User's and Administrator's Manual

AudioCodes Room Experience (RX) Suite

RXV200

Version 3.0

16:12
Monday, Nov 21, 2022
John
Available
16:12 - 16:30
Reserve
Introduction To Meeting Space Devices - Part 1
Available
Introduction To Meeting Space Devices - Part 2
Available

This page is intentionally left blank.

Notice

Information contained in this document is believed to be accurate and reliable at the time of publishing. However, due to ongoing product improvements and revisions, AudioCodes cannot guarantee accuracy of published 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: March-31-2026

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.

Security Vulnerabilities

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

Customer Support

Customer technical support and services are provided by AudioCodes or by an authorized AudioCodes Service Partner. For more information on how to buy technical support for AudioCodes products and for contact information, please visit our website at https://www.audiocodes.com/services-support/maintenance-and-support.

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 website at https://online.audiocodes.com/documentation-feedback.

Stay in the Loop with AudioCodes

Notes and Warnings

Canada Warning

This device contains licence-exempt transmitter(s)/receiver(s) that comply with Innovation, Science and Economic Development Canada’s licence-exempt RSS(s). Operation is subject to the following two conditions:

- This device may not cause interference.
- This device must accept any interference, including interference that may cause undesired operation of the device.

Le présent appareil est conforme aux CNR d’ISED applicables aux appareils radio exempts de licence. L’exploitation est autorisée aux deux conditions suivantes :

- l’appareil ne doit pas produire de brouillage;
- l’utilisateur de l’appareil doit accepter tout brouillage radioélectrique subi, même si le brouillage est susceptible d’en compromettre le fonctionnement.

Radio apparatus containing digital circuitry which can function separately from the operation of a transmitter or an associated transmitter, shall comply with ICES-003. In such cases, the labelling requirements of the applicable RSS apply, rather than the labelling requirements in ICES-003. This Class B digital apparatus complies with Canadian ICES-003.

Cet appareil numérique de la classe B est conforme à la norme NMB-003 du Canada.

IC SAR Warning:

This equipment should be installed and operated with minimum distance 20 cm between the radiator and your body.

Lors de l’ installation et de l’ exploitation de ce dispositif, la distance entre le radiateur et le corps est d ’au moins 20 cm.

Related Documentation

Document Name
RXV81 RXV200 RX-PAD RX-PANEL Release Notes
RX-PANEL Meeting Room Scheduler Quick Guide
RX-PANEL Meeting Room Scheduler Datasheet
One Voice Operation Center (OVOC) User’s Manual
Device Manager Administrator’s Manual

Document Revision Record

LTRT	Description
18295	Updated to Version 2.8.208 Updated Time Zone.
18296	Updated to Version 2.8.574 (M1)
18297	Updated to Version 2.8.855 (M2)
18298	Updated to Version 2.8.917 (M3) 802.1x authentication parameters
18299	Updated to Version 3.0; provisioning source auto discovery; admin password brute force protection

Table of Contents

1 Introduction 1

Highlights 1

Management 1

Specifications 2

Security Guidelines 2

2 Getting Started 3

Review Package Contents 3

Position RX-PANEL 3

Mount RX-PANEL 4

Connect Cables 5

Power up RX-PANEL 6

Pair RX-PANEL with MTRA via MS Teams 6

3 RX-PANEL Operation 7

RX-PANEL Controls 7

Reserve Meetings 8

Manage Reservations 10

4 User Settings 12

Access User Settings 12

Configure Accessibility Settings 13

View RX-PANEL Information 14

View Microsoft Teams Information 14

Reboot the Device 15

5 Admin Settings 16

Access Device Admin Settings 16

Log in to Device Administration 16

Brute Force Protection for Admin Password 17

Change the Admin Password 17

Show or Hide Password Characters While Typing 18

Configure the Admin Login Timeout 18

Sign out 19

Configure the Display 19

Set Date and Time 20

Configure Wi-Fi 21

Connect to an Available Wi-Fi Network 21

Connect Manually to a Wi-Fi Network 21

Configure Wi-Fi Security with Certificate-based Authentication 24

Configure Power Saving 24

Configure UI Language and Input 25

Modify IP Network Settings 25

Set up a Proxy Server 26

Configure 802.1x Settings 26
Configure VLAN Settings 29
Enroll a Device with Intune Policies 30
Create a Dynamic Group 30
Create an Exclusion Group 30
Remove Devices from Intune Admin Center 31
Enroll Certificates using SCEP 33
Provision Certificates in .pfx Format 34
Update RX-PANEL Remotely 34
6 System Monitoring and Debugging 36
Monitor the System Status 36
Configure Log Settings for Collecting Logs 37
Enable Remote Logging 38
Copy Diagnostic Data to SD Card 38
Reset the System Configuration 39
Configure Provisioning Source Auto Discovery Settings 39
Perform a Full Factory Reset 40
Reset User Data 40
Restart the Teams App 41
Perform Debug Recording 41
Control Screen Capture 41
Control Remote Package Capture 41
Return to Previous Version 42
7 Android-based Teams Devices Parameters 43

1 Introduction

The AudioCodes PANEL-RX Meeting Room Scheduler is a purpose-built Microsoft Teams Panel with an intuitive touchscreen display. Neatly installed right at the entrance to the meeting room, the RX-PANEL's brightly colored status LED enables users to quickly see the meeting room's availability from a distance. Users can also view the meeting details on its sleek and clear LCD screen and reserve a meeting room on the spot.

Refer to the AudioCodes website for additional information.

⚠ Microsoft Teams Android devices now utilize Intune Android Open Source Project (AOSP) device management. AOSP device management is a mobile device management (MDM) platform specifically designed for Teams devices. This update delivers more reliable user experience, an enhanced deployment process for administrators, and serves as the foundation for future innovations and advanced management capabilities for Microsoft Teams Android devices, including Teams Rooms, Teams panels, Teams phones, and Teams displays.

AOSP Device Management replaces the legacy Android Device Administrator solution previously used to manage Teams devices.

For detailed information on the AOSP migration process, please refer to the relevant Microsoft documentation.

Highlights

feature highlights are:

RX-PANEL supports the following features:

- Utilizes plug-and-play simplicity to boost the meeting room experience with a dedicated panel showing the meeting details and room availability.
- Easily reserve the room for ad-hoc meetings.
- Unique, clearly-visible status LED indicating meeting space availability.
- Glass and wall mountable for a professional and spotless appearance.
- Dedicated special touch buttons (Home and Back).
- High-resolution 8-inch touchscreen.
- Runs Android 12 for improved security.
- Can be managed by AudioCodes Device Manager.

Part number: TEAMS-RX-PANEL– MSRP

Management

RX-PANEL is managed using AudioCodes' On-prem or Live Platform Device Manager, enabling IT admins to monitor and upgrade the devices from anywhere. Using Device Manager, IT admins can easily monitor and manage all devices from a centralized location. Management includes:

- Monitoring
- Firmware management / upgrade
- Alarm management
- Provisioning of device language, date, and time settings

Admins can monitor the status of the device's software modules from the System State screen (see Monitor the System Status on page 36).

Specifications

- For RX-PAD specifications, see the RX-PAD datasheet.
- For RX-PANEL specifications, see the RX-PANELdatasheet.

Security Guidelines

For detailed security guidelines regarding AudioCodes Native Teams Android-based devices, refer to the document Security Guidelines for AudioCodes Native Teams Android based Devices.

2 Getting Started

Getting started with RX-PANEL consists of:

1. Installing:
   - Reviewing the
   - Positioning
   - Mounting
   - Cabling
   - Powering up

- Review Package Contents below
- Position RX-PANEL below
- Mount RX-PANEL on the next page
- Connect Cables on page 5
- Power up RX-PANEL on page 6
- Pair RX-PANEL with MTRA via MS Teams on page 6

For more details, see the *RX-PANEL Meeting Room Scheduler Quick Guide* shipped with the product or available from AudioCodes.

Review Package Contents

Make sure you received the following in the shipped box, in addition to the RX-PANEL unit:

- Ethernet cable
- 4 screws, 4 wall anchors, 1 template (for concrete wall mount)
- Glass-mounting bracket (for glass partition mount)

⚠ Power Supply (PS) is not supplied but can be ordered separately.

Position RX-PANEL

Position the device at the entrance to a conference room. Mount the device on either of the following:

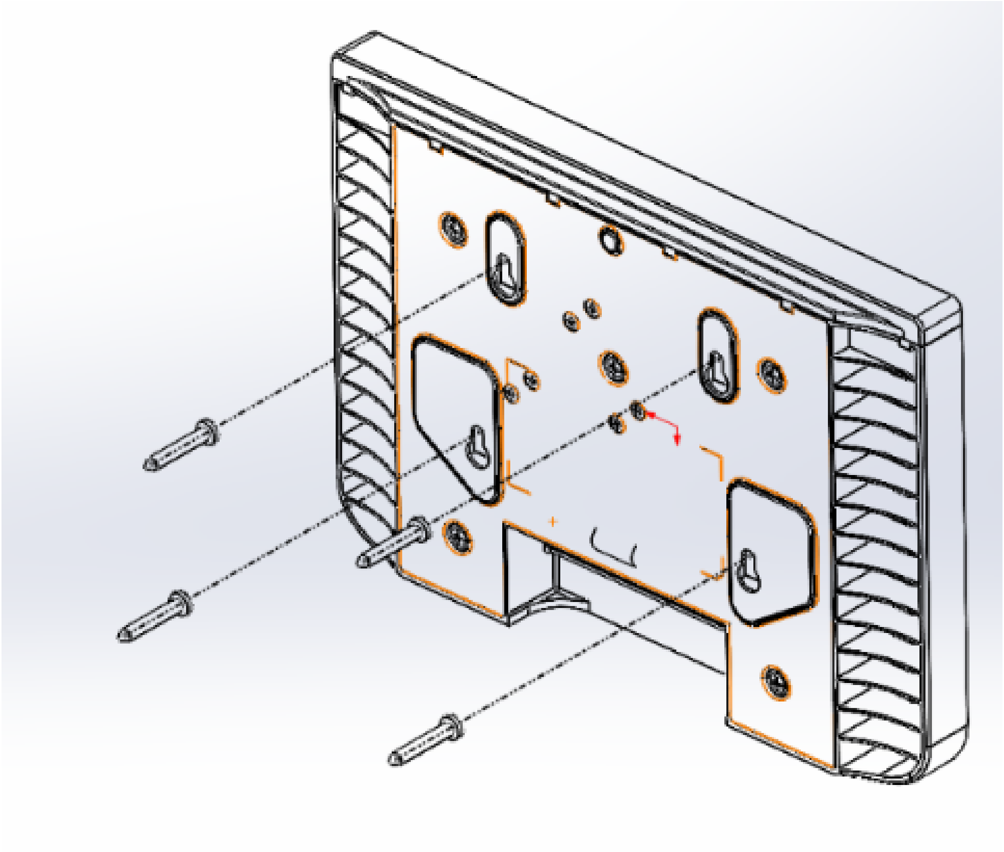
- Concrete wall
- Glass partition

⚠ The device is suitable for mounting at a height no more than 2m.

Mount RX-PANEL

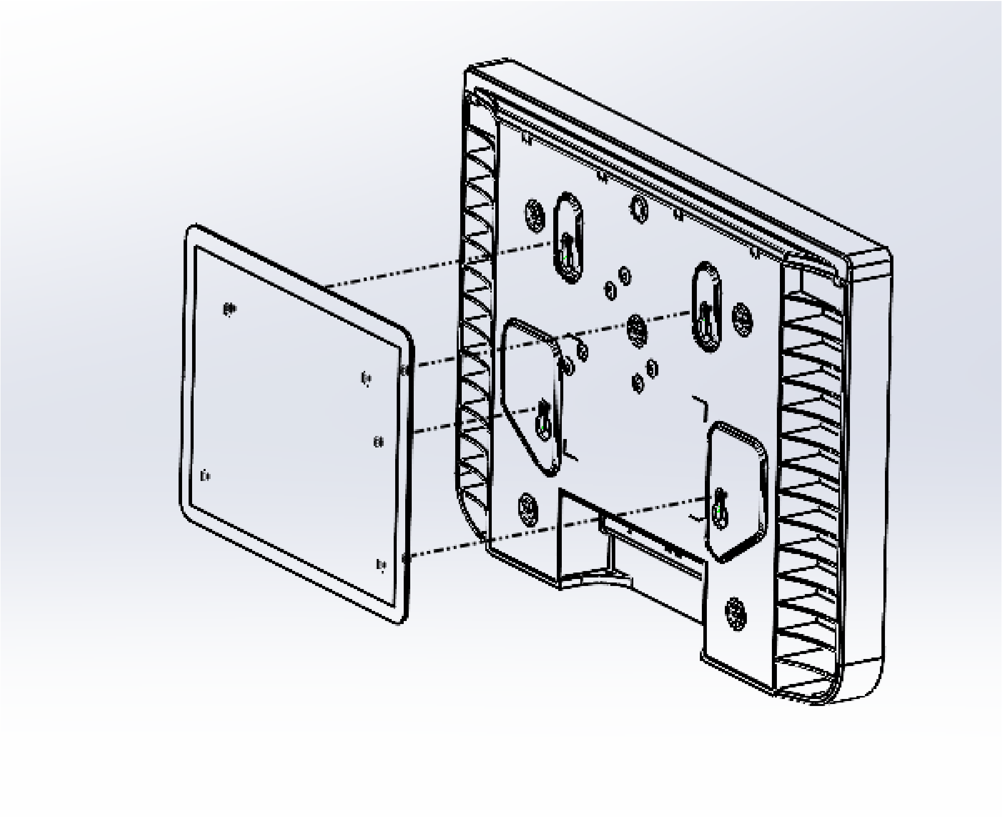
- **Concrete wall (see the following figure)**

Use the supplied template to mark locations for 4 wall anchors; insert the 4 screws into them.



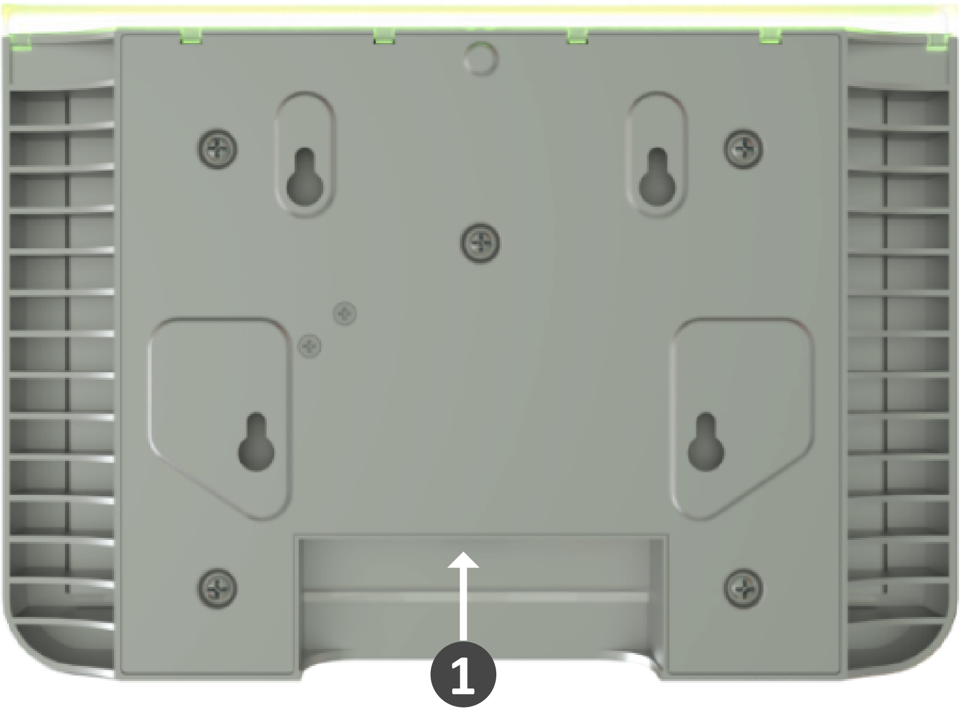
- **Glass partition (see the following figure)**

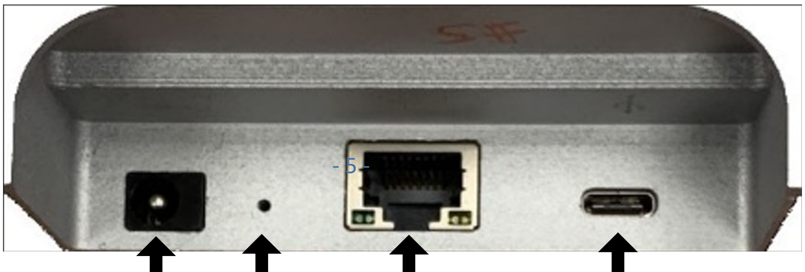
Remove the bracket’s adhesive strip cover, fix the bracket on the glass and hang RX-PANEL on it.



Connect Cables

The figures below show the RX-PANEL rear connector ports.





#	Description
1	■ The preceding figure left shows the ports' location (concealed view). ■ The preceding figure right shows theports.
2	DC jack for 12V power supply
3	Reset (Insert pin, unplug PoE, keep pin inserted, plug in PoE, keep pressing for 10 seconds)
4	Ethernet LAN/PoE GbE, RJ-45
5	USB Type C connector (for maintenance purposes)

Power up RX-PANEL

Connect the RX-PANEL LAN / PoE port to any PoE Ethernet switch; the unit powers up.

Pair RX-PANEL with MTRA via MS Teams

To allow for advanced meeting functions, your RX-PANEL must be paired at MS Teams level with the meeting room's MTRA device (RXV200 or RXV81).

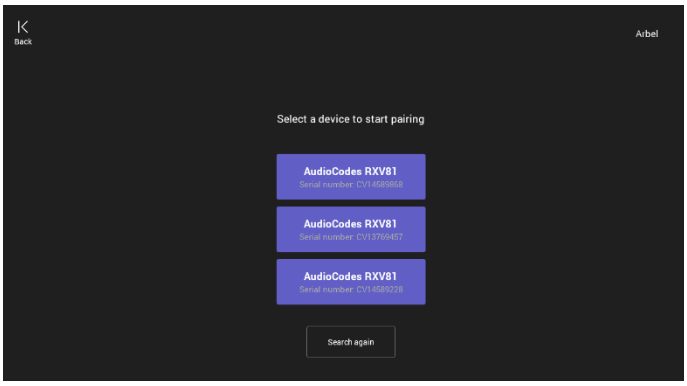
➢ To pair RX-PANEL with an MTRA:

1. **1.** If not already logged in, log in to Device Administration to get admin access (see Log in to Device Administration on page 16).

2. Under 'Device admin settings', scroll down and tap **Teams Admin Settings**, then tap again **Teams Admin Settings**.

3. In the 'Teams Admin Settings' menu, tap the **Device Pairing** option in 'Teams Admin Settings' menu. The available MTRA devices are displayed.

4. Tap the relevant device to pair it with your RX-PANEL.



Select a device to start pairing

AudioCodes RXV81
Serial number: CV14589868
AudioCodes RXV81
Serial number: CV13769457
AudioCodes RXV81
Serial number: CV14589228
Search again

2. **5.** Tap the **Backgrounds** option to select a background of your choice.
3. **6.** Click the **LED settings** option to select the LED color indicating busy state.
4. **7.** Click the **Meetings** option to define advanced meeting check-in functions.

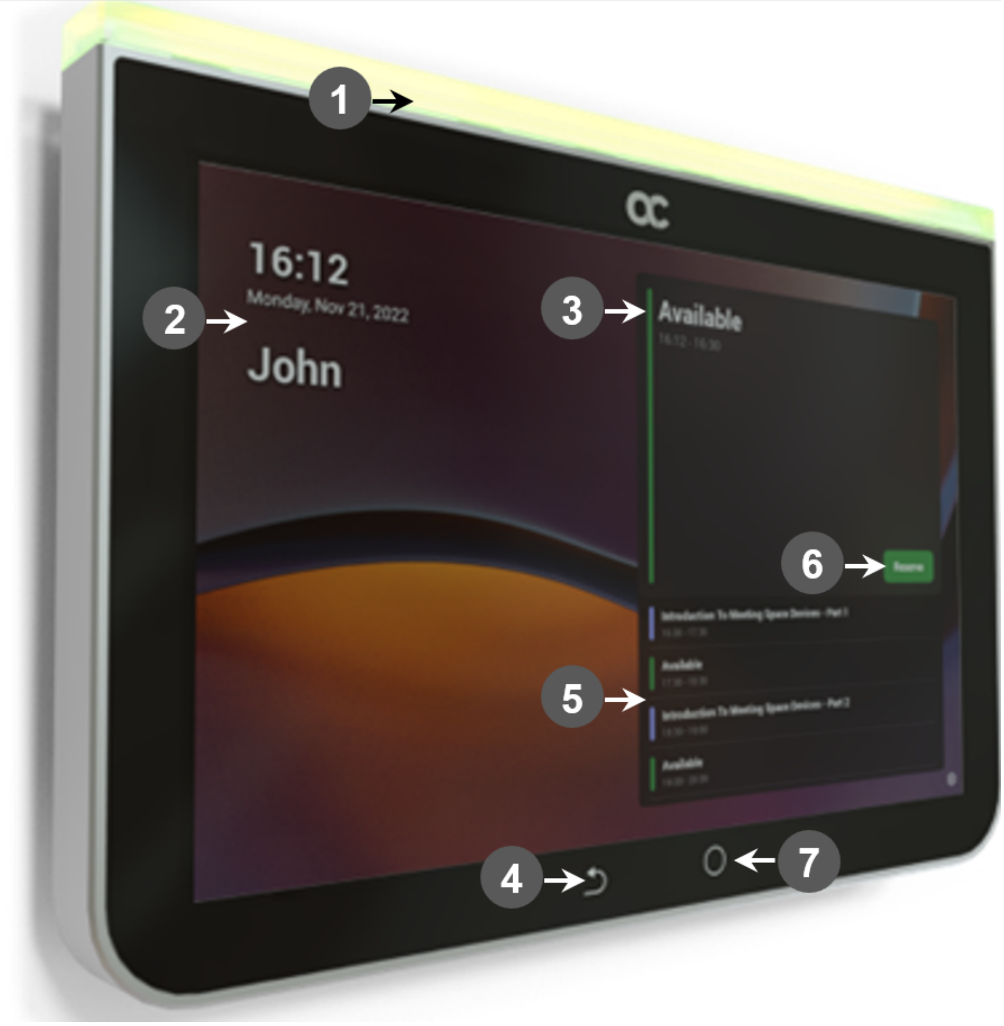
3 RX-PANEL Operation

This chapter explains how to use the RX-PANEL for handling meetings and reservations:

- RX-PANEL Controls below
- Reserve Meetings on the next page
- Manage Reservations on page 10

RX-PANEL Controls

Use the following table as reference to the following figure.



L-R	Description
1	Space availability status LED, viewable from a distance: ■ Green = meeting space available; optionally reserve it right now

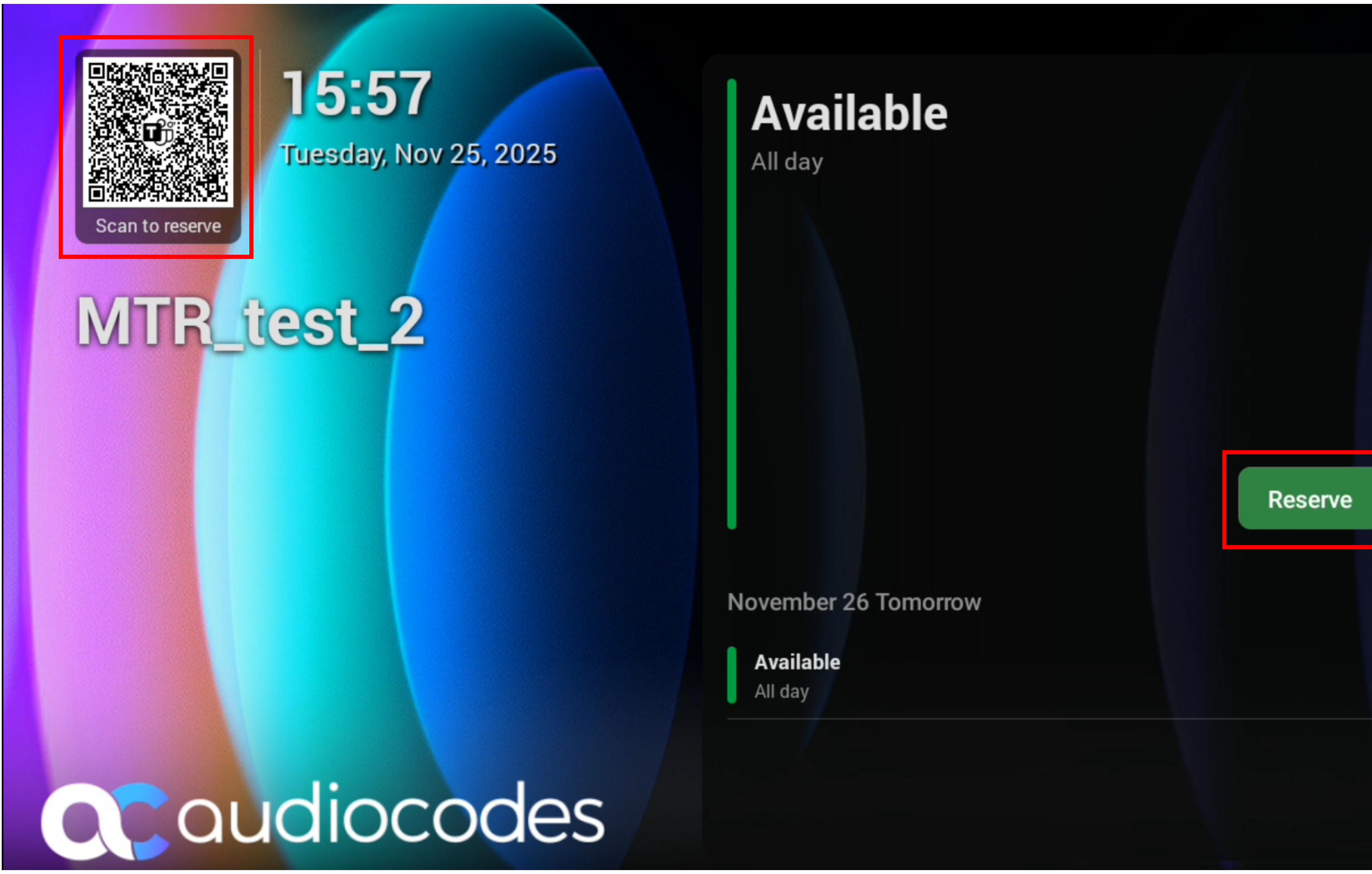
L-R	Description
	■ Red or purple = meeting space unavailable ■ Flashing red is a system status alert indicating, for example, recovery mode. ■ Flashing green and blue indicates restore to defaults.
2	Meeting details; meeting time | date | organizer
3	Meeting space availability status
4	'Back' button; tap to return to the screen previously accessed
5	All meeting spaces and availability statuses
6	Tap to reserve an available meeting space for an ad hoc meeting
7	■ Tap to return to the home screen from any screen. ■ Long-press to access Settings.
Note: Admin can change background wallpaper | color of status indicator | text contrast, etc.	

Reserve Meetings

You can reserve an ad hoc meeting when the RX-PANEL LED is green.

➢ **To reserve an ad hoc meeting:**

1. Activate RX-PANEL.

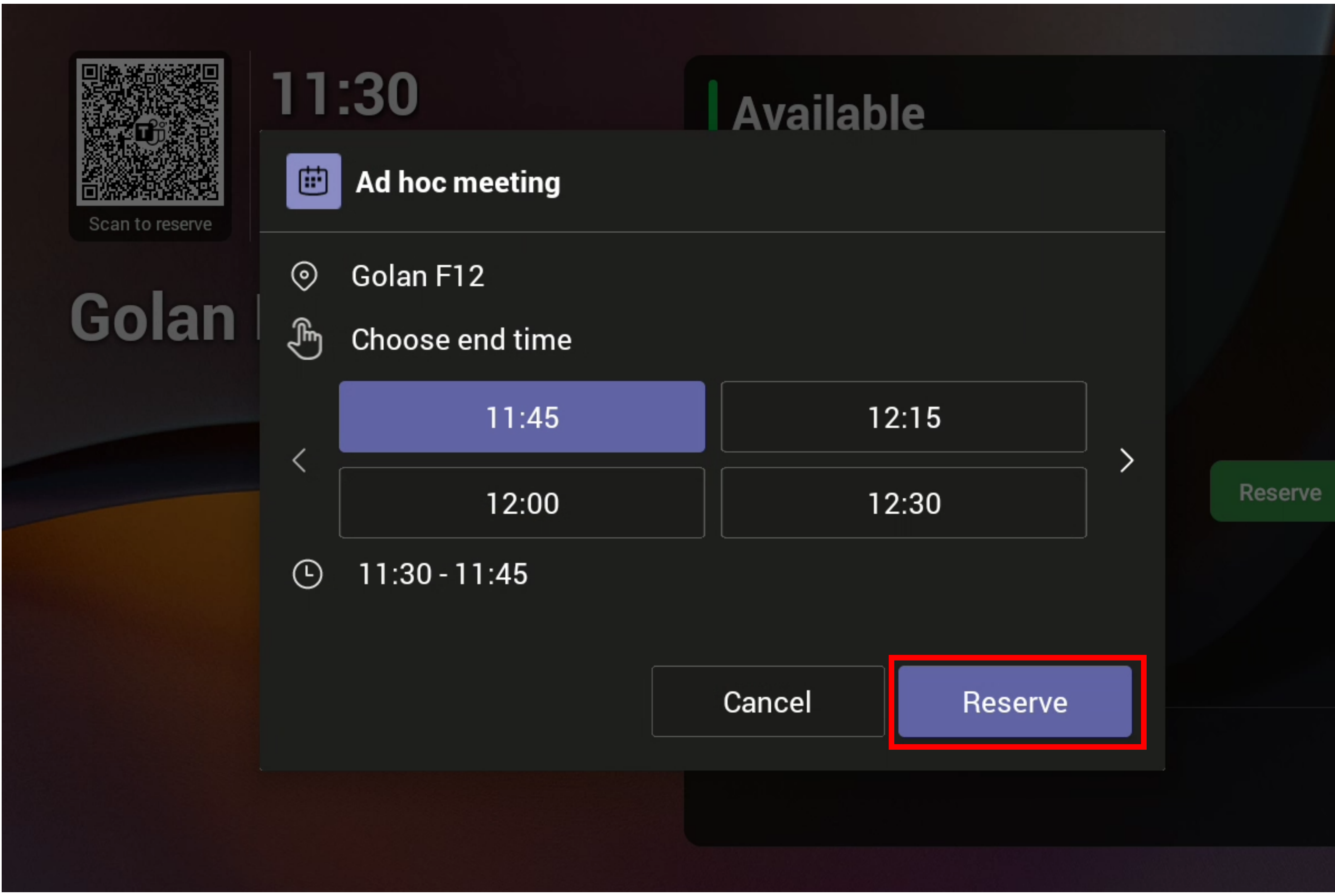


2. Do either of the following:

- Scan the QR Code in the home screen (see the Microsoft Teams documentation on reserving rooms with a QR code).

> ⚠ This feature is enabled by default and can be disabled under **Device settings** > **Admin settings** > **Meetings**.

- Tap **Reserve** (only if RX-PANEL is paired with an MTRA device– RXV81 or RXV200).

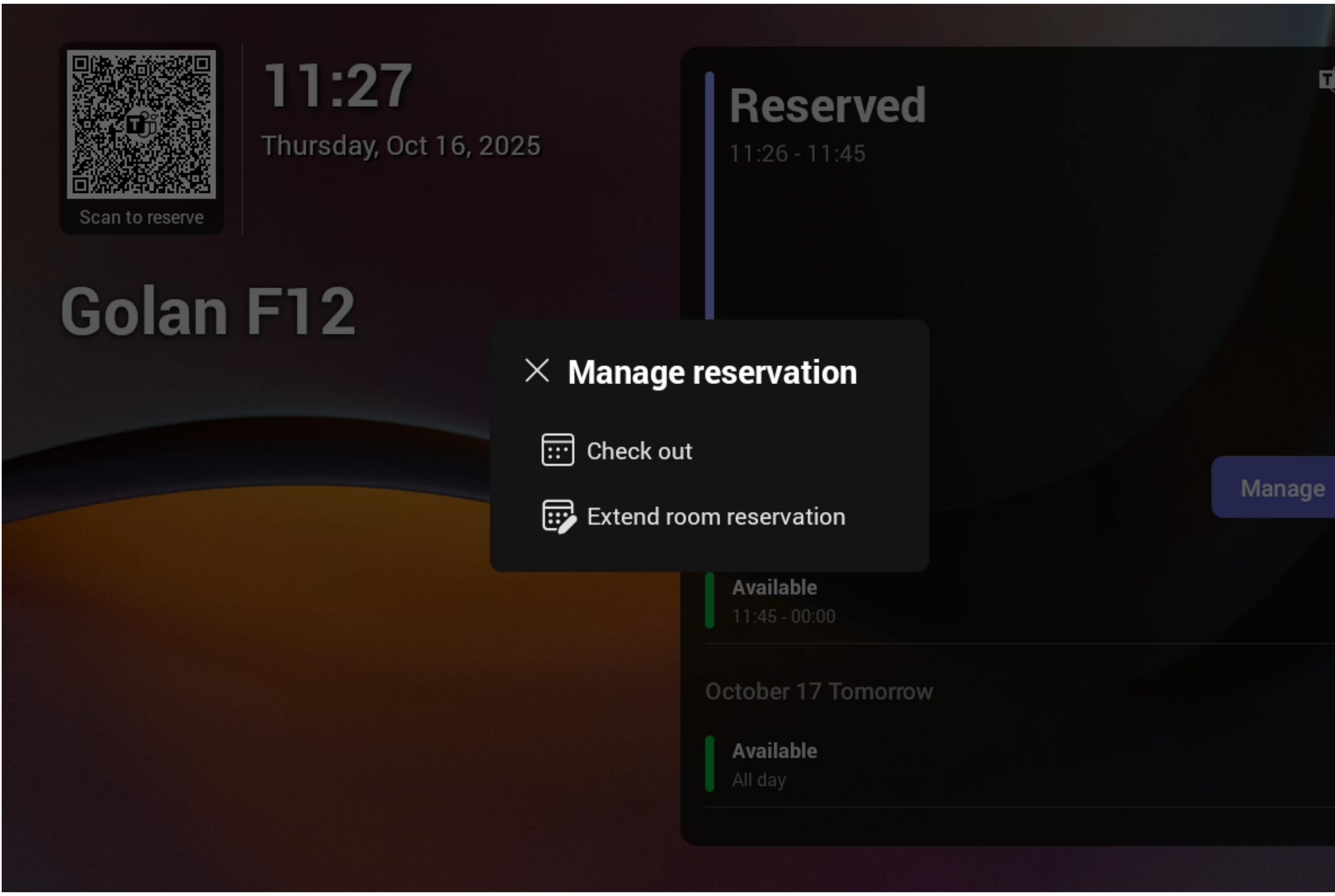


Tap **<** or **>** to navigate to the end time, then tap **Reserve**.

Manage Reservations

➢ **To manage a reservation:**

1. Activate RX-PANEL and tap **Manage**.



2. Tap **Check out** and in the verification prompt, tap **Check out**; this ends your room reservation.
3. Optionally, tap **Extend room reservation**.
4. Choose the end time and then tap **Reserve**.

4 User Settings

RX-PANELs are delivered configured with their default settings. Users can customize some of them from the 'Settings' page to suit their personal preferences, without needing Admin login:

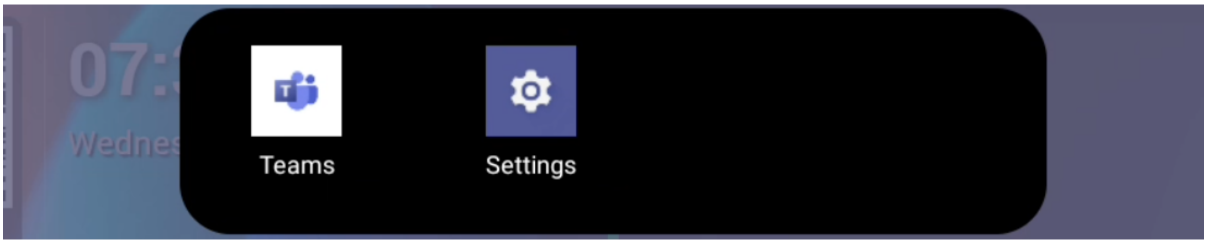
- Configure Accessibility Settings on the next page
- View RX-PANEL Information on page 14
- View Microsoft Teams Information on page 14
- Reboot the Device on page 15

To access the 'Settings' page, see Access User Settings below.

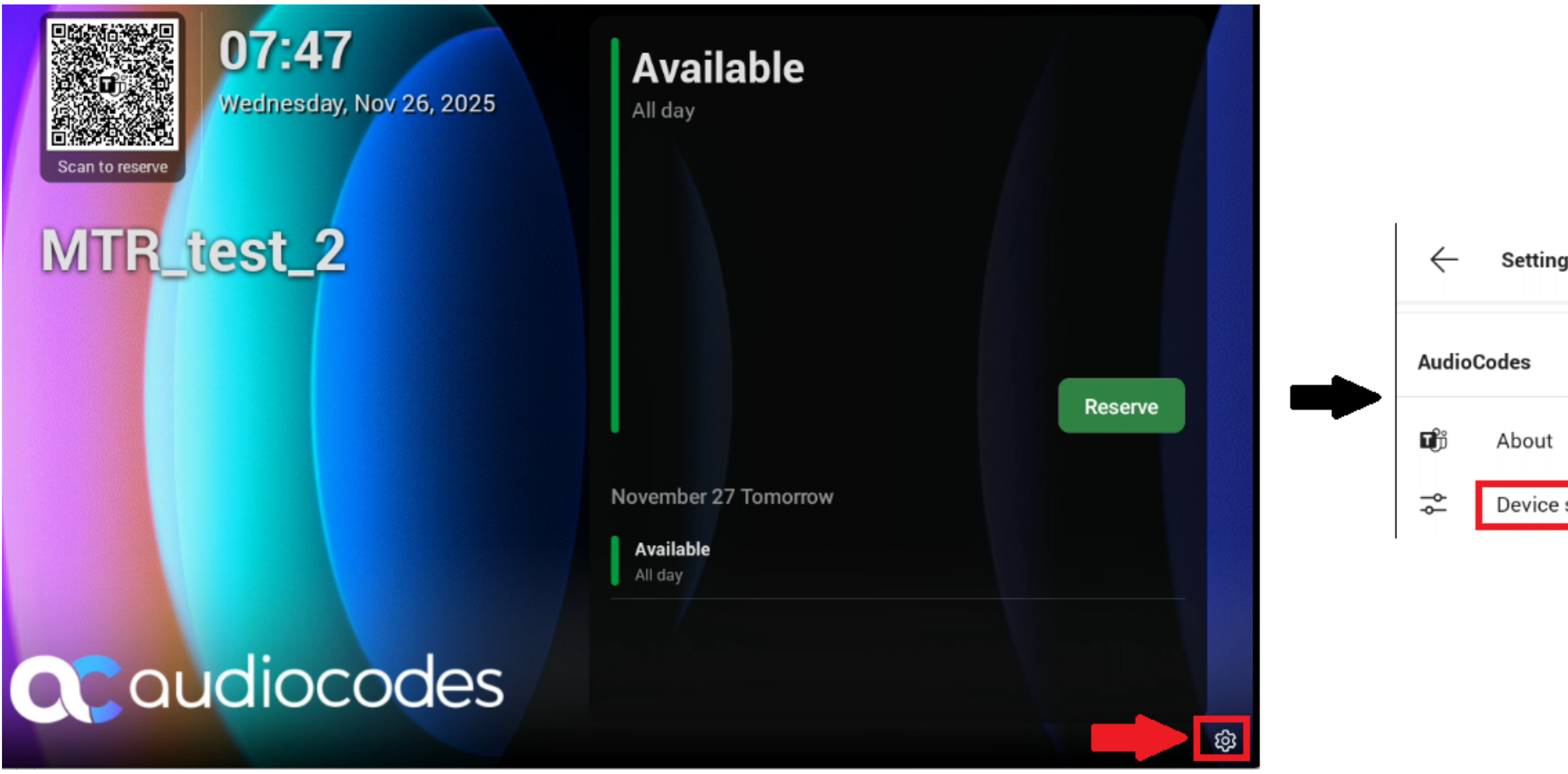
Access User Settings

There are several ways to access the 'Settings' page from the homepage:

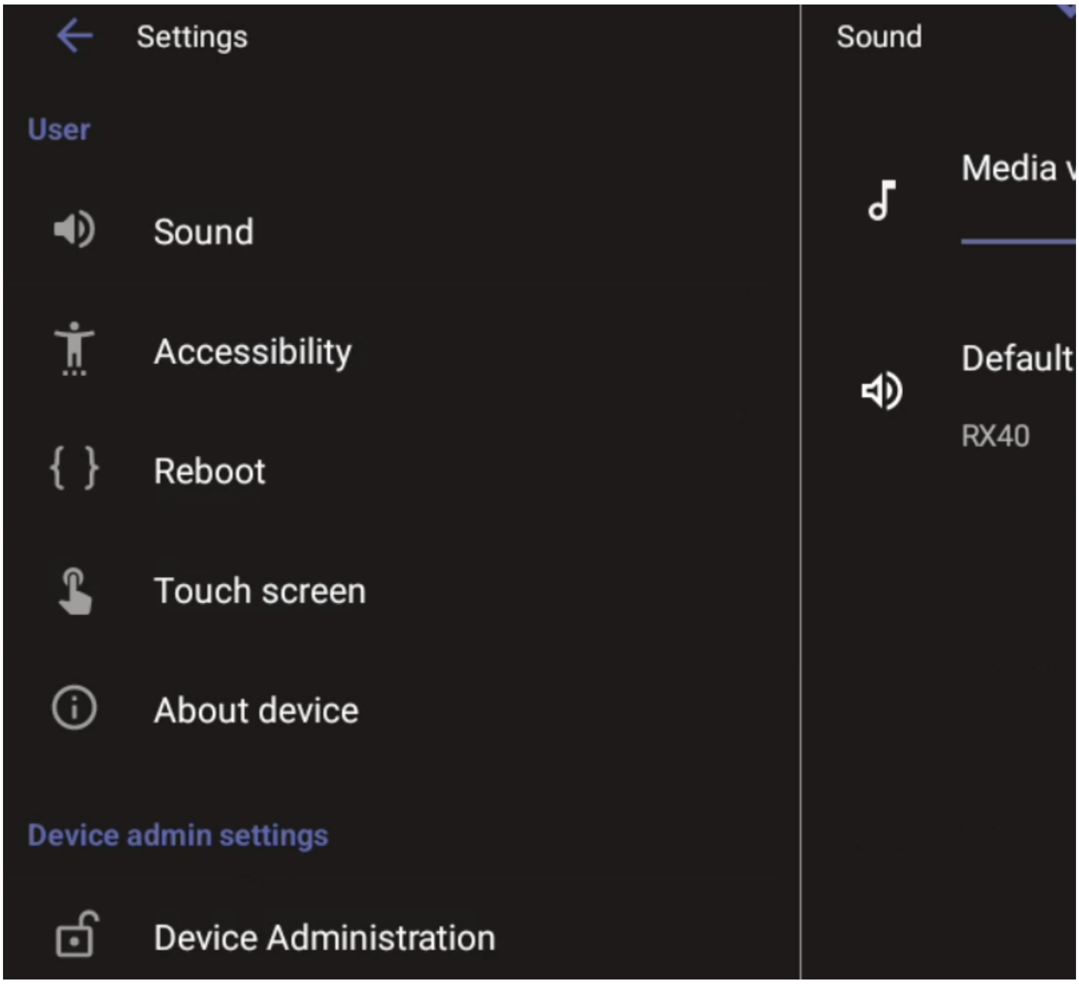
- Swipe down to display the main menu tray, then tap **Settings**.



- Tap the wheel icon in the bottom right corner of the homepage, then tap **Device Settings**.



Any user can configure User settings:



⚠ Viewing and configuring Device Admin settings requires Admin login. For details, see Admin Settings on page 16.

Configure Accessibility Settings

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

➢ **To configure the Accessibility setting:**

1. Navigate to ‘Settings’ (see Access User Settings on the previous page).
2. Under ‘User’, tap Accessibility.
3. Adjust the settings to suit personal requirements.

Feature	Description
TalkBack	If turned on, provides spoken feedback, which is helpful for vision-

Feature	Description
	impaired users.
Font Size	Increases or decreases the font size on the screen.
High Contrast Text	High contrast display modes to improve readability for users with visual impairments
Color Correction	Adjusts colors for users with color blindness.

View RX-PANEL Information

The ‘About’ screen gives you quick access to information about the RX-PANEL deployment.

➢ **To access the About page:**

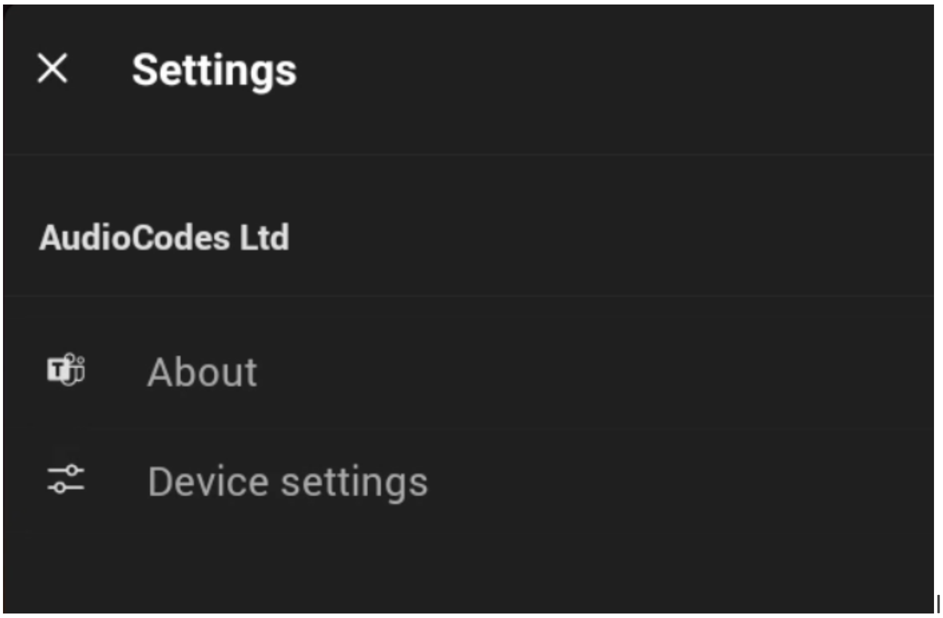
1. Navigate to ‘Settings’ (see Access User Settings on page 12).
2. Under ‘User’, tap **About device**.

⚠ Admins can monitor the status of the device’s software modules from the System State page (see Monitoring the System Status).

View Microsoft Teams Information

➢ **To view the About Microsoft Teams from the RX-PANEL:**

1. On the homepage, tap the wheel icon in the bottom right corner, then tap **Settings**.
2. Press the **About** option.



Settings

AudioCodes Ltd

About

Device settings

Reboot the Device

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

➢ **To reboot:**

1. Navigate to ‘Settings’ (see Access User Settings on page 12).
2. Under ‘User’, tap **Reboot**.
3. Tap .
4. Confirm the reboot.

5 Admin Settings

Admin Settings are IT level settings that require admin login prior to access (see Accessing Admin Settings). These settings are set up with initial default values. Admins can view or modify them to suit their enterprise requirements.

- Configure the Display on page 19
- Set Date and Time on page 20
- Configure Wi-Fi on page 21
- Configure Power Saving on page 24
- Configure UI Language and Input on page 25
- Modify IP Network Settings on page 25
- Enroll Certificates using SCEP on page 33
- Provision Certificates in .pfx Format on page 34

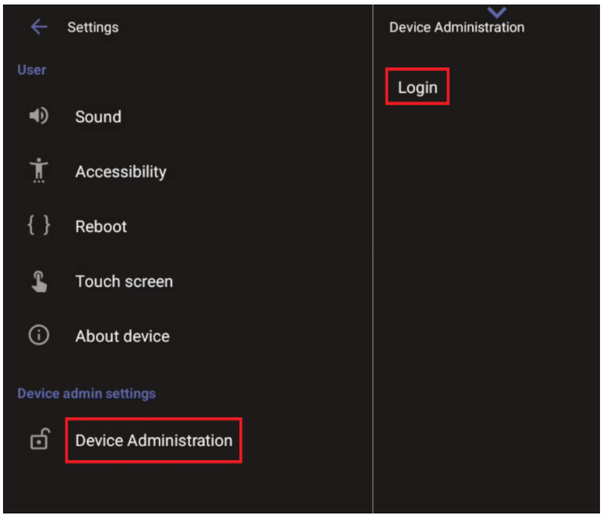
Access Device Admin Settings

To view and access Device Admin settings, you need to be logged into Device Administration (see Log in to Device Administration below).

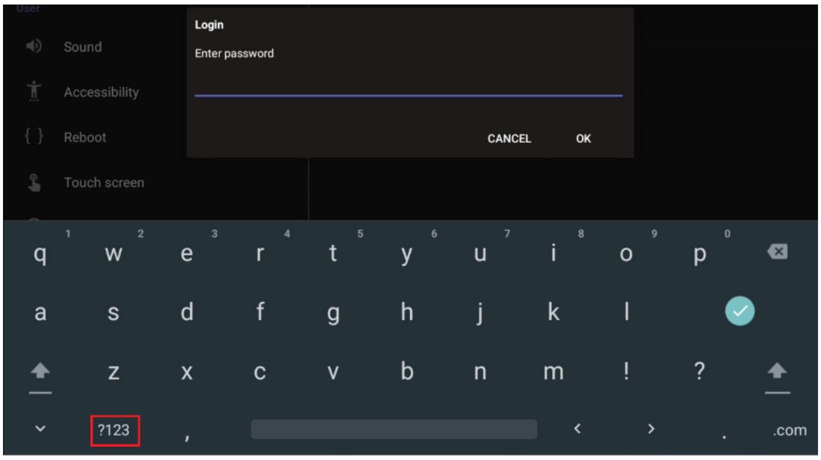
Log in to Device Administration

➢ To log into Device Administration:

1. Navigate to the 'Settings' page (see Access User Settings on page 12).
2. Under ‘Device Admin Settings’, tap **Device Administration**, then tap **Login**.



3. Enter the password using the virtual keyboard, then tap **OK**.



Login

Enter password

CANCEL OK

⚠ 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. To switch between these types, use the **?123** / **ABC** toggle key.

Upon successful login, the available device admin options appear under 'Device Administration' and can be set as required. If you log out or the admin login timeout has passed, the admin options disappear.

⚠ Upon initial login, you are required to change the default password (which is **1234**).

Brute Force Protection for Admin Password

After 5 consecutive wrong login attempts, retry is blocked during a period of 1 minute. This period increases with the number of failed attempts to 5, 10, and 15 minutes.

Failed logins can be at the UI and SSH levels and are added up together for both. For example, 2 wrong passwords at the UI level and 1 wrong password for SSH access are counted as 3 attempts.

Change the Admin Password

➢ Default Password Change at Initial Login

Upon initial login, you are prompted to change the password using the virtual keyboard. The new password must follow the following conventions:

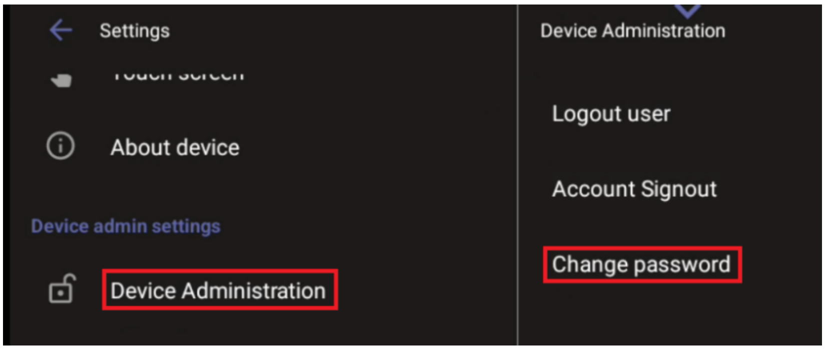
- The password length must be greater than or equal to 8.
- The password must contain one or more uppercase characters.
- The password must contain one or more lowercase characters.
- The password must contain one or more numeric values.
- The password must contain one or more special characters.

- 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.

➢ **Subsequent Password Changes**

You can change the Admin password at any time. To do this:

1. Log in as Admin with the current password.
2. Tap **Device Administration**, then tap **Change Password**, and specify the new password.



Show or Hide Password Characters While Typing

By default, when the login password is typed in, the characters are briefly displayed. To not display the characters:

1. If not already logged in, log in to Device Administration to get admin access (see Log in to Device Administration on page 16).
2. Under 'Device Admin Settings', scroll down and tap **Security**.
3. Tap the **Show passwords** toggle option to turn it off (or back on).

Configure the Admin Login Timeout

The Admin login timeout can be configured using the following cfg configuration file parameter:

```
settings/admin_logout_timeout,values=3
```

- Default: 3 (minutes)
- Valid values: 1-10 (minutes)

- Timing begins when exiting the 'Device Settings' menu.
- When the timeout expires, the device logs out automatically.
- The functionality works for both registered and unregistered devices.

➢ Manual Logout

When logged in to Device Administration, you can manually log out to instantly return the MTRA to non-admin mode:

1. On the RX-PAD, under ‘Device admin settings’, tap **Device Administration**.
2. Tap **Logout User** and then confirm.

Sign out

You can also sign out of the (Teams) and optionally sign back in with another account.

➢ To sign out:

1. Under ‘Device admin settings’, tap **Device Administration**.
2. Tap **Account Signout** and then confirm.

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

➢ To sign out of the MTRA using Microsoft TAC:

- Navigate to the 'Devices' > 'Teams Rooms' screen. From the **…** menu located in the uppermost right corner of the screen, select **Actions** and then **Sign out**.

Configure the Display

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

➢ To configure Display settings:

1. If not already logged in, log in to Device Administration to get admin access (see Log in to Device Administration on page 16).
2. Under ‘Device admin settings’, scroll down and tap **Display**.
3. To decrease or increase screen brightness, tap the **Brightness level** scale.
4. To set the screen timeout, tap **Screen timeout**. Tap the option of your choice and then tap ← to go back to the previous screen.
5. To set or deactivate a screen saver, tap **Screen saver**.
   - To activate or deactivate the screen saver, tap the **Off** toggle.

- To specify the screen saver display, tap **Current screen saver**, then select the requested screen saver and tap ← to go back.

Set Date and Time

➢ To configure Date & Time settings:

1. If not already logged in, log in to Device Administration to get admin access (see Log in to Device Administration on page 16).
2. Under 'Device admin settings', scroll down and tap **Date & Time**.
3. Adjust according to your preferences.

➢ Configuring time zones on Teams devices

> ⚠
> - AudioCodes recommends using Geolocation (the default setting) as the time zone configuration method.
>
>   With Geolocation, if no other changes to the time zone settings are made, the device retrieves the time from its geographical location.
> - Manual time zone setting is **NOT** recommended. Choosing a time zone manually may cause retrieval of the incorrect time zone, and cause functionality issues.

You can configure the time zone using one of the following methods, which are listed in order of preference for best performance:

- **Geolocation (Default):**
  - The default geolocation method uses a device's public IP address to obtain its location. If the devices are behind NAT, they use a STUN server to discover their public IP addresses.
  - A common STUN server example is Google's publicly accessible server: stun.l.google.com:19302 (default URL).
- **DHCP Option 100/101 (posix/tzdbx):**
  - Configuration is obtained from DHCP server (once defined as available).
- **Admin Provisioning:**

  Use one of the following:
  - Device Manager, created in configuration parameters setup.
  - AudioCodes Device Manager supports provisioning of the device's language, and date and time setting.

The supported parameters for Device Manager configuration can be found in product specific Admin and User guides. For Teams Admin Center, see the relevant Microsoft documentation on creating a configuration profile.

Configure Wi-Fi

The RX-PANEL device can connect to an Access Point via Wi-Fi.

Network administrators can configure Wi-Fi parameters for the device. The parameters are concealed from the user's view. Users can enable or disable Wi-Fi in the device's user interface.

⚠ Wi-Fi *cannot* be enabled or 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.

Connect to an Available Wi-Fi Network

⚠ 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.

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

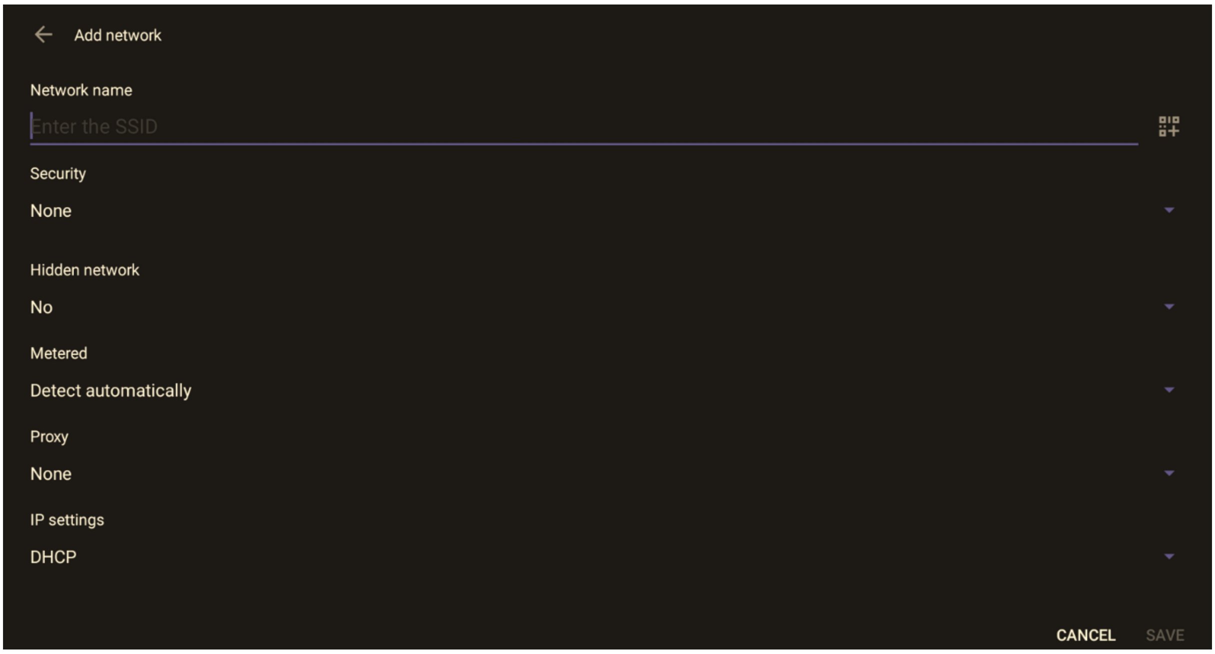
1. If not already logged in, log in to Device Administration to get admin access (see Log in to Device Administration on page 16).
2. Under 'Device admin settings', scroll down and tap **Wi-Fi**.
3. Activate **Use Wi-Fi** and then view a list of available connections.
4. Select the Wi-Fi network you want and then use the virtual keyboard displayed to enter the password.

Connect Manually to a Wi-Fi Network

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

1. **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.**
2. If not already logged in, log in to Device Administration to get admin access (see Log in to Device Administration on page 16).
3. Under 'Device admin settings', scroll down and tap **Wi-Fi**.
4. Tap **Add network** and then enter the SSID of the network to add manually.
5. From the 'Security' drop-down, select a security key strength (encryption method). For certificate based authentication, see also Configure Wi-Fi Security with Certificate-based Authentication on page 24.
6. Tap **Advanced options** and 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.



Network name

Enter the SSID

Security

None

Hidden network

No

Metered

Detect automatically

Proxy

None

IP settings

DHCP

- '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 the following table, using the Configuration File.

Table 5-1: Configuration File Wi-Fi Parameters

Parameter	Description
network/wireless/adavanced_ options/dns1	Defines the IP of the wireless DNS1.
network/wireless/adavanced_ options/dns2	Defines the IP of the wireless DNS2.
network/wireless/adavanced_ options/gateway	Defines the IP address of the wireless gateway
network/wireless/adavanced_ options/hidden_network	Defines the name of the wireless hidden network.
network/wireless/adavanced_ options/ip_addr	Defines the IP address of the static Wi-Fi network if you're operating with a static Wi-Fi

Parameter	Description
	network.
network/wireless/adavanced_ options/ip_settings	Used to define DHCP.
network/wireless/adavanced_ options/network_prefix_length	Defines the network prefix length to be used.
network/wireless/adavanced_ options/proxy	Defines the proxy wireless server source.
network/wireless/adavanced_ options/proxy/auto_config/pac_url	Defines the URL of the PAC file.
network/wireless/adavanced_ options/proxy/manual/exclusion_list	Defines the list of IP addresses that will be blocked.
network/wireless/adavanced_ options/proxy/manual/proxy_ hostname	Defines the name of the proxy host.
network/wireless/adavanced_ options/proxy/manual/proxy_port	Defines the proxy port.
network/wireless/anon_identity	Defines the anonymous wireless users who won't be seen.
network/wireless/ca_cert	Defines which CA certificate to use.
network/wireless/client_cert	Defines which client certificate to use.
network/wireless/domain	Defines the domain name.
network/wireless/eap_method	Defines the EAP method.
network/wireless/identity	Defines the identity of the user.
network/wireless/password	Defines the password of the network.
network/wireless/phase2_method NONE,MSCHAPV2,GTC,PAP,MSCHAP	Defines the encryption method. Phase 2 applies only to the 802.1x EAP method.
network/wireless/security	Defines the security method (encryption protocol).

Configure Wi-Fi Security with Certificate-based Authentication

To configure a Wi-Fi network using certificate-based authentication (**EAP-TLS**), administrators must first load the required certificates into the device. This includes the **client certificate** and its associated **private key**. Certificates can be loaded either manually or via provisioning, using the following parameters:

```
security/device_certificate_url=
security/device_private_key_url=
security/CA certificate/0/uri=
```

Once the certificates are loaded, the administrator can configure a secure Wi-Fi connection via the user interface under **Wi-Fi menu > Add Network** (see Connect Manually to a Wi-Fi Network on page 21).

To use **EAP-TLS** for authentication, configure the following parameters:

```
network/wireless/eap_method=TLS
network/wireless/ca_cert=
network/wireless/client_cert=
```

➢ Example Configuration

The following is an example of the Wi-Fi configuration using EAP-TLS:

```
network/wireless/ssid=RAX10-2.4G-5G
network/wireless/security=802.1x_EAP
network/wireless/eap_method=TLS
network/wireless/phase2_method=NONE
network/wireless/ca_cert=SYSTEM
network/wireless/domain=Cisco
network/wireless/client_cert=USRPKEY_device_crt
network/wireless/identity=ipp
```

Configure Power Saving

You can configure the device to turn off its LED during off-work hours, thereby consuming minimum power.

➢ To configure Power Saving:

1. If not already logged in, log in to Device Administration to get admin access (see Log in to Device Administration on page 16).
2. Under ‘Device admin settings’, scroll down and tap **Power Saving**.

3. Enable power saving and then specify work start and end times.

   During work time, the device LED will be on (no power saving).

   Before the **Start Time** and *after* the **End Time**, its LED will be turned off.

Configure UI Language and Input

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

➢ **To set language and input:**

1. If not already logged in, log in to Device Administration to get admin access (see Log in to Device Administration on page 16).
2. Under ‘Device admin settings’, scroll down and tap **Languages & input**.
3. Adjust as required:
   - Tap **Languages** to change the UI language.
   - Tap **On-screen keyboard** to adjust the default Android Keyboard or add an on-screen keyboard. To adjust the keyboard, click it and configure settings under ‘Preferences’ and ‘Advanced’ as required.
   - Tap **Physical keyboard** to connect a physical keyboard. You can specify whether the physical keyboard should connect in addition to the physical keyboard or replace it.
   - Tap **Text-to-speech output** to adjust its speech rate and pitch.

Modify IP Network Settings

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

➢ **To modify network settings:**

1. If not already logged in, log in to Device Administration to get admin access (see Log in to Device Administration on page 16).
2. Under ‘Device admin settings’, scroll down and tap **Modify network**.
3. Perform the required action or actions:
   - View **IP address** and **Network state** (read-only).
   - Click **IP settings** to set to **DHCP** or **Static**.
   - Set up a proxy (see Set up a Proxy Server on the next page).
   - Configure 802.1x settings (see Configure 802.1x Settings on the next page).
   - Configure VLAN settings (see Configure VLAN Settings on page 29).

Set up a Proxy Server

Administrators can manually configure the with an HTTP proxy server:

1. Navigate to 'Modify network' (see Modify IP Network Settings on the previous page) and tap **Proxy**.
2. Fill in the **Proxy hostname**, **Proxy port**, and optionally the bypass IP address.
3. Select **DONE**.

Configure 802.1x Settings

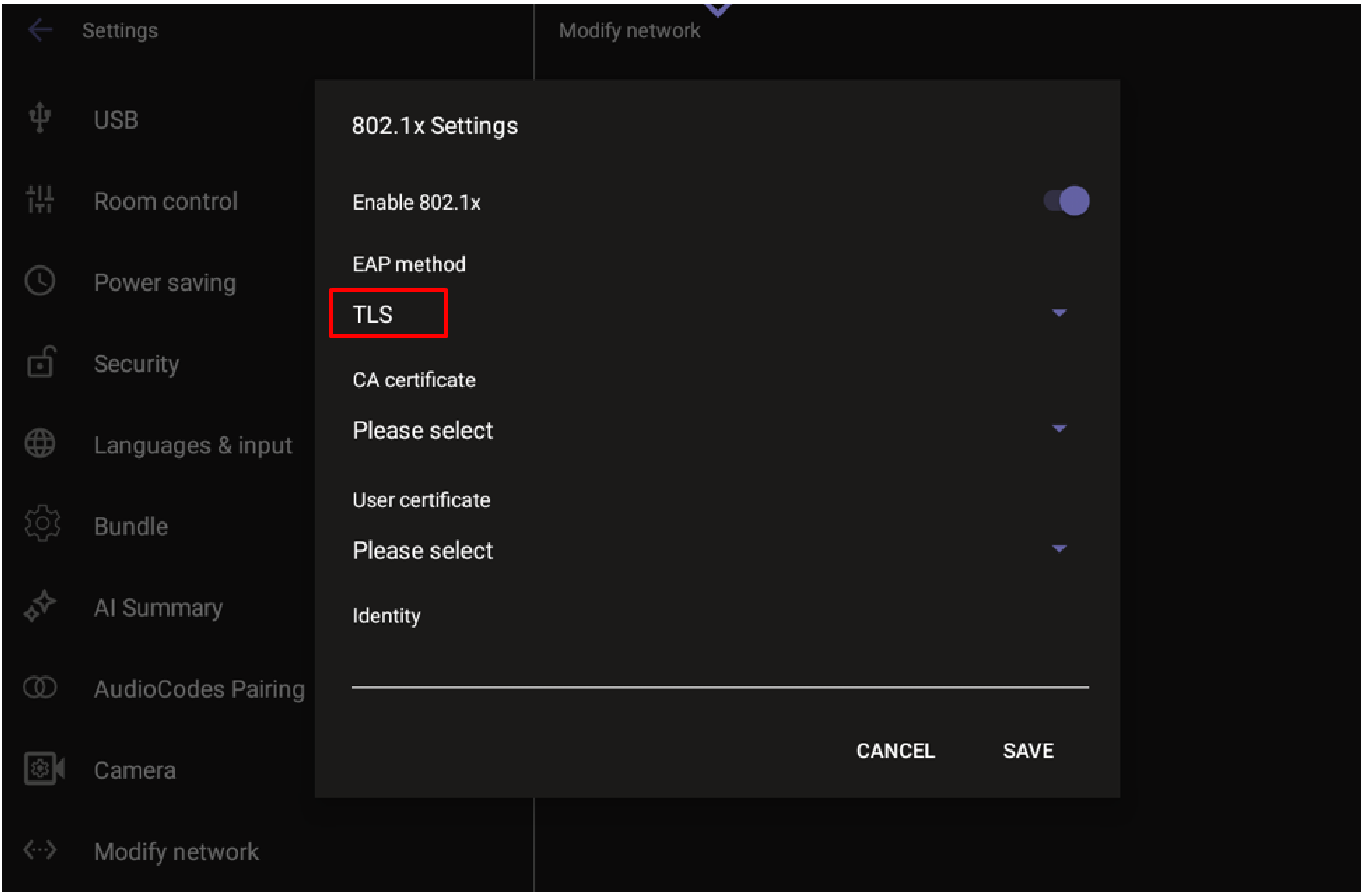
802.1x Authentication is the IEEE Standard for Port-based Network Access Control (PNAC) (refer to https://1.ieee802.org/security/802-1x/ for more information). It is used to enable port-based authentication.

⚠ Instead of performing the following steps, 802.1x Authentication can be enabled and predefined via provisioning, by setting the following parameters:

```
network/lan/_802_1x/status=true or false
network/lan/_802_1x/eap_tls/ca_cert=<CA FILE NAME>
network/lan/_802_1x/eap_tls/client_cert=<Client certificate
file name>
network/lan/_802_1x/eap_tls/identity=<identity name>
network/lan/_802_1x/eap_type=eap_tls
```

➢ To configure 802.1x settings:

1. Navigate to 'Modify network' (see Modify IP Network Settings on the previous page) and select **802.1x Settings**.
2. Tap **Enable 802.1x** and then tap **Save**.
3. Once 802.1x is enabled, choose the security method and strength. A commonly used option is EAP-TLS.



802.1x Settings

Enable 802.1x

EAP method

TLS

CA certificate

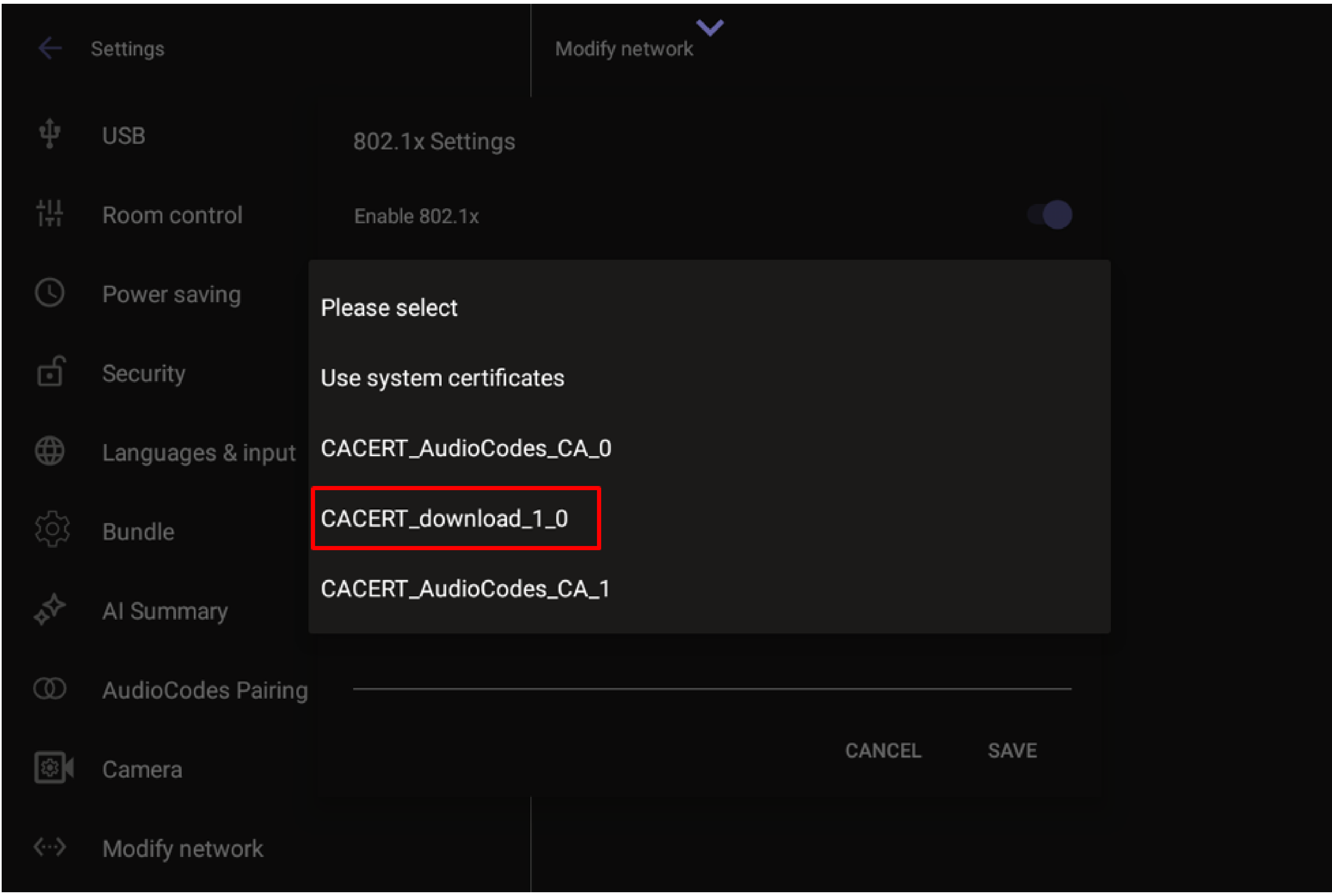
Please select

User certificate

Please select

Identity

4. Next, select the certificate source. The device can use either system certificates or certificates previously uploaded by an administrator, which will appear in the certificate list.



Settings

Modify network

USB

Room control

Power saving

Security

Languages & input

Bundle

AI Summary

AudioCodes Pairing

Camera

Modify network

802.1x Settings

Enable 802.1x

Please select

Use system certificates

CACERT_AudioCodes_CA_0

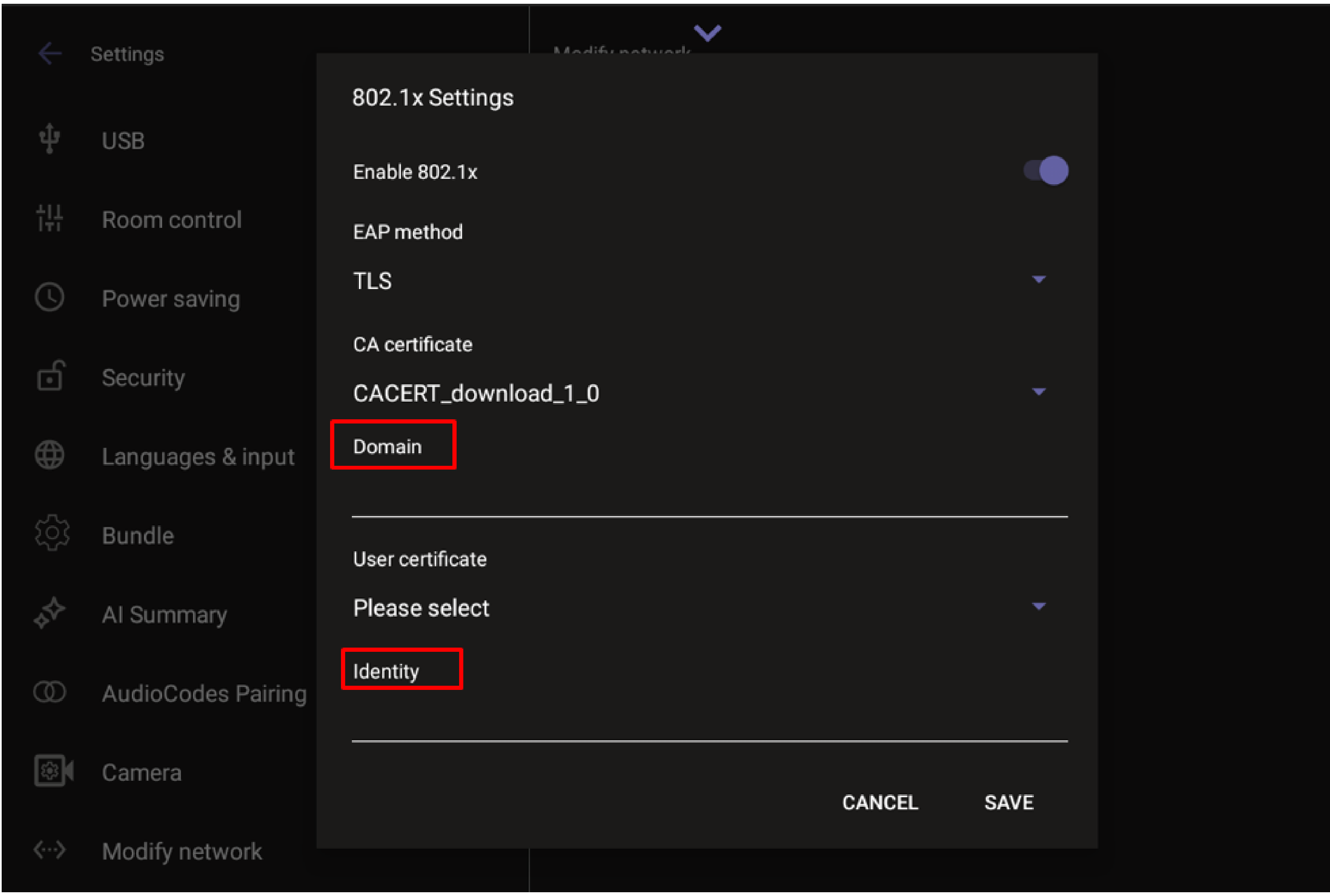
CACERT_download_1_0

CACERT_AudioCodes_CA_1

CANCEL SAVE

5. After selecting the appropriate certificate file, set the following:

   - **Identity** – the device identity used during authentication.
   - **Domain** – the domain the device is intended to join.



802.1x Settings

Enable 802.1x

EAP method

TLS

CA certificate

CACERT_download_1_0

Domain

User certificate

Please select

Identity

6. Click **Save** once all fields have been defined.

Configure VLAN Settings

Administrators can configure the VLAN discovery mode. If the mode is automatic, a time interval for running VLAN must be set.

➢ To configure VLAN:

1. Navigate to ‘Modify network’ (see Modify IP Network Settings on page 25) and select **VLAN Settings**.
2. Select the requested VLAN Discovery mode, then tap **OK**:
   - Disabled (no VLAN)
   - Manual configuration
   - Automatic configuration through:
     - CDP (Cisco Discovery Protocol), which is a proprietary Data Link Layer protocol
     - LLDP (Link Layer Discovery Protocol), which is a standard layer 2 discovery protocol

- Both CDP and LLDP

3. If you selected an automatic configuration, set the requested periodic **VLAN Interval** between CDP/LLDP advertisements. Default is 30 seconds.

You can increase or decrease the intervals between the CDP/LLDP packets that are sent, based on network traffic and topology.

⚠ 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.

Starting from version 1.19, this VLAN and LLDP switch information is retrieved when the parameter network/lan/lldp/enabled=**1**. This is true even if VLAN is retrieved from **CDP**, or if VLAN is disabled or **Manual**.

Enroll a Device with Intune Policies

Admins can enroll AudioCodes Teams Android-based devices in Intune in either of the following ways:

- By Create a Dynamic Group below
- By Create an Exclusion Group below

An enrolled device can be removed from Intune (see Remove Devices from Intune Admin Center on the next page).

Create a Dynamic Group

See the AudioCodes Device Enrollment in Microsoft Endpoint Manager to learn how to create dynamic groups in Intune for enrolling AudioCodes Android- based Teams devices.

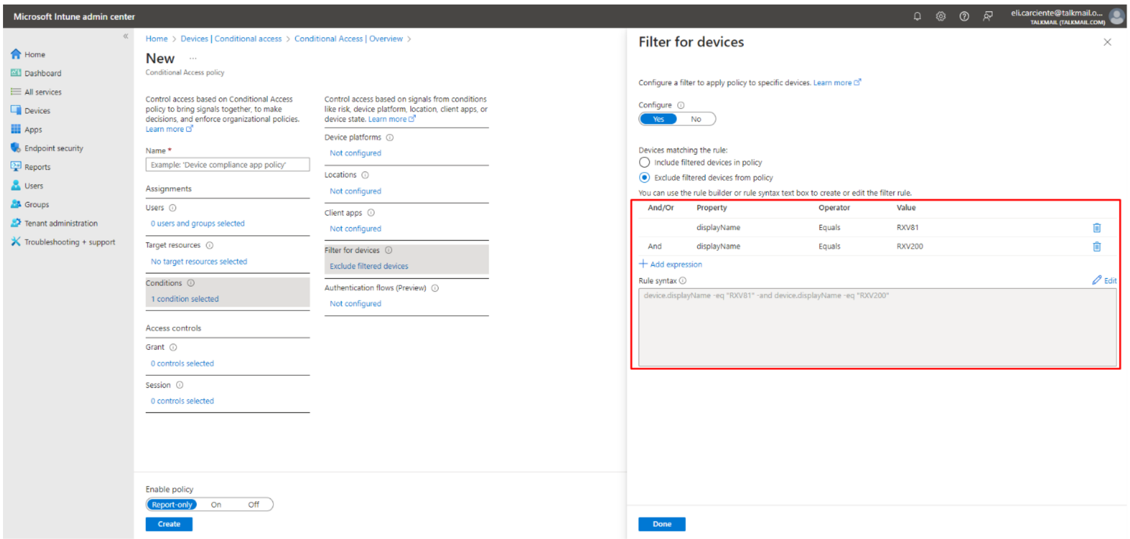
Create an Exclusion Group

The information presented here shows how to exclude AudioCodes Android- based Teams devices from the organization's Intune policies.

➢ **To exclude devices from the organization's Intune policies:**

Remove all conditions that were previously configured:

1. Access Microsoft Azure Government Portal Home > Conditional Access Policies > Require Hybrid Joined or Intune to Access Cloud Resources Conditional Access policy as shown in the following figure.
2. Exclude the device from Intune policies and replace **displayName -contains RXVxx** where RXVxx is the name of the device model (device.model).



Microsoft Intune admin center
Home
Dashboard
All services
Devices
Apps
Endpoint security
Reports
Users
Groups
Tenant administration
Troubleshooting + support
Home > Devices | Conditional access > Conditional Access | Overview >
New
Conditional Access policy
Create
Done

Filter for devices

Configure a filter to apply policy to specific devices. Learn more

Configure: [✓ Yes] No

Devices matching the rule:
○ Include filtered devices in policy
● Exclude filtered devices from policy

You can use the rule builder or rule syntax text box to create or edit the filter rule.

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

Rule syntax

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

Filter for devices: Exclude filtered devices

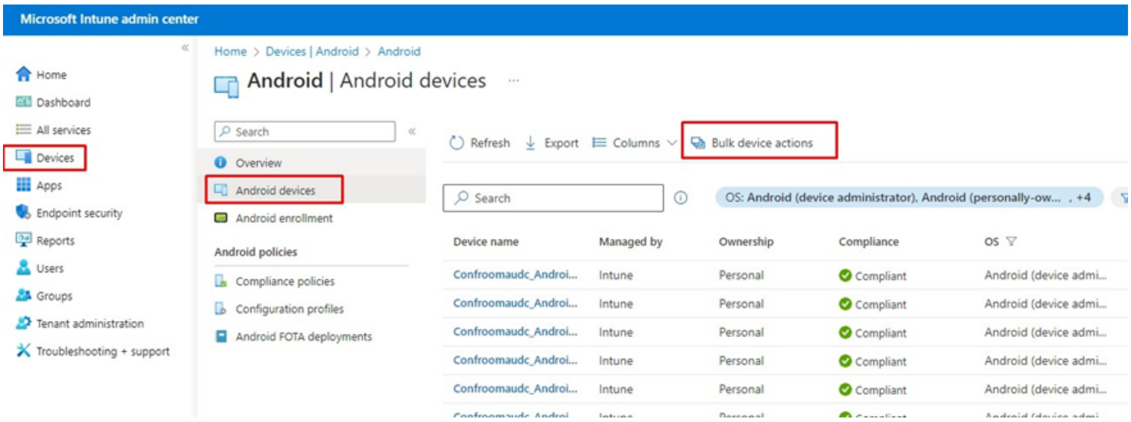
Enable policy: [✓ Report-only] On Off

Remove Devices from Intune Admin Center

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

➢ To remove devices from Intune admin center:

1. Go to Microsoft 365 admin center (portal.office.com) and log in with an Administration account.
2. Navigate to **Devices > Android devices**.

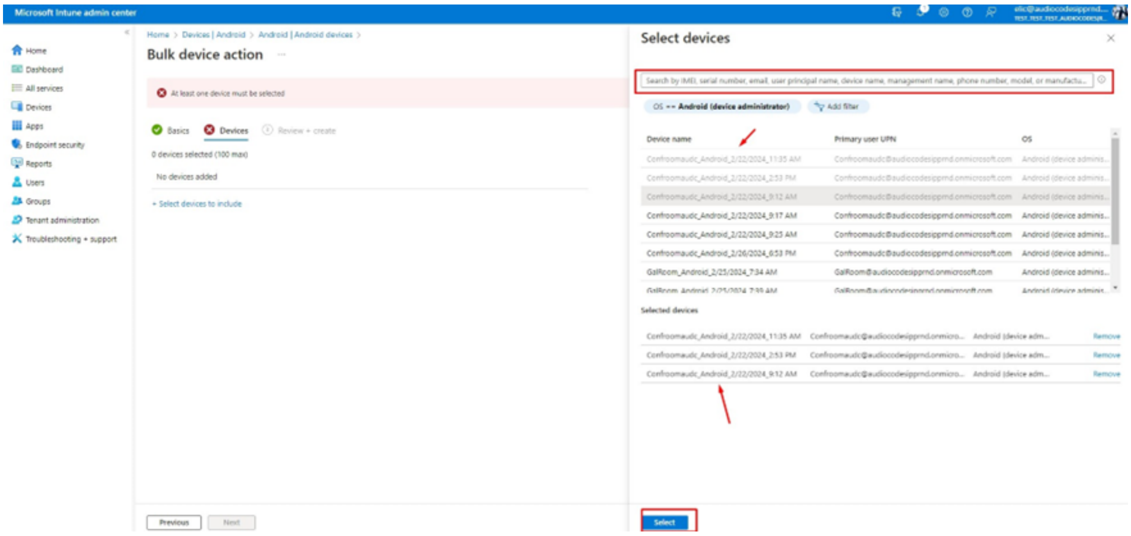


OS: Android (device administrator), Android (personally-ow... , +4

Device name	Managed by	Ownership	Compliance	OS
Confroomaudc_Androi...	Intune	Personal	Compliant	Android (device admi...
Confroomaudc_Androi...	Intune	Personal	Compliant	Android (device admi...
Confroomaudc_Androi...	Intune	Personal	Compliant	Android (device admi...
Confroomaudc_Androi...	Intune	Personal	Compliant	Android (device admi...
Confroomaudc_Androi...	Intune	Personal	Compliant	Android (device admi...

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

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



Bulk device action

At least one device must be selected

0 devices selected (100 max)

No devices added

Select devices

Search by IMEI, serial number, email, user principal name, device name, management name, phone number, model, or manufactu...

OS == Android (device administrator)

Device name	Primary user UPN	OS
Confroomaudc_Android_2/22/2024_11:35 AM	Confroomaudc@audiocodesipprnd.onmicrosoft.com	Android (device adminis...
Confroomaudc_Android_2/22/2024_2:53 PM	Confroomaudc@audiocodesipprnd.onmicrosoft.com	Android (device adminis...
Confroomaudc_Android_2/22/2024_9:12 AM	Confroomaudc@audiocodesipprnd.onmicrosoft.com	Android (device adminis...
Confroomaudc_Android_2/22/2024_9:17 AM	Confroomaudc@audiocodesipprnd.onmicrosoft.com	Android (device adminis...
Confroomaudc_Android_2/22/2024_9:25 AM	Confroomaudc@audiocodesipprnd.onmicrosoft.com	Android (device adminis...
Confroomaudc_Android_2/26/2024_6:53 PM	Confroomaudc@audiocodesipprnd.onmicrosoft.com	Android (device adminis...
GalRoom_Android_2/25/2024_7:34 AM	GalRoom@audiocodesipprnd.onmicrosoft.com	Android (device adminis...
GalRoom_Android_2/25/2024_7:39 AM	GalRoom@audiocodesipprnd.onmicrosoft.com	Android (device adminis...

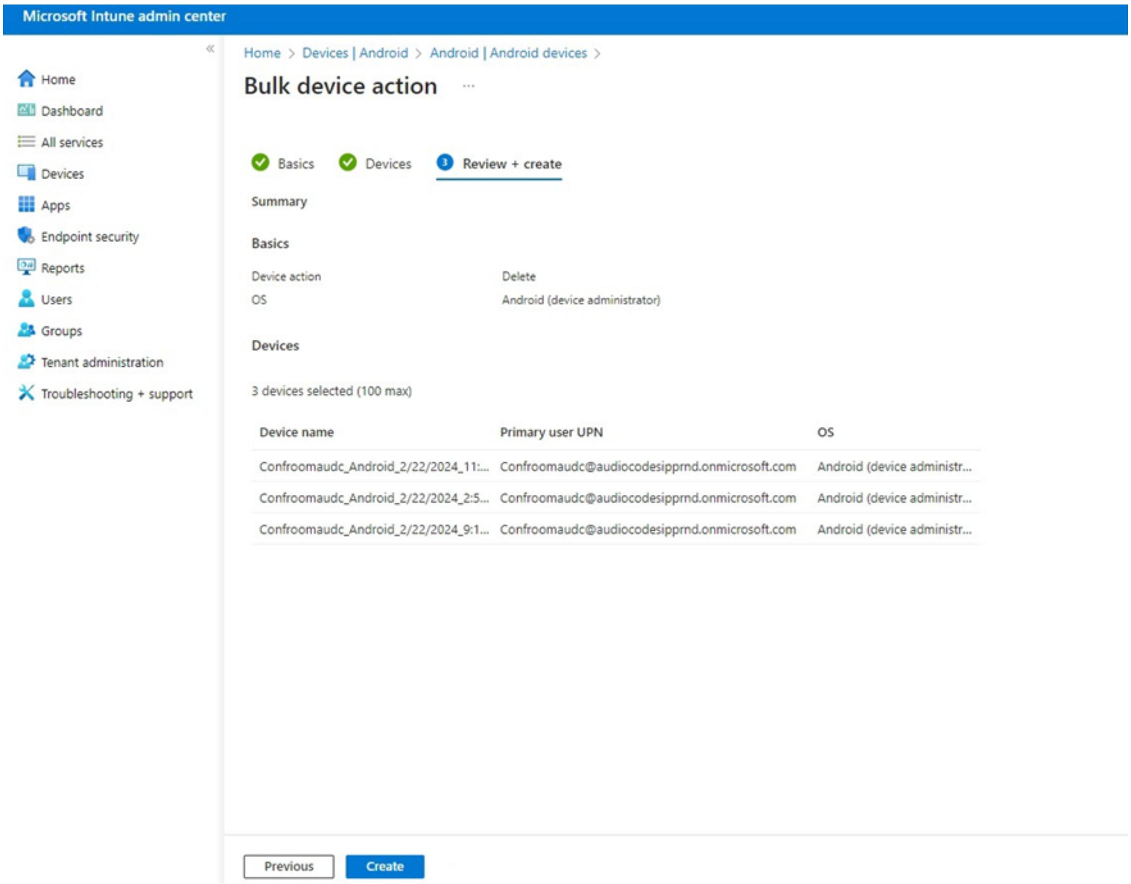
Selected devices

Confroomaudc_Android_2/22/2024_11:35 AM	Confroomaudc@audiocodesipprnd.onmicro...	Android (device adm...	Remove
Confroomaudc_Android_2/22/2024_2:53 PM	Confroomaudc@audiocodesipprnd.onmicro...	Android (device adm...	Remove
Confroomaudc_Android_2/22/2024_9:12 AM	Confroomaudc@audiocodesipprnd.onmicro...	Android (device adm...	Remove

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

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

7. Under the **Review + Create** tab, make sure your definitions are correct and then click **Create**.



Bulk device action

Summary

Basics

Device action	Delete
OS	Android (device administrator)

Devices

3 devices selected (100 max)

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

8. Admin receives a notification that a delete action from Intune was successfully initiated on all devices and that n devices were removed.

It may take some time to completely sync the devices with the account. After deleting the devices, wait for 30 minutes before signing in.

Enroll Certificates using SCEP

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

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

Network administrators must configure the following three parameters:

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

The following table shows the SCEP parameter descriptions.

Parameter	Description
security/SCEPEnroll/ca_fingerprint	Define the thumbprint (hash value) for the CA certificate. Default value: `NULL` Network admins must set its value as in the following example: `3EBE50003ABF1DF5E6B5A3230B02B856`
security/SCEPEnroll/password_challenge	Define the enrollment challenge password. Default value: `NULL` Network admins must set its value as in the following example: `7A7F9FC4BB7625F0935E67EA6D6322ED`
security/SCEPServerURL	Define the NDES server’s URL. Default: `NULL` Network admins must set its value as in the following example: `https://ndes_derver`
security/SCEPEnroll/renewal/advancethres	Define the renewal advance threshold of

Parameter	Description
hold	the device certificate. Configure between 50 and 100 (in units of percentage). Default: `80` The default value 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` The default value indicates a renewal of the certificate (CAROOT.crt.) will be initiated when 90 percent of its validity is reached.

Provision 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.

- 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.

Update RX-PANEL Remotely

For instructions on how to update the device remotely, refer to https://docs.microsoft.com/en-us/microsoftteams/devices/remote-update.

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.

During the update, notifications are displayed, indicating the device being updated and alerting the user not to reboot.

If prompted, tap **OK** to confirm the alert.

6 System Monitoring and Debugging

From the 'Debugging' page on the RX-PAD, Admin users can perform system monitoring and debugging for troubleshooting purposes.

➢ **To access the 'Debugging' page:**

1. If not already logged in, log in to Device Administration to get admin access (see Log in to Device Administration on page 16).
2. Navigate to ‘Device Admin Settings’ (see Access Device Admin Settings on page 16).
3. Scroll down and tap **Debugging**.

The 'Debugging' page gives you various options for monitoring performance and debugging issues:

- Monitor the System Status below
- Enable Remote Logging on page 38
- Copy Diagnostic Data to SD Card on page 38
- Reset the System Configuration on page 39
- Reset User Data on page 40
- Perform Debug Recording on page 41
- Control Screen Capture on page 41
- Return to Previous Version on page 42

Additional procedures for device monitoring and troubleshooting are:

- Performing Recovery Operations using the Power Button
- Restoring RXV200 Firmware via USB Disk

⚠ Additionally:

- An enhanced bug report is available for efficient debugging. This report, which can be extracted via the Device Manager or manually from the device, contains information such as pack up time metrics and output of `ps`, `top`, `meminfo`, and `df` commands. (The `df` commands retrieve information about file system disk space usage).

Monitor the System Status

Admins can monitor the state of the device’s modules from the System State screen. This screen can indicate the reason for unsuccessful initial provisioning, network related issues, or Device Manager connection issues.

System State monitoring enables debugging via the device’s screen *without requiring external systems*. The admin can check connectivity *independently of external apps*.

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

➢ To monitor the device’s module states:

1. Access the 'Debugging' page (see System Monitoring and Debugging on the previous page).
2. Scroll down and tap **System State**, then scroll down to the requested information.

Configure Log Settings for 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 issues related to the device.

➢ To configure log settings:

1. Access the 'Debugging' page (see System Monitoring and Debugging on the previous page).
2. Tap **Log settings**.
3. Tap **Log Level** and then select either **Verbose**, **Debug**, **Info**, **Warning**, **Error**, **Assert** or **None**.
4. Tap **Log Package Filter** and enter the filter.
5. Tap **Log Tag Filter** and enter the filter.
6. Tap **Log Buffer Filter**.
7. Tap **Current filter for logs**.

➢ To collect logs:

1. Reproduce the issue.
2. Access the Microsoft Admin Portal and under the **Devices** tab click the **Diagnostics** icon.
3. Click the **Diagnostics** icon 🗋 and click **Proceed** in the upcoming dialog to confirm. The logs are uploaded to the server:
4. Click the **History** tab.
5. Click **Download** to download the logs.

Enable 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 SD-card and collected after the event. Remote Logging via Syslog is different. The logs are collected in real time.

⚠ Network administrators can also enable Syslog using Secure Shell (SSH) protocol.

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

1. Access the 'Debugging' page (see System Monitoring and Debugging on page 36).
2. Tap **Remote logging**.
3. Configure the **Remote IP address** and **Remote port** and enable **Remote Logging**; the device starts sending logs to the Syslog server.

➢ **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 ""
```

Copy Diagnostic Data to SD Card

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. Access the 'Debugging' page (see System Monitoring and Debugging on page 36).
2. Tap **Diagnostic Data**.
3. Tap **OK** to confirm 'Copy logs to sdcard'; the device creates all necessary logs and copies them to the **SD Card/Logs** folder.
4. 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

Reset the System Configuration

Administrators can use one of the following reset methods depending on the issue:

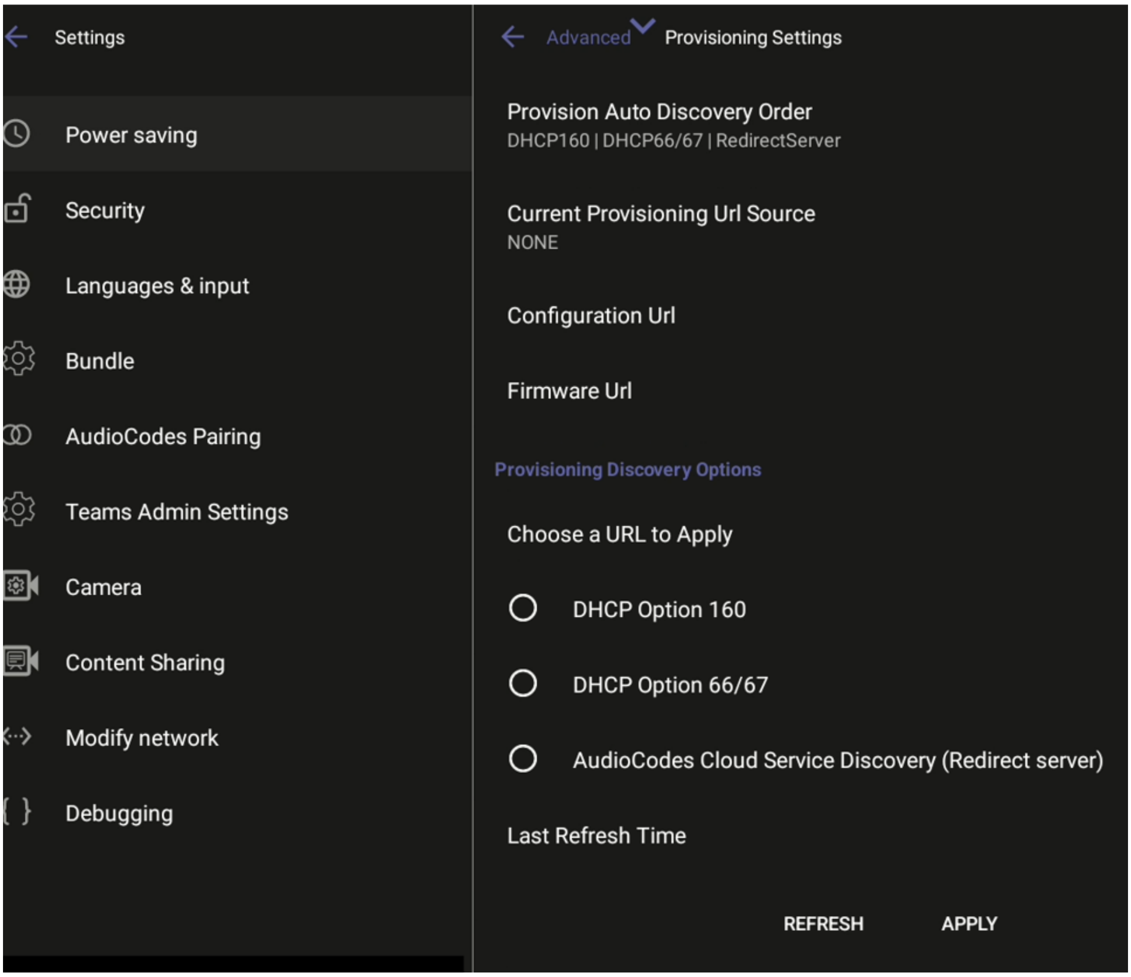
- Configure Provisioning Source Auto Discovery Settings below
- Perform a Full Factory Reset on the next page

Configure Provisioning Source Auto Discovery Settings

Admins can select the preferred discovery option for the RX-PANEL without affecting other devices in the network. This action restarts the device but does *not* perform a factory reset.

➢ **To set up provisioning source discovery:**

1. Access the 'Debugging' page (see System Monitoring and Debugging on page 36).
2. Tap **Advanced**, then **Provisioning Settings**. The page displays the current order for provisioning auto discovery, as well as the URL locations of the provisioning, configuration, and firmware sources.



Settings

Power saving

Security

Languages & input

Bundle

AudioCodes Pairing

Teams Admin Settings

Camera

Content Sharing

Modify network

Debugging

Advanced Provisioning Settings

Provision Auto Discovery Order
DHCP160 | DHCP66/67 | RedirectServer

Current Provisioning Url Source
NONE

Configuration Url

Firmware Url

Provisioning Discovery Options

Choose a URL to Apply

○ DHCP Option 160

○ DHCP Option 66/67

○ AudioCodes Cloud Service Discovery (Redirect server)

Last Refresh Time

REFRESH APPLY

3. Select the desired discovery option for the device and click **APPLY**. After restarting, the device will use the selected option for provisioning. If no provisioning source is discovered, the system will use an alternate discovery option based on the Discovery Order setting.
4. To update the page with the latest changes and locations, click **REFRESH**.

Perform a Full Factory Reset

This option is the equivalent of restoring to defaults, including logout and device reboot.

➢ To erase all data (factory reset):

1. Access the 'Debugging' page (see System Monitoring and Debugging on page 36).
2. Tap **Erase all data (factory reset)**, then tap **OK** to confirm.

Reset User Data

This function resets all user-defined settings that are not admin settings, such as brightness, contrast, fonts, etc.

The user is signed out after performing this operation.

Restart the 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:

1. Access the 'Debugging' page (see System Monitoring and Debugging on page 36).
2. Tap **Restart Teams App**; only the Teams app is restarted.

Perform Debug Recording

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

> ⚠ DSP recording can be activated on the fly without requiring the network administrator to reset the device.

➢ To set up recording:

1. Access the 'Debugging' page (see System Monitoring and Debugging on page 36).
2. Tap **Debug Recording**, then tap **Voice record** to enable the feature.
3. Tap **Remote IP address** to input the IP address of the device whose traffic you want to record.
4. Tap **Remote port** and input it (Default: 50000).
5. Start Wireshark on your PC to capture audio traffic.

Control Screen Capture

By default, Screen Capture is enabled (using AudioCodes' SSH protocol based Android Device Utility or the Device Manager). If disabled, the phone won't allow its screens to be captured.

➢ To enable or disable screen capture:

1. Access the 'Debugging' page (see System Monitoring and Debugging on page 36).
2. Scroll down and turn the **Screen Capture** toggle button on or off.

Control Remote Package Capture

If SSH is enabled, admins can capture traffic packages using the ‘rpcapd’ (Remote Packet Capture) network sniffer application, which allows them to analyze and debug Android traffic on their desktop PC using the app's integral SSH server.

By default, Remote Package Capture is disabled. You can enable it to allow capturing of remote packages.

➢ **To enable or disable remote package capture:**

1. Access the 'Debugging' page (see System Monitoring and Debugging on page 36).
2. Scroll down and turn the **Remote Package Capture** toggle button on or off.

Return to Previous Version

When a customer receives a build for testing and completes the testing, they must switch back to the previous firmware version. This version is the General Availability build running on the device.

➢ **To return to the previous version:**

1. Access the 'Debugging' page (see System Monitoring and Debugging on page 36).
2. Tap **Return to previous version**. The device changes the active firmware slot and undergoes a factory reset.

7 Android-based Teams Devices Parameters

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

Parameter	Possible Values	Default Value
general/power_saving	**0** or **1**	0
phone_lock/enabled	**0** or **1**	0
phone_lock/timeout	(Number of seconds)	900
phone_lock/lock_pin	(Pin number)	123456
display/language	(Language)	English
display/screensaver_enabled	**0** or **1**	1
display/screensaver_timeout	(Number of seconds)	1800
display/backlight	(Number between 0 and 100 inclusive)	80
display/high_contrast	**0** or **1**	0
date_time/timezone	(Timezone)	(Retrieved from network)
date_time/time_format	**12** or **24**	24
network/ip_address	Manually defined by customer if needed	
network/subnet_mask		
network/default_gateway		
network/primary_dns		
network/pecondary_dns		
network/pc_port	**0** or **1**	1
office_hours/start	(Time in 24-hour XX:XX format)	08:00
office_hours/end	(Time in 24-hour XX:XX	17:00

Parameter	Possible Values	Default Value
	format)	
logging/enabled	**0** or **1**	0
logging/levels	**Verbose**, **Debug**, **Info**, **Warn**, **Error**, **Assert** or **None**	Verbose
admin/default_password		1234
admin/ssh_enabled	**0** or **1**	0
security/SSLCertificateErrorsMode	**IGNORE**, **NOTIFICATION** or **DISALLOW**	DISALLOW
security/ca_certificate/[0-4]/uri	(URI to download the customer's root CA)	User downloads, left blank by default
provisioning/period/daily/time	(Time in 24-hour XX:XX format)	0:00
provisioning/period/hourly/hours_ interval		24
provisioning/period/type	**HOURLY**, **DAILY**, **WEEKLY**, **POWERUP**, **EVERY5MIN** or **EVERY15MIN**	DAILY
provisioning/period/weekly/day		Sunday
provisioning/period/weekly/time	(Time in 24-hour XX:XX format)	0:00
provisioning/random_provisioning_ time		120

This page is intentionally left blank.

International Headquarters

6 Ofra Haza Street

Naimi Park

Or Yehuda, 6032303, Israel

Tel: +972-3-976-4000

Fax: +972-3-976-4040

AudioCodes Inc.

80 Kingsbridge Rd

Piscataway, NJ 08854, USA

Tel: +1-732-469-0880

Fax: +1-732-469-2298

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

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

Documentation Feedback: https://online.audiocodes.com/documentation-feedback

Document #: LTRT-18299