

# RXV81 Microsoft Teams Rooms on Android Video Collaboration Bar

Version 1.19



**Microsoft Partner**

Gold Communications





---

## Table of Contents

---

<b>1</b>	<b>Introduction.....</b>	<b>9</b>
1.1	Highlights .....	9
1.2	Benefits.....	11
1.3	Hardware Features .....	11
1.4	Specifications.....	12
1.5	Security Guidelines .....	14
1.5.1	Microsoft Teams Security Guidelines .....	14
1.5.2	Android Level Security Hardening .....	14
1.5.2.1	Google Play Services .....	14
1.5.2.2	Running Android in Kiosk Mode .....	14
1.5.2.3	Screen Lock.....	15
1.5.2.4	AudioCodes Private Key.....	15
1.5.2.5	Android Debug Bridge (ADB) .....	15
1.5.2.6	App Signing .....	15
1.5.2.7	Web Browser .....	15
1.5.2.8	Remote Configuration Management .....	15
1.5.2.9	AudioCodes Device Manager Validation.....	15
1.5.2.10	Sandboxing.....	16
1.5.2.11	Keystore .....	16
1.5.2.12	Device Certificate .....	16
1.5.2.13	Data Protection.....	16
1.5.2.14	Device File System.....	16
1.5.2.15	Debugging Interface .....	16
1.5.3	Android Security Updates .....	16
1.5.4	AudioCodes Root CA Certificate .....	17
1.6	Certificate Enrollment using SCEP.....	18
1.7	Provisioning Certificates in .pfx Format .....	19
<b>2</b>	<b>Setting up the RXV81 .....</b>	<b>21</b>
2.1	Getting Started.....	21
<b>3</b>	<b>Signing in .....</b>	<b>23</b>
3.1	Multi-Cloud Sign-in.....	23
3.1.1	Remote Provisioning and Sign in from Teams Admin Center .....	23
<b>4</b>	<b>Getting Started.....</b>	<b>27</b>
4.1	Modifying Camera Settings .....	28
4.2	Starting a New Meeting.....	31
4.3	Dialing a Number .....	34
4.4	Enabling Proximity Join .....	35
4.5	Sharing a Whiteboard .....	36
4.6	About Microsoft Teams .....	38
4.7	Signing out.....	39
<b>5</b>	<b>Configuring Device Settings.....</b>	<b>41</b>
5.1	Configuring Device Admin Settings .....	44
5.1.1	Display Settings .....	44
5.1.2	Date & Time .....	46
5.1.3	Wi-Fi Settings.....	47
5.1.3.1	Connecting to an Available Wi-Fi Network.....	47
5.1.3.2	Manually Connecting to a Wi-Fi Network .....	48

5.1.4	Camera .....	51
5.1.4.1	Configuring Camera Frequency .....	52
5.1.5	Bluetooth .....	52
5.1.6	Security .....	53
5.1.7	Languages & input .....	55
5.1.8	Modify network .....	56
5.1.9	Calling .....	59
5.1.10	DSCP .....	60
5.1.11	Debugging .....	62
5.1.11.1	Log Settings   Collecting Logs .....	63
5.1.11.2	Remote Logging .....	65
5.1.11.3	Diagnostic Data .....	66
5.1.11.4	Reset configuration .....	67
5.1.11.5	Restart Teams app .....	67
5.1.11.6	Company Portal Login .....	67
5.1.11.7	Getting Company Portal Logs .....	67
5.1.11.8	Launch Mobile Teams .....	68
5.1.11.9	Debug Recording .....	68
5.1.11.10	Erase all data (factory reset) .....	69
5.1.11.11	Screen Capture .....	69
5.2	Performing Recovery Operations using the Power Button .....	70
5.3	Restoring Device Firmware via USB Disk .....	71
5.4	Configuring User Settings .....	72
5.4.1	Sound .....	72
5.4.2	Accessibility .....	72
5.4.3	Setting Live Captions .....	72
5.4.4	Hiding Names and Meeting Titles .....	72
5.4.5	Reboot .....	73
5.4.6	About .....	73
<b>6</b>	<b>Viewing LEDs to Determine Status .....</b>	<b>75</b>
<b>7</b>	<b>Using RXV81 in Ad Hoc Peripheral Mode .....</b>	<b>77</b>
<b>8</b>	<b>Updating Microsoft Teams Devices Remotely .....</b>	<b>79</b>
<b>9</b>	<b>Replacing Remote Controller Batteries .....</b>	<b>81</b>
9.1	Assessing the RC's Battery Level .....	81
9.2	Restarting / Rebooting the RXV81 .....	82
9.3	Powering Down/Up the RXV81 .....	83
<b>10</b>	<b>Supported Parameters .....</b>	<b>85</b>

---

## List of Figures

---

Figure 4-1: Home Screen .....	28
Figure 4-2: Login when the RXV81 is in <i>idle state</i> .....	28
Figure 4-3: Camera settings .....	30
Figure 4-4: New meeting – Invite someone .....	31
Figure 4-5: New meeting – Enter the name of a person .....	31
Figure 4-6: New meeting – Select the name of a person .....	32
Figure 4-7: Dial pad .....	34

---

## List of Tables

---

Table 1-1: Specifications .....	12
Table 1-2: SCEP Parameters .....	18
Table 5-1: Configuration File Wi-Fi Parameters .....	49
Table 5-2: Recovery Operation Options using the RXV81's Power Button .....	70
Table 6-1: Viewing RXV81 LEDs to Determine Status .....	75

This page is intentionally left blank.

## 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: Jan-29-2023

## Trademarks

AudioCodes Ltd. All rights reserved. AudioCodes, AC, HD VoIP, HD VoIP Sounds Better, IPmedia, Mediant, MediaPack, What's Inside Matters, OSN, SmartTAP, VMAS, VoIPerfect, VoIPerfectHD, Your Gateway To VoIP, 3GX, VocaNom, AudioCodes One Voice and CloudBond 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.

## 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
One Voice Operation Center (OVOC) Release Notes
One Voice Operation Center (OVOC) User's Manual
Device Manager Administrator's Manual

This page is intentionally left blank.



# 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.

The 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, the 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 the remote control (RC).

In addition to standalone mode, the RXV81 can be used in ad hoc peripheral mode. In this mode, customers connect the 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.

The 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.

## 1.1 Highlights

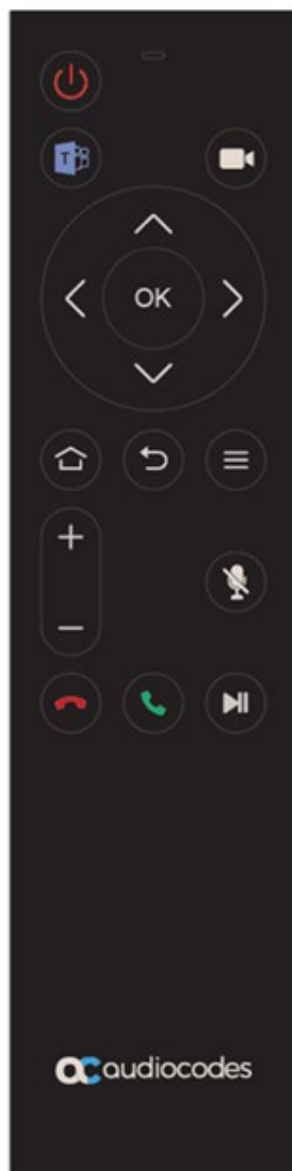
RXV81 feature highlights:

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

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

- **Unique Bluetooth Remote Control.**

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 (12M Storage)**  
Covers a 110° viewing angle capturing every seat in the room even in tight spaces with challenging lighting conditions. D: 120°/ H: 110°/ V: 75°
- **Easy to Manage from Anywhere.**  
Enhance the meeting experience with centralized device management and monitoring from any location.
- **Peripheral Mode.**  
The 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 managed Bluetooth remote control unit.
- Managed using AudioCodes' One Voice Operations Center (OVOC) Device Manager or Microsoft's Teams admin center (TAC).

## 1.3 Hardware Features

- The 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: 120°/ H: 110°/ V: 75°
- Adjustable camera position with ePTZ support - 5x zoom - digital 5x zoom in. Manually vertically (up/down) adjustable  $\pm 15^\circ$ .
- 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 Specifications

The following table shows the RXV81 specifications.

**Table 1-1: Specifications**

Feature	Details
<b>Video capabilities</b>	<ul style="list-style-type: none"> <li>Ultra HD 4k image sensor</li> <li>Super-wide angle horizontal field of view: 110°</li> <li>Lens: Fixed focus</li> <li>ePTZ capable, digital 5x zoom in</li> <li>Output resolution: 1080p</li> <li>Frame rate: 30 fps</li> <li>Manually adjustable, vertically (up/down) ±15°</li> <li>High Dynamic Range (HDR) automatically ON - Wide Dynamic Range (WDR).</li> </ul>
<b>Audio</b>	<ul style="list-style-type: none"> <li>Full duplex, noise suppression, acoustic Echo Cancellation, voice separation</li> <li>6x beamforming microphone array</li> <li>Voice pickup range: 4.5m (15ft)</li> <li>10W speaker</li> </ul>
<b>Device Interfaces</b>	<ul style="list-style-type: none"> <li>HDMI output to TV</li> <li>Power/reset button</li> <li>USB 3.0 Type A (host) marked 1 to allow touch LCD or connectivity to wireless KB via BT USB dongle</li> <li>Ethernet: 10/100/1000 Mbps (RJ-45) network interface</li> <li>USB2.0 Type-C (device) marked 2 to connect to PC/MAC BYOD device (peripheral mode)</li> <li>3 status LEDs indicating camera on/off, mute on, call state, device health</li> <li>Wi-Fi (dual band support)</li> <li>Bluetooth 5.0</li> <li>12V/3A DC power input</li> <li>Bluetooth managed remote controller</li> </ul>
<b>Network Provisioning</b>	<ul style="list-style-type: none"> <li>TCP/IP (IPv4), DHCP/ static IP; Time and date synchronization via SNTP; VLAN support; QoS support: IEEE 802.1p/Q tagging (VLAN)</li> <li>Layer 3 TOS and DSCP RTCP support: (RFC 1889)</li> <li>IP address configuration: TCP/IP (IPv4), DHCP/static IP Time and date synchronization: SNTP</li> <li>QoS support: IEEE 802.1p/Q tagging (VLAN), Layer 3 TOS and DSCP RTCP support: (RFC 1889)</li> </ul>
<b>OS</b>	<ul style="list-style-type: none"> <li>Android 9.0 with short-term roadmap for Android 12</li> </ul>
<b>Security</b>	<ul style="list-style-type: none"> <li>Encryption: TLS (Transport Layer Security), SRTP encryption for media, AES256</li> <li>Network Access Control: IEEE 802.1x</li> <li>Built-in certificate</li> </ul>
<b>Management</b>	<ul style="list-style-type: none"> <li>AudioCodes Device Manager, a plugin of AudioCodes One Voice Operations Center (OVOC)</li> </ul>
<b>Microsoft Teams Features (Android MTR)</b>	<ul style="list-style-type: none"> <li>✓ Calendar integration (with meeting preview) and one click to join Teams meetings</li> <li>✓ Meet now option</li> <li>✓ Simple sign-in interface from browser or smartphone with a code</li> </ul>

Feature	Details
	<ul style="list-style-type: none"> <li>✓ 'Direct guest join' to allow joining a third-party meeting</li> <li>✓ 'Cast info' from mobile to the RXV81 screen over Bluetooth</li> <li>✓ 'Room remote' using Teams mobile app allowing to control the RXV81</li> <li>✓ Remote sign-out from Microsoft Teams admin center (TAC).</li> <li>✓ Hide names and meeting titles for individual devices</li> <li>✓ Meeting stage</li> <li>✓ Multi-spotlight</li> <li>✓ Docked meeting controls</li> <li>✓ Reactions</li> <li>✓ Control camera/mic for attendees</li> <li>✓ Live Captions in regular one-on-one calls and in Teams meetings</li> <li>✓ Whiteboard support when signed in with personal account (short term roadmap for whiteboard support with room account)</li> <li>✓ Multi-cloud sign-in support</li> </ul> <ul style="list-style-type: none"> <li>▪ Remote provisioning and sign-in from TAC</li> </ul>
<b>RXV81 Device Feature Set</b>	<ul style="list-style-type: none"> <li>▪ Camera settings with different privileges for user and Admin</li> <li>▪ In idle (Admin) and during a call/meeting (all users), long-pressing the camera button on the RC allows: <ul style="list-style-type: none"> <li>✓ Defining/editing a new preset</li> <li>✓ Moving to different presets</li> <li>✓ Changing all settings options</li> </ul> </li> <li>▪ Video quality: Resolution of 1080p on the decoder side and 720p on the encoding side</li> <li>▪ RXV81 integration with AudioCodes OVOC-DM</li> <li>▪ RXV81 Alerts to AudioCodes OVOC-DM: <ul style="list-style-type: none"> <li>✓ Notification sent to screen/TV and to Device Manager if Remote Control is disconnected or if it's malfunctioning</li> <li>✓ Notification sent to screen/TV and to Device Manager if Remote Control battery voltage level falls low, indicating what percentage level remains unused</li> <li>✓ Remote Control flashes if the connection to the RXV81 fails.</li> </ul> </li> <li>▪ Camera frequency set per power supply: <ul style="list-style-type: none"> <li>✓ 110V – 60Hz</li> <li>✓ 220V – 50Hz</li> </ul> </li> <li>▪ Shortcut keys for administrators to manually perform recovery operations</li> <li>▪ Ad Hoc Peripheral Mode allows connecting the RXV81 via USB to the PC as a peripheral device (Feature in Preview)</li> </ul>

## 1.5 Security Guidelines

The 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

### 1.5.1 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](#)

### 1.5.2 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.

#### 1.5.2.1 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.

#### 1.5.2.2 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).

### 1.5.2.3 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.

### 1.5.2.4 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.

### 1.5.2.5 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.

### 1.5.2.6 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.

### 1.5.2.7 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.

### 1.5.2.8 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.

### 1.5.2.9 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.

#### 1.5.2.10 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.

#### 1.5.2.11 Keystore

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

#### 1.5.2.12 Device Certificate

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

#### 1.5.2.13 Data Protection

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

#### 1.5.2.14 Device File System

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

#### 1.5.2.15 Debugging Interface

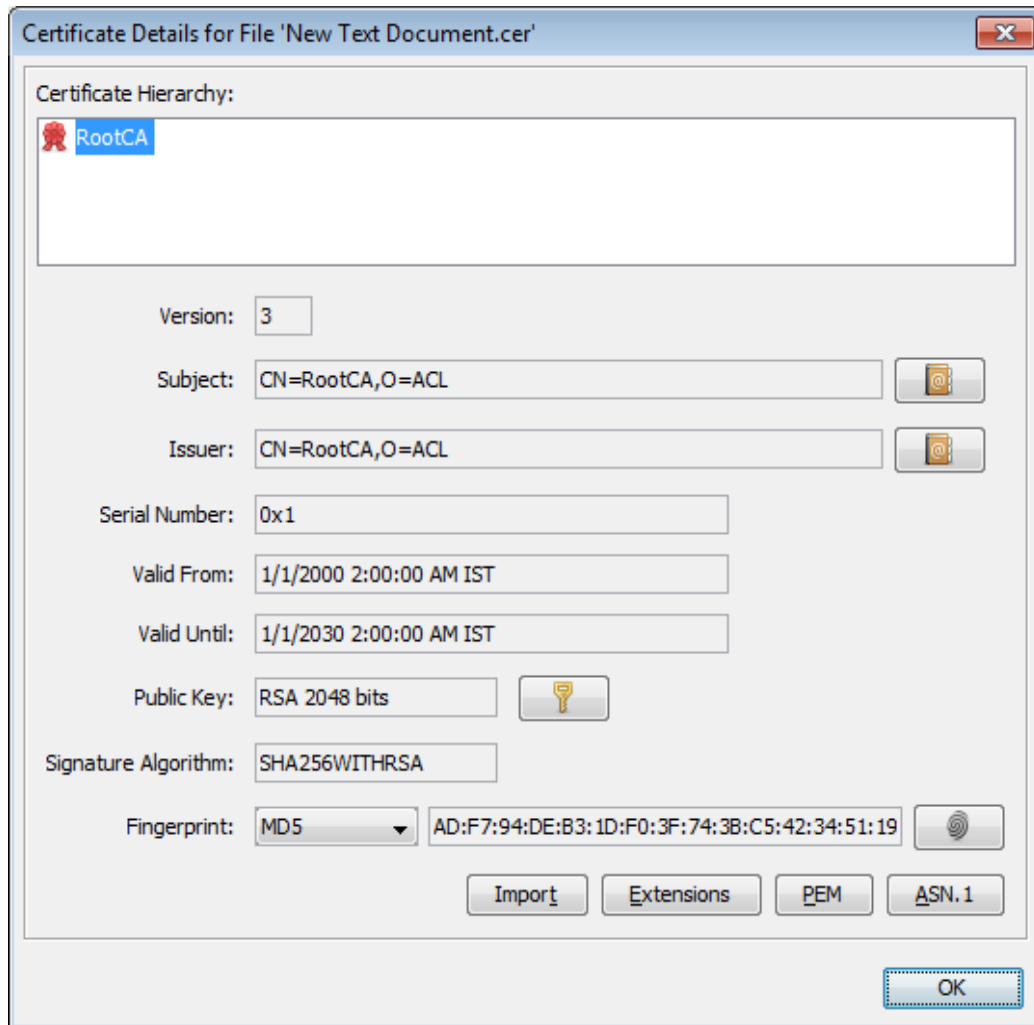
- The device leverages SSH as a debugging interface.
- AudioCodes recommends that customers disable SSH on the device – this can be done via the AudioCodes Device Manager (OVOC).
- AudioCodes recommends changing the Admin password from the default, which can be done via Teams Admin Center or AudioCodes 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.

### 1.5.3 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> ).



## 1.5.4 AudioCodes Root CA Certificate



```
-----BEGIN CERTIFICATE-----
MIIDMTCCAhmGAWIBAgIBATANBgkqhkiG9w0BAQsFADAfMQwwCgYDVQQKEwNBQ0wx
DzANBgNVBAMTB1Jvb3RDQTAeFw0wMDAxMDEwMDAwMDBaFw0zMDAxMDEwMDAwMDBa
MB8xDDAKBgNVBAoTA0FDTDEPMA0GA1UEAxMGUm9vdENBMTIIBIjANBgkqhkiG9w0B
AQEFAAOCAQ8AMIIBCgKCAQEA6GK495KUCXAm/UE17G4/cjnZN4LNaxYEEYzbfZL0a
EhgSKYt/LQ+iUcDhojsneusNgrcGkpWkklKsGsvGWmSRNULV01CW+TX2VJN73+hh
V0uzhyOIYAUhbDaoqNM6Kp5b7sJ1ew4Ig9kfd/ma9Cz15koESLlw/inLj/r+rD96
mUCPElWrKspv7Qy4I14fsK/yMArixRopTL1munVVPpSFM9Jh8IY3JHyr5CQJXKKs
EhGAJsnHaRqsR2Su3X/WtslgEF+cvP34pxhlhFL29nMfnaFATSS3rgGaFlSv11ZS
esLMqkWjp9cqGYrvt7K61sYnvMMb+o/KbWqVokXb+Fr7bwIDAQABO3gwdjAMBgNV
HRMEBTADAQH/MB0GA1UdDgQWBBDQXySn9hz15lDraZ+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-----
```

## 1.6 Certificate Enrollment using SCEP

[Feature in preview] 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 1-2: 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): <b>3EBE50003ABF1DF5E6B5A3230B02B856</b>
security/SCEPEnroll/password_challenge	Define the enrollment challenge password. Default value: NULL. Network admins must set its value to (for example): <b>7A7F9FC4BB7625F0935E67EA6D6322ED</b>
security/SCEPServerURL	Define the NDES server's URL. Default: NULL. Network admins must set its value to (for example): <b>https://ndes_server</b>
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.

## 1.7 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.

Device pfx (*.pfx)	PWD	<input type="text"/>	<input type="text"/>	<input type="button" value="Browse"/>
--------------------	-----	----------------------	----------------------	---------------------------------------



**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.

This page is intentionally left blank.

## 2 Setting up the RXV81



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

- Package contents
- Mounting
- Cabling

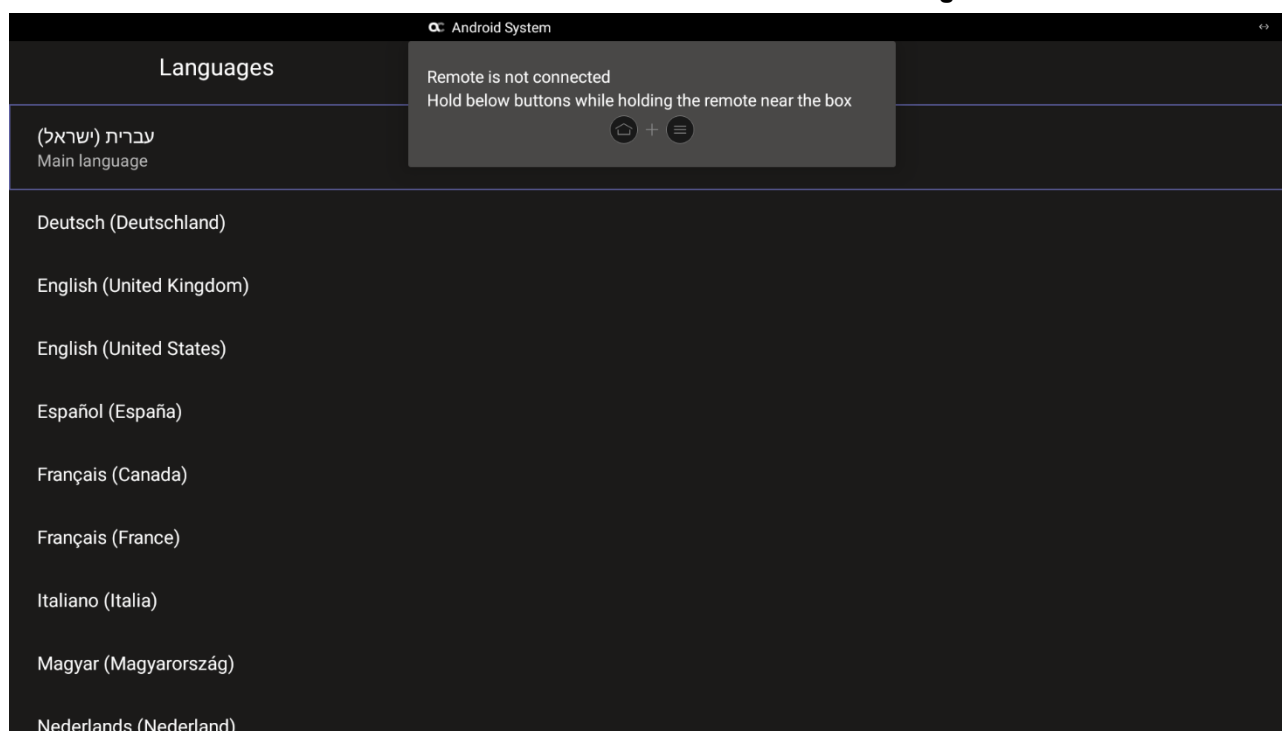
### 2.1 Getting Started

After mounting and cabling the RXV81 device as shown in the *Deployment Guide*, pair the supplied remote control with the RXV81. The instructions here show how to pair.

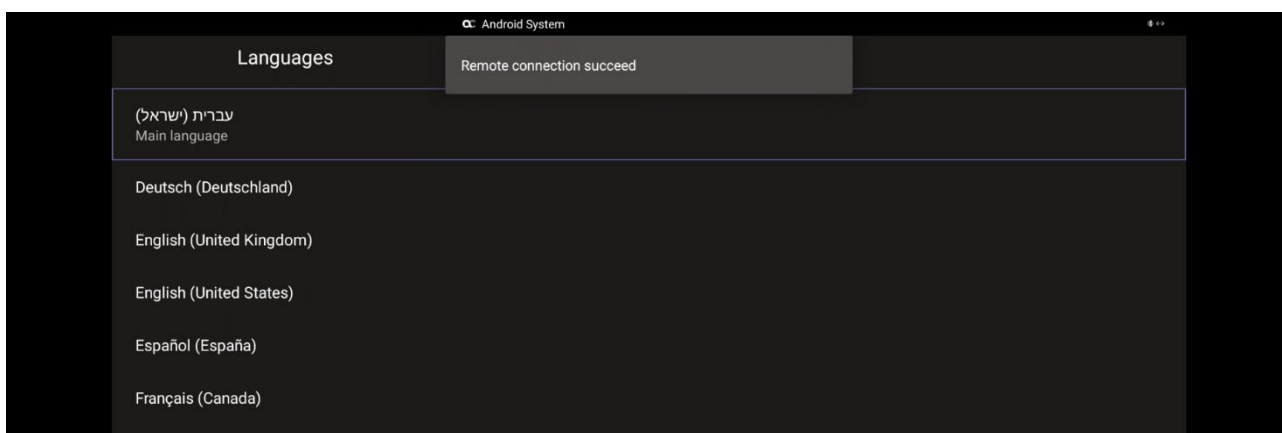
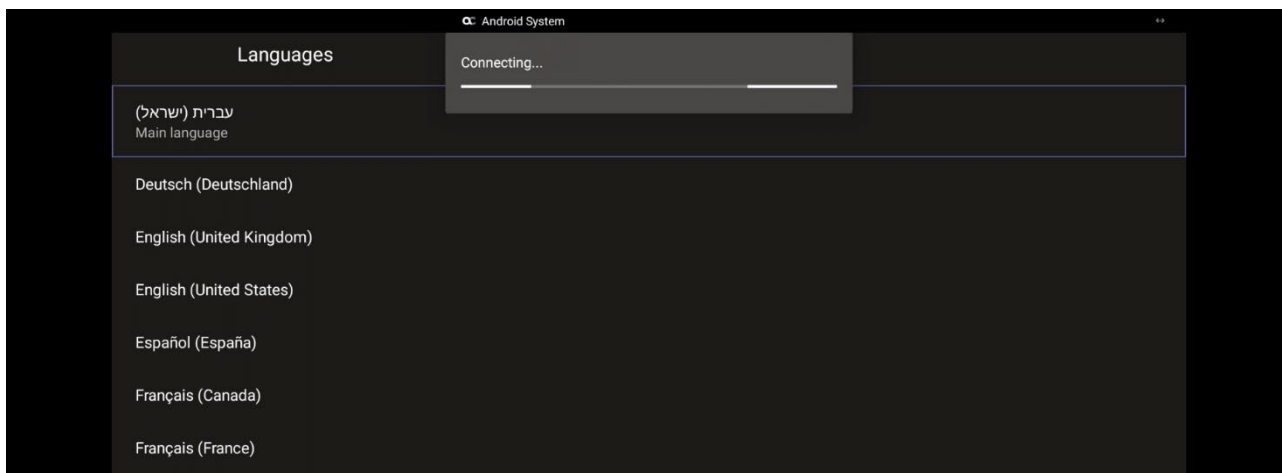
➤ **To pair the RC with the RXV81:**

1. After cabling, remove the RC from its packaging and insert the batteries supplied into it.
2. View in the display the message:

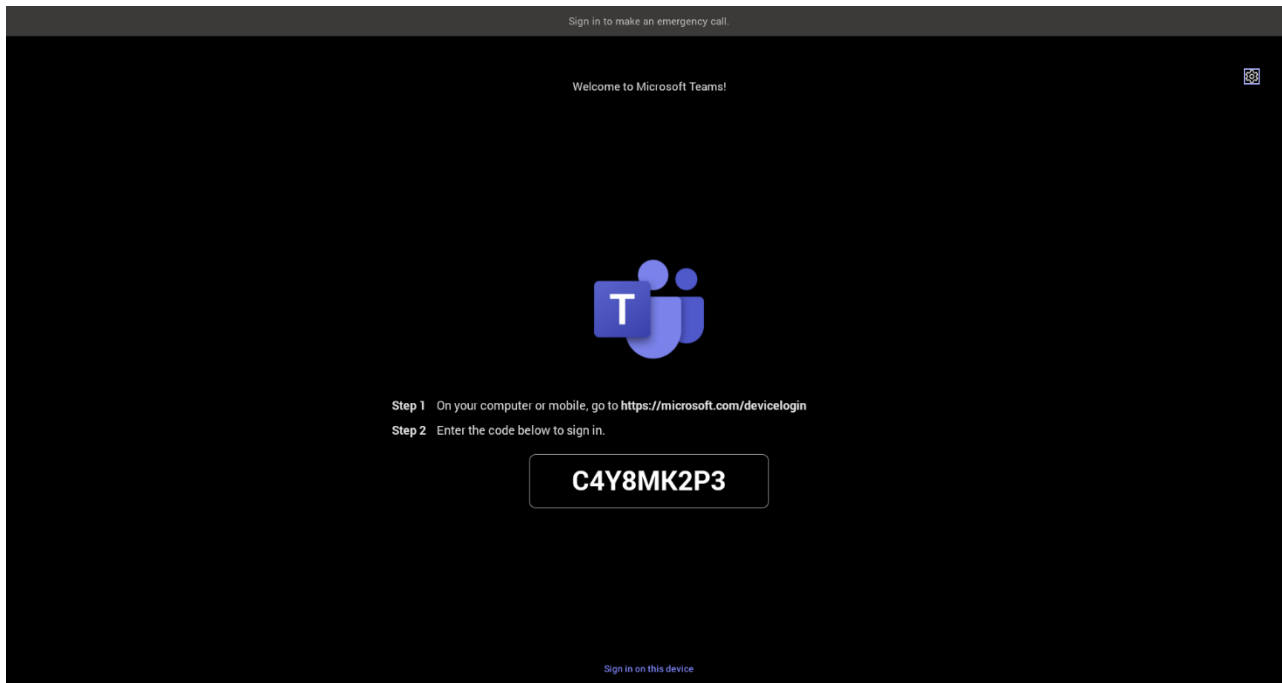
**Remote is not connected. Hold below buttons while holding the remote near the box.**



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.

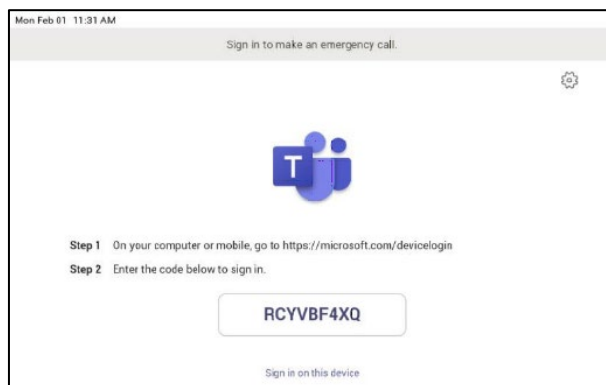


### 3 Signing in



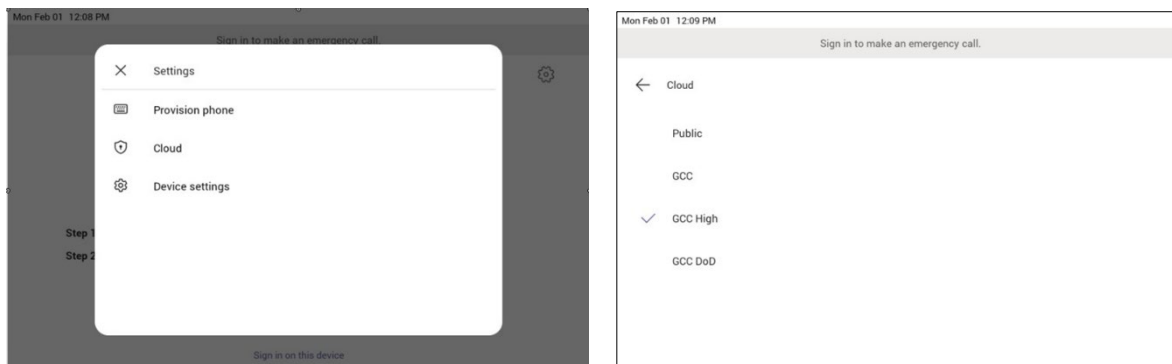
**Note:** See the *RXV81 Standalone Video Collaboration Bar Deployment Guide* shipped with the product or available from AudioCodes for detailed information on how to sign in to the device.

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.



#### 3.1 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.



##### 3.1.1 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.

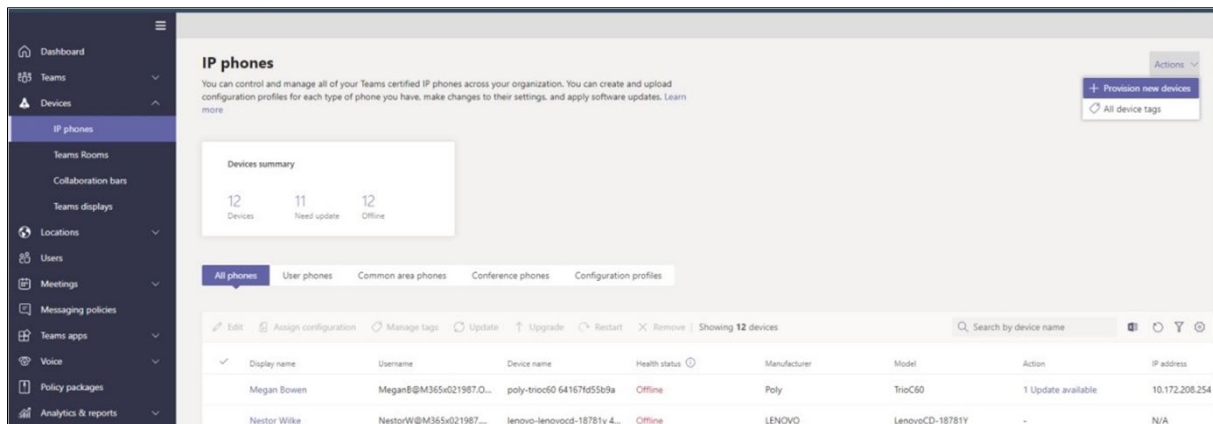
IT admins can remotely provision and sign in to a Teams device.

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.

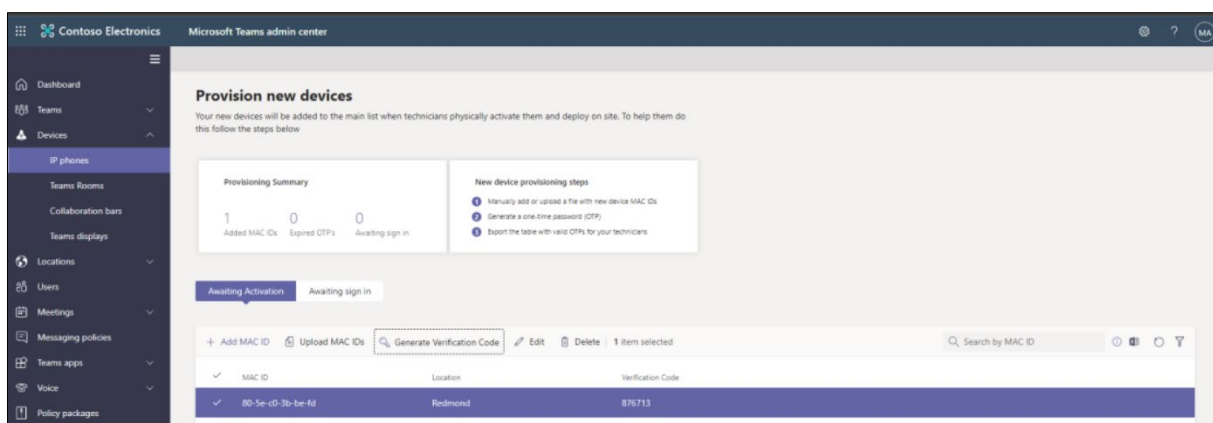
Upload a file to add a device MAC address

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.

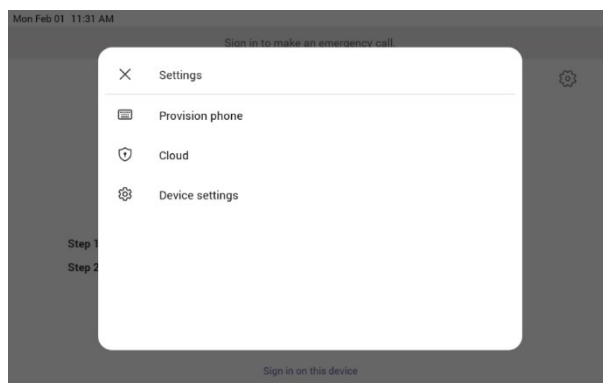


You'll need to provide the list of MAC IDs and verification codes to the field technicians. You can export the detail directly in a file and share the file with the technician who is doing the actual installation work.

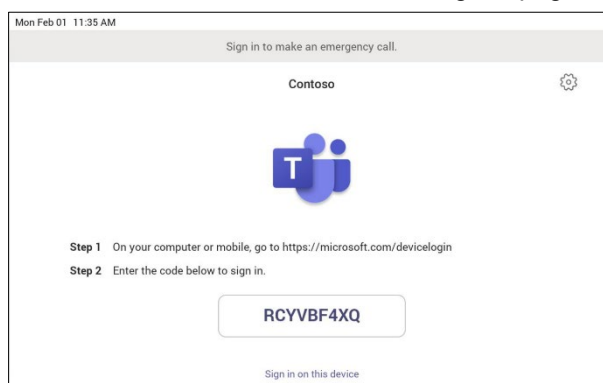
*Step 3: Provisioning on the device*

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**.





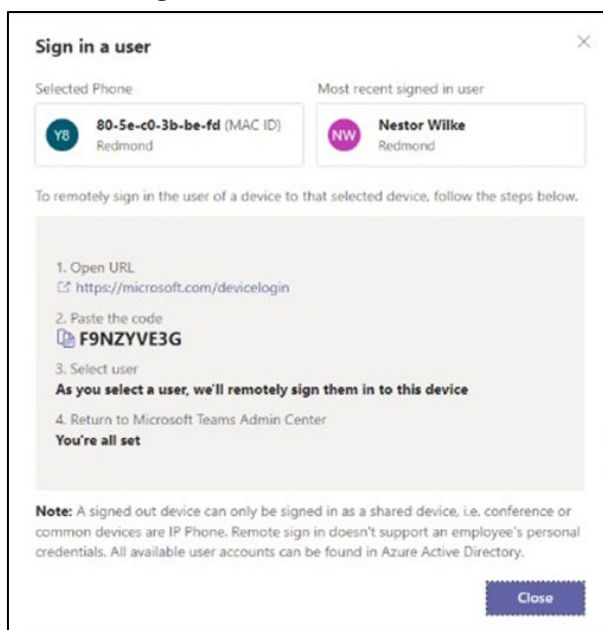
The technician is then expected to enter the device-specific Verification code that was provided in the Teams admin center on the phone's user interface. Once the device is provisioned successfully, the tenant name will be available on the sign in page.



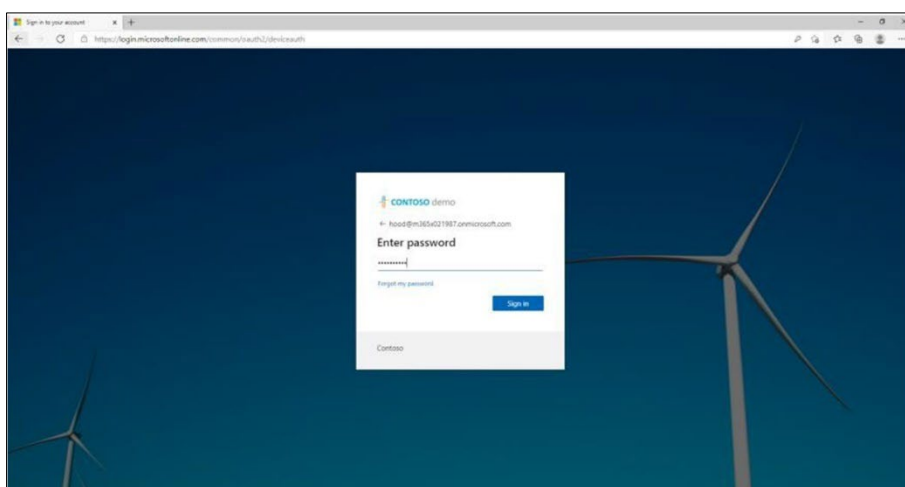
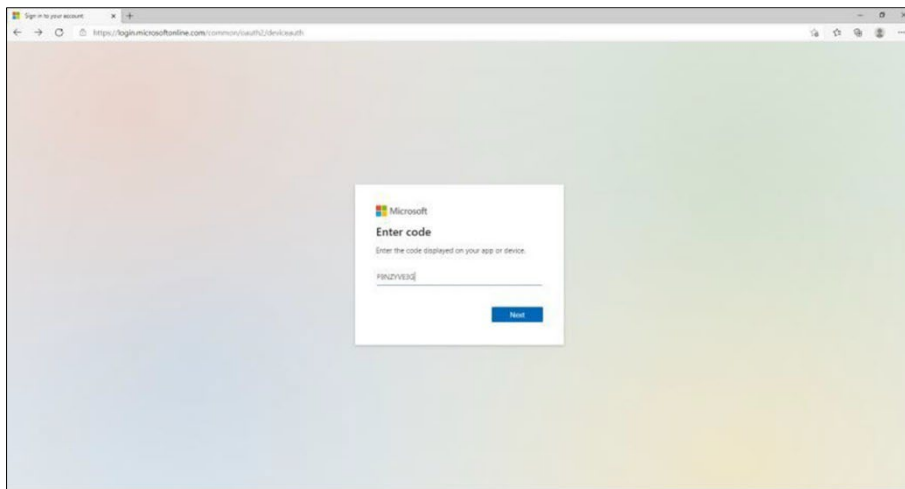
#### Step 4: Sign in remotely

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

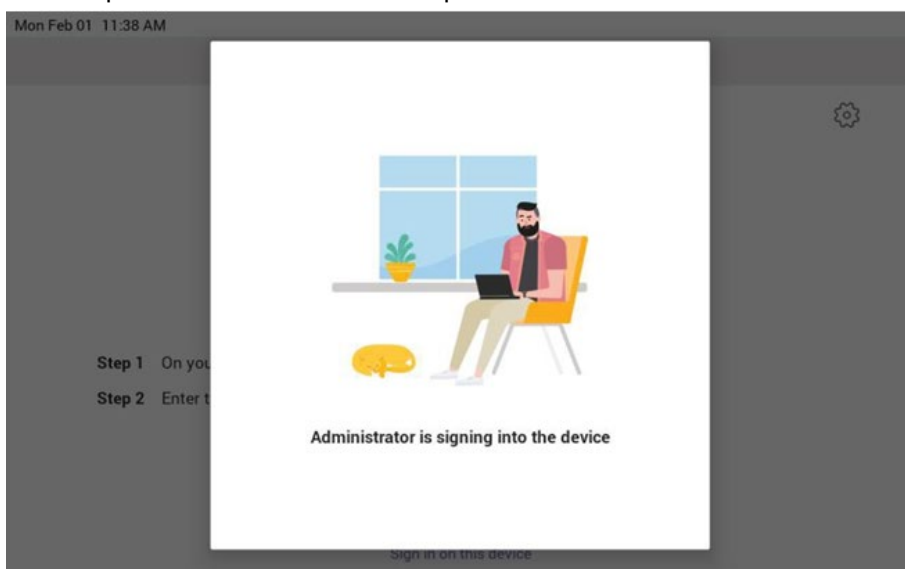
1. Select a device from the **Awaiting sign in** tab.
2. Follow the instructions in **Sign in a user**, and then select **Close**.



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.

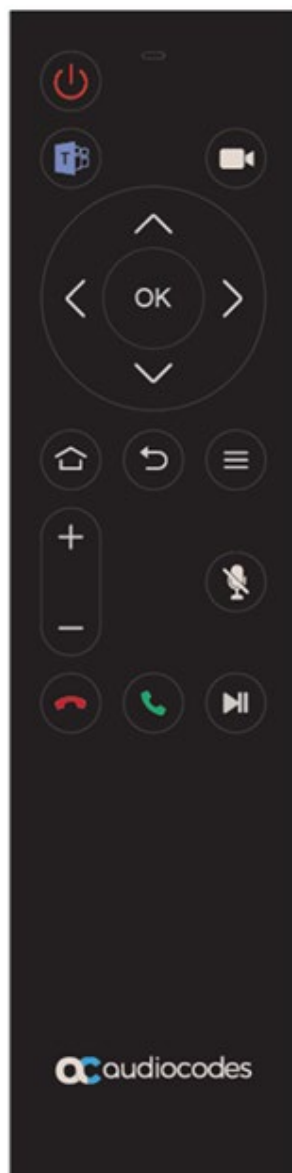


## 4 Getting Started



**Note:** See the *RXV81 Standalone Video Collaboration Bar Deployment Guide* shipped with the product or available from AudioCodes for information on how to synchronize the remote controller and the Teams application.

The figure below shows AudioCodes' remote controller.



- The software on the remote controller is managed by the RXV81.
- The remote controller leverages Bluetooth which enables full control and bi-directional communication (very much like touch control). See also Section 5.1.5.
- The keys on the remote controller (Mute, Teams) are illuminated.

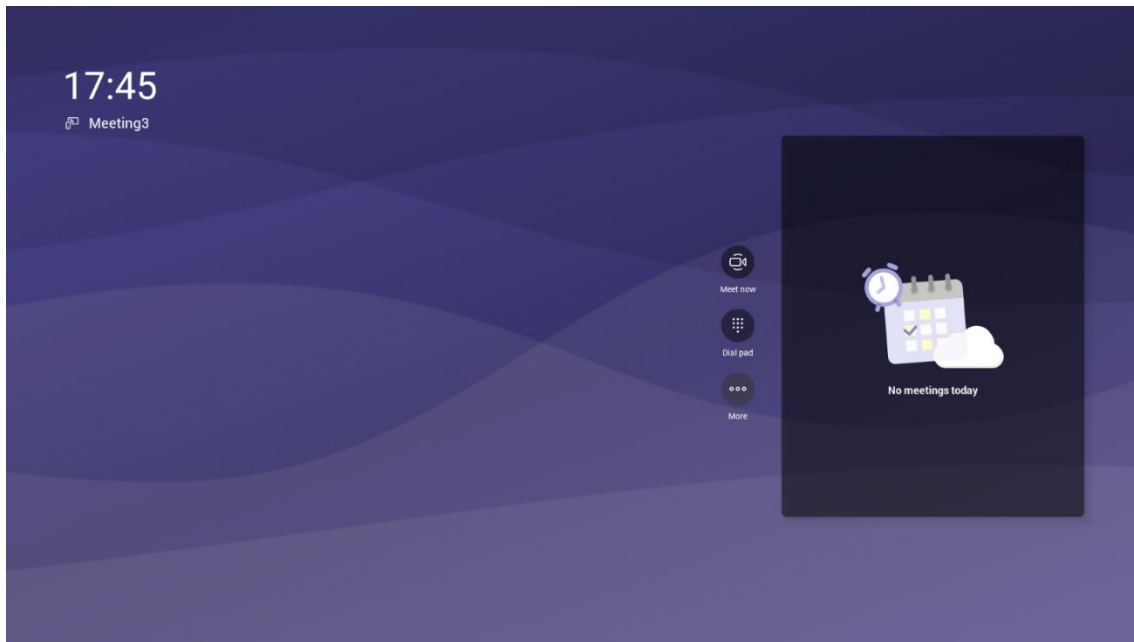


**Note:** The remote controller flashes if the connection to the RXV81 fails.

➤ **To get started:**

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


**Figure 4-1: Home Screen**



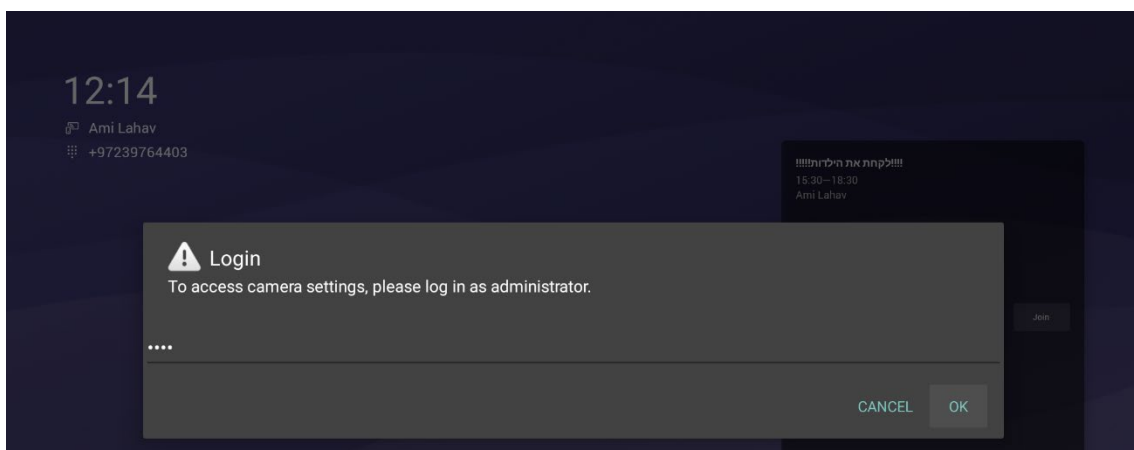
## 4.1 Modifying Camera Settings

You can modify the camera settings relating to the look and feel of the video user interface, to suit your preferences.

➤ **To access the camera settings:**

- On the remote controller, long-press the camera icon .
  - After long-pressing the remote controller's camera button, a prompt to log in as the administrator is displayed before it proceeds to the **Camera settings** tab:

**Figure 4-2: Login when the RXV81 is in *idle state***



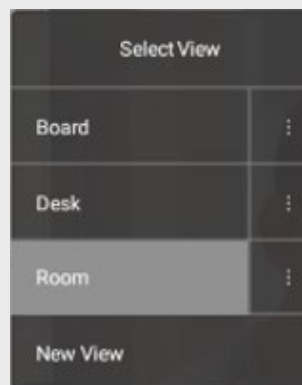
**Note:**

- During a call, *all users* who are signed into the RXV81 – Admins *and* personal users - can change **Camera settings**, including the presets. All have the permissions required to do so. When the call ends, the 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 the 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.



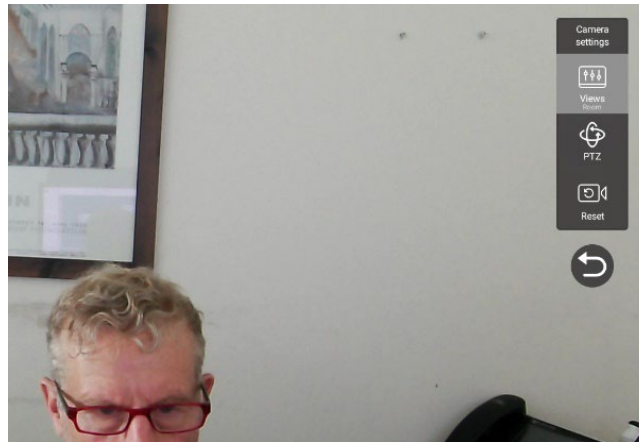
- For example, if a preset is configured to zoom in and focus on the whiteboard in a room, users in a video call/meeting can switch to it and later switch back to the full room preset or any other predefined preset. It's recommended to have a few presets configured for locations frequently zoomed in 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.

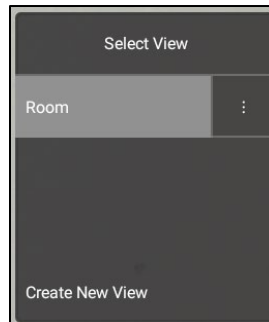
➤ **To add a camera preset when in idle mode:**

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

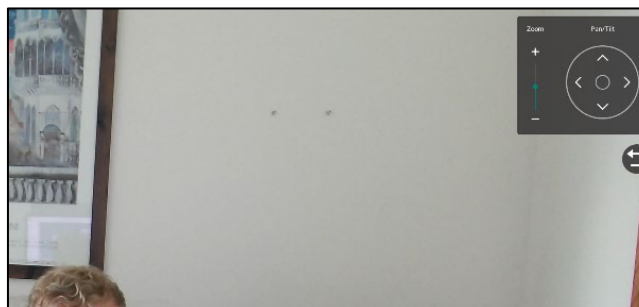
**Figure 4-3: Camera settings**



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.

## 4.2 Starting a New Meeting



**Note:** You can navigate and select in the RXV81 using the:

- Remote controller -OR-
- Touch screen

➤ **To start a new meeting:**

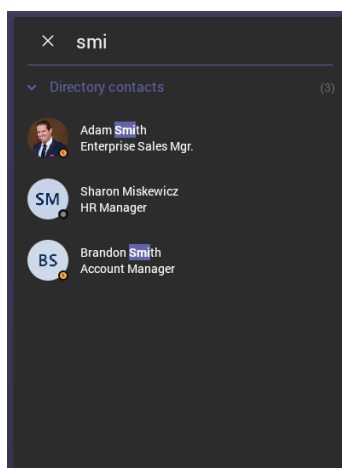
1. In the home screen shown in the preceding figure, navigate to and select the **Meet Now** option.

**Figure 4-4: New meeting – Invite someone**



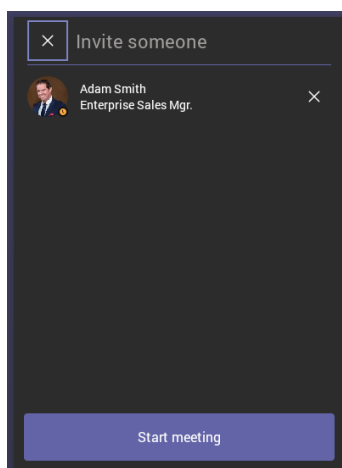
2. In the 'Invite someone' field, enter the name of a person to invite; after entering the first letters in the name, matching contacts from directory are displayed.

**Figure 4-5: New meeting – Enter the name of a person**



3. Select the name of the person to invite.

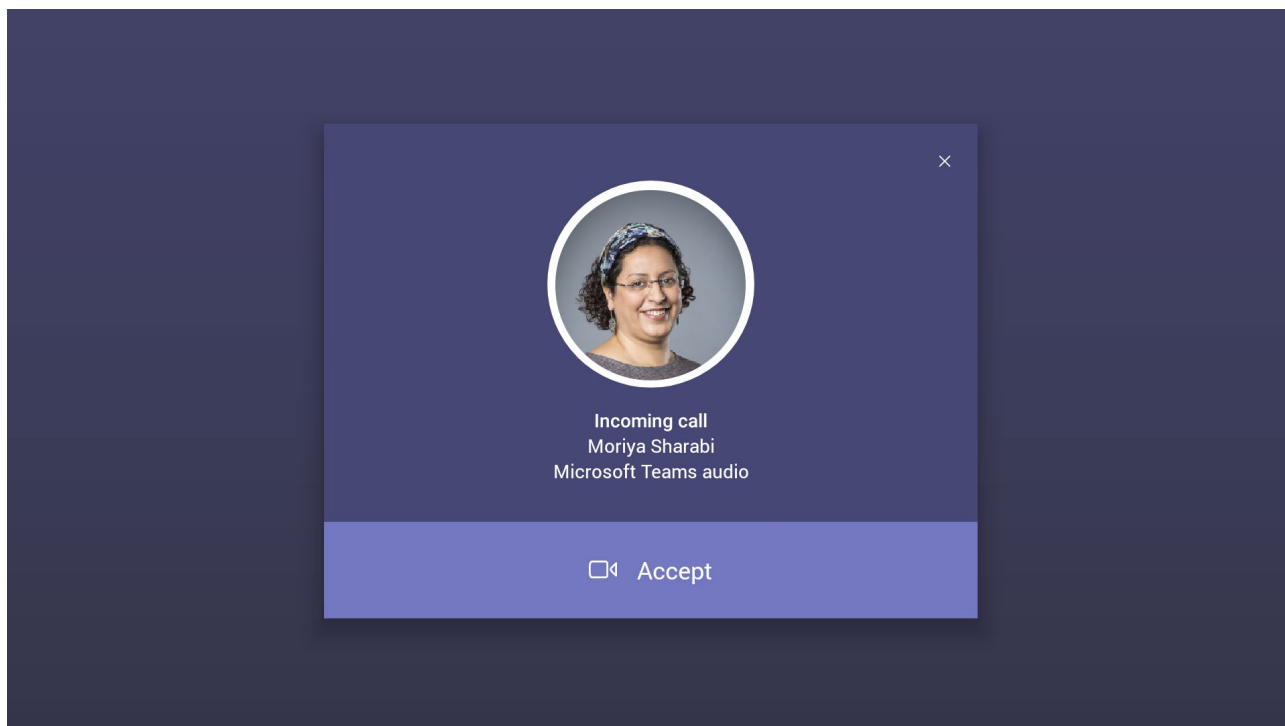
Figure 4-6: New meeting – Select the name of a person



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

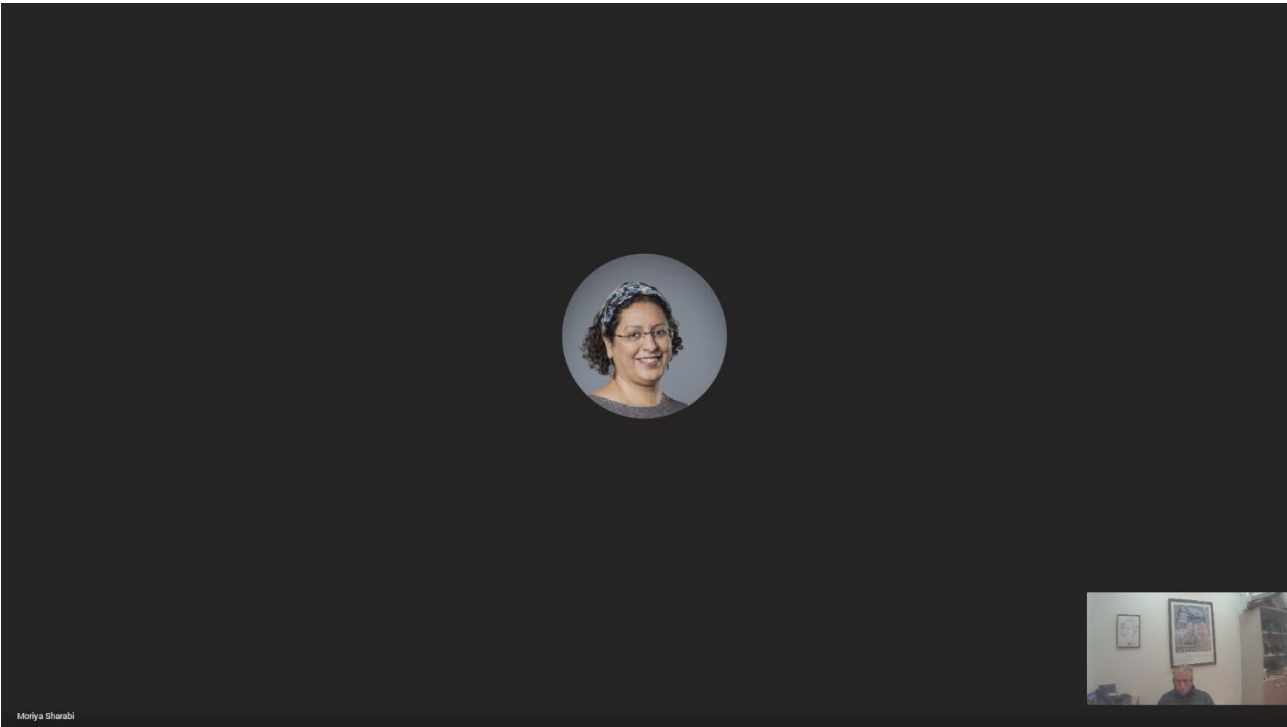
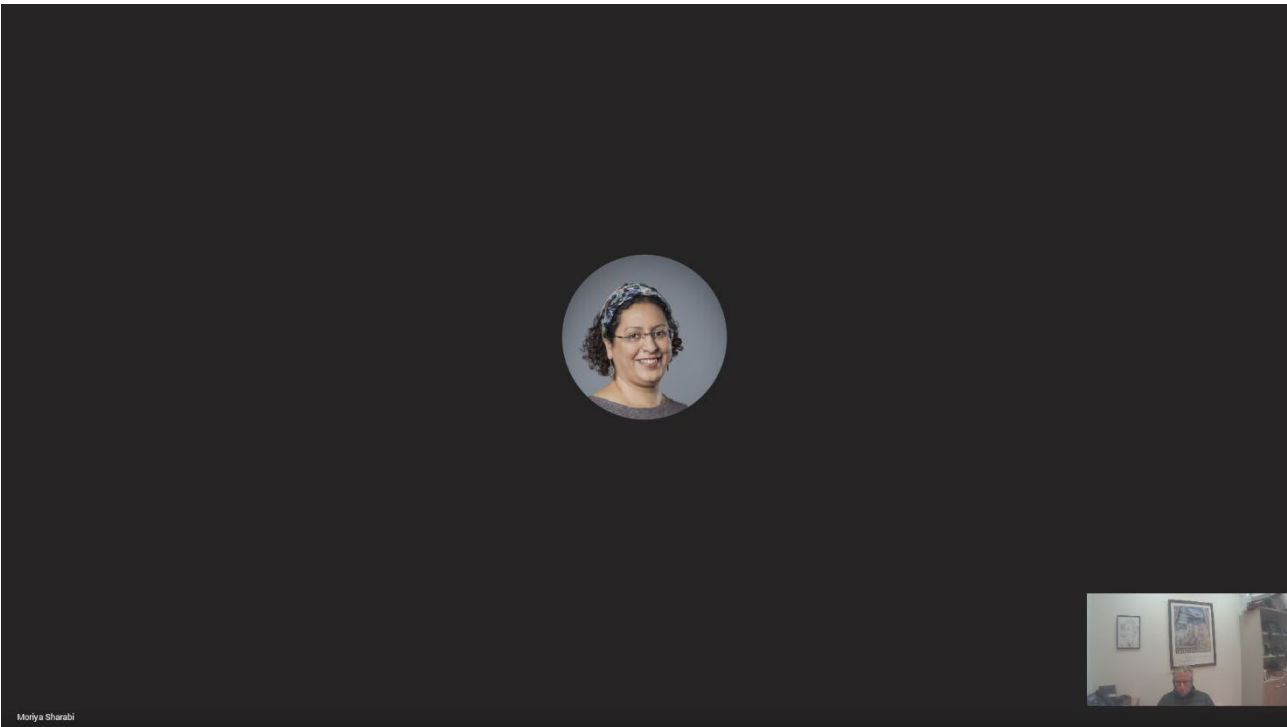


**Note:** The server allocates a meeting ID number and sends an invite message to all participant devices. All devices simultaneously indicate an incoming call (the 'Calling' screen is displayed). The server manages every aspect of the call.



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





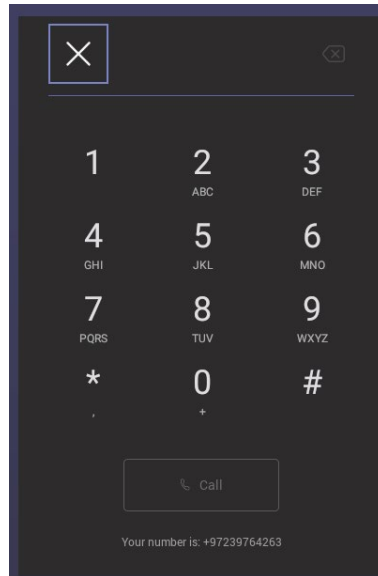
## 4.3 Dialing a Number

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 4-7: Dial pad**

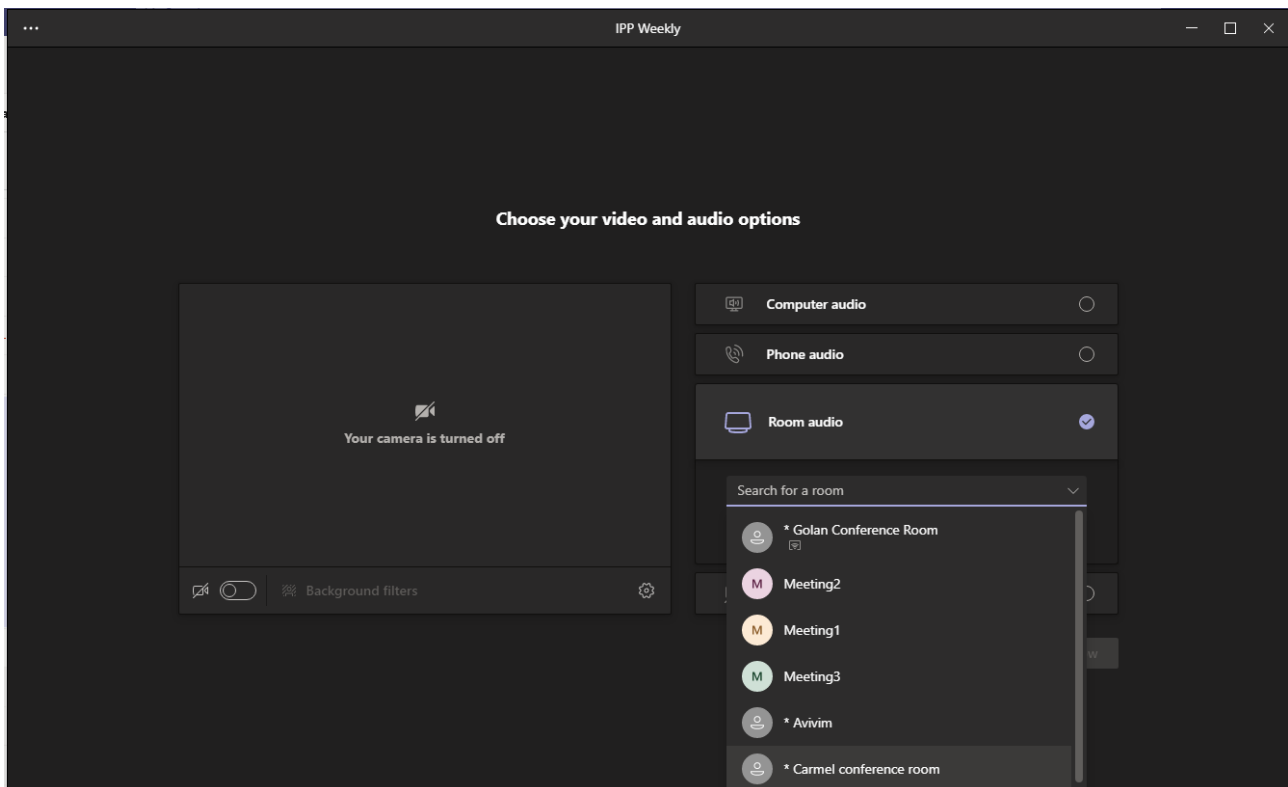


2. Enter the digits of the destination to call and select **Call**.

## 4.4 Enabling Proximity Join

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

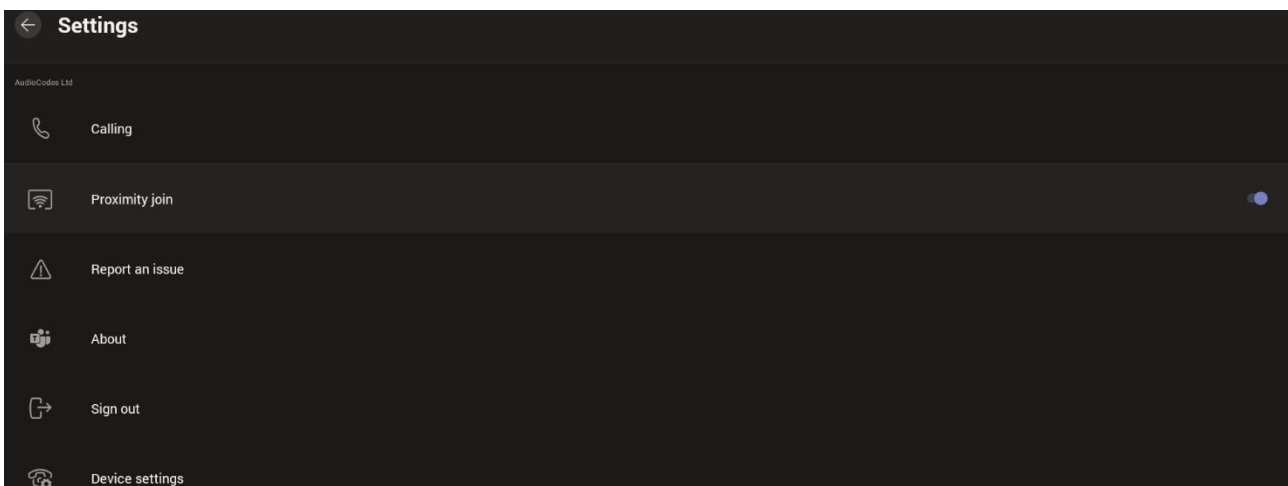
The feature functions in combination with Bluetooth and 'Bluetooth Beacons', an integral feature in Microsoft Teams Rooms (MTRs). The MTR device is RXV81. If you bring a laptop or a Teams Mobile Client near the RXV81, it'll offer the RXV81 as the room audio device. The figure below shows how to select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

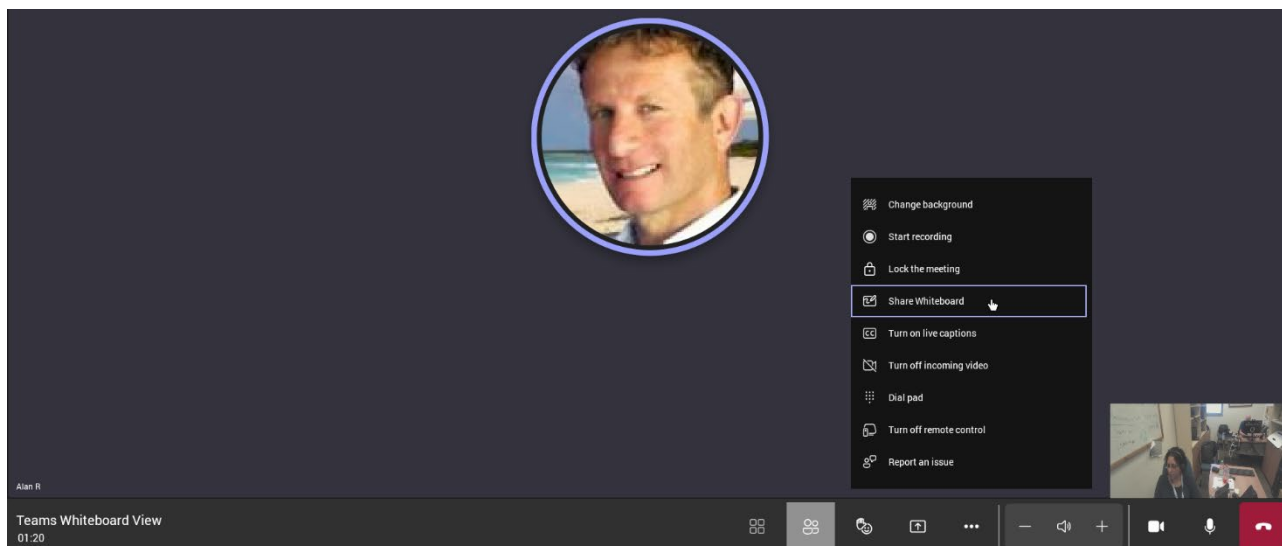


## 4.5 Sharing a Whiteboard

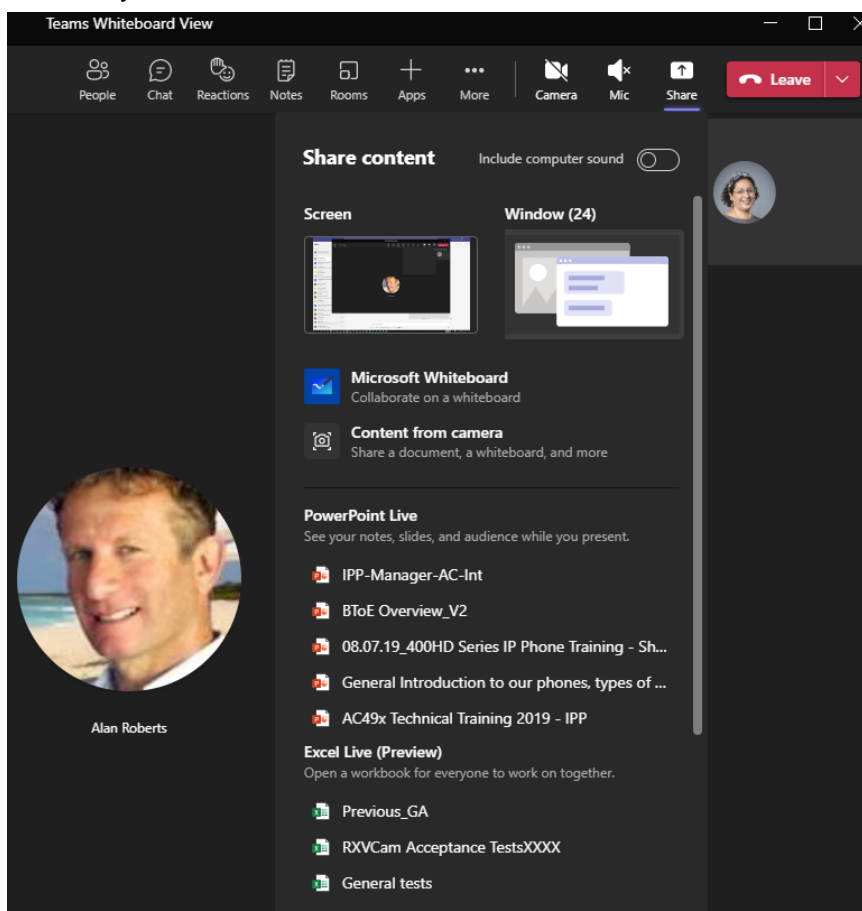
Teams meetings on the RXV81 allow participants to open a virtual whiteboard – a digital canvas - on which they can sketch, illustrate, collaborate, brainstorm, plan, and share perspectives with one another in real time. The focus switches away from the presenting participant to the whiteboard. For more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

➤ **To share the Whiteboard:**

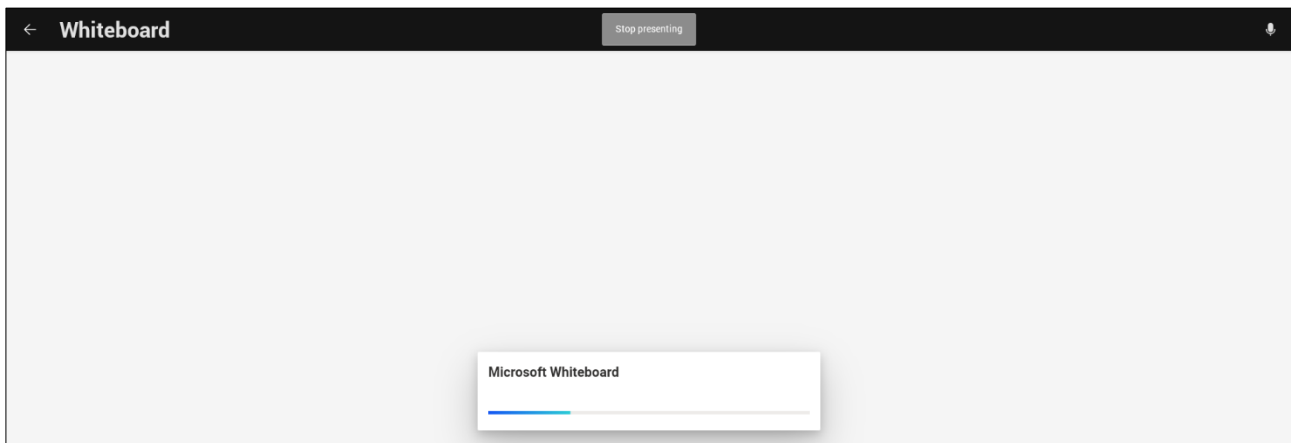
1. From the Settings menu, select **Share Whiteboard**.



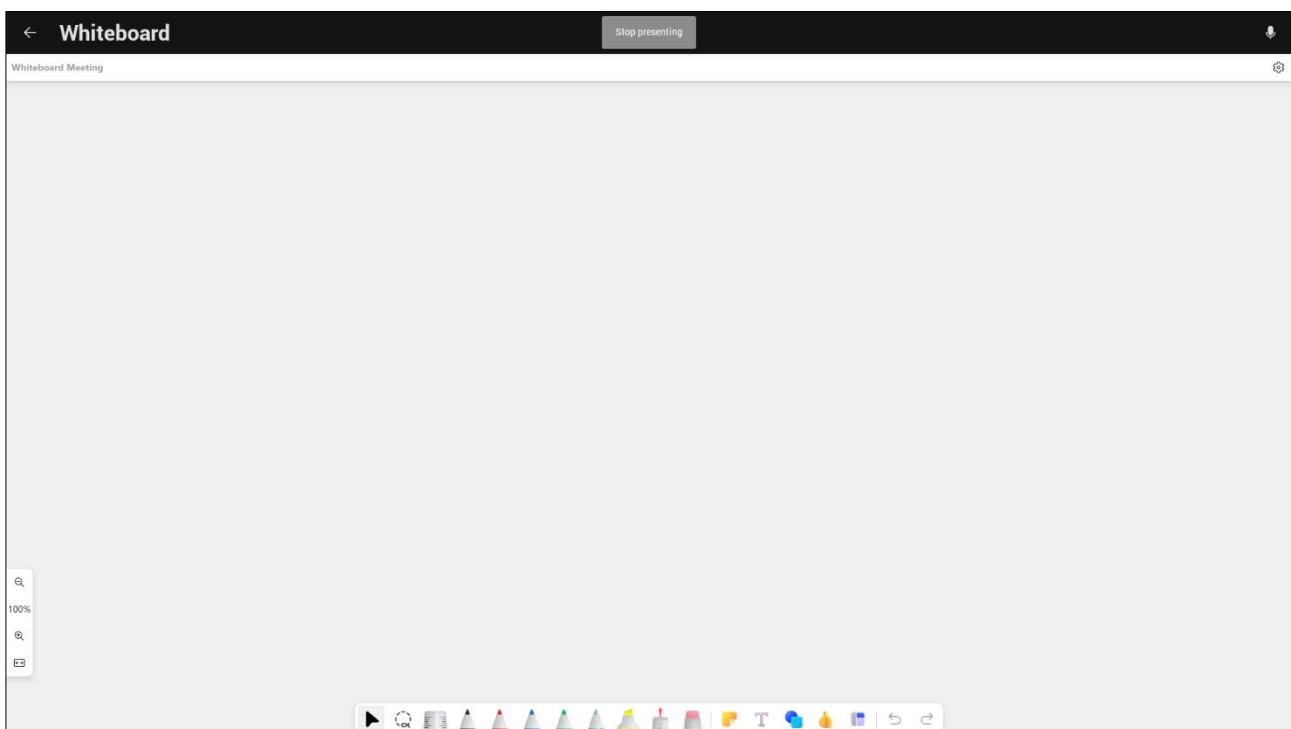
2. Alternatively, access the Whiteboard from **Share content**:



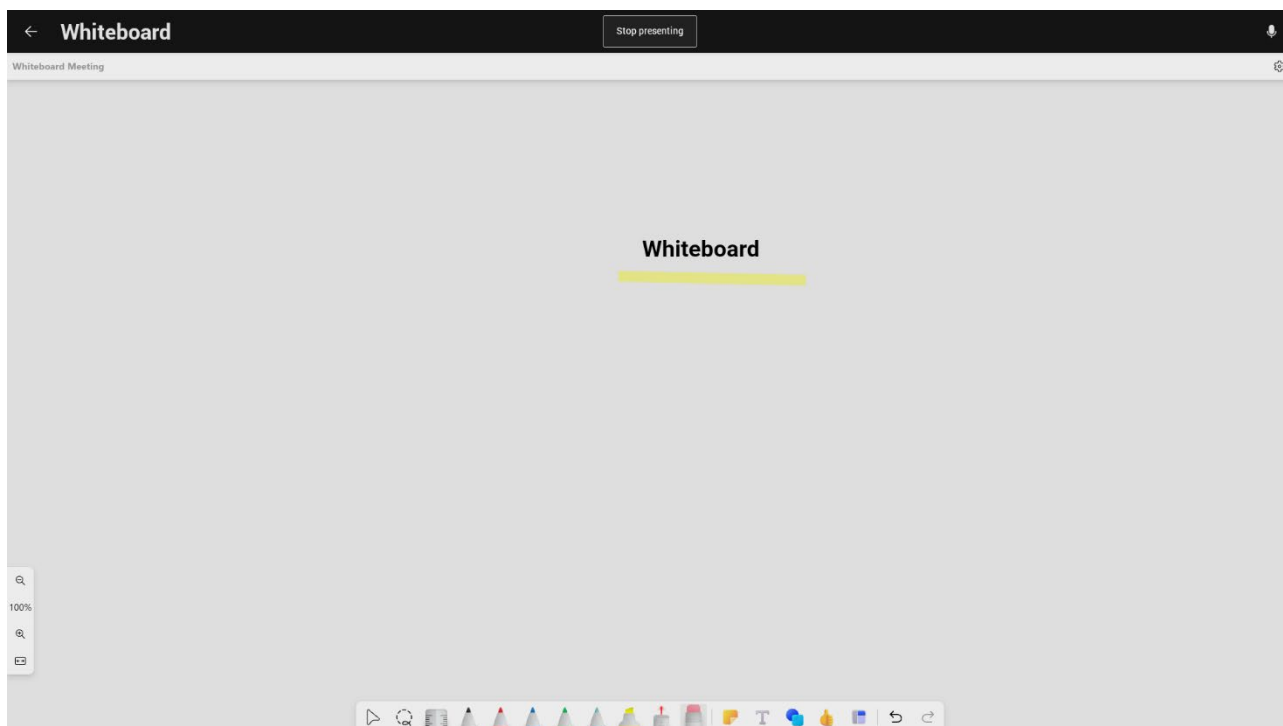
3. View the following Microsoft Whiteboard initializing indication:



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

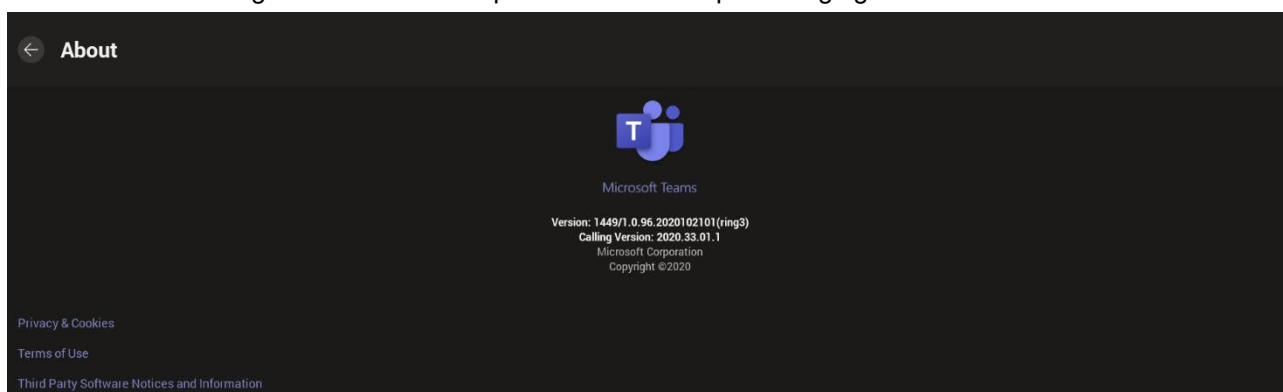


5. Edit the Whiteboard; every participant with privileges can edit it.



## 4.6 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.



## 4.7 Signing out

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

➤ **To sign out:**

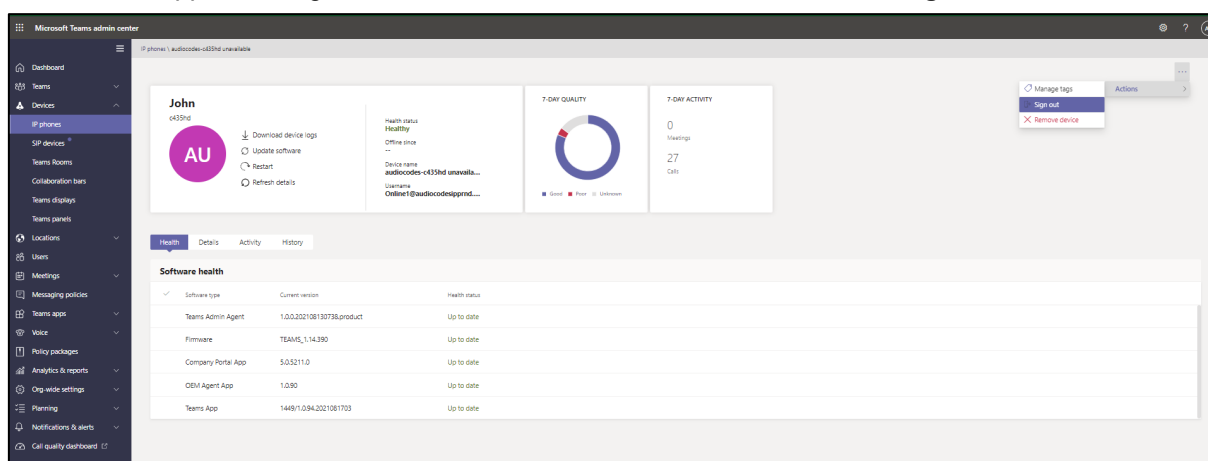
- Navigate to and select **Sign out** in the Settings screen shown in the preceding figure.



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

➤ **To sign out of the 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.



## 5 Configuring Device Settings

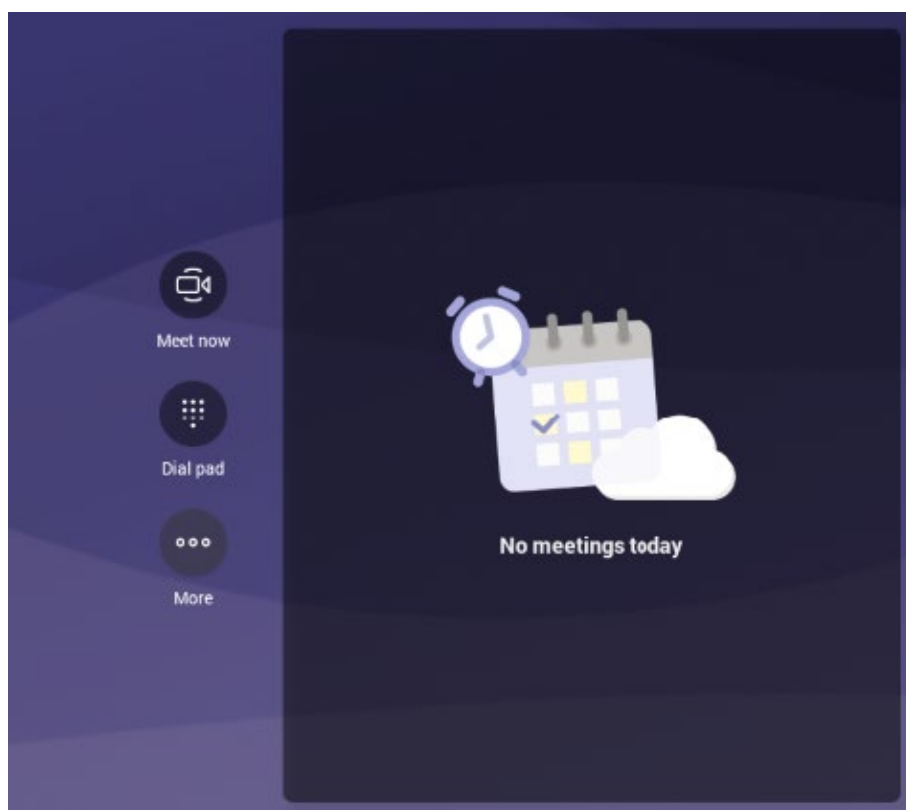
The section familiarizes you with the RXV81's settings. RXV81s are delivered configured with their default settings. Customers can customize them to suit enterprise requirements.



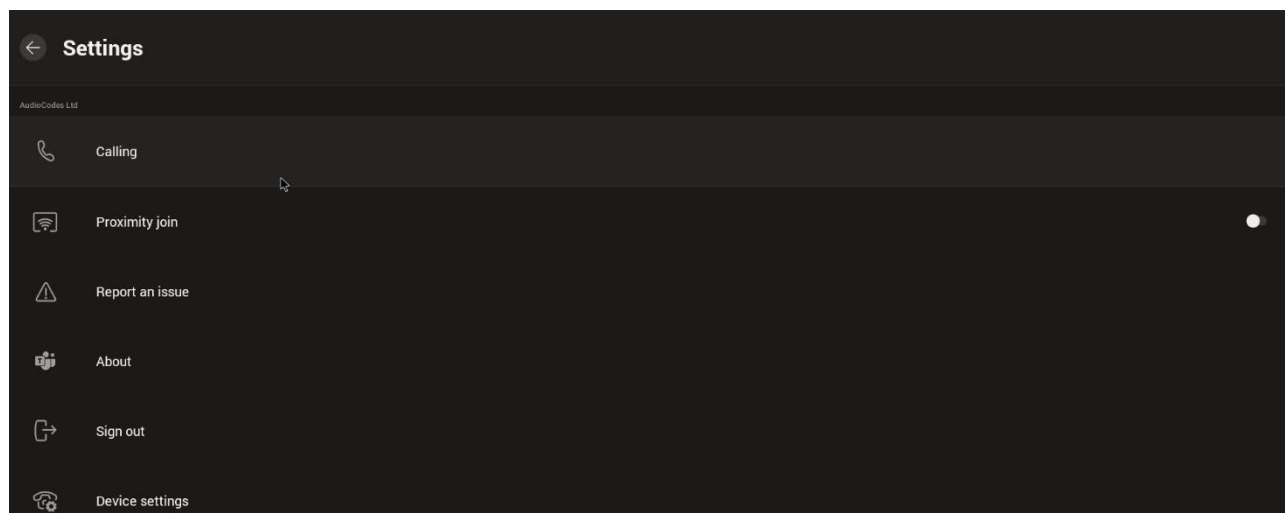
**Note:** Navigate and select options using the remote controller or touch screen.

➤ To access device settings:

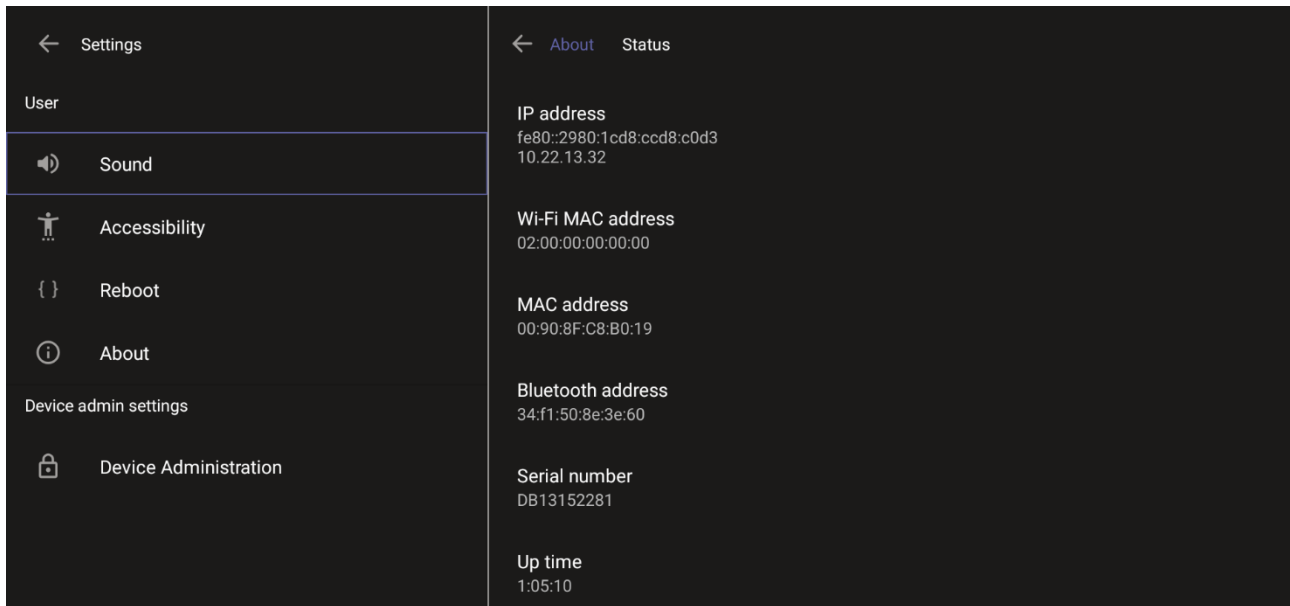
1. In the home screen, navigate to and select the **More** option



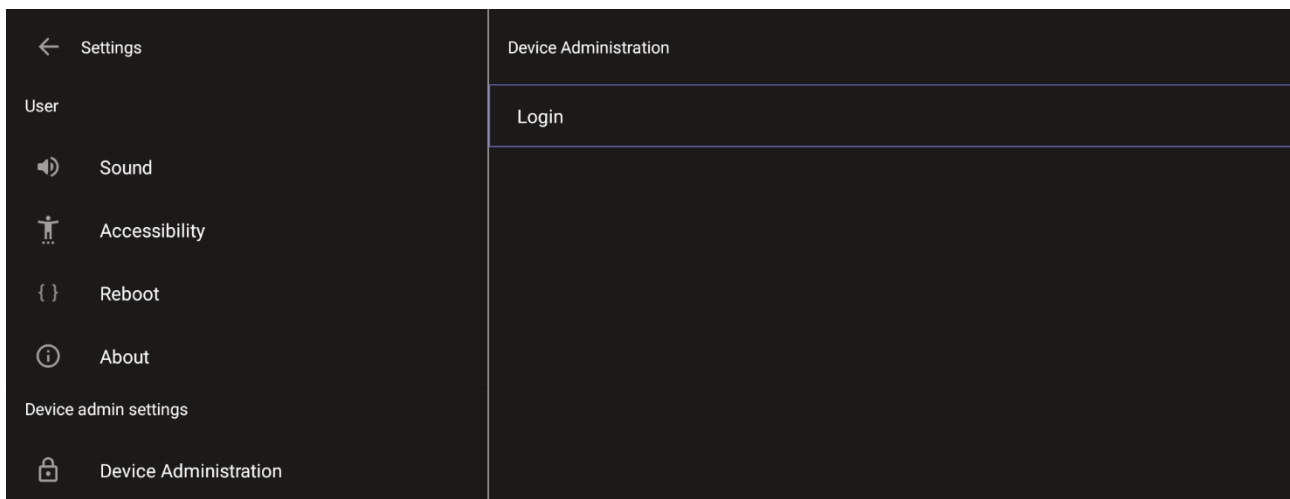
2. Navigate to and select **Settings**.



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



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

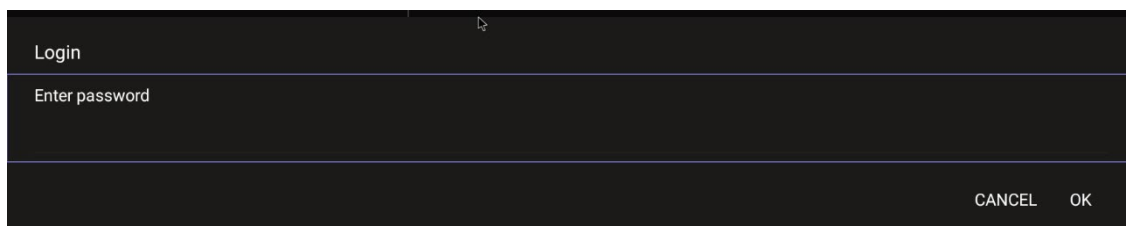


5. Log in as administrator.



**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.

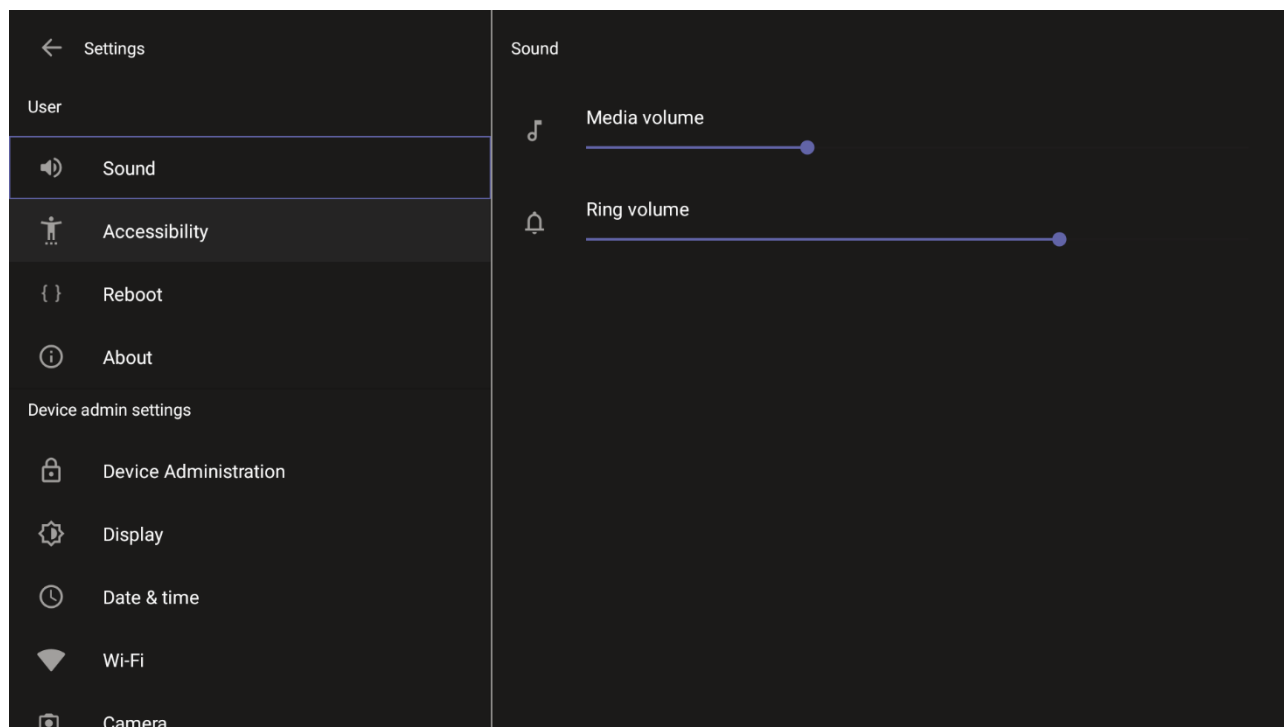
9. Enter a password; you're prompted to verify the password you entered. Criteria required for a strong password are provided (for strengthened security) in order to Log in as Administrator:
  - The password length must be greater than or equal to 8.
  - The password must contain one or more uppercase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



## 5.1 Configuring Device Admin Settings

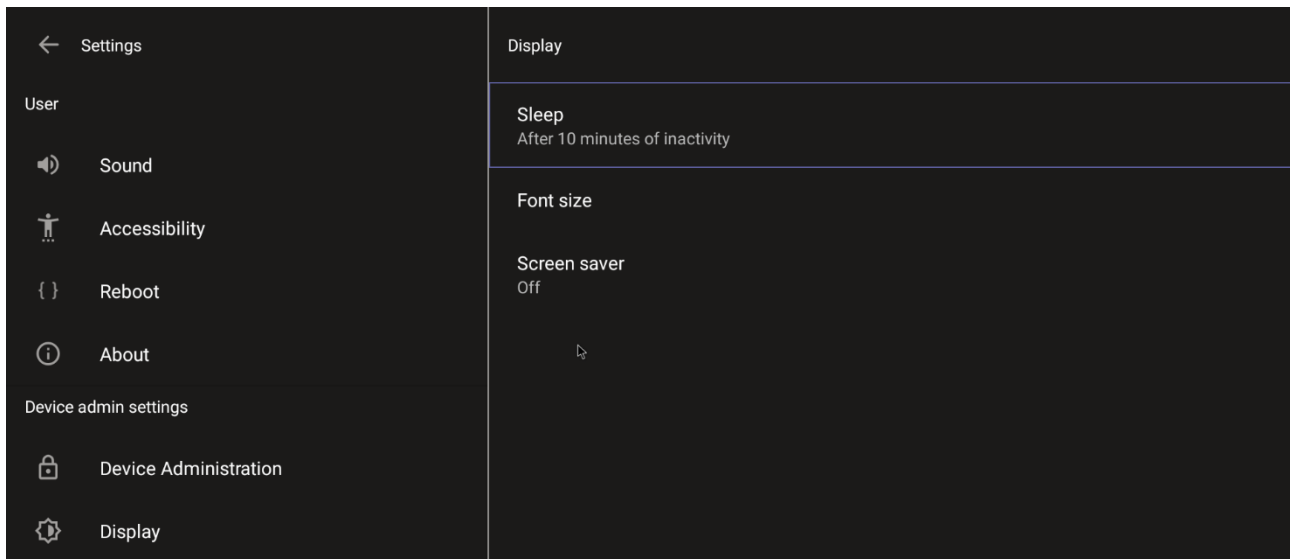
After logging in as Device Administration as shown in the previous section, you can configure Device Administration settings: Display, Date & Time, Wi-Fi, Camera.

### 5.1.1 Display Settings

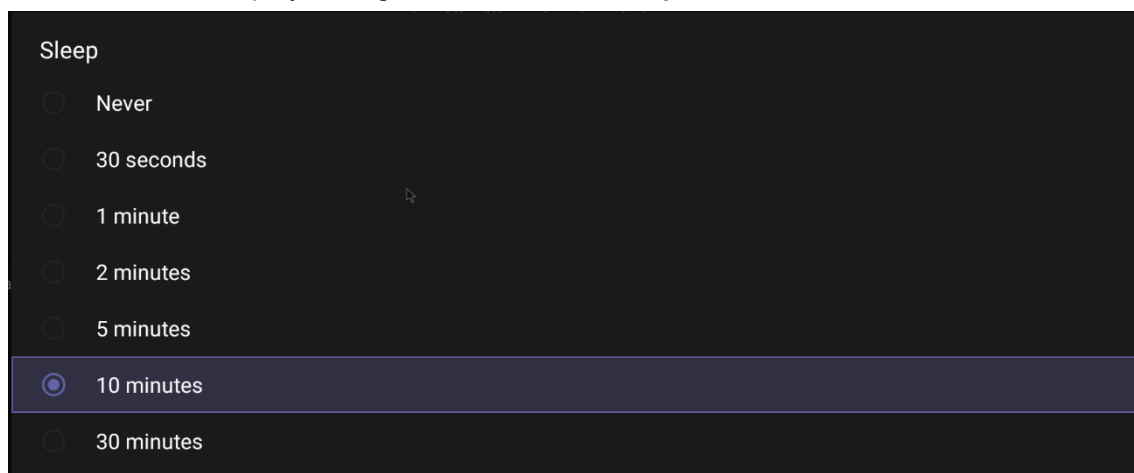
Modify these settings to suit your preferences related to the look and feel of the user interface.

➤ **To configure Display settings:**

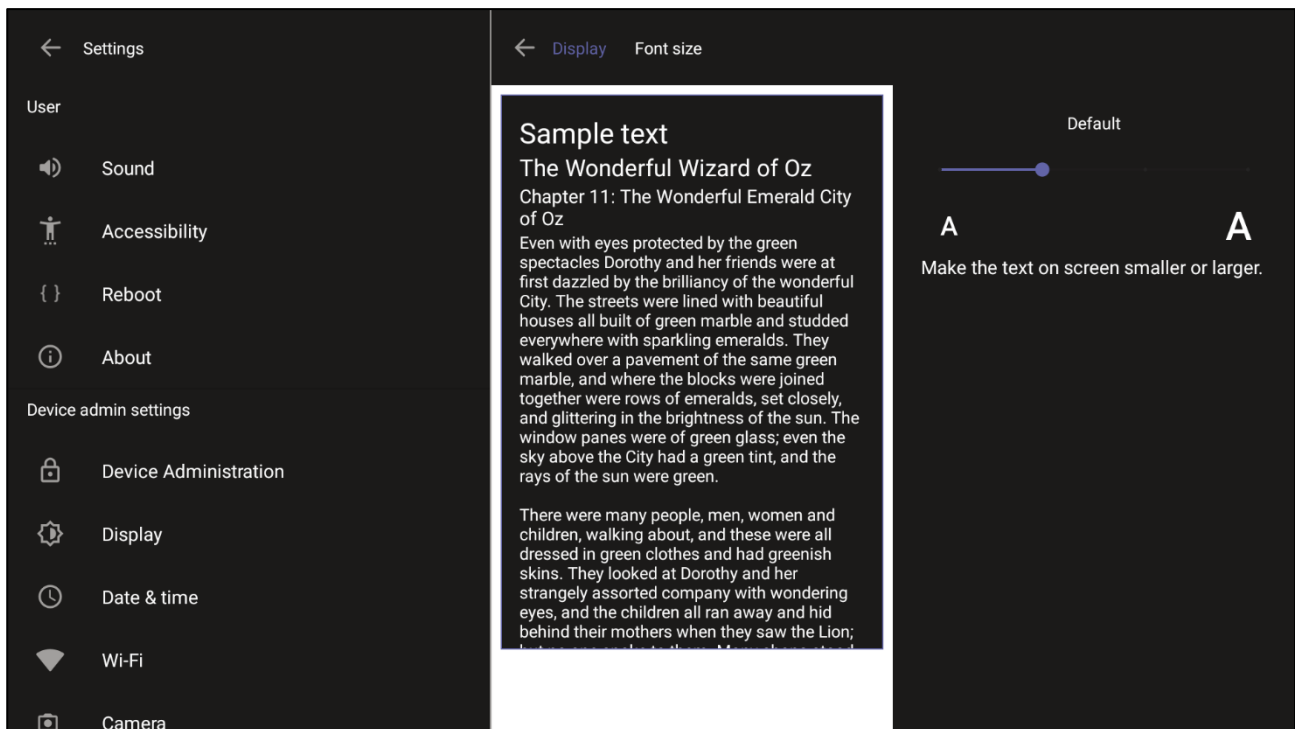
1. Under 'Device admin settings', navigate to and select **Display**.



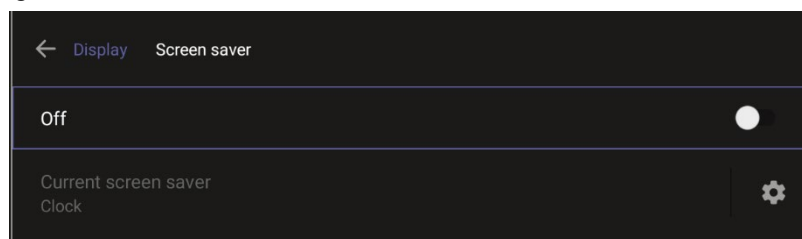
2. Under 'Display', navigate to and select **Sleep**.



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**.



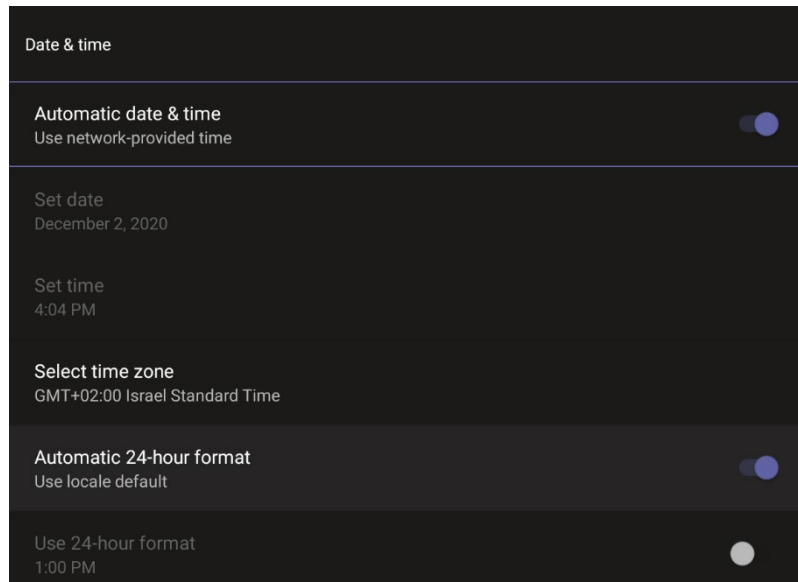
6. Navigate to and select **Off** to switch it on and then choose the screen saver.

## 5.1.2 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**).

### 5.1.3 Wi-Fi Settings

The RXV81 can connect to an Access Point via Wi-Fi.



**Note:** See the *Deployment Guide* for detailed information on how to set up Wi-Fi.

Network administrators can configure Wi-Fi parameters for the 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.

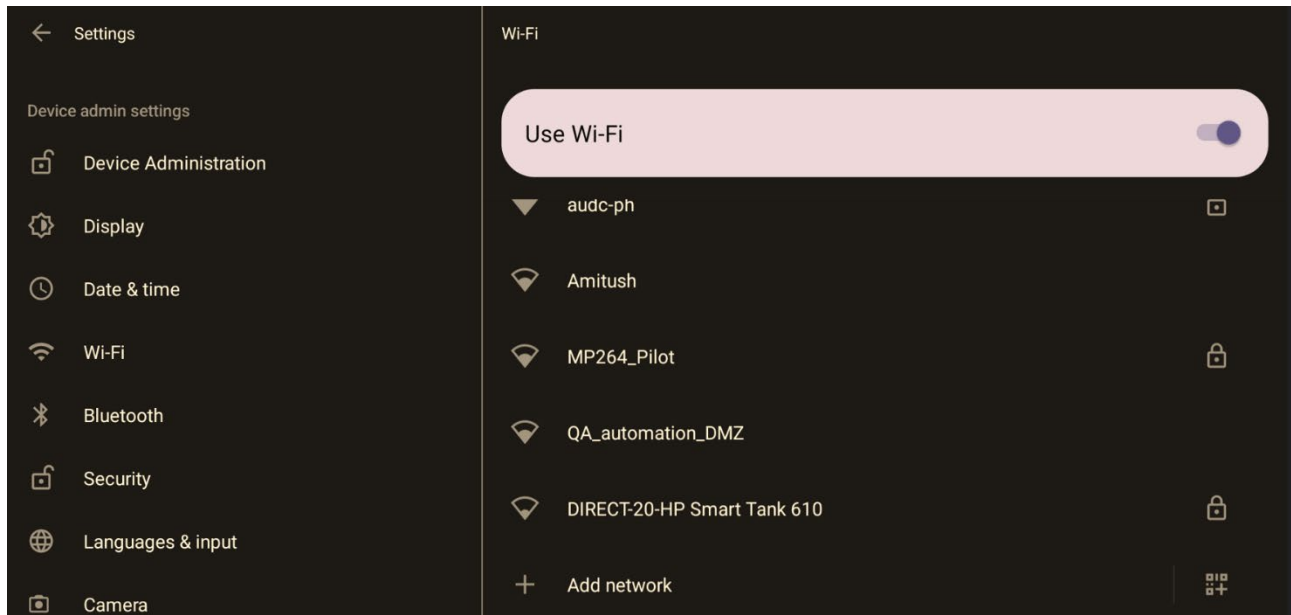
#### 5.1.3.1 Connecting to an Available Wi-Fi Network

➤ 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'.

### 5.1.3.2 Manually Connecting to a Wi-Fi Network

- To manually connect to a Wi-Fi network:



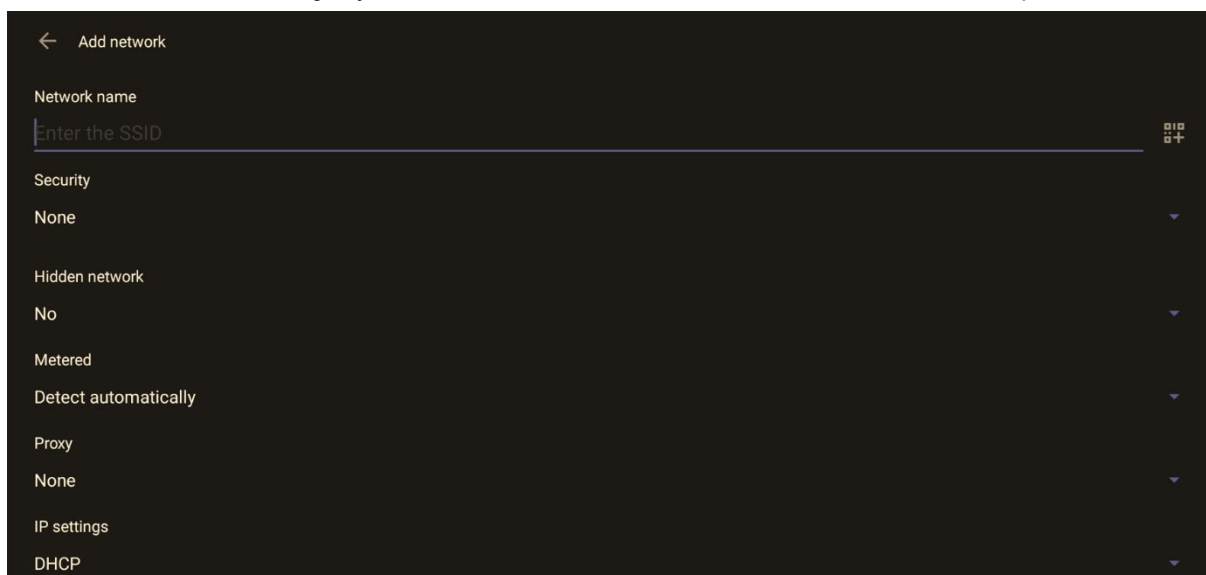
**Note:** Make sure to first disconnect your Ethernet cable. If it's connected, the device will not be able to connect to a Wi-Fi network.

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 5-1](#), using the Configuration File.

**Table 5-1: Configuration File Wi-Fi Parameters**

Parameter	Description
network/wireless/advanced_options/dns1	Defines the IP of the wireless DNS1.
network/wireless/advanced_options/dns2	Defines the IP of the wireless DNS2.
network/wireless/advanced_options/gateway	Defines the IP address of the wireless gateway
network/wireless/advanced_options/hidden_network	Defines the name of the wireless hidden network.
network/wireless/advanced_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/advanced_options/ip_settings	Used to define DHCP.
network/wireless/advanced_options/network_prefix_length	Defines the network prefix length to be used.
network/wireless/advanced_options/proxy	Defines the proxy wireless server source.
network/wireless/advanced_options/proxy/auto_config/pac_url	Defines the URL of the PAC file.
network/wireless/advanced_options/proxy/manual/exclusion_list	Defines the list of IP addresses that will be blocked.
network/wireless/advanced_options/proxy/manual/host	Defines the name of the proxy host.

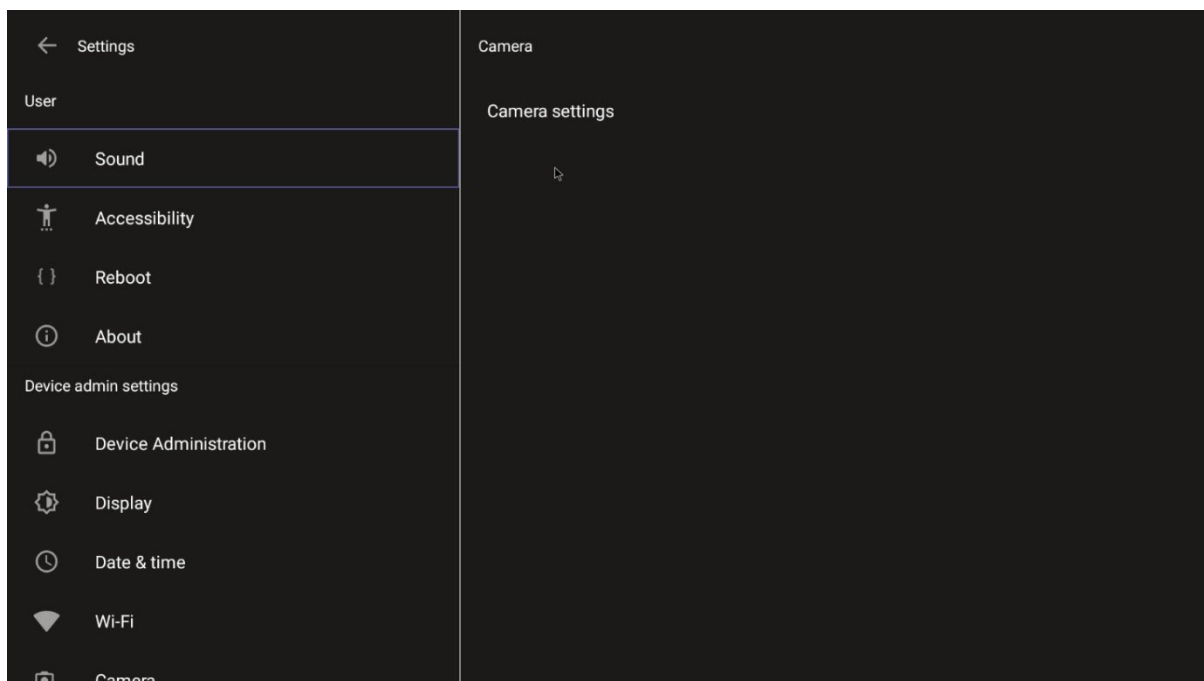
Parameter	Description
options/proxy/manual/proxy_hostname	
network/wireless/advanced_options/proxy/manual/proxy_port	Defines the proxy port.
network/wireless/anon_identity	Defines the anonymous wireless users who won't be seen.
network/wireless/ca_cert	Defines which CA certificate to use.
network/wireless/client_cert	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).

### 5.1.4 Camera

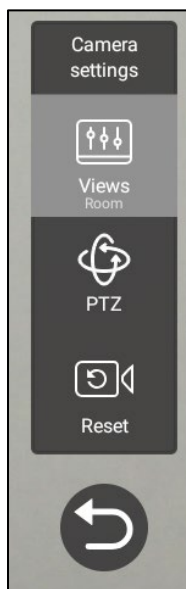
Settings controlling the look and feel of the video UI can be set to suit individual preferences.

➤ **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:

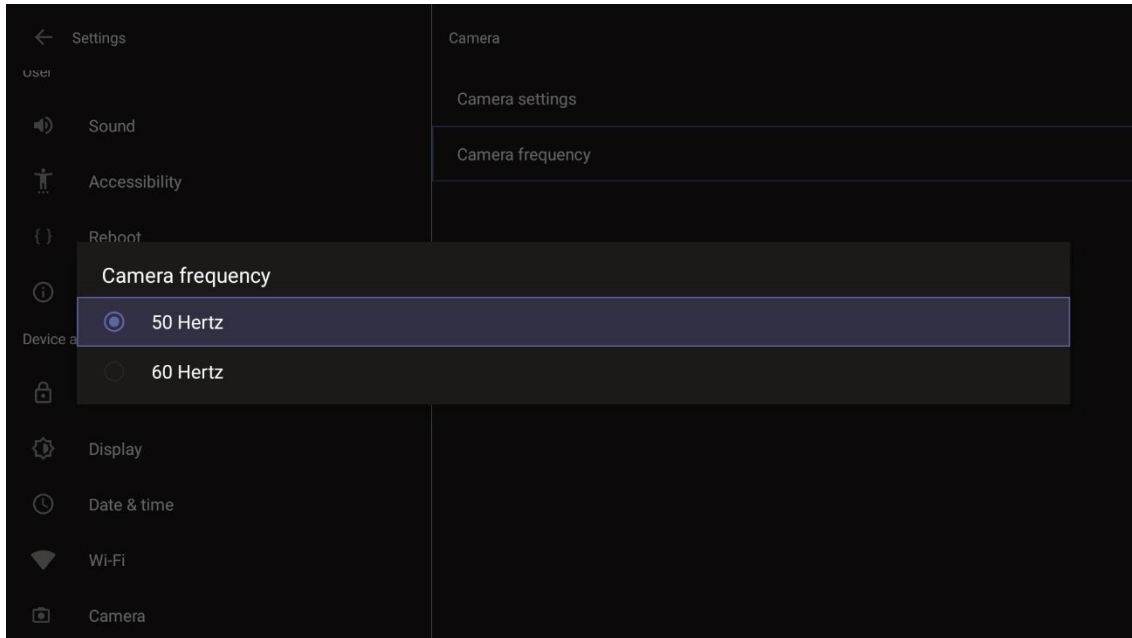


3. Create and edit presets using PTZ control. For more information, see [here](#).

### 5.1.4.1 Configuring Camera Frequency

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

- 110V – 60Hz
- 220V – 50Hz



### 5.1.5 Bluetooth

Bluetooth is currently used for the remote controller and the 'Proximity Join' feature.

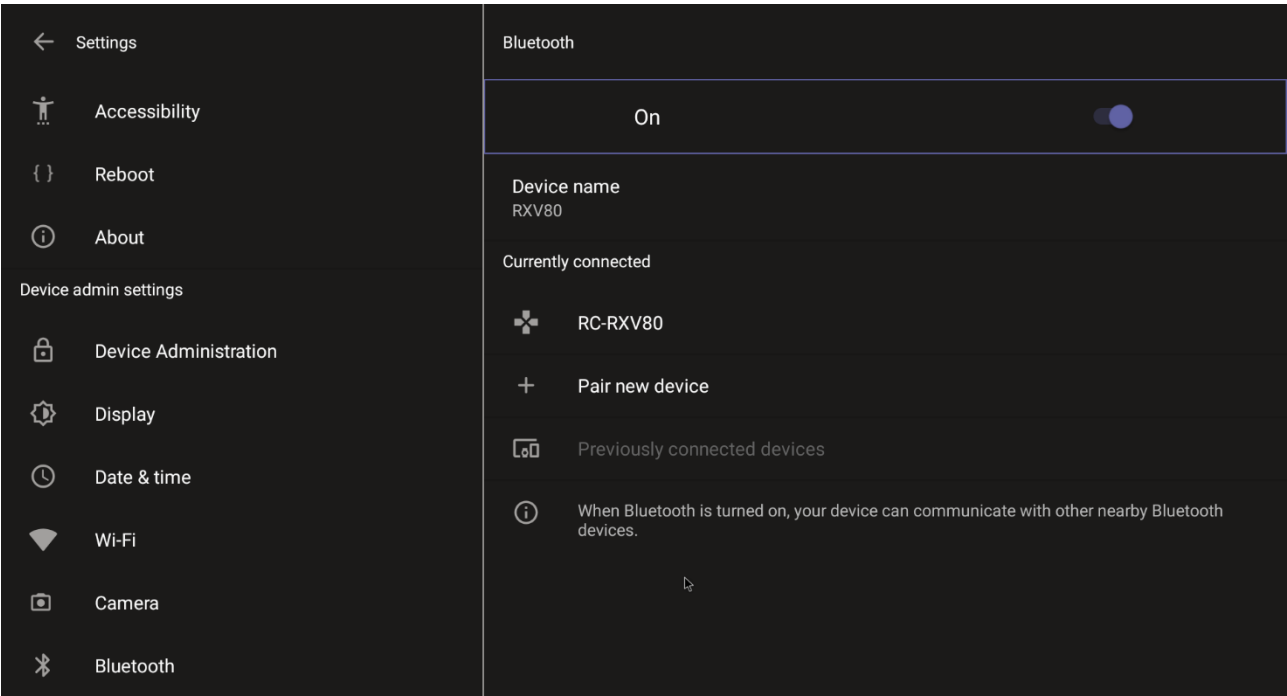


**Note:** The built-in Bluetooth capability can support only one Bluetooth feature at the time (the remote controller or the 'Proximity join' feature). To use both the remote controller and 'Proximity Join' in parallel, the Bluetooth dongle provided with RXV81 bundles must be used. The dongle fully supports the remote controller and **the** 'Proximity Join' feature. Note that if your package does not include a dongle, you can contact AudioCodes to obtain one. After it's inserted, the RXV81 must be restarted.

Bluetooth must be enabled to support use of the remote controller and the 'Proximity Join' feature. For information on how to enable/disable Bluetooth and on how to locate the remote controller manually (without using the popup automatically displayed at the start to pair the remote controller), see the *RXV81 Deployment Guide*.

➤ **To pair a new device:**

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



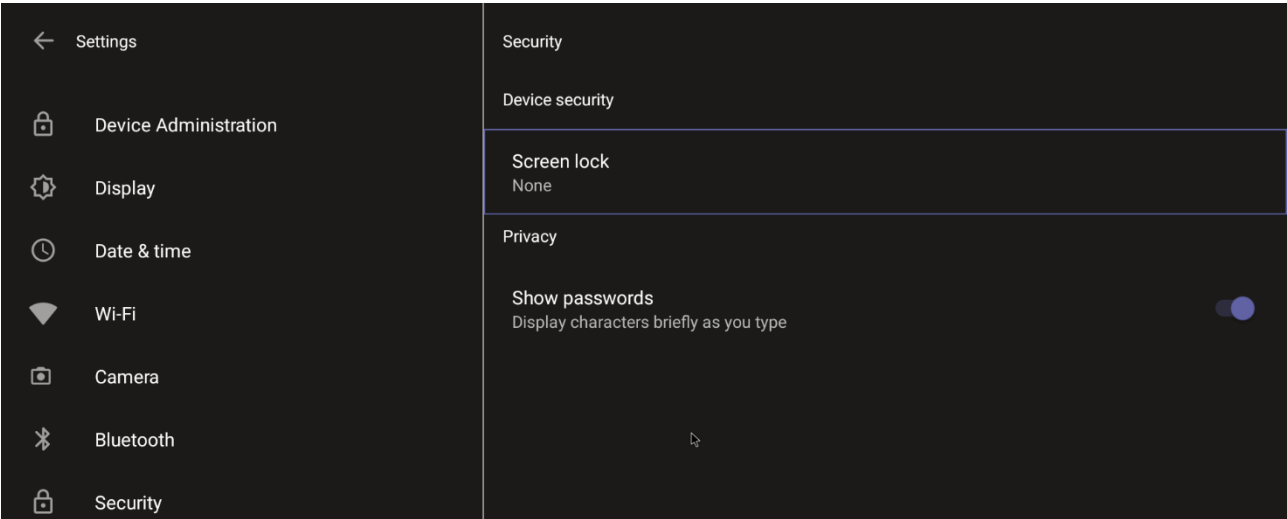
- 2. Navigate to and select **Pair new device**.

5.1.6 Security

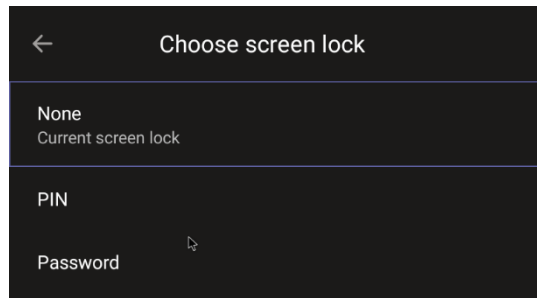
As a security precaution, the RXV81 can be locked and unlocked. The setting helps secure the device against breaches.

➤ To secure the device:

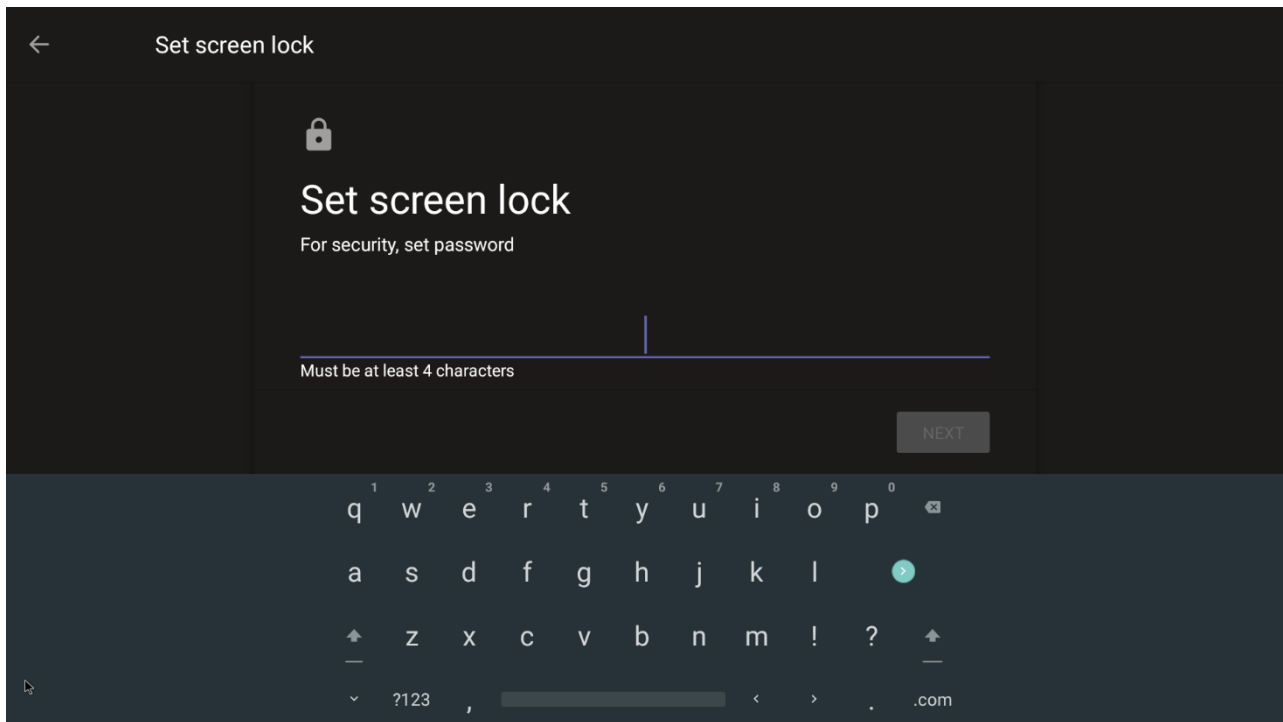
- 1. Under 'Device admin settings', navigate to and select **Security**.



- 2. Navigate to and select **Screen lock** [The phone automatically locks after a configured period to secure it against unwanted use. If left untouched for 10 minutes (default), it automatically locks and is inaccessible to anyone who doesn't know its lock code.]



3. Navigate to and select **PIN**.



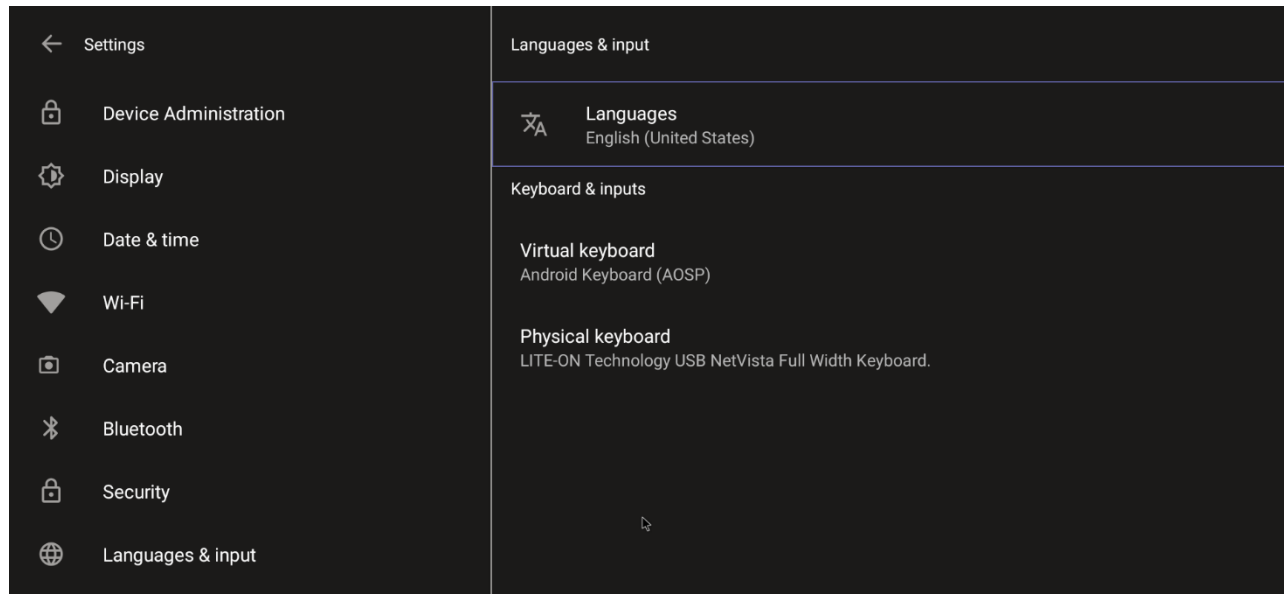
4. Enter a PIN, click **Next** and then navigate to and select **Password**; a screen like the preceding is displayed. Set the password (must also be at least four characters) and then again navigate to and select **Next**. You've successfully configured screen lock.

## 5.1.7 Languages & input

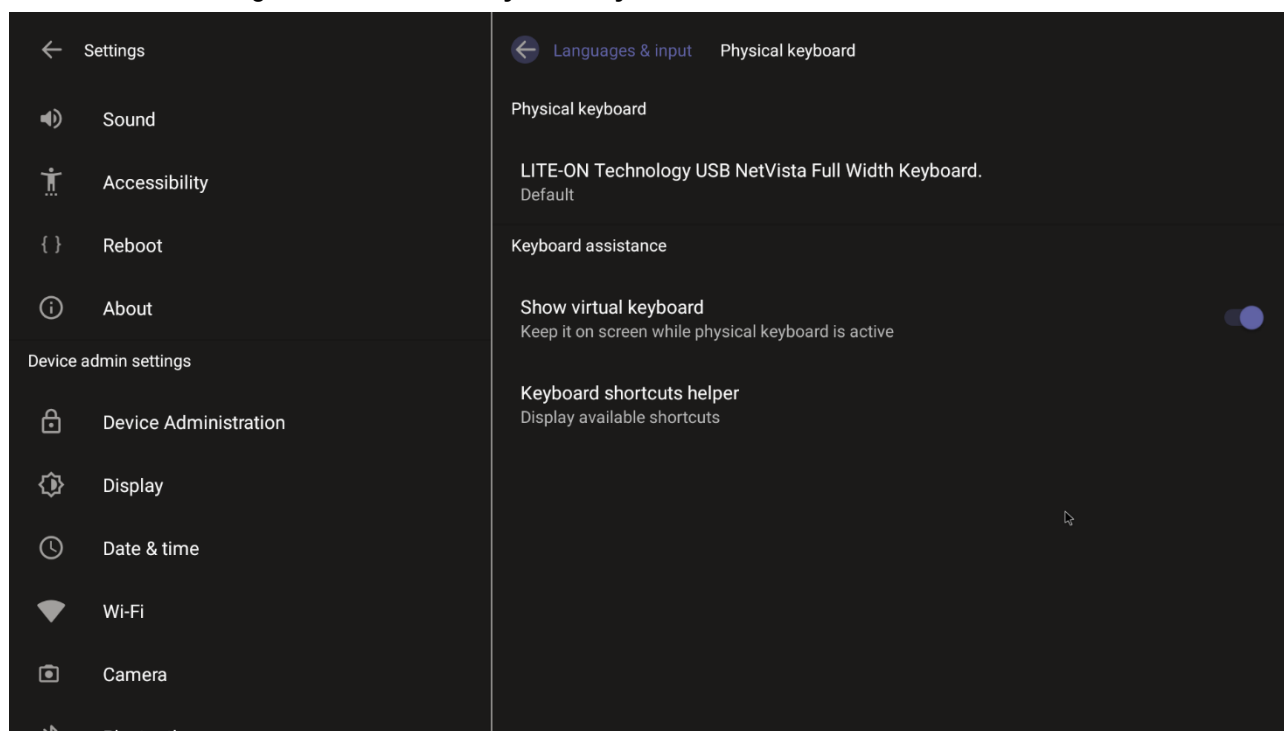
This setting allows users to customize inputting to suit personal requirements.

➤ **To set language and input:**

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



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



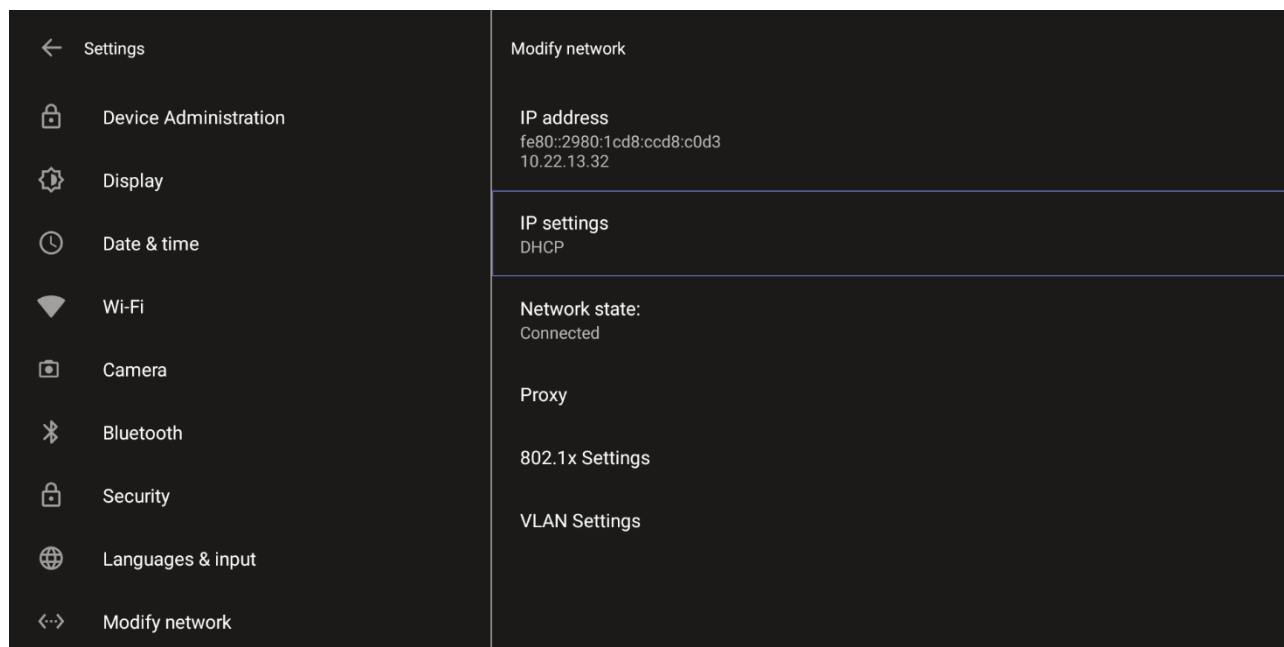
3. Navigate to and select **Show virtual keyboard**.

## 5.1.8 Modify network

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

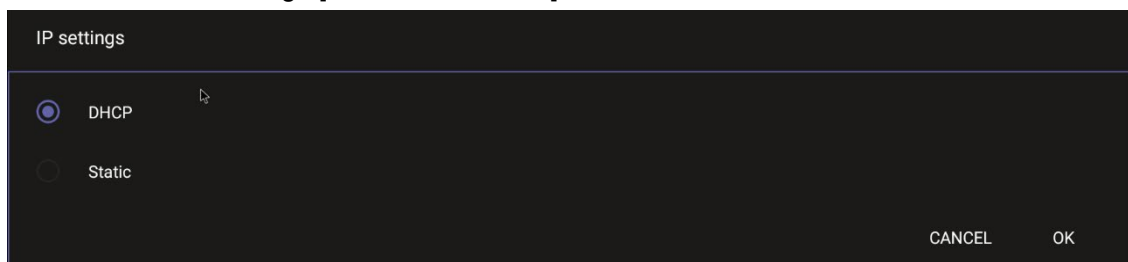
➤ **To modify network settings:**

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

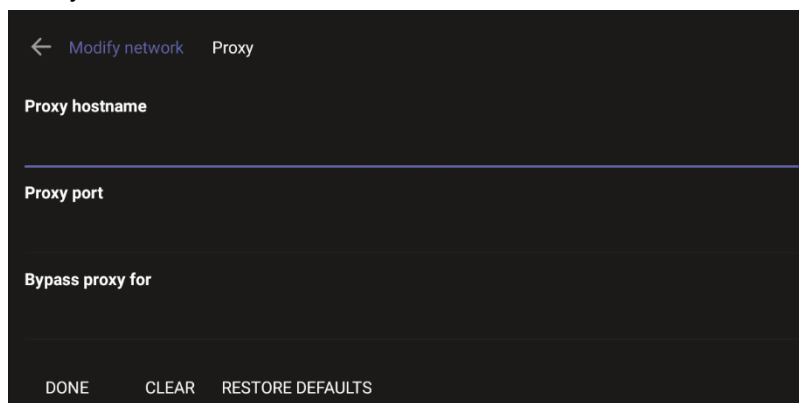


2. Navigate to and select:

- IP Address [Read Only]
- IP Settings [DHCP or Static IP]

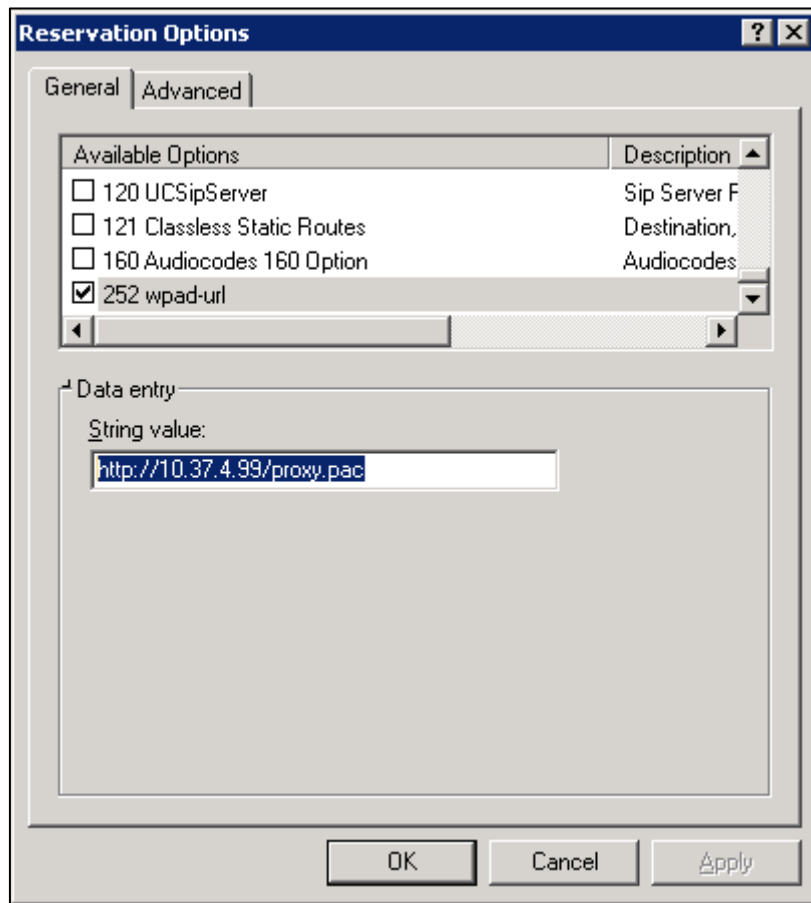


- Network state [Read Only]
- Proxy





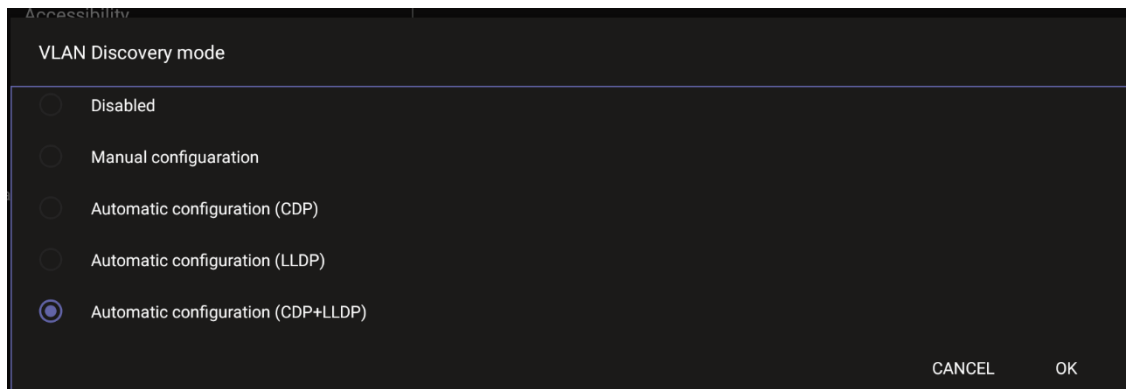
- ◆ Manually (from the screen shown in the preceding figure). Allows you to configure the RXV81 with an HTTP proxy server. Configure the proxy hostname and proxy port and then navigate to and select **Done**.
- ◆ **DHCP Option 252** (recommended). Option 252 provides a DHCP client with a URL to use to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

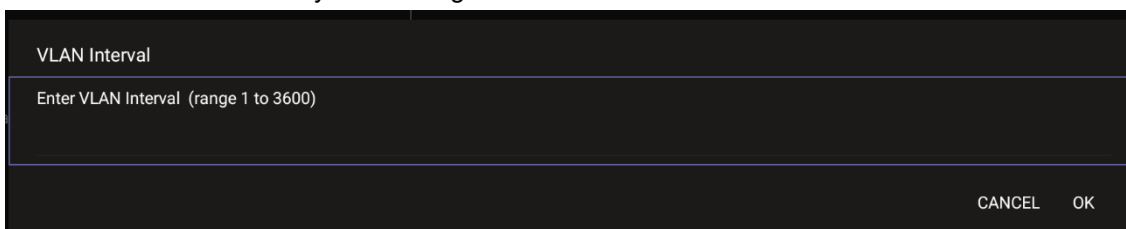


Cisco Discovery Protocol (CDP) is a Cisco proprietary Data Link Layer protocol  
Link Layer Discovery Protocol (LLDP) is a standard, layer two discovery protocol



**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:**

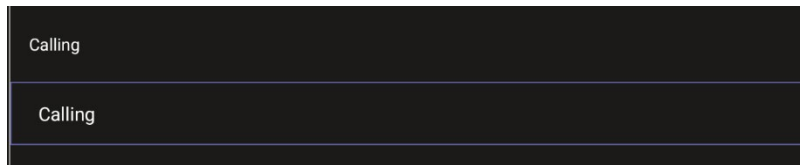
- In versions before 1.19, if network VLAN mode '/network/lan/vlan/mode' was set to LLDP, the device retrieved the VLAN and LLDP switch information (for location purposes) from LLDP.
- From version 1.19, LLDP switch information (for location purposes) is retrieved when parameter network/lan/lldp/enabled=1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

## 5.1.9 Calling

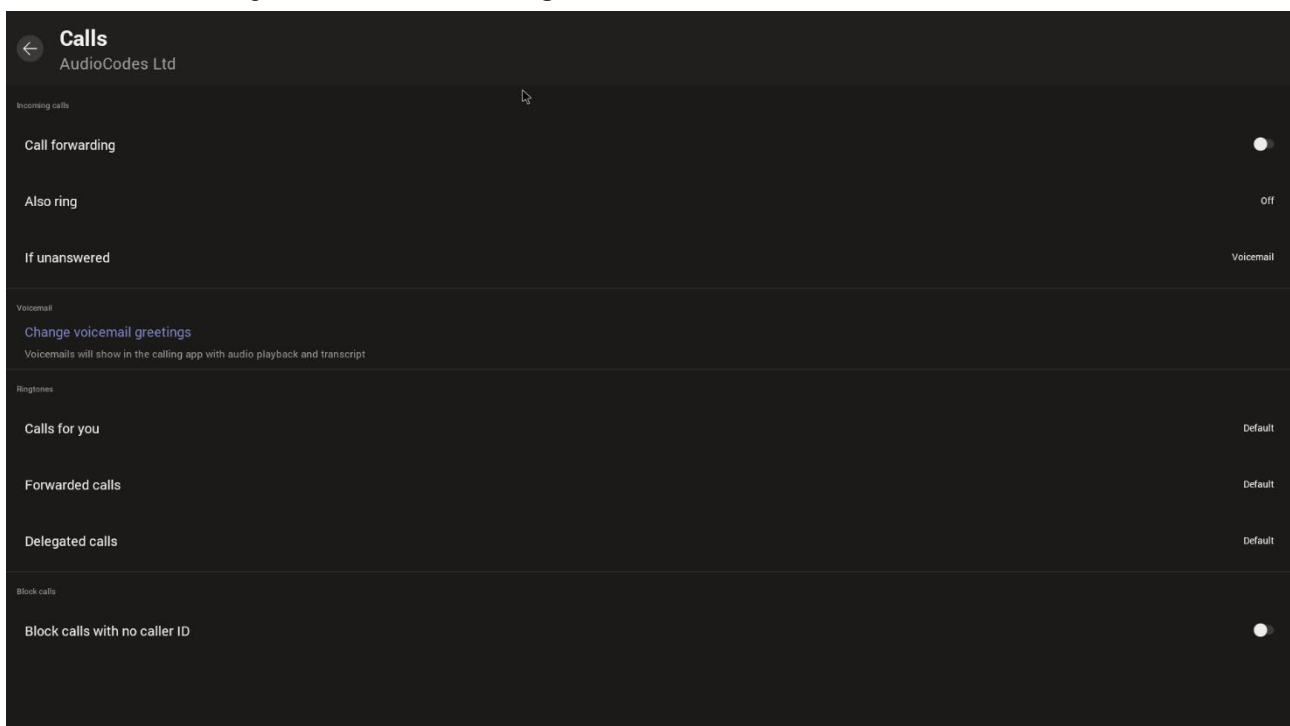
This setting enables the user to configure call-associated functionalities to suit personal preferences.

➤ **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**.

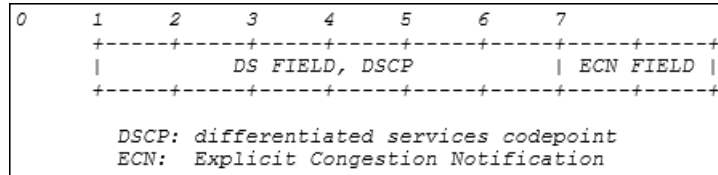


- In the Calls screen, navigate to and select:
  - ♦ **Call forwarding** to enable automatically redirecting incoming calls to another destination.
  - ♦ **Also ring** to configure other phones to ring on incoming calls; only displayed if **Call forwarding** is disabled.
  - ♦ **If unanswered** to configure 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.

## 5.1.10 DSCP

The 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.

2057	47.390455	192.168.2.104	172.17.178.203	UDP	84 50006 → 50012 Len=42
2058	47.390541	192.168.2.104	172.17.178.203	UDP	228 50006 → 50012 Len=186
2059	47.393899	192.168.2.104	172.17.178.203	UDP	151 50006 → 50012 Len=109
2060	47.395193	172.17.178.203	192.168.2.104	UDP	114 50012 → 50006 Len=72
2061	47.395209	172.17.178.203	192.168.2.104	UDP	114 50012 → 50006 Len=72

```

> Frame 2057: 84 bytes on wire (672 bits), 84 bytes captured (672 bits) on interface \Device\NPF_{296D2E63-3934-4B8A-BFAB-666A4B797EE2}, id 0
> Ethernet II, Src: AudioCod_9c:1a:38 (00:90:8f:9c:1a:38), Dst: VMware_ff:63:15 (00:0c:29:ff:63:15)
> Internet Protocol Version 4, Src: 192.168.2.104, Dst: 172.17.178.203
  0100 .... = Version: 4
  .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0xb8 (DSCP: EF PHB, ECN: Not-ECT)
    1011 10.. = Differentiated Services Codepoint: Expedited Forwarding (46)
    .... ..00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)
  Total Length: 70
  Identification: 0xd3ba (54202)
  > Flags: 0x4000, Don't fragment
  Fragment offset: 0
  Time to live: 64
  Protocol: UDP (17)
  Header checksum: 0x4447 [validation disabled]
  [Header checksum status: Unverified]
  Source: 192.168.2.104
  Destination: 172.17.178.203
  > User Datagram Protocol, Src Port: 50006, Dst Port: 50012
  
```

The figure below shows the recommended DSCP setting for Video.

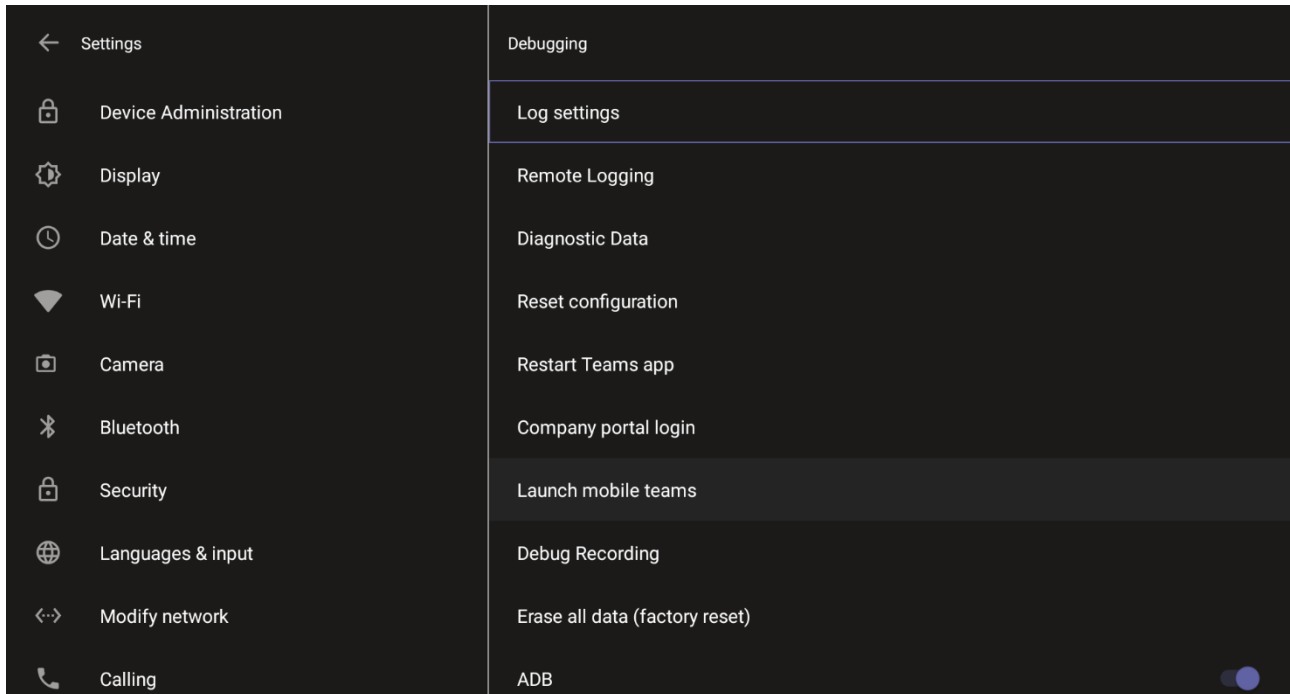
2290 8.194033	192.168.2.103	172.17.178.101	UDP	1022 50036 → 50023 Len=980
2291 R.194102	192.168.2.103	172.17.178.101	UDP	1022 50036 → 50023 Len=980
<p>Frame 2290: 1022 bytes on wire (8176 bits), 1022 bytes captured (8176 bits) on interface \Device\NPF_{296D2E63-3934-4B8A-BFAB-666A4B797EE2}, id 0</p> <p>Ethernet II, Src: DolbyLab_10:02:04 (00:d0:46:10:02:04), Dst: VMware_ff:63:15 (00:0c:29:ff:63:15)</p> <p>Internet Protocol Version 4, Src: 192.168.2.103, Dst: 172.17.178.101</p> <p>0100 .... = Version: 4</p> <p>.... 0101 = Header Length: 20 bytes (5)</p> <p>▼ Differentiated Services Field: 0x88 (DSCP: AF41, ECN: Not-ECT)</p> <p>1000 10.. = Differentiated Services Codepoint: Assured Forwarding 41 (34)</p> <p>.... ..00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)</p> <p>Total Length: 1008</p> <p>Identification: 0x8368 (33640)</p> <p>Flags: 0x4000, Don't fragment</p> <p>Fragment offset: 0</p> <p>Time to live: 64</p> <p>Protocol: UDP (17)</p> <p>Header checksum: 0x9186 [validation disabled]</p> <p>[Header checksum status: Unverified]</p> <p>Source: 192.168.2.103</p>				

## 5.1.11 Debugging

Admin users can perform debugging for troubleshooting purposes.

➤ **To perform Debugging:**

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



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

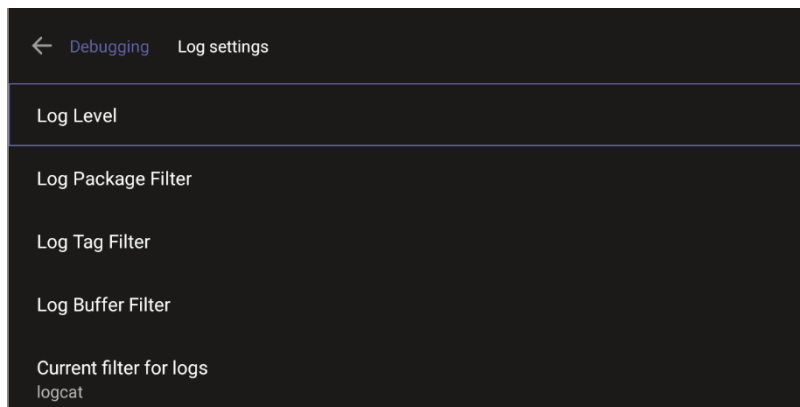
- Log settings (see [Log Settings](#))
- Remote Logging (see under [Remote Logging](#))
- Diagnostic Data (see under [Diagnostic Data](#))
- Reset configuration (see under [Reset configuration](#))
- Restart Teams app (see under [Restart Teams app](#))
- Company portal login (see under [Company Portal Login](#))
- Launch mobile teams (see under [Launch Mobile Teams](#))
- Debug Recording (see under [Debug Recording](#))
- Erase all data (see under [Erase all data](#))
- Screen Capture (see under [Screen Capture](#))

### 5.1.11.1 Log Settings | Collecting Logs

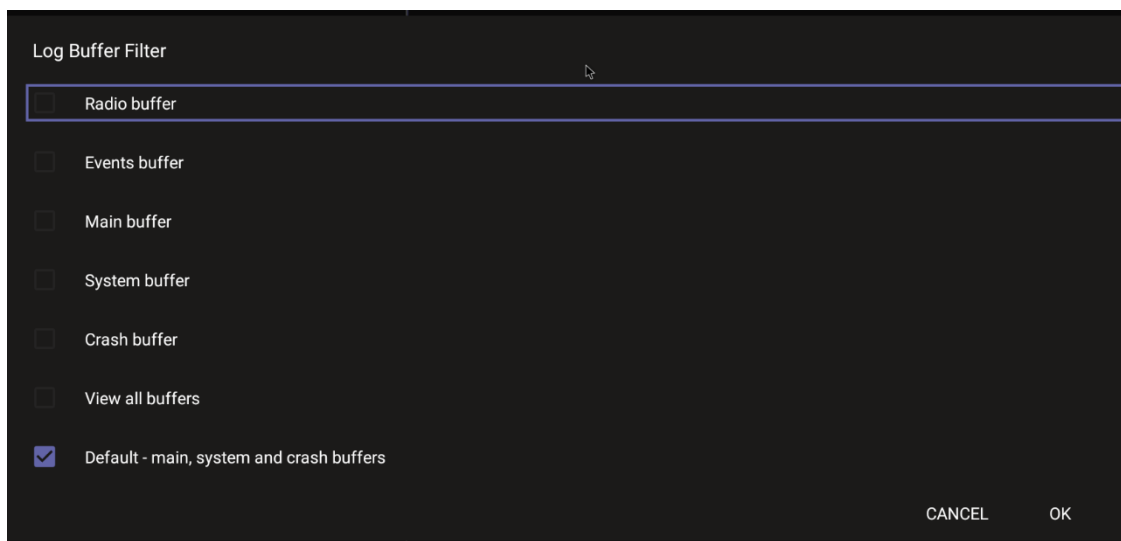
Device diagnostics (Logcat) can be collected using the Microsoft Admin Portal. For support purposes, general logs can be collected also using the Microsoft Admin Portal. The logs can help debug Teams application issues and also for issues related to the device.

➤ **To configure log settings:**

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



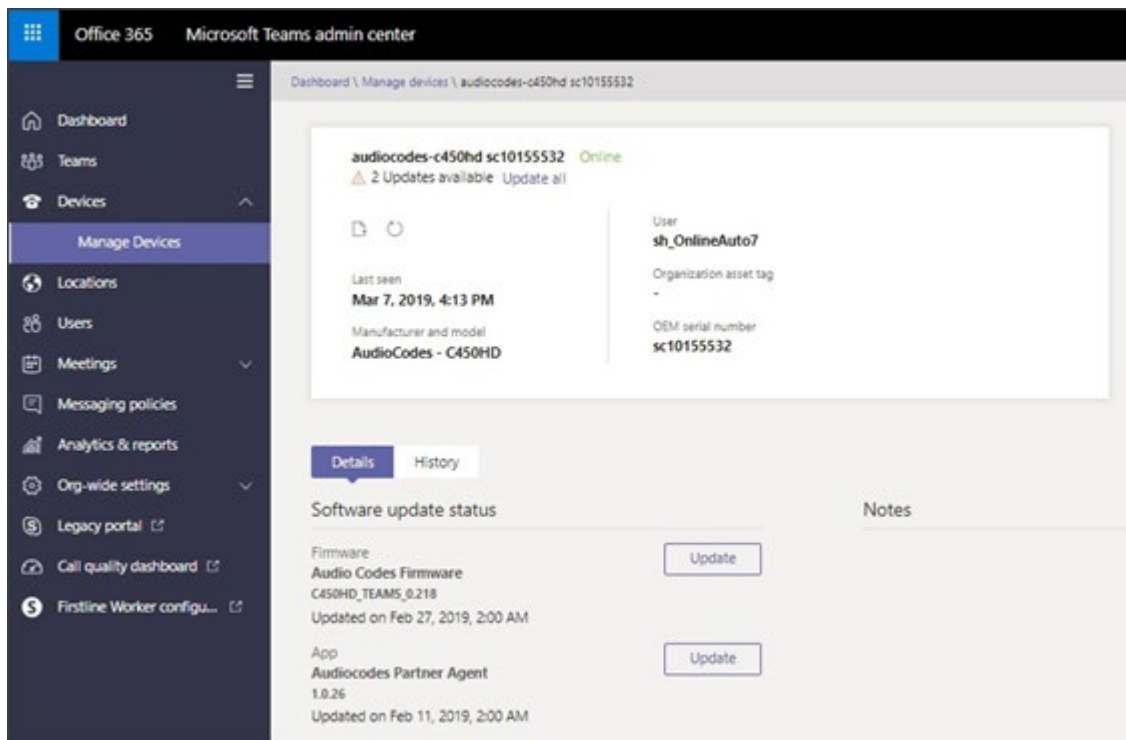
2. Navigate to and select **Log Level** and then select either
  - Verbose, Debug, Info, Warning, Error, Assert -or- None
3. Navigate to and select **Log Package Filter** and enter the filter.
4. Navigate to and select **Log Tag Filter** and enter the filter.
5. Navigate to and select **Log Buffer Filter**.



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

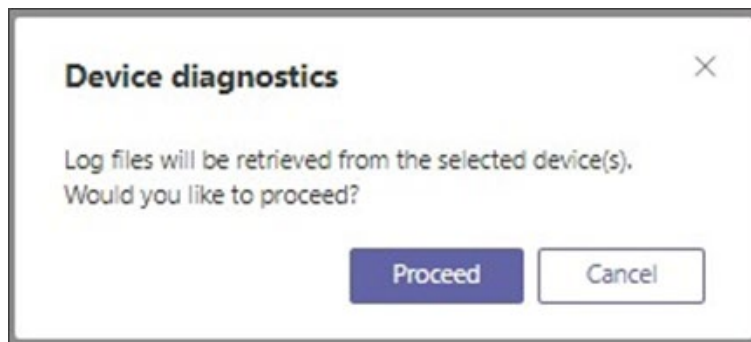
➤ **To collect logs:**

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



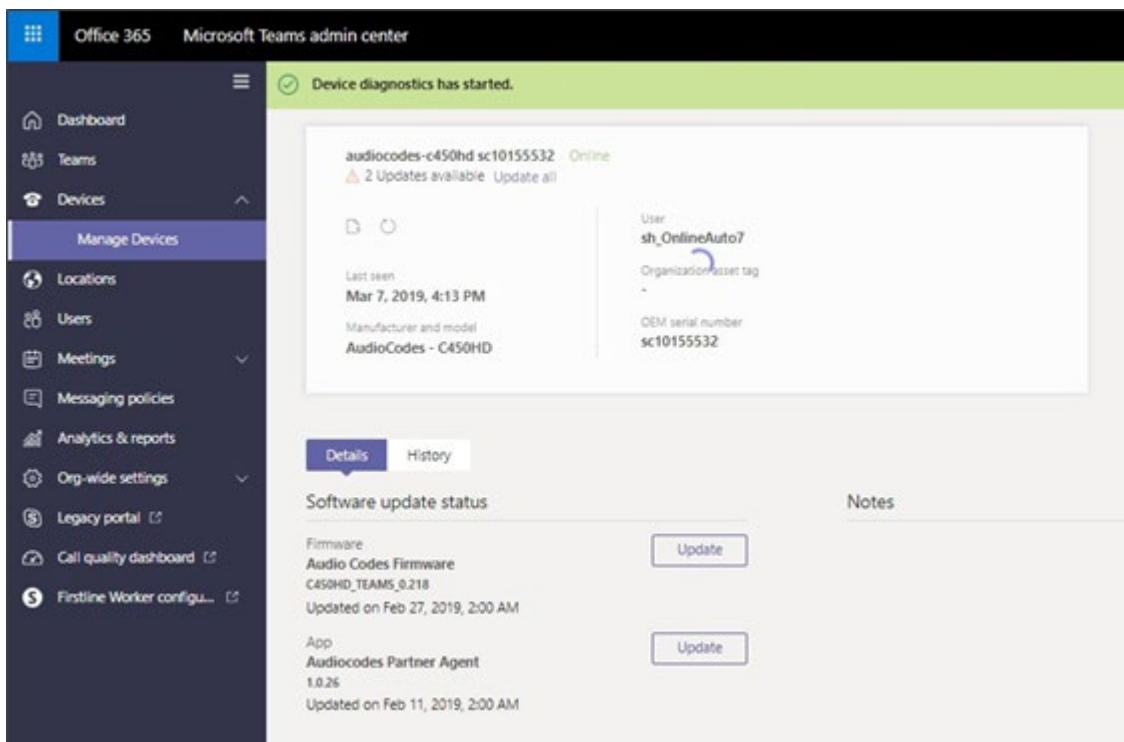
**Note:** The preceding figure is for illustrative purposes. It shows an AudioCodes phone. The same screen is displayed for the RXV81.

3. Click the **Diagnostics** icon.

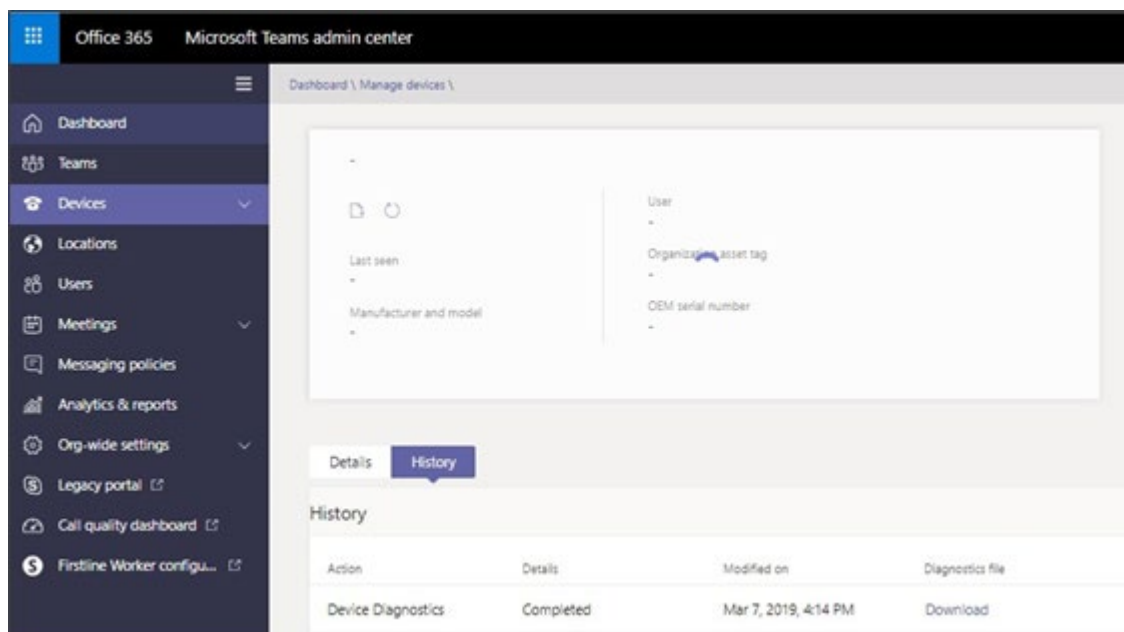




4. Click **Proceed**; the logs are uploaded to the server.



5. Click the **History** tab.



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

#### 5.1.11.2 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 ""
```

### 5.1.11.3 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'; the 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):

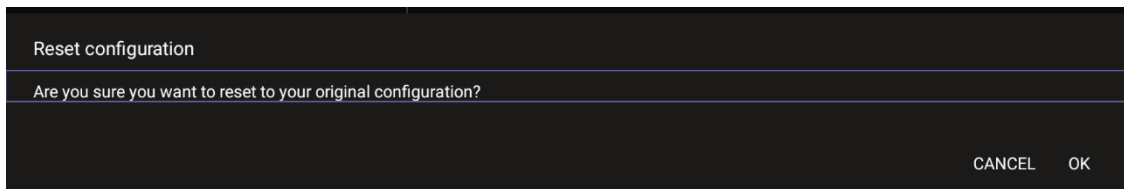
- dmesg.log
- dumpstate-TEAMS\_1.3.16-undated.txt
- dumpstate\_log-undated-2569.txt
- logcat.log

#### 5.1.11.4 Reset configuration

Admin users can opt to 'clean up' their configuration history and return the 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:

<https://docs.microsoft.com/en-us/MicrosoftTeams/rooms/rooms-operations#microsoft-teams-rooms-reset-factory-restore>

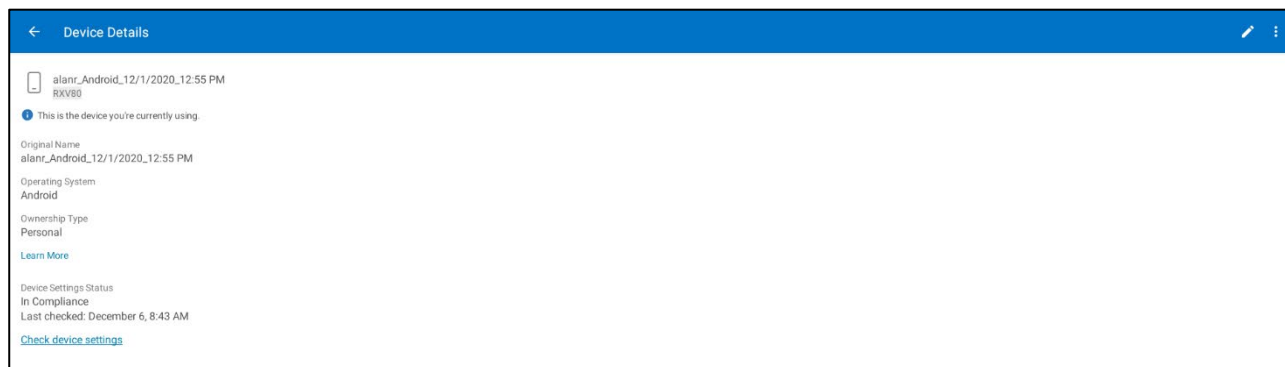
#### 5.1.11.5 Restart Teams app

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.

#### 5.1.11.6 Company Portal Login

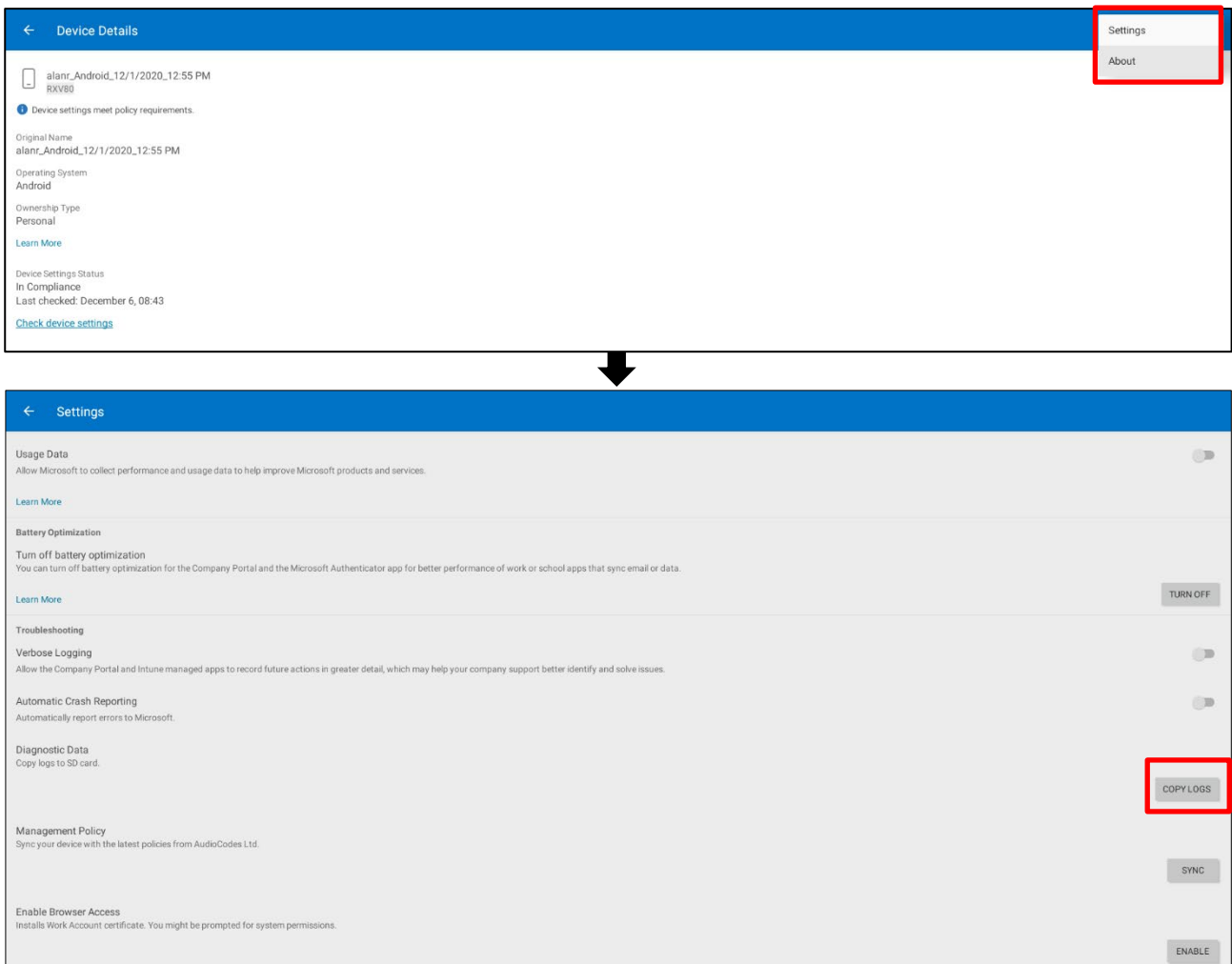


#### 5.1.11.7 Getting Company Portal Logs

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 the 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.

### 5.1.11.8 Launch Mobile Teams

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

### 5.1.11.9 Debug Recording

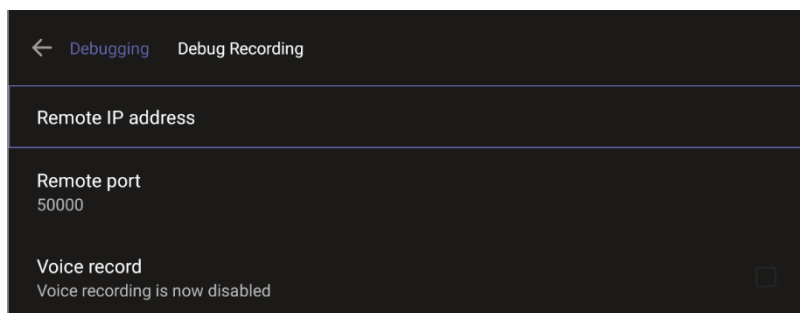
This feature enables Admin users to perform media/DSP debugging.



**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**.



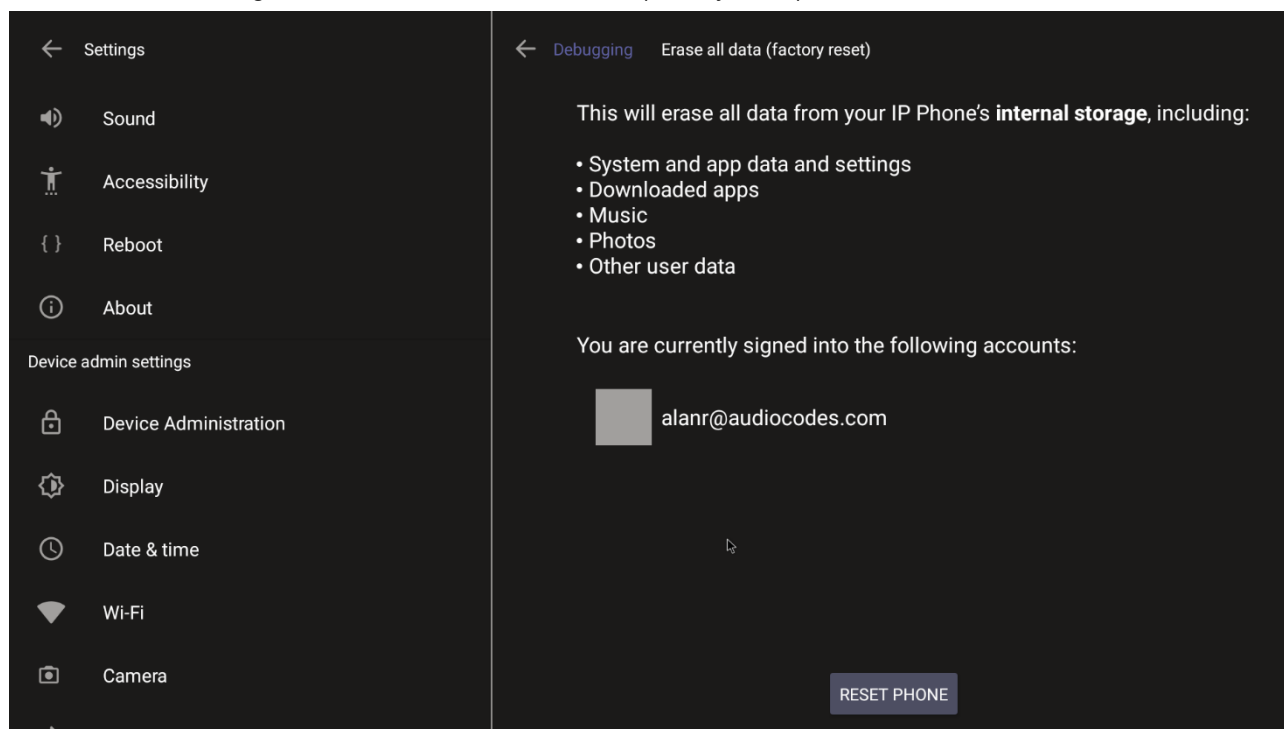
2. Navigate to and select **Voice record** to enable the feature.
3. Navigate to and select **Remote IP address** to input the IP address of the device whose traffic you want to record.
4. Navigate to and select **Remote port** and input it (Default: 5000).
5. Start Wireshark on your PC to capture audio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

#### 5.1.11.10 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**.

#### 5.1.11.11 Screen Capture

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

## 5.2 Performing Recovery Operations using the Power Button

Network administrators can perform recovery operations using the power button on the rear panel of the 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 the RXV81 while long-pressing the power button for as long as is required for the action (see [Table 5-2](#) 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 5-2: Recovery Operation Options using the 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	

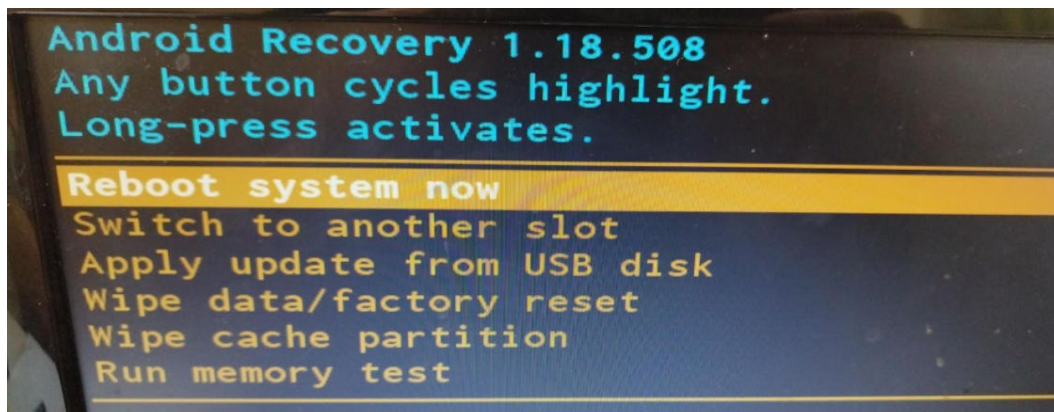
3. Short-press the power button to move down the menu options, and long-press to select an option.

## 5.3 Restoring Device Firmware via USB Disk

For recovery purposes, firmware can be applied to the 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 5-2](#) 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.

## 5.4 Configuring User Settings

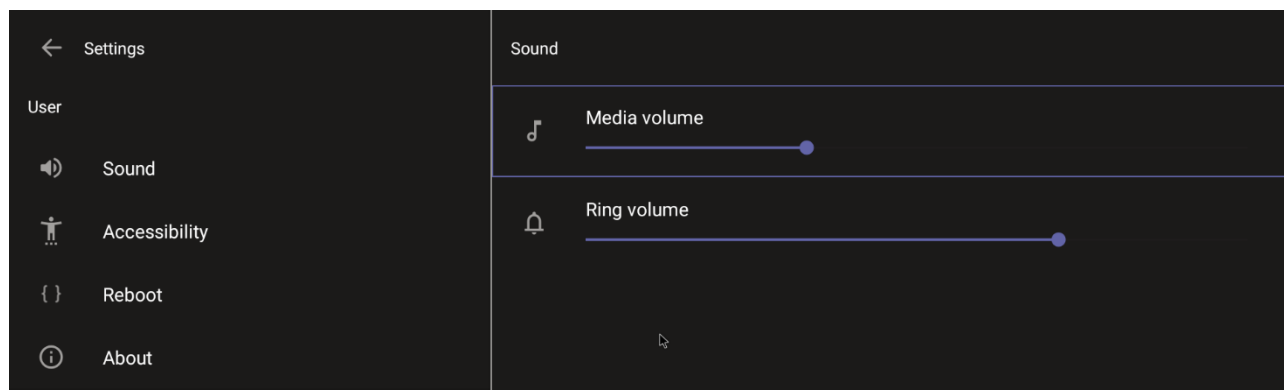
In the 'Settings' screen you can optionally configure the following User settings: Sound, Accessibility, Reboot and About (read-only).

### 5.4.1 Sound

You can customize phone volume for a friendlier user experience.

➤ **To configure sound settings:**

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

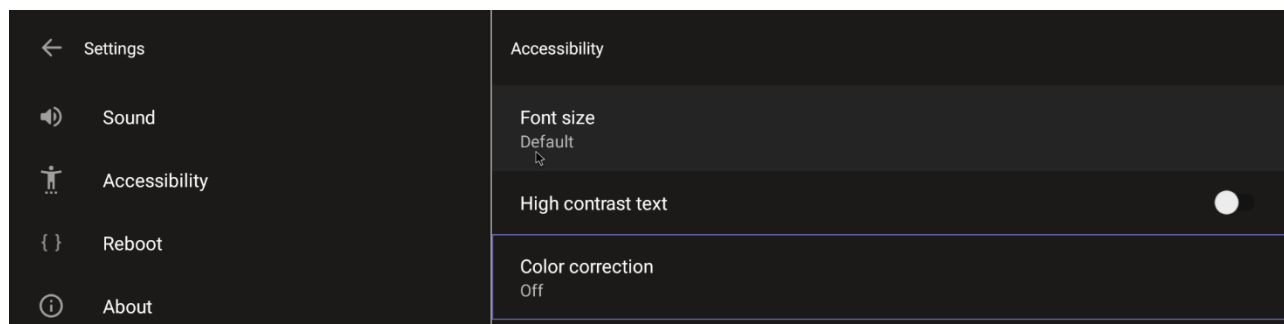


### 5.4.2 Accessibility

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

➤ **To configure the Accessibility setting:**

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



2. Adjust the settings to suit personal requirements.

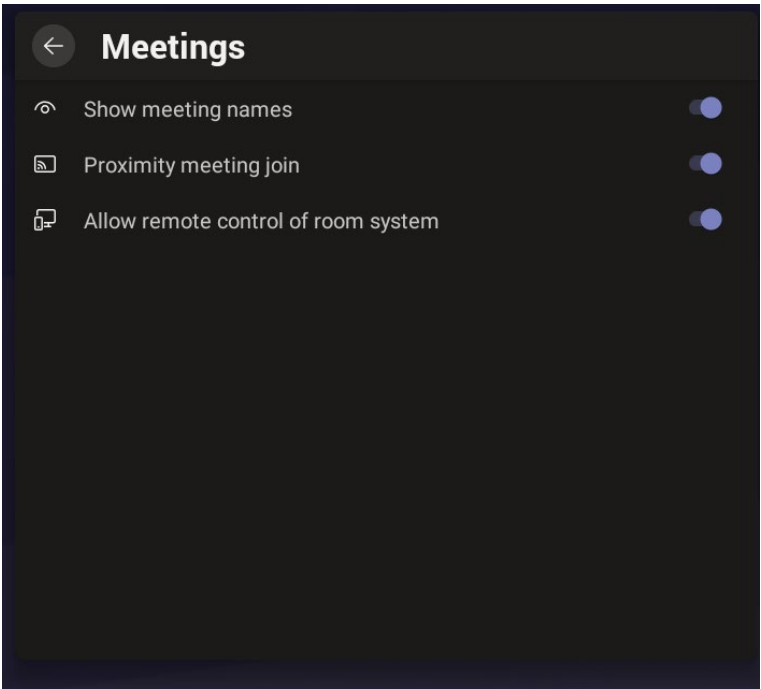
### 5.4.3 Setting Live Captions

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

### 5.4.4 Hiding Names and Meeting Titles

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





5.4.5 Reboot

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

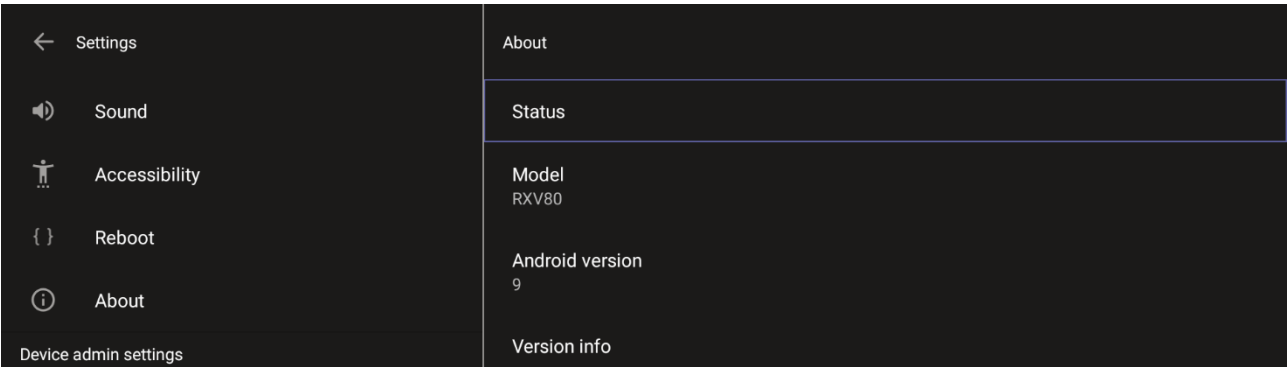
- **To reboot the RXV81:**
  - Under ‘User’, navigate to and select **Reboot**.



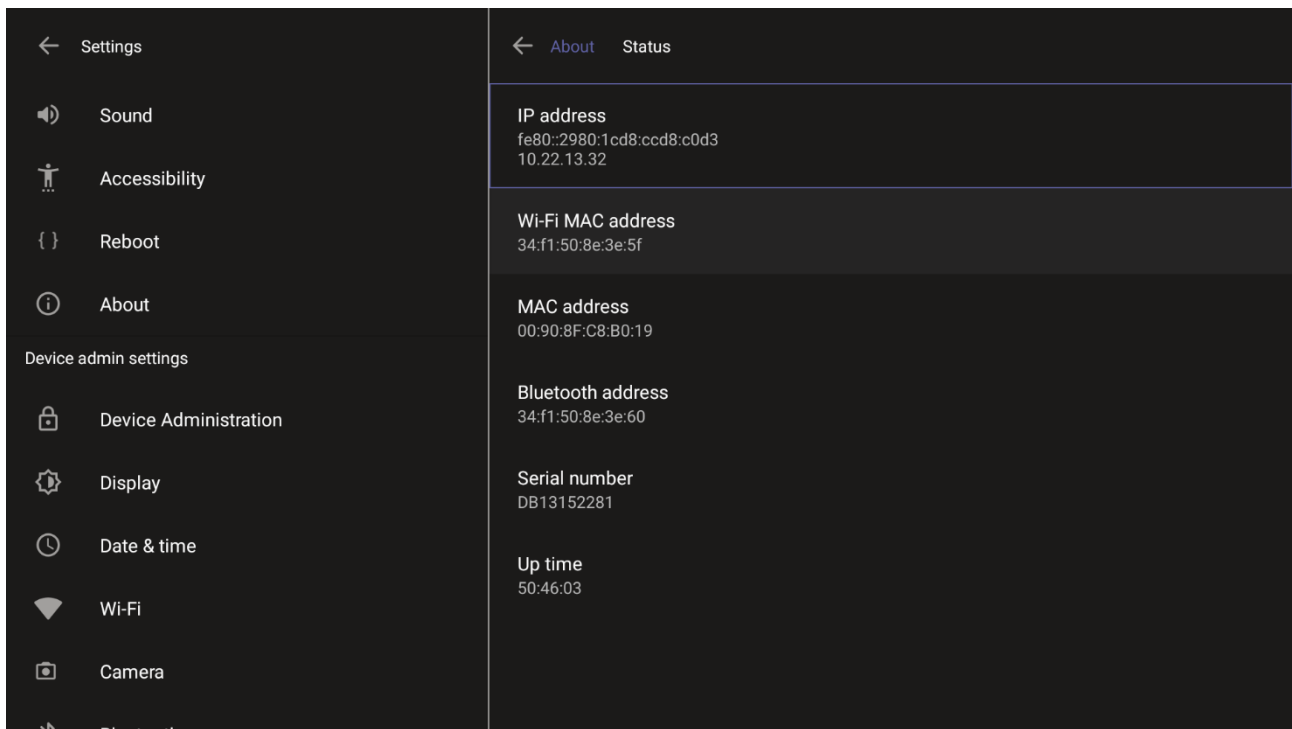
5.4.6 About

The ‘About’ screen gives you quick access to information about the RXV81 deployment.

- **To access the About screen:**
  - 1. Under ‘User’, navigate to and select **About**.



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






3. View the RXV81's firmware information.

## 6 Viewing LEDs to Determine Status

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



**Table 6-1: Viewing RXV81 LEDs to Determine Status**

	<b>Red / white / red &amp; white</b>
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
	<b>Blue</b>
Blue on	In a call (active call or meeting)
Blue flashing	Incoming call
	<b>Camera on/off</b>
White on	Camera on
White off	Camera off

This page is intentionally left blank.

## 7 Using RXV81 in Ad Hoc Peripheral Mode


In addition to standalone mode, the RXV81 MTR on Android Video Collaboration Bar can be used in ad hoc peripheral mode. In this mode, customers connect the 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 Remote Control (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 *Deployment Guide* for detailed information on cabling the RXV81.

Connect the device's  USB Type C port to a BYOD (Bring Your Own Device) (PC/laptop) running a UC client.

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 Remote Control 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 Microsoft Teams Devices Remotely

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



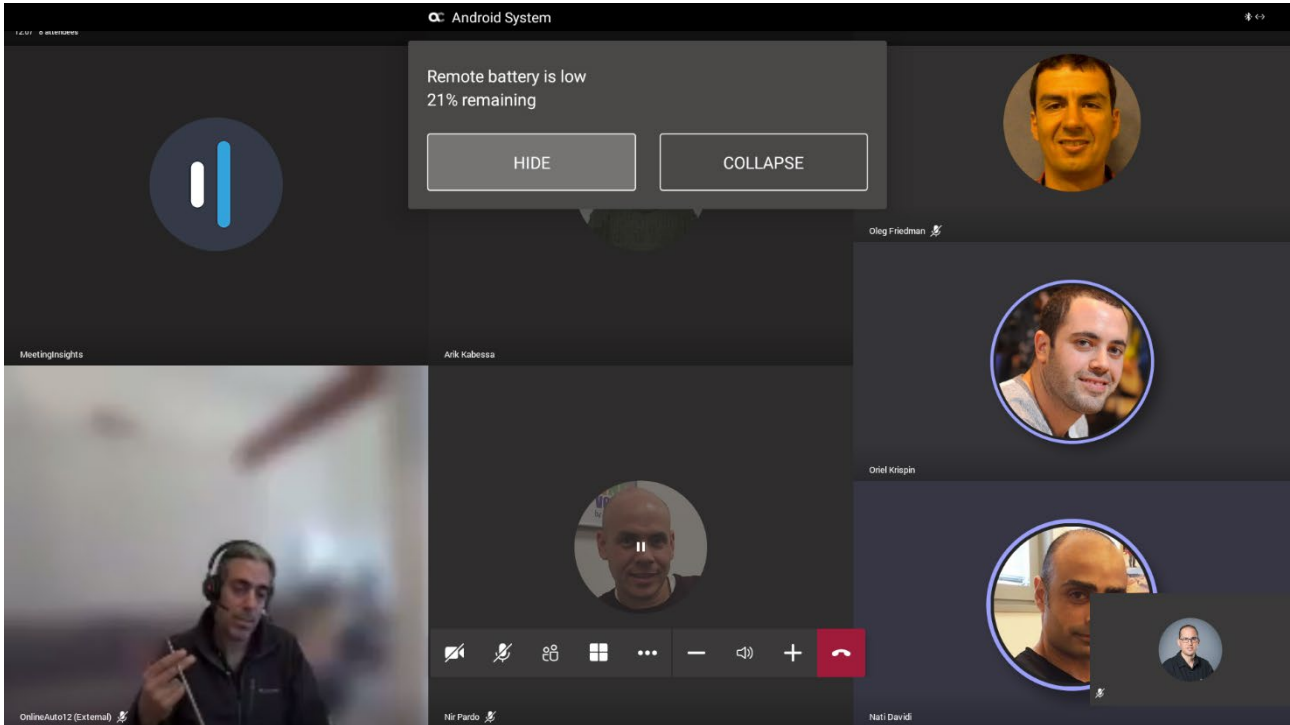
**Note:** Before an update is pushed to a device, the firmware detects whether the user is using the device or not. If they are, the user is notified and given an option to delay the update or apply it, nonetheless. The feature avoids disrupting users' ongoing activities on their devices, such as calls.

This page is intentionally left blank.



## 9 Replacing Remote Controller Batteries

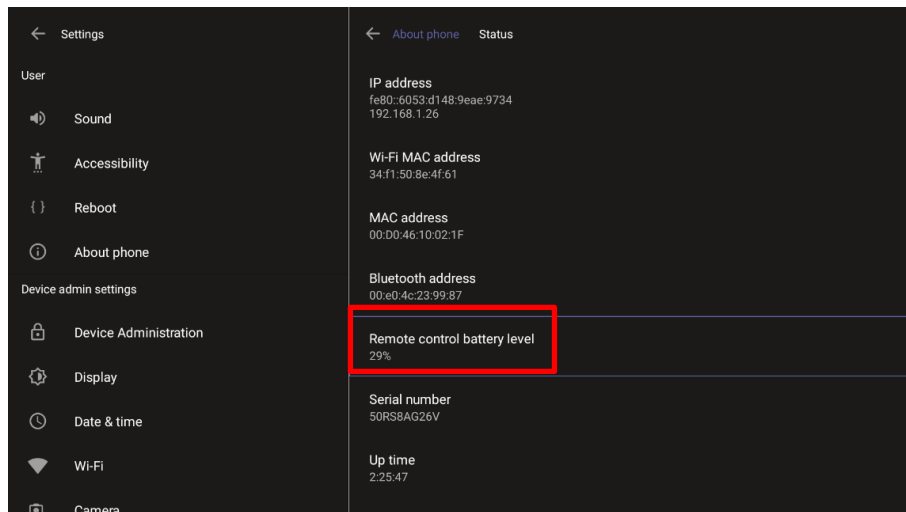
If the remote controller batteries run low, the RXV81 application notifies you about the issue. A notification is sent to the screen/TV as well as to AudioCodes' Device Manager if battery voltage level falls low, indicating what percentage level remains unused.



Select **HIDE** to conceal the notification.

### 9.1 Assessing the RC's Battery Level

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 the RXV81

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

➤ **To restart / reboot the RXV81:**

- Long-press the remote controller's power on/off button for about five seconds.  
-OR-
- Long-press the RXV81 back button for ~5 seconds, then release it.

## 9.3 Powering Down/Up the RXV81

The RXV81 can be powered down/up.

➤ **To power down the RXV81:**

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

➤ **To power up the RXV81:**

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

This page is intentionally left blank.

## 10 Supported 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**

1 Hayarden Street,  
Airport City  
Lod 7019900, 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/>

©2023 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, VolPerfect, VolPerfectHD, Your Gateway To VoIP, 3GX, VocaNom and AudioCodes One Voice 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-18252

