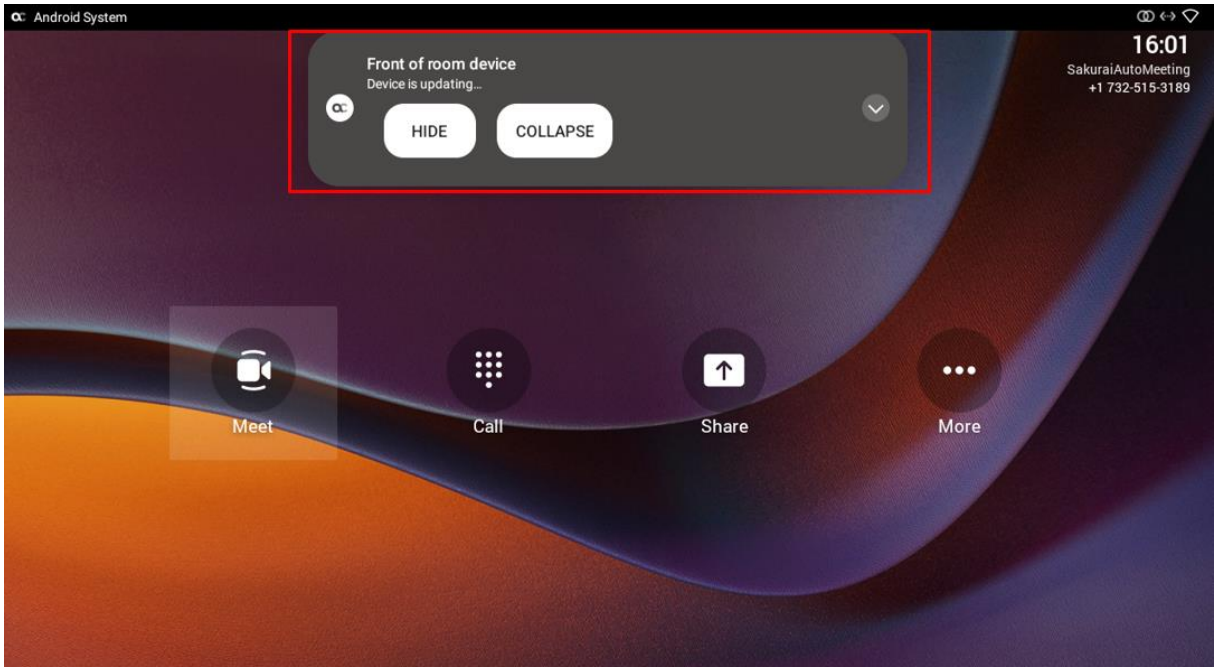
Figure 3-1: Home Page



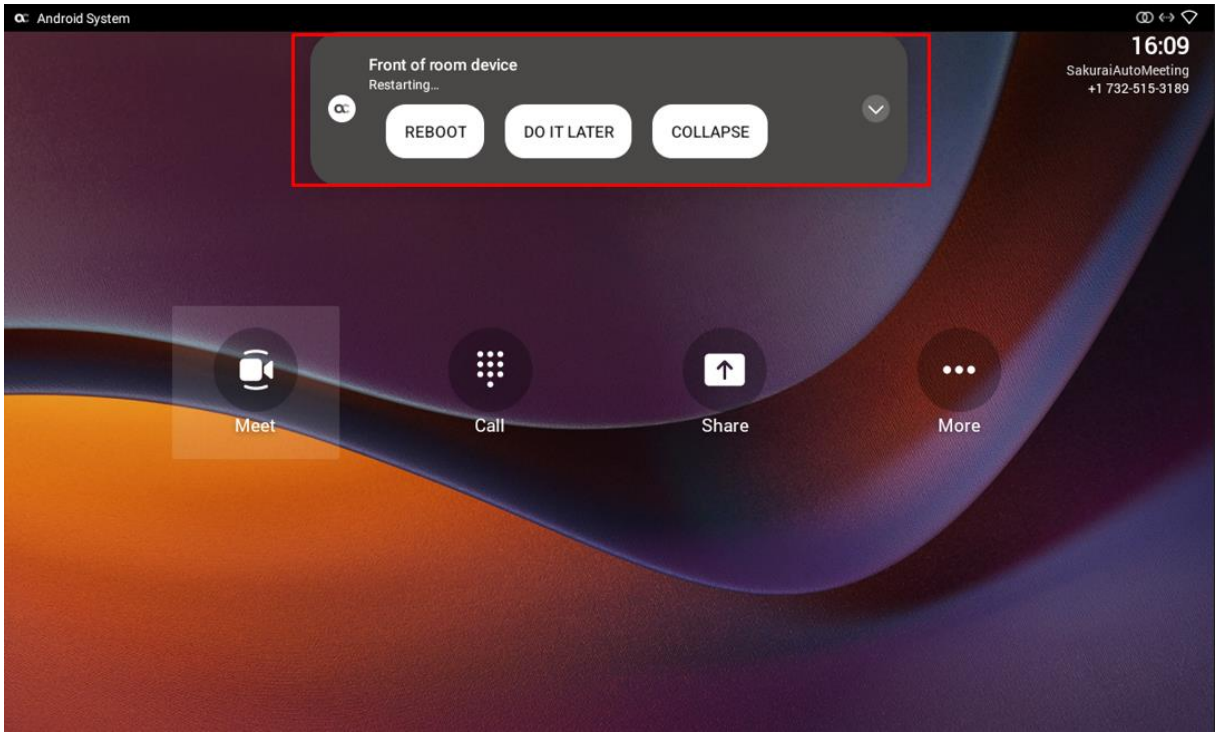
3.1 Managing Notification Messages

Notification messages that pop up on the RXV81 device are seamlessly mirrored in the bundled RX-PAD. When a message pops up in the RXV81 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 notification 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.

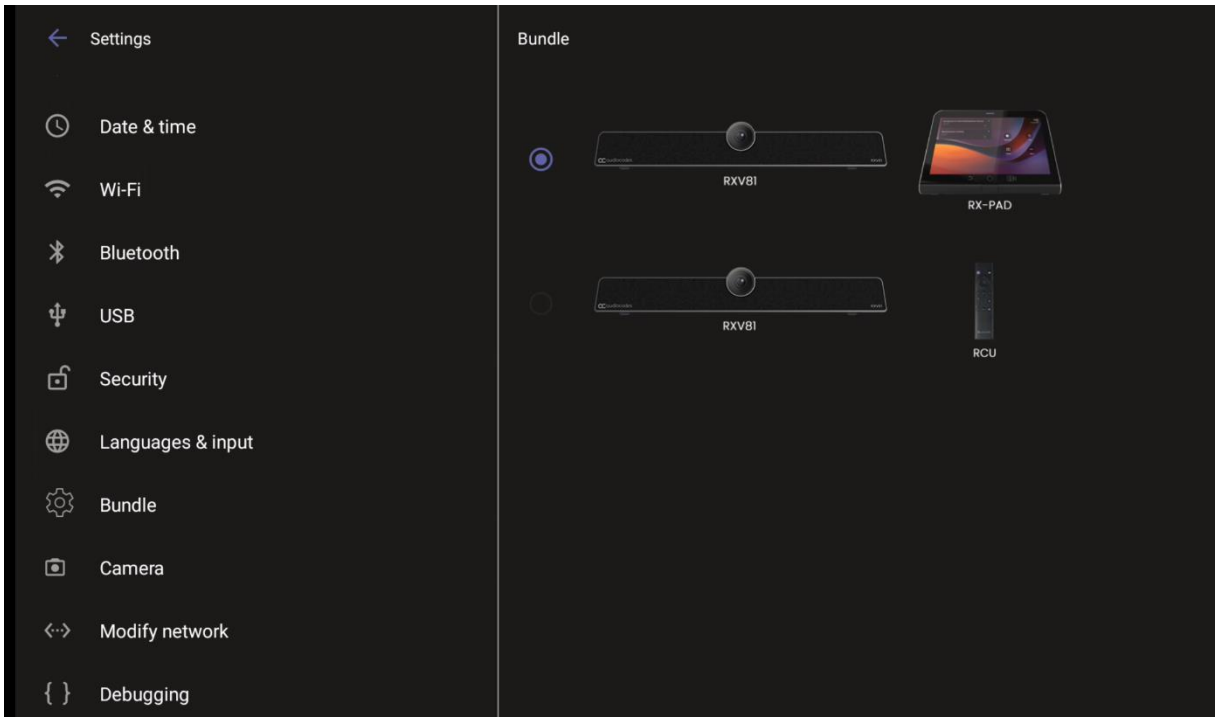


3.2 Configuring a Bundle

Admins can configure an RXV81 bundle. Information about available bundles can be seen here.

➢ **To configure a bundle:**

- Use the RX-PAD Keypad app that controls RXV81 to navigate to the Bundles page. Admin must be logged in to access the page.



3.3 Modifying RXV81 Camera Settings

You can modify RXV81 Camera Settings relating to the look and feel of the video user interface, to suit your preferences.

➢ **To access RXV81 Camera Settings:**

- On the RCU, long-press the camera icon
- In RX-PAD, long-press the camera icon on the device.

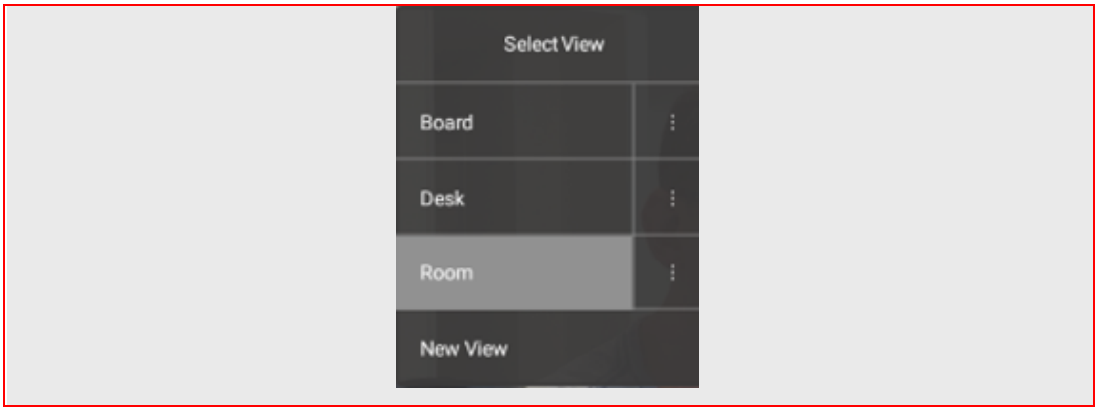
Figure 3-2: RXV81 Camera Settings when using RCU (not RX-PAD)

Note:

- During a call, *all users* who are signed into RXV81 – Admins *and* personal users - can change **Camera settings**, including the presets. All have the permissions required to do so. When the call ends, RXV81 reverts to its preconfigured presets.
- Using a Teams shared account, only the Admin can access **Camera Settings** in idle and edit camera presets; the user can only move between the defined presets during a video call/meeting. The user can change **Camera Settings** during the meeting but the changes are not saved.
- Changing camera settings during a meeting can be done without turning off the video to remote parties.
- The option to access **Camera settings** from RXV81's **Device Settings** still exists; administrator permissions will be required in this case.

- The **Camera settings** option allows saving different camera settings to be used in a video call so that users can switch easily between predefined camera settings (camera presets) per user requirements in the call.

Note: Users can toggle between the presets, a convenient way to move from one preset to another, to view each preset and to reconfigure a preset. Click the **Camera Views** option and in the **Select View** menu that opens, choose the required preset.



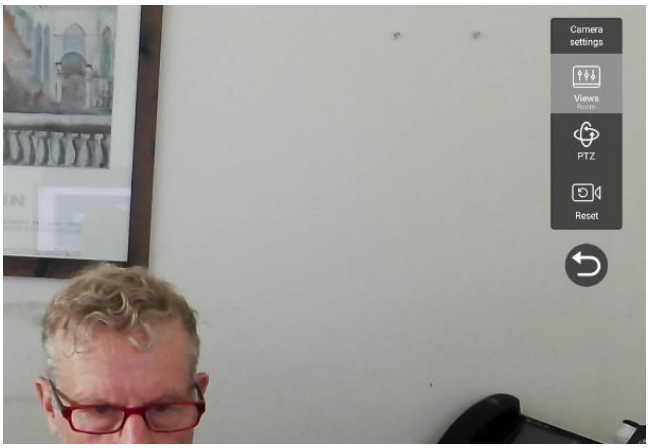
- For example, if a preset is configured to zoom in and focus on the whiteboard in a room, users in a video call/meeting can switch to it and later switch back to the full room preset or any other predefined preset. It's recommended to have a few presets configured for locations frequently zoomed in and focused on:
  - **Full room view** to capture all participants and action in a meeting room
  - **Presenter or single user / desk view** to focus on a single user in the room, usually the presenter
  - **Whiteboard view** if there's a whiteboard in the room
  - **Sunlight or dark modes** if direct sunlight enters the room at specific times of the day/year

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

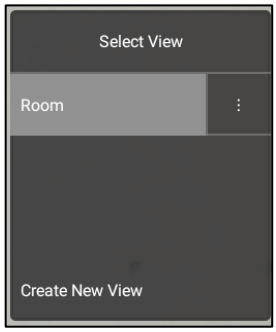
➢ **To add a camera preset when in idle mode:**

1. Long-press the camera button to access **Camera settings**.

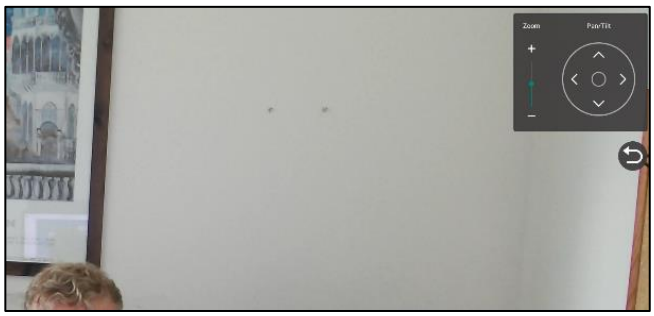
Figure 3-3: Camera settings



2. Navigate to and select **Views** to create a view; you can create up to three views.



3. Navigate to and select **PTZ** to define pan, tilt, and zoom settings for each view.



4. Navigate to and select **Reset** for the camera settings to return to their defaults.

3.4 Starting a New Meeting

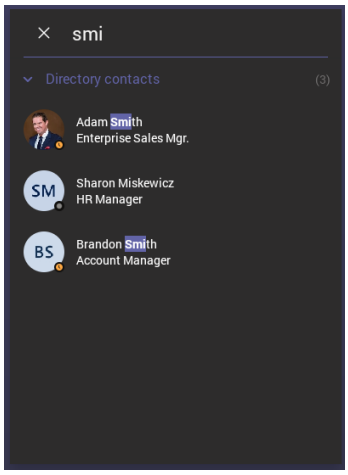
➢ **To start a new meeting:**

1. In the home screen, navigate to and select the **Meet Now** option.

Figure 3-4: New meeting – Invite someone

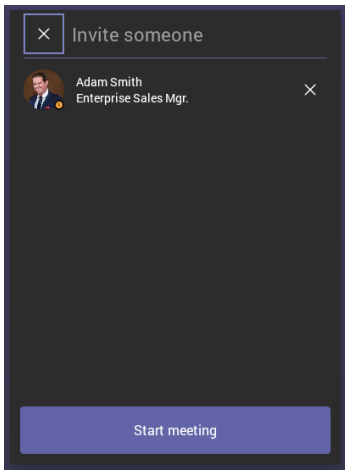
2. In the 'Invite someone' field, enter the name of a person to invite; after entering the first letters in the name, matching contacts from directory are displayed.

Figure 3-5: New meeting – Enter the name of a person



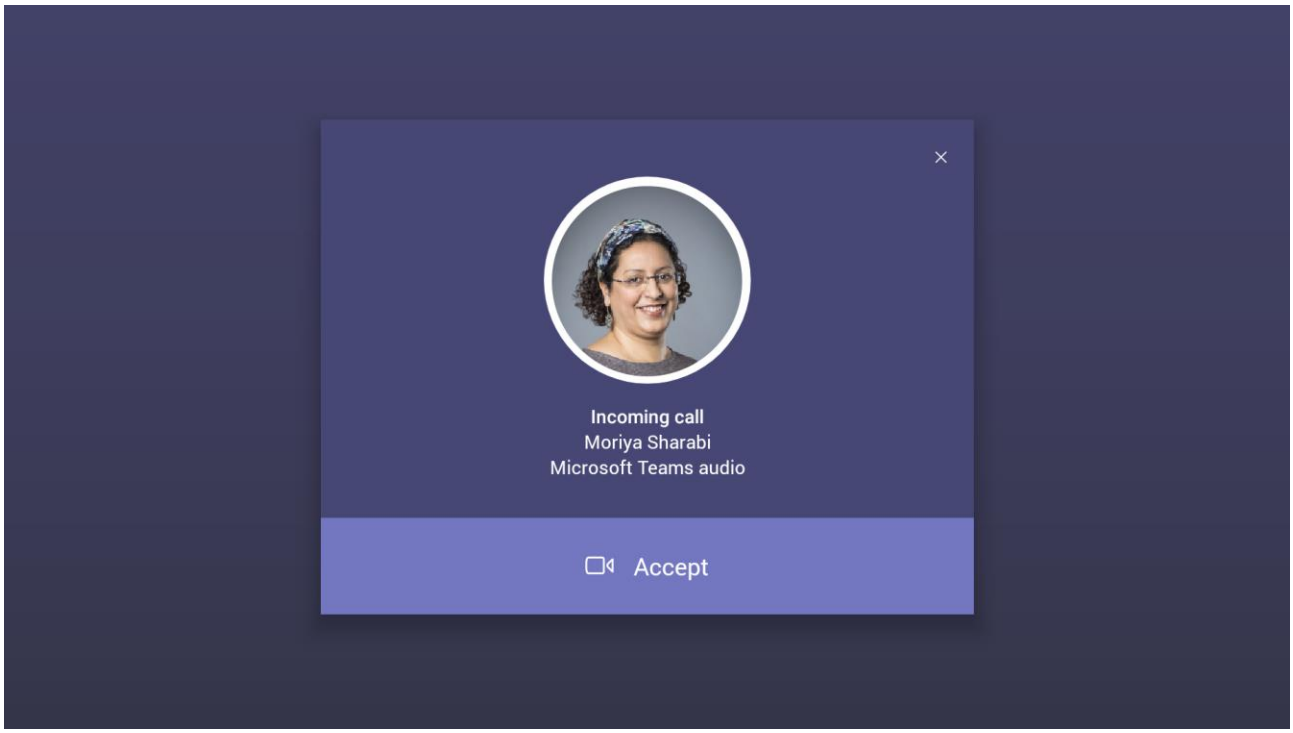
3. Select the name of the person to invite.

Figure 3-6: New meeting – Select the name of a person

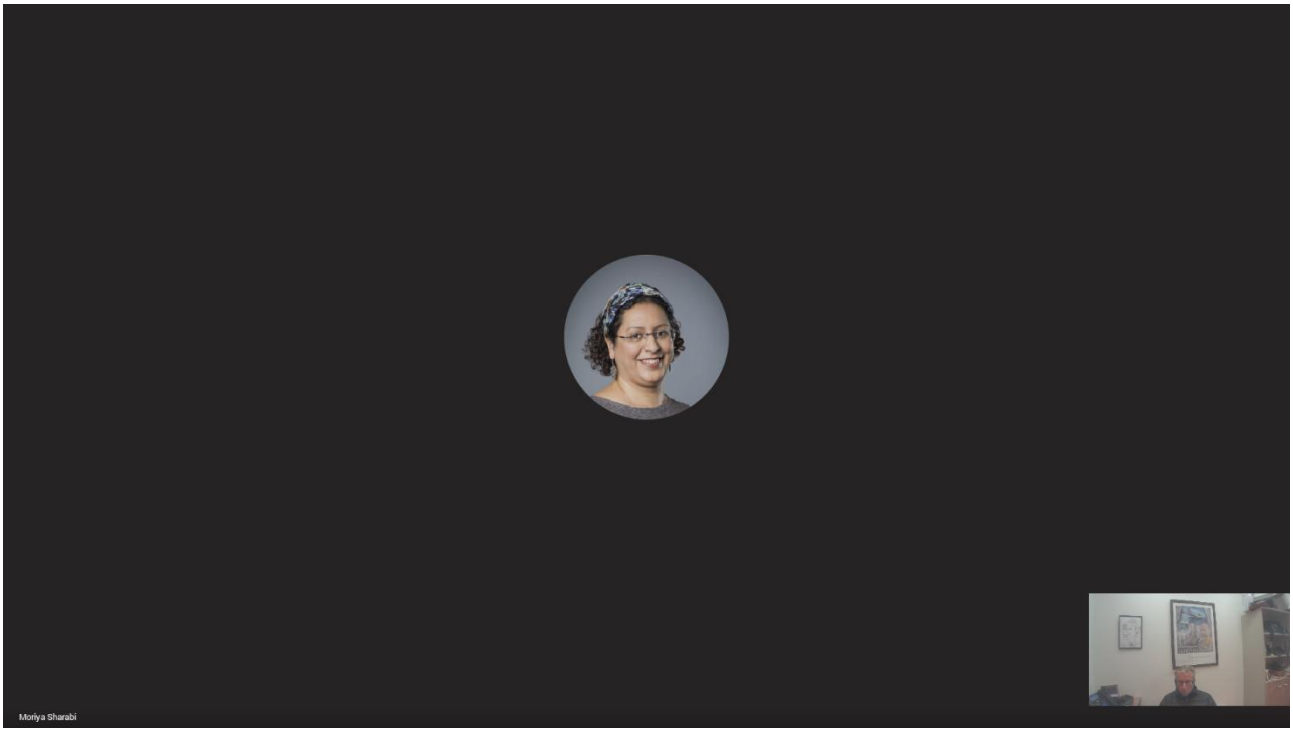


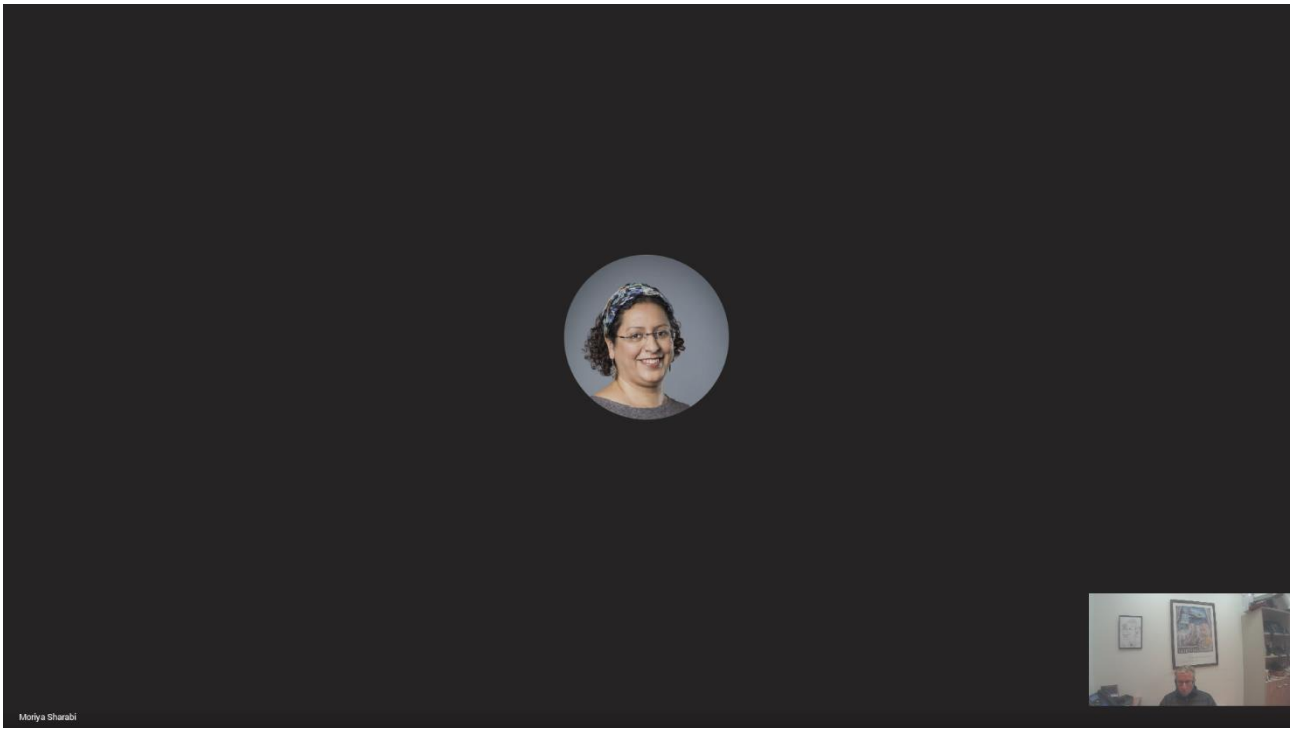
4. Invite someone else – or others – and then select **Start meeting**.

Note: The server allocates a meeting ID number and sends an invite message to all participant devices. All devices simultaneously indicate an incoming call (the 'Calling' screen is displayed). The server manages every aspect of the call.



5. Select **Accept**. Note that according to the icon in the 'Incoming call' screen shown in the preceding figure, the caller has video capability.


Moriya Sharabi


Moriya Sharabi

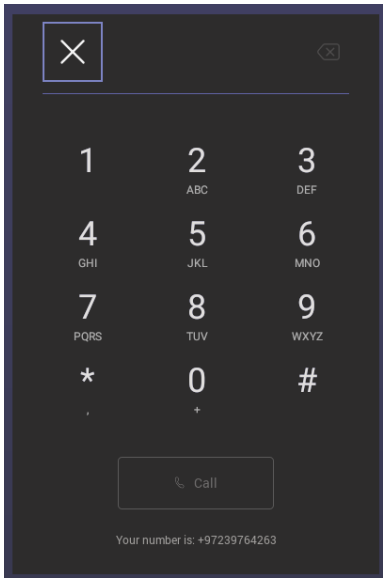
3.5 Dialing a Number

You can manually dial someone's phone number.

➢ **To dial a phone number:**

1. In the home screen, navigate to and select the **Dial pad** option.

Figure 3-7: Dial pad

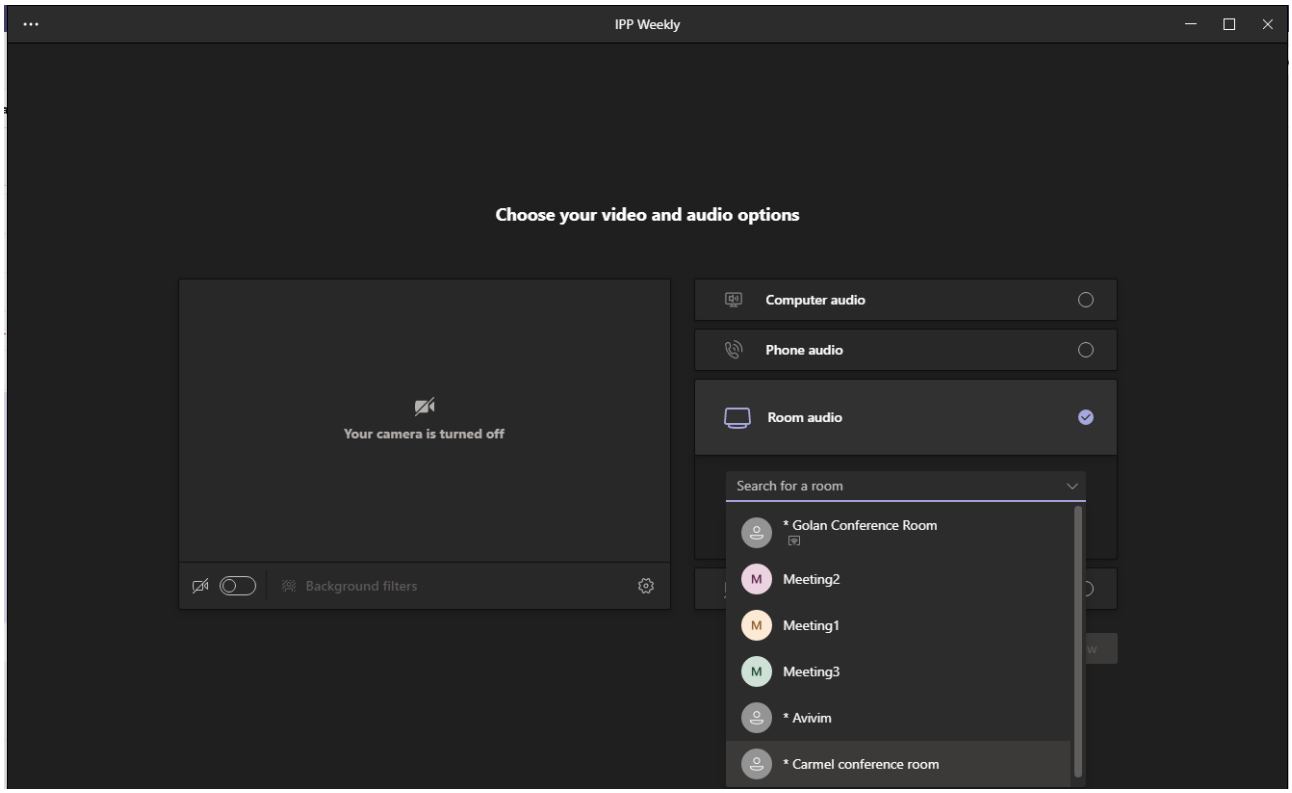


2. Enter the digits of the destination to call and select **Call**.

3.6 Enabling Proximity Join

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

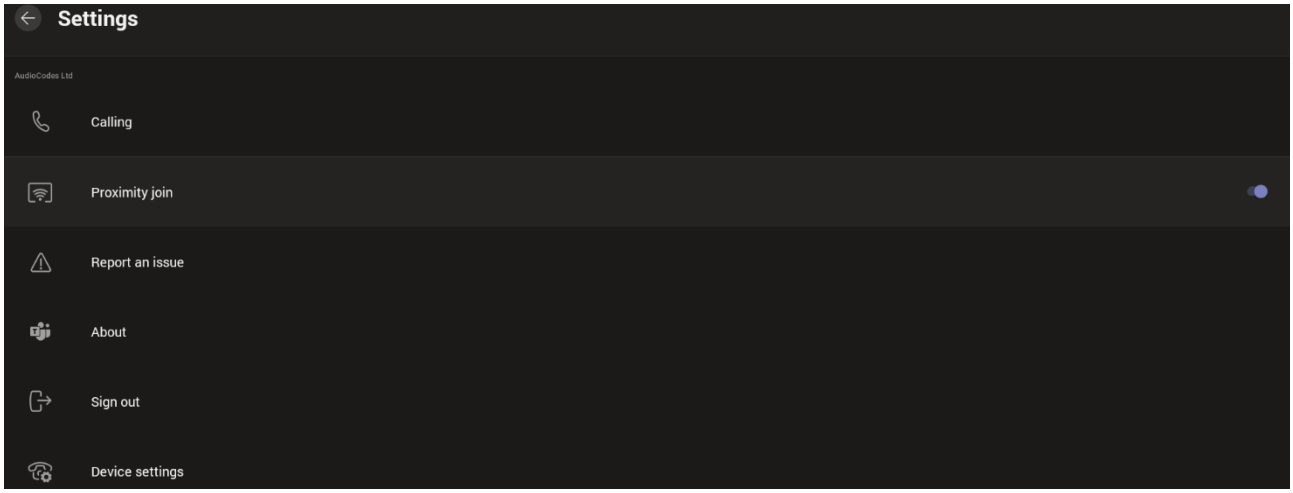
The feature functions in combination with Bluetooth and 'Bluetooth Beaconing', an integral feature in Microsoft Teams Rooms (MTRs). The MTR device is RXV81. If you bring a laptop or a Teams Mobile Client near RXV81, it'll offer RXV81 as the room audio device. The figure below shows how to select the room audio device.



After you select the room audio device, the meeting is opened without any audio device on your PC client, and then the room meeting device (RXV81) gets a request to join the meeting.

➢ To enable 'Proximity join':

- In the Settings screen, navigate to and select **Proximity join**. If it's disabled, it'll become enabled and vice versa.

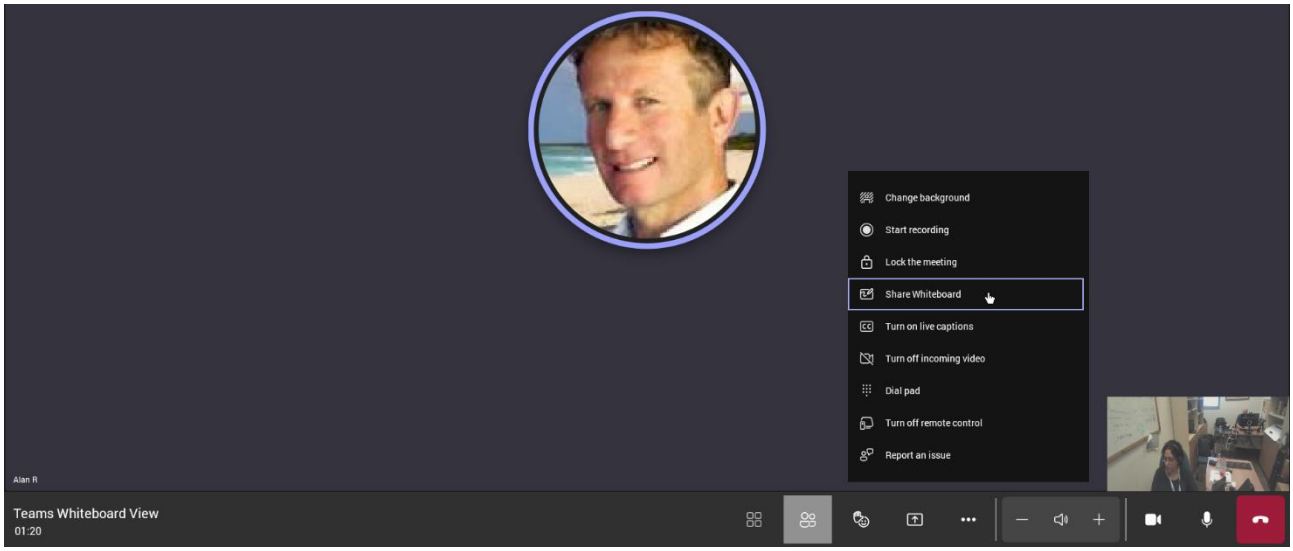


3.7 Sharing a Whiteboard

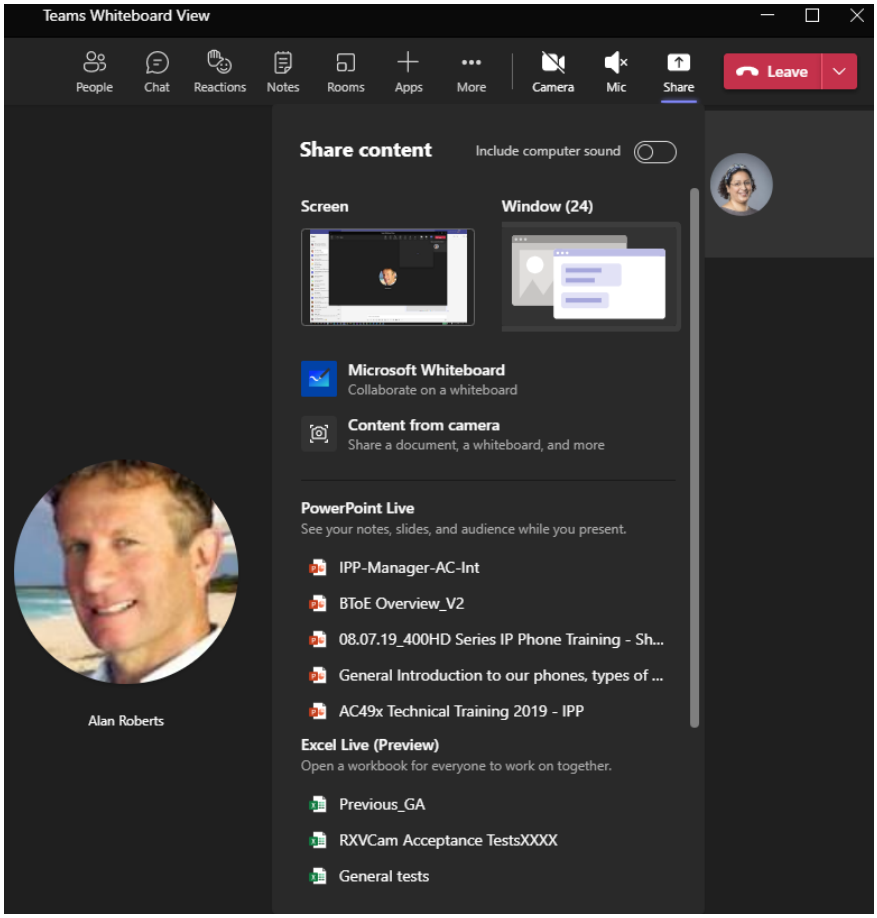
Teams meetings on RXV81 allow participants to open a virtual whiteboard – a digital canvas - on which they can sketch, illustrate, collaborate, brainstorm, plan, and share perspectives with one another in real time. The focus switches away from the presenting participant to the whiteboard. For more information about this Microsoft feature, see here.

➢ **To share the Whiteboard:**

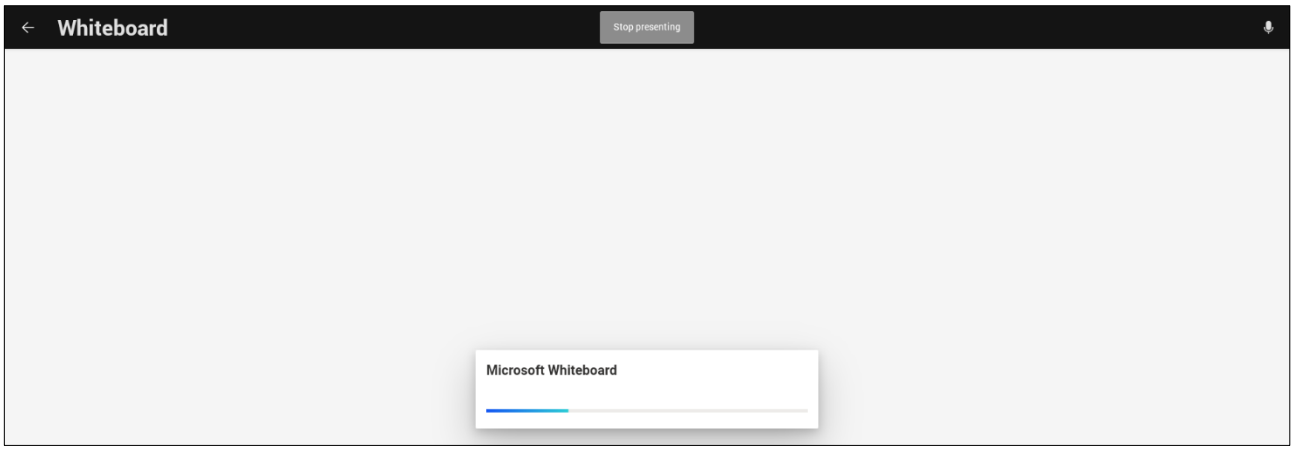
1. From the Settings menu, select **Share Whiteboard**.



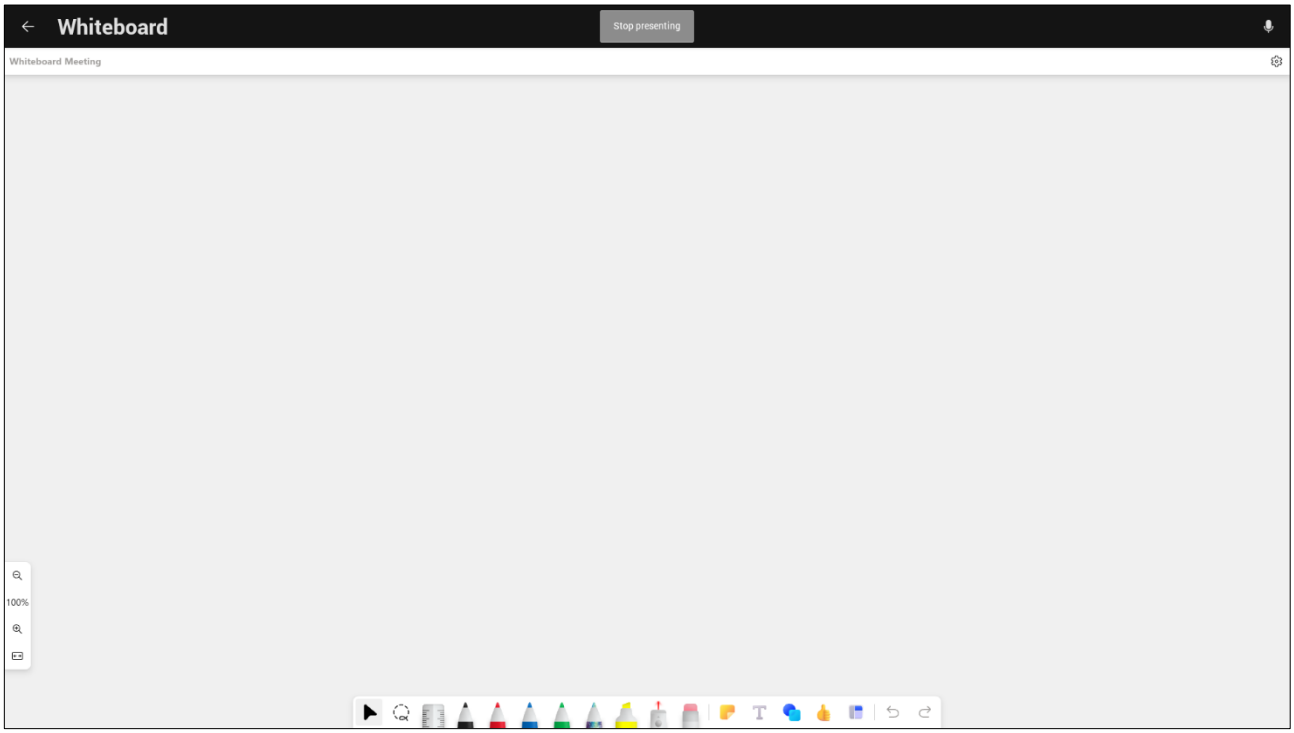
2. Alternatively, access the Whiteboard from **Share content**:



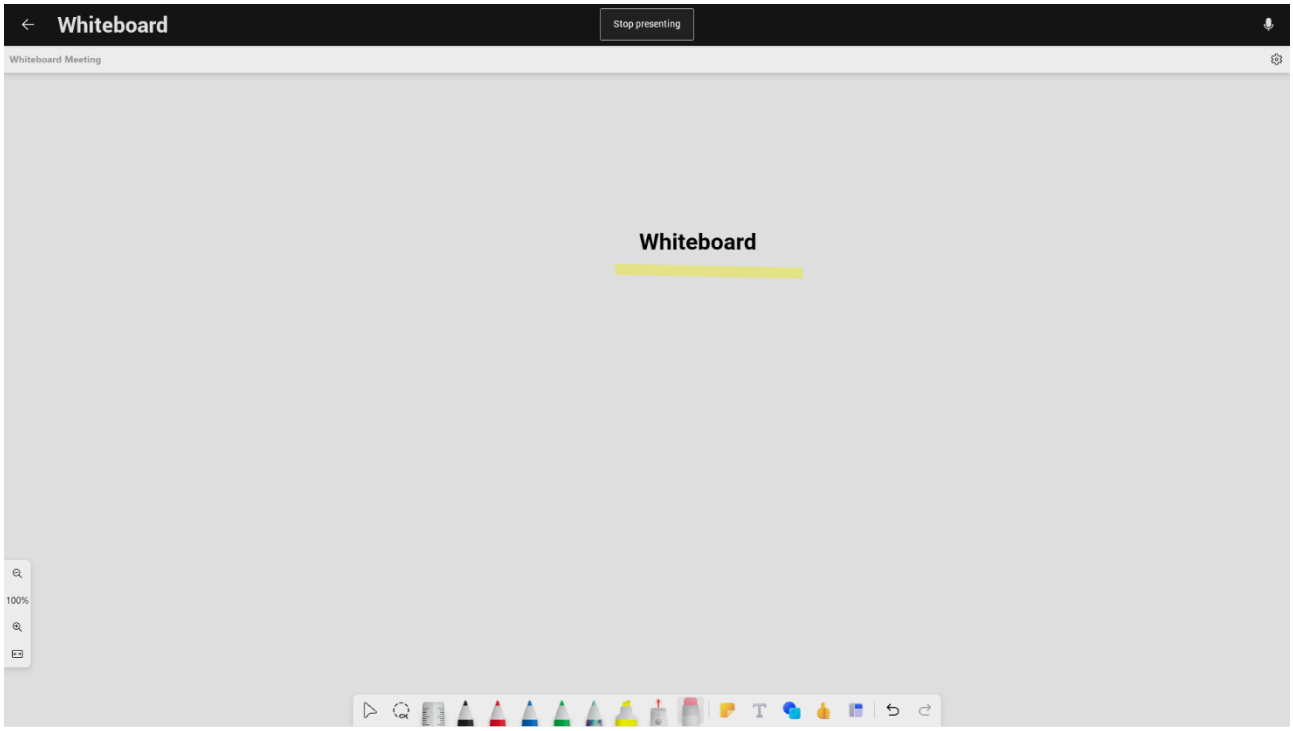
3. View the following Microsoft Whiteboard initializing indication:



4. View the Whiteboard in the Teams desktop application or in Teams client:



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



3.8 Screen Sharing

RXV81 enables users to share their PC screen via the RX-PAD HDMI In port. The feature extends HDMI In functionality.

Note:

- A short HDMI cable connects the PC/laptop to the RX-PAD HDMI In port.
- The connection between RX-PAD and RXV81 is thus 'cableless'.

Two modes are available:

- 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.

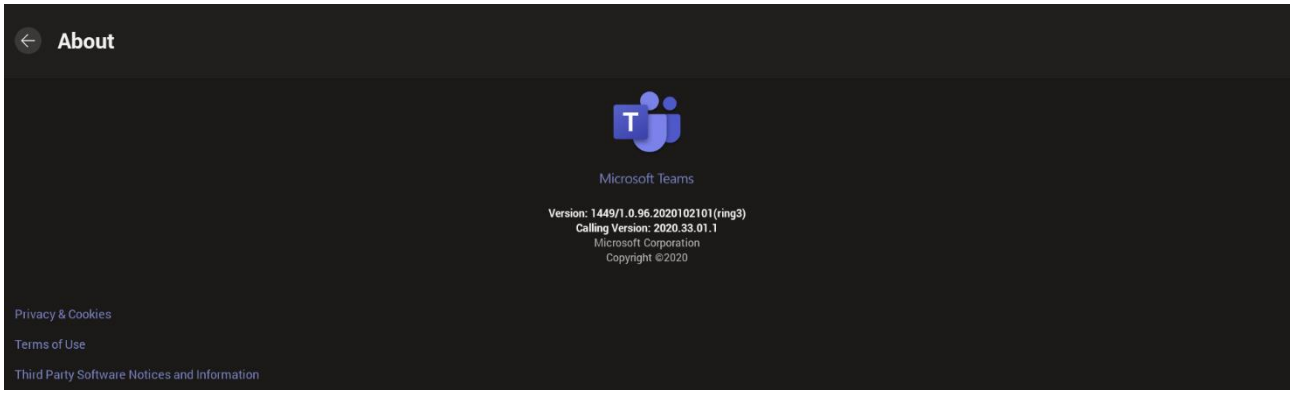
To enable utilization of this feature, make sure the following is permitted in the organization's firewall settings:

- 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

3.9 About Microsoft Teams

Information about the Microsoft Teams application can be viewed by navigating to and selecting the Settings screen's **About** option shown in the preceding figure.



3.10 Signing out

You can sign out of the application as one user and optionally sign in again as another.

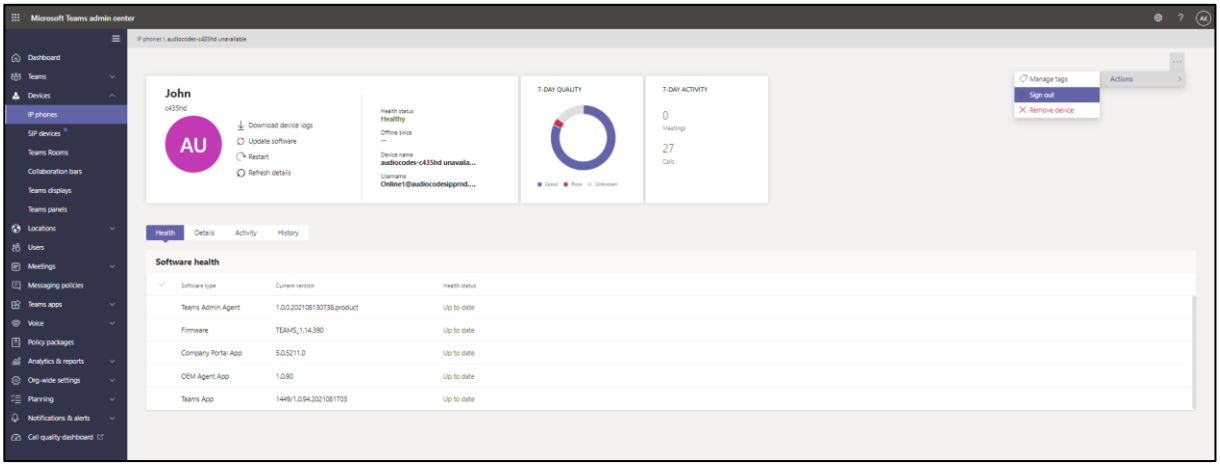
➢ **To sign out:**

- Navigate to **Teams admin settings** > **Teams sign out** and confirm in the prompt below.

Optionally, remote sign-out can be performed from Microsoft Teams admin center (TAC). Admins can provision RXV81 from the TAC, remotely sign in, and also sign out.

➢ **To sign out of RXV81 using Microsoft TAC:**

- Navigate to the TAC screen shown in the figure below and from the ⋯ menu located in the uppermost right corner of the screen, select **Actions** and then **Sign out**.



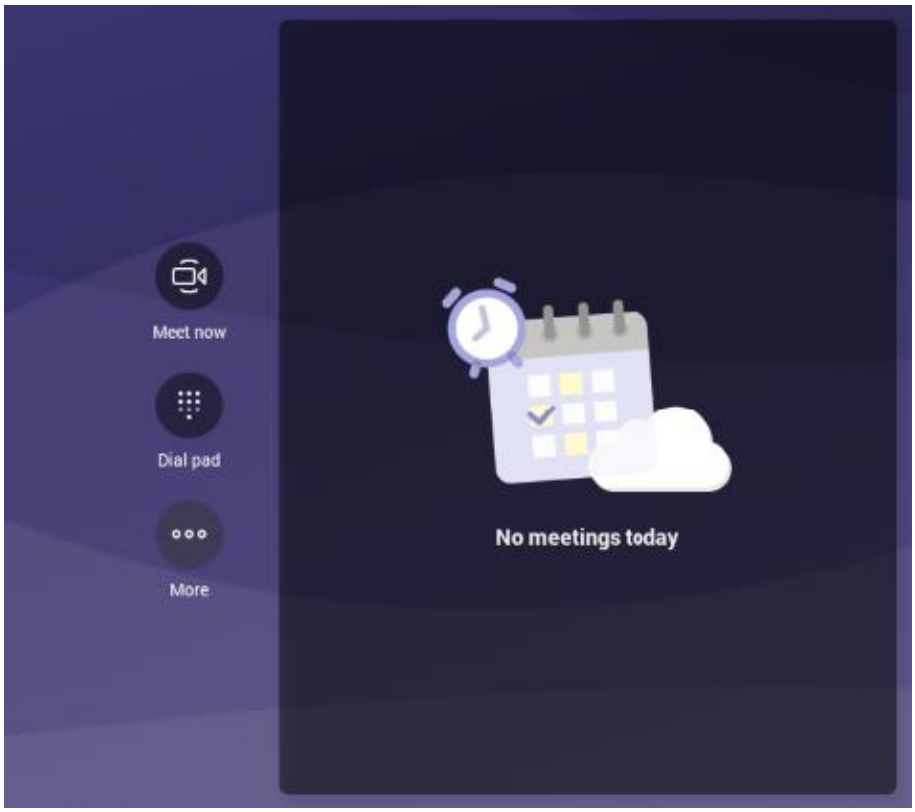
This page is intentionally left blank.

4 Configuring RXV81 Settings

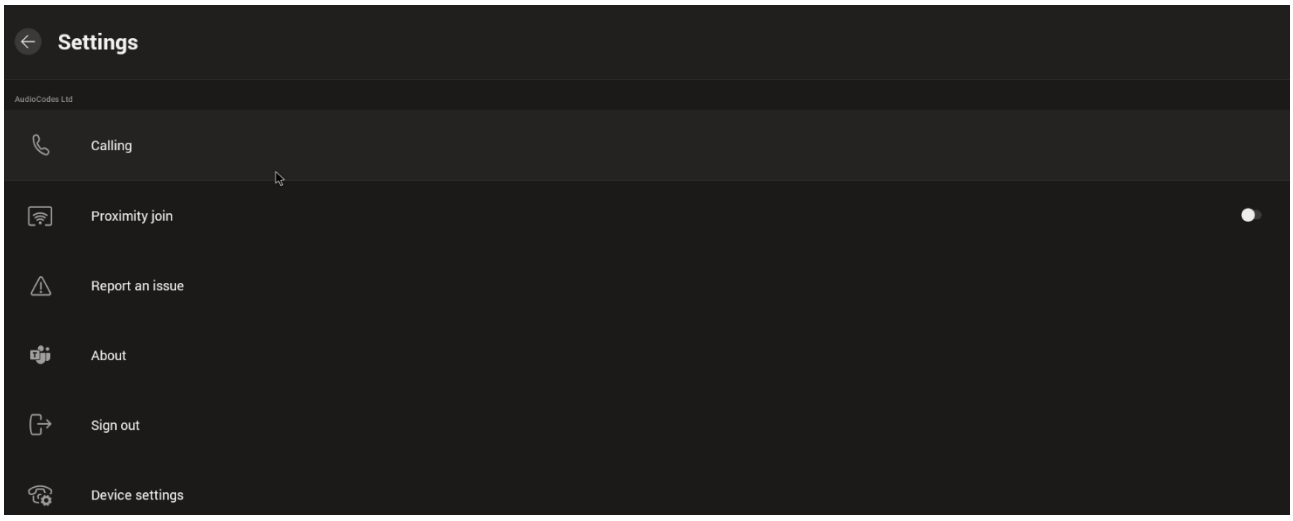
The section familiarizes you with RXV81's settings. RXV81s are delivered configured with their default settings. Customers can customize them to suit enterprise requirements.

➢ **To access device settings:**

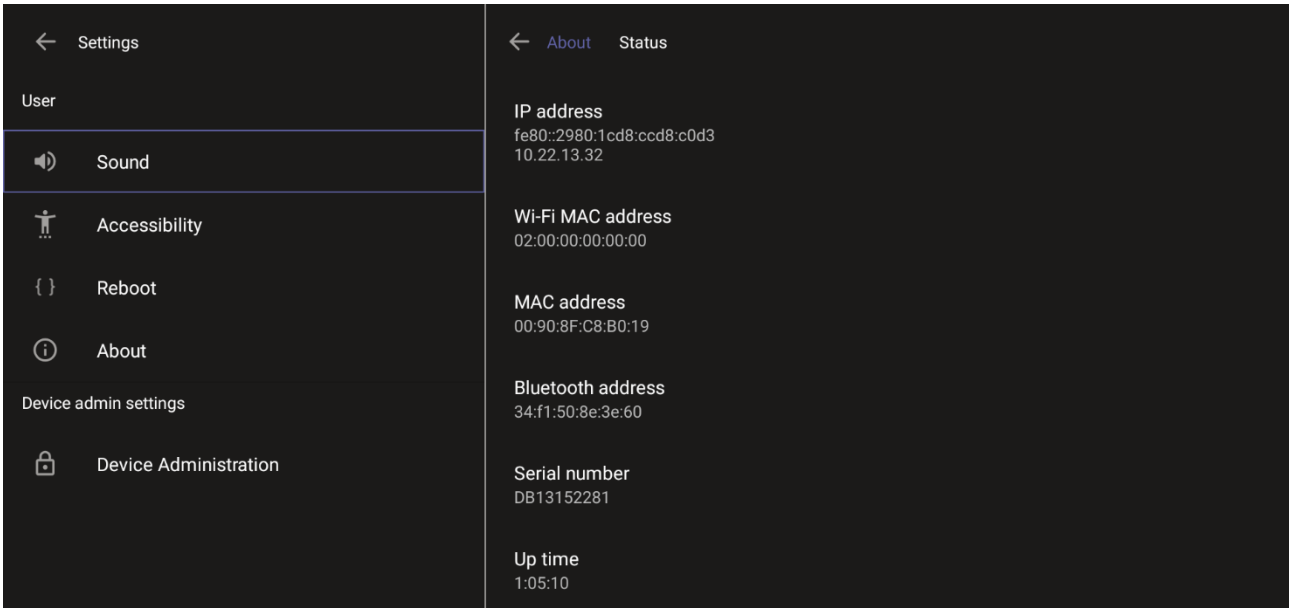
1. In the home screen, navigate to and select the **More** option.



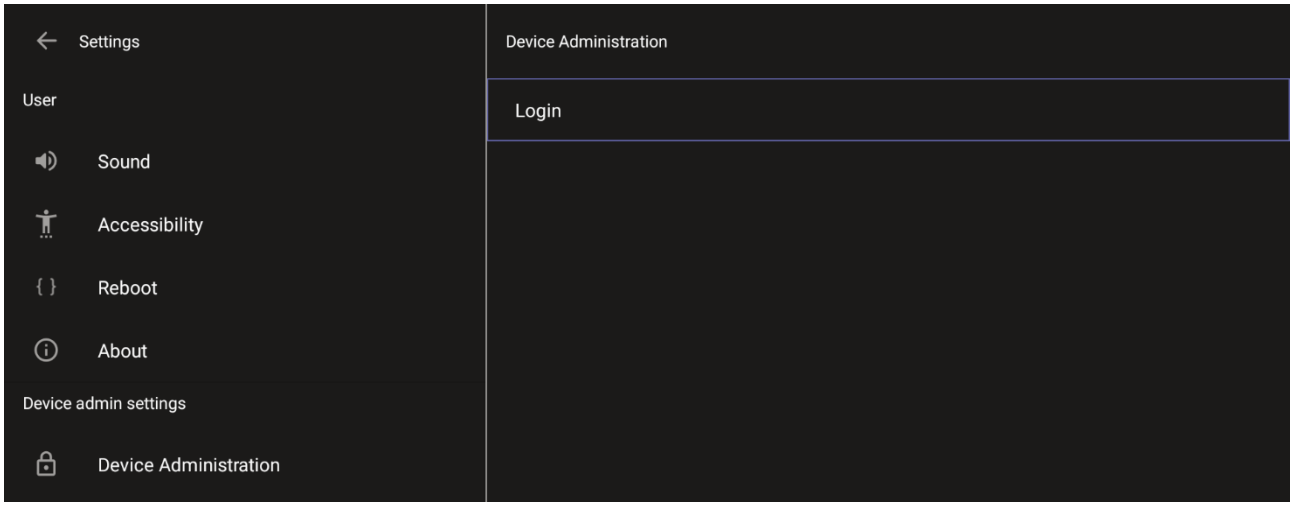
2. Navigate to and select **Settings**.



3. Navigate to and select **Device settings**.



4. Navigate to and select **Device Administration**.



5. Log in as administrator.

Note: Logging in as Administrator is required for debugging options. It's password protected. Default: **1234**. After logging in as Admin, you can log out | change password.

6. Select **Login**.

7. Enter the password (**1234**) in the 'Enter password' field; use the virtual keyboard to enter the password.

Note: The virtual keyboard pops up for all 'Settings' fields to allow inputting characters and / or numbers. Two virtual keyboard types can be displayed: Numeric or QWERTY.

8. Select **OK**; you're prompted to change password.

Note:

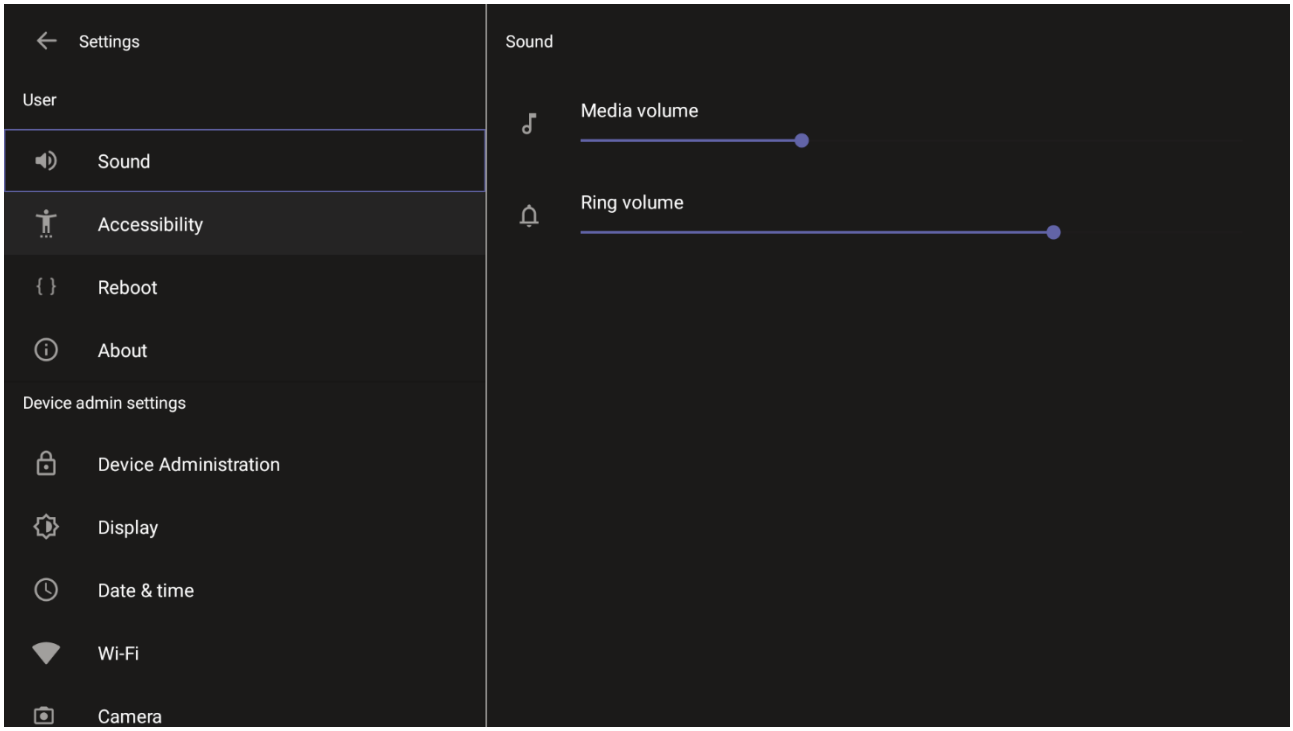
- The default password must be changed before access to the device via SSH is allowed.
- The default password can be changed per device from the GUI, or via bulk configuration of multiple devices using Microsoft's TAC or AudioCodes' Device Manager.

9. Enter a password; you're prompted to verify the password you entered. Criteria required for a strong password are provided (for strengthened security) in order to Log in as Administrator:
   - The password length must be greater than or equal to 8.
   - The password must contain one or more uppercase characters.
   - The password must contain one or more lowercase characters.
   - The password must contain one or more numeric values.
   - The password must contain one or more special characters.

Note: These virtual keyboards are also displayed when the admin needs to enter an IP address to debug, or when they need to enter their PIN lock for the security setting.

After logging in, the Settings screen now also displays the settings under the section 'Device admin settings'.

10. Click **OK**; the Settings screen now also displays 'Device admin settings', in addition to the 'User' settings.



4.1 Device Admin Settings

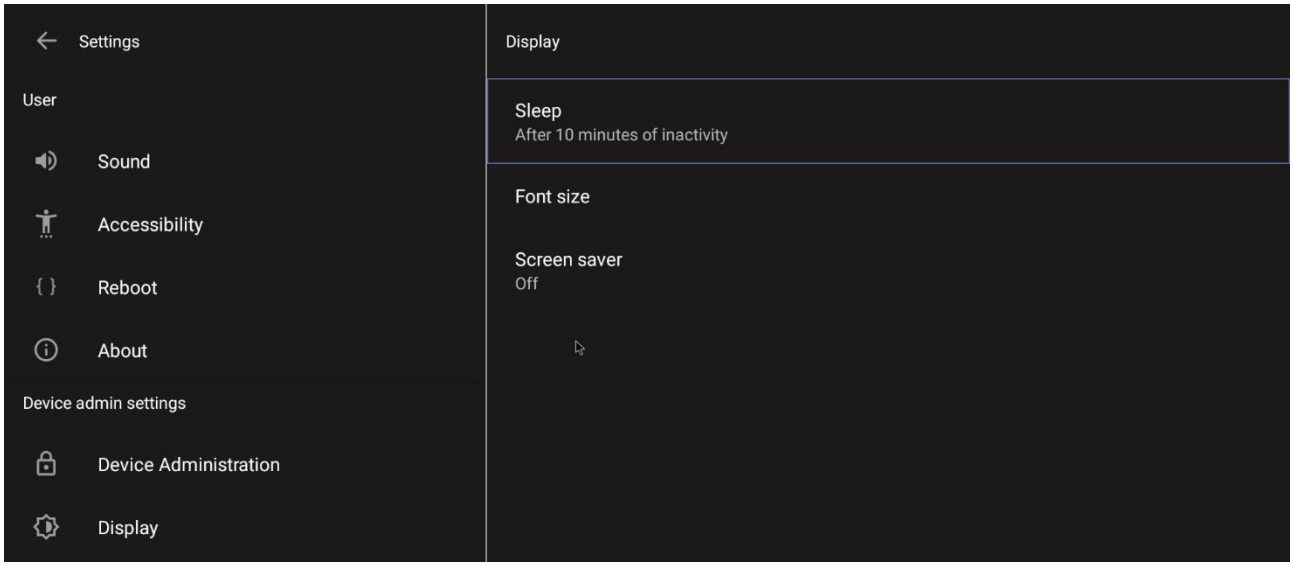
After logging in as Device Administration as shown in the previous section, you can configure Device Administration settings: Display, Date & Time, Wi-Fi, Camera.

4.1.1 Configuring Display

Modify these settings to suit your preferences related to the look and feel of the user interface.

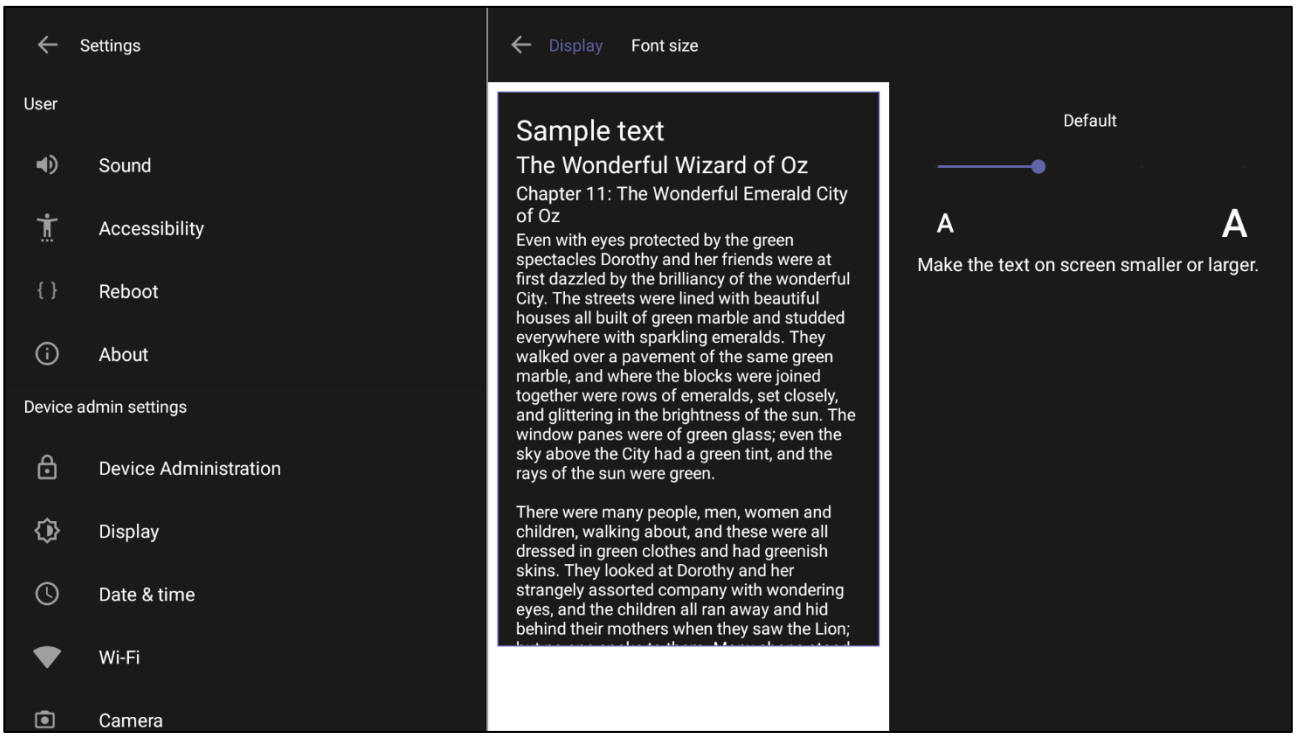
➢ **To configure Display settings:**

1. Under 'Device admin settings', navigate to and select **Display**.



2. Under 'Display', navigate to and select **Sleep**.

3. Navigate to and select the time to lapse before the interface 'goes to sleep'. Default: 10 minutes.
4. Navigate to and select **Font size**.



5. Navigate to and select **Screen saver**.

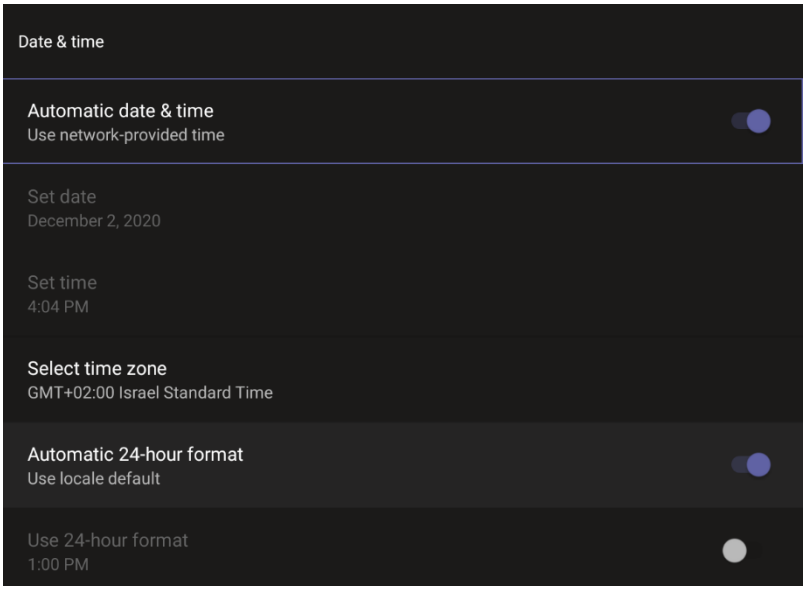
6. Navigate to and select **Off** to switch it on and then choose the screen saver.

4.1.2 Configuring Date & Time

Date and time are automatically retrieved from the deployed Network Time Protocol (NTP) server.

➢ **To configure Date & Time:**

1. Under 'Device admin settings', navigate to and select **Date & Time**.



2. Navigate to and select **Use 24-hour format** [Allows you to select the Time format].

Note: The device automatically detects time zone via geographical location (**Automatic Time Zone Detection**).

4.1.3 Configuring Wi-Fi

RXV81 can connect to an Access Point via Wi-Fi. Network administrators can configure Wi-Fi parameters for RXV81. The parameters are concealed from the user's view. Users can enable | disable Wi-Fi in the device's user interface.

Note: Wi-Fi cannot be enabled | disabled using SSH command.

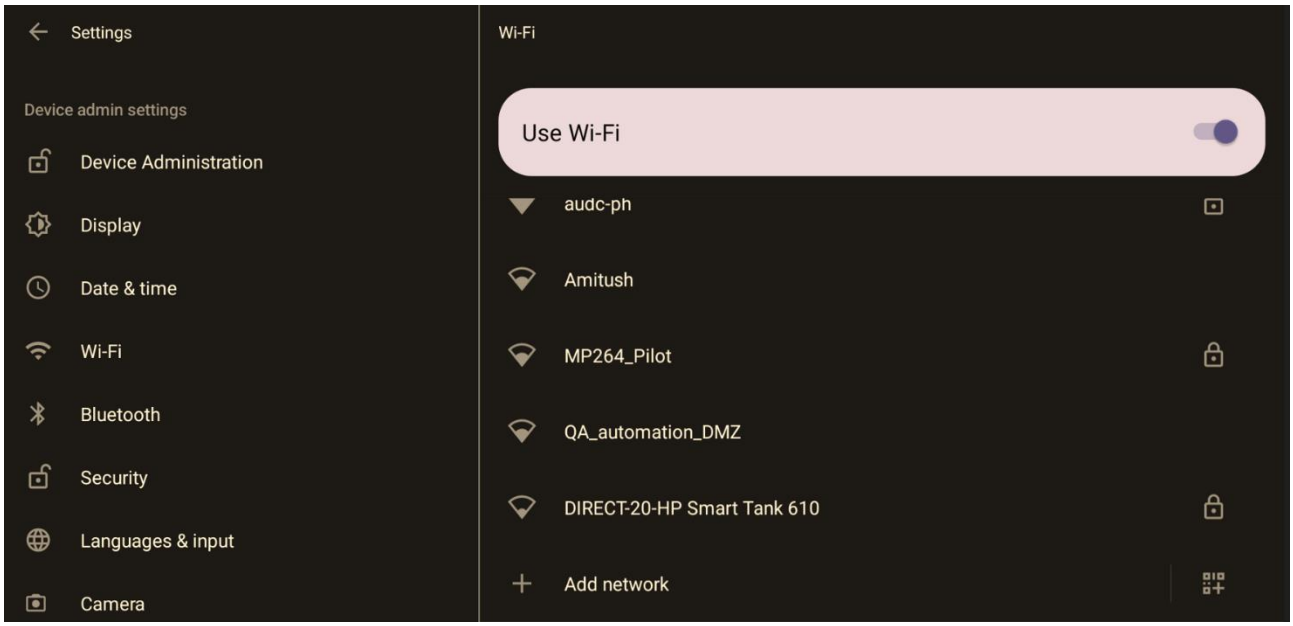
The Wi-Fi connection is transparent to users; which frequency is used, 2.4 GHz or 5 GHz, is made for users by the device; users cannot disable one or the other.

4.1.3.1 Connecting to an Available Wi-Fi Network

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

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

1. Under 'Settings', navigate to **Wi-Fi** and enable **Use Wi-Fi**.



2. View a list of available connections.
3. Select the Wi-Fi network you want and enter the password.
4. View the network you selected 'Connected'.

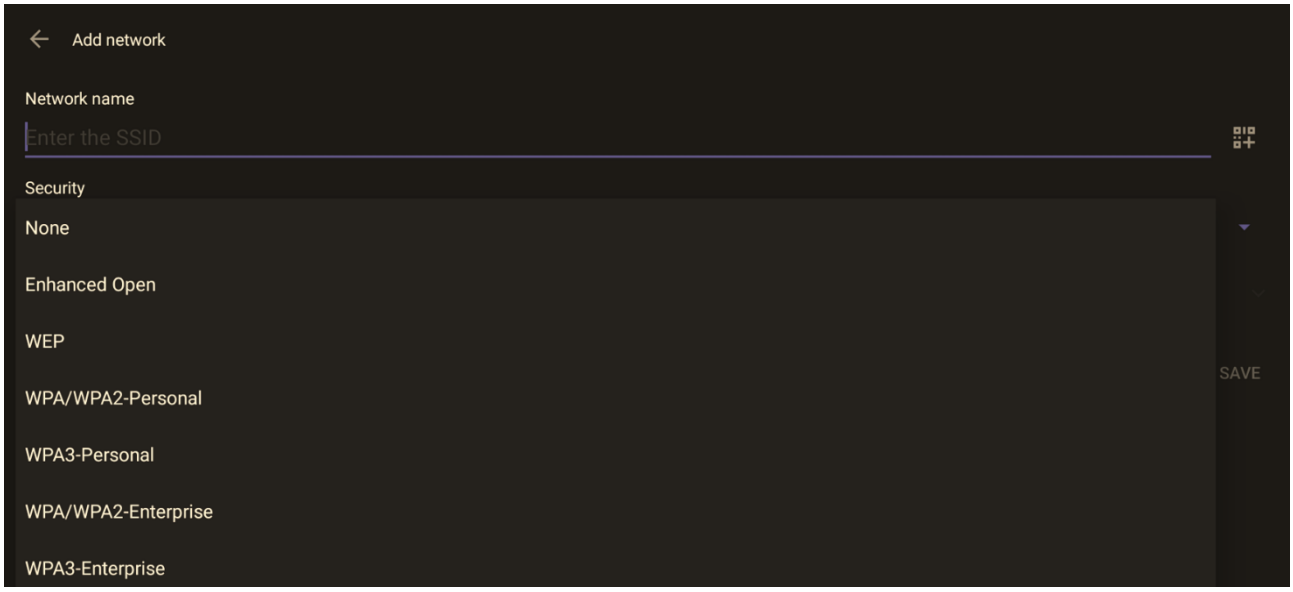
4.1.3.2 Manually Connecting to a Wi-Fi Network

➢ **To manually connect to a Wi-Fi network:**

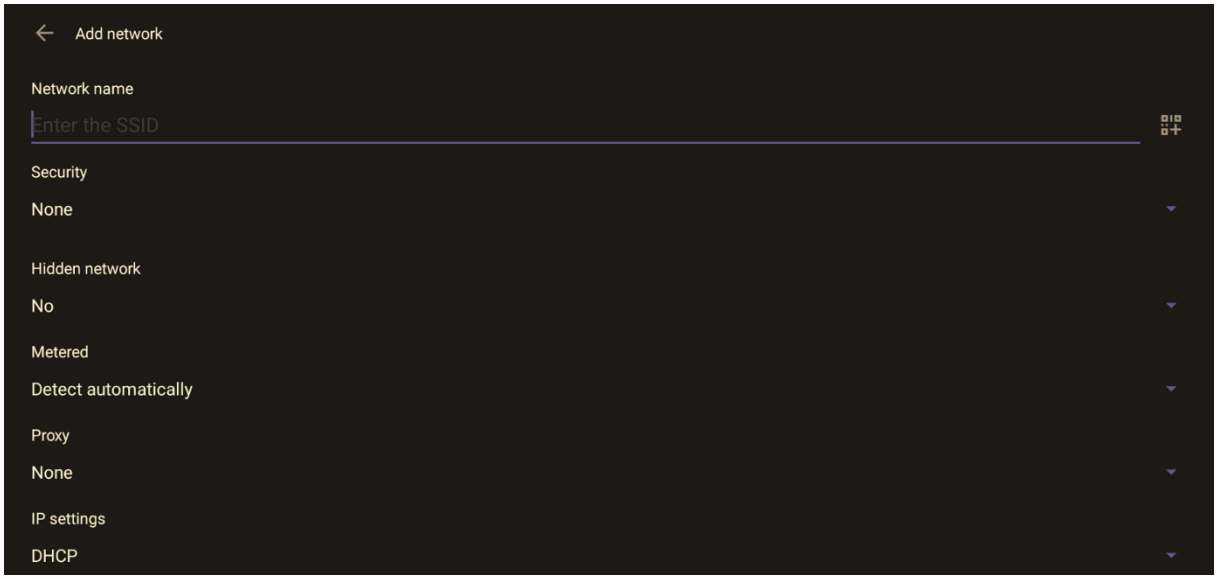
Note: Make sure to first disconnect your Ethernet cable. If it's connected, the device will not be able to connect to a Wi-Fi network.

1. Under **Wi-Fi**, select **Add network** and then enter the SSID of the network to add manually.

2. From the 'Security' drop-down, select a security key strength (encryption method).



3. Optionally meter the selected network. Leave the setting at its default value of **Detect automatically** if you don't want to meter the network. Select a **Metered** option to meter it.



Note:

- 'Proxy' and 'DHCP' will automatically be configured by the network.
- Enabling the setting **Turn on Wi-Fi automatically** allows the device to automatically connect in the future to the highest signal-quality network remembered by the device.
- As an alternative to manually configuring Wi-Fi settings via the device's user interface, you can configure the Wi-Fi settings described in Table 4-1, using the Configuration File.

Table 4-1: Configuration File Wi-Fi Parameters

Parameter	Description
network/wireless/adavanced_ options/dns1	Defines the IP of the wireless DNS1.
network/wireless/adavanced_ options/dns2	Defines the IP of the wireless DNS2.
network/wireless/adavanced_ options/gateway	Defines the IP address of the wireless gateway
network/wireless/adavanced_ options/hidden_network	Defines the name of the wireless hidden network.
network/wireless/adavanced_ options/ip_addr	Defines the IP address of the static Wi-Fi network if you're operating with a static Wi-Fi network.
network/wireless/adavanced_ options/ip_settings	Used to define DHCP.
network/wireless/adavanced_ options/network_prefix_length	Defines the network prefix length to be used.
network/wireless/adavanced_ options/proxy	Defines the proxy wireless server source.
network/wireless/adavanced_ options/proxy/auto_config/pac_url	Defines the URL of the PAC file.
network/wireless/adavanced_ options/proxy/manual/exclusion_list	Defines the list of IP addresses that will be blocked.
network/wireless/adavanced_ options/proxy/manual/proxy_ hostname	Defines the name of the proxy host.

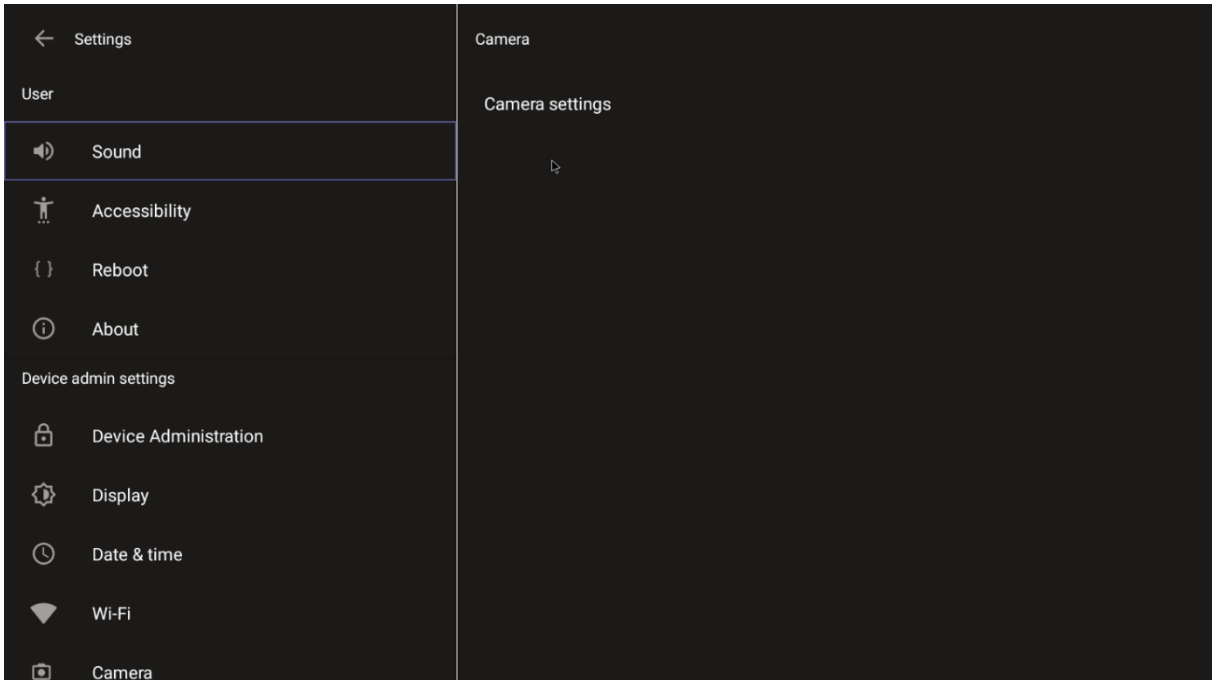
Parameter	Description
network/wireless/adavanced_ options/proxy/manual/proxy_port	Defines the proxy port.
network/wireless/anon_identity	Defines the anonymous wireless users who won't be seen.
network/wireless/ca_cert	Defines which CA certificate to use.
network/wireless/client_cert	Defines which client certificate to use.
network/wireless/domain	Defines the domain name.
network/wireless/eap_method	Defines the EAP method.
network/wireless/identity	Defines the identity of the user.
network/wireless/password	Defines the password of the network.
network/wireless/phase2_method NONE,MSCHAPV2,GTC,PAP,MSCHAP	Defines the encryption method. Phase 2 applies only to the 802.1x EAP method.
network/wireless/security	Defines the security method (encryption protocol).

4.1.4 Configuring Camera Settings

Settings controlling the look and feel of the video UI can be set to suit individual preferences.

➢ **To configure Camera settings:**

1. Under 'Device admin settings', navigate to and select **Camera**.



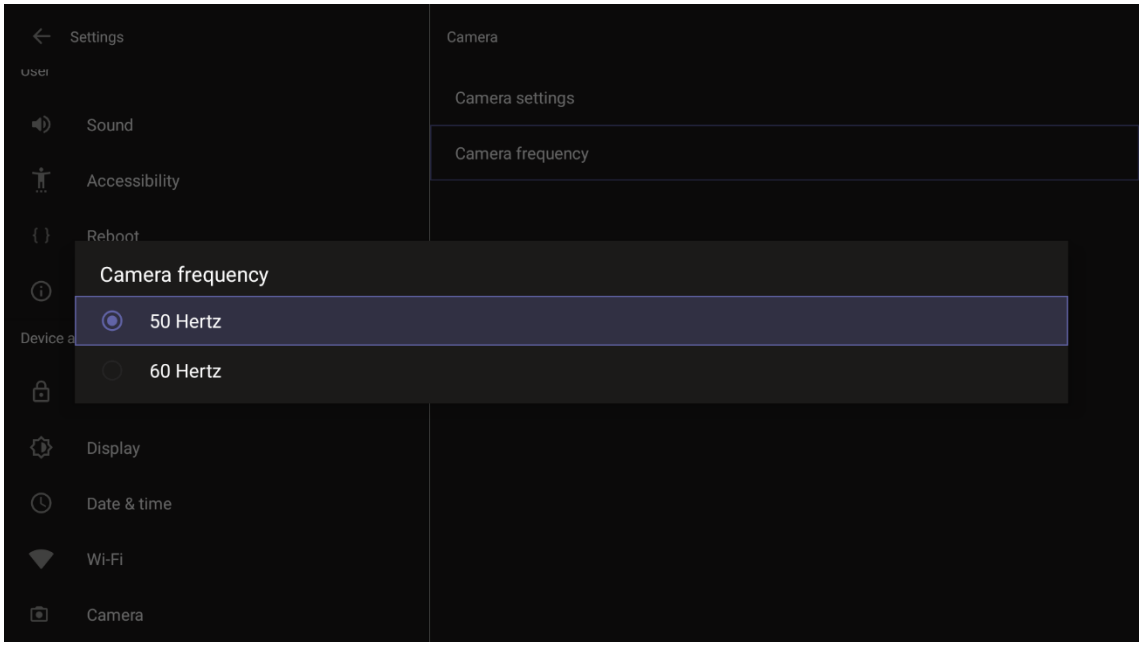
2. Navigate to and select **Camera settings**; the video stream is played and the following is displayed on the right side of the screen:

3. Create and edit presets using PTZ control.

4.1.4.1 Configuring Camera Frequency

The **Camera frequency** (under **Device settings**) must be set per the power supply as follows:

- 110V – 60Hz
- 220V – 50Hz



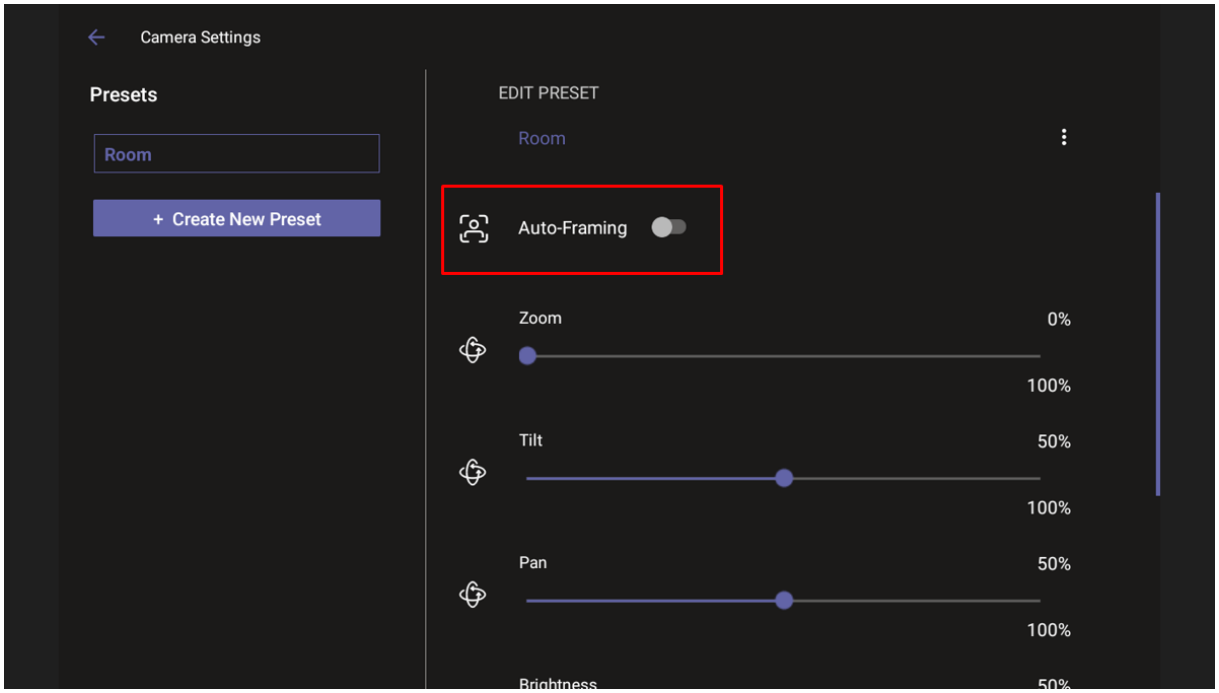
4.1.5 Auto Framing

An Auto-Framing option is available under Camera Settings.

- To enable Auto-Framing on RXV81 paired with RX-PAD, use the camera hard key to access the Camera Settings page.
- For RXV81 paired with the Remote Controller unit (RCU), long-press the RCU's camera button to access the Camera Settings page.

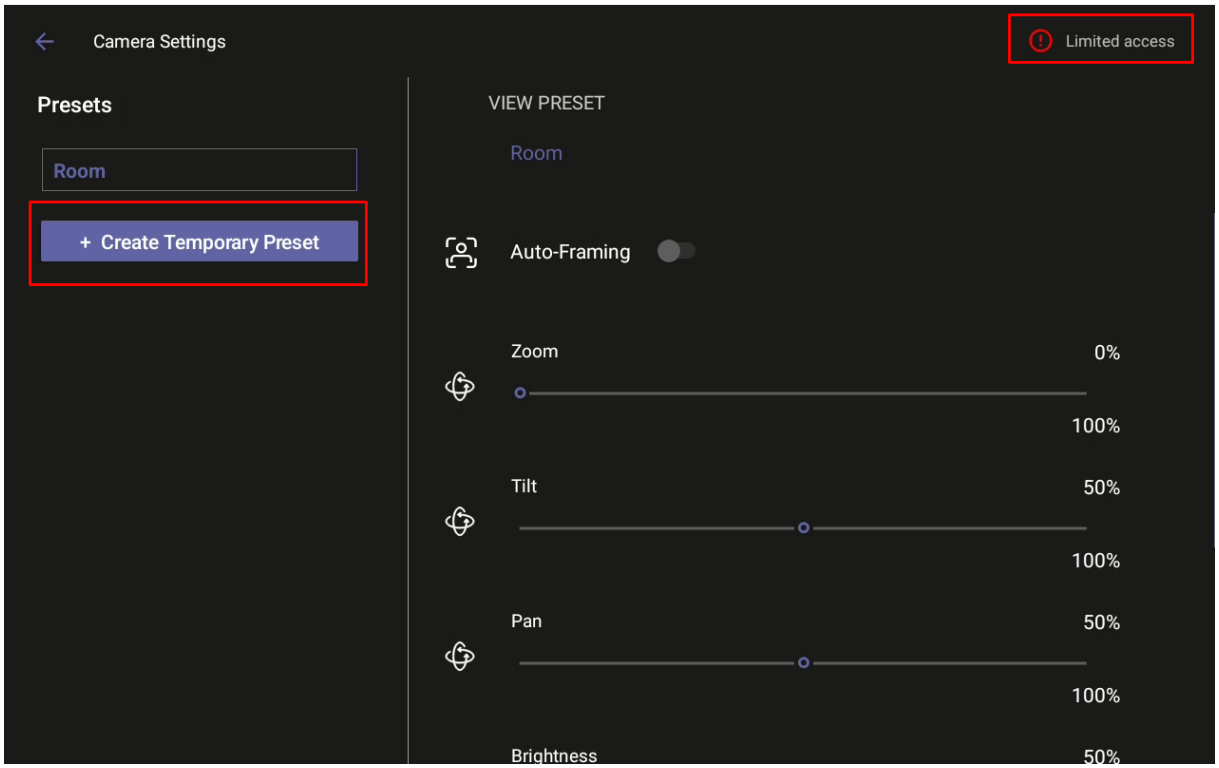
Note:

- 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.

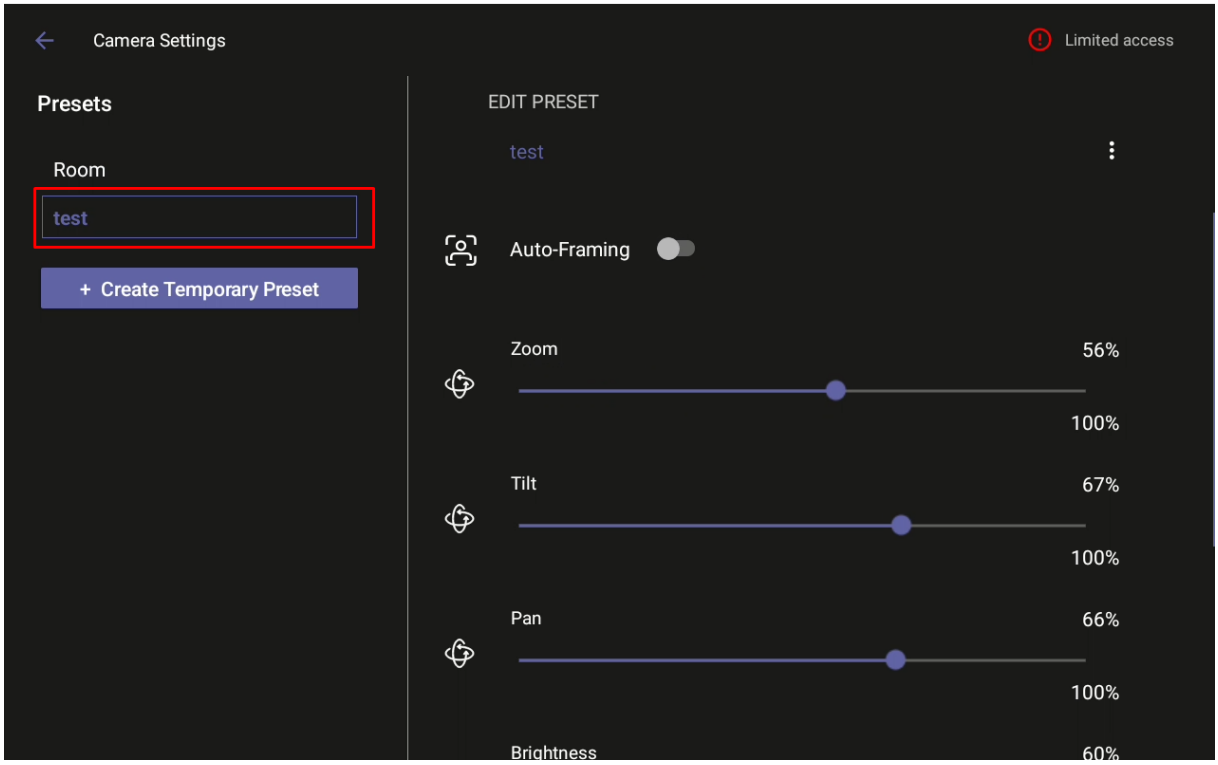


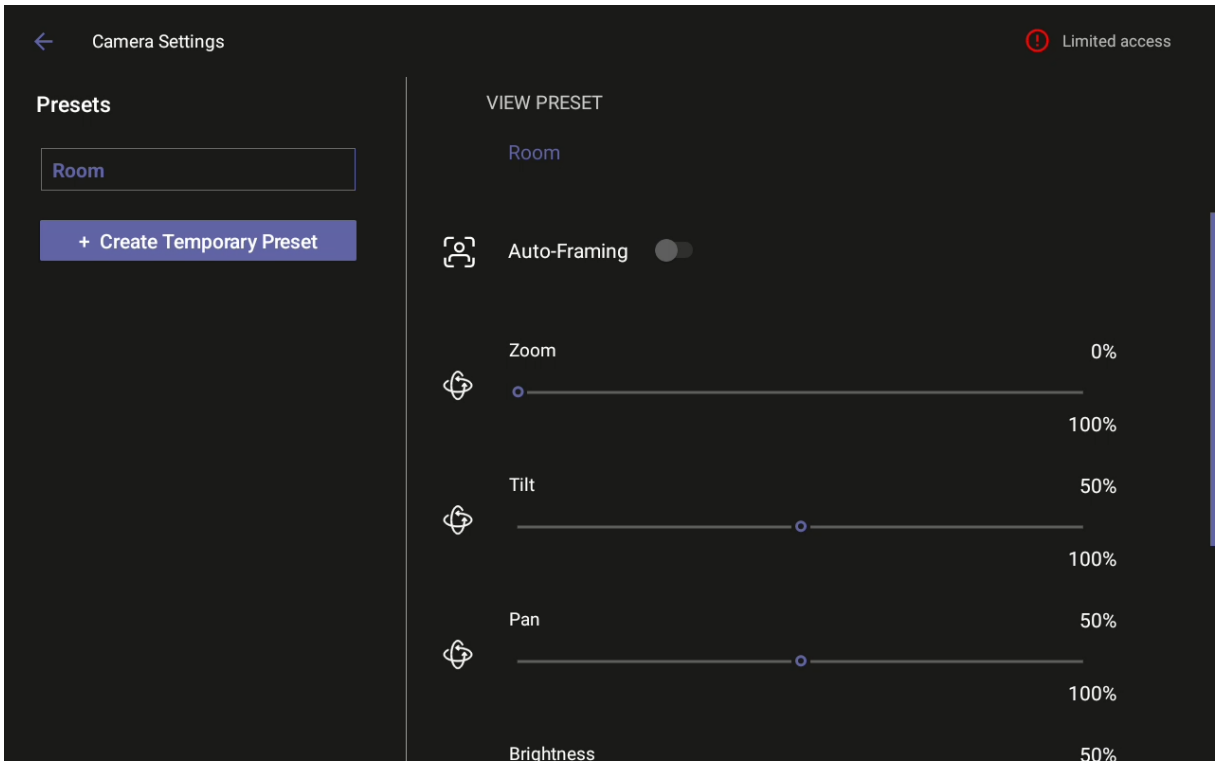
When Auto-Framing is enabled, PTZ (Pan Tilt Zoom) functions are disabled.

End users without administrator permissions can create temporary presets in the Camera Settings page as shown in the figures below.



If this end user leaves the meeting, the temporary presets will be erased when they later reenter Camera Settings or if another end 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
Limited access
Presets
Room
test
+ Create Temporary Preset
EDIT PRESET
test
Auto-Framing
Zoom
56%
100%
Tilt
67%
100%
Pan
66%
100%
Brightness
60%

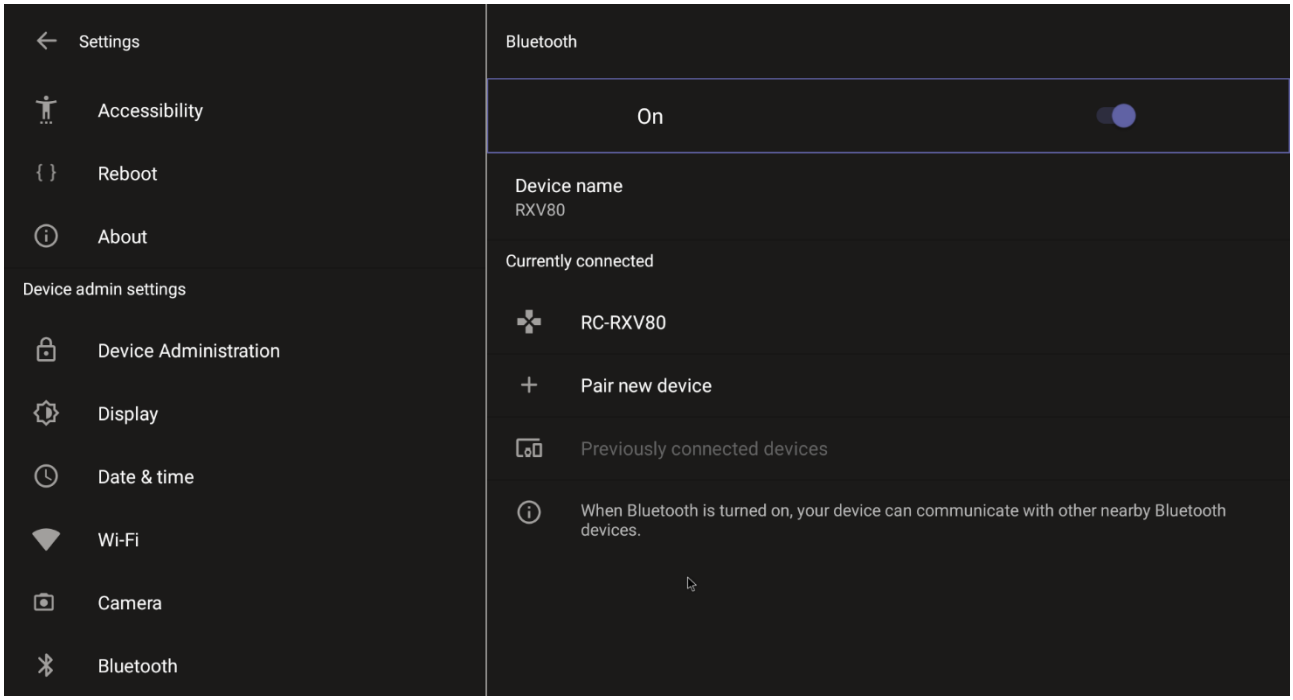

Camera Settings
Limited access
Presets
Room
+ Create Temporary Preset
VIEW PRESET
Room
Auto-Framing
Zoom
0%
100%
Tilt
50%
100%
Pan
50%
100%
Brightness
50%

4.1.6 Pairing RC with RXV81 via Bluetooth

Bluetooth is currently used to pair the RC with RXV81.

➢ **To pair a new device:**

1. Under 'Device admin settings', navigate to and select **Bluetooth**.



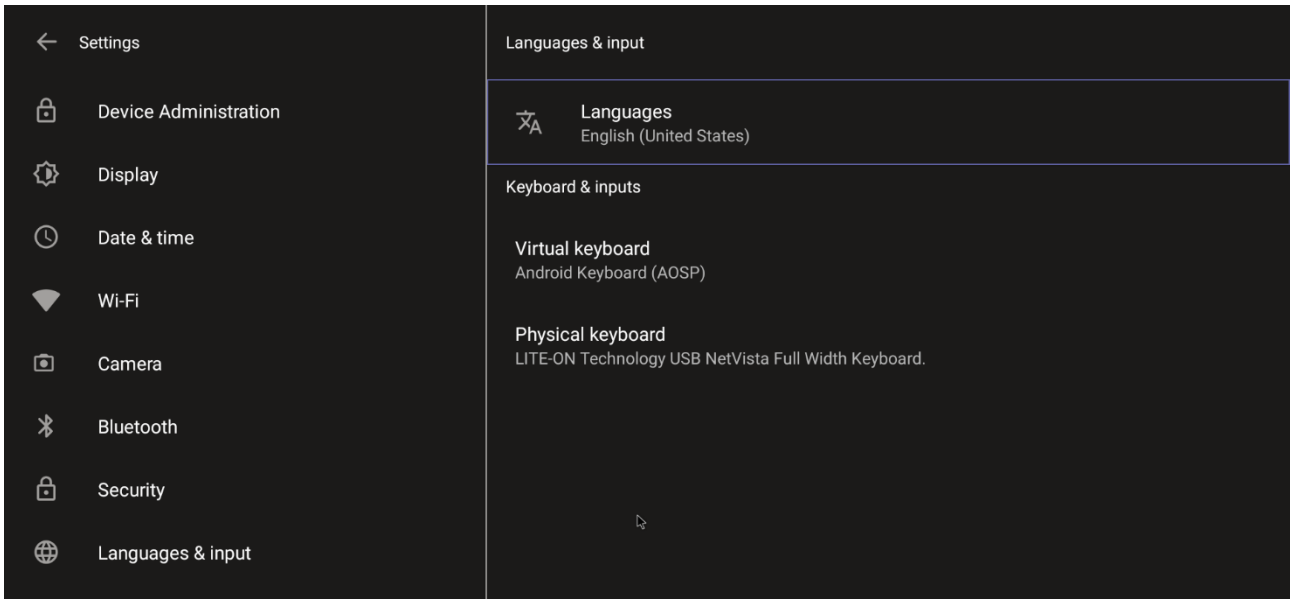
2. Navigate to and select **Pair new device**.

4.1.7 Configuring UI Language & Input

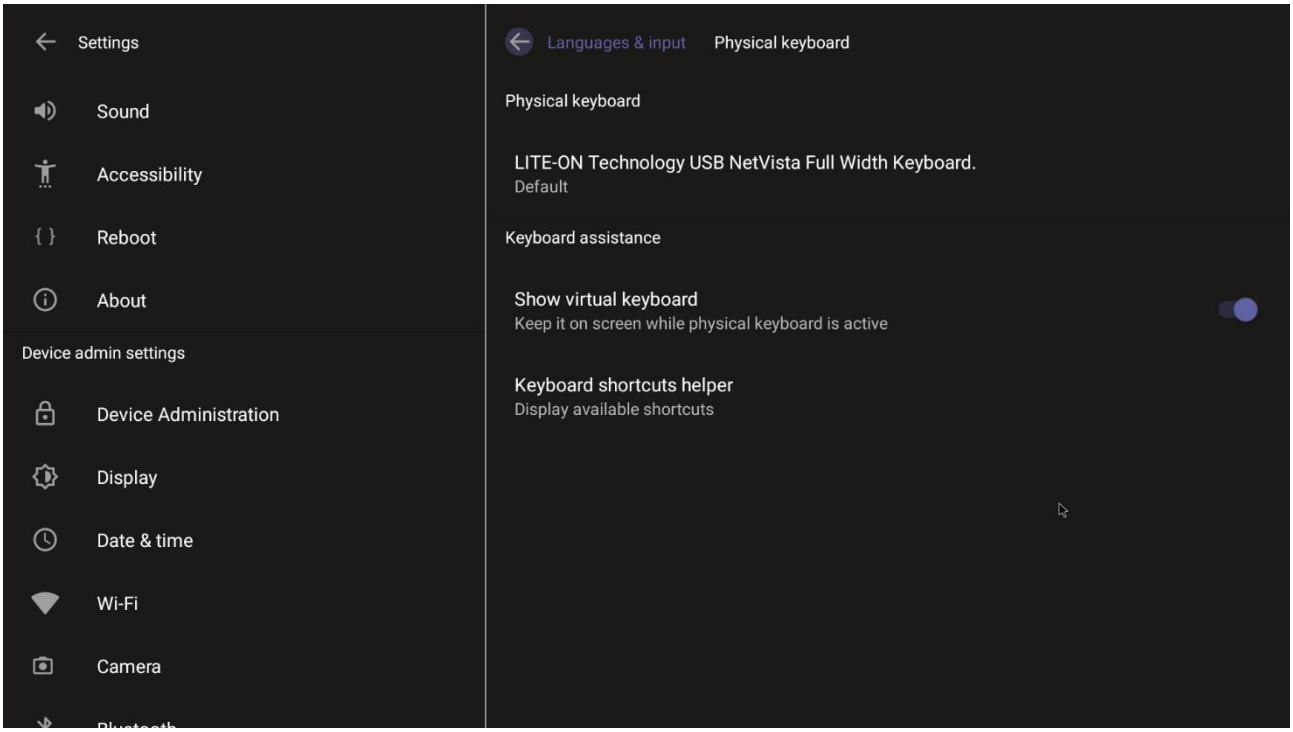
This setting allows users to customize inputting to suit personal requirements.

➢ **To set language and input:**

1. Under 'Device admin settings', navigate to and select **Languages & input**.



2. Navigate to and select **Physical keyboard**.



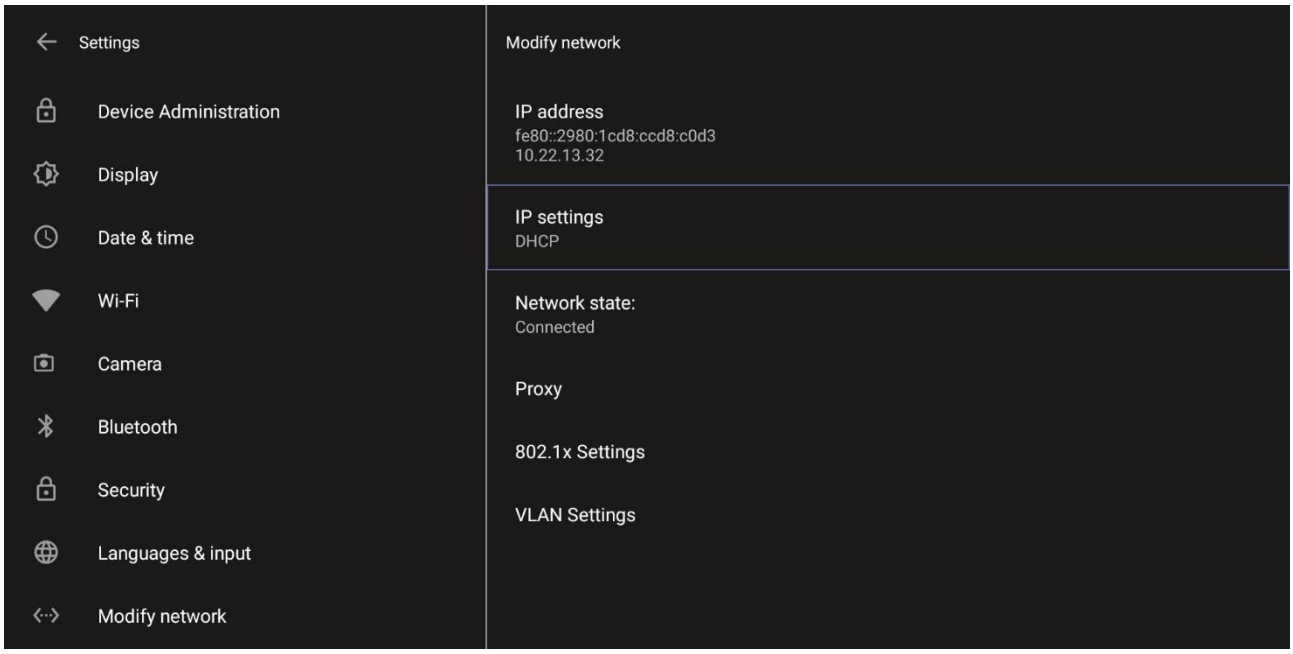
3. Navigate to and select **Show virtual keyboard**.

4.1.8 Modifying IP Network Settings

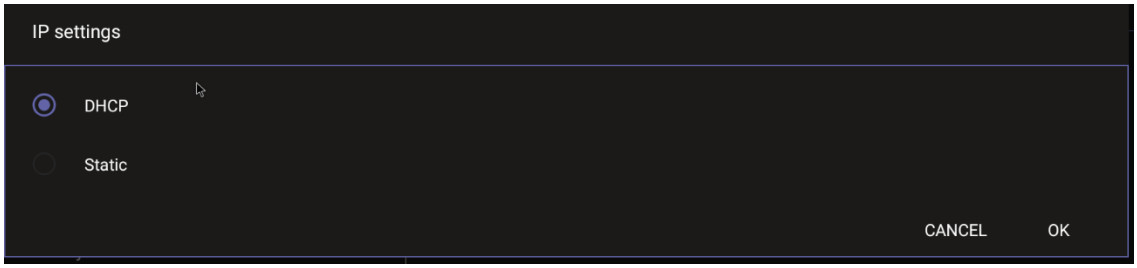
This setting enables the Admin user to determine IP network information and to modify IP network settings.

➢ **To modify network settings:**

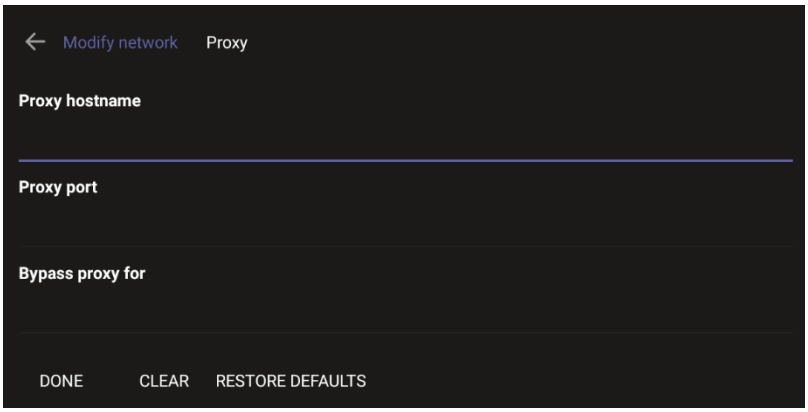
1. Under 'Device admin settings', navigate to and select **Modify network**.



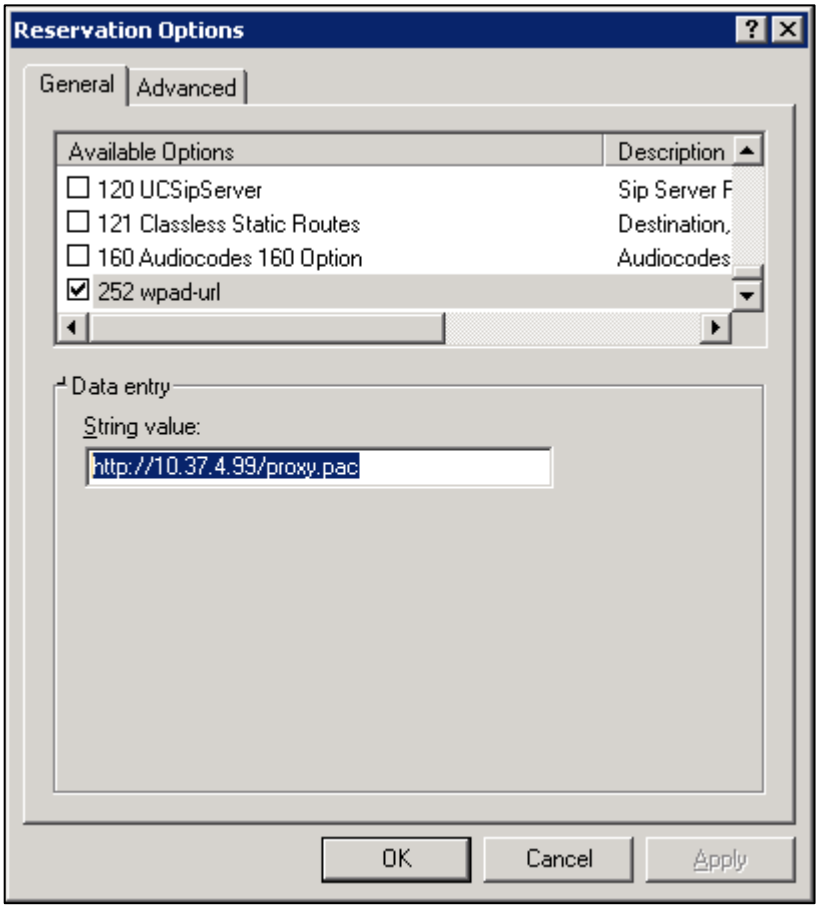
2. Navigate to and select:
   - IP Address [Read Only]
   - IP Settings [DHCP or Static IP]



   - Network state [Read Only]
   - Proxy



- Manually (from the screen shown in the preceding figure). Allows you to configure RXV81 with an HTTP proxy server. Configure the proxy hostname and proxy port and then navigate to and select **Done**.
- **DHCP Option 252** (recommended). Option 252 provides a DHCP client with a URL to use to configure its proxy settings:



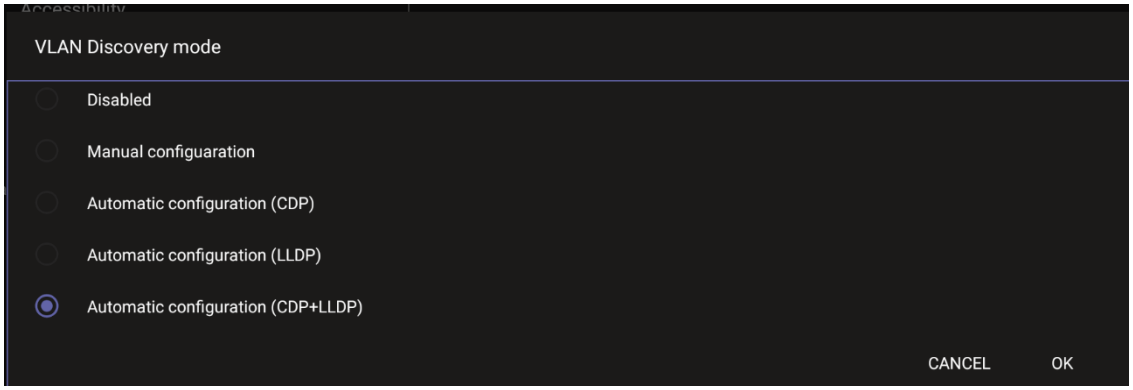
The proxy setting is provided in a Proxy Auto-Configuration (PAC) file that contains a set of rules coded in JavaScript which allows a web browser to determine whether to send web traffic directly to the Internet or to be sent via a proxy server. PAC files control how the phone handles HTTP, HTTPS, and FTP traffic. Example of a basic PAC file:

```
function FindProxyForURL(url, host)
{
return "PROXY 10.13.2.40:3128";
}
```

- 802.1x Settings [Allows enabling 802.1x]

  802.1X Authentication is the IEEE Standard for Port-based Network Access Control (PNAC). See https://1.ieee802.org/security/802-1x/ for more information.

- VLAN Settings
  - Allows you to configure 'VLAN Discovery mode' to Manual configuration, Automatic configuration (CDP), Automatic configuration (LLDP) or Automatic configuration (CDP+LLDP)]



Cisco Discovery Protocol (CDP) is a Cisco proprietary Data Link Layer protocol
Link Layer Discovery Protocol (LLDP) is a standard, layer two discovery protocol

Note: The VLAN configuration is by default **data VLAN** rather than voice VLAN, in compliance with the requirement specified here for the device not to advertise itself as a voice device. The default CDP/LLDP configuration is **data VLAN**.

- Allows you to configure 'VLAN Interval'.

'VLAN interval' refers to CDP/LLDP advertisements' periodic interval. Default: 30 seconds. You can increase or decrease the intervals between the CDP/LLDP packets that are sent, based on network traffic and topology.

Note:

- In versions before 1.19, if network VLAN mode '/network/lan/vlan/mode' was set to LLDP, the device retrieved the VLAN and LLDP switch information (for location purposes) from LLDP.
- From version 1.19, LLDP switch information (for location purposes) is retrieved when parameter network/lan/lldp/enabled=1 (even when VLAN is retrieved from **CDP** or VLAN is disabled or VLAN is **Manual**).

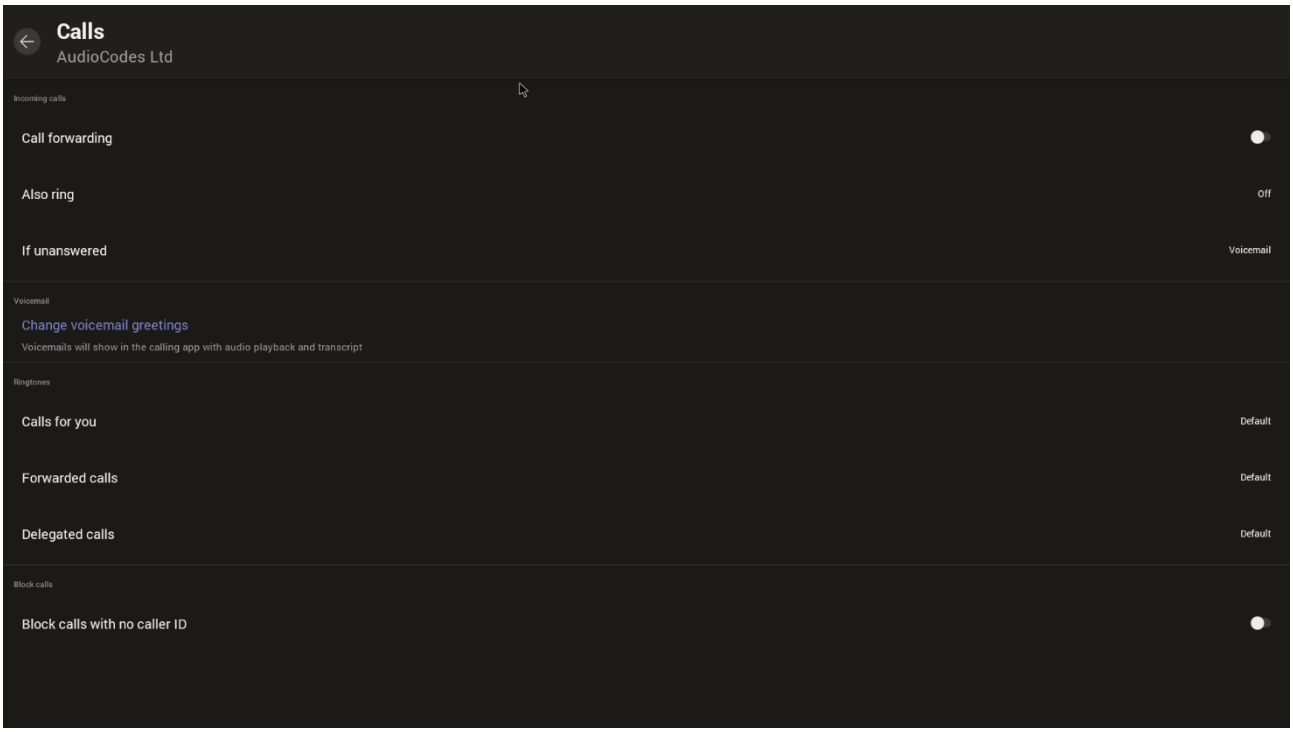
4.1.9 Configuring Call Settings

This setting enables the user to configure call-associated functionalities to suit personal preferences.

➢ **To configure call settings:**

1. From the home page, navigate to and select **More** and then navigate to and select **Settings**.

2. Navigate to and select **Calling**.

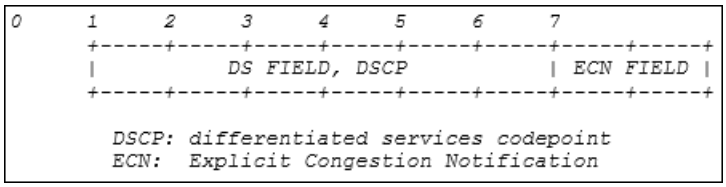


- In the Calls screen, navigate to and select:
  - **Call forwarding** to enable automatically redirecting incoming calls to another destination.
  - **Also ring** to configure other phones to ring on incoming calls; only displayed if **Call forwarding** is disabled.
  - **If unanswered** to configure the destination to which unanswered calls will be sent; only displayed if **Call forwarding** is disabled. Select either Off, Voicemail, Contact or number.
  - **Calls for you** to configure the ringtone played on your phone when calls come in.
  - **Forwarded calls**
  - **Delegated calls** to configure the ringtone played to delegates.
  - **Block calls with no caller ID** to block calls that do not have a Caller ID.

4.1.10 Configuring DSCP for QoS

RXV81 Teams application supports DS (Differentiated Services) containing a differentiated Services Code Point (DSCP) value and an ECN (Explicit Congestion Notification) value, for monitoring Quality of Service (QoS).

DSCP is part of the IP header that defines the type of routing service to tag outgoing voice packets originated from the device. It informs routers that this packet must receive a specific QoS. Values can be set in decimal (e.g., 184) or hexadecimal (e.g., 0xb8). The default value is 0xb8 (184).



The DSCP value for **audio** is **0x46**.

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

See also Microsoft's website for more information.

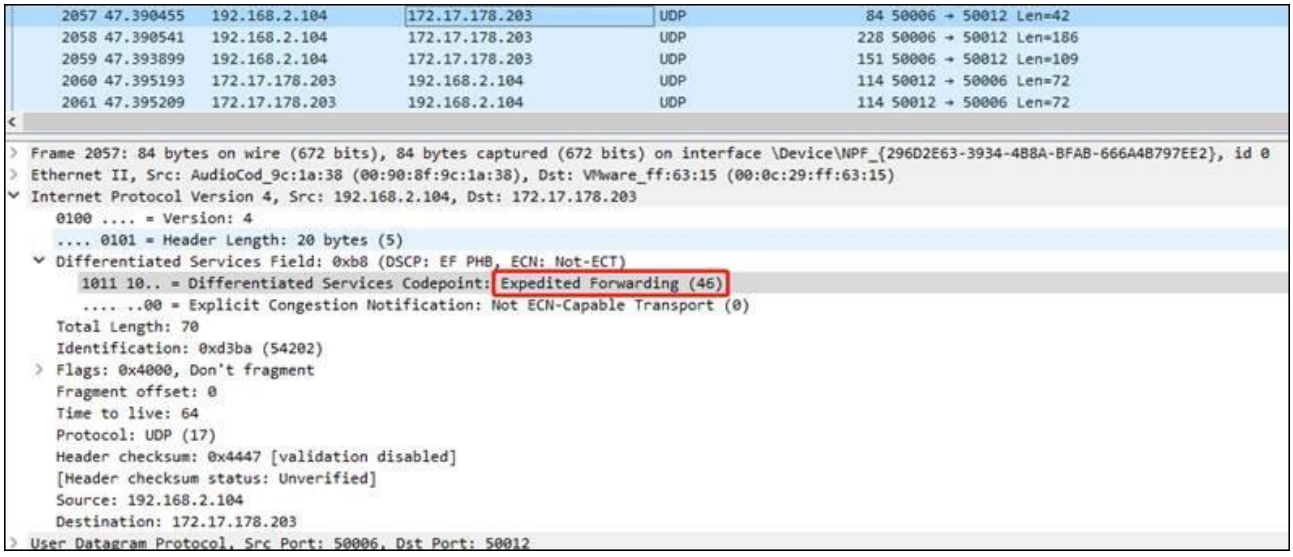
Note: The DSCP value can be adjusted on the server; it cannot be adjusted on the client.

The figure below shows the recommended port ranges.

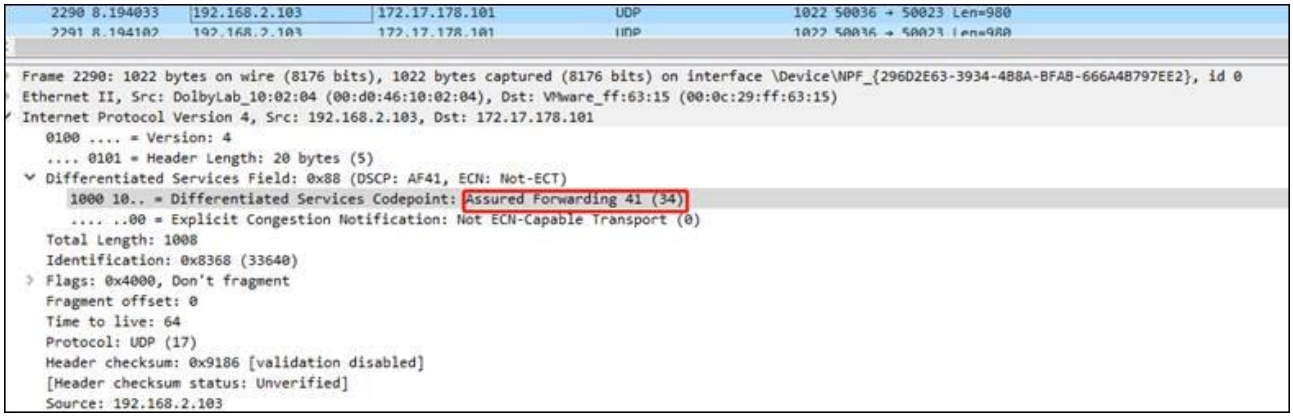
Table 1. Recommended initial port ranges

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

The figure below shows the recommended DSCP setting for Audio.



The figure below shows the recommended DSCP setting for Video.

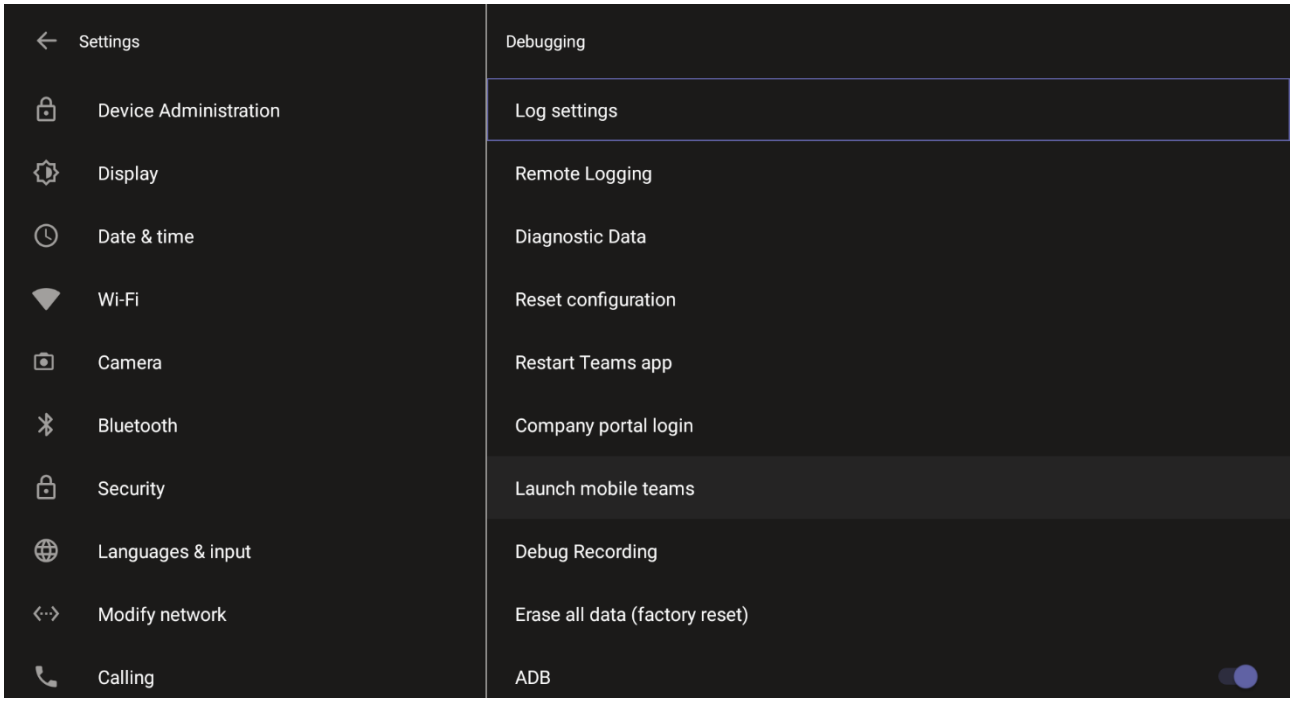


4.1.11 Debugging

Admin users can perform debugging for troubleshooting purposes. A bug report is available to allow admins to perform efficient debugging. The report also includes information such as pack up time, ps, top, meminfo and df commands (information about file system disk space usage) for optimized debugging.

➢ **To perform debugging:**

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



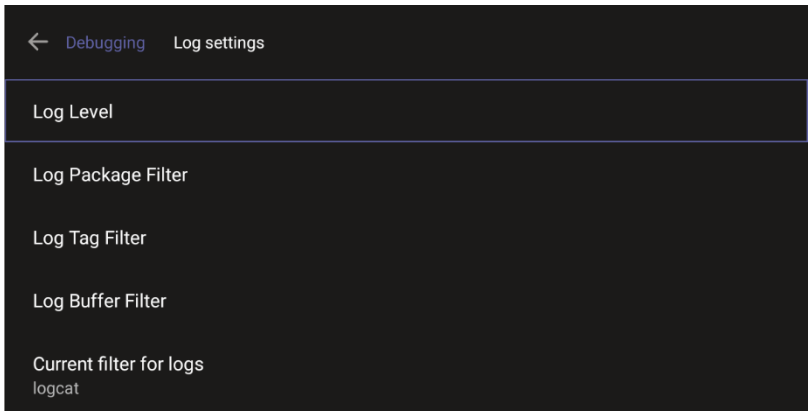
2. Use the following debugging features available to Admin users:
   - Log settings (see Log Settings)
   - Remote Logging (see under Remote Logging)
   - Diagnostic Data (see under Diagnostic Data)
   - Reset configuration (see under Reset configuration)
   - Restart Teams app (see under Restart Teams 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)

4.1.11.1 Log Settings | Collecting Logs

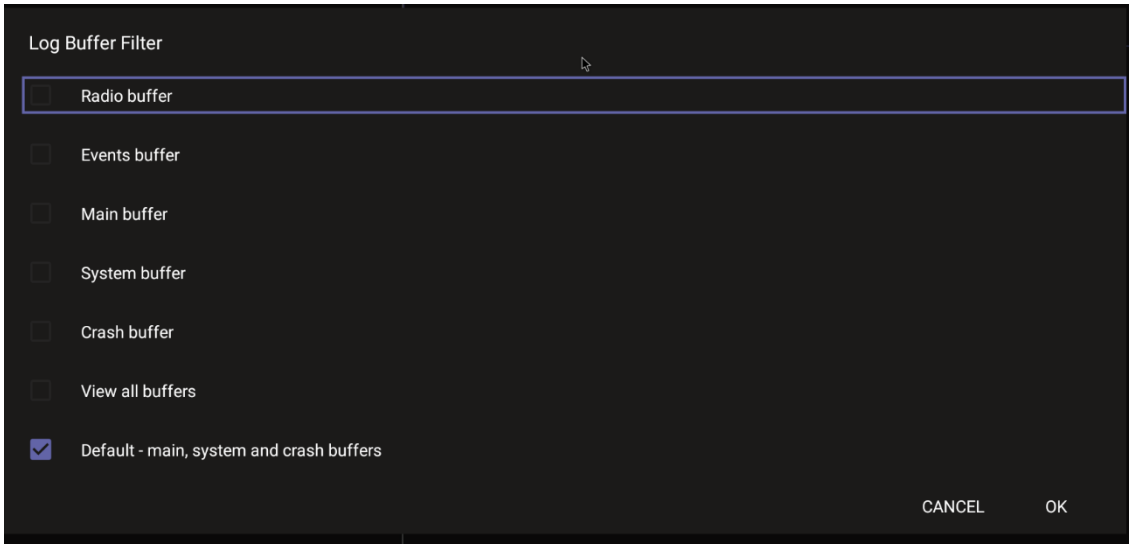
Device diagnostics (Logcat) can be collected using the Microsoft Admin Portal. For support purposes, general logs can be collected also using the Microsoft Admin Portal. The logs can help debug Teams application issues and also for issues related to the device.

➢ **To configure log settings:**

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



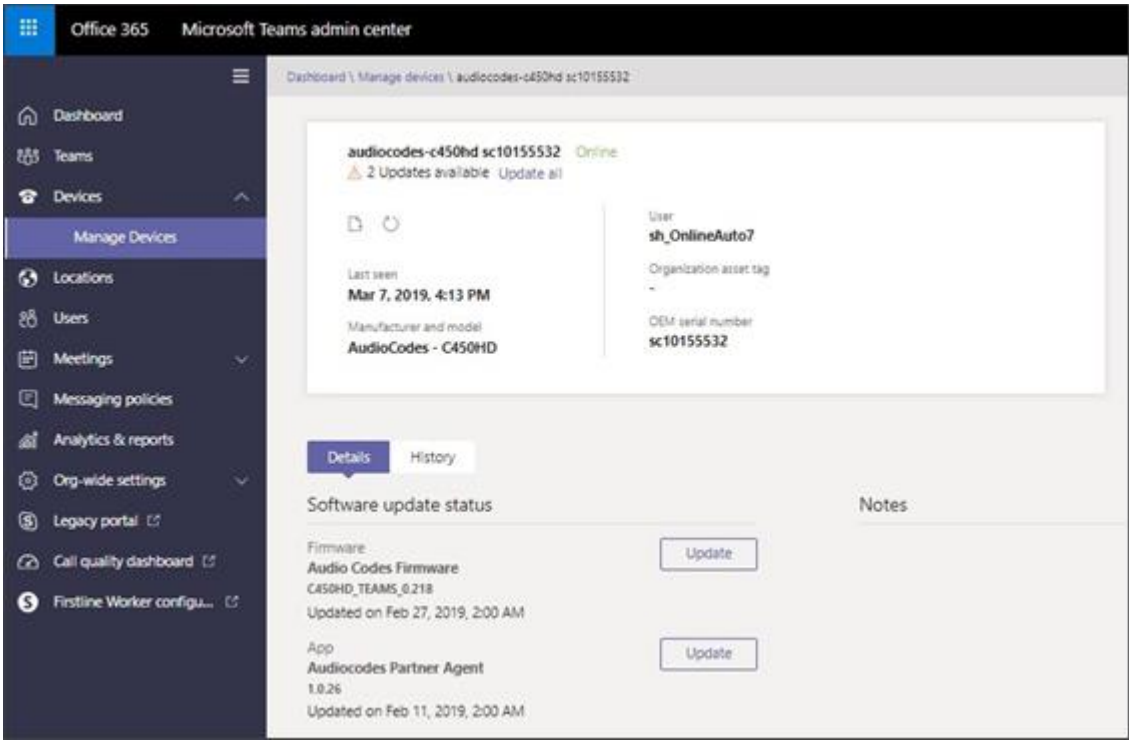
2. Navigate to and select **Log Level** and then select either
   - Verbose, Debug, Info, Warning, Error, Assert -or-None
3. Navigate to and select **Log Package Filter** and enter the filter.
4. Navigate to and select **Log Tag Filter** and enter the filter.
5. Navigate to and select **Log Buffer Filter**.



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

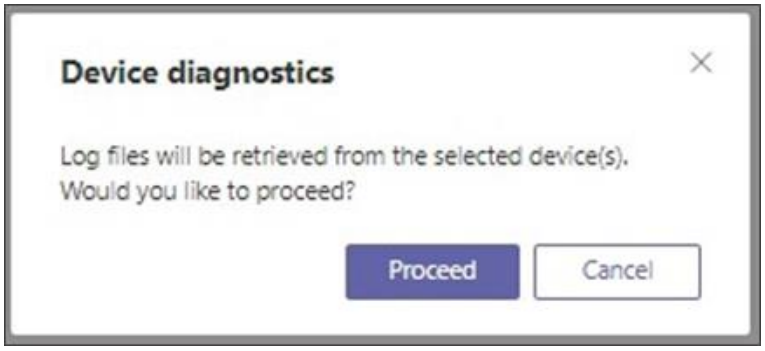
➢ **To collect logs:**

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

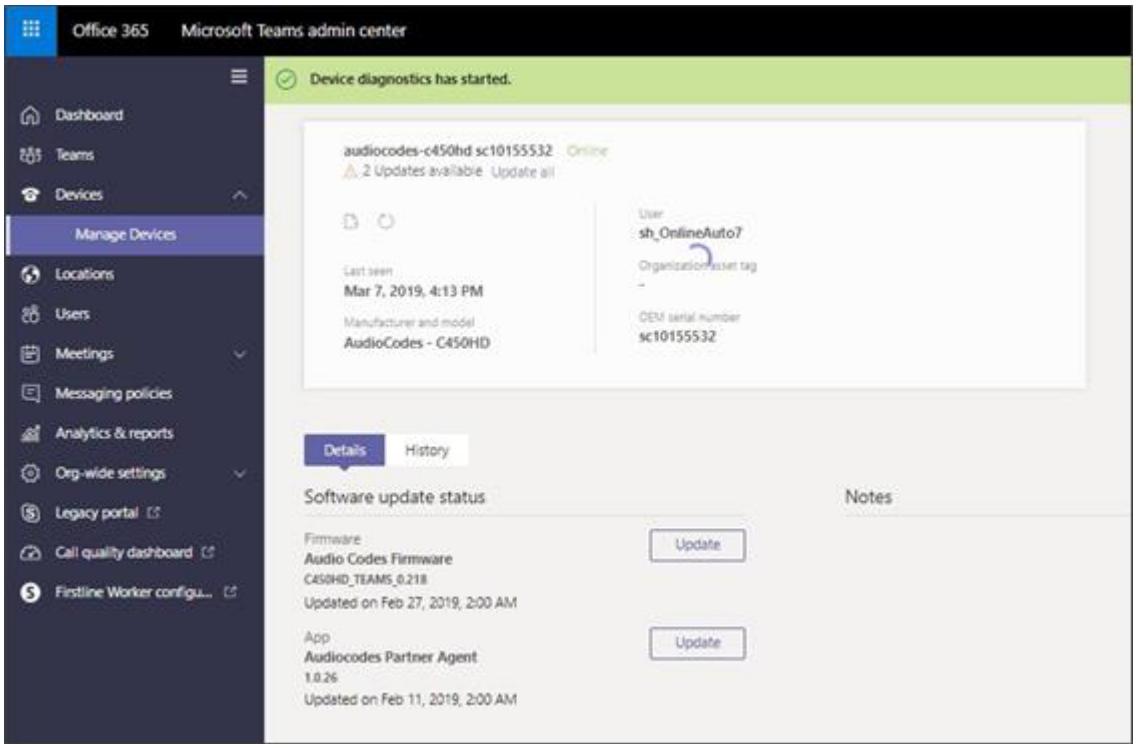


Note: The preceding figure is for illustrative purposes. It shows an AudioCodes phone. The same screen is displayed for RXV81.

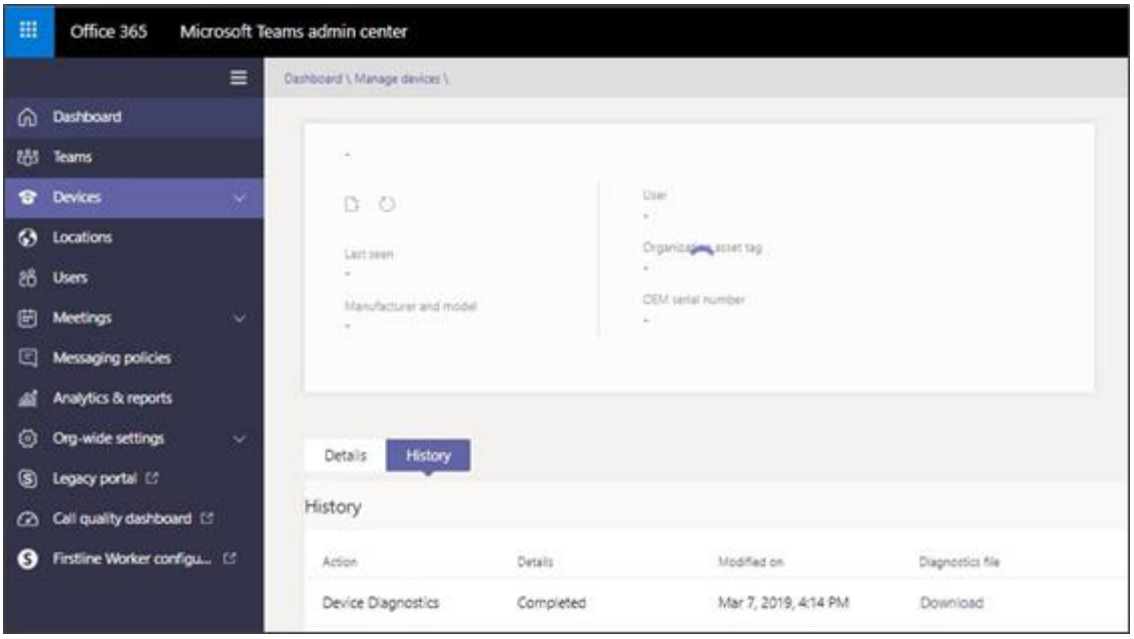
3. Click the **Diagnostics** icon.



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



5. Click the **History** tab.



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

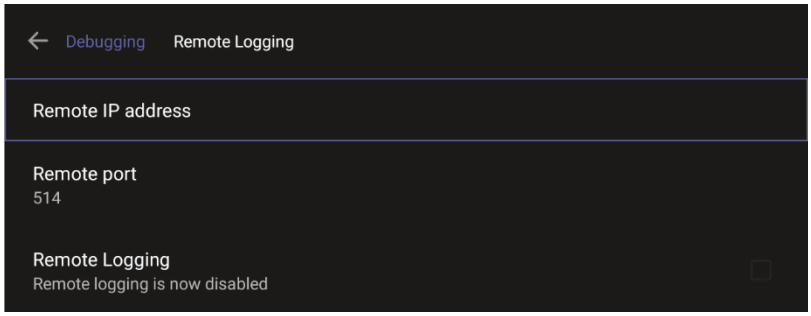
4.1.11.2 Remote Logging

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:**

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



8. 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 ""
```

4.1.11.3 Diagnostic Data

Admin users who need to get logs from the device can dump the logs to the phone's Secure Digital (SD) Card and then later collect them using Secure Copy Protocol (SCP) based on Secure Shell (SSH) protocol. Whenever an issue occurs, the Admin can dump the logs into the SD Card.

➢ **To use the tool:**

1. Navigate to and select **Diagnostic Data**.

2. Navigate to and select **OK** to confirm 'Copy logs to sdcard'; RXV81 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):

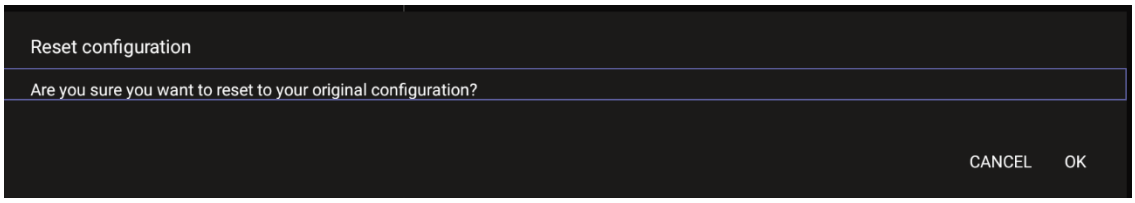
- dmesg.log
- dumpstate-TEAMS_1.3.16-undated.txt
- dumpstate_log-undated-2569.txt
- logcat.log

4.1.11.4 Reset configuration

Admin users can opt to 'clean up' their configuration history and return RXV81 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.

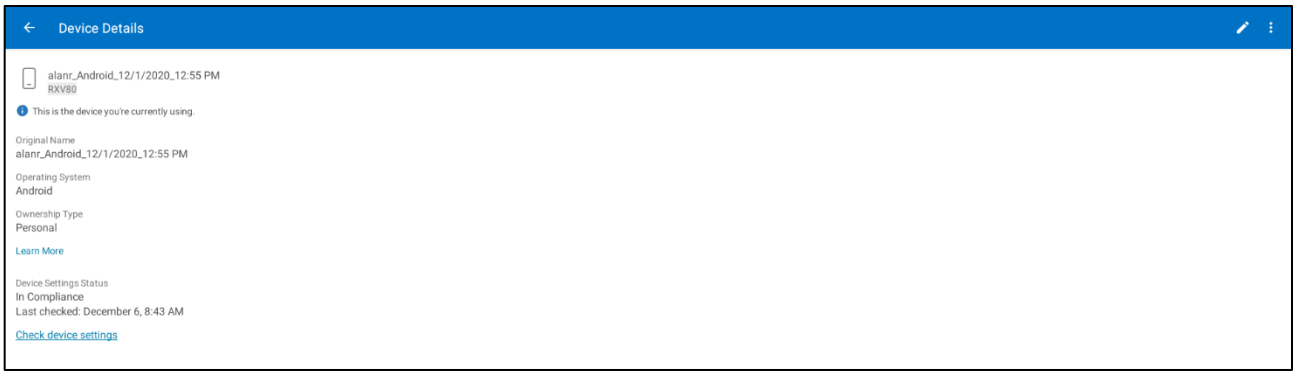
4.1.11.5 Restart Teams app

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.

4.1.11.6 Company Portal Login

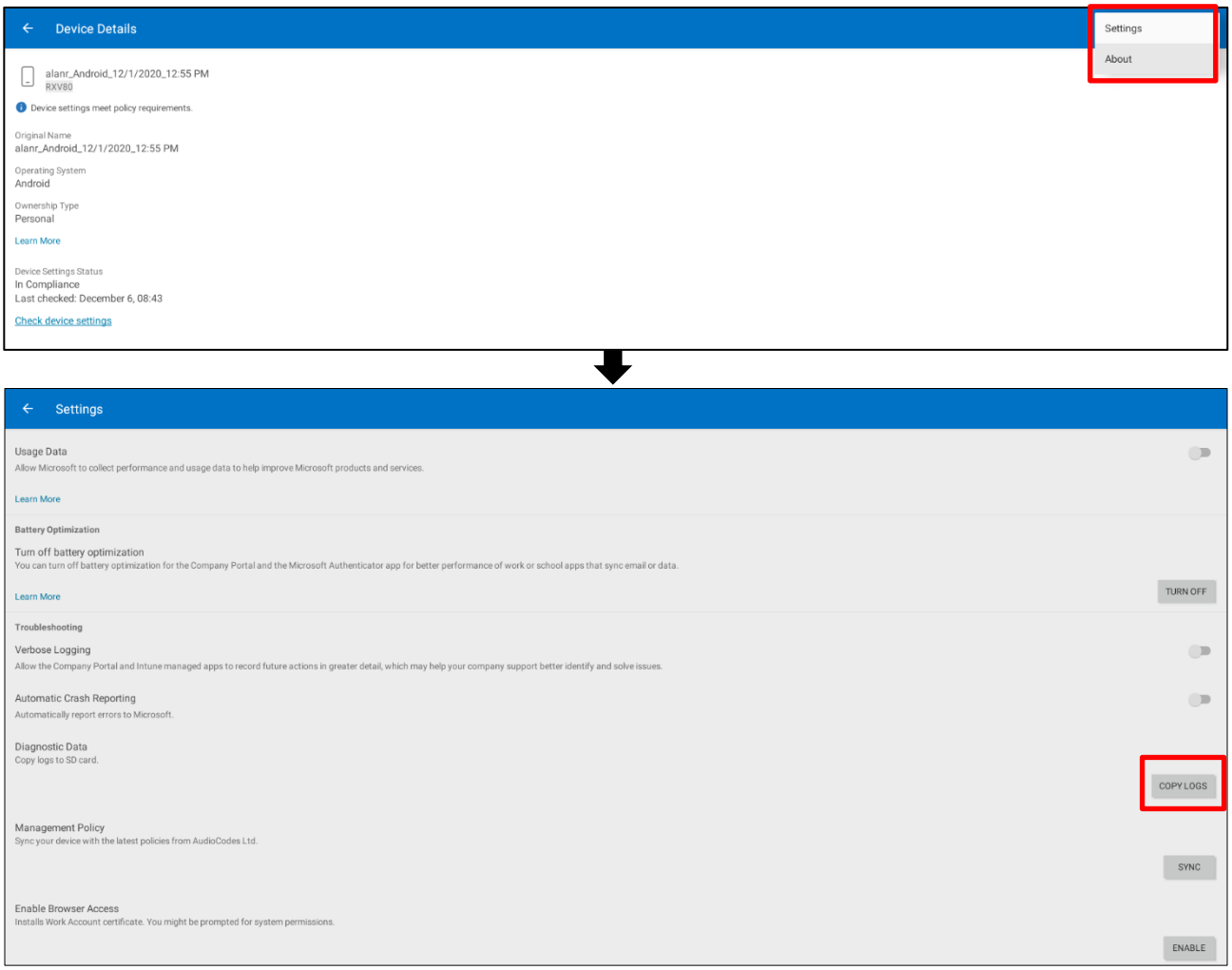


4.1.11.7 Getting Company Portal Logs

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

➢ **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 RXV81 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.

4.1.11.8 Launch Mobile Teams

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

4.1.11.9 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 phone.

➢ **To reset the configuration:**

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

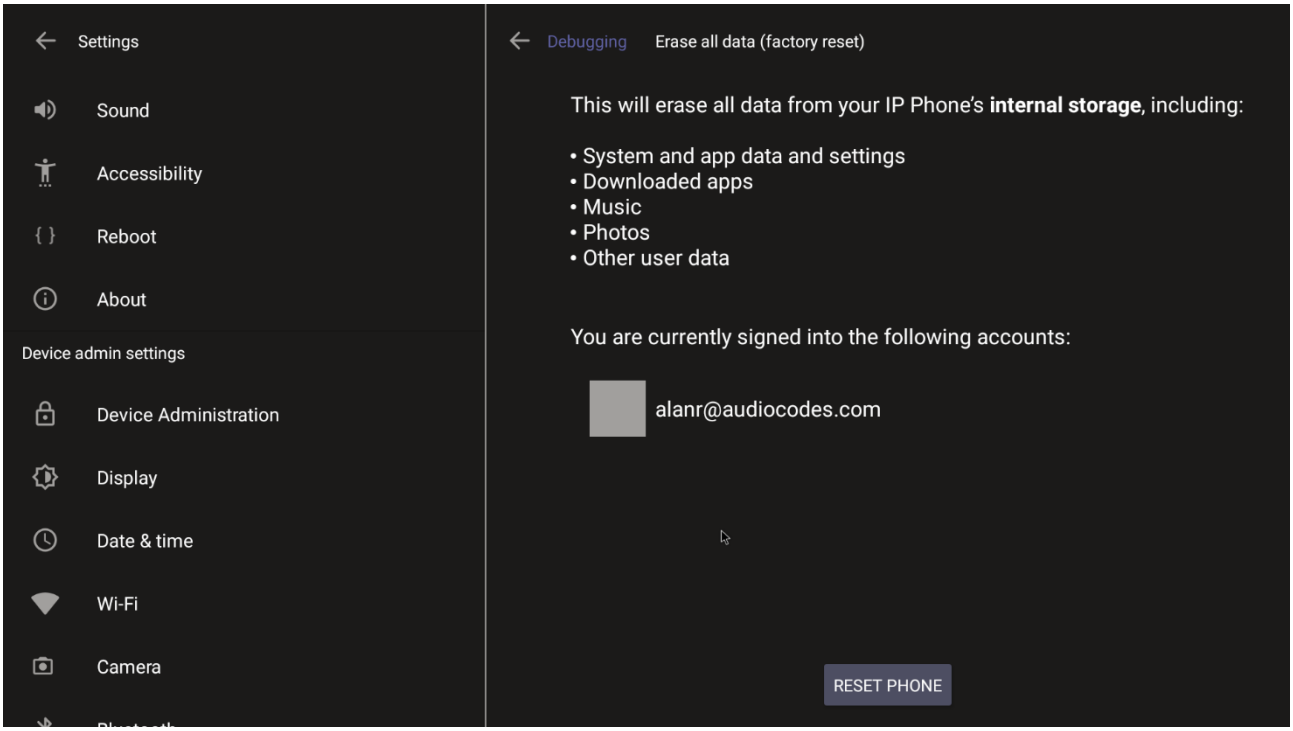
2. Navigate to and select **Voice record** to enable the feature.
3. Navigate to and select **Remote IP address** to input the IP address of the device whose traffic you want to record.
4. Navigate to and select **Remote port** and input it (Default: 5000).
5. Start Wireshark on your PC to capture audio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

4.1.11.10 Erase all data (factory reset)

This option is the equivalent of restore to defaults, 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**.

4.1.11.11 Screen Capture

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

4.2 Performing Recovery Operations using Power Button

Network administrators can perform recovery operations using the power button on the rear panel of RXV81.

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

The following figure shows the power button.

➢ **To perform recovery operations:**

1. Disconnect the power cord from RXV81 while long-pressing the power button for as long as is required for the action (see Table 4-2 below for the available actions - see the **Action** column - and durations – see the **Long-press for** column).
2. Reconnect the power cord and continue pressing the power button for however long is necessary.

Table 4-2: Recovery Operation Options using RXV81's Power Button

Stage	Action	Long-press for	LED Flashes 3x
On Uboot	NOTHING	< = 2 seconds	
	ENTER_RECOVERY	2-4 seconds	RED
	SWITCH_AB_SLOT	4-6 seconds	WHITE
	ENTER LOADER	6-8 seconds	BLUE
	RESTORE_DEFAULT	8-10 seconds	BLUE + WHITE
	SHUTDOWN	> = 10 seconds	

3. Short-press the power button to move down the menu options, and long-press to select an option.

4.3 Restoring RXV81 Firmware via USB Disk

For recovery purposes, firmware can be applied to RXV81 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 Table 4-2 above (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.

4.4 User Settings

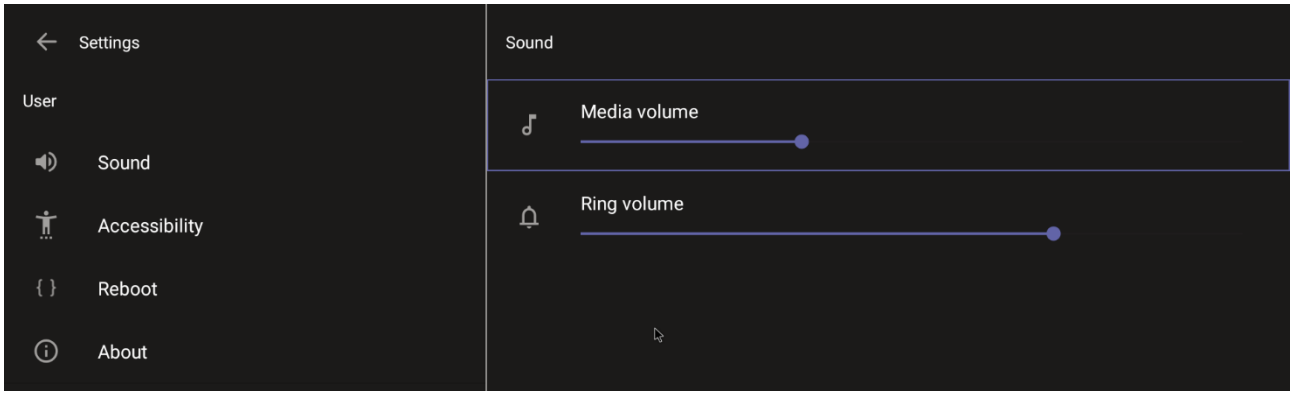
In the 'Settings' screen you can optionally configure the following User settings: Sound, Accessibility, Reboot and About (read-only).

4.4.1 Setting the Volume

You can customize phone volume for a friendlier user experience.

➢ **To configure sound settings:**

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

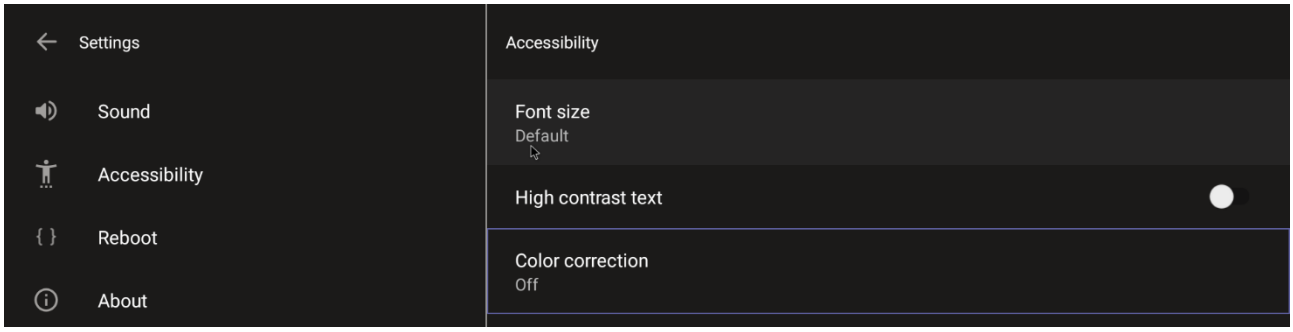


4.4.2 Configuring Accessibility Settings

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**.



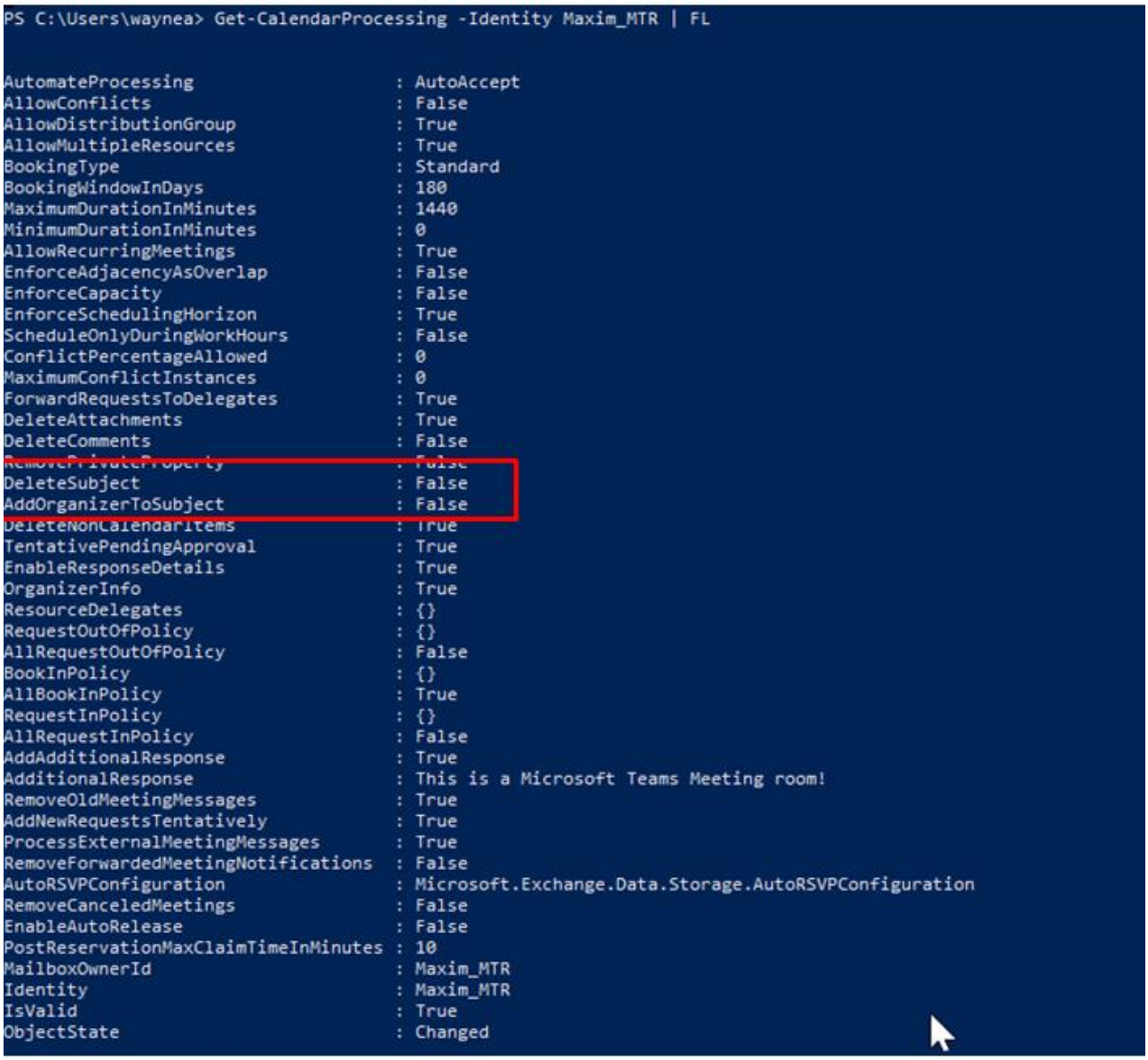
2. Adjust the settings to suit personal requirements.

4.4.3 Setting Live Captions

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

4.4.4 Enabling Display of Meeting Name using Exchange Online PowerShell

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

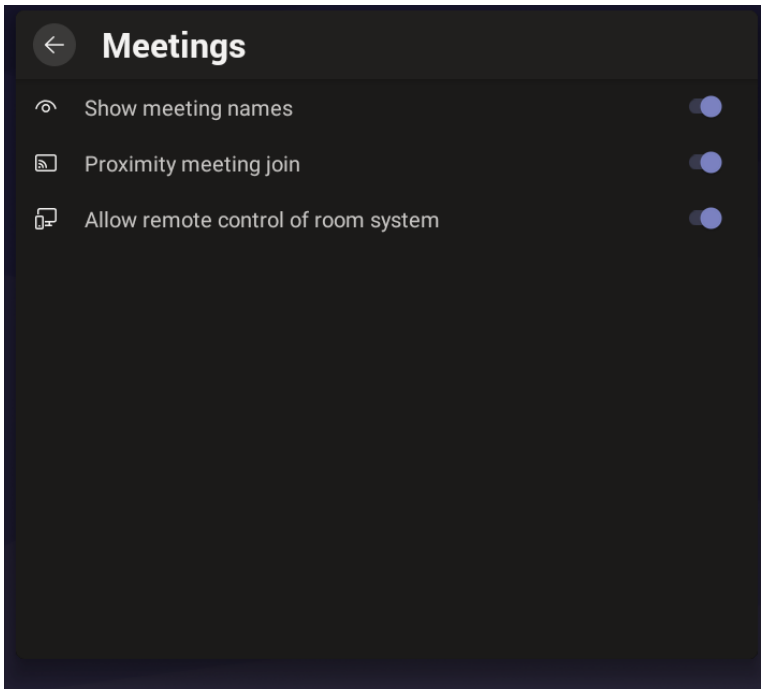


'Identity' is the name of the account to which admin wants to apply these two settings:

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

4.4.5 Hiding Names and Meeting Titles

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



4.4.6 Rebooting RXV81

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

➢ **To reboot:**

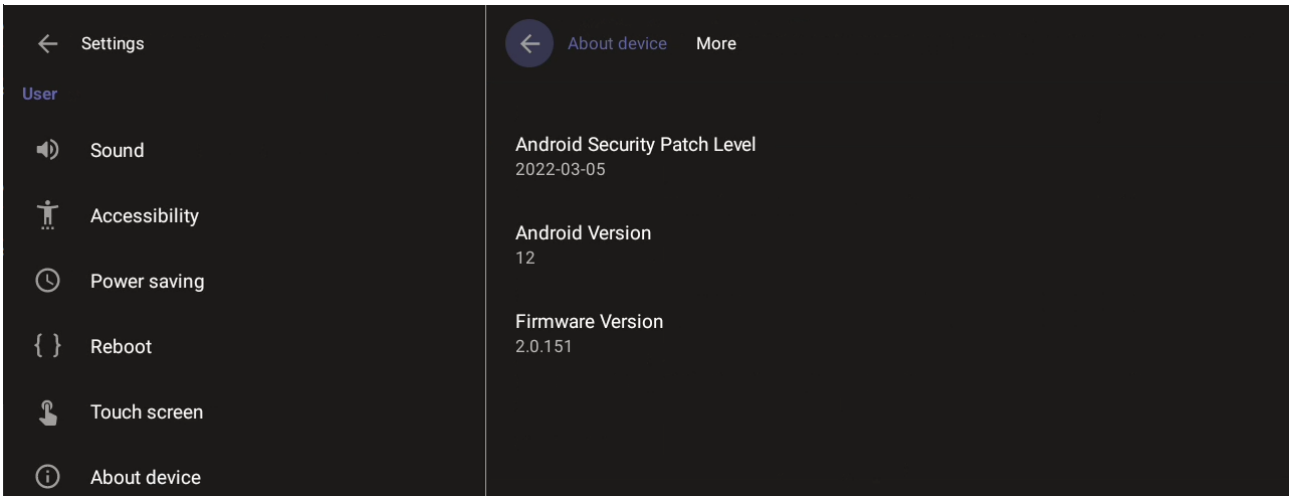
- Under 'User', navigate to and select **Reboot**.

4.4.7 Viewing About RXV81

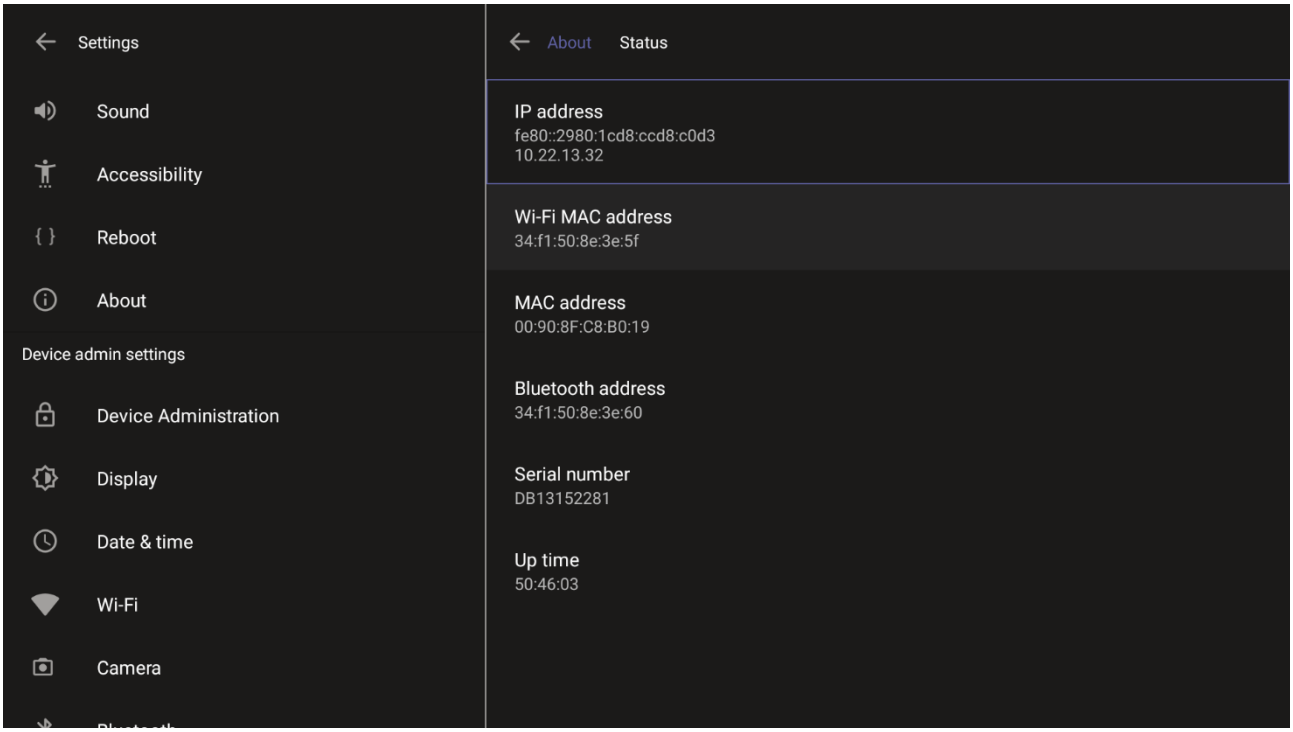
The 'About' screen gives you quick access to information about RXV81 deployment.

➢ **To access the About screen:**

1. Navigate to and select **About device**.



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



3. View RXV81's firmware information.

4.5 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 below
- Create an exclusion group – see below

4.5.1 Creating a Dynamic Group

See here how to create dynamic groups in Intune for enrolling AudioCodes Android-based Teams devices.

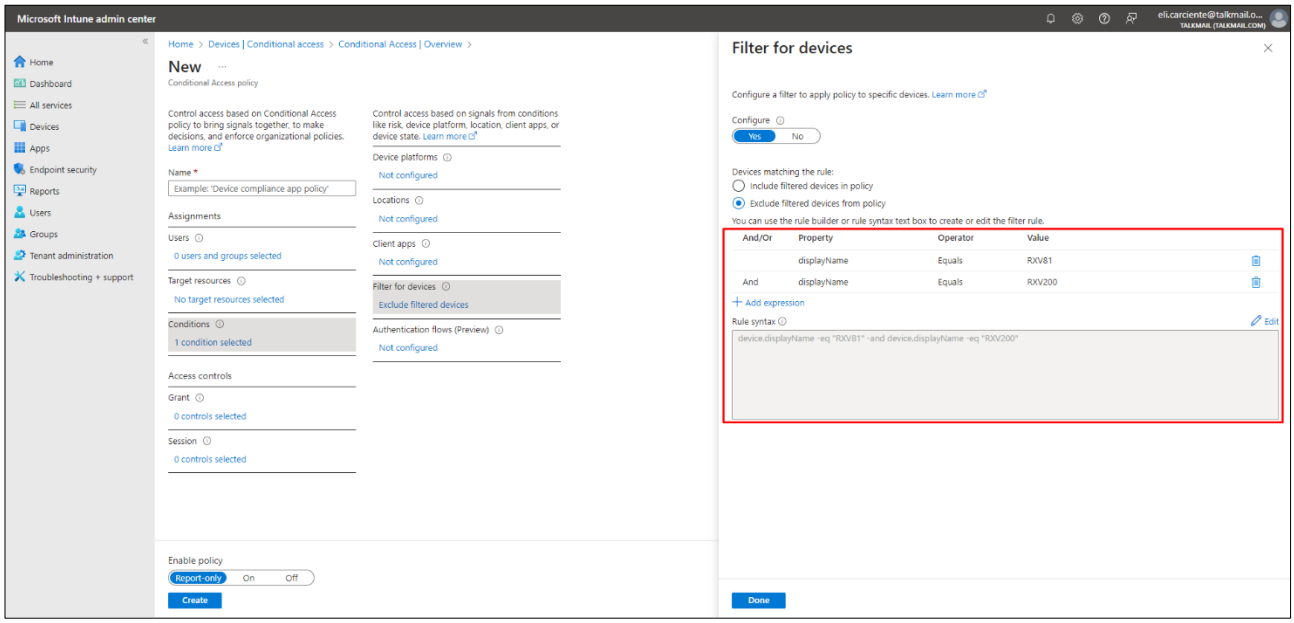
4.5.2 Creating an Exclusion Group

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 RXVxx**

    where **RXVxx** is the name of the device model (**device.model**).

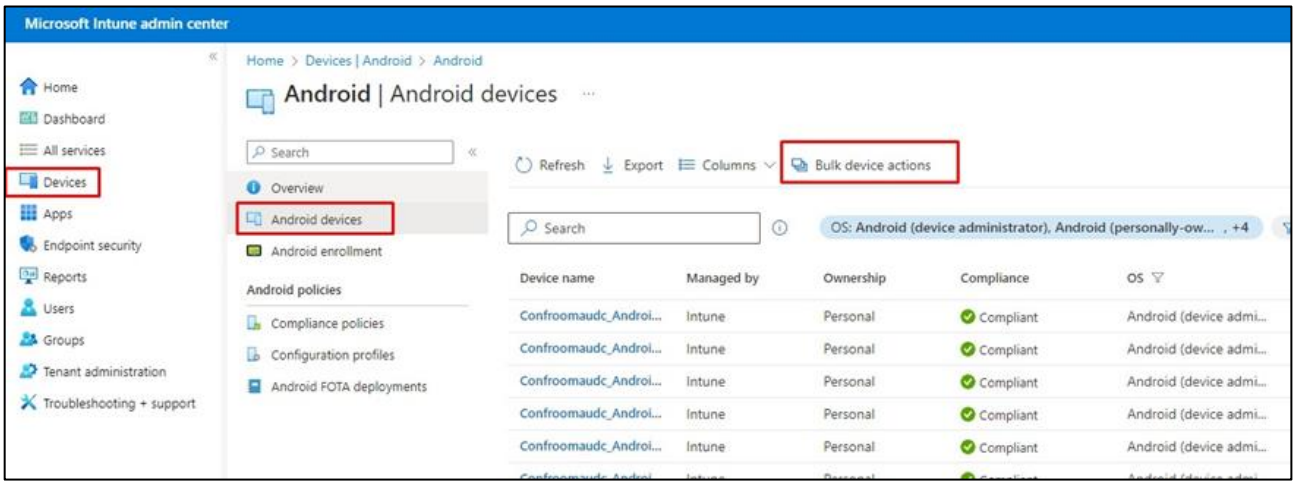


4.6 Removing Devices from Intune admin center

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

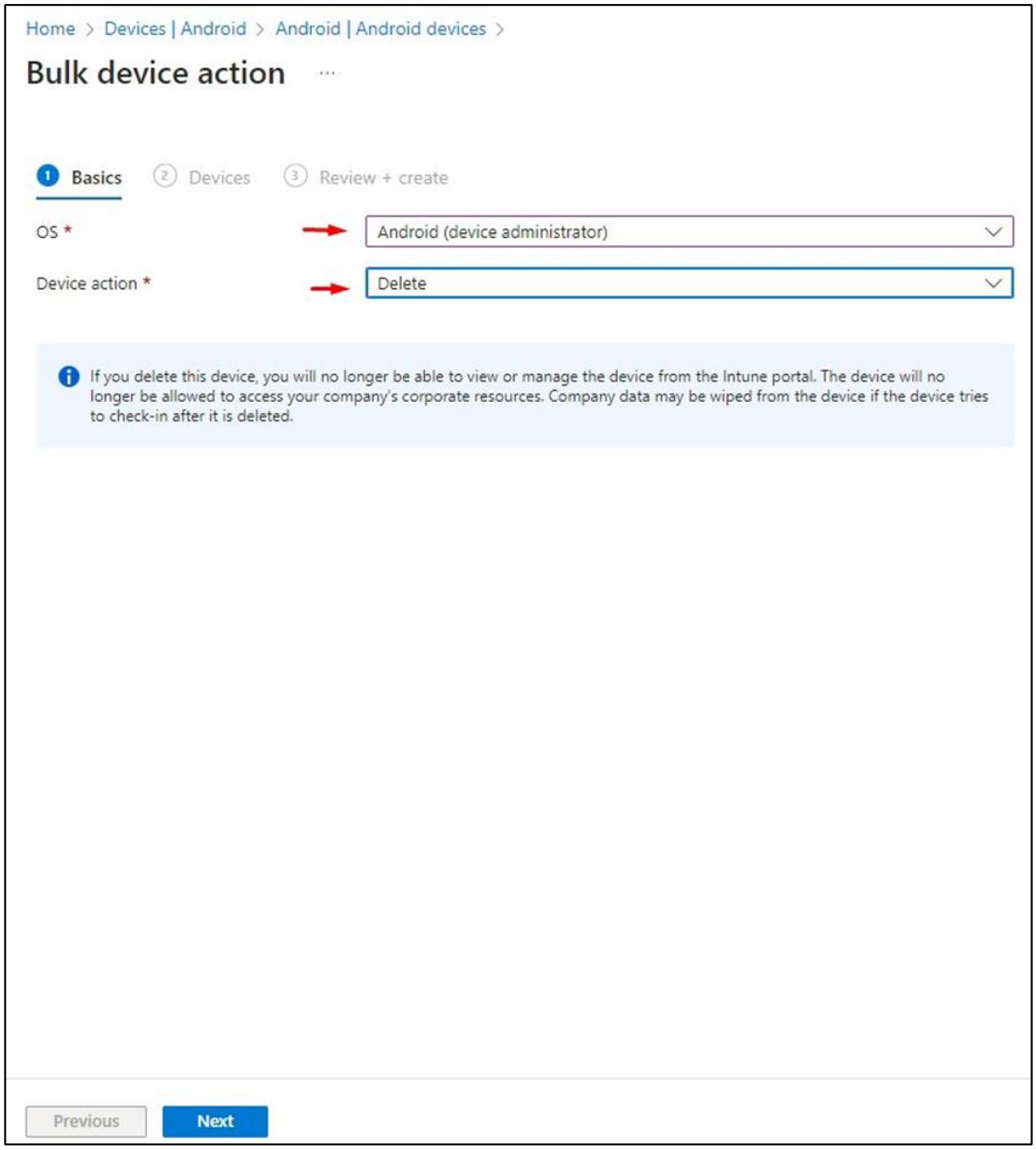
➢ **To remove devices from Intune admin center:**

4. Go to Microsoft 365 admin center [portal.office.com] and log in with an Administration account.
5. Navigate to **Devices** > **Android devices**.

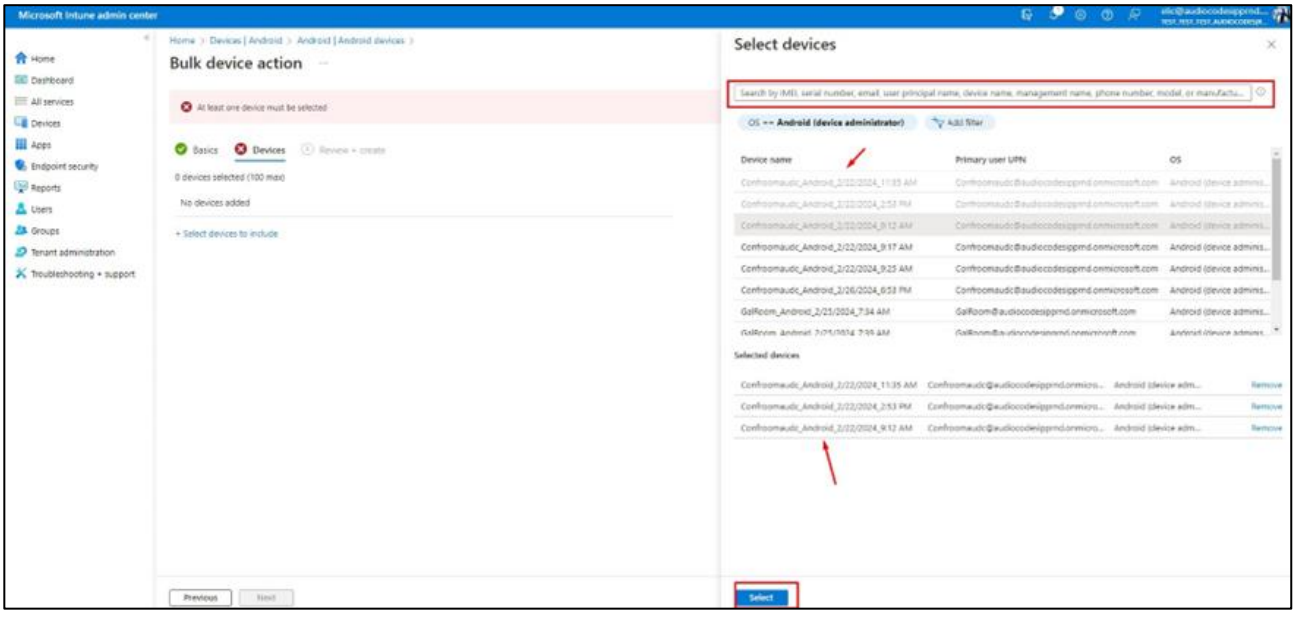


Note: The Intune admin center service is licensed according to the terms of individual licenses so not all network admins will be able to navigate to it. Check if the license you're using includes the service or not.

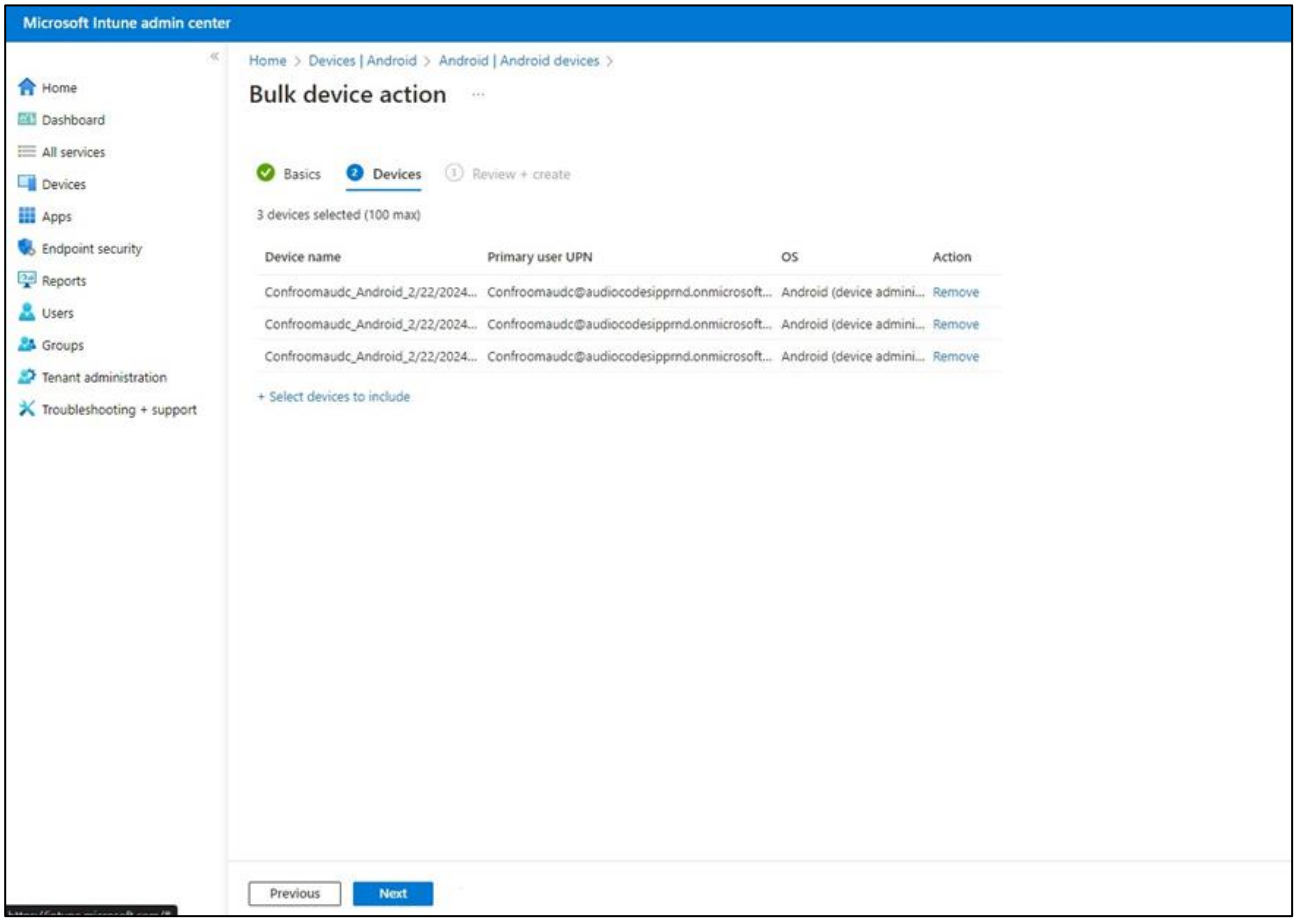
6. Click **Bulk device actions**.



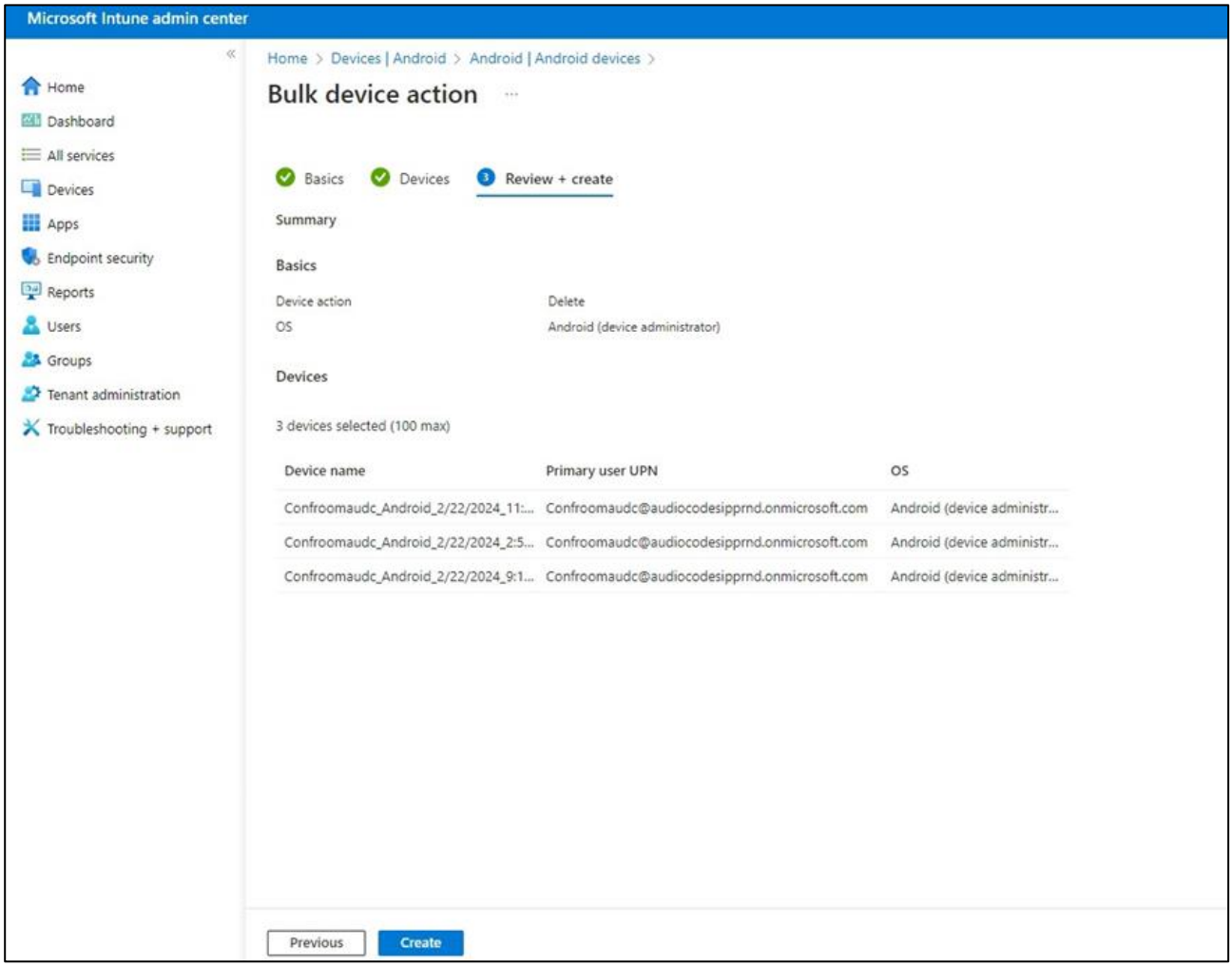
7. From the 'OS' drop-down under the **Basics** tab, select **Android (device administrator)**. From the 'Device action' drop-down, select **Delete**. Click **Next**.



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



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



10. 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.

This page is intentionally left blank.

5 Viewing RXV81 Status LEDs

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

Table 5-1: Viewing RXV81 LEDs to Determine Status

●	**Red / white / red & white**
White on	Device is powered on, signed in to Teams
White flashing	Device is in booting phase
Red on	Device is in mute (highest priority state)
Red flashing	Network connectivity lost / Device is in upgrade mode / RCU connectivity lost
Red + white on	Device is powered on, network is connected, but not signed into Teams
●	**Blue**
Blue on	In a call (active call or meeting)
Blue flashing	Incoming call
○	**Camera on/off**
White on	Camera on
White off	Camera off

This page is intentionally left blank.

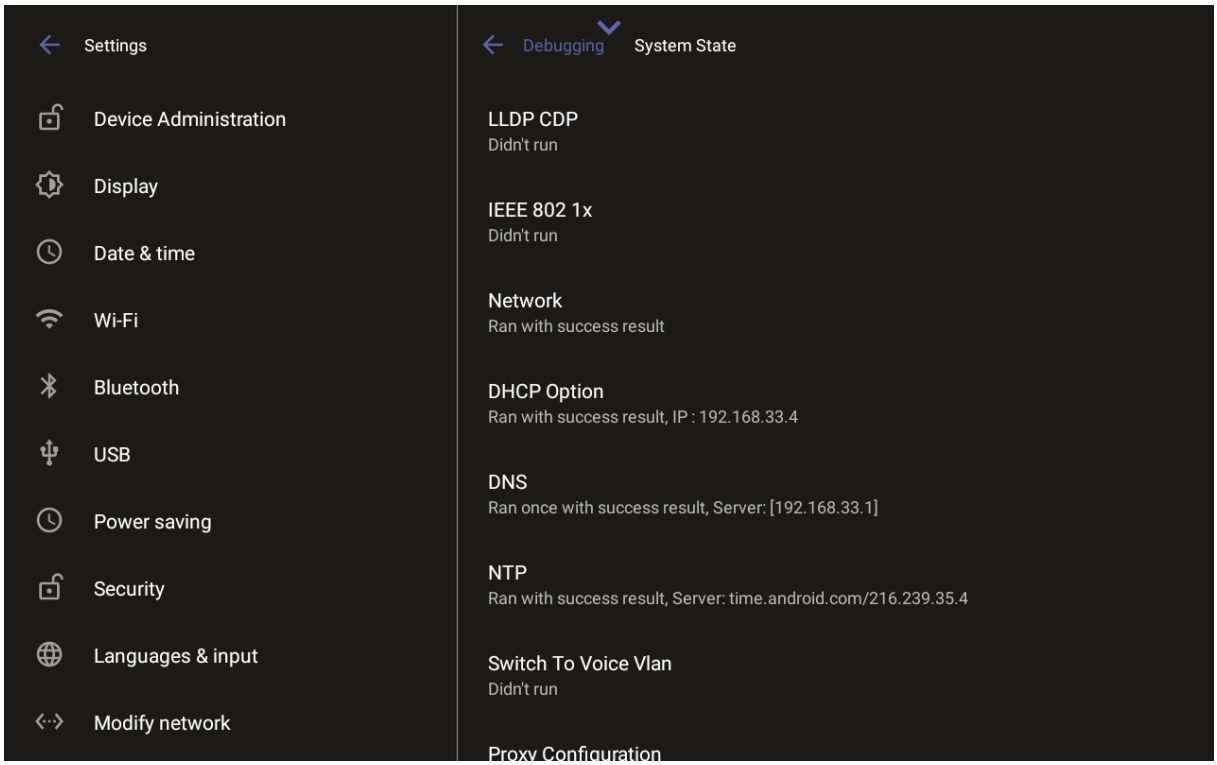
6 Monitoring Device Modules States

AudioCodes provides out-of-the-box troubleshooting capability: Admins can monitor the state of the device's 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*.

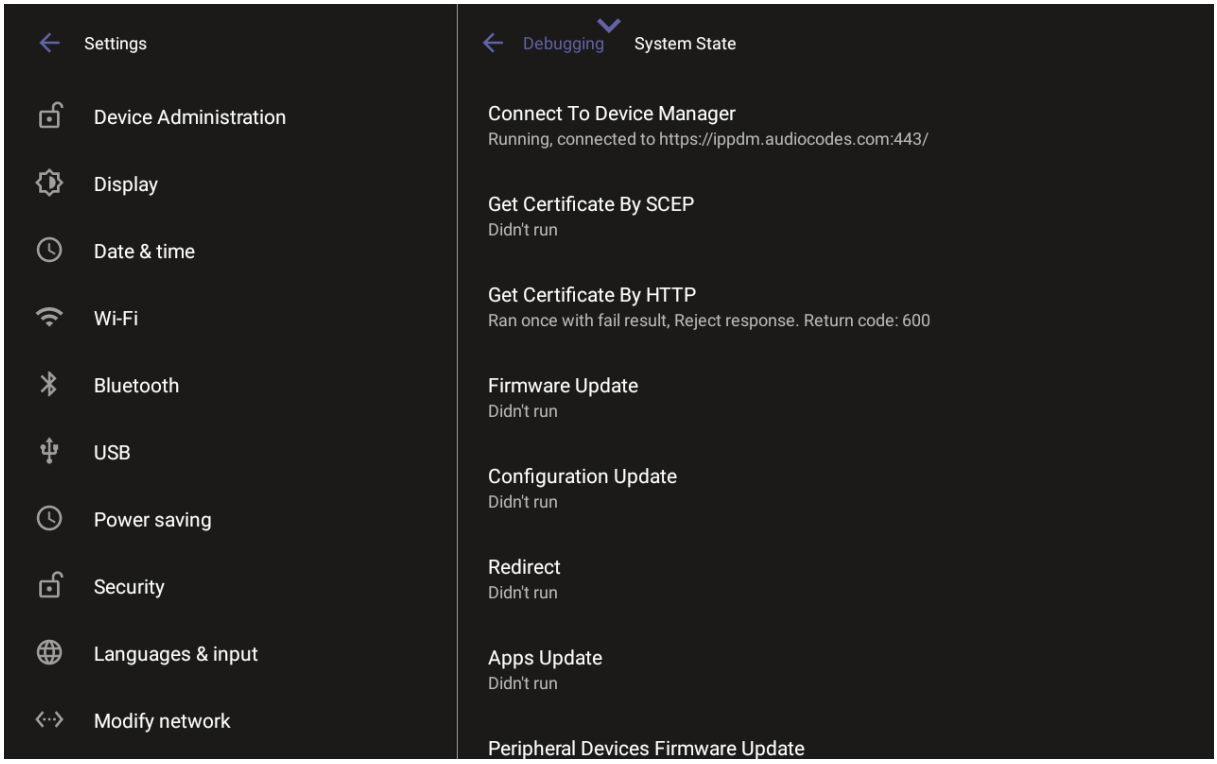
➢ **To monitor the device's modules state:**

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



Note:

- Each state displays its operational result: Successful or Failed
- For some states, the reason of failure will be displayed as well.



Note:

- Each state displays its operational result: Successful or Failed
- For some states, the reason of failure will be displayed as well.

7 Using RXV81 in Ad Hoc Peripheral Mode

In addition to standalone mode, RXV81 can be used in ad hoc peripheral mode. In this mode, you can connect RXV81 to a BYOD (Bring Your Own Device) (PC/laptop) running a UC client; the BYOD displays meeting video and content and meetings are controlled via the BYOD (join, accept, manage participants). Audio/video (camera ePTZ, mic mute) can be controlled via the UC client or the RC (camera on / off, mute, volume).

Supported RC actions that participants can perform during a video call / meeting when using the device with the ad hoc USB A/V peripheral include:

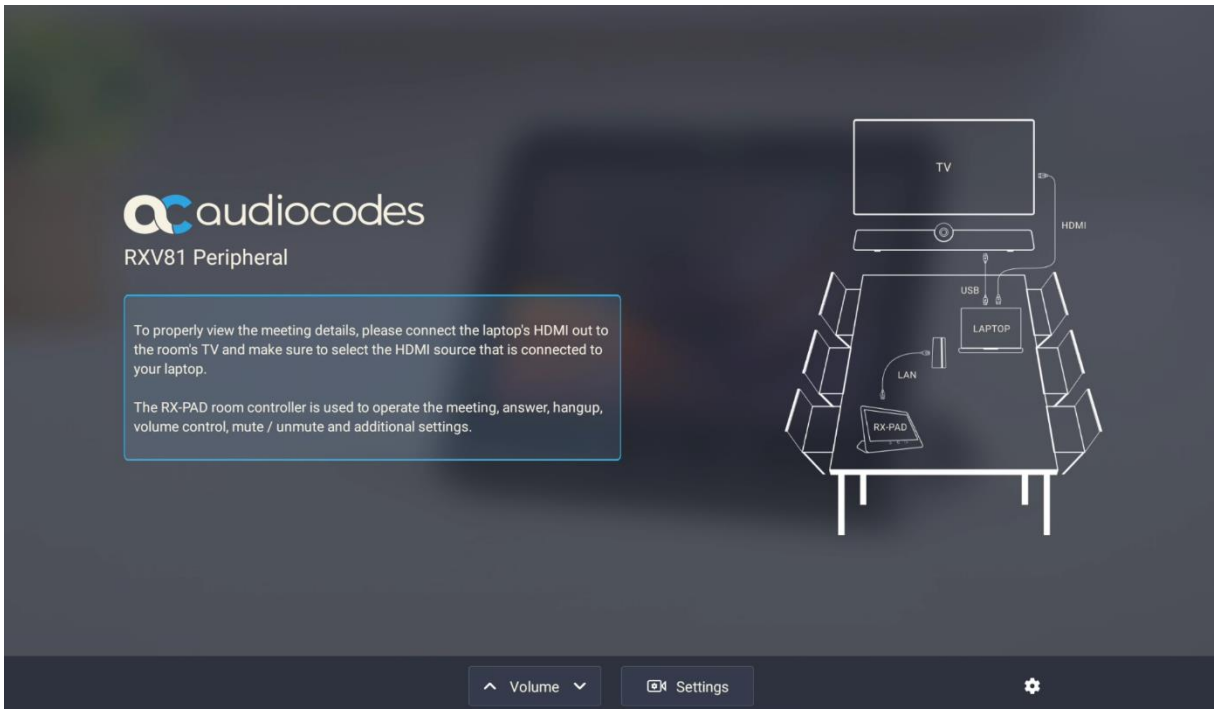
- Volume
- Mute
- Camera on/off

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

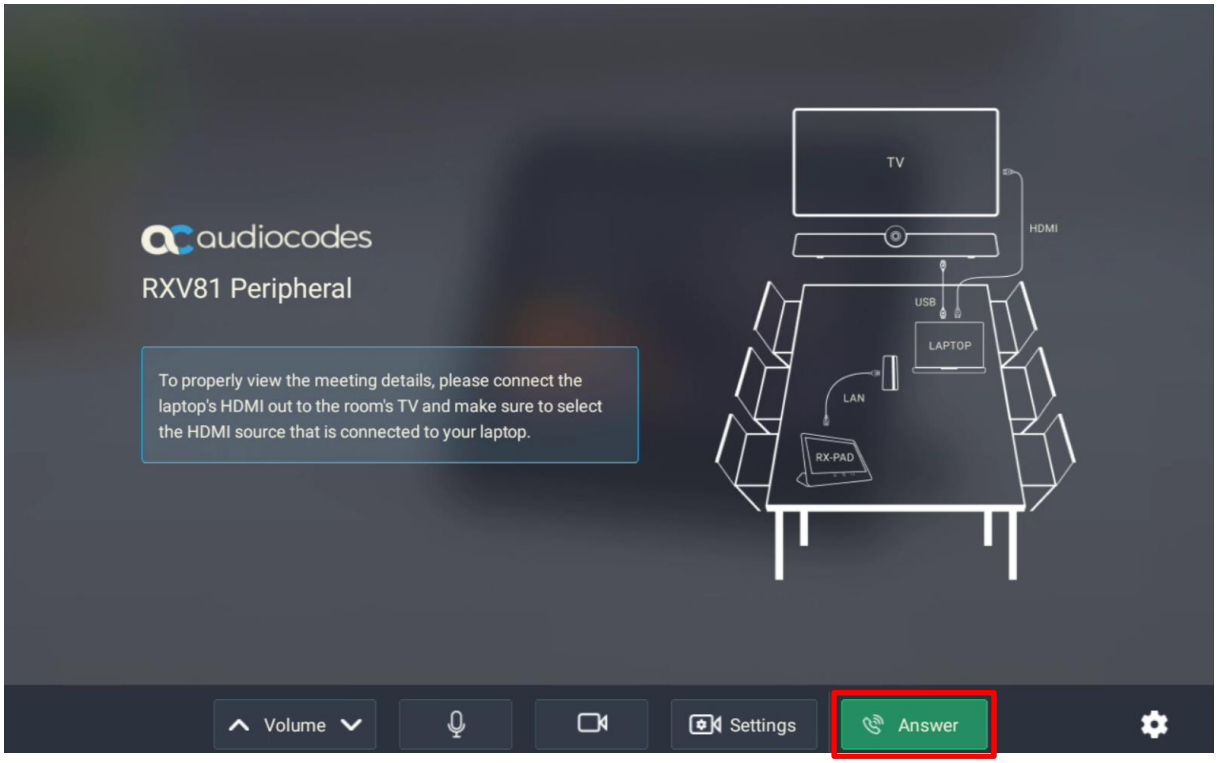
Ad hoc peripheral mode is a versatile feature designed to enhance RXV81 functionality. The mode enables seamless integration of RXV81 with a PC/laptop by utilizing RXV81's audio and camera capabilities as primary audio and camera sources for the PC/laptop.

➢ **To use RXV81 in ad hoc peripheral mode:**

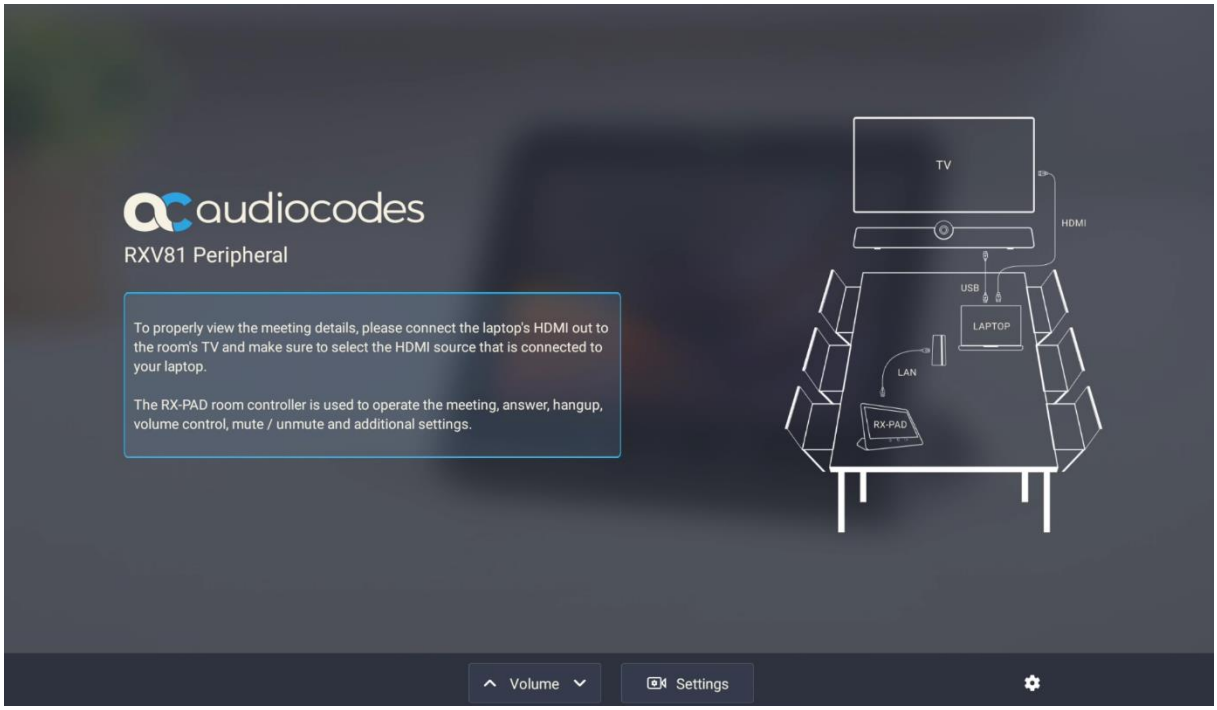
1. Connect the device's USB Type C port to a BYOD (Bring Your Own Device) (PC/laptop) running a UC client; the device automatically moves to ad hoc peripheral mode and RX-PAD displays the following:



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



3. View peripheral ad hoc mode displayed on RXV81 as follows:



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

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

> In addition to the USB cable already connected to your laptop, please connect your laptop to the TV using the HDMI cable to properly view meeting details and content sharing.
>
> On your TV, make sure to select the HDMI source that is connected to your laptop.
>
> Note that you can still use your RXV81 RC to increase or decrease volume, mute or unmute audio, and switch the camera on or off.

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

This page is intentionally left blank.

8 Updating the RXV81 MTR Remotely

For instructions on how to update RXV81 Microsoft Teams Room remotely, see https://docs.microsoft.com/en-us/microsoftteams/devices/remote-update.

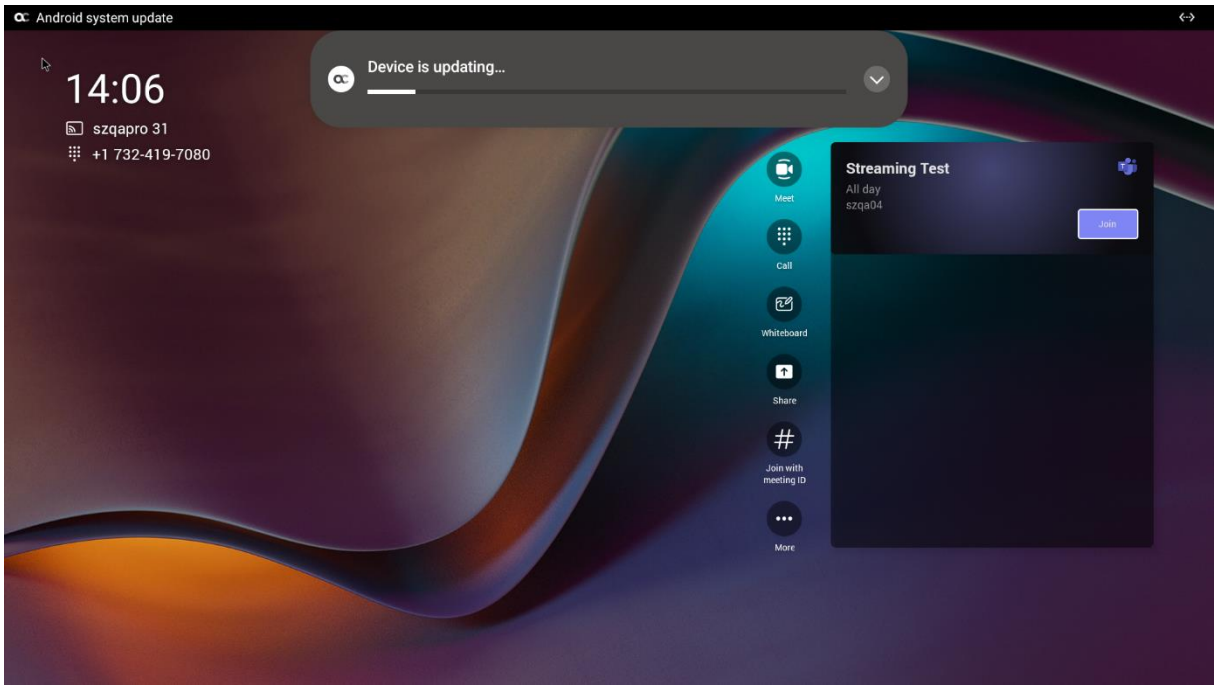
Note: Before an update is pushed to a device, the firmware detects whether the user is using the device or not. If they are, the user is notified and given an option to delay the update or apply it, nonetheless. The feature avoids disrupting users' ongoing activities on their devices, such as calls.

8.1 Updating RXV81 Audio and Camera Peripherals Firmware

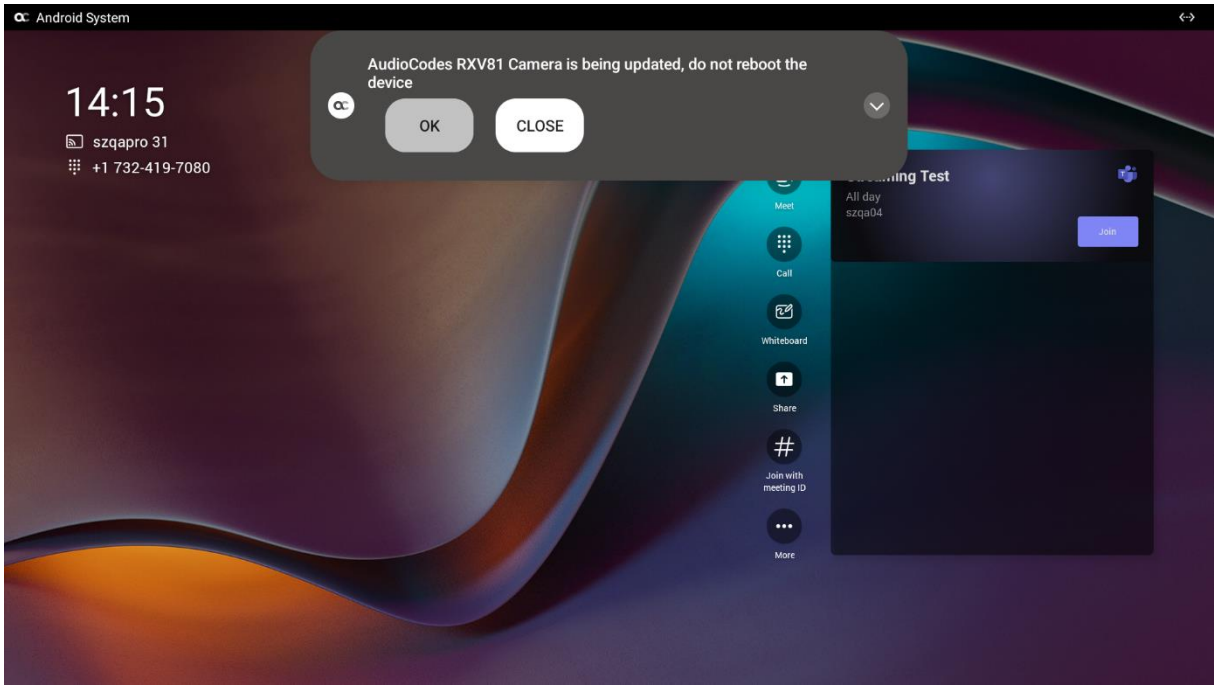
Updating RXV81 audio and camera peripherals firmware is a safe and streamlined process. Peripherals are updated at the same time as the RXV81 firmware update; audio and camera peripheral updates are integrated directly within the RXV81 firmware update process to ensure a safe overall update experience for the RXV81 device, prioritizing device integrity.

Over-the-air (OTA) firmware updates include 'Pre | Post Firmware Burn' scripts to check before audio / video (A/V) is updated. After an OTA update is downloaded but before it is burned, a PreFirmwareBurn script is executed. After the firmware is burned, a PostFirmwareBurn script is executed. Here's the user experience:

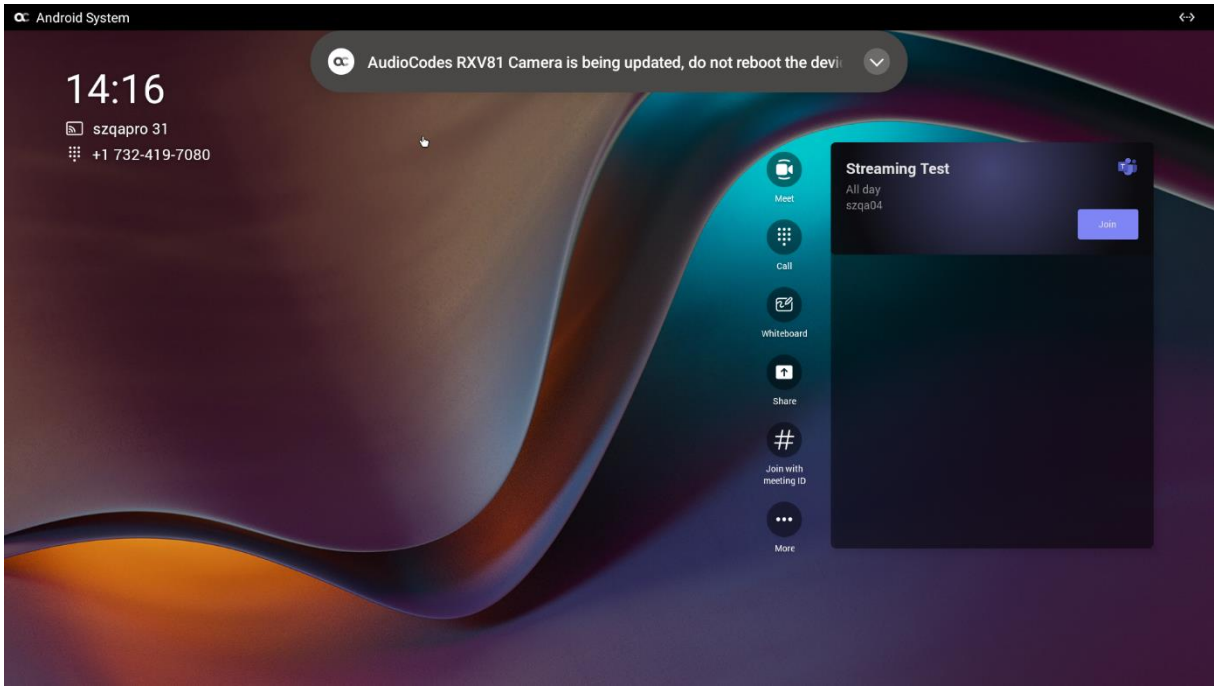
1. View 'Device is updating...'



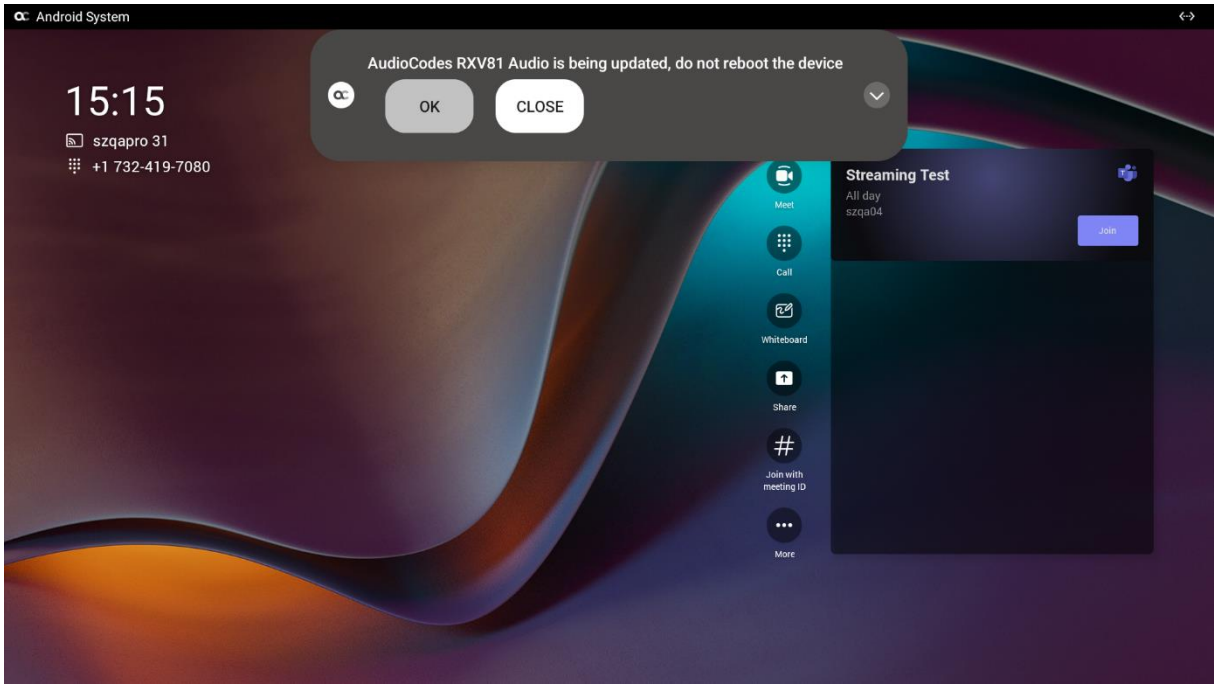
2. View the notification 'AudioCodes RXV81 Camera is being updated, do not reboot the device'.



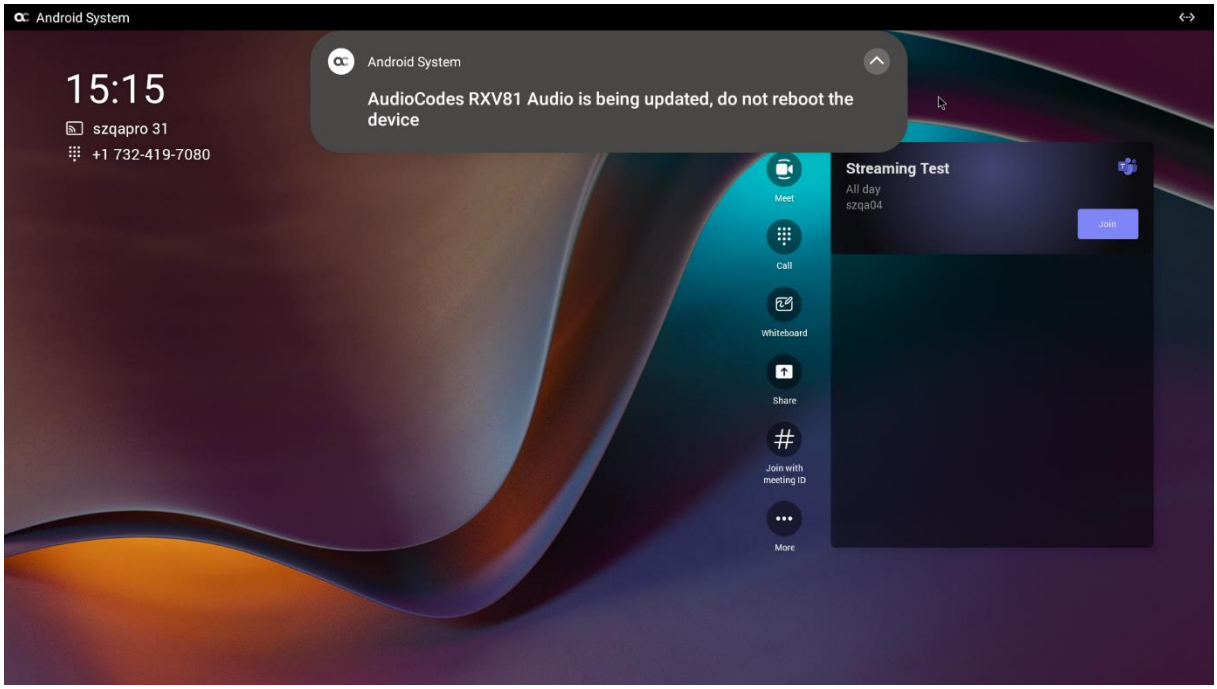
3. Click **OK**; view the following:



4. After the camera update, view the notification 'AudioCodes RXV81 Audio is being updated, do not reboot the device'.



5. Click **OK**; view the following:

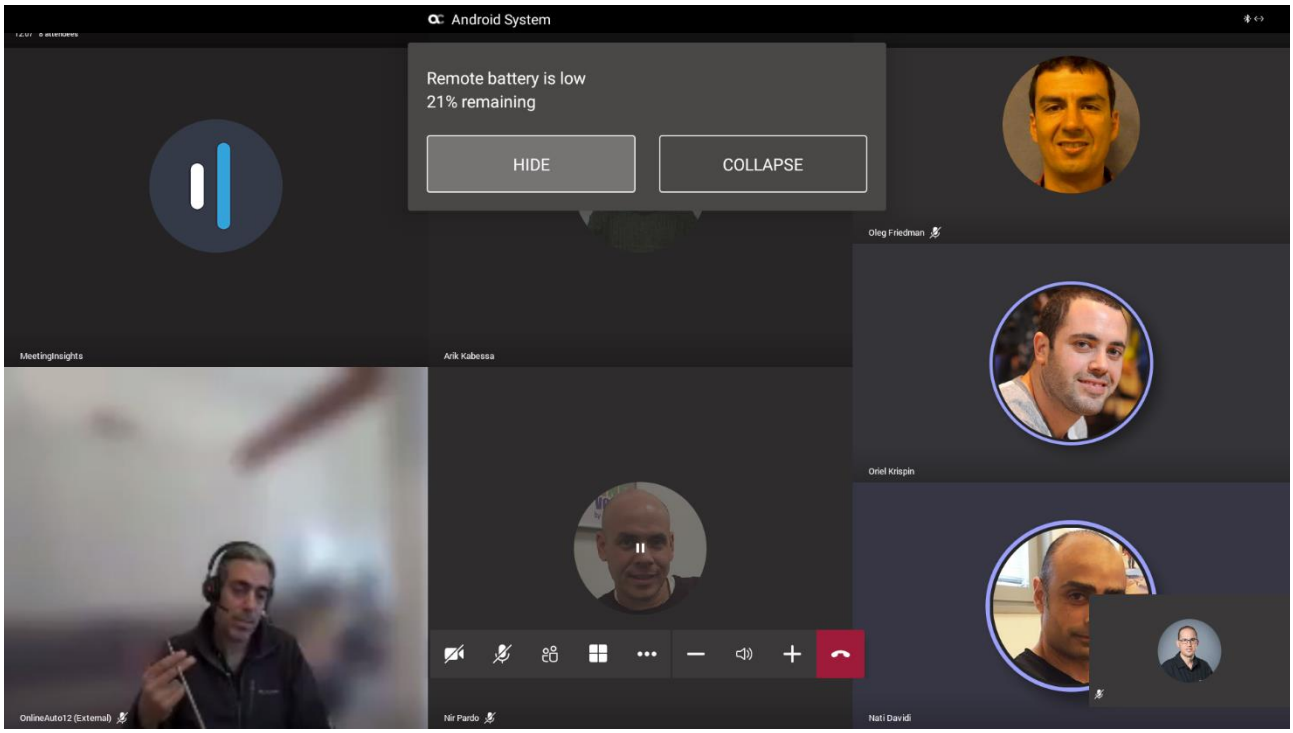


6. After the audio update, view a 'Restarting…' notification.

This page is intentionally left blank.

9 Replacing RC Batteries

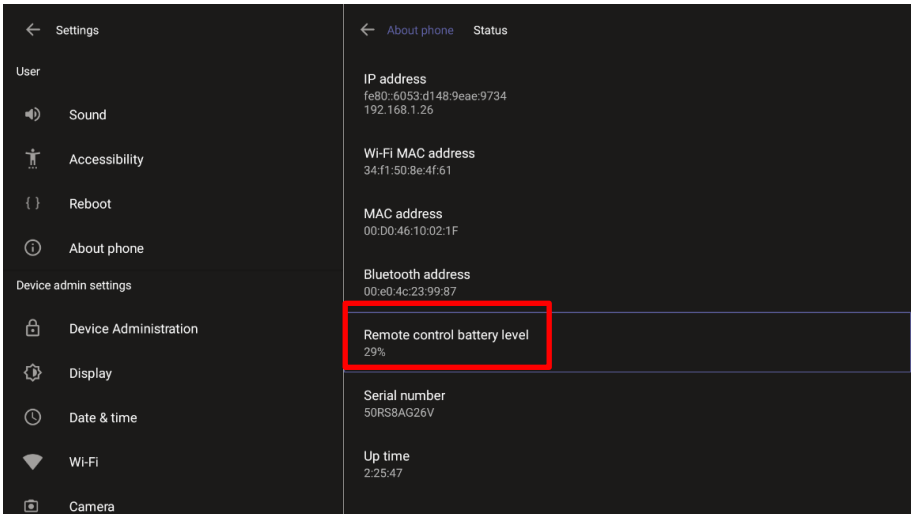
[Only applies to users who acquired the RC bundle] If the RC batteries run low, the RXV81 application notifies you about the issue. A notification is sent to the screen/TV as well as to AudioCodes' Device Manager if battery voltage level falls low, indicating what percentage level remains unused.



Select **HIDE** to conceal the notification.

9.1 Assessing RC Battery Level

[Only applies to users who acquired the RC bundle] You can determine the RXV81 remote controller's battery level through the Status screen (**About** > **Status**) using the setting **Remote control battery level**.



9.2 Restarting / Rebooting RXV81

RXV81 sometimes needs to be restarted / rebooted, for example, after inserting the Bluetooth dongle.

➢ **To restart / reboot RXV81:**

- Long-press the RC power on/off button for about five seconds (only applies to users with an RC)

  -or-

- Long-press the RXV81 back button for ~5 seconds, then release it.

9.3 Powering Down/Up RXV81

RXV81 can be powered down/up.

➢ **To power down RXV81:**

- Long-press the RXV81 back button for 12 seconds; the device is powered down.

➢ **To power up RXV81:**

- Long-press the RXV81 back button for 12 seconds; the device is powered up.

10 RX-PAD Meeting Room Controller

Note:

- Only applies to users who acquire the RXV81 bundle **TEAMS-RXV81-B10**.
- Optionally replaces RXV81's RC for management and control functions.
- See the RX-PAD Meeting Room Controller Pairing Guide for instructions how to pair the controller with RXV81.

AudioCodes' RX-PAD is a center-of-room intelligent touch controller that provides access to the RXV-81 meeting room.

RX-PAD enables capabilities such as one-click collaboration initiation with an integrated calendar, content sharing and camera adjustments, and more.

Requiring only a PoE cable for quick installation, RX-PAD leverages plug-and-play simplicity to provide a familiar Microsoft Teams meeting experience.

See AudioCodes' website here for more information about RX-PAD.

10.1 Using RX-PAD

Use the figure and the table following as a reference to using RX-PAD.

Table 10-1: Reference to Using RX-PAD

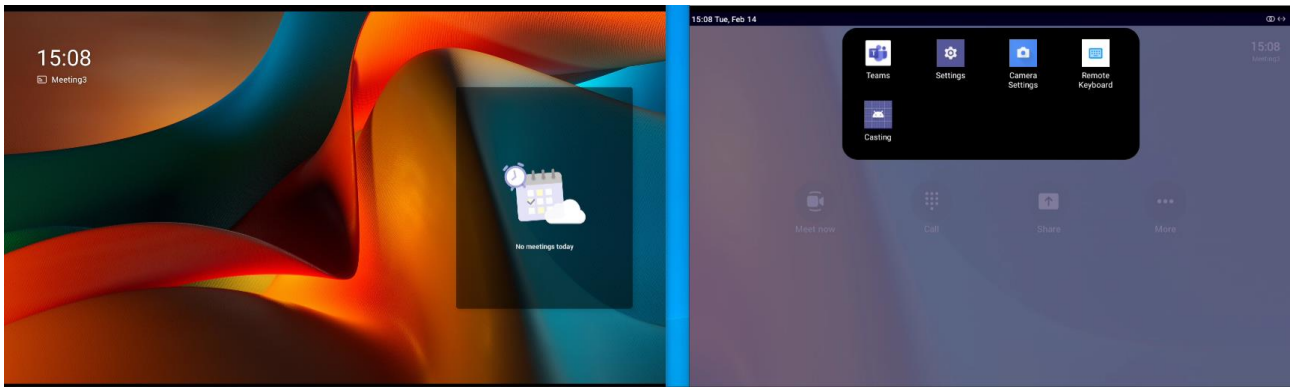
L-R	Description
1	'Back' button; press to return to the screen previously accessed.
2	Press to return to the home screen from any screen. Long-press to open the device's 'Settings' screen.
3	Press to access 'Camera Settings'.
4	Press to open administrator-related menus, including 'Settings'.
5	One-click to join with an integrated calendar for quick and rapid collaboration initiation.
6	Human proximity motion sensor concealed under the plastic that allows the user to hold their hand near the sensor location to 'wake up' the device while in screensaver mode, triggering automatic lighting to greet the user.
7	LED indications: ▪ If illuminated red (constantly, without flashing), it indicates 'No network'. ▪ Flashing red indicates a system alert, for example, when a user tries to charge via the device's USB port. ▪ Flashing yellow indicates that the device is in the process of a software upgrade.

10.2 Using RX-PAD to Adjust RXV81 Camera Settings

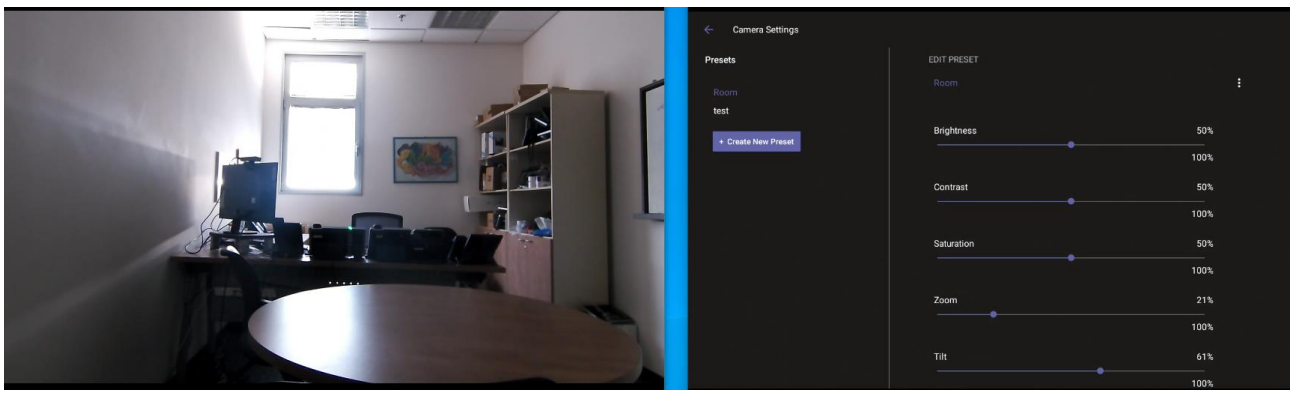
RX-PAD can be used to control RXV81 camera settings.

➢ **To adjust RXV81 camera settings:**

1. In RX-PAD, pull down the notification bar and select the **Camera Settings** icon -OR- on the physical interface of the RX-PAD, tap the camera icon (labeled 3 in the preceding figure).

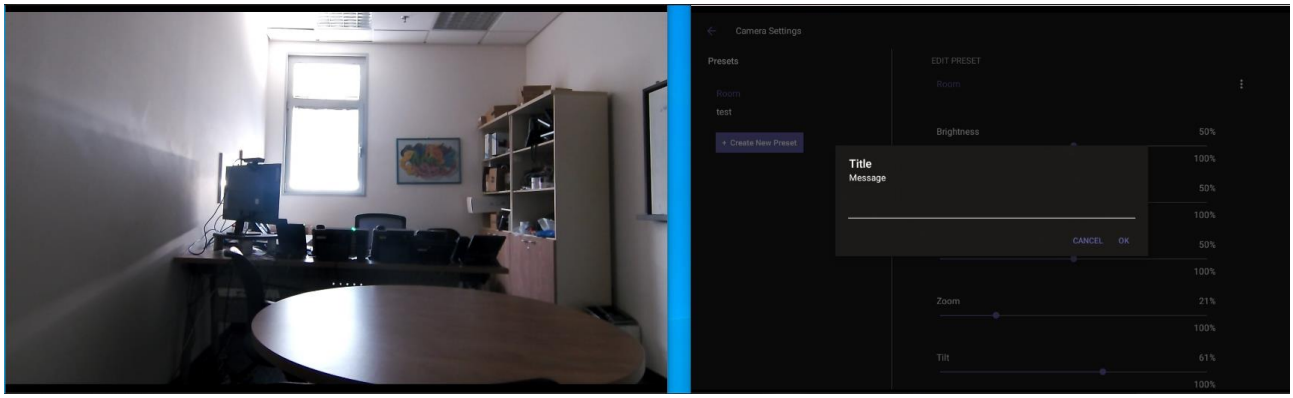


2. View the camera settings menu and a preview of the room in which RXV81 is located.



3. In the Camera Settings page, adjust the Brightness, Contrast, Saturation, Zoom and Tilt.

4. Optionally, save the current settings in the running preset, or save them in a separate preset using the **Create New Preset** button.



This page is intentionally left blank.

11 Remote Controller (RC)

Note: Only applies to users who acquire the RXV81 bundle **TEAMS-RXV81**. See here for bundle details.

The figure below shows AudioCodes' remote controller.

- The software on the remote controller is managed by RXV81.
- The remote controller leverages Bluetooth which enables full control and bi-directional communication (very much like touch control). See also Section 4.1.5.
- The keys on the remote controller (Mute, Teams) are illuminated.

Note: The remote controller flashes if the connection to RXV81 fails.

This page is intentionally left blank.

12 Android-based Teams Devices Parameters

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

- general/silent_mode = 0 (default)/1
- general/power_saving = 0 (default)/1
- phone_lock/enabled = 0 (default)/1
- phone_lock/timeout = 900 (default) (in units of seconds)
- phone_lock/lock_pin = 123456
- display/language = English (default)
- display/screensaver_enabled = 0/1
- display/screensaver_timeout = 1800 (seconds)
- display/backlight = 80 (0-100)
- display/high_contrast = 0 (default) /1
- date_time/timezone = +02:00
- date_time/time_dst = 0 (default) /1
- date_time/time_format = 12 (default) / 24
- network/dhcp_enabled = 0/1
- network/ip_address =
- network/subnet_mask =
- network/default_gateway =
- network/primary_dns =
- network/pecondary_dns =
- network/pc_port = 0/1
- office_hours/start = 08:00
- office_hours/end = 17:00
- logging/enabled = 0/1
- logging/levels = Verbose, Debug, Info, Warn, Error, Assert, None
- admin/default_password = 1234
- admin/ssh_enabled=0/1 (default)
- security/SSLCertificateErrorsMode = IGNORE, NOTIFICATION, DISALLOW (default)
- security/ca_certificate/[0-4]/uri – uri to download costumer's root-ca
- provisioning/period/daily/time
- provisioning/period/hourly/hours_interval
- provisioning/period/type = HOURLY, DAILY (default), WEEKLY, POWERUP, EVERY5MIN, EVERY15MIN
- provisioning/period/weekly/day
- provisioning/period/weekly/time
- provisioning/random_provisioning_time

International Headquarters
Naimi Park
6 Ofra Haza Street
Or Yehuda, 6032303, Israel
Tel: +972-3-976-4000
Fax: +972-3-976-4040

AudioCodes Inc.
80 Kingsbridge Rd.,
Piscataway, NJ 08854, USA
Tel: +1-732-469-0880
Fax: +1-732-469-2298

Contact us: https://www.audiocodes.com/corporate/offices-worldwide
Website: https://www.audiocodes.com/

©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, and 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-18261