

RXV80 Standalone Video Collaboration Bar

Version 1.13



Microsoft Partner
Gold Communications



Table of Contents

1	Introduction	9
1.1	About AudioCodes' RX Suite	9
1.2	Specifications.....	10
1.3	Security Guidelines	11
1.3.1	Microsoft Teams Security Guidelines.....	11
1.3.2	Android Level Security Hardening.....	11
1.3.2.1	Google Play Services	11
1.3.2.2	Running Android in Kiosk Mode.....	11
1.3.2.3	Screen Lock	12
1.3.2.4	AudioCodes Private Key.....	12
1.3.2.5	Android Debug Bridge (ADB).....	12
1.3.2.6	App Signing.....	12
1.3.2.7	Web Browser.....	12
1.3.2.8	Remote Configuration Management.....	12
1.3.2.9	AudioCodes Device Manager Validation	12
1.3.2.10	Sandboxing	13
1.3.2.11	Keystore.....	13
1.3.2.12	Device Certificate	13
1.3.2.13	Data Protection.....	13
1.3.2.14	Device File System.....	13
1.3.2.15	Debugging Interface	13
1.3.3	Android Security Updates	13
1.3.4	AudioCodes Root CA Certificate.....	14
2	Setting up the RXV80	15
3	Getting Started.....	17
3.1	Modifying Camera Settings	18
3.2	Starting a New Meeting.....	21
3.3	Dialing a Number	24
3.4	Enabling Proximity Join.....	25
3.5	About Microsoft Teams	26
3.6	Signing out.....	26
4	Configuring Device Settings.....	27
4.1	Configuring Device Admin Settings.....	30
4.1.1	Display Settings	30
4.1.2	Date & Time	32
4.1.3	Wi-Fi Settings.....	33
4.1.3.1	Configuring Wi-Fi.....	33
4.1.4	Camera	35
4.1.4.1	Configuring Camera Frequency	36
4.1.5	Bluetooth.....	36
4.1.6	Security.....	37
4.1.7	Languages & input	39
4.1.8	Modify network	40
4.1.9	Calling.....	41
4.1.10	Debugging.....	43
4.1.10.1	Log Settings Collecting Logs.....	44
4.1.10.2	Remote Logging	46
4.1.10.3	Diagnostic Data.....	47
4.1.10.4	Reset configuration.....	48
4.1.10.5	Restart Teams app	48
4.1.10.6	Company Portal Login	48

4.1.10.7	Getting Company Portal Logs	48
4.1.10.8	Launch Mobile Teams	49
4.1.10.9	Debug Recording.....	49
4.1.10.10	Erase all data (factory reset).....	50
4.1.10.11	ADB	51
4.1.10.12	Screen Capture	51
4.1.10.13	Remote Packet Capture	51
4.2	Configuring User Settings	52
4.2.1	Sound	52
4.2.2	Accessibility	52
4.2.3	Reboot	52
4.2.4	About	53
5	Updating Microsoft Teams Devices Remotely	55
6	Replacing Remote Controller Batteries.....	57
6.1	Restarting / Rebooting the RXV80	57
7	Supported Parameters	59

List of Figures

Figure 3-1: Home Screen.....	18
Figure 3-2: Camera Settings	18
Figure 3-3: Login when the RXV80 is in idle state.....	19
Figure 3-4: Camera settings - Save View	20
Figure 3-5: Camera settings - Save View	20
Figure 3-6: New meeting – Invite someone	21
Figure 3-7: New meeting – Enter the name of a person.....	21
Figure 3-8: New meeting – Select the name of a person.....	22
Figure 3-9: Dial pad	24

List of Tables

Table 1-1: Specifications.....	10
Table 4-1: Wi-Fi Parameters.....	33
Table 4-2: Wi-Fi Parameters per Index	33

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: May-18-2021

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
RXV80 Standalone Video Collaboration Bar Deployment Guide
RXV80 Standalone 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

The AudioCodes RXV80 standalone video collaboration bar delivers an intuitive meeting room experience in video-enabled meeting rooms, and is especially designed for huddle rooms. Integrated processing capabilities deliver unified communication in a standalone device, enabling remote participants to see and hear everyone in the room with outstanding video image clarity and enhanced voice quality.

Feature highlights:

- **Wide-angle 4K Camera & HDR Video Mapping**

Covers a 110° viewing angle capturing every seat in the room even in tight spaces with challenging lighting conditions

- **Seamless Integration with the Microsoft Teams UC Platform**

Enables quick and easy deployment, installation, and moderation with click-to-join functionality for both video-enabled collaboration and voice-only conference calls.

- **Intuitive & Cost-effective Meeting Experience**

Leverages touch controller and existing TV speakers without relying on personal devices such as laptops or phones.

AudioCodes' remote controller software is managed by the RXV80; the controller leverages Bluetooth which enables full control and bi-directional communication. Remote controller keys (Mute, Teams) are illuminated.

- **Operational Efficiency**

Enhances meeting experience with centralized management, monitoring, and continuous productivity.

- **Dynamic Levelling & Intelligent Acoustics™**

Boosts quiet or distant voices while distinguishing speech from noise.

1.1 About AudioCodes' RX Suite

The RX Suite offering initially consisted of a portfolio of meeting room solutions to enhance meeting productivity through high-quality audio conferencing plus the Meeting Insights app to handle meeting recording, post-meeting analytics, and action item follow up.

Collaboration Bars for Microsoft Teams provides customers a simple and easy-to-use Teams meeting experience in more spaces across their organizations. The RX Suite has a line of conferencing devices that address a wide range of meeting room environments from huddle rooms to boardrooms.

The RXV80 Collaboration Bar for Microsoft Teams, part of the RX Suite, dramatically enhances the experience of Teams users seeking next-level experiences.

Jointly developed with Dolby Communications Business Group, the video conferencing solution integrates Dolby audio and video quality with AudioCodes' expertise in integrating with Microsoft Teams.

The RXV80 ensures that users experience exceptional audio and video quality whether they're in the meeting room or anywhere else.

1.2 Specifications

The following table shows the RXV80 specifications.

Table 1-1: Specifications

Feature	Details
Video capabilities	<ul style="list-style-type: none"> ▪ Ultra HD 4k Image Sensor ▪ 1/1.8" CMOS ▪ Super-wide Angle Horizontal Field of View: 110° ▪ Lens: Fixed focus, f/1.8 aperture ▪ HDR video mapping ▪ EPTZ capable ▪ H.264 Baseline and High Profile ▪ Output Resolution: 1080p ▪ Frame Rate: 30 fps
Audio	<ul style="list-style-type: none"> ▪ Full duplex, noise suppression, acoustic echo cancellation, voice separation ▪ Audio output through HDMI (developed in partnership with Dolby) ▪ 4X beamforming microphone array ▪ Voice pickup range: 4.5m (15ft) ▪ Audio frequency: G.711a/G.711u/G.722/G.729ab/Opus ▪ Audio range: Super wideband, 160Hz – 16kHz
Device Interfaces	<ul style="list-style-type: none"> ▪ Single HDMI output to TV ▪ HDMI input (roadmap) ▪ USB 3.0 host ports (x2) ▪ Wi-Fi (dual band support) ▪ Bluetooth (BLE support) ▪ Network: 10/100/1000 Mb (RJ-45) network interface ▪ Kensington lock ▪ Supports tripod mounting
Network Provisioning	<ul style="list-style-type: none"> ▪ 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	<ul style="list-style-type: none"> ▪ Android 9.0
UC Platform Support	<ul style="list-style-type: none"> ▪ Microsoft Teams ▪ Intuitive meeting experience with calendar integration and click-to-join (one-touch or proximity join experience)
Security	<ul style="list-style-type: none"> ▪ Encryption: TLS (Transport Layer Security), SRTP encryption for media, AES256 ▪ Network Access Control: IEEE 802.1x ▪ Built-in certificate

1.3 Security Guidelines

The RXV80 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

1.3.1 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](#)

1.3.2 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.

1.3.2.1 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.

1.3.2.2 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).

1.3.2.3 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.

1.3.2.4 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.

1.3.2.5 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.

1.3.2.6 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.

1.3.2.7 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.

1.3.2.8 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.

1.3.2.9 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.

1.3.2.10 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.

1.3.2.11 Keystore

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

1.3.2.12 Device Certificate

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

1.3.2.13 Data Protection

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

1.3.2.14 Device File System

The device file system is encrypted on the RXV80 device – customers may enforce a policy of device encryption via Microsoft Intune.

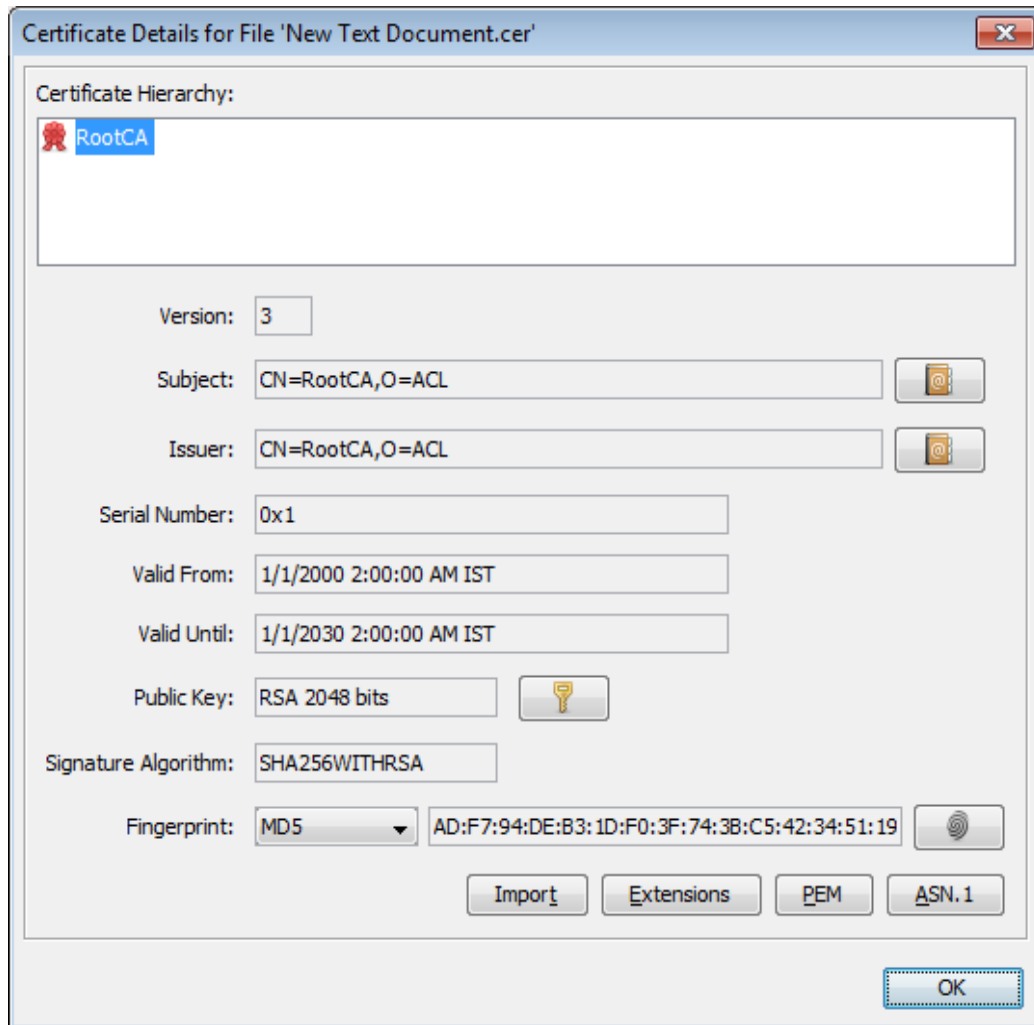
1.3.2.15 Debugging Interface

- 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.

1.3.3 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>).

1.3.4 AudioCodes Root CA Certificate



```
-----BEGIN CERTIFICATE-----
MIIDMTCCAhmGAWIBAgIBATANBgkqhkiG9w0BAQsFADAfMQwwCgYDVQQKEwNBQ0wx
DzANBgNVBAMTB1Jvb3RDQTAeFw0wMDAxMDEwMDAwMDBaFw0zMDAxMDEwMDAwMDBa
MB8xDDAKBgNVBAoTA0FDTDEPMA0GA1UEAxMGUm9vdENBMIIBIjANBgkqhkiG9w0B
AQEFAAOCAQ8AMIIBCgKCAQEA6GK495KUCXAm/UE17G4/cjnZN4LNaxYEFYzbfZL0a
EhgSKYt/LQ+iUcDhojsneusNgrcGkpWkklKsGsvGwMSRNULV01CW+TX2VJN73+hh
V0uzhyOIYAUhbDaoqNM6Kp5b7sJ1ew4Ig9kfd/ma9Czl5koESLlw/inLj/r+rD96
mUcPElWrKspv7Qy4I14fsK/yMArixRopTL1munVVPpSFM9Jh8IY3JHyr5CQJXKKs
EhGAJsnHaRqsR2Su3X/WtslgEF+cvP34pxhlhFL29nMfnaFATSS3rgGaFlSv11ZS
esLMqkWjp9cqGYrvt7K61sYnvMMb+o/KbWqVokXb+Fr7bwIDAQABO3gwdjAMBgNV
HRMEBTADAQH/MB0GA1UdDgQWBBDQXySn9hz15lDraZ+iXddZGREB+zBHBgNVHSME
QDA+gBQDXySn9hz15lDraZ+iXddZGREB+6EjpcEwHzEMMAoGA1UEChMDQUNMMQ8w
DQYDVQQDEwZSb290Q0GCAQEWdQYJKoZIhvcNAQELBQADggEBAI0rUywowmWWJnH3
JOfKiS3+VnX5hJITZymvWanMXUz/6FonHccPXEByTrUYwhiWx3dwELAFXDFKkxMp
0KKWZ4F39cAOLRjqhzya+xUeeJ9HQZCXyAJ6XgvTfn2BtyZk9Ma8WG+H1hNvvTZY
QLbWsjQdu4eFniEufeYDke1jQ6800LwMlFlc59hMQCeJTEnRx4HdJbJV86k1gBUE
A7fJTlePrRnXNDRz6QtADWoX3OmN7Meqen/roTwvLpEP22nYwvB28dq3JetlQKwu
XC4gwI/o8K2wo3pySLU9Y/vanXXCr0/en5l3RDz1YpYWmQwHA8jJiU8rxdhr+VNQ
Zv6R/Ys=
-----END CERTIFICATE-----
```

2 Setting up the RXV80



Note: See the *RXV80 Standalone Video Collaboration Bar Deployment Guide* shipped with the product or available from AudioCodes for information related to the hardware of the RXV80, including:

- Package contents
- Mounting
- Cabling

This page is intentionally left blank.

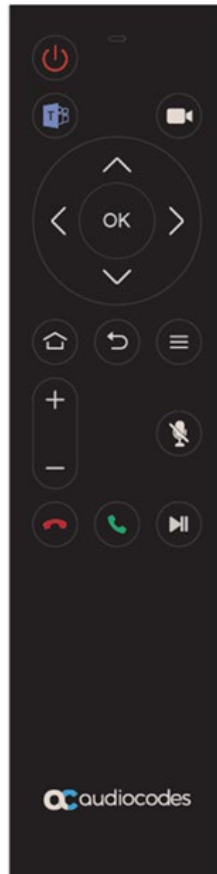
3 Getting Started



Note: See the *RXV80 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 app
- Sign in

The figure below shows AudioCodes' remote controller.



- The software on the remote controller is managed by the RXV80.
- 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.

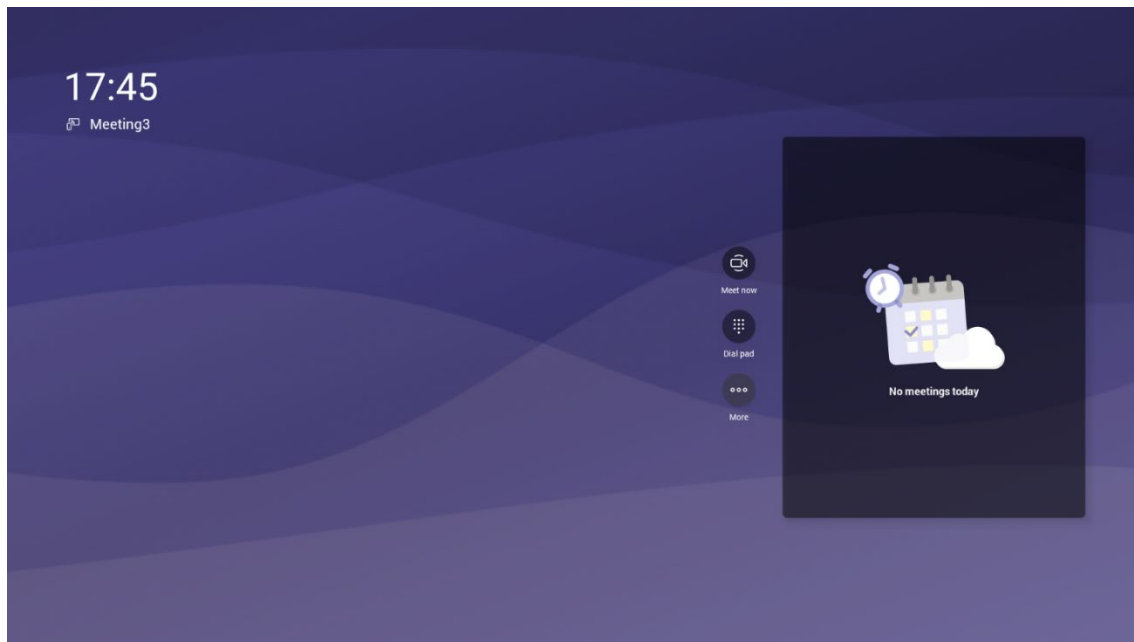


Note: The remote controller flashes if the connection to the RXV80 fails.

➤ **To get started:**

1. After signing in, view the RXV80 home page.

Figure 3-1: Home Screen



3.1 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:**


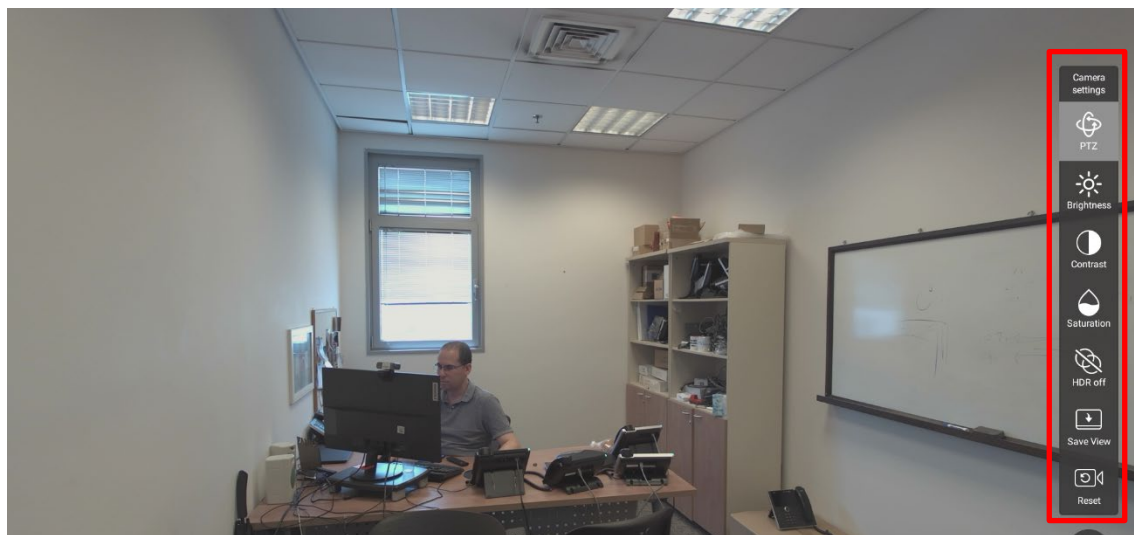
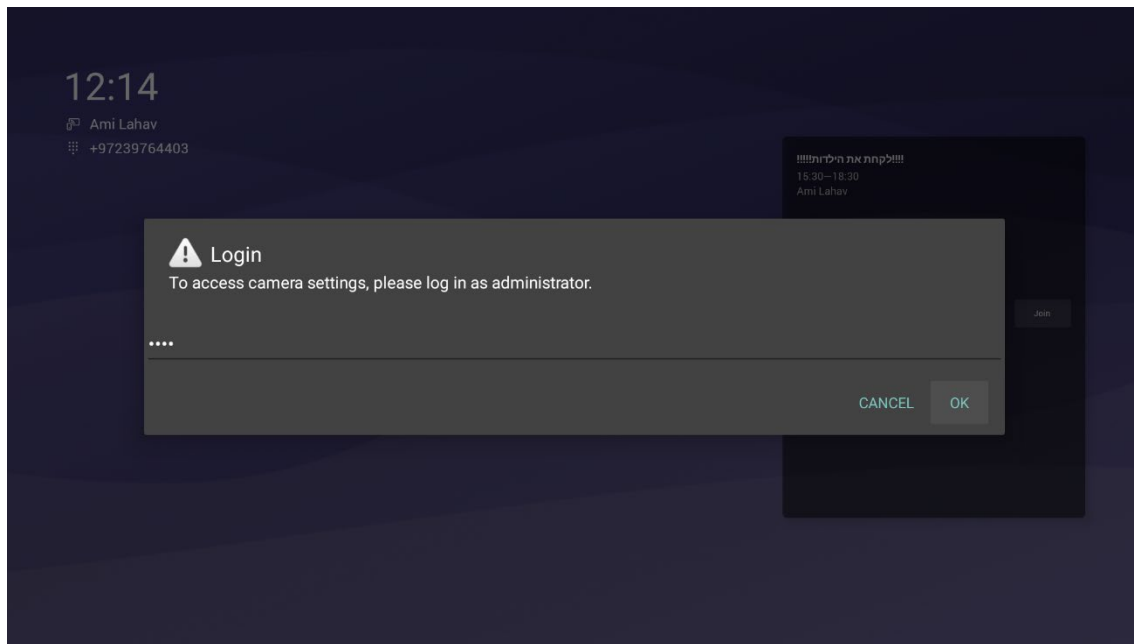
- On the remote controller, long-press the camera icon .

Figure 3-2: Camera Settings



- When the RXV80 is in *idle state* (i.e. *not* during a call / meeting), permissions are required to *preset* the camera. 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 3-3: Login when the RXV80 is in *idle state***Note:**

- During a call, all users can change **Camera settings**. When the call ends, the RXV80 reverts to its preconfigured presets.
- The option to access **Camera settings** from the RXV80's **Device Settings** still exists; administrator permissions will be required in this case as well.

- **Camera settings** allow administrators to save 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. For example, if a preset is configured to zoom in and focus on the whiteboard in a room, users in a video call/meeting will be able to switch to the relevant preset, focus on the whiteboard, 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

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

- Long-press the camera button to access **Camera settings**; all camera settings can be changed; at the end of the procedure, save the new preset; the **Camera settings** bar includes a **Save View** option as shown in the next figure.

Figure 3-4: Camera settings - Save View

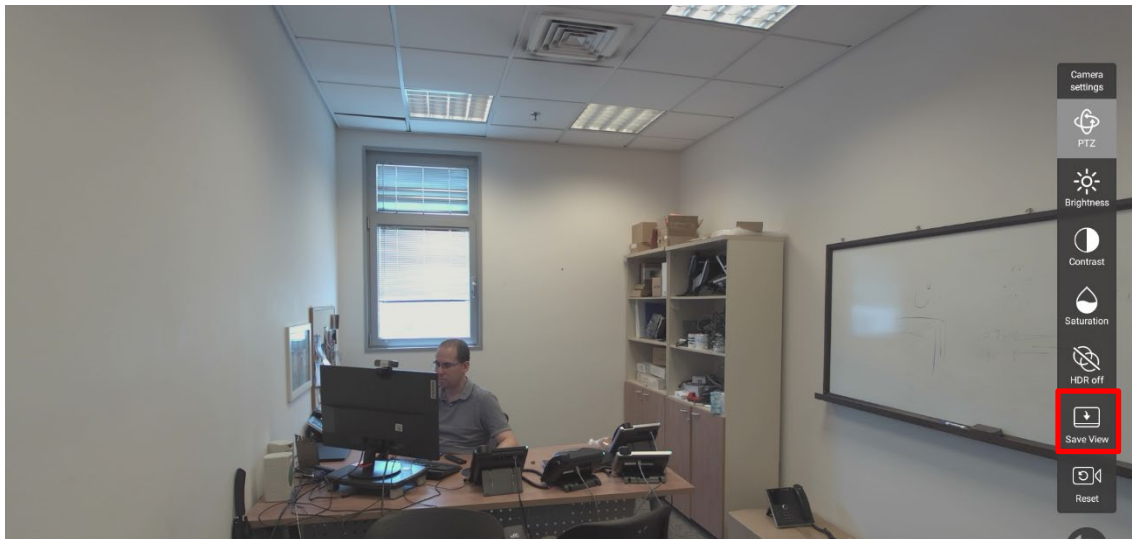
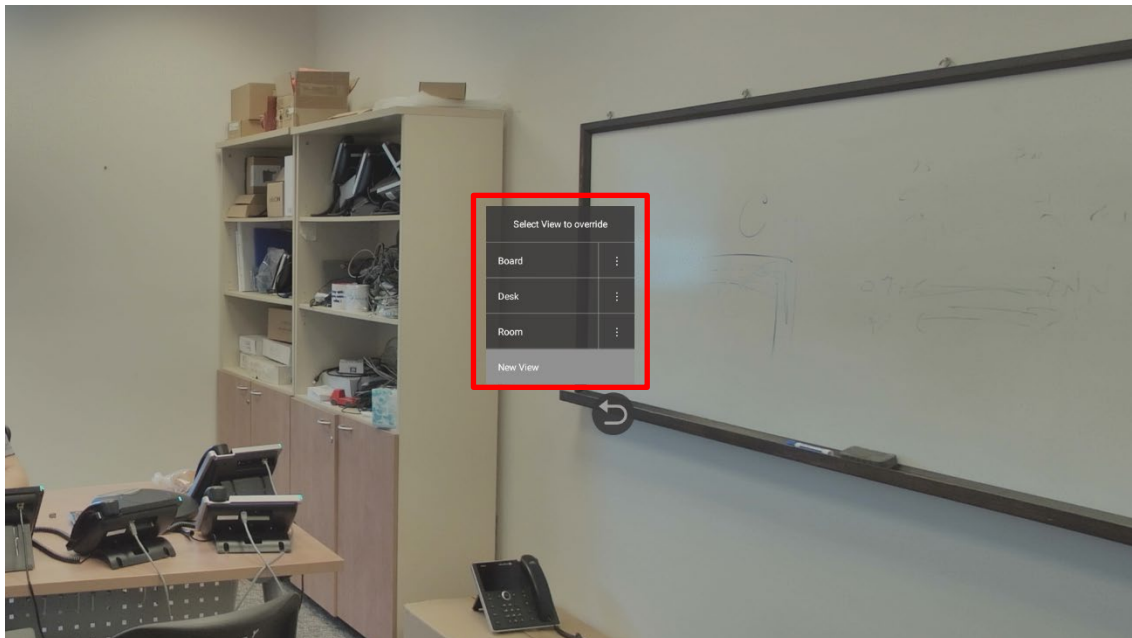


Figure 3-5: Camera settings - Save View



1. Navigate to and select **PTZ** to create and edit presets using PTZ control. You can create and edit up to three presets and assign specific pan, tilt, and zoom settings for each one.
2. Navigate to and select **Brightness** and then adjust the brightness using the -/+ buttons or the sliding scale.
3. Navigate to and select **Contrast** and then adjust the contrast using the -/+ buttons or the sliding scale.
4. Navigate to and select **Saturation** (perceived color relating to chromatic intensity) and then adjust it using the -/+ buttons or the sliding scale.
5. Navigate to and select **HDR on** or **off**. High Dynamic Range allows dynamic metadata to be added on a frame-by-frame basis so viewers will always receive the intended image. HDR is adapted to the specific abilities of your monitor, allowing for an improved image.
6. Navigate to and select **Reset** for the camera settings to return to their defaults.

3.2 Starting a New Meeting



Note: You can navigate and select in the RXV80 using the:

- Remote controller -OR-
- Touch screen

➤ **To start a new meeting:**

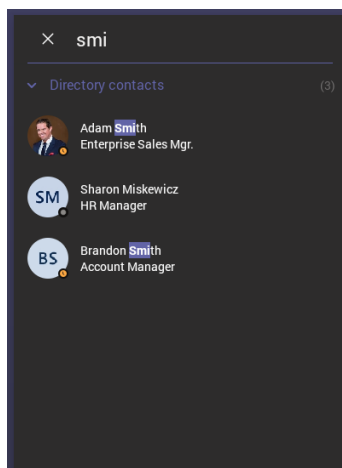
1. In the home screen shown in the preceding figure, navigate to and select the **Meet Now** option.

Figure 3-6: New meeting – Invite someone



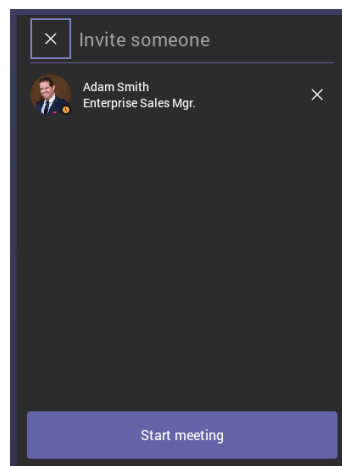
2. In the 'Invite someone' field, enter the name of a person to invite; after entering the first letters in the name, matching contacts from directory are displayed.

Figure 3-7: New meeting – Enter the name of a person



3. Select the name of the person to invite.

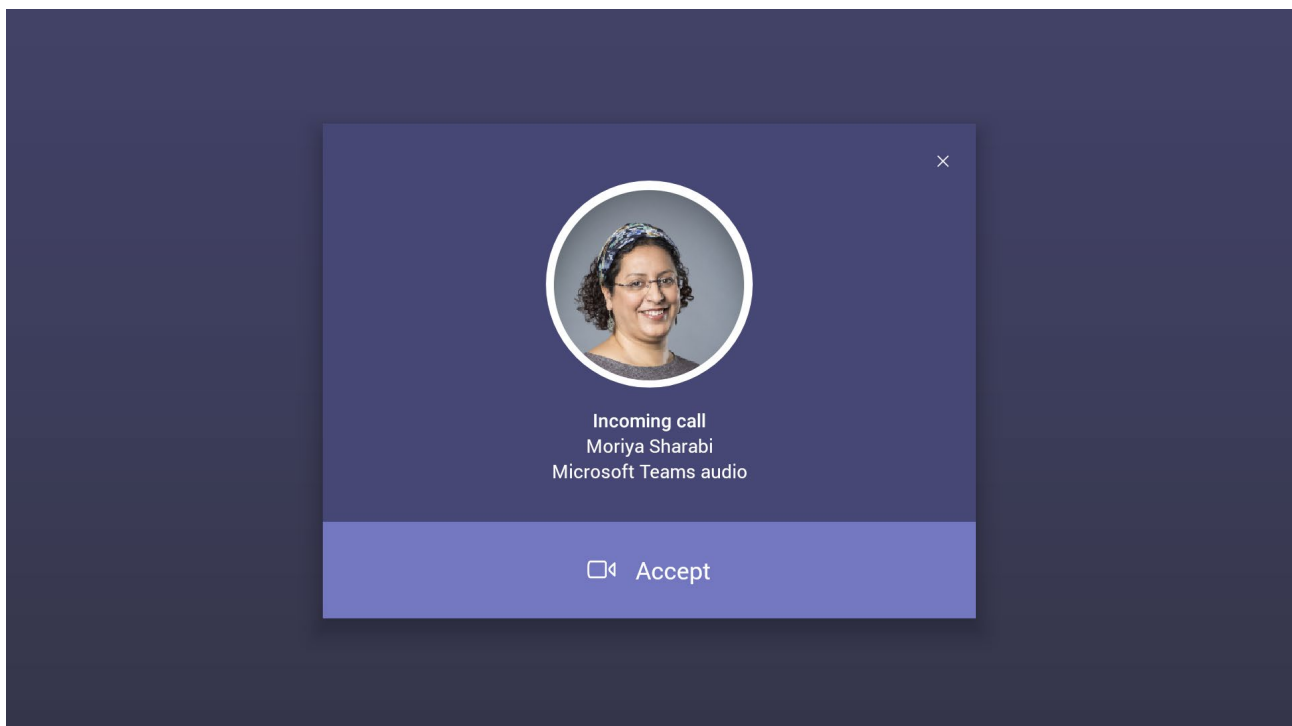
Figure 3-8: New meeting – Select the name of a person



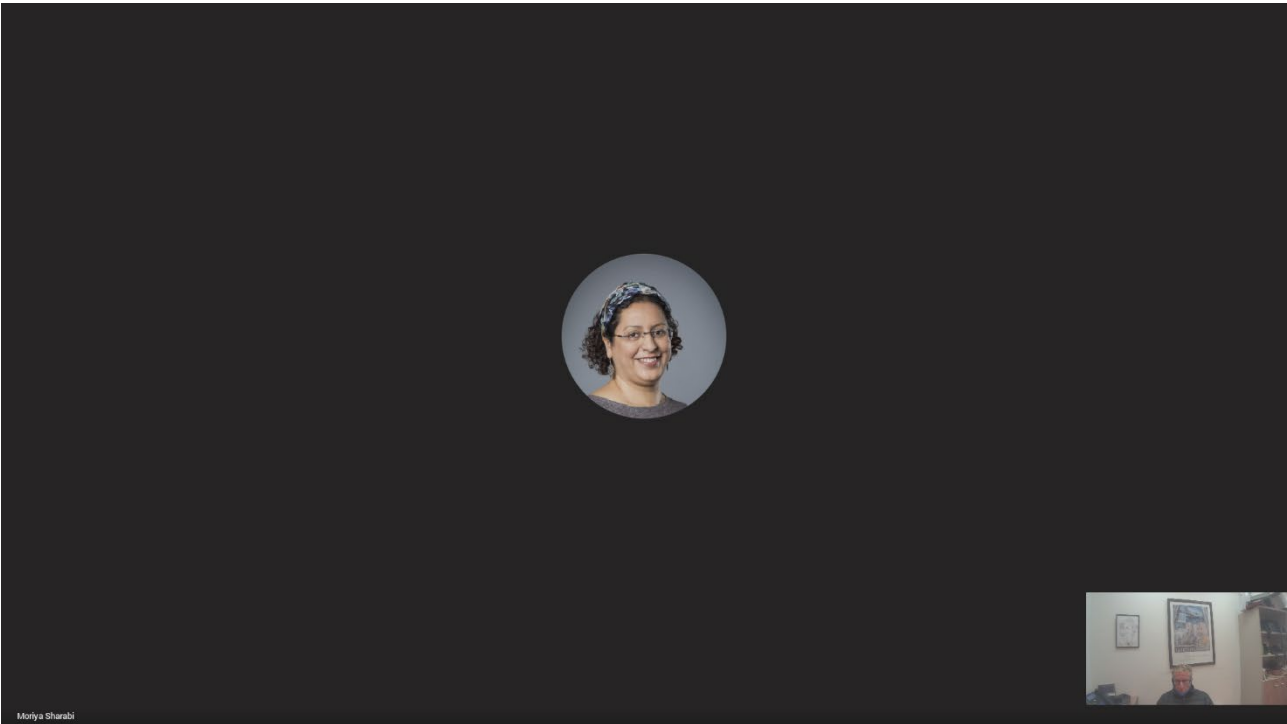
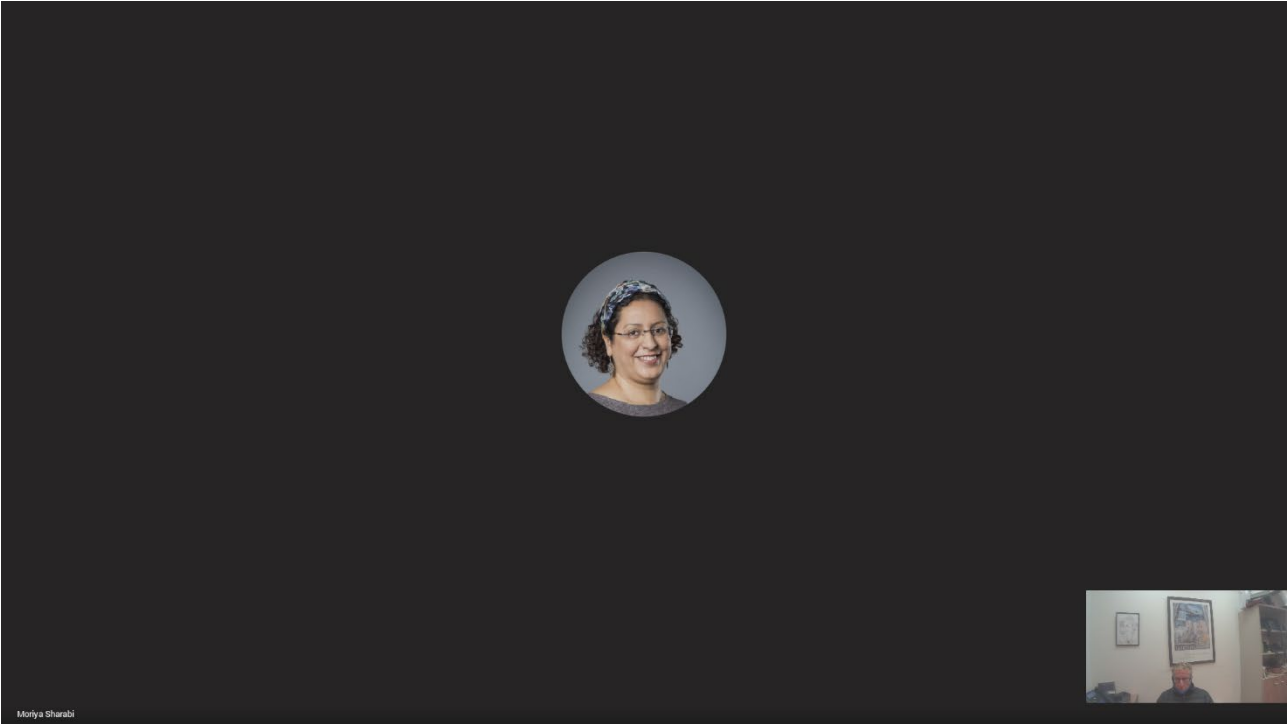
4. Invite someone else – or others – and then select **Start meeting**.



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.



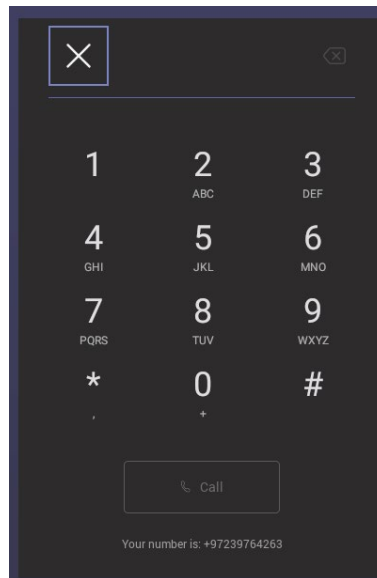
3.3 Dialing a Number

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 3-9: Dial pad



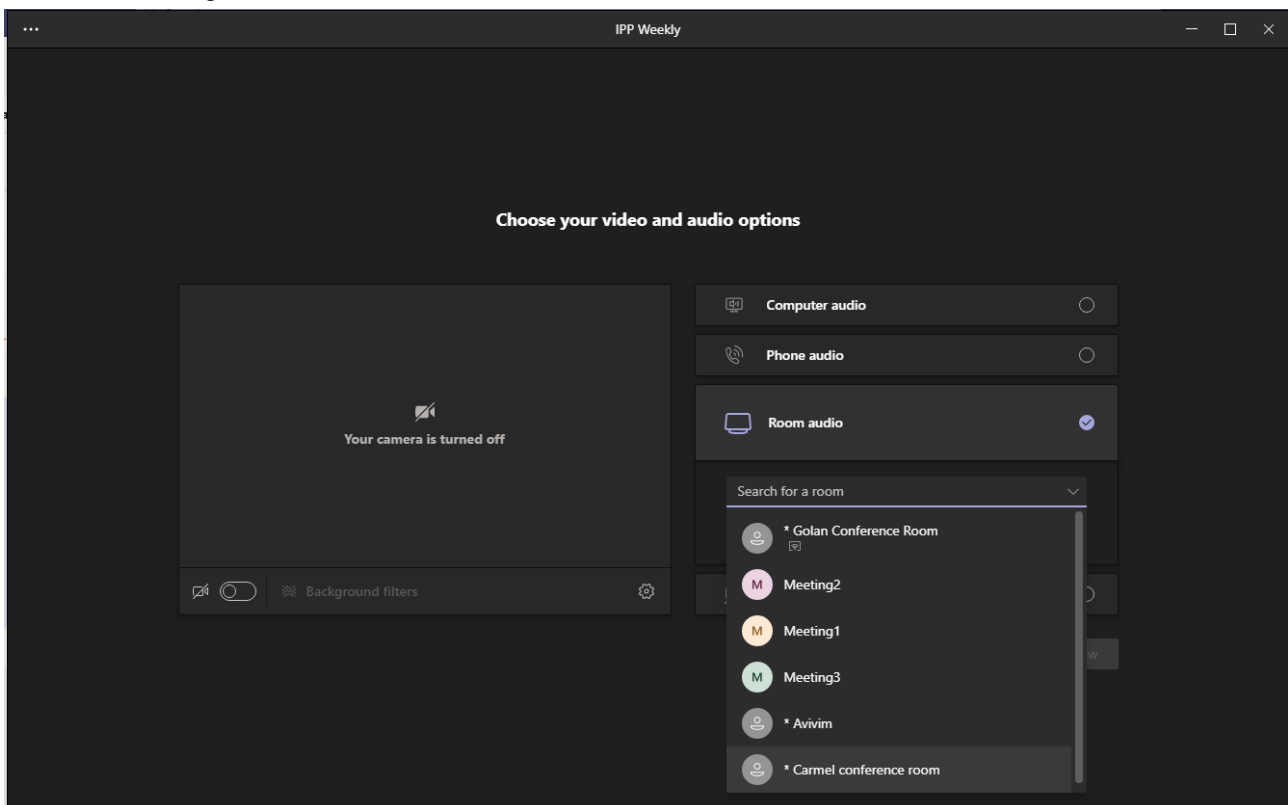
2. Enter the digits of the destination to call and select **Call**.

3.4 Enabling Proximity Join

'Proximity Join' allows you to discover and add a nearby, available Microsoft Teams Room, i.e., the RXV80, 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 meeting room device as mentioned is the RXV80. If you bring a laptop or a Teams Mobile Client near the RXV80, the Teams Mobile Client will offer the RXV80 as the room audio device.

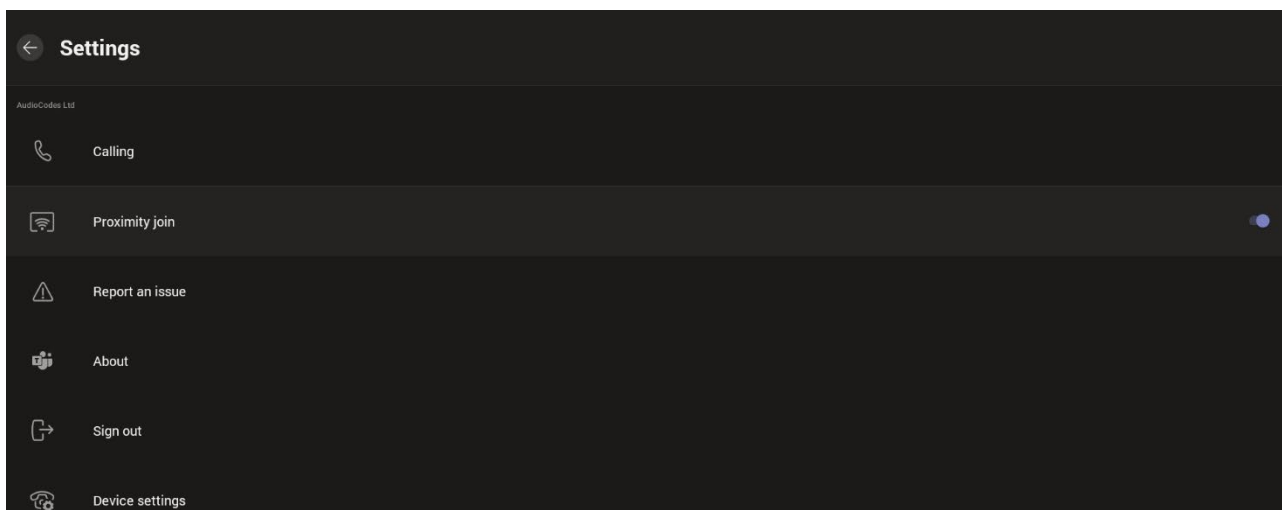
The figure below shows how to select the room audio device.



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 (RXV80) gets a request to join the meeting.

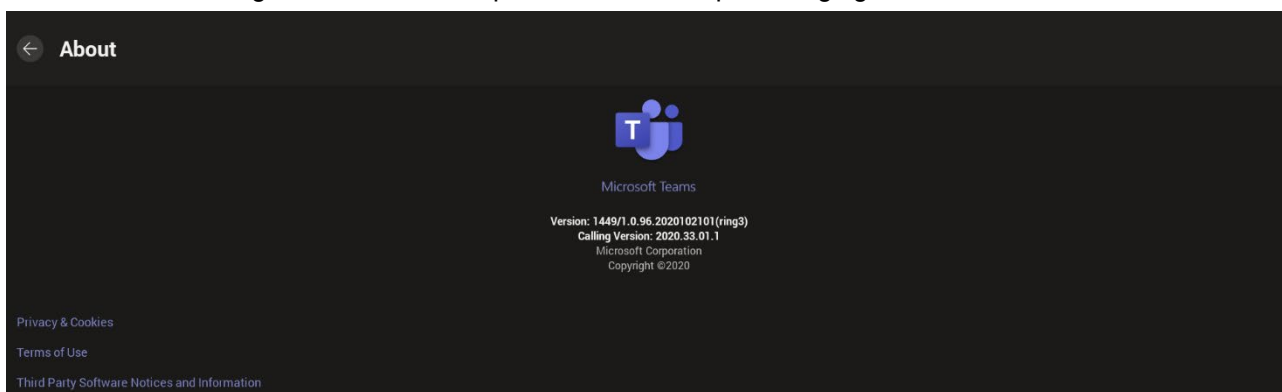
➤ **To enable 'Proximity join':**

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



3.5 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.



3.6 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.



4 Configuring Device Settings

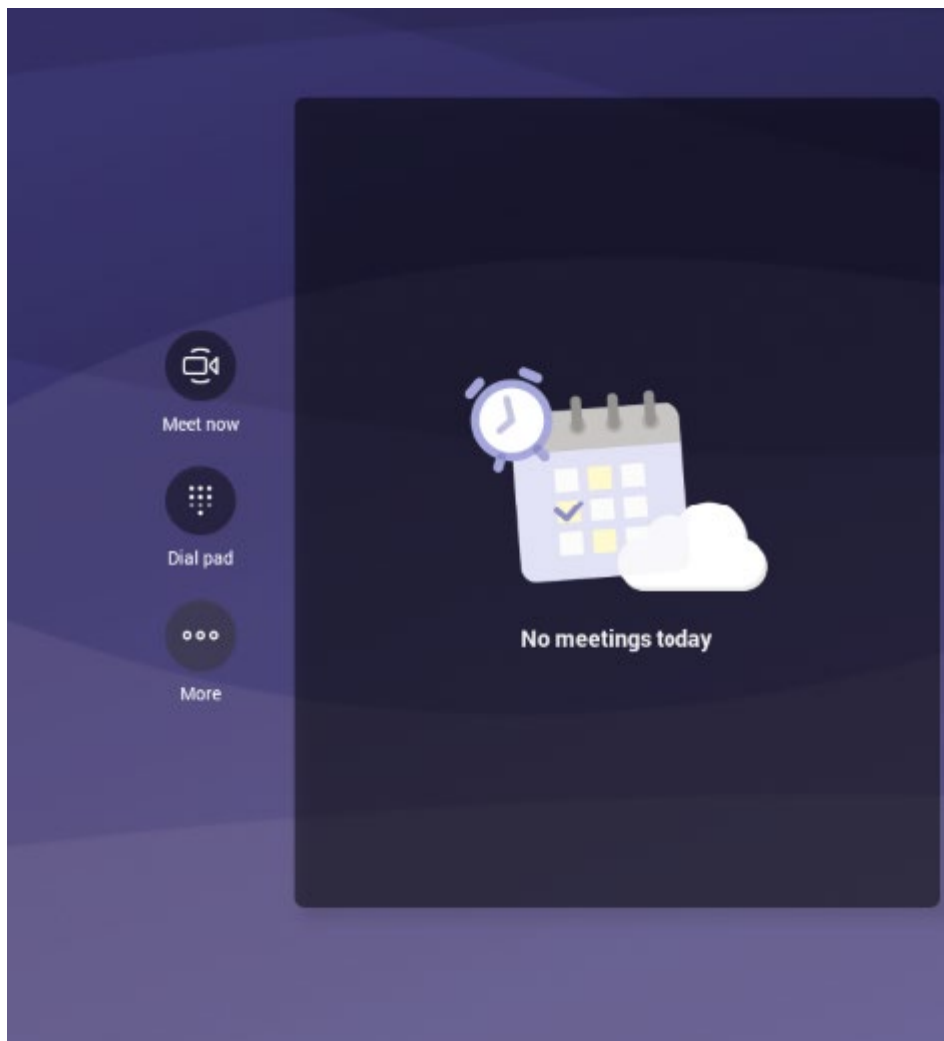
The section familiarizes you with the RSV80's settings. RSV80s are delivered to customers configured with their default settings. Customers can customize these settings to suit specific enterprise requirements.



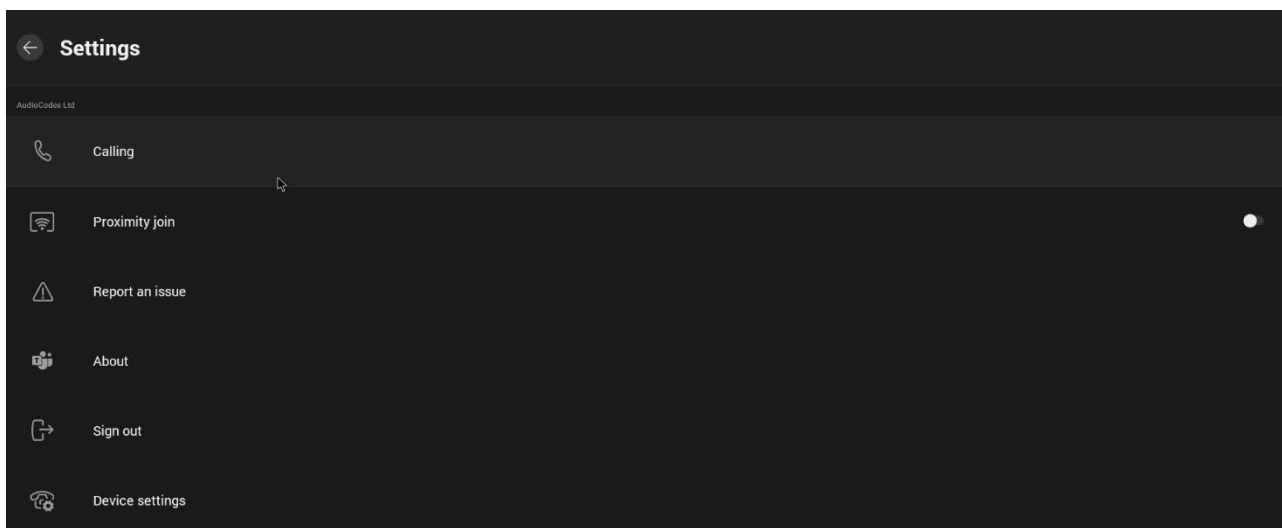
Note: Navigate and select options using the remote controller or touch screen.

➤ **To access device settings:**

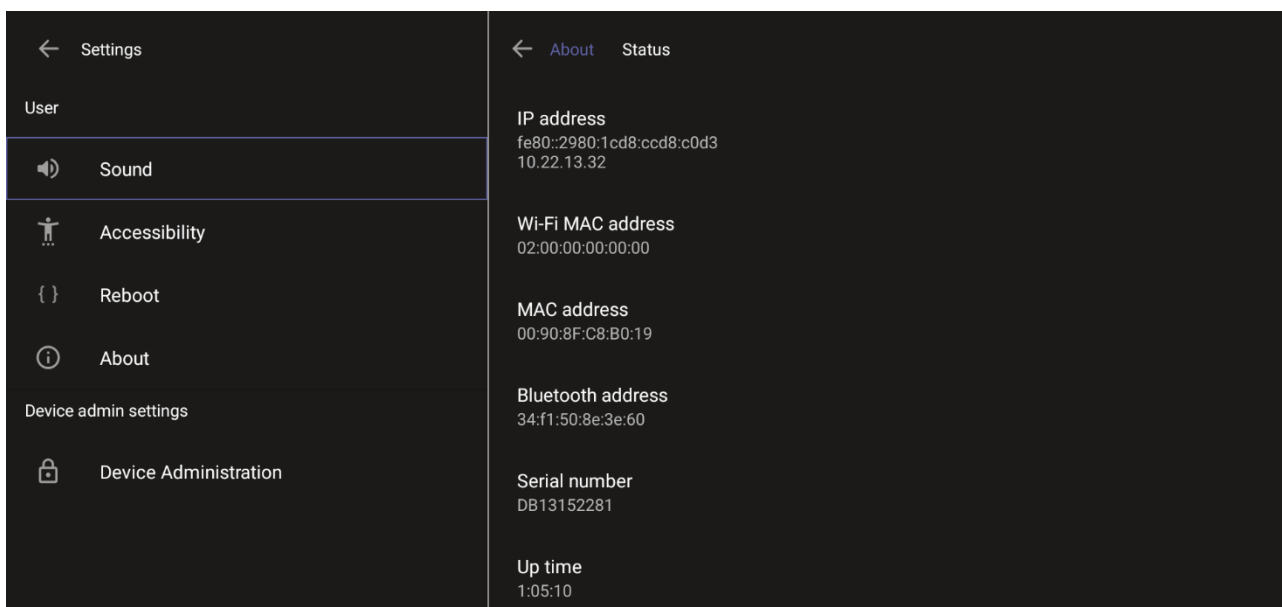
1. In the home screen, navigate to and select the **More** option



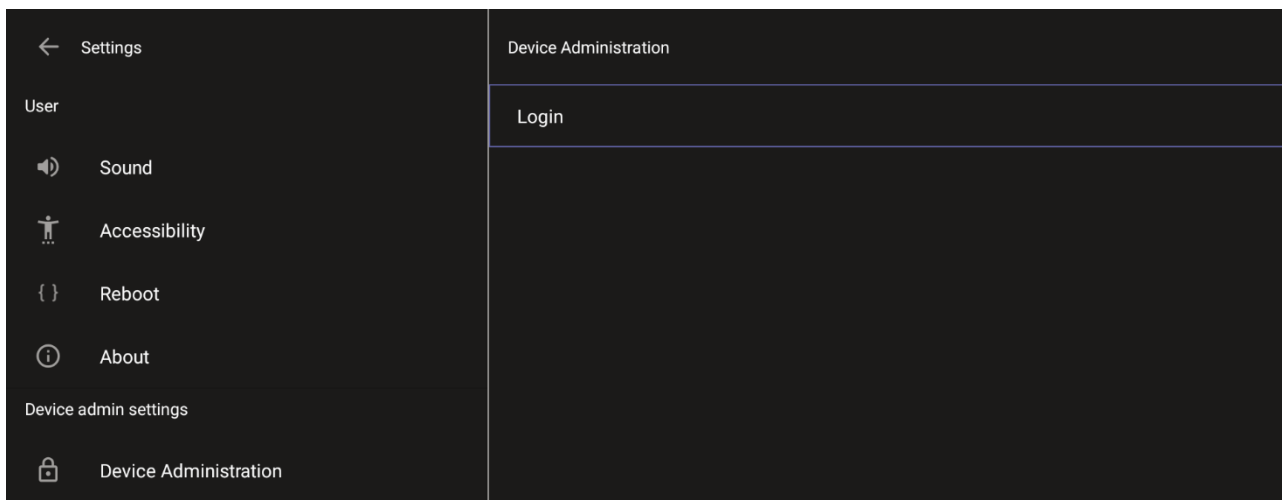
2. Navigate to and select **Settings**.



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 some debugging options. It is password protected. Default password: **1234**. After logging in as an Administrator, you can log out | change password.

6. Select **Login**.

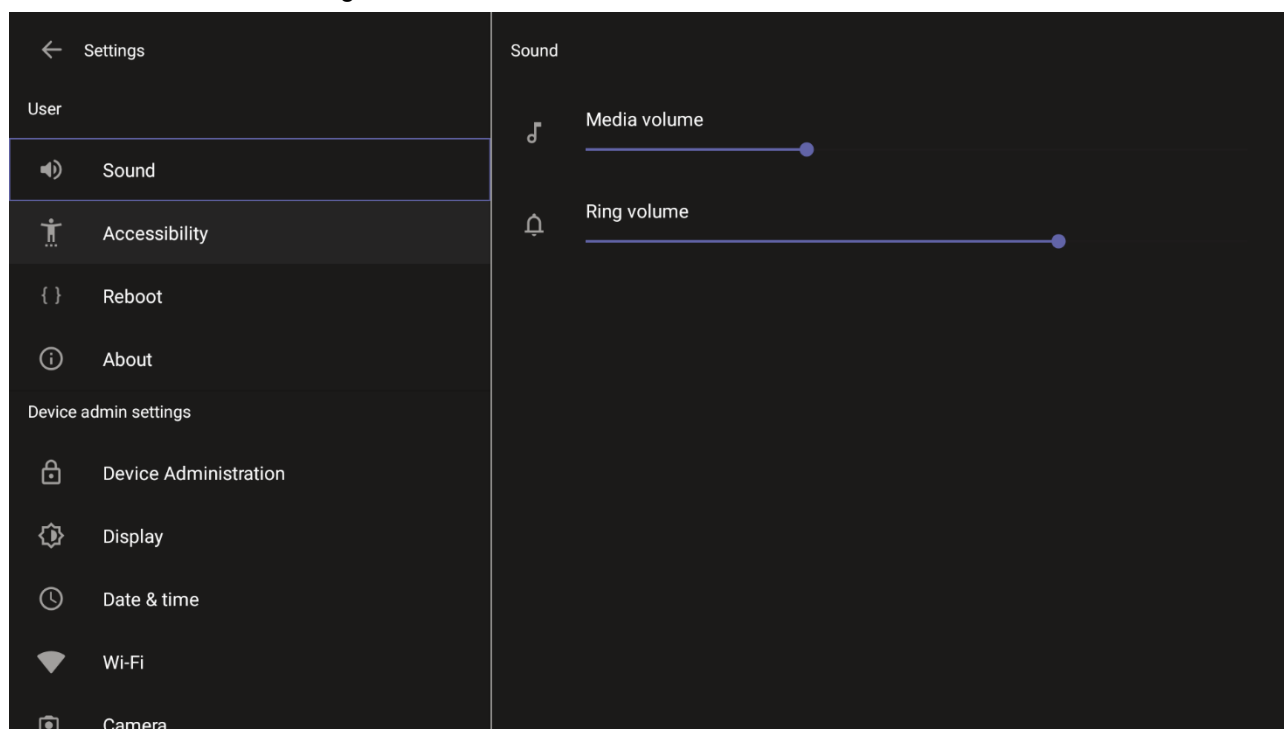
7. Enter the password in the 'Enter password' field; use the virtual keyboard to enter the password (**1234**). Note that the virtual keyboard pops up for all 'Settings' fields to allow inputting characters and / or numbers. Two virtual keyboard types can be displayed: Numeric or QWERTY.



Note: These virtual keyboards are also displayed when network administrators need 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'.

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



4.1 Configuring Device Admin Settings

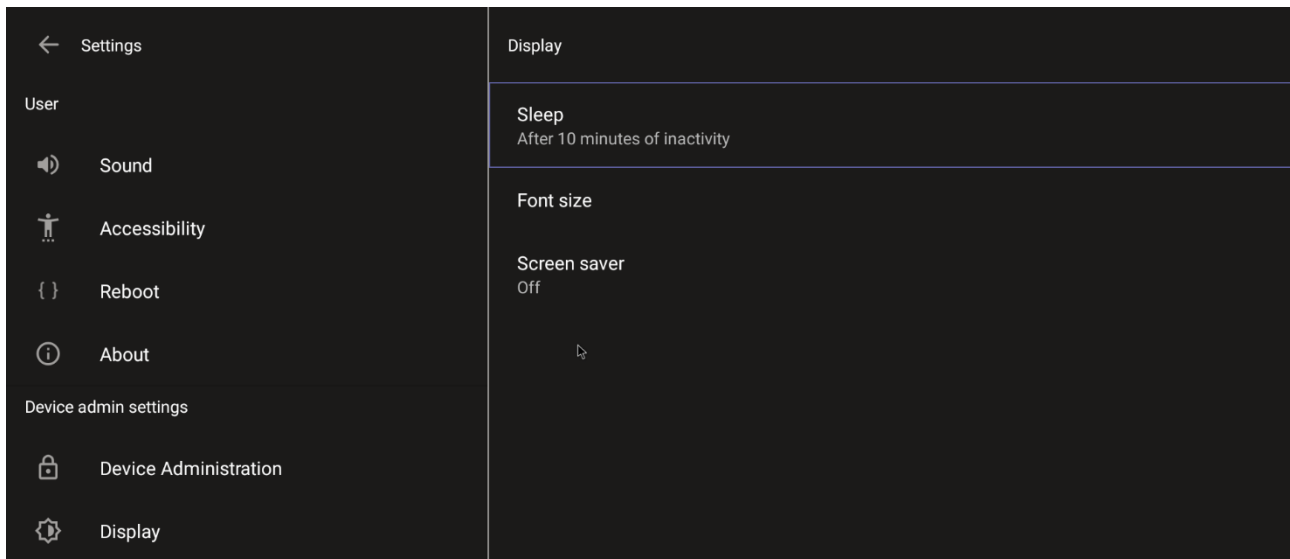
After logging in as Device Administration as shown in the previous section, you can configure Device Administration settings: Display, Date & Time, Wi-Fi, Camera.

4.1.1 Display Settings

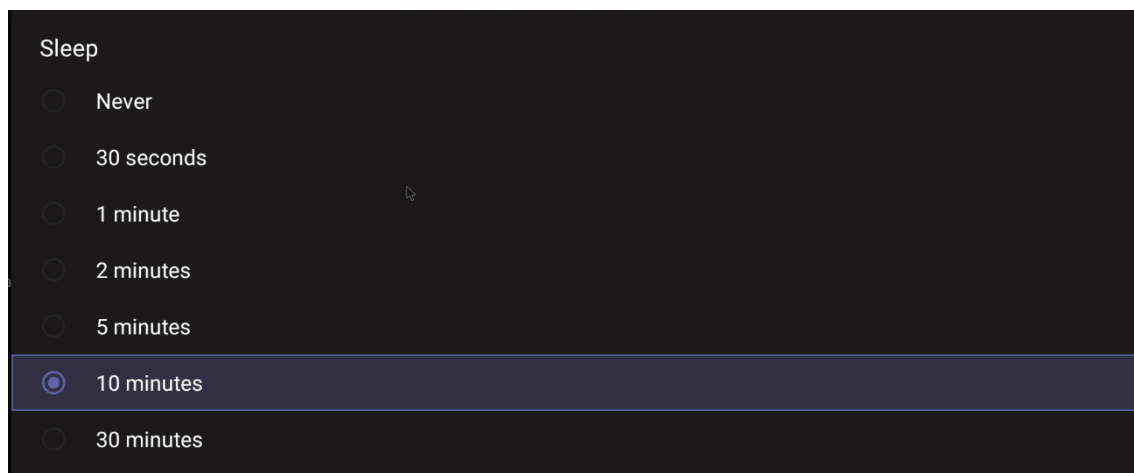
Modify these settings to suit your preferences related to the look and feel of the user interface.

➤ **To configure Display settings:**

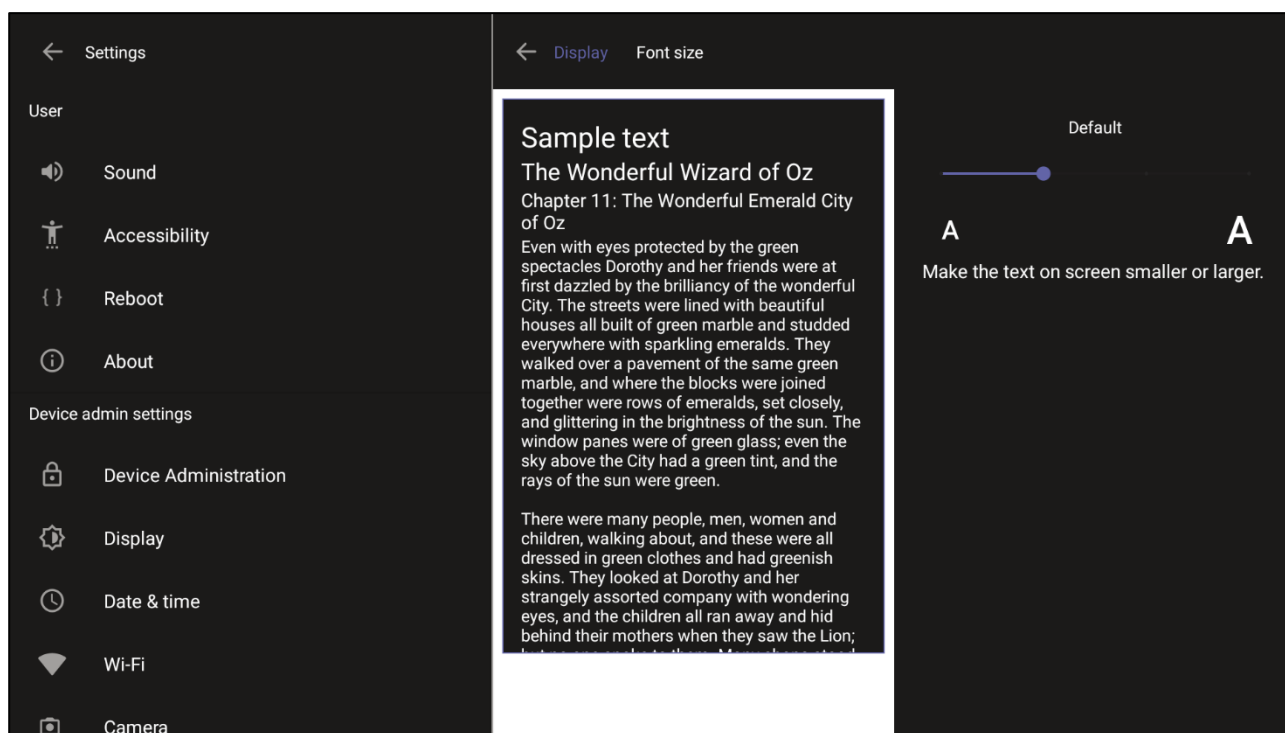
1. Under 'Device admin settings', navigate to and select **Display**.



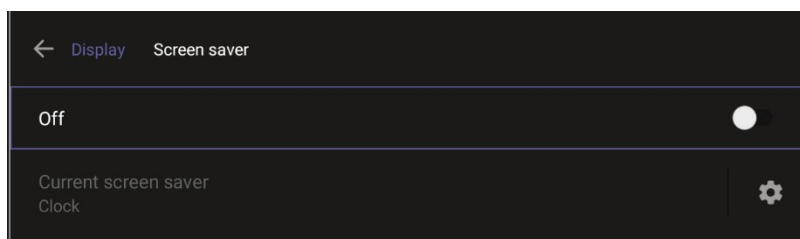
2. Under 'Display', navigate to and select **Sleep**.



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**.



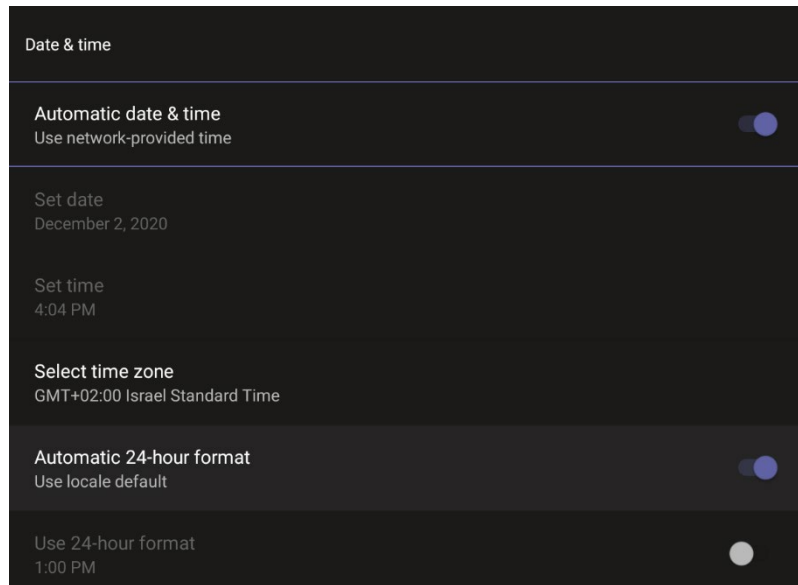
6. Navigate to and select **Off** to switch it on and then choose the screen saver.

4.1.2 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].

4.1.3 Wi-Fi Settings

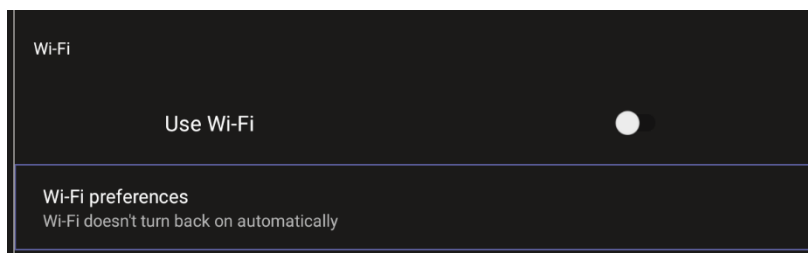
The RXV80 can connect to an Access Point via Wi-Fi.



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

➤ **To configure Wi-Fi settings:**

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



2. Navigate to and select **Use Wi-Fi**.

4.1.3.1 Configuring Wi-Fi

Network administrators can configure Wi-Fi parameters for the phone. The parameters are concealed from the user's view. Use the following table as reference.

Table 4-1: Wi-Fi Parameters

Parameter	Description
network/wifi_enabled	Enables/disables the Wi-Fi feature.
network/wifi_pc_bridge	Enables network connectivity for the PC behind the phone; for debugging purposes.
network/wifi_ipv4_method	Defines the Dynamic or Static IP address for Wi-Fi.
network/wifi_channel_mode	Enables the Wi-Fi channel mode: <ul style="list-style-type: none"> ▪ 2.4G only ▪ 5G only ▪ 2.4G+5G

The following table shows the parameters per index. The phone can currently store 16 connected SSIDs.

Table 4-2: Wi-Fi Parameters per Index

Parameter	Description
network/wifi/[0-15]/ssid	Saves the Access Point's SSID.
network/wifi/[0- 15]/password	Saves the password for some authentication methods which need it, e.g., WPA2PERSONAL, WPA2PERSONAL
network/wifi/[0- 15]/security	Saves the Access Point's authentication method: • WPA2PERSONAL • WPA2PERSONAL • WPA2ENTERPRISE • WPA2ENTERPRISE
network/wifi/[0- 15]/auto_reconnect	Configure this parameter to reconnect this SSID automatically.
network/wifi/[0- 15]/identity	Saves the identity for some authentication methods that need

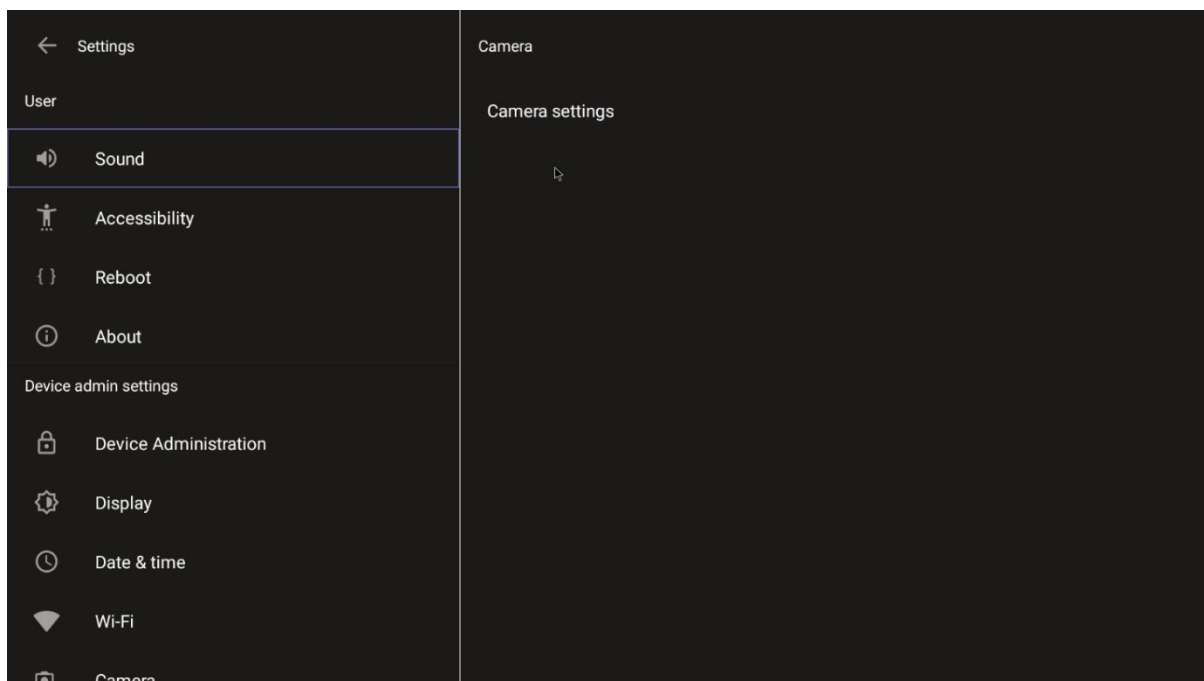
Parameter	Description
	it, e.g., WPAPERSONAL, WPA2PERSONAL
network/wifi/[0- 15]/anonymous_ identity	Saves the anonymous identity for some authentication methods that need it, e.g., WPAENTERPRISE, WPA2ENTERPRISE, etc.
network/wifi/[0- 15]/phase2_ authentication	Phase 2 authentication for WPAENTERPRISE, WPA2ENTERPRISE. The phone supports PAP, MSCHAP, MSCHAPV2, CHAP, MD5, GTC
network/wifi/[0-15]/pin_ code	Defines the PIN code for the WPS PIN code authentication method.
network/wifi/[0- 15]/wps_ method	Defines the WPS method. The phone supports PIN and push button.
network/wifi/[0- 15]/client_ cert	Defines the certificate path for WPAENTERPRISE, WPA2ENTERPRISE certificate authentication.
network/wifi/[0- 15]/private_ key	Defines the private key path for WPAENTERPRISE, WPA2ENTERPRISE certificate authentication.

4.1.4 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:

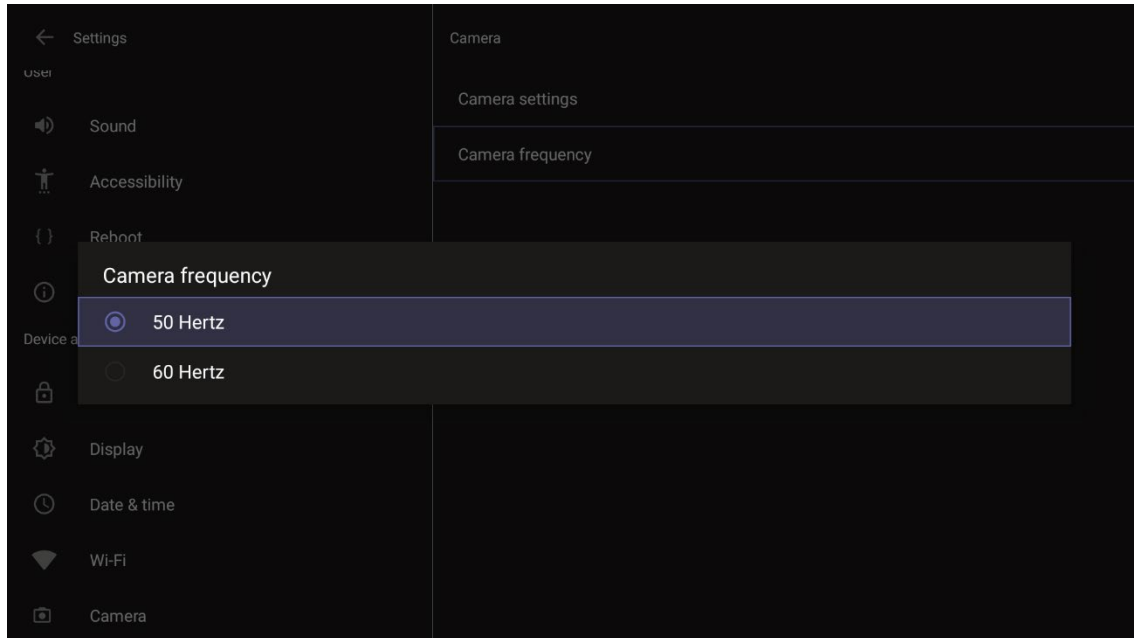


3. Create and edit presets using PTZ control. For more information, see [here](#).
4. Adjust the camera for lighting conditions. For more information, see [here](#).

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 Bluetooth

Bluetooth is currently used for the remote controller and the 'Proximity Join' feature. Bluetooth speakers (selected types only) will be supported in the future.

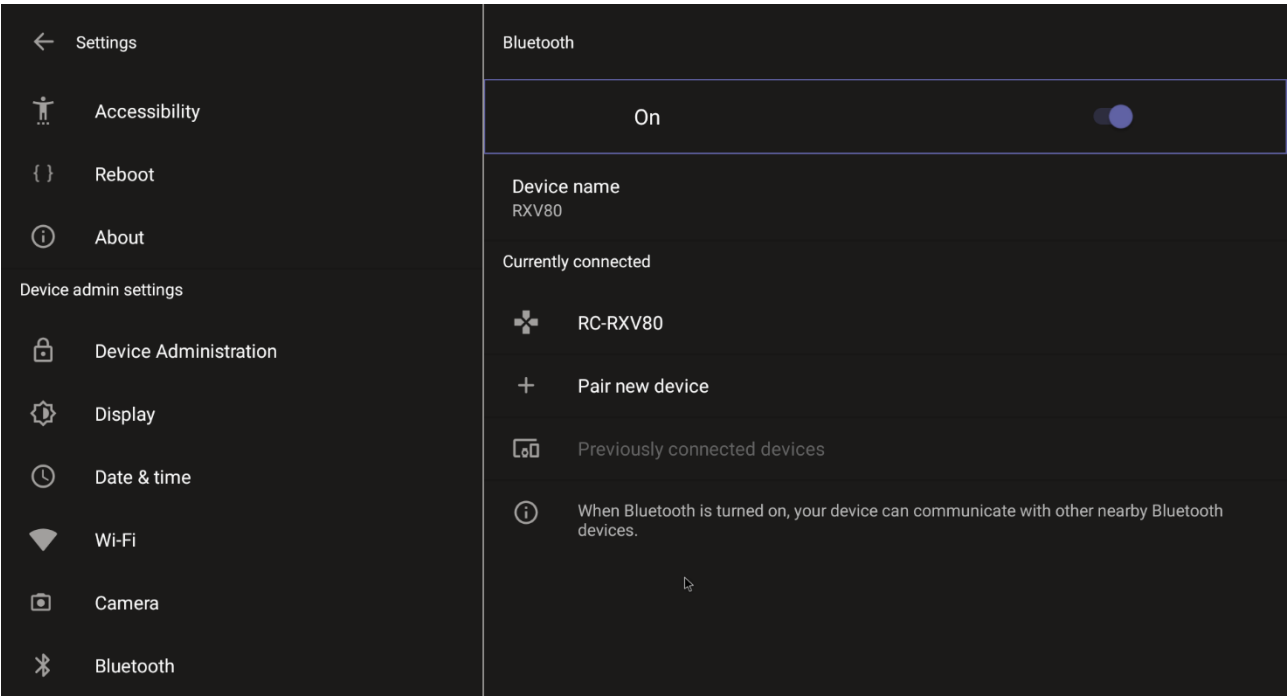


Note: The built-in Bluetooth capability can support only one Bluetooth feature at the time (the remote controller or the 'Proximity join' feature). To use both the remote controller and 'Proximity Join' in parallel, the Bluetooth dongle provided with RXV80 bundles must be used. The dongle fully supports 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 RXV80 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 *RXV80 Deployment Guide*.

➤ **To pair a new device:**

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



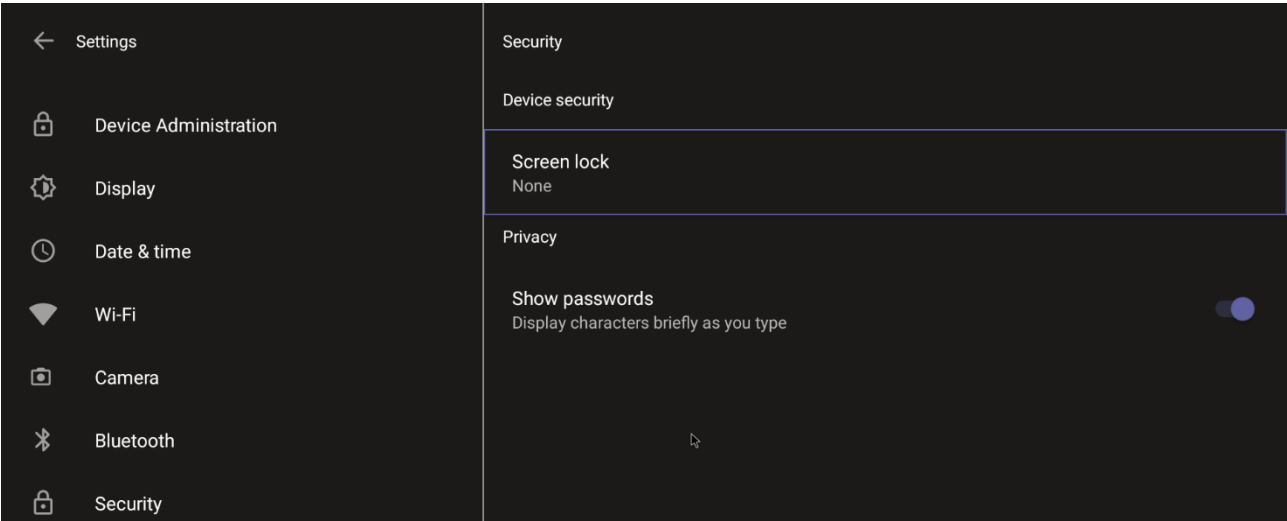
- 2. Navigate to and select **Pair new device**.

4.1.6 Security

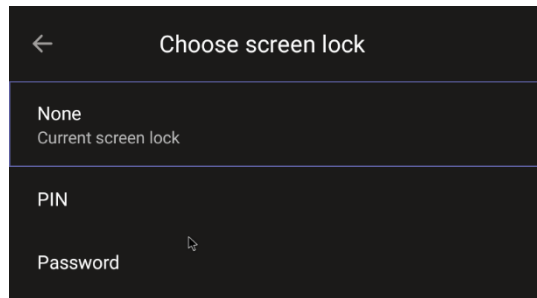
As a security precaution, the RXV80 can be locked and unlocked. The setting helps secure the device against breaches.

➤ To secure the device:

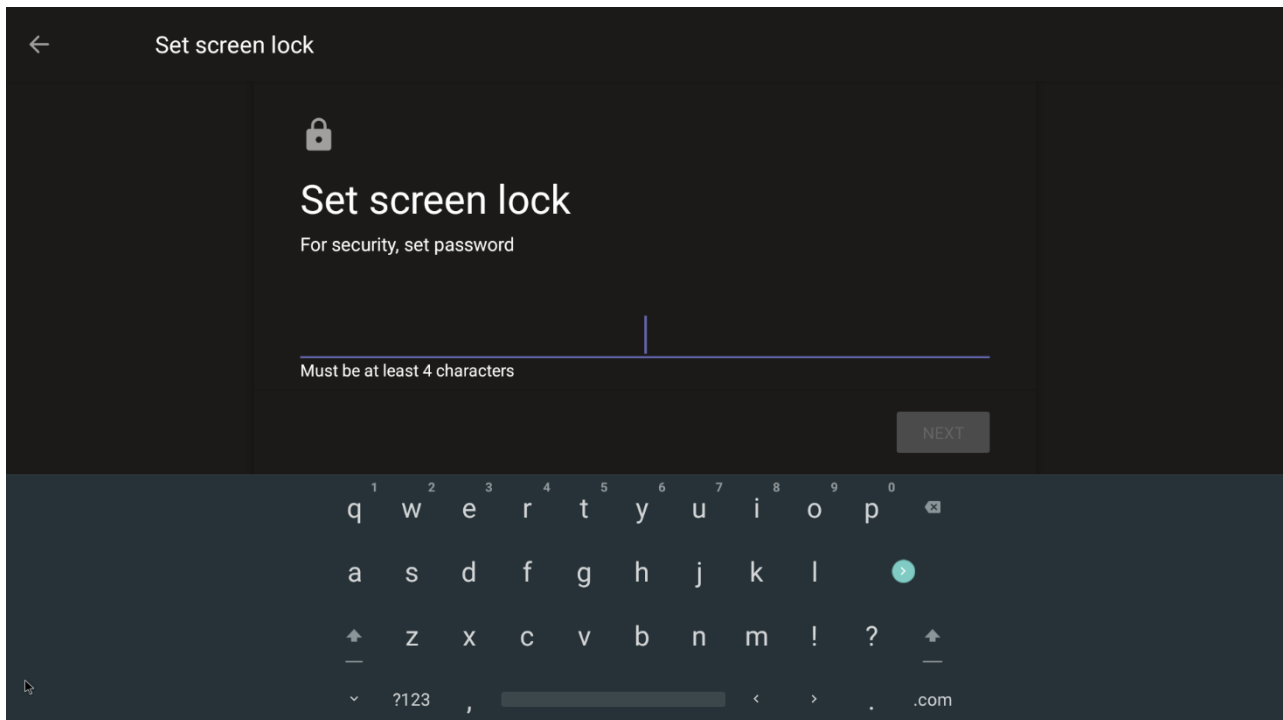
- 1. Under 'Device admin settings', navigate to and select **Security**.



- 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**.



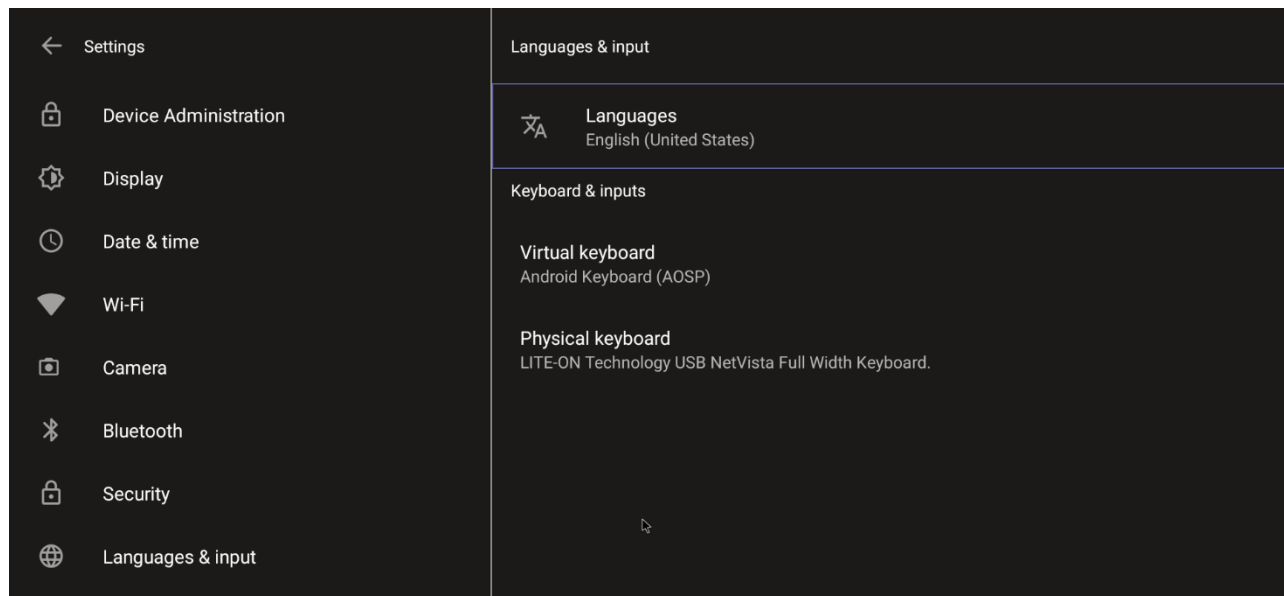
4. Enter a PIN, click **Next** and then navigate to and select **Password**; a screen like the preceding is displayed. Set the password (must also be at least four characters) and then again navigate to and select **Next**. You've successfully configured screen lock.

4.1.7 Languages & input

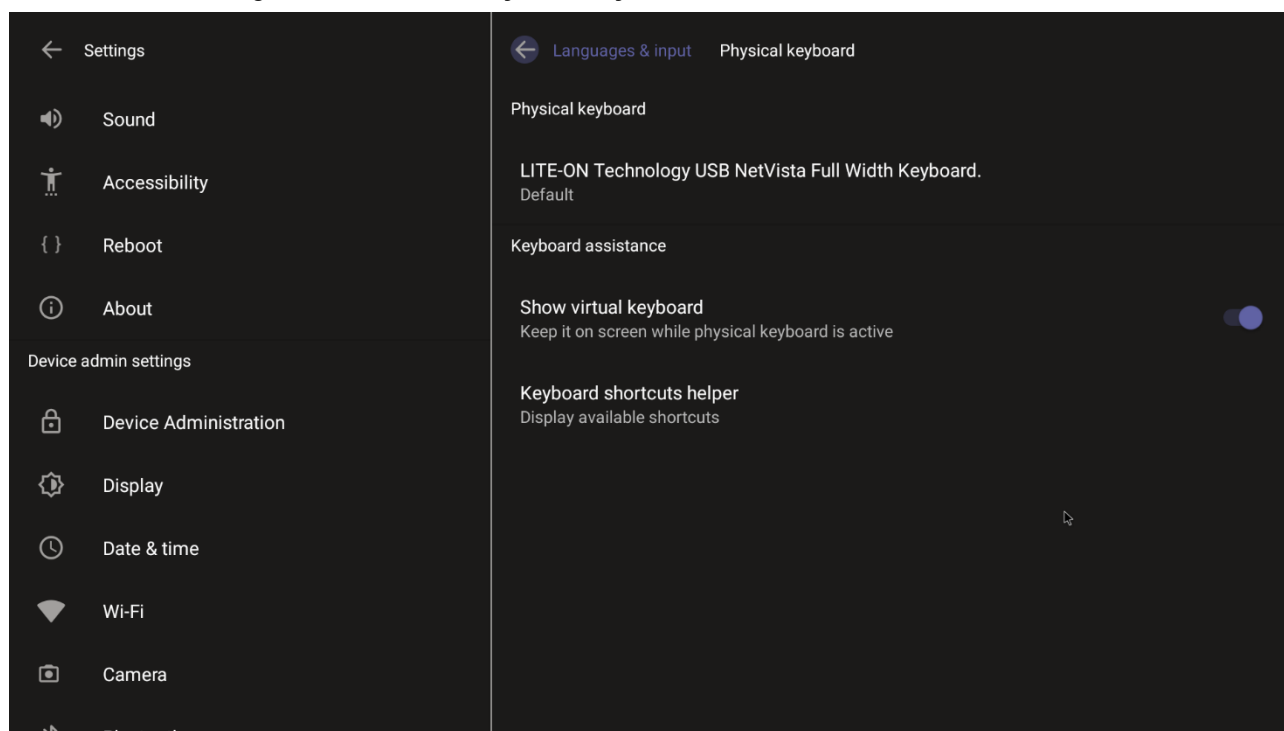
This setting allows users to customize inputting to suit personal requirements.

➤ **To set language and input:**

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



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



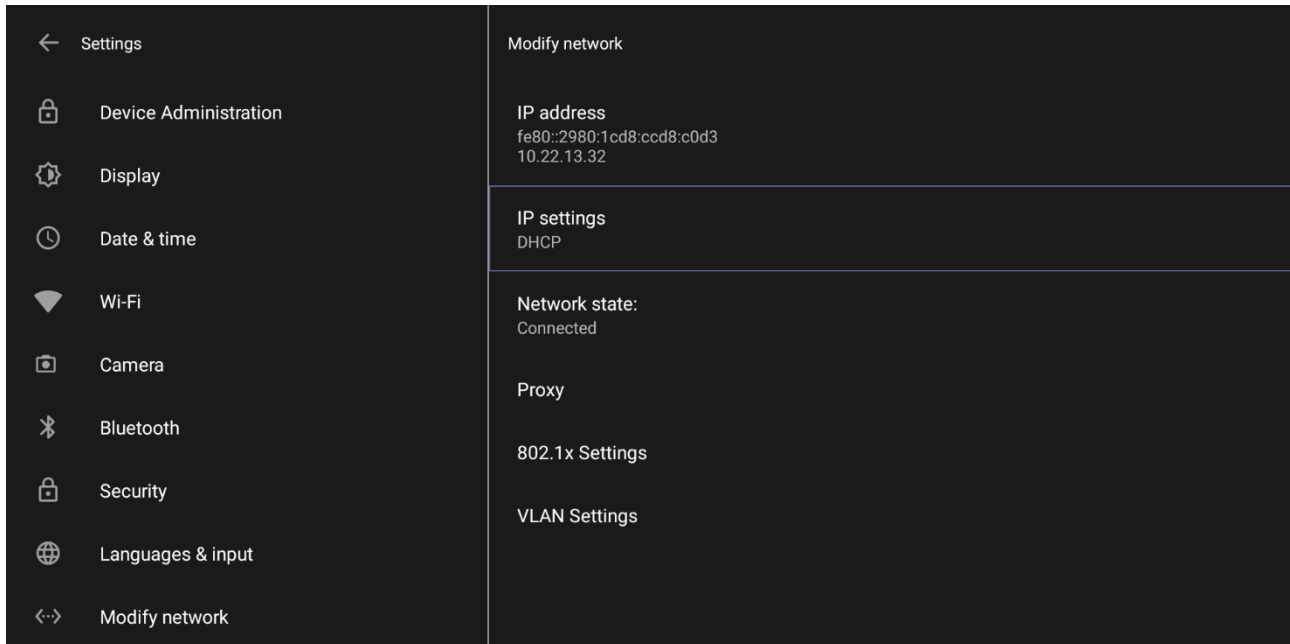
3. Navigate to and select **Show virtual keyboard**.

4.1.8 Modify network

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

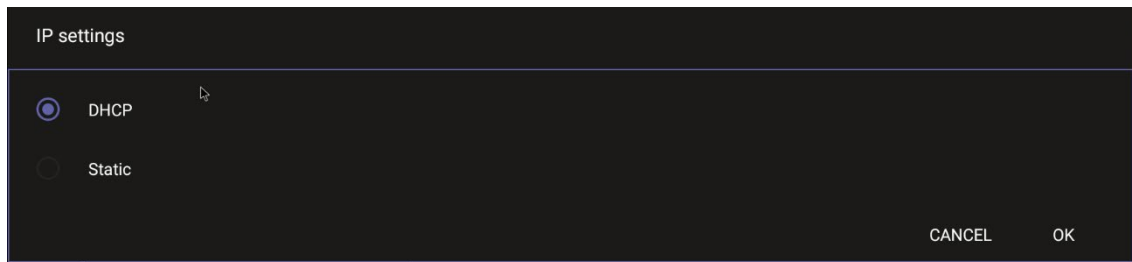
➤ **To modify network settings:**

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

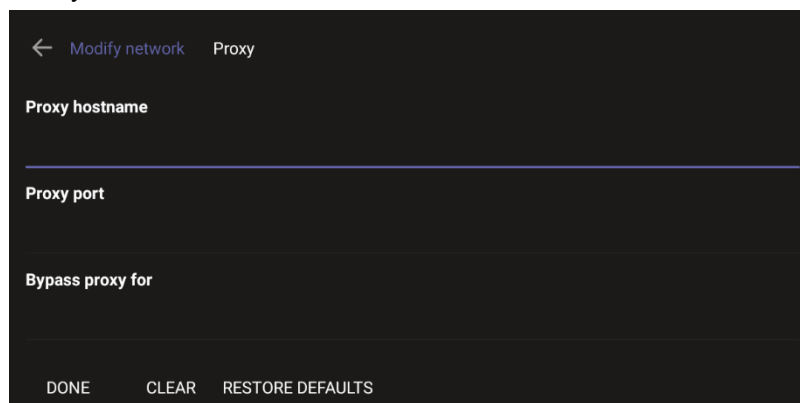


2. Navigate to and select:

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



- Network state [Read Only]
- Proxy



Allows you to configure the RSV80 with an HTTP proxy server. Configure the proxy host name and proxy port and then navigate to and select **Done**.

- 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

- ◆ 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.

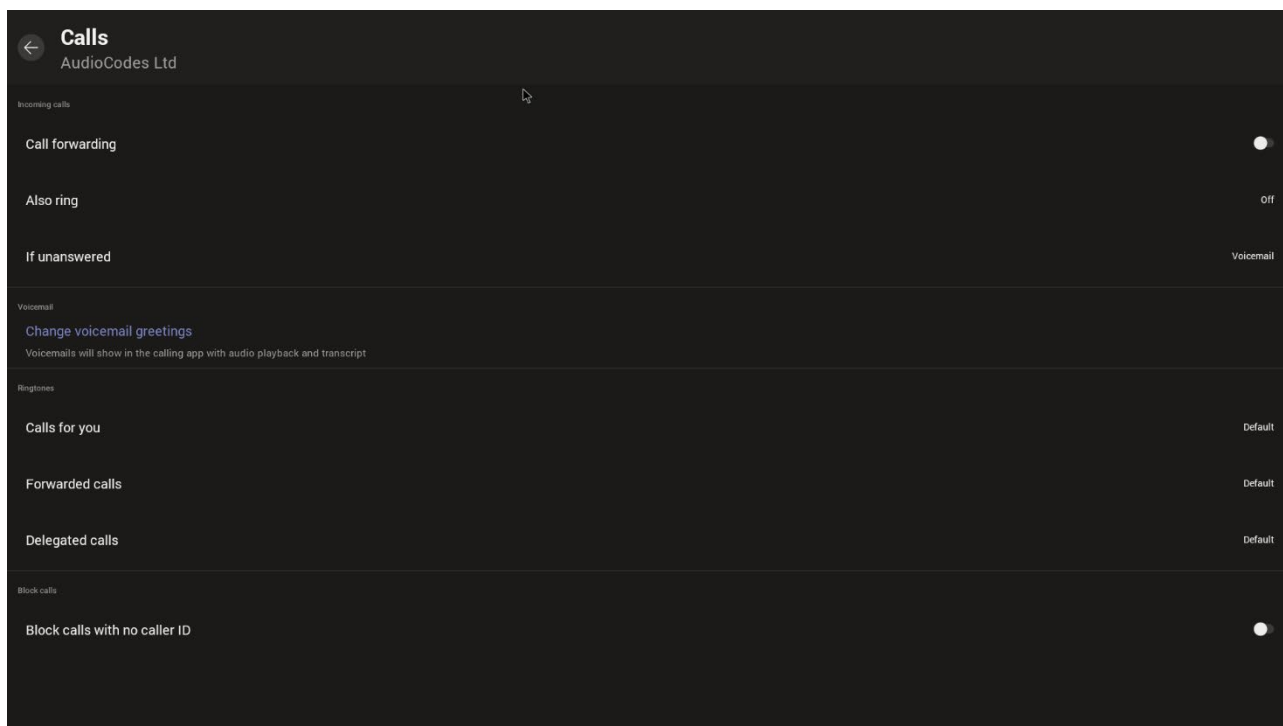
4.1.9 Calling

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**.



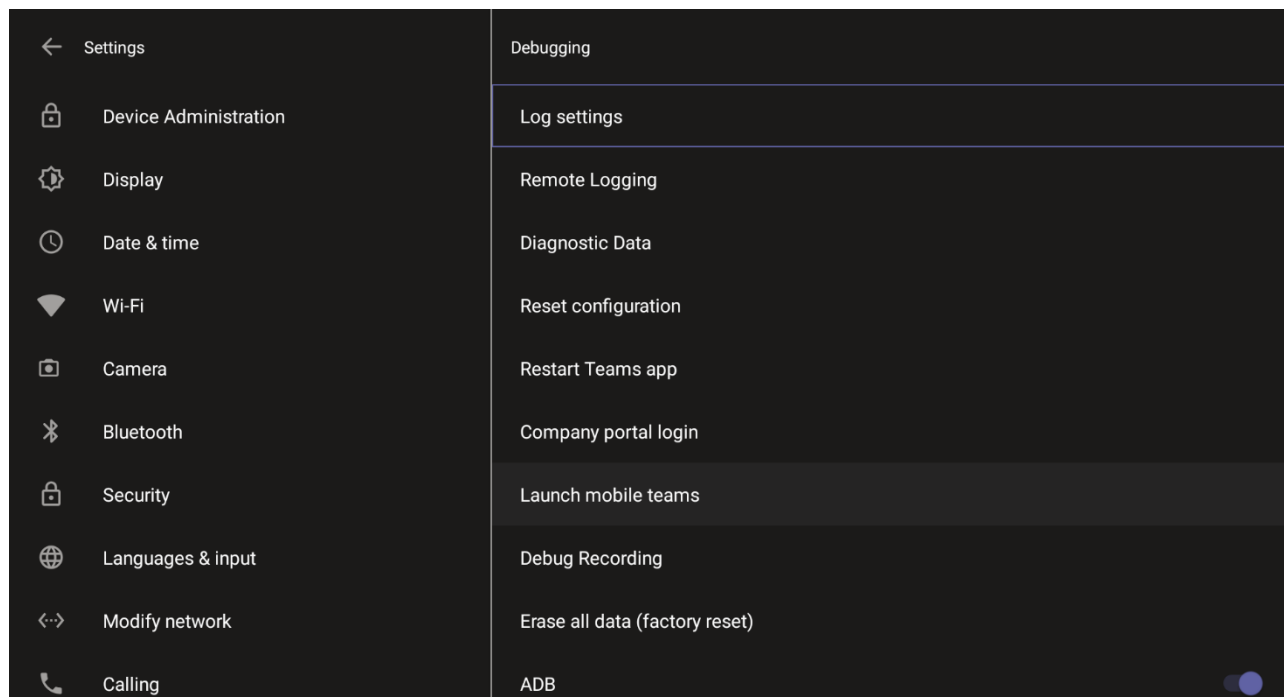
- In the Calls screen, navigate to and select:
 - ◆ **Call forwarding** to enable automatically redirecting incoming calls to another destination.
 - ◆ **Also ring** to configure other phones to ring on incoming calls; only displayed if **Call forwarding** is disabled.
 - ◆ **If unanswered** to configure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

4.1.10 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:

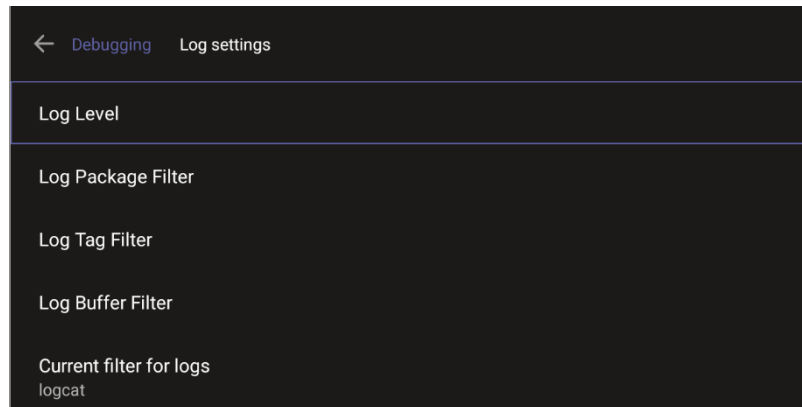
- Log settings (see [Log Settings](#))
- Remote Logging (see under [Remote Logging](#))
- Diagnostic Data (see under [Diagnostic Data](#))
- Reset configuration (see under [Reset configuration](#))
- Restart Teams app (see under [Restart Teams app](#))
- Company portal login (see under [Company Portal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

4.1.10.1 Log Settings | Collecting Logs

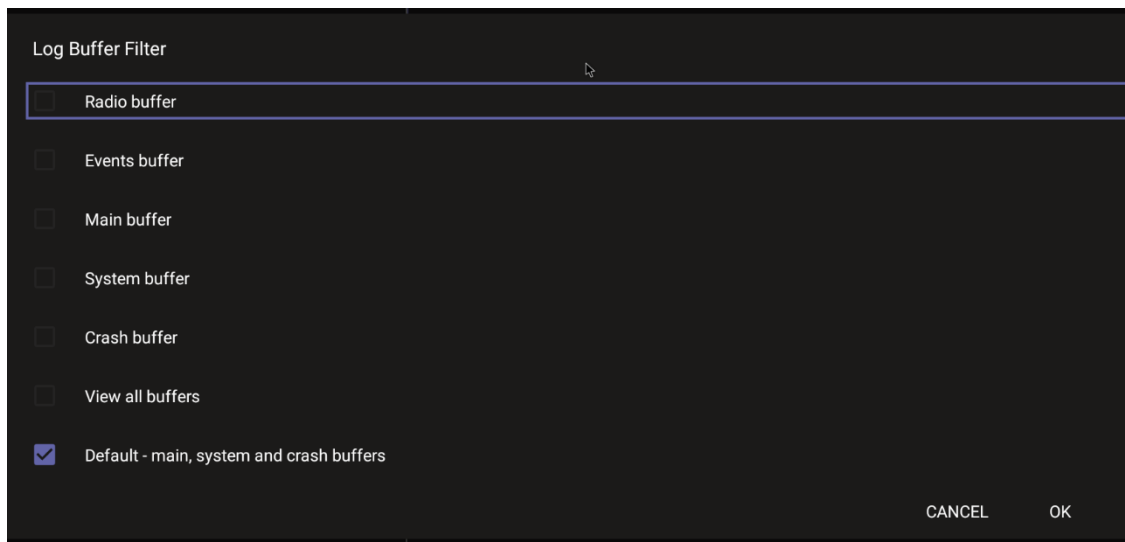
Device diagnostics (Logcat) can be collected using the Microsoft Admin Portal. For support purposes, general logs can be collected also using the Microsoft Admin Portal. The logs can help debug Teams application issues and also for issues related to the device.

➤ **To configure log settings:**

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



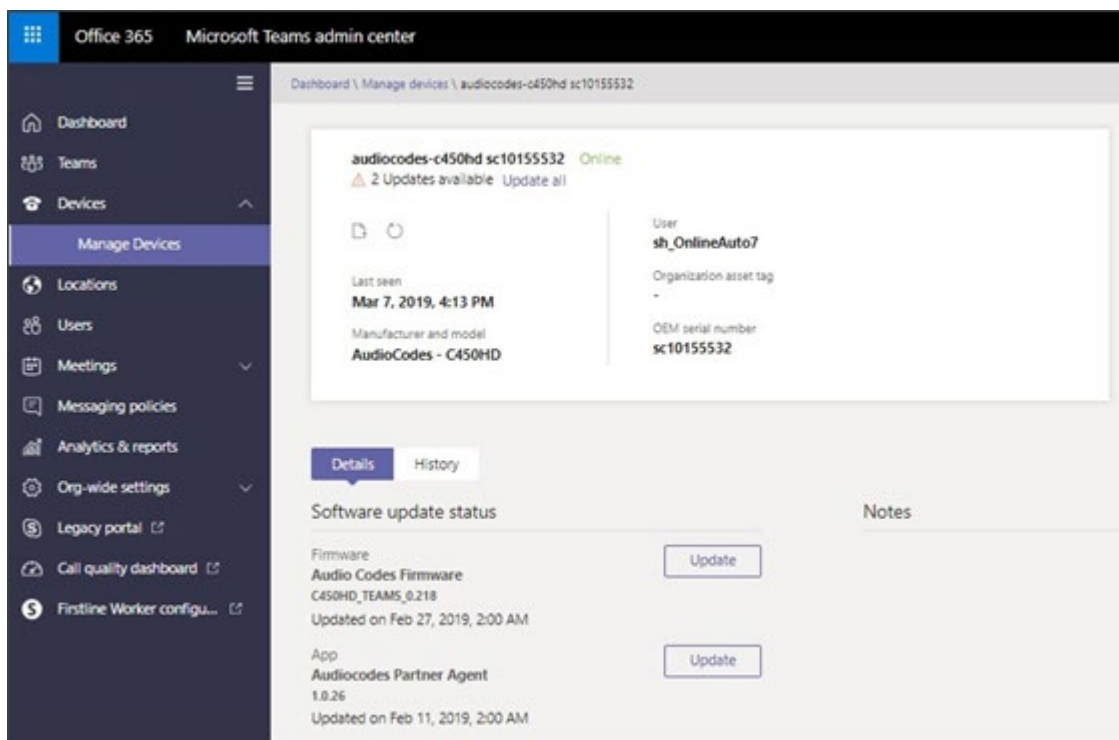
2. Navigate to and select **Log Level** and then select either
 - Verbose, Debug, Info, Warning, Error, Assert -or- None
3. Navigate to and select **Log Package Filter** and enter the filter.
4. Navigate to and select **Log Tag Filter** and enter the filter.
5. Navigate to and select **Log Buffer Filter**.



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

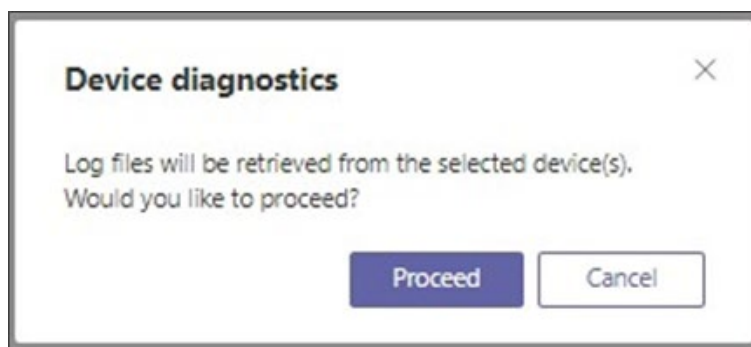
➤ **To collect logs:**

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

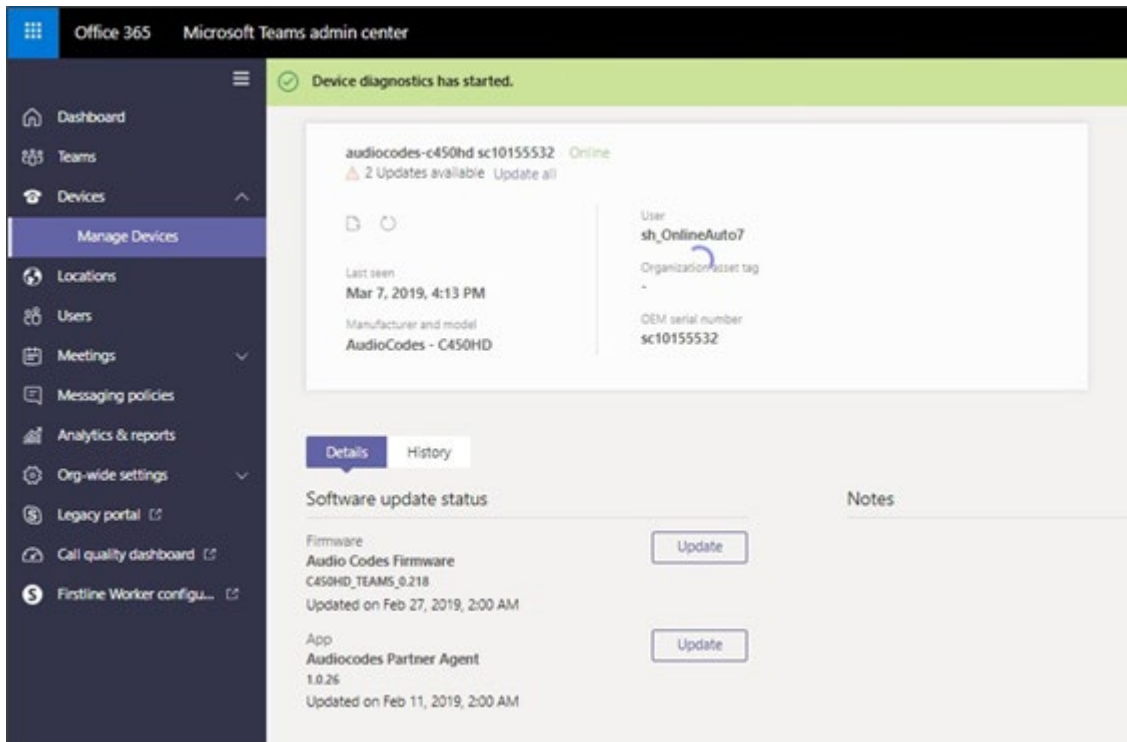


Note: The preceding figure is for illustrative purposes. It shows an AudioCodes phone. The same screen is displayed for the RXV80.

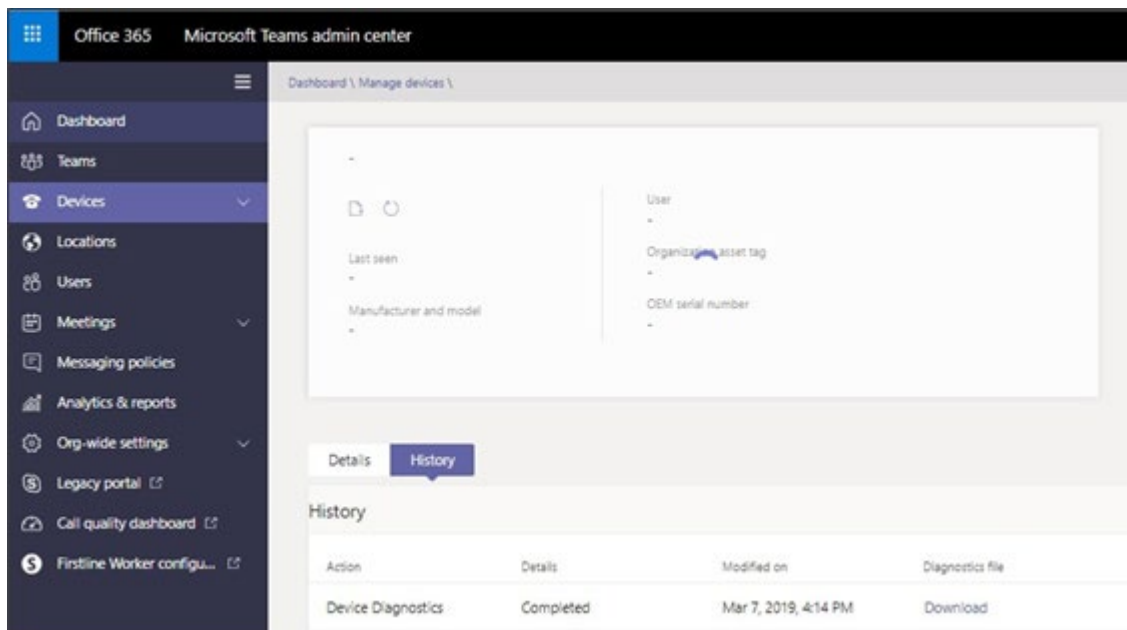
3. Click the **Diagnostics** icon.



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



5. Click the **History** tab.



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

4.1.10.2 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 ""
```

4.1.10.3 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 RXV80 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):

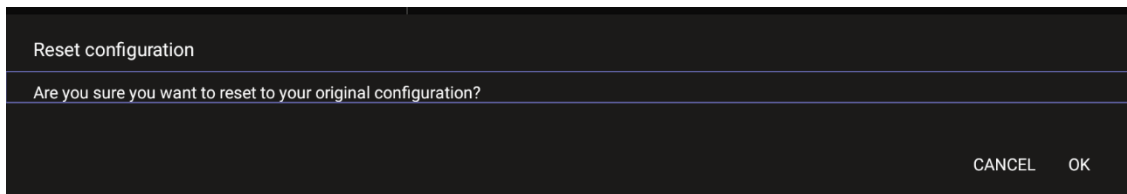
- dmesg.log
- dumpstate-TEAMS_1.3.16-undated.txt
- dumpstate_log-undated-2569.txt
- logcat.log

4.1.10.4 Reset configuration

Admin users can opt to 'clean up' their configuration history and return the RXV80 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>

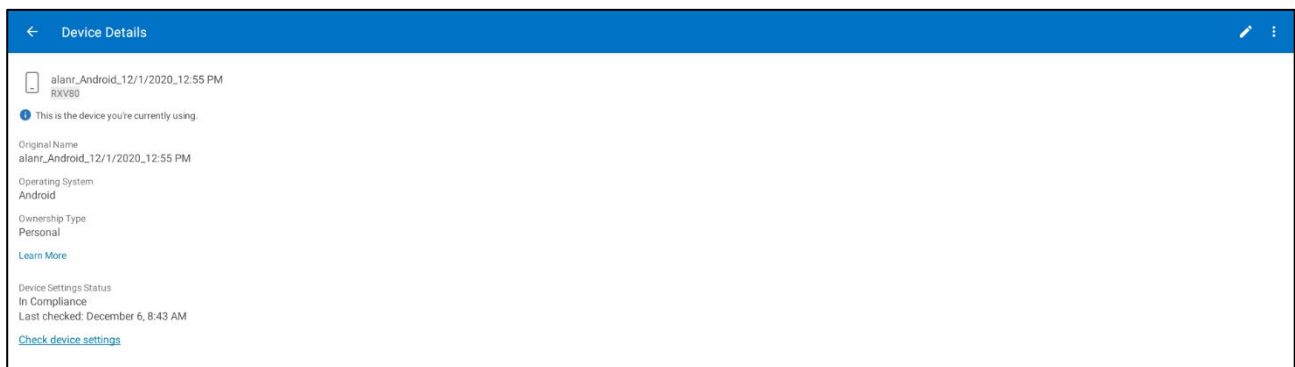
4.1.10.5 Restart Teams app

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.

4.1.10.6 Company Portal Login

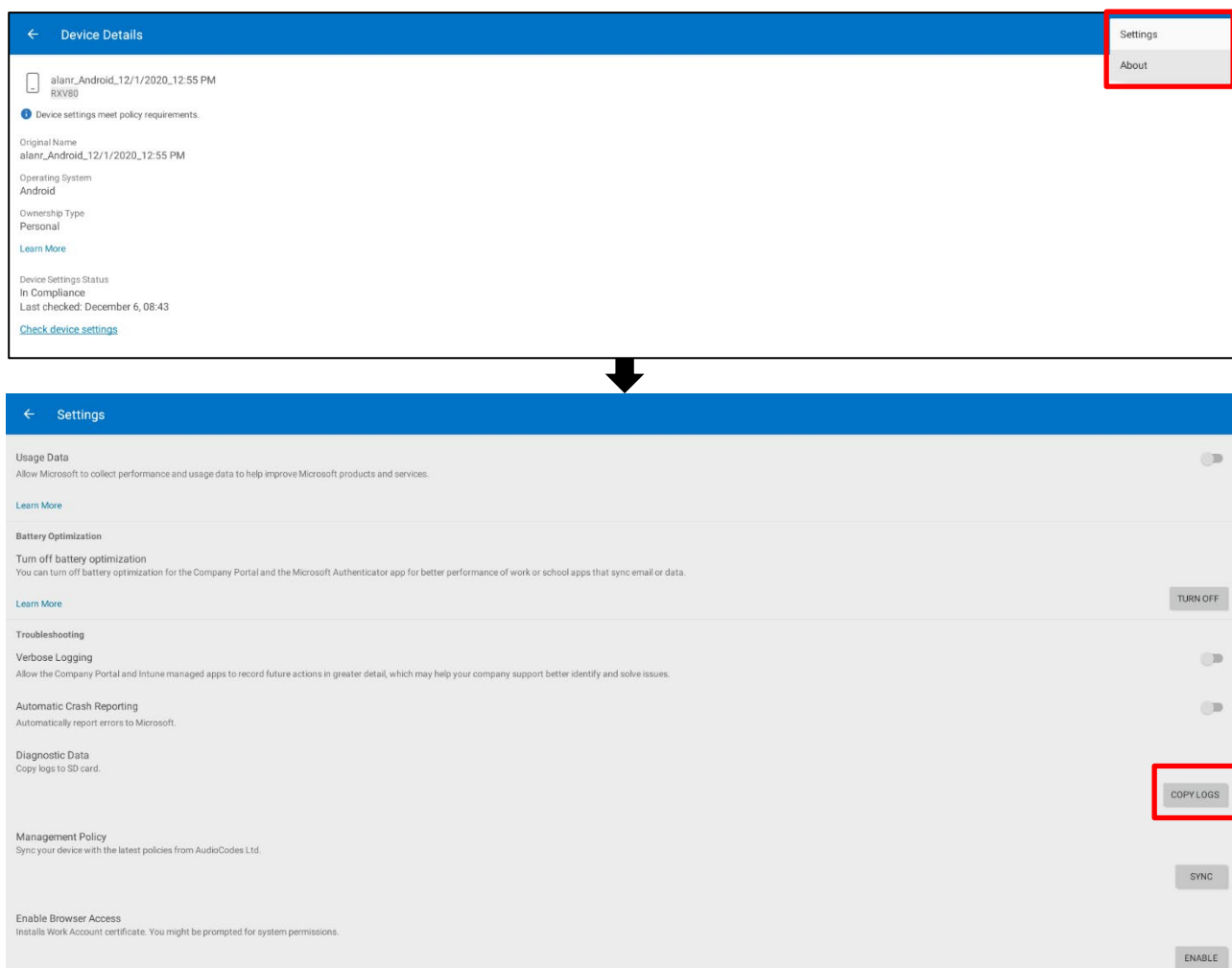


4.1.10.7 Getting Company Portal Logs

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 RXV80 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.

4.1.10.8 Launch Mobile Teams

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

4.1.10.9 Debug Recording

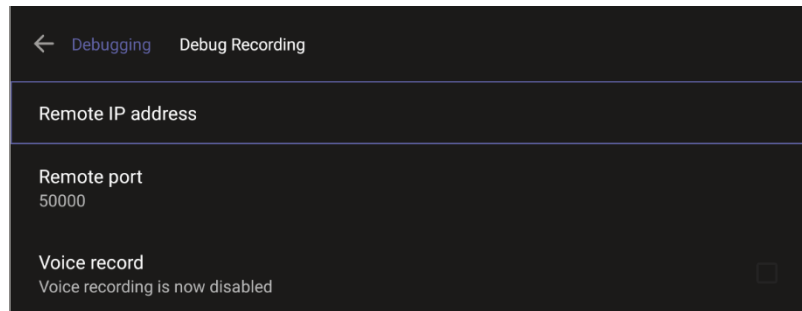
This feature enables Admin users to perform media/DSP debugging.



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**.



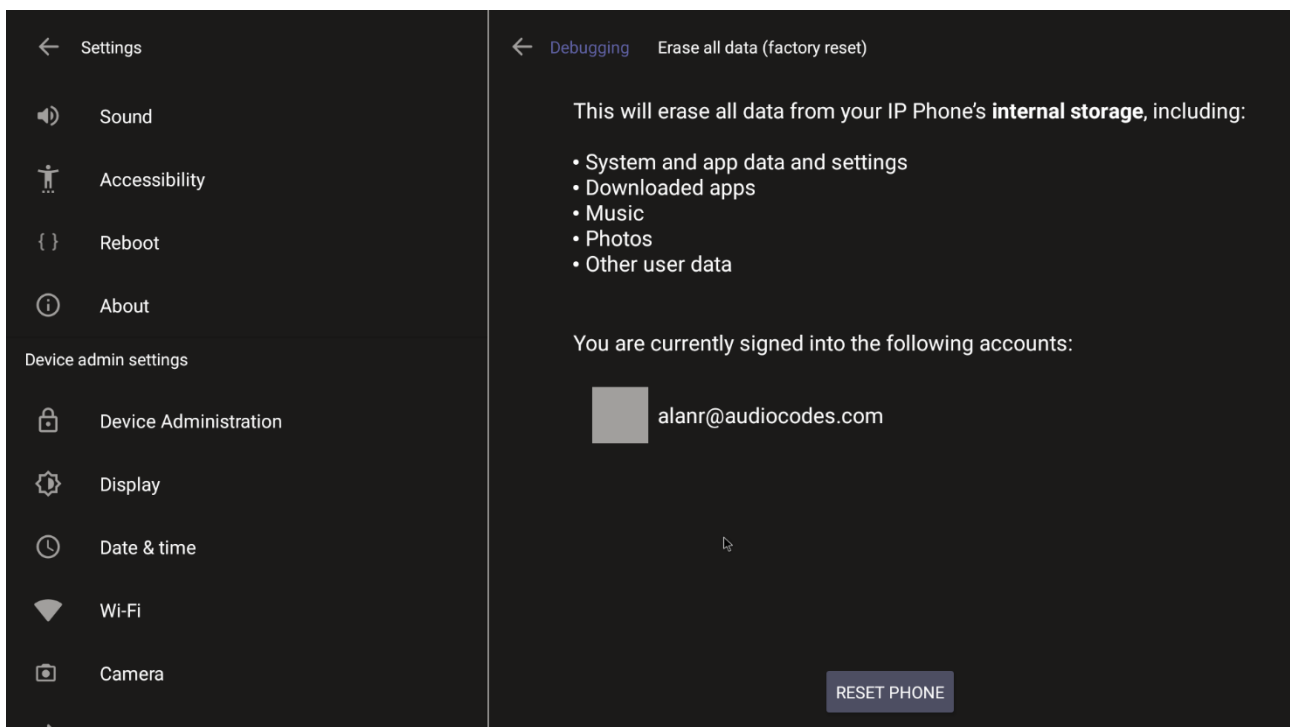
2. Navigate to and select **Voice record** to enable the feature.
3. Navigate to and select **Remote IP address** to input the IP address of the device whose traffic you want to record.
4. Navigate to and select **Remote port** and input it (Default: 5000).
5. Start Wireshark on your PC to capture audio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

4.1.10.10 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**.

4.1.10.11 ADB

The Android Debug Bridge is a command-line tool used to debug the Teams app. The setting is disabled by default; leave it unchanged at the default unless there's a real necessity to use it.

➤ **To enable ADB:**

- Navigate to and select the option.

4.1.10.12 Screen Capture

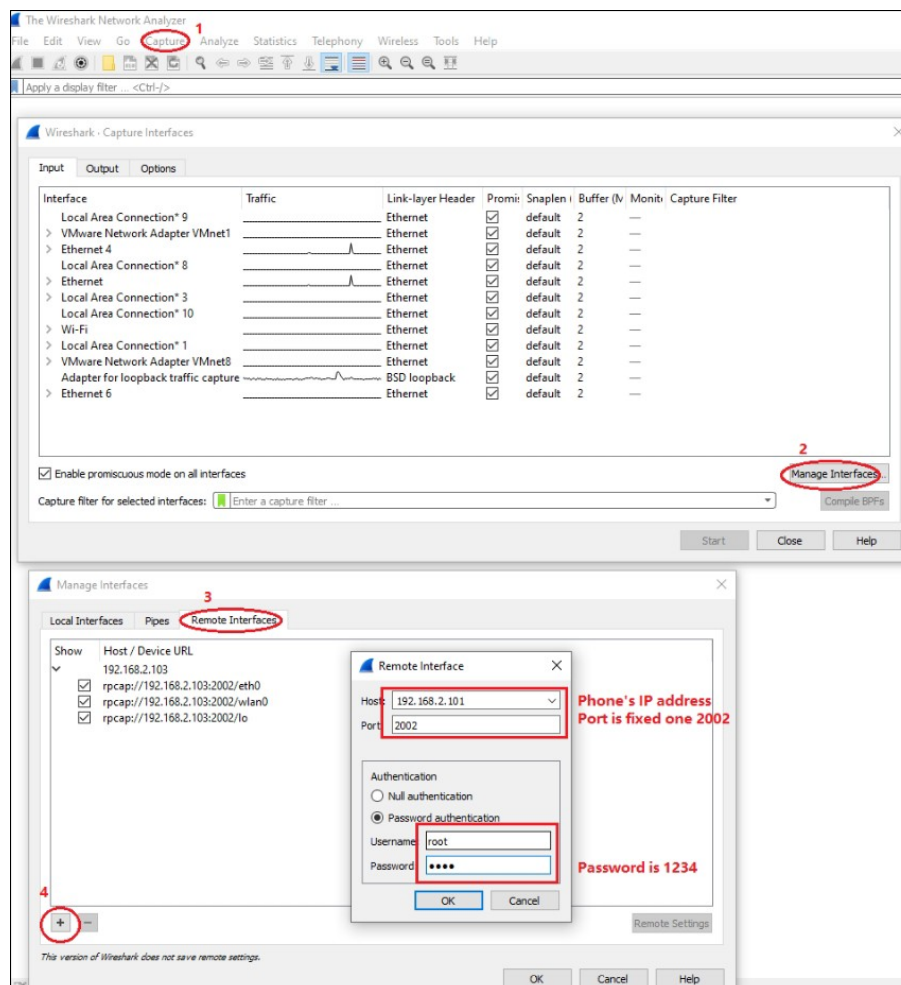
By default, this setting is enabled. If disabled, the phone won't allow its screens to be captured.

4.1.10.13 Remote Packet Capture

The 'rpkcap' (Remote Packet Capture) network sniffer application allows the Admin user to analyze and debug Android traffic on their desktop PC using the app's integral SSH server. Traffic is captured using the Android OS feature VpnService. Wireshark sshdump tool is supported. Traffic is captured as a pcap file. MITM (Man-in-the-Middle) functionality allows admins to decrypt traffic in Wireshark. Though it's recommended, others can be used.

➤ **To enable Remote Packet Capture:**

1. Navigate to and select the option.
2. After 'rpkcap' is enabled on the phone, use Wireshark to connect with it. Follow **the steps below** to connect to the phone.



3. View the phone interfaces. Choose your preferred interface with which to capture packets.

4.2 Configuring User Settings

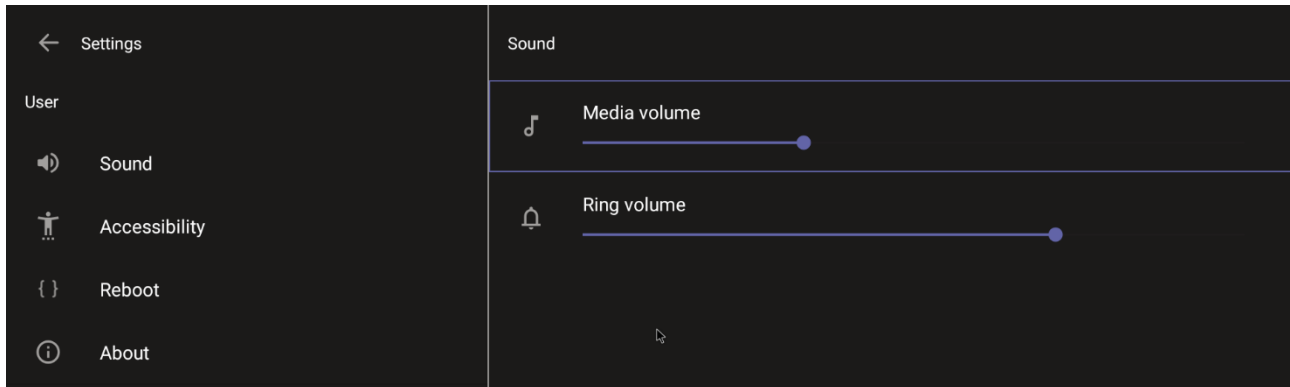
In the 'Settings' screen you can optionally configure the following User settings: Sound, Accessibility, Reboot and About (read-only).

4.2.1 Sound

You can customize phone volume for a friendlier user experience.

➤ **To configure sound settings:**

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

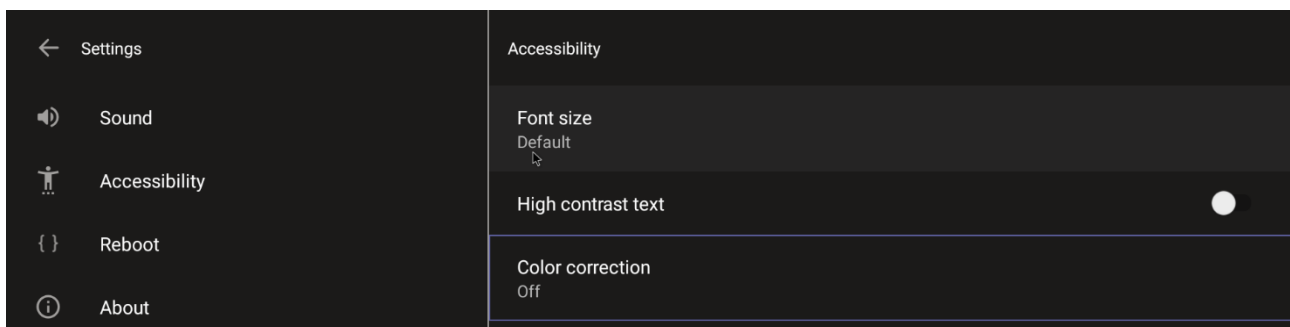


4.2.2 Accessibility

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**.



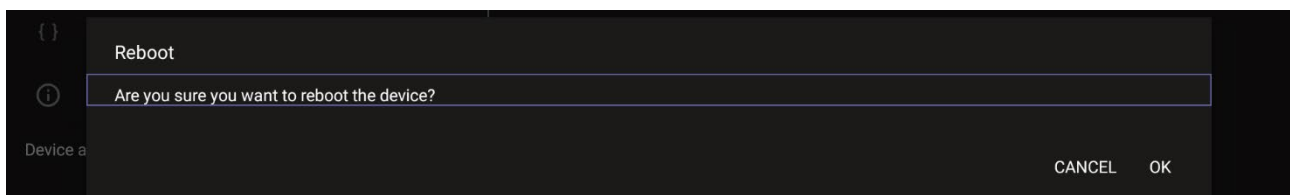
2. Adjust the settings to suit personal requirements.

4.2.3 Reboot

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

➤ **To reboot the RXV80:**

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

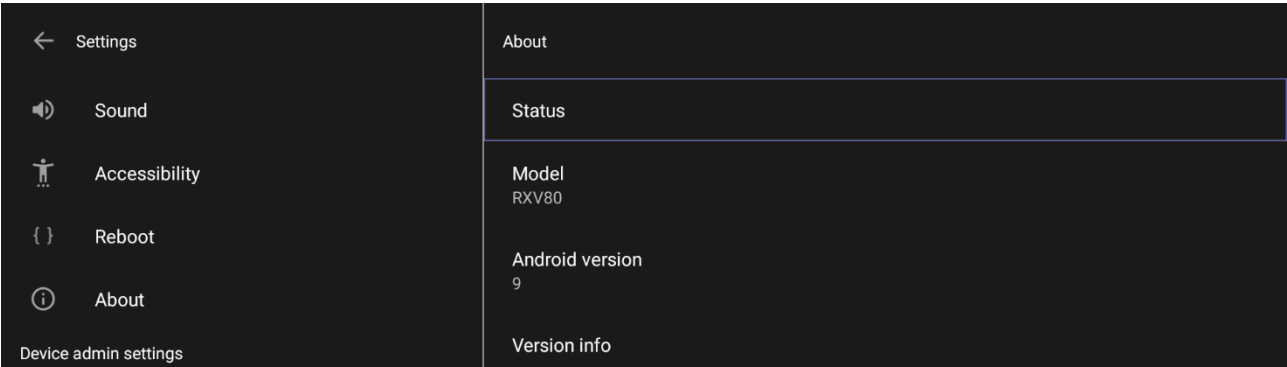


4.2.4 About

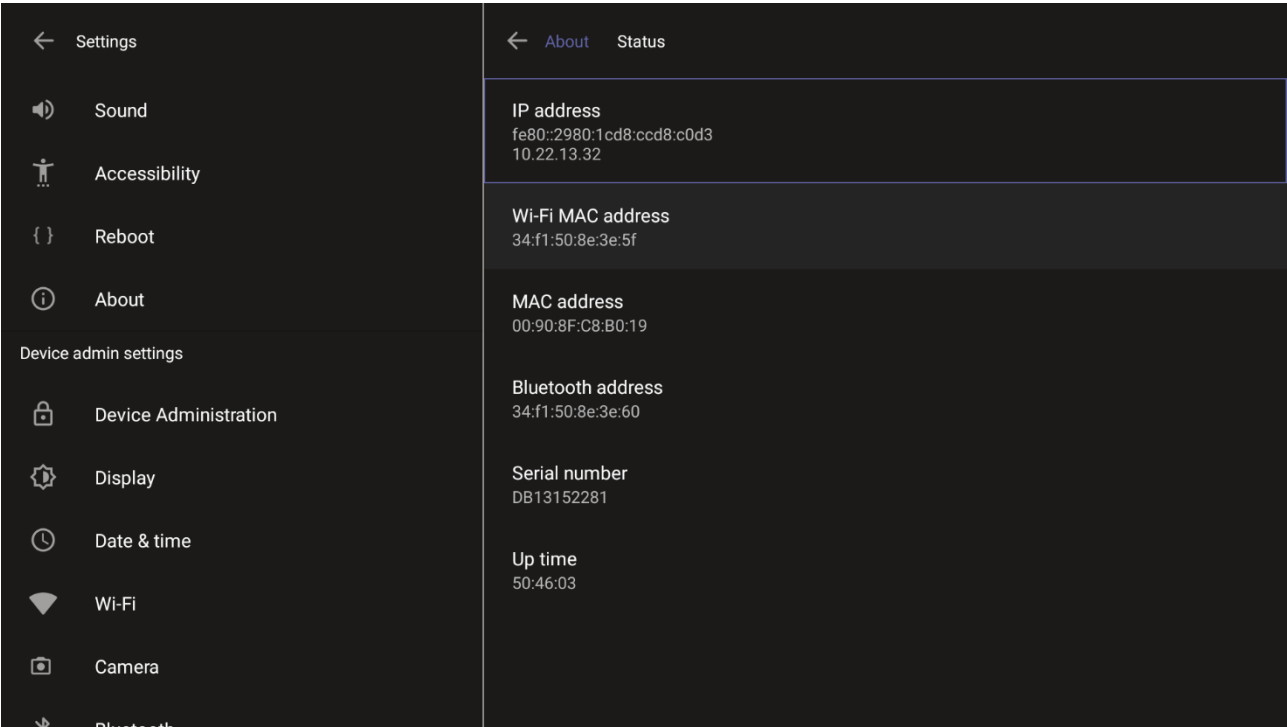
The 'About' screen gives you quick access to information about the RXV80 deployment.

➤ **To access the About screen:**

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



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



- 3. View the RXV80's firmware information.

This page is intentionally left blank.

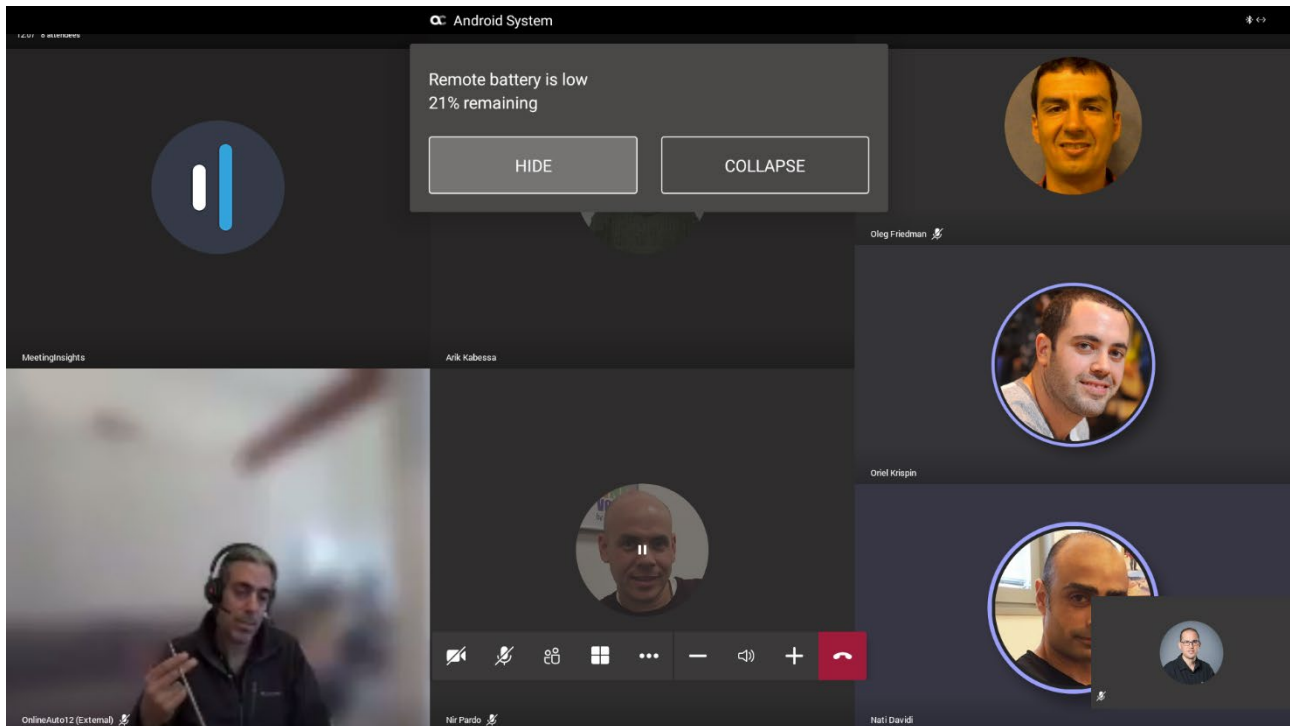
5 Updating Microsoft Teams Devices Remotely

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

This page is intentionally left blank.

6 Replacing Remote Controller Batteries

If the remote controller batteries run low, the RXV80 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.

6.1 Restarting / Rebooting the RXV80

The RXV80 sometimes needs to be restarted / rebooted, for example, after inserting the Bluetooth dongle.

➤ **To restart / reboot the RXV80:**

- Long-press the remote controller's power on/off button for about five seconds.

This page is intentionally left blank.

7 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.

200 Cottontail Lane,
Suite A101E,
Somerset, NJ 08873
Tel: +1-732-469-0880
Fax: +1-732-469-2298

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

Website: <https://www.audiocodes.com/>

©2021 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 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.

Document #: LTRT-18172

