User's and Administrator's Manual

AudioCodes 400HD IP Phone Series

C470HD IP Phone

Microsoft Teams Application

Version 2.7



audiocodes

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: August-24-2026

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



Related Documentation

Document Name
Release Notes
C470HD-C455HD-C436HD-C435HD-C430HD IP Phones for Microsoft Teams Release Notes
Quick Guides
C470HD IP Phone for Microsoft Teams Quick Guide
Video Tutorials
IP Phones How To Video Tutorials
Miscellaneous
Security Guidelines for AudioCodes' Android-based Devices
Android Device Utility User's Manual
Device Manager Administrator's Manual
Device Manager Deployment Guide
https://docs.microsoft.com/en-us/MicrosoftTeams/phones-for-teams

Document Revision Record

LTRT	Description
13459	Initial document release for Version 2.7; ISED warning added; SIP fallback (emergency calling) feature when Teams unavailable; line key assignment; mandatory change of lock PIN; minimum and maximum ring volume; logging Application Not Responding (ANR) error / core dumps; disabling speakerphone; return to previous version; added note to Call Transfer
13466	Updated to Ver. 2.7.M2; Dim screen functionality updated; 802.1x authentication parameters added
13471	Updated to Ver. 2.7.M3; revised Specifications section; lock PIN change enforcement via TAC
13473	Updated to Ver. 2.7.M4; general manual revision and restructure
13478	Wall mounting text removed, not relevant for C470HD

LTRT	Description
13479	Updated to Ver. 2.7.M5

Notes and Warnings

FCC Caution

Part 15.21

Any Changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

Part 15.19

This device complies with part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

Part 15.105

Note: This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

FCC RF Radiation Exposure Statement

1. This Transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.
2. This equipment complies with RF radiation exposure limits set forth for an uncontrolled environment.
3. This equipment should be installed and operated with minimum distance 20cm between the radiator& your body.

User manuals for license-exempt radio apparatus shall contain the following or equivalent notice in a conspicuous location in the user manual or alternatively on the device or both.

[EN] This device complies with Industry Canada license-exempt RSS standard(s). Operation is subject to the following two conditions:

(1) this device may not cause interference, and

(2) this device must accept any interference, including interference that may cause undesired operation of the device.

[FR] Le présent appareil est conforme aux CNR d'Industrie Canada applicables aux appareils radio exempts de licence. L'exploitation est autorisée aux deux conditions suivantes :

(1) l'appareil nedoit pas produire de brouillage, et

(2) l'utilisateur de l'appareil doit accepter tout brouillage radioélectrique subi, même si le brouillage est susceptible d'en compromettre le fonctionnement.

[EN] 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.

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

IC SAR Warning

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

[FR] 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.

ISED Warning

[EN] Operation of 5150-5250 MHz is restricted to indoor use only.

This device complies with Innovation, Science, and Economic Development Canada licence-exempt RSS standard(s). Operation is subject to the following two conditions:

(1) this device may not cause interference, and

(2) this device must accept any interference, including interference that may cause undesired operation of the device.

Privacy of communications may not be ensured when using this phone.

[FR] Le fonctionnement de 5150-5250 MHz est limité à une utilisation en intérieur uniquement.

Le présent appareil est conforme aux CNR d' Innovation, Sciences et Développement économique Canada applicables aux appareils radio exempts de licence. L'exploitation est autorisée aux deux conditions suivantes :

(1) l'appareil nedoit pas produire de brouillage, et

(2) l'utilisateur de l'appareil doit accepter tout brouillage radioélectrique subi, même si le brouillage est susceptible d'en compromettre le fonctionnement.

La confidentialité des communications peut ne pas être garantie lors de l'utilisation de ce téléphone

Radiation Exposure Statement

[EN] The device is compliance with RF exposure guidelines, users can obtain Canadian information on RF exposure and compliance. The minimum distance from body to use the device is 20cm.

[FR] Le présent appareil est conforme Après examen de ce matériel aux conformité ou aux limites d'intensité de champ RF, les utilisateurs peuvent sur l'exposition aux radiofréquences et la conformité and compliance d'acquérir les informations correspondantes. La distance minimale du corps à utiliser le dispositif est de 20cm.

Table of Contents

1 C470HD IP Phone 1
Teams Features Supported by C470HD 2
C470HD Specifications 3
Functional Features 3
Hardware 5
Migration to Android Open Source Project (AOSP) 6
URLs and Ports (Security) to Allow for AudioCodes Teams Phones 7
Security Guidelines for Android-based Native Teams Devices 7
2 Set up the C470HD IP Phone 8
Unpack the Device 8
Explore the Device (Front and Rear Views) 9
C470HD Front View 9
C470HD Rear View 13
Connect Cables 14
Clean the Phone Screen 14
3 Start up C470HD 15
Sign In to Your device Teams Phone 15
Sign in on Your C470HD 15
Sign in from your PC or Smartphone 18
Remote Provisioning and Sign-in from Teams Admin Center (TAC) 18
Configure C470HD Device Settings 23
User-level Device Settings 25
Device Settings Configured by Administrator 28
Modify network 29
Debugging 35
Set up Accessibility 35
Enable Google Talkback 36
Configure Wi-Fi 39
Connect to an Available Wi-Fi Network 39
Manually Connect to a Wi-Fi Network 40
Set up via Configuration File 42
Configure Wi-Fi with Hidden SSID 44
Configure Wi-Fi Security Methods 44
Configure Wi-Fi TLS 44
Configure VLAN via DHCP Option when CDP-LLDP is Not Allowed 46
Lock or Unlock the Phone 47
Automatic Lock 47
Unlock 47
Enable Power Saving 50
Restore the Phone to Default Settings 51
Perform a Hard Restore 52

Perform a Soft Restore 52
Perform User Data Reset 52
Start up the Phone from Recovery Mode 53
Perform Manual Recovery Operations 54

4 Use Your Phone 56

Get Acquainted with the Phone Screen 56
Change Your Presence Status 60
Set a Status Message 61
Configure Teams Application Settings 62
Make and Manage Calls 67
Make a Call 68
Dial a Missed Call 68
Select to Dial 69
Park a Call 69
Make an Emergency Call 69
End an Established Call 71
Manage Call History 71
Set up a Phone for Hot Desking 72
Use Boss-Admin 72
Page to a Group of Phones (Multicast) 73
Answer Calls 78
Answer a Call 78
Transfer a Call 79
Transfer a Call to Frequent Contacts 79
Transfer a Call to Work Voicemail 79
Transfer Calls and Meetings across Devices 80
Reject an Incoming Call and Send It Directly to Voicemail 80
Adjust Volume 80
Adjust Ring Volume 81
Adjust Tones Volume 81
Adjust Handset Volume 81
Adjust Speaker Volume 81
Adjust Headset Volume 82
Play Incoming Call Ringing through USB Headset 82
Opt in or out of Call Queues 82
Create and Manage Contacts from the People Screen 83
Manage Speed Dial and Line Keys 84
Add a Speed Dial 85
Remove a Speed Dial 87
Add a Speed Dial Group 88
Assign a Line Key for Speed Dial or Feature 88
Manage Meetings 93
Schedule a Meeting 93
View and Join Meetings 95

Use Live Captions ... 97
Hide Names and Meeting Titles for Individual Devices ... 97
React during a Meeting ... 97
Manage Voicemail ... 97
View and Play Voicemail Messages ... 97
Enable Voicemail Support on CAP Users ... 98
Other Operations ... 99
Configure Better Together over Bluetooth ... 99
Connect a Device ... 102
Sign Out ... 103
5 Perform Administrator-Related Operations ... 105
Configure Time on Teams Devices ... 105
Set up Automatic Provisioning ... 106
Configure the Model Name in DHCP Option 60 ... 107
Log in as Administrator ... 107
Perform Password and Security Related Actions ... 108
Define Password Complexity ... 108
Configure Admin Login Timeout ... 109
Force Users to Change their Device Lock PIN Using TAC Configuration Profile ... 110
Load Certificates to Phones ... 111
Load Certificates using AudioCodes Android Device Utility ... 112
Certificate Enrollment using SCEP ... 113
Disable a Device's USB Port ... 115
Manage Phones with the Device Manager ... 116
Configure a Periodic Provisioning Cycle ... 117
Manage Devices with HTTPS ... 118
Configure QoS on PC Port ... 118
Disable or Re-enable Wi-Fi and Bluetooth via Device Manager ... 119
Supported Parameters ... 119
Configure Phone Behavior ... 121
Configure Minimum and Maximum Ringer Volumes via the Phone's Configuration File ... 121
Configure Noise Reduction ... 122
Disable the Phone's Speaker Hard Key ... 122
Enable a Phone to be used as an Audio Device ... 124
Update Phone Firmware Manually ... 125
Update Microsoft Teams Devices Remotely ... 127
Apply a Partial Configuration Profile ... 128
Enroll a Device with Intune Policies ... 128
Create an Exclusion Group ... 128
Remove Devices from Intune Admin Center ... 129
Set up Emergency Handling ... 132
Set up an E911 Emergency Location ... 132
Enable Users to Make Calls even if Teams is Unavailable ... 133
6 Troubleshooting ... 137

Basic Phone Troubleshooting for Users 137
Device Troubleshooting Options 139
Monitor Phone Process Statuses 139
Get Audio Debug Recording Logs 140
Capture Traffic Using 'rpcapd' 141
Enable Port Mirroring Network Monitoring 143
Return to Previous Version 144
Android Device Utility 144
Capture the Phone Screens 146
Run Tcpdump 147
Get Information about Phones 148
Perform Remote Logging (Syslog) 150
Get Diagnostics 153
Get Logs 154
Activate and Deactivate DSP Recording 155
SSH based Debugging 157
Microsoft Teams Admin Center 157
Collect Logs 157
DSCP 160
Additional Debugging Options 161
Export Logs to USB when Phone is in Recovery Mode 161
Encounter an ANR Error - Core Dump 161
Retrieve Bug Report Automatically Produced if 'Boot Reason' is FATAL or PANIC 162

1 C470HD IP Phone

The AudioCodes Microsoft Teams-native C470HD IP phone is a feature-rich, high-end business phone for Microsoft Teams. A native Microsoft Teams Total Touch high-end business phone, it features a large color touch screen and full UC integration. The phone is equipped with a large, single surface, full touch interface, incorporating an exceptionally sharp 5.5" color touch screen, with optional support for Wi-Fi and Wireless.

AudioCodes IP phones can be offered as part of its Managed IP Phones solution, which defines the IP phone as an IT-managed entity and delivers unique and complete lifecycle management of end-user desktop devices.

C470HD Features:

- Native support for Microsoft Teams
- Graphical portrait 5.5” color touch screen (1280 x 720) with multi-lingual support
- GbE support
- USB headset support
- Wireless support

400HD IP Phone Series Highlights:

- Superior voice quality
- Full duplex speaker phone
- Robust security mechanisms
- PoE or external power supply
- Centralized management supported by AudioCodes Device Manager (available for download free of charge)
- Power-saving mode for MWI LED and LCD is automatically activated during non-working hours. The phone's uppermost-right LED is switched off and the LCD is dimmed. This conserves energy and minimizes light disturbance, providing a seamless and efficient user experience.



AudioCodes Teams phones can operate in a Survivable Branch Appliance (SBA) environment. Branch office survivability is aimed at providing limited calling functionality when a phone no longer has connectivity with the Teams cloud. Basic functionalities are:

- Making PSTN calls
- Receiving PSTN calls
- Hold & Resume of PSTN calls

If a user attempts to make a Teams call and the internet connection is down, they’ll be notified that they can try calling a phone number instead. A ‘No internet connection’ indication is displayed suggesting that calling a phone number is available.

See here for video blogs and blogs about AudioCodes' Teams phones.

See here for videos and webinars about AudioCodes' Teams phones.

See here marketing material related to all AudioCodes' Teams phones.

Teams Features Supported by C470HD

The following table lists Teams features supported by theC470HD IP phone.

Teams Feature	C470HD
Mute	√
Hold/Resume	√
Call Transfer	√
Consultative Transfer	√
End call	√
Escalate P2P call to Teams Meeting / Conference (Add-hoc Conference)	√
Call Queue	√
Contacts / People	√
Speed Dials dedicated keys	√
Auto-dialing to call an extension	√
Favorites list for speed dial	√
Distinctive ringtone per call type	√
Hot Desking	√
Survival Branch Appliance	√
Talkback	√
Meeting details: Exchange calendar, contact pictures, Corporate Directory access	√
Meeting actions: Meet Now, one-click join, meeting call controls (mute/unmute, hold/resume, hang up, add/remove participant, raise hand, live captions)	√

Teams Feature	C470HD
Common Area Phone (CAP)	√
CAP: Advanced calling	√
CAP: Voice Mail (only applicable when 'CAP: Advanced calling' is enabled)	√
Music on Hold (MoH)	√
Call Park	√
Call Merge	√
Delegation	√
E911	√
Better Together (over wireless)	Supported only for C470HD with DBW suffix
Talkback	√
Call Group Pickup	Supported, but configured from Teams client

C470HD Specifications

The following tables summarize the phone's specifications.:

- Functional Features below
- Hardware on page 5

Functional Features

Feature	Details
Media processing	■ Voice Coders: G.711 codec PCMA (A-Law), G.711 codec PCMU (µ-Law), G.722 ■ Acoustic Echo Cancelation: G.168-2004 compliant, 64-msec tail length ■ Adaptive Jitter Buffer ■ Voice Activity Detection

Feature	Details
	■ Comfort Noise Generation ■ Packet Lost Concealment ■ RTP/RTCP Packetization (RFC 3550, RFC 3551), SRTP (RFC 3711)
Microsoft Teams phones feature set	■ Authentication and security: ✓ Sign in with user credentials and based on IP phone policies ✓ Sign in using PC/Smartphone ✓ Modern Authentication ✓ Phone lock/unlock; unlock with smart PIN ✓ 802.1x Authentication ✓ SSH access ✓ HTTP/HTTPS Proxy Server ✓ VLAN (LLDP/CDP/manual) ■ Incoming/Outgoing P2P and PSTN calls ■ In-call controls via UI ■ Calendar and Presence integration and meeting actions ■ Survivable Branch Appliance (SBA) For a detailed list of features, see Teams Features Supported by C470HD on page 2. See also here for related Microsoft documentation.
Configuration and management	■ Teams Admin Center (TAC) for provisioning and logging ■ AudioCodes OVOC / Device Manager ■ AudioCodes Redirect Server
Debugging tools	■ AudioCodes' Android Device Utility (see Android Device Utility on page 144) ■ Log upload to Microsoft server ■ Remote logging via Syslog ■ Diagnostic data ■ SSH Access ■ Phone screen capture ■ TCPdump ■ Audio Debug recording logs

Feature	Details
	■ Echo Canceler (EC) debug recording ■ Media logs (*.blog) ■ Port mirroring network monitoring ■ Remote Packet Capture network sniffer application
Localization support	■ Multi-lingual support; the language pack list is not yet final and is subject to modification. ■ Virtual Keyboard: QWERTY | Numeric ■ Global Network Banner ■ Dark Theme

Hardware

Feature	Details
Screen	Graphical portrait 5.5" color touch screen, 1280 x 720 resolution
Wired connectivity	■ Two RJ-45 [Gigabit Ethernet (GbE)] (10/100/1000BaseT Ethernet) ports: LAN and PC port ■ RJ-9 port (jack) for headset ⚠ USB port for USB headset: The phone is a PoE Class 3 device (also when connecting a standard USB headset). If used with a loud USB speakerphone, an external power supply must be used. For more information, contact AudioCodes.
Wireless connectivity	Applies to devices with **DBW** (Dual Band Wi-Fi), as specified in their name): ■ Wi-Fi Dual Band 2.4GHz and 5GHz 802.11a/b/g/n/ac ■ Wi-Fi supported protocols: WEP, WPA/WPA2-Personal, WPA3-Personal, WPA/WPA2-Enterprise, WPA3-Enterprise, WPA3-Enterprise 192-bit (802.1X) PEAP only ■ BT-BLE 5.2 for BToB and BT headsets
Bluetooth support	Integrated optional Bluetooth support (applies to devices with **DBW**): ■ Bluetooth headset support

Feature	Details
	■ Microsoft Better Together for device pairing ■ Max. # of Bluetooth devices that can connect simultaneously to device: 1 ■ Bluetooth Wideband Speech (WBS) supported for headsets
Hearing aid compatibility	Hearing Aid Compatibility (HAC) support
Power	■ 12V DC jack ■ Power supply AC 100 ~ 240V ■ PoE Class 2: IEEE802.3af (optional) ■ PoE Class 3: IEEE802.3af (optional)
Presence indicator LED	Presence indicator corner LED (Yellow / Green / Red / Blue)
Function keys	■ Hold ■ Mute ■ Transfer ■ Volume ■ Headset (including LED) ■ Speaker (including LED) ■ Back ■ Home

Migration to Android Open Source Project (AOSP)

Migration to Android Open Source Project (AOSP) is supported. Intune offers an AOSP mobile device management (MDM) solution referred to as AOSP Device Management. This MDM platform is used for Teams Android-based devices that enroll in Intune, replacing Android Device Administrator. AOSP Device Management leverages a new agent and Authenticator app, eliminating dependencies on the Company Portal app.

For details see the related documentation:

- AOSP Migration Guide for AudioCodes Teams Devices
- The relevant Microsoft Learn page

These guides provide customers with detailed instructions and best practices for a smooth migration. They also show how to migrate Teams Android devices to AOSP Device Management.



All migration actions are performed in the Microsoft Intune Company Portal. Phone firmware has been upgraded with the Authenticator app.

URLs and Ports (Security) to Allow for AudioCodes Teams Phones

This section shows network administrators which URLs/Ports to allow when deploying Teams phones (security).

From the device point of view, the following table summaries the ports the phone uses. See also Microsoft's guide to the ports the phone uses.

Table 1-1: URLs / Ports to Allow when Deploying Teams Phones (Security)

Server Role	Service Name	Port	Protocol	Notes
DNS Server	All	53	DNS	-
AudioCodes Device Manager	AudioCodes DM	443	HTTPS	AudioCodes device management server
AudioCodes Redirect service	AudioCodes DM	443	HTTPS	AudioCodes redirect service redirect.audiocodes.com
NTP timeserver	Android NTP	123	UDP	-
Time Zone Database	Time Zones	443	HTTPS	Time Zone Database (often called tz or zoneinfo)
Microsoft Apps Artifacts server	Package manager	-	-	Microsoft will be requested for the protocol and port and FQDN. These URLs are provided by the Admin agent.

Security Guidelines for Android-based Native Teams Devices

Refer to the following document: Security Guidelines for AudioCodes Native Teams Android-based Devices.

2 Set up the C470HD IP Phone

The following instructions show how to set up the phone:

- Unpack the Device below
- Explore the Device (Front and Rear Views) on the next page
- Connect Cables on page 14
- Mount the Phone
- Clean the Phone Screen on page 14

Unpack the Device

When unpacking, make sure the items listed in the phone's *Quick Guide* are present and undamaged.

If anything appears to be missing or broken, contact the distributor from whom you purchased the phone for assistance.

For detailed information, refer to the phone's *Quick Guide* (scan the barcode on the box in which the phone was shipped or see Related Documentation on page iii).

Explore the Device (Front and Rear Views)

Use the following graphics to identify and familiarize yourself with the device's hardware functions:

- C470HD Front View below
- C470HD Rear View on page 13

C470HD Front View

The front view of the phone is shown in the figure and described in the table.

Figure 2-1: C470HD Front View

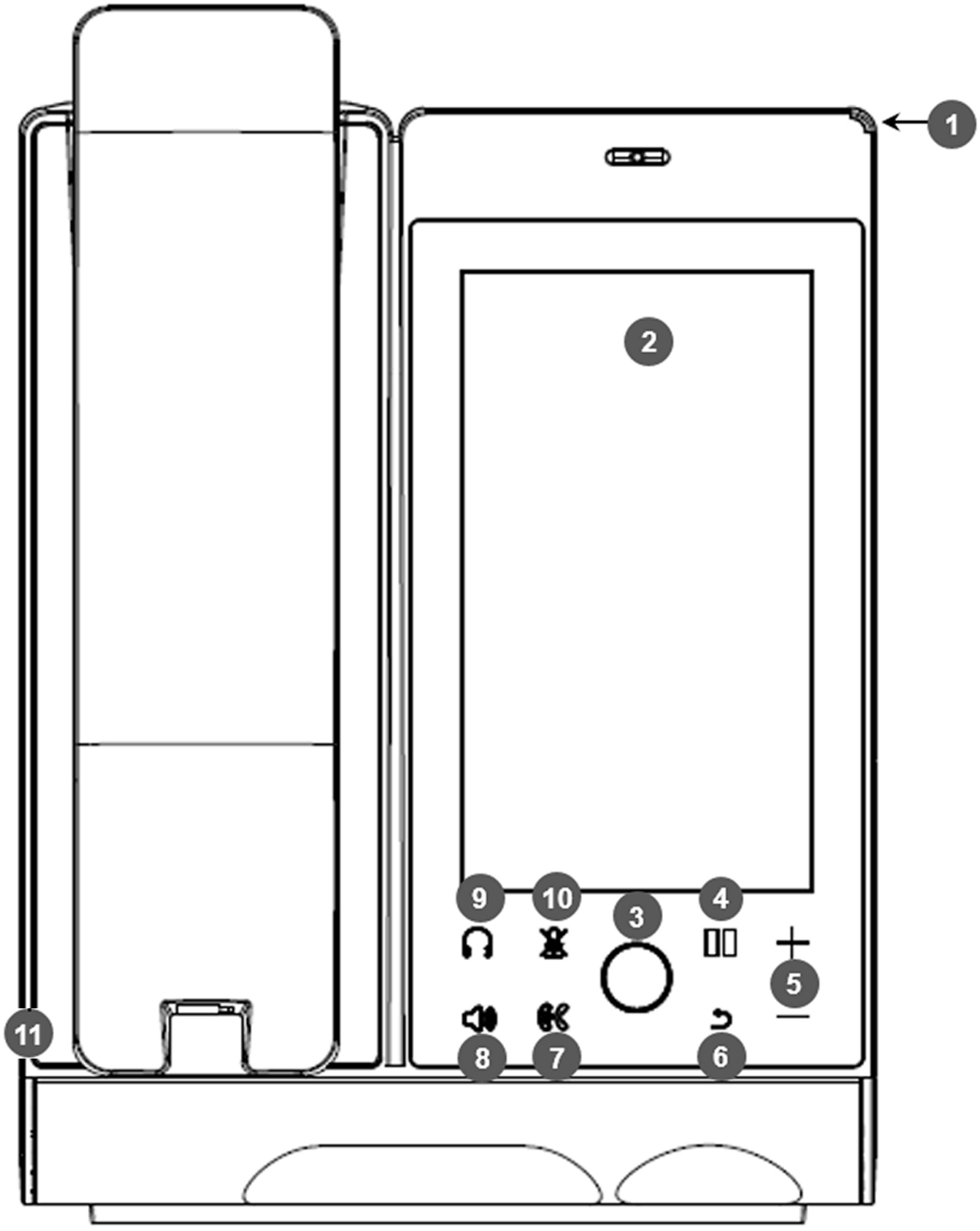
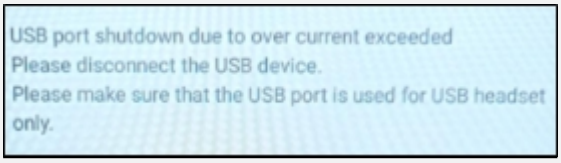


Table 2-1: C470HD Font View Description

Item #	Label/Name	Description
1	Ring LED	Indicates phone status: ■ Green: Idle state

Item #	Label/Name	Description
		■ Flashing red: Incoming call (ringing) ■ Red: Answered call
2	TFT touch screen	Thin Film Transistor touch screen, a type of LCD (Liquid Crystal Display) interactive screen which displays calling information and lets you configure phone features by touching the glass.
3	Home	■ Tap the key to return to the phone's home (idle) screen from any screen. ■ Long-press the key to open the device Settings screen. ■ Visual indications: ✓ If the key is illuminated red (constantly, without flashing), it indicates 'No network'; tapping the key then gives the user direct access to the Network menu. ✓ Flashing red indicates a system alert, for example, when a user tries to charge via the device's USB port (see the note after this table). ✓ Flashing yellow indicates that the phone is in the process of a software upgrade.
4	Hold	Tap to place an active call on hold.
5	Volume	Increases or decreases the volume of the handset, headset, speaker, ring tone or call progress tones. See Adjust Volume on page 80 for detailed information.
6	'Back' key	Tap to return to the previous screen.
7	Call transfer	Tap to transfer a call to a third party.
8	Speaker	Tap to activate the speaker, allowing a hands-free conversation.
9	Headset	Tap to activate a call using an external headset.
10	Mute	Tap to mute an established call.
11	USB port	For a USB headset. See also the note below.

A USB delimiter enables the phone to identify when the USB port is overloaded and to then display an alert on the screen. An alert is also sent to the OVOC. The feature helps to deter users from using the USB port for purposes other than for a USB headset, e.g., for charging devices. If users use the USB port for a headset, the alert will not be sent.



C470HD Rear View

The ports located on the rear of the phone are described in the table.

Figure 2-2: C470HD Rear View

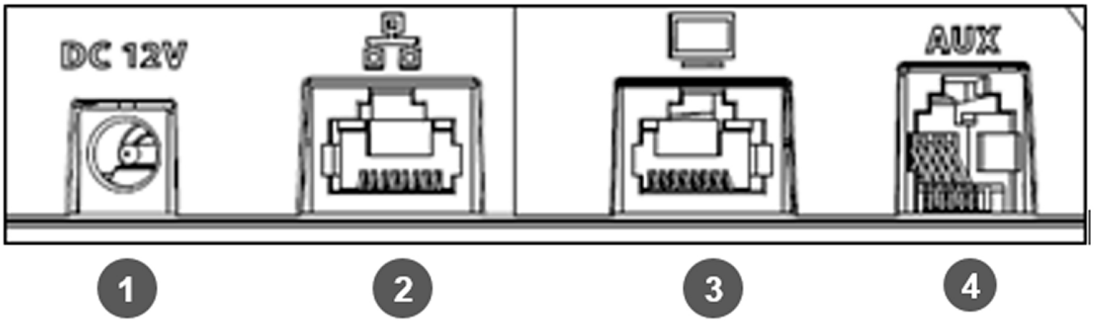


Table 2-2: C470HD Rear View Description

#	Description
1	12V DC power jack that connects to the AC power adapter.
2	RJ-45 port to connect to the Ethernet LAN cable for the LAN connection (uplink - 10/100/1000 Mbps). If you're using Power over Ethernet (PoE), power to the phone is supplied from the Ethernet cable (draws power from either a spare line or a signal line).
3	RJ-45 port to connect the phone to a PC (10/100/1000 Mbps downlink).
4	Headset jack, i.e., RJ-9 port that connects to an external headset.

Connect Cables

For detailed information on how to cable the phone, refer to the phone's *Quick Guide* (scan the barcode on the box in which the phone was shipped or see Related Documentation on page iii).

Clean the Phone Screen

AudioCodes recommends frequently cleaning devices' screens especially screens on devices in common use areas such as conference rooms and lobbies.

➢ **To clean a device's screen:**

1. Disconnect all cables.
2. Spray onto a clean, dry, microfiber duster a medicinal isopropyl alcohol and water solution of 70:30. Don't oversaturate the duster. If it's wet, squeeze it out.
3. Lightly wipe the screen of the device.
4. Wait for the screen to dry before reconnecting cables.

3 Start up C470HD

Before users can start up their phones, the network administrator must have set them up for automatic provisioning (see Set up Automatic Provisioning on page 106).

To start up your phone:

1. Sign In to Your device Teams Phone below.
2. Configure C470HD Device Settings on page 23.
3. Set up Accessibility on page 35.
4. Configure Wi-Fi on page 39.
5. Configure VLAN via DHCP Option when CDP-LLDP is Not Allowed on page 46 (performed by your network administrator as required).
6. Lock or Unlock the Phone on page 47.
7. Enable Power Saving on page 50.

It will be necessary to repeat this only if the phone is restored to default settings (see Restore the Phone to Default Settings on page 51).

Sign In to Your device Teams Phone

IMPORTANT: For sign-in to work, Time settings must be handled automatically (which is the default configuration). Only administrators should modify these settings. For details see Configure Time on Teams Devices on page 105.

You may sign in:

- On your phone (see Sign in on Your C470HD below)
- From your PC or smartphone (see Sign in from your PC or Smartphone on page 18)

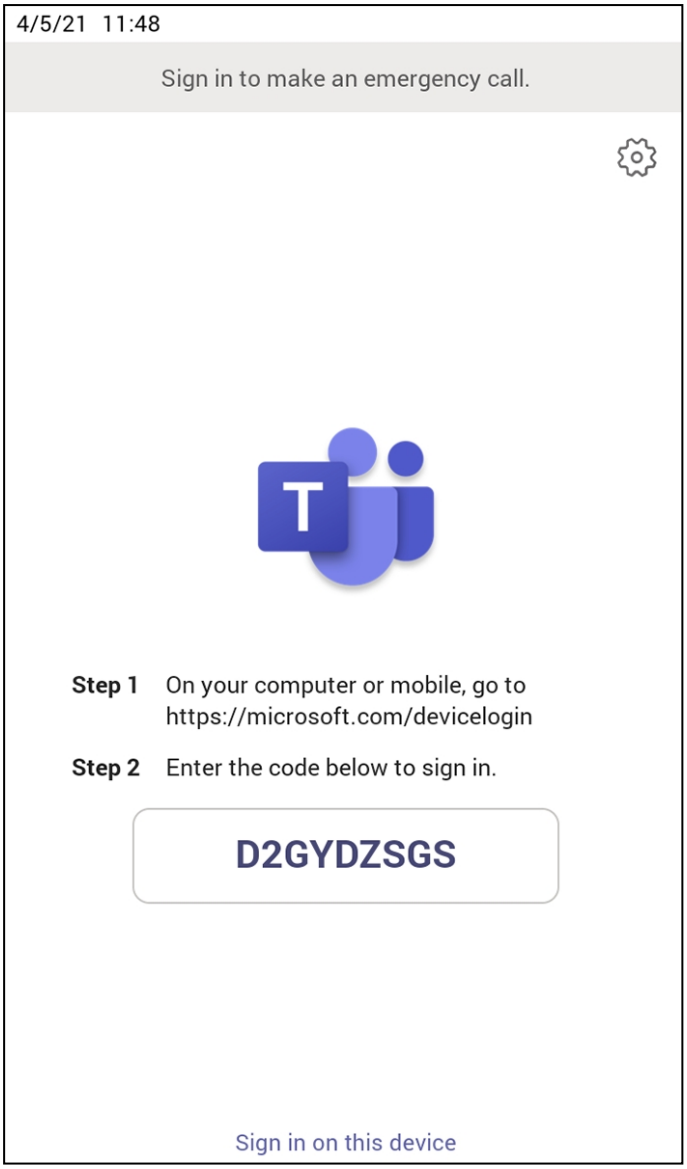
Sign in on Your C470HD

➢ **To sign in:**

1. Connect the device to the network; the language selection screen is displayed.



2. Select the preferred language; the Sign-in screen is displayed:

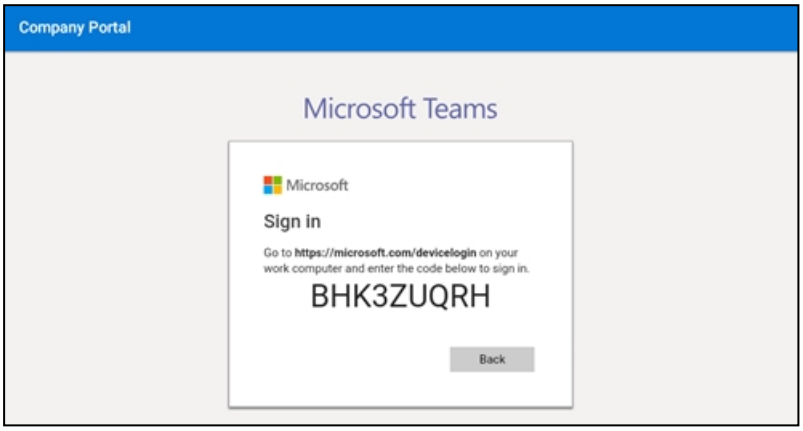


3. Open your browser and point it to **https://microsoft.com/devicelogin** as instructed in the screen; you are prompted to enter the displayed code.
4. Enter the code and then click **Next**.
5. Click your account, enter your password (which is the same password as the Windows password on your PC) and then click **Sign in**. You may close the window after successful sign-in.
6. Observe that the phone returns to the initial code screen. In that screen, tap **Sign in on this device**.
7. Tap the 'Email, phone or username' field; a virtual keyboard pops up. Enter one of them and then tap **Sign in**. The home screen opens.
   - If you opt to **Sign in from another device**, complete authentication from your PC or smart phone (see below). This is recommended if you're using Multi Factor Authentication (MFA).

Sign in from your PC or Smartphone

➢ **To sign in from your PC or Smartphone (recommended when MFA is used):**

1. In the browser on your PC or smartphone, enter the URL indicated in the Microsoft Teams Sign-in page. The phone's Web interface is displayed.
2. Following sign-in instructions.



If the internet connectivity check fails, a 'No Internet Access' warning pops up on the phone screen. This can point to a problem that is preventing the phone from fully functioning in a Teams environment. Contact your system administrator if you account a problem.

If connected to the network via Ethernet, the Teams device will dynamically update location information for emergency calling services based on changes to network attributes including chassis ID and port ID.

Updating the location is based on LLDP-MED (Link Layer Discovery Protocol – Media Endpoint Discovery). This is a standard link layer protocol used by network devices to advertise their identity, capabilities, and neighbors on a local area network based on IEEE802 technology, principally wired Ethernet.

Remote Provisioning and Sign-in from Teams Admin Center (TAC)

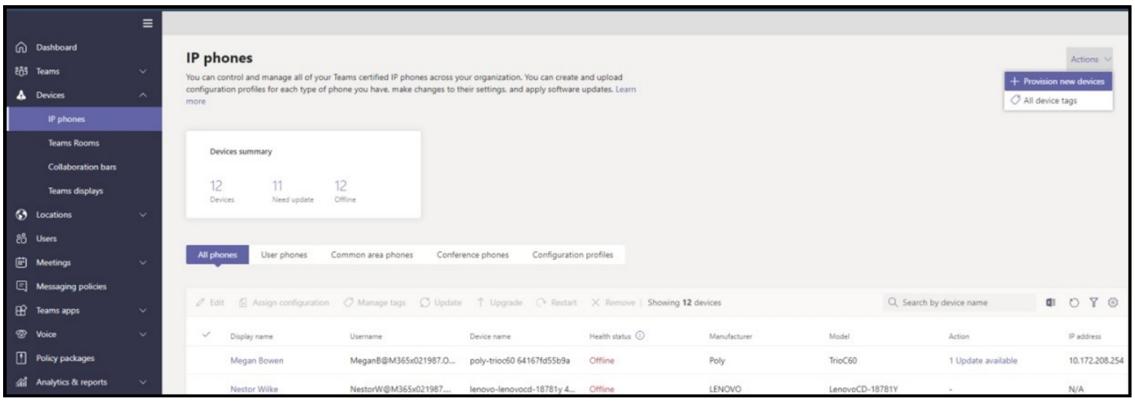
Network administrators can remotely provision and sign in to a Teams device. To provision a device remotely, the administrator needs to upload the MAC IDs of the devices being provisioned and create a verification code. The remote device provisioning process can be completed from the Teams Admin Center (TAC). For details and instructions, click Microsoft's article on Remote provisioning and sign in for Teams Android devices.

Remote provisioning sign-in makes it possible for a technician to access and set up the phone by entering a TAC generated code, without having to provide user credentials.

Step 1: Add a device MAC address

Provision the device by imprinting a MAC address on the device.

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



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

Manually add a device MAC address

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

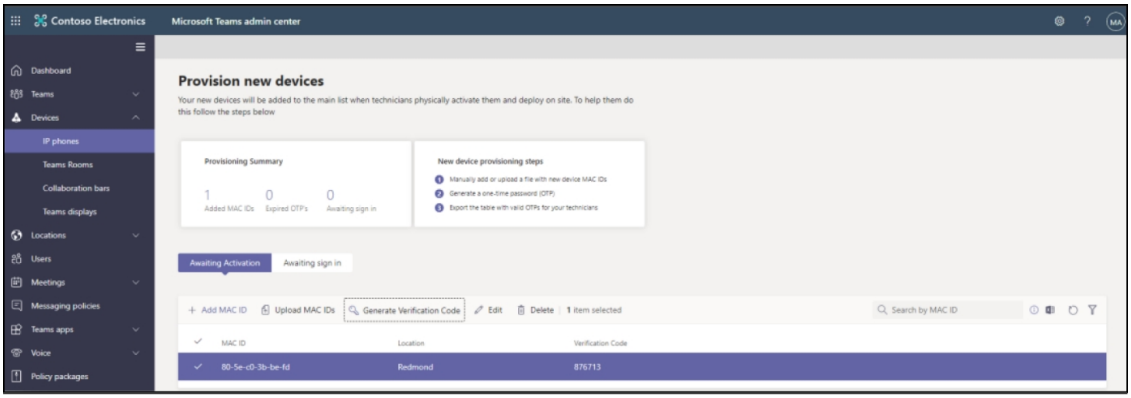
Upload a file to add a device MAC address

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

Step 2: Generate a verification code

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

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

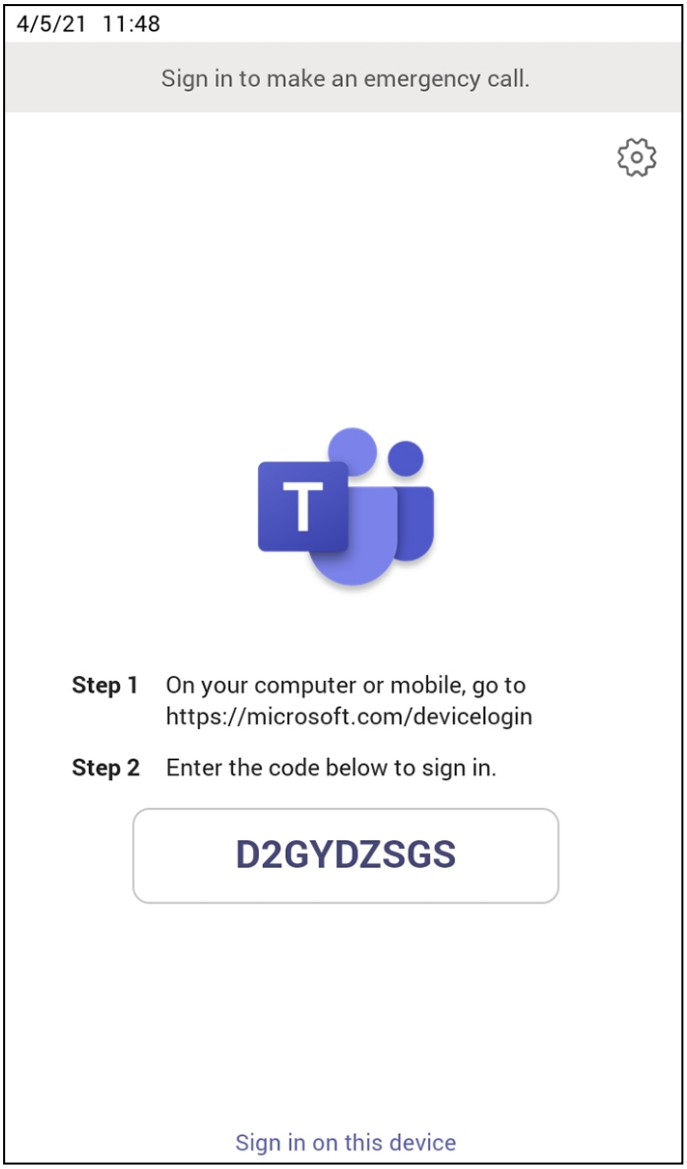


You need to provide the list of MAC IDs and verification codes to the field technicians. You can export the details directly in a file and share the file with the technician who is doing the actual installation work.

➢ Step 3: Provisioning on the device

Once the device is powered up and connected to the network, the technician provisions the device:

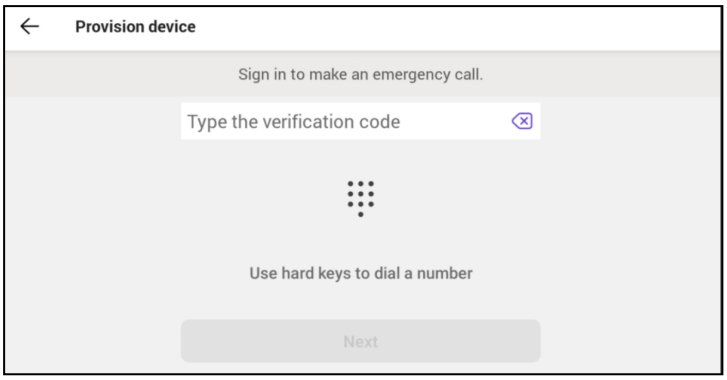
1. Taps the 'Settings' gear icon on the top right of the ‘Sign in’ screen



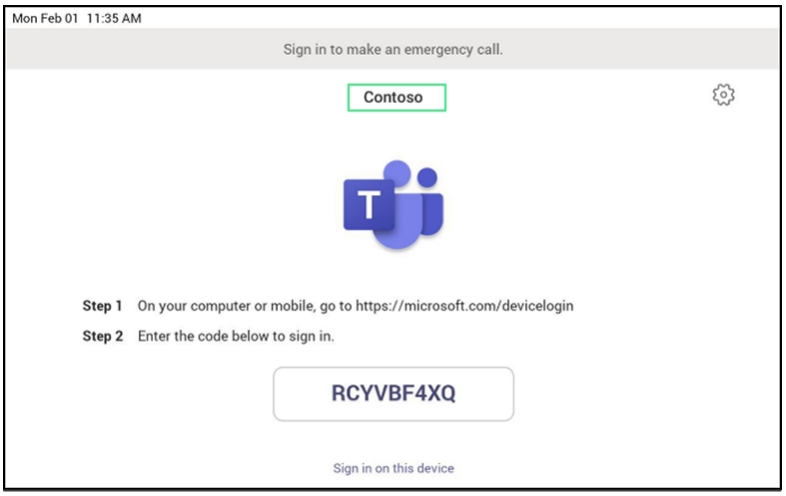
2. On the Settings screen, taps **Provision phone**.



3. Types the device-specific verification code that was provided in the Teams Admin Center on the phone's user interface.



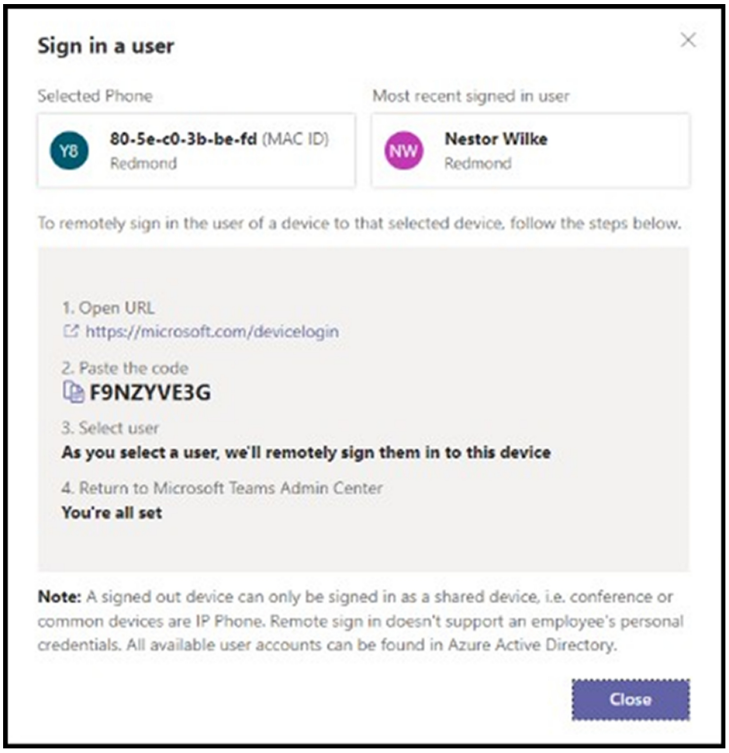
Once the device is provisioned successfully, the tenant name is available on the sign in page.



Step 4: Sign in remotely

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

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



The tenant administrator then completes authentication on the device from any browser or smartphone.

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

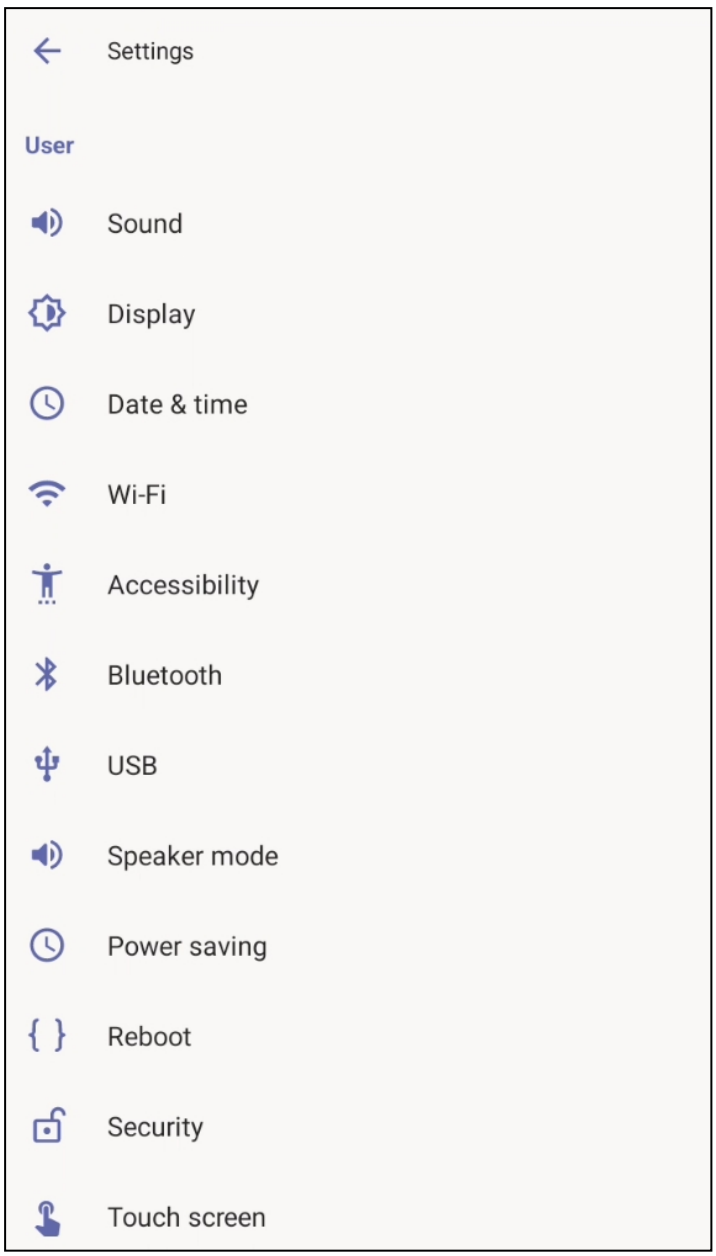


Configure C470HD Device Settings

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

➢ **To access device settings:**

1. In the home screen, tap the user (avatar) picture, then tap the **Settings > Device settings**.



2. View or configure the settings under 'User'. Tap a setting to open the setting. For a description of user settings see User-level Device Settings on the next page.
3. To view or configure settings configured by the system administrator:
   a. Scroll down and open 'Device admin settings'.
   b. Log in as administrator.

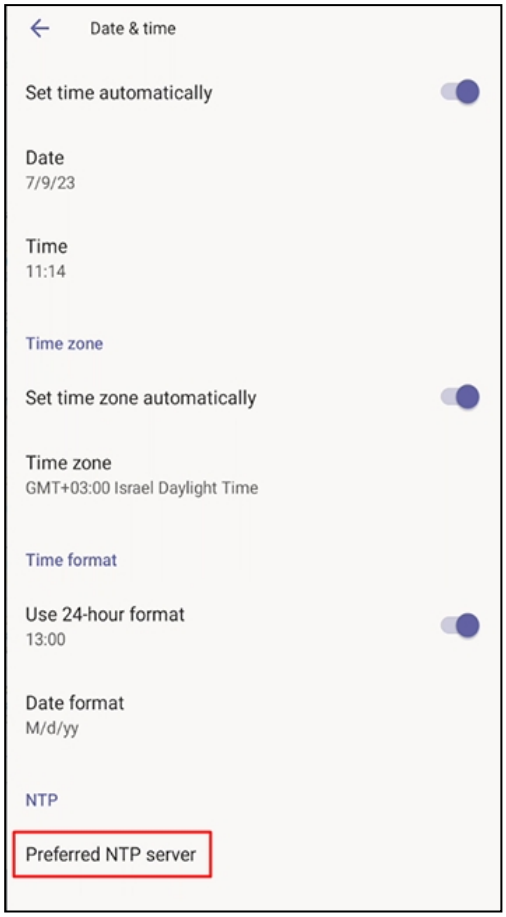
   For a description of administrator-level settings see Device Settings Configured by Administrator on page 28.

User-level Device Settings

The following table describes the C470HD device settings that can be configured by regular users. No administrator login is required to set up these features.

To access these settings, tap the user (avatar) picture in the home screen, then tap **Settings > Device settings**.

Setting	Description
Sound	Allows you to customize the phone volume for a friendlier user experience: ■ Media volume ■ Ring & notification volume
Display	Opens the 'Display' screen, where you can adjust: ■ Brightness level ■ Screen timeout ■ Screen saver
Date & time	■ Automatic date & time: If enabled, date and time are automatically retrieved from the deployed Network Time Protocol (NTP) server. ■ Time zone ■ 24-hour format ■ Date format Also supported is a simplified version of NTP called Simple Network Time Protocol (SNTP). Both can be used to synchronize device clocks. SNTP is typically used if full implementation of NTP is not required. See also Configure Time on Teams Devices on page 105.
NTP Preferred NTP server	Administrators can use this parameter to *manually* define the NTP server, to comply with enterprise security requirements if those requirements preclude using DHCP Option 42. Manual configuration takes precedence over DHCP Option 42 and the time servers. Two ways to manually define the NTP server are available: ■ Administrators can define it in the phone's GUI.

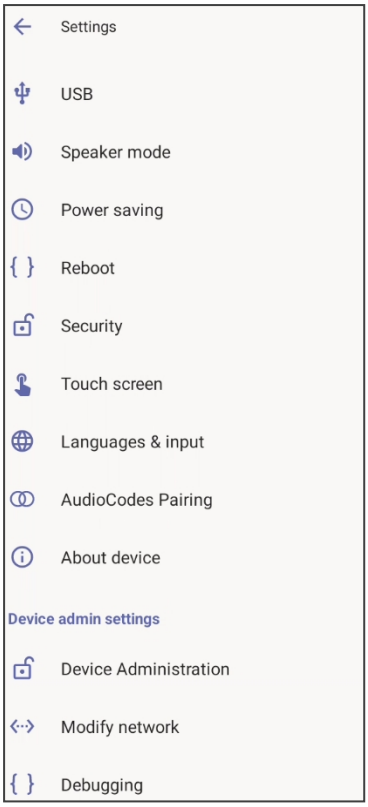
Setting	Description
	 ■ Administrators can alternatively use the parameter 'date_ time/ntp/server_address' in the phone's .cfg configuration file. See also Configure Time on Teams Devices on page 105.
Wi-Fi	[Only available for phones with integrated Wi-Fi (DBW-suffix), and only if not restricted (see Disable or Re-enable Wi-Fi and Bluetooth via Device Manager on page 119)] The phone can connect to an Access Point via Wi-Fi. See the phone's *Quick Guide* for detailed information on setting up Wi-Fi. See also Configure Wi-Fi on page 39 in this document for information about configuring the feature.
Accessibility	Allows making the phone screen reader-friendlier: ■ Font size ■ High contrast text ■ Color correction ■ Talkback (see also Enable Google Talkback on page 36).

Setting	Description
USB	If enabled, allows the phone to be used as an audio device (see Enable a Phone to be used as an Audio Device on page 124).
Speaker Mode	Use to enable or disable the speaker. If disabled, the user needs to speak into the handset during calls.
Power Saving	Allows users to contribute to power saving in the enterprise. Set: ■ **Enable power saving**. ■ **Start time** – only relevant if power saving is enabled. The device consumes minimal energy before the user arrives at the office. ■ **End time** – only relevant if power saving is enabled. The device consumes minimal energy after the user leaves the office.
Reboot	Enables users to reboot the device. Log in as Administrator for more debugging settings to be available.
Security	Helps secure the enterprise telephony network against breaches. ■ **Screen lock** – tap to select the requested lock type (Pattern, PIN, or Password) to secure it against unwanted use, or to remove an existing lock. After setting up a lock, a Settings icon appears to its right.  Tap to change the timeout (default is 10 minutes) after which the phone automatically locks and is inaccessible to anyone who does not know its lock code. If you are using a Pattern lock, you can also make the pattern briefly visible when you draw the pattern. ■ **Show passwords** – if turned on, the screen displays characters briefly when you type the PIN or password.

Setting	Description
	 To apply default security settings to multiple phones, administrators can specify them in the phones' configuration files. Relevant parameters are: • `phone_lock/enabled` – set to `1` to enable screen locking with PIN identification. • `phone_lock/timeout` – duration of inactivity after which the phone is locked (in seconds). • `phone_lock/lock_pin` – initial PIN code.
Touch screen	Allows users to disable the phone's touch screen (for example, to clean it without tapping buttons). To re-enable the screen after cleaning, touch it with your finger.
Languages & input	Allows users to customize inputting to suit personal requirements.
AudioCodes pairing	Displays the name of the phone and allows you to pair it to a nearby connected PC.
About device	Provides users with device information. ■ To determine the device's IP address, select the **Status** option. ■ To get information about the Android version, select **Android version**. ■ To get information about the version, select **Version info**.

Device Settings Configured by Administrator

To view or configure administrator-level C470HD device settings and debugging options, you need to log in as administrator. Navigate to **Device Settings > Device admin settings > Device Administration**.



Administrator login is password protected. The default password is 1234 (or 1111 in early versions) and must be changed at the first login.

Device settings only available for administrators include Modify network below and Debugging on page 35.

Modify network

Modify network settings enable administrators to determine network information and to modify network settings:

- **IP Address** [Read Only]

- **IP Settings** [DHCP or Static IP]
- **Network state** [Read Only]
- **Enable PC port**
- **Enable PC port mirror**
- Proxy below
- 802.1x Settings on the next page
- VLAN Settings on page 34

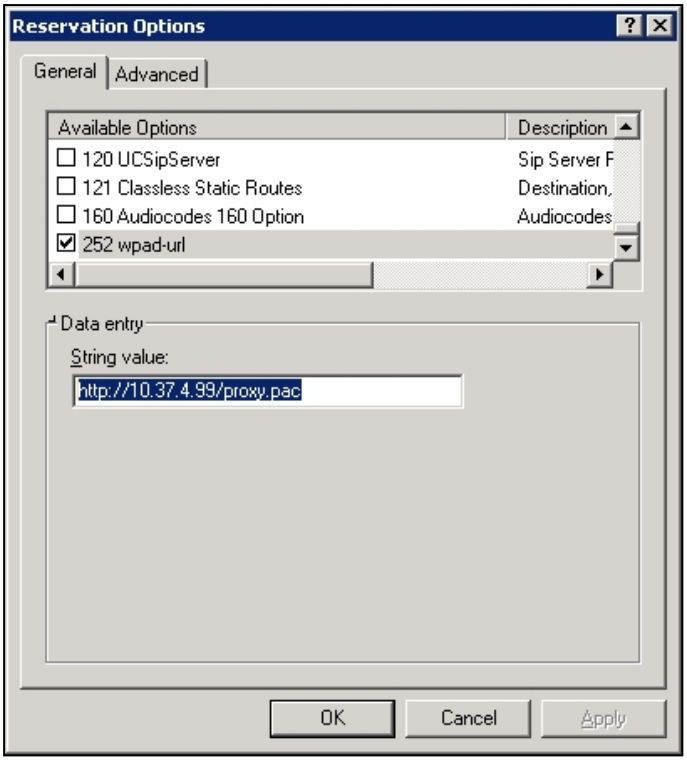


LLDP switch information is retrieved (for location purposes) when the parameter 'network/lan/lldp/enabled'=1 (even when VLAN is retrieved from **CDP** or VLAN is disabled or VLAN is **Manual**). In versions prior to 1.19, if network VLAN mode 'network/lan/vlan/mode' was set to **LLDP**, the phone retrieved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

Proxy

The phone can be configured with an HTTP (or HTTPS) Proxy server by an Admin user in two ways:

- **Manually**. The Admin user can use this method to configure HTTP proxy server parameters through the Teams application:
  a. Log in as Administrator and tap **Modify network**.
  b. Tap the **Proxy** option and then configure the proxy host name and port:
- **Over DHCP with Option 252**. It's recommended that the Admin user uses this method when provisioning multiple phones. Option 252 provides a DHCP client with a URL to use to configure its proxy settings:



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

Example of a basic PAC file:

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

If the enterprise features a proxy server that requires user authentication, the network administrator can use the PAC file and DHCP Option 252 to configure the proxy server. Alternatively, the administrator can configure the proxy server using the following parameters:

```
http_client/fwd_proxy/ip=
http_client/fwd_proxy/password=
http_client/fwd_proxy/port=8080
http_client/fwd_proxy/username=
```

802.1x Settings

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.

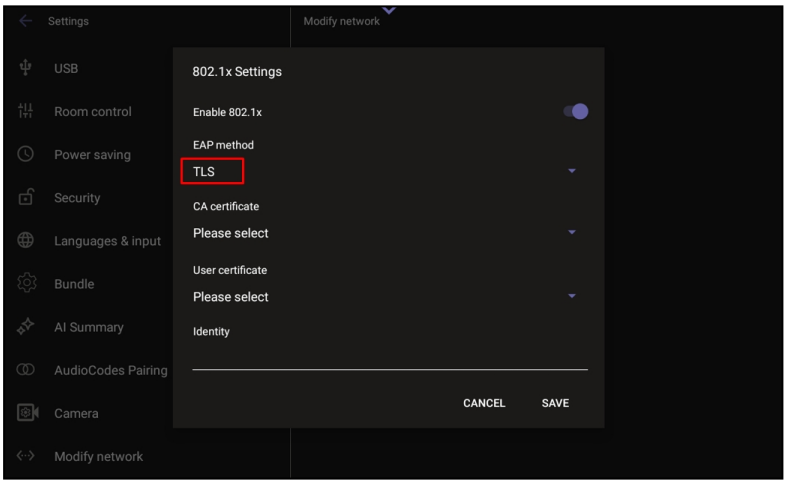
Instead of performing the following steps, 802.1x Authentication can be enabled and predefined via provisioning, by setting the following parameters:

`network/lan/_802_1x/status=true` or `false`

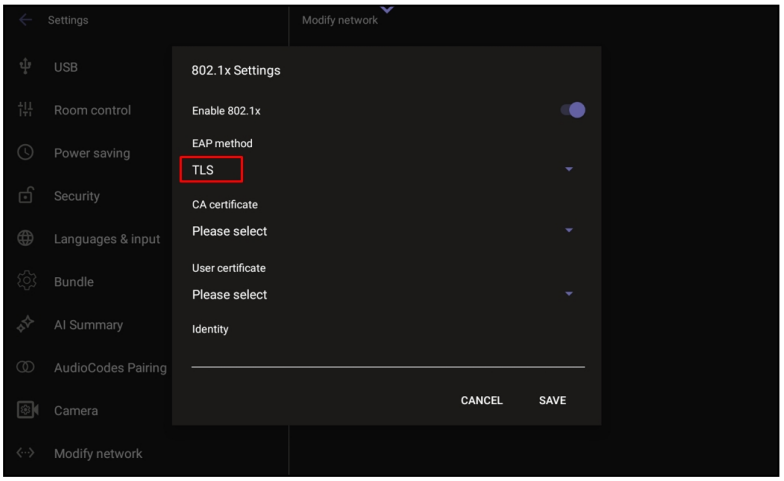
```
network/lan/_802_1x/eap_tls/ca_cert=<CA FILE NAME>
network/lan/_802_1x/eap_tls/client_cert=<Client certificate file name>
network/lan/_802_1x/eap_tls/identity=<identity name>
network/lan/_802_1x/eap_type=eap_tls
```

➢ To configure an 802.1x Authentication method:

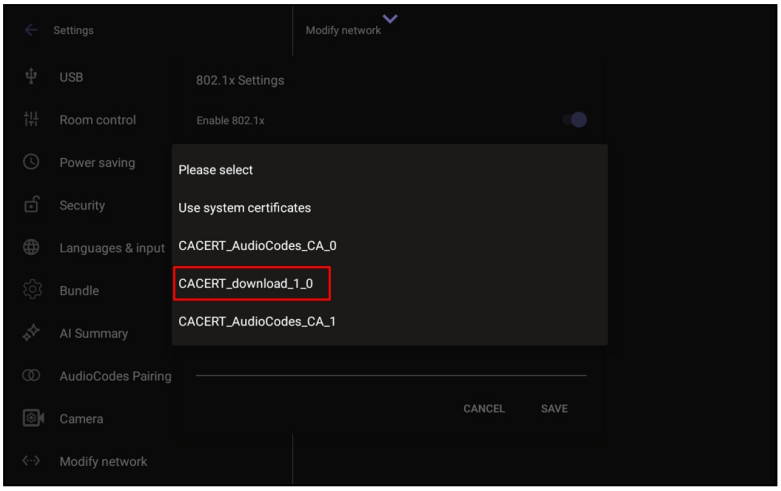
1. After logging in as administrator, go to the 'Modify Network' screen and access the 802.1x Settings screen.
2. Tap the **Enable 802.1x** toggle switch and then tap **Save**.
3. Once enabled, the administrator needs to choose the security method and strength. Commonly used is EAP-TLS.



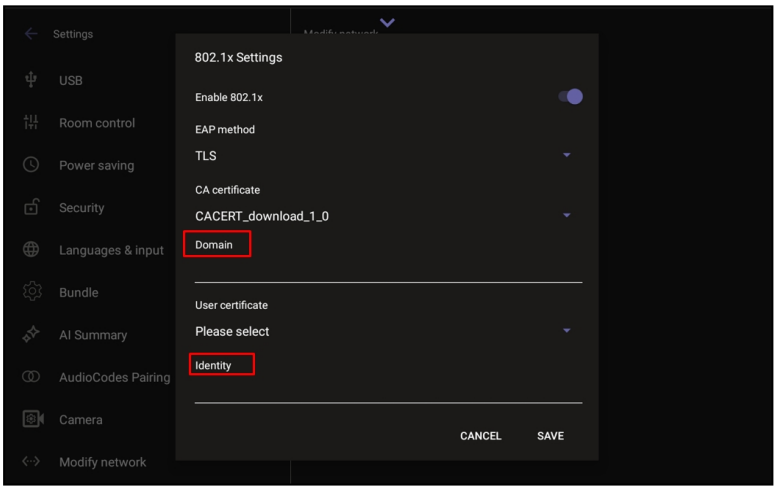
4. Next is to choose which certificates to use:
   a. The device can use the system certificates -



b. Or a certificate that has been loaded by the administrator, which will look as follows:



5. After choosing which certificate file to use, the administrator needs to set the **Identity** and the **Domain** the device is intended to enter:



6. Tap **Save** after defining all the above.
7. From the 'EAP method' drop-down, tap the method: **MD5** or **TLS** (for example).

> In version 2.3, the option for non-validating a CA certificate was removed.

8. Enter this information:
   - **Identity**: User ID
   - **Password**
   - **Root certificate** (not required for every method)
   - **Device certificate** (not required for every method)
9. Press the **Save** softkey.

The 802.1x settings are not only available via the phone screen, they are also supported in the device Configuration File, enabling network administrators to perform pre-staging configuration for 802.1x. The 802.1x settings available in the Configuration File are:

- Enable/Disable
- EAP method
- Identity
- Password

VLAN Settings

Navigate to **VLAN Settings > VLAN Discovery mode.**

Tap the mode you require as per the following guidelines, and then tap **OK**:

- Cisco Discovery Protocol (**CDP**) is a Cisco proprietary Data Link Layer protocol.
- Link Layer Discovery Protocol (**LLDP**) is a standard, layer two discovery protocol.
- If you tap **Automatic configuration** (DCP, LLDP or both), you need to specify the **VLAN Interval** or leave it at its default value (30 seconds). The VLAN interval refers to CDP/LLDP advertisements' periodic interval. You can increase or decrease the intervals between the CDP/LLDP packets that are sent, based on network traffic and topology.
- If you tap **Manual configuration**, you need to specify the **VLAN ID** and **VLAN Priority**. Changes will only be applied after these fields have been set.

Debugging

Allows the Admin user to perform debugging for troubleshooting purposes. Available after logging in as administrator.

- Log settings
- Remote logging (see Perform Remote Logging (Syslog) on page 150 for more information)
- Diagnostic data (see Get Diagnostics on page 153 for more information)
- Reset configuration (see Perform User Data Reset on page 52 for more information)
- Restart Teams app
- Debug recording (for Media/DSP debugging) (see Activate and Deactivate DSP Recording on page 155 for more information)
- Erase all data (factory reset) (the equivalent of restore to defaults; including logout and device reboot)
- **SSH** – if enabled, allows remote connection via SSH. This option must be enabled to use the **rpcapd** (Remote Packet Capture) network sniffer application for capturing screenshots and traffic packages from a desktop PC using the app's integral SSH server.
- **Screen capture** – enabled by default. If disabled, the phone won't allow its screens to be captured.
- **Remote packet capture** – enables capturing traffic packages using **rpcapd**.
- **Advanced > Rediscover provisioning server** – use to let the device detect the applicable provisioning server and retrieve configuration settin

Set up Accessibility

As part of our ongoing commitment to inclusive design, AudioCodes Teams phones incorporate a range of accessibility features to support users with diverse physical, visual, auditory, and cognitive needs. These features are designed to enhance usability, promote independence, and ensure that all users can interact effectively with their communication devices. From high contrast displays and large touchscreens to headset compatibility and personalized settings, the following tools and options help create a more accessible experience for every user:

- **High Contrast Text, Font Size, and Color Correction**

  Teams phones support high contrast display modes, adjustable font size, and color correction options to improve readability for users with visual impairments.

- **Large Touchscreen Displays**

Models like the C455HD, C456HD, and C470HD offer large, high-resolution touchscreens (up to 5") that enhance visibility and ease of interaction.

- **USB and Bluetooth Headset Support**

  Support for USB and Bluetooth headsets allows users with hearing aids or specialized audio devices to connect easily.

- **Hot Desking**

  This feature allows users to sign in and access their personalized settings, including accessibility preferences, on any shared device.

- **Real-Time Text (RTT) Support**

  RTT enables users to view real-time text input from others during calls and meetings. Notifications appear on incoming call screens and banners, and RTT can be viewed simultaneously with live captions. Users can disable RTT from the in-call menu if needed.

  Note: Phone devices support view-only RTT; sending text input is not supported.

- **Localization and Language Support**

  Phones support multiple languages and regional settings, which is essential for users with language-related accessibility needs.

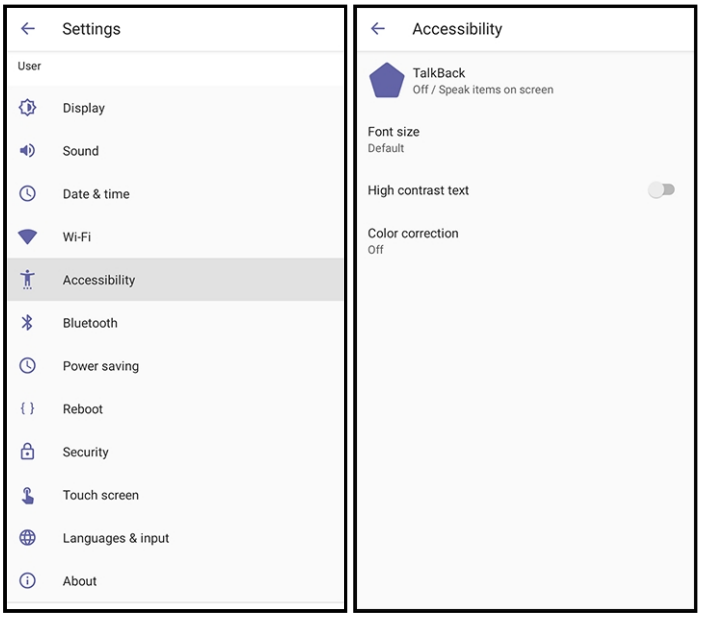
Enable Google Talkback

AudioCodes' Native Teams Android devices feature Google TalkBack, an accessibility service that allows blind and low-vision users to interact with their devices by giving them spoken feedback so they can use their devices without looking at the screen.

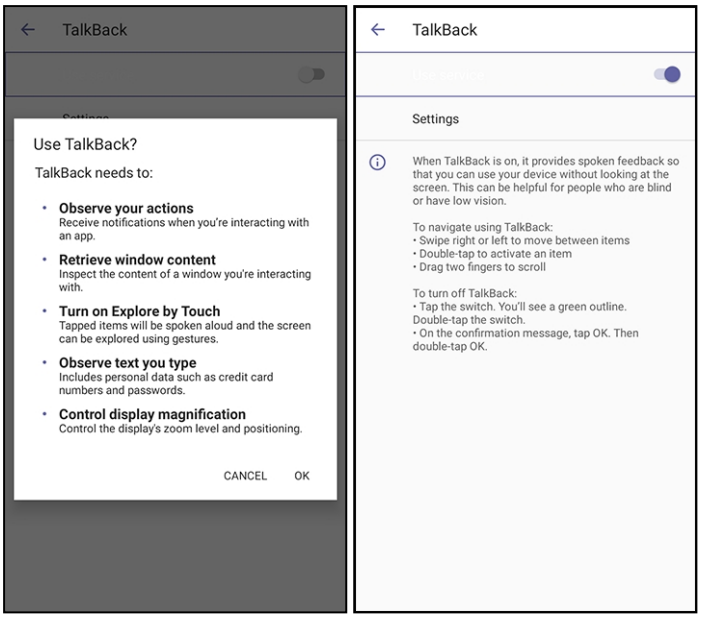
The feature improves the experience of these users.

➢ To enable the feature:

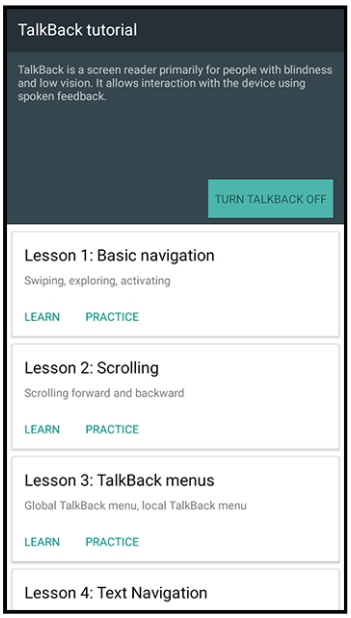
1. Open the Accessibility screen (**Settings** > **Device settings** > **Accessibility**).



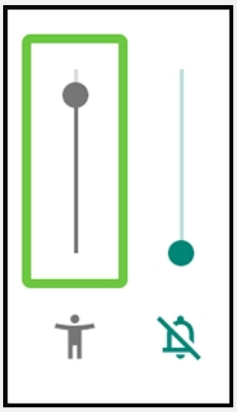
2. Tap and turn on the **TalkBack** option. You are asked to consent to providing control options to TalkBack.



3. Tap **OK** to switch the feature on. Listen to the audio tutorial that begins playing. The tutorial explains how to interact with the device.

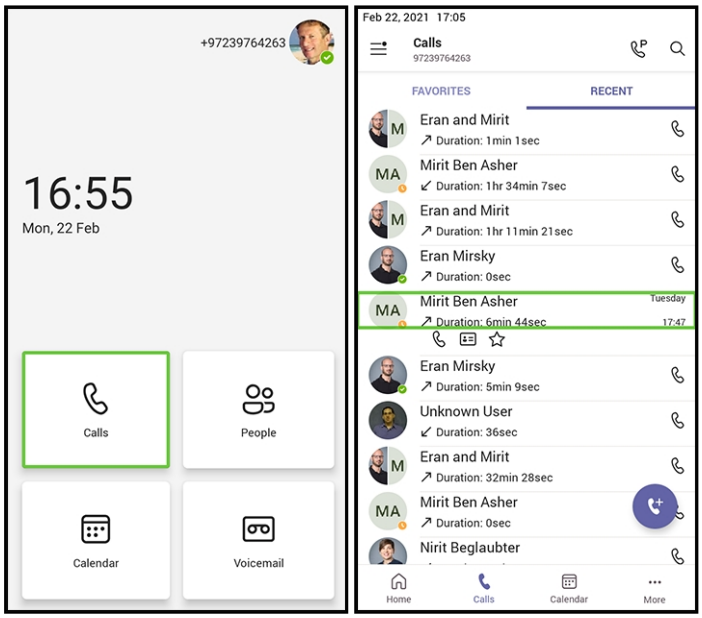


- After TalkBack is switched on, operations are performed by *tapping to select* and then *double-tapping to activate*.
- To turn up the volume, tap the **+** key on the phone and in the volume pop-up shown in the figure below, tap the slider to select it; audio announces what level you're at. Double-tap the slider at the level you want.



- To switch off TalkBack, re-access the Accessibility screen and then switch the feature off the same way.

4. After the tutorial, from the 'Home' screen open (for example) the Calls screen; audio announces what you did; the Calls screen opens.



➢ To interact with the Calls screen:

1. In the Calls screen, tap the **Recent** tab; audio informs you what you selected.
2. Tap a listed call; audio informs you whether the call was outgoing or incoming and to / from whom it was made and the day on which it was made.
3. Double-tap the listed call; three icons below it appear.

4. Tap the phone icon; audio informs you that you can view the person's profile. Double-tap the icon; the person's profile screen opens displaying their name, position, email, hyperlinked work phone number and hyperlinked mobile phone number.
5. Tap the star icon; audio informs you that you can add to Favorites; double-tap to activate it.

Configure Wi-Fi

This chapter and its sub-chapters apply only to devices that support Wi-Fi, i.e., devices with a **DBW** suffix in their Product Name.

If wireless functionality is restricted on the phone, Wi-i-Fi and Bluetooth options are hidden from the phone screen, and you cannot configure or use Wi-Fi or Bluetooth connections.

Only administrators can apply or remove this restriction. For details see Disable or Re-enable Wi-Fi and Bluetooth via Device Manager on page 119.

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

- Users can enable or disable Wi-Fi using the phone screen.
- Wi-Fi cannot be enabled or disabled using SSH.
- The Wi-Fi connection is transparent to users. The phone decides which frequency is used, 2.4 GHz or 5 GHz; users cannot disable either.

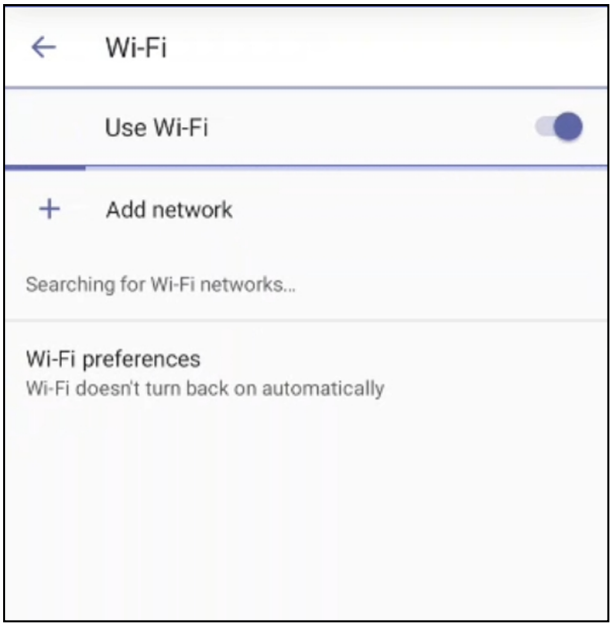
Network administrators can configure Wi-Fi settings in the phone screen.

Connect to an Available Wi-Fi Network

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

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

1. In the 'Wi-Fi' screen (**Settings** > **Wi-Fi**), turn on the **Use Wi-Fi** setting.



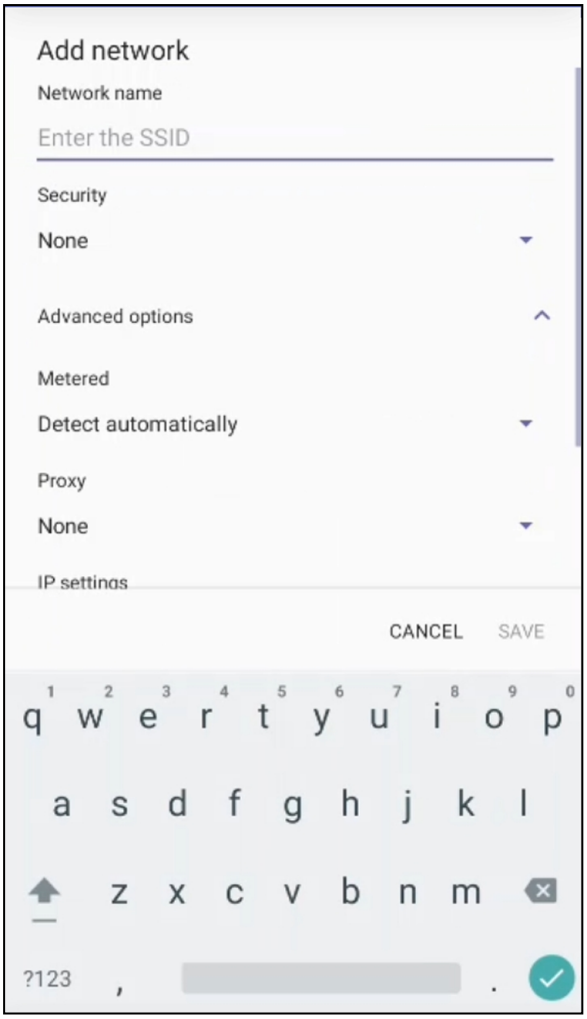
2. View a list of available connections.
3. Tap the Wi-Fi network you want and enter the password.
4. View the network you selected 'Connected'.

Manually Connect to a Wi-Fi Network

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

> Make sure to first disconnect your Ethernet cable. If the cable is connected, the device will not be able to connect to a Wi-Fi network.

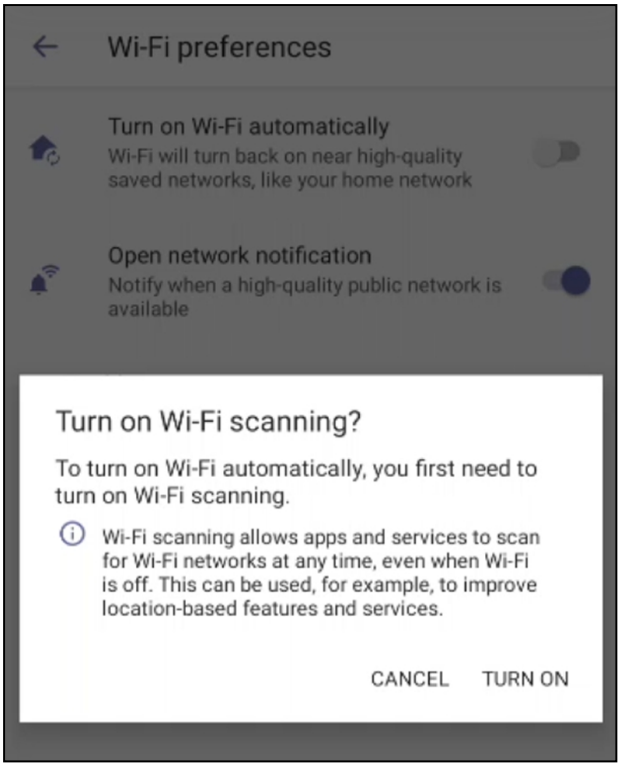
1. In the Wi-Fi screen (**Settings** > **Wi-Fi**), tap **+ Add network** and then enter the SSID of the network to add manually.



2. From the 'Security' drop-down, tap a security key strength (encryption method).
3. Optionally meter the selected network. Expand **Advanced Options**. Leave the setting at its default value of **Detect automatically** if you don't want to meter the network. Tap a **Metered** option to meter it.

Proxy and **DHCP** will automatically be configured by the network.

Enabling the setting **Turn on Wi-Fi automatically** shown in the 'Wi-Fi preference' shown below allows the device to automatically connect in the future to the highest signal-quality network remembered by the device.



Set up via Configuration File

As an alternative to manually configuring Wi-Fi settings via the phone's user interface as shown above, you can configure the Wi-Fi settings described in the next table, using the Configuration File.

Table 3-1: Configuration File Wi-Fi Settings

Wi-Fi Setting	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. See also here.
network/wireless/adavanced_ options/ip_addr	Defines the IP address of the static Wi-Fi network if you’re operating with a static Wi-Fi network.
network/wireless/adavanced_ options/ip_settings	Used to define DHCP.

Wi-Fi Setting	Description
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/advanced_ options/hidden_network	Defines whether the network name should be hidden (see Configure Wi-Fi with Hidden SSID on the next page).
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	Defines the encryption method. Phase 2 applies only to the 802.1x EAP method. Valid values: NONE, MSCHAPV2, GTC,PAP, or MSCHAP.
network/wireless/security	Defines the security method (encryption protocol).
network/wireless/ssid	Defines the SSID of the network.

Configure Wi-Fi with Hidden SSID

This feature applies to customers using Wi-Fi access points with hidden SSID. To connect to the Wi-Fi network, the administrators must configure the customers' phones according to the instructions presented here.

➢ **To configure Wi-Fi with hidden SSID:**

1. Open the 'Settings' screen and navigate to **Wi-Fi > + Add network**.
2. Enter the SSID (Network name) and then tap **Advanced Options**.
3. From the 'Hidden network' drop-down, tap **YES** and then **Save**.



See also Configure Wi-Fi on page 39 for information about the equivalent configuration file parameter 'network/wireless/adavanced_options/hidden_network'.

Configure Wi-Fi Security Methods

When connecting to a new Wi-Fi network, the administrator can define the security strength of that network according to network connection type, as shown in the table below. These parameters can be selected via the UI of the phone or can be provisioned.

Network Type	Wi-Fi Security Method / Configuration Value
Enhanced Open	network/wireless/security=OWE
WPA/WPA2-Personal	network/wireless/security=WPA_WPA2_PSK
WPA/WPA2-Enterprise	network/wireless/security=802.1X_EAP
WPA3-Personal	network/wireless/security=SAE
WPA3-Enterprise	network/wireless/security=802.1x_EAP_WPA3
WPA3-Enterprise 192-bit	network/wireless/security=802.1x_EAP_WPA3_192

Configure Wi-Fi TLS

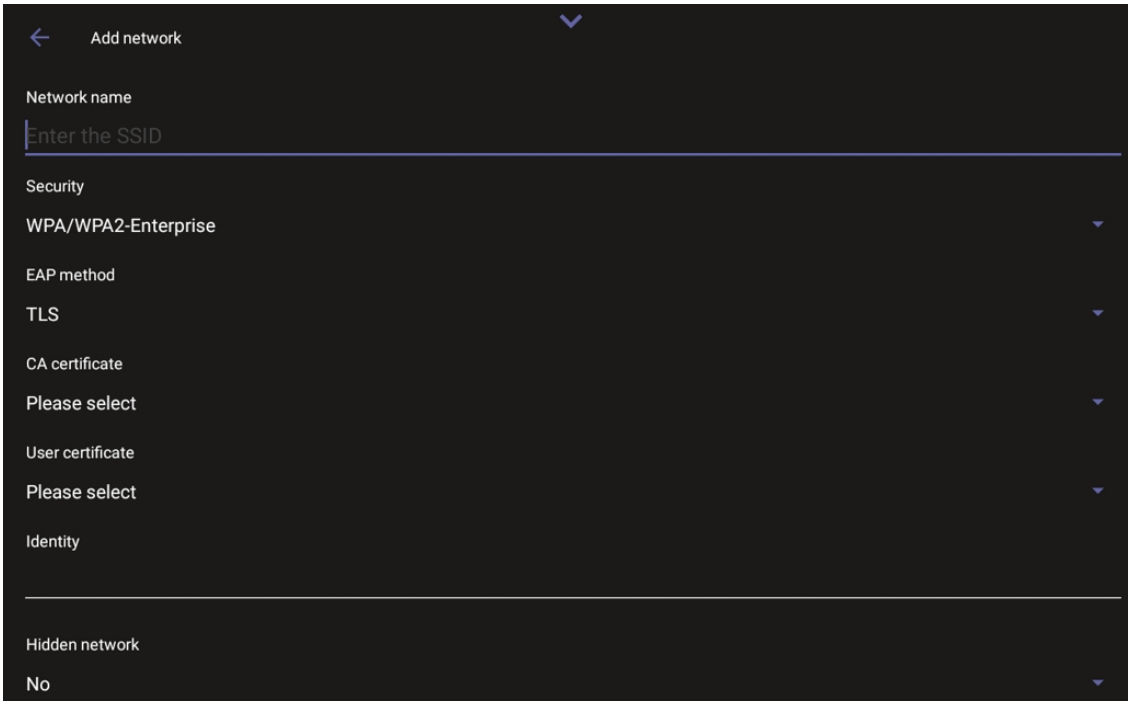
To configure a Wi-Fi network using certificate-based authentication (EAP-TLS), administrators must first load the required private certificates into the device. This includes the CA certificate, the client certificate, and the associated private key. Certificates can be loaded either manually or via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



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

```
network/wireless/eap_method=TLS
```

```
network/wireless/ca_cert=
```

```
network/wireless/client_cert=
```

Example Configuration

Below is an example of the Wi-Fi parameters after configuration:

```
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 VLAN via DHCP Option when CDP-LLDP is Not Allowed

AudioCodes Android devices can configure VLAN via a DHCP Option when CDP/LLDP is not allowed in the organization. The following DHCP Options offer a VLAN ID: Option 43, 132, 128, 129, 144, 157, 191. If the device gets more than one of these DHCP Options, it will apply only one according to the aforementioned order of priority.

Administrators can automatically configure **VLAN Discovery Mode** to CDP/LLDP/CDP+LLDP to get VLAN via a DHCP Option, or manually as described below. If VLAN Discovery Mode is disabled, the devices will not get VLAN via a DHCP Option.



- When CDP/LLDP is allowed in the organization, devices will get VLAN via CDP/LLDP Discovery; they will not get it from a DHCP Option. LLDP/CDP Discovery takes precedence over a DHCP Option.
- Valid range of VLAN ID values: 0~4094.

The following table specifies the syntax to use for the different DHCP options.

Table 3-2: DHCP Option Syntax

DHCP Option	Syntax
DHCP Option 43 (vendor-encapsulated-options)	DHCP Server, for MSCPEClient Vendor Class, 010 VLANID (VLAN identifier) has two types: ■ VLANID=544(string), packet: 0a0400353434, VLANID=544 ■ VLANID=0x10(Hex), packet: 0x0a 0x02 0x00 0x10, VLANID=16
DHCP Option 128/129/144/157/191	Syntax: VLAN-A=<value>;(value=hex, octal or decimal). Examples: ■ VLAN-A=12 VLAN ID is decimal 12.

	■ VLAN-A=0xc VLAN ID is Hex 0xc (i.e., decimal 12). ■ VLAN-A=014 VLAN ID is octal 014 (i.e., decimal 12).
DHCP Option 132	Syntax: <value>; only supports a decimal value. ■ Example: 5 VLAN ID is 5.

Lock or Unlock the Phone

As a security precaution, the phone can be locked and unlocked:

- Automatic lock (see Automatic Lock below)
- Unlock (see Unlock below)

Automatic Lock

Users can lock their phones as a security precaution. To configure the phone with a screen lock option, see the 'Security' setting in Configure C470HD Device Settings on page 23.


You cannot lock the phone if the lock option is not configured.

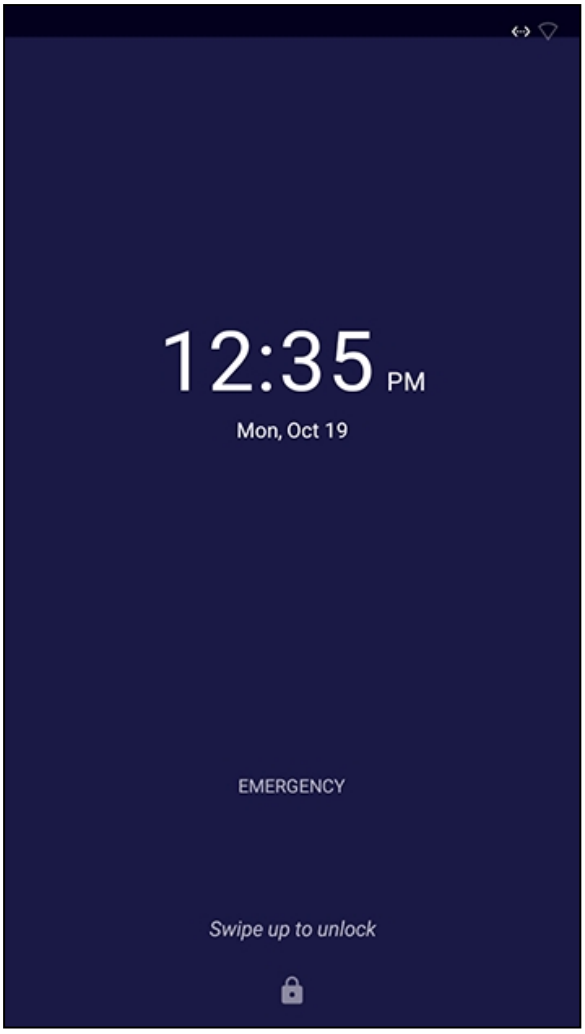
➢ **To lock the phone:**

- Press the back key on the phone for at least three seconds for the device to automatically lock.

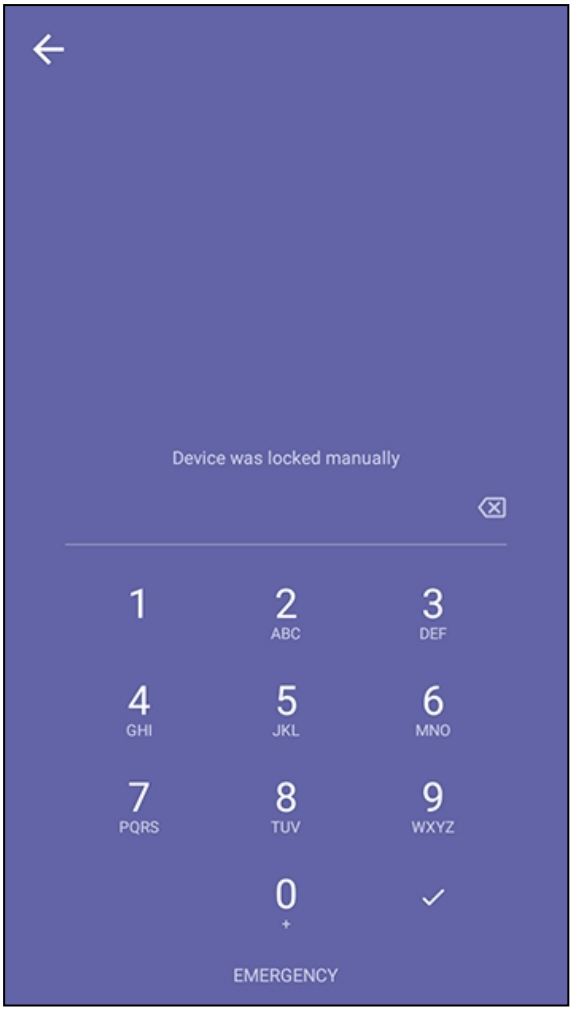
Unlock

➢ **To unlock the phone:**

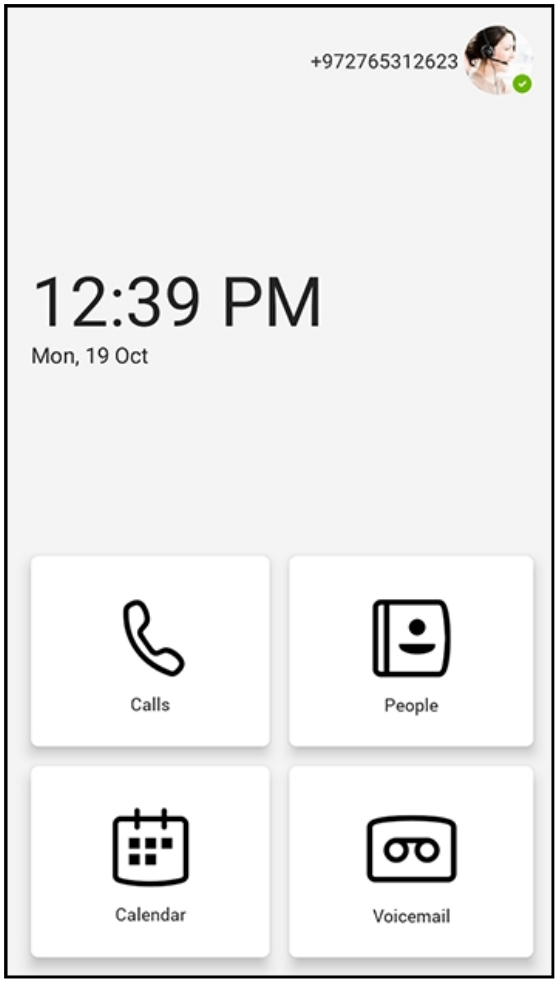
1. When the screen shown in the figure below is displayed, tap the lock icon and swipe up.



2. In the virtual keyboard that opens, start typing your unlock PIN code; the phone displays the digits as you type.



3. When the phone detects the unlock code, it unlocks.

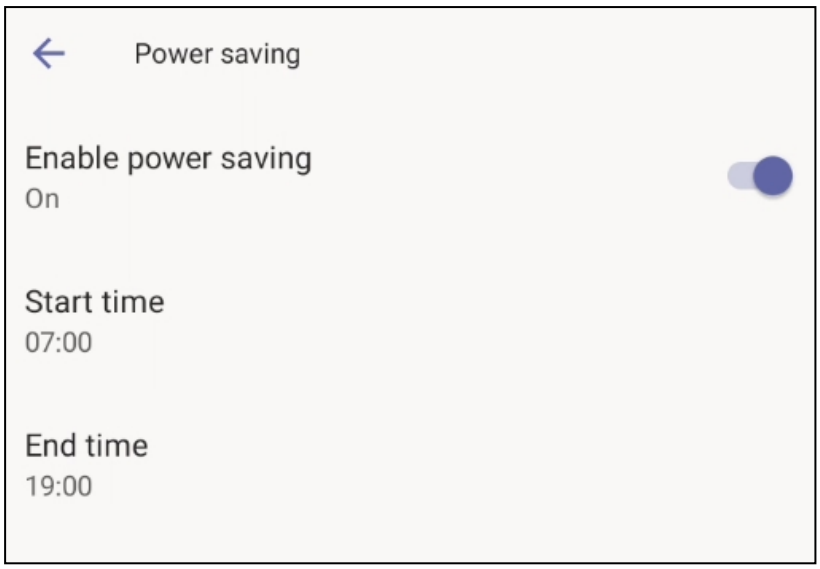


Enable Power Saving

This feature automatically activates power-saving mode during non-working hours. By default, during off hours, the phone's uppermost-right Presence LED is switched off. This conserves energy and minimizes light disturbance, providing a seamless and efficient user experience.

➢ **To enable this feature:**

- In the phone screen, navigate to **Device Settings** > **Power saving**.



- By default, the feature is enabled.
- The feature is based on off work hours.

The Configuration File parameters below also support the feature. They can be synchronized with the settings in the phone screen.

- `general/power_saving` – by default set to `1` (power saving enabled)
- `office_hours/end`
- `office_hours/start`

The **Enable power saving** setting does not control the screen saver or dim the LCD. To configure these settings, see **Device Settings > Display** in Configuring Device Settings.

Restore the Phone to Default Settings

Users can restore the device to factory default settings at any time.

Click here to view a video clip showing how to reset the AudioCodes Teams phone to its factory default settings. The principle is similar across all AudioCodes Teams phones.

The feature can be used if the Admin user has forgotten their password, for example.

Restoring the phone to factory default settings brings up the phone with its original bundled Teams application.

Two kinds of restore are available:

- Perform a Hard Restore on the next page
- Perform a Soft Restore on the next page

You can also:

- Perform User Data Reset below
- Start up the Phone from Recovery Mode on the next page
- Perform Manual Recovery Operations on page 54

Perform a Hard Restore

You can restore the phone's settings to their defaults when the phone is up and running.

➢ **To perform a hard restore while the phone is up and running:**

1. Long-press the **HOLD** key on the phone (30 seconds); the screen shown below is displayed and the device performs a restore to default factory settings.



   After the restore, the phone automatically reboots and goes through the Wizard and sign-in process.

2. Select **OK**; the sign-in screen is displayed (see Sign In to Your device Teams Phone on page 15 for more information).

Perform a Soft Restore

Users must log in as Administrator to perform a soft restore.

➢ **To perform a soft restore:**

1. Log in as Administrator on page 107.
2. On the phone's Device Settings screen, scroll down and tap **Debugging**, then **Erase all data (factory reset)**.A

Perform User Data Reset

AudioCodes Teams devices provide a **User data reset** option that is similar to factory reset except that it preserves predefined data after firmware upgrade. The option enables the data to be retained to handle devices more efficiently in scenarios where the factory reset option is inappropriate.

➢ **To access the functionality:**

1. Log in as Administrator on page 107.
2. On the phone's Device Settings screen, scroll down and tap **Debugging**, then **User data reset**.

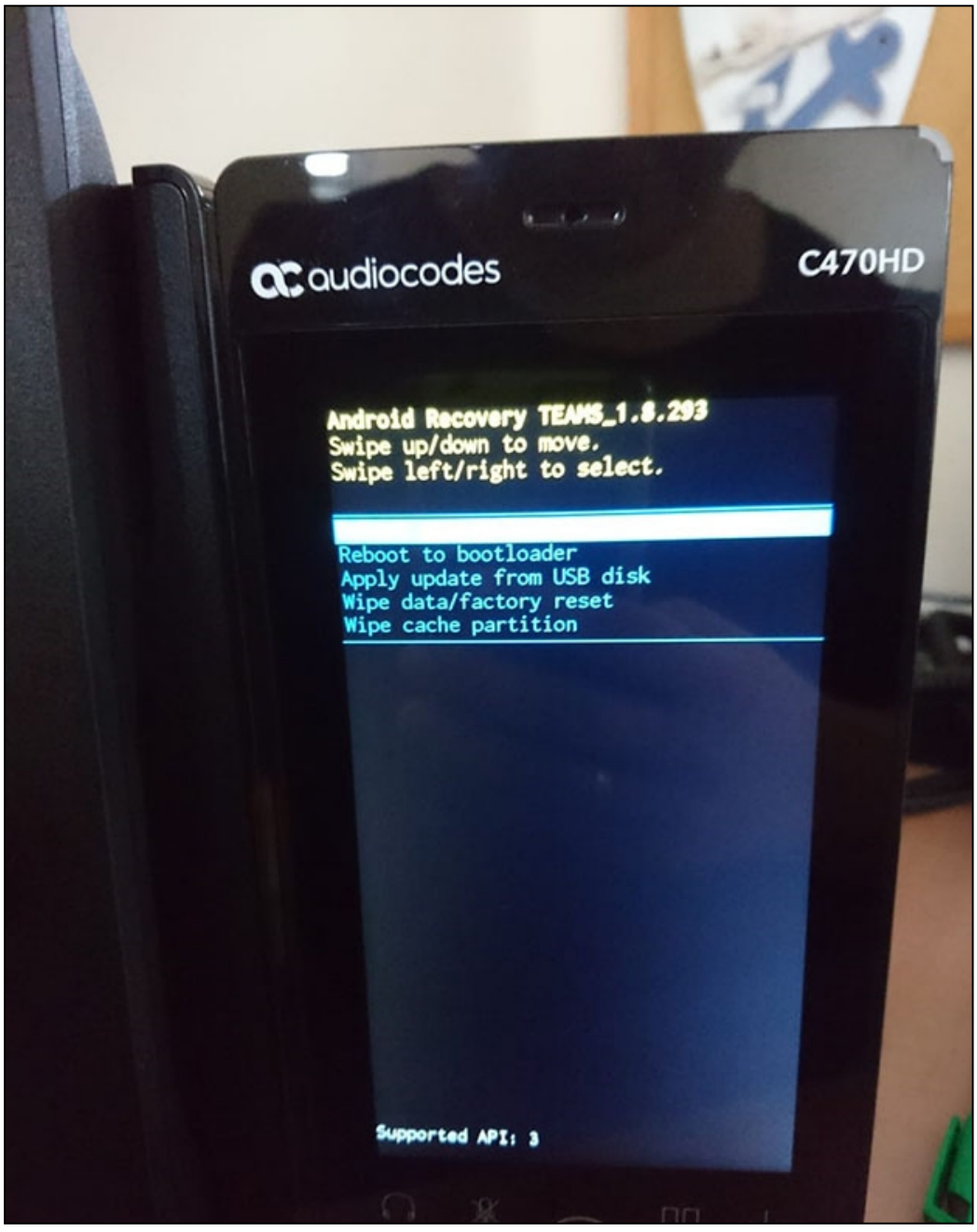
After 'User data reset', network settings are preserved.

Start up the Phone from Recovery Mode

If a phone goes into recovery mode, you can boot it using the touch screen.

➢ **To boot the phone:**

1. In the screen of the phone that has gone into recovery mode, swipe down or up to navigate to **Reboot to bootloader**.



2. Swipe left or right to select the option; the phone reboots and the issue is resolved.

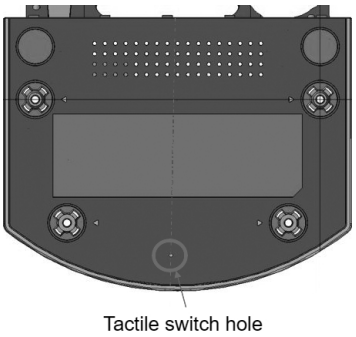
Perform Manual Recovery Operations

Besides manual recovery options, the Android phones also feature an independent, automatic problem detection and recovery attempt capability that can culminate in recovery mode or in switching image slots. Android phones also feature a 'hardware watchdog'. This feature resets the phone if Android is stacked and doesn't respond (though Android stacking is unlikely). There's no recovery process; the phone is only reset.

All AudioCodes devices have a reset key or a combination of keys on the keypad to reset it.

Click here to view a video clip demonstrating how to recover the phone and reboot it to its original out-of-the-box state. The principle is similar across AudioCodes Teams phones.

The following figure shows the reset key located on the base of the C470HD.



While a device is powering up, you can perform recovery operations by long-pressing the device's reset key.
When long-pressing the reset key, the device's main LED changes color after every *n* seconds; each color is aligned with a recovery operation option.

When?	Action	Press for how long?	LED flashes 3x after release
Start pressing immediately after power up (on U-Boot / Universal Boot Loader)	Recovery mode (you can restore defaults from there)	~ 4 seconds	Red
	Switch slots A / B	~ 10 seconds	Green
	Loader	~ 15 seconds	Blue / Yellow
	Restore defaults	~25 seconds	Green + blue / Green + yellow

When?	Action	Press for how long?	LED flashes 3x after release
When successfully booted (on Android)	Reboot	From the 'Admin' menu	-
	Restore defaults	Long-press **Hold** key for ~15 seconds	Flashes yellow once after release

4 Use Your Phone

Your phone allows you to perform a multitude of operations, including:

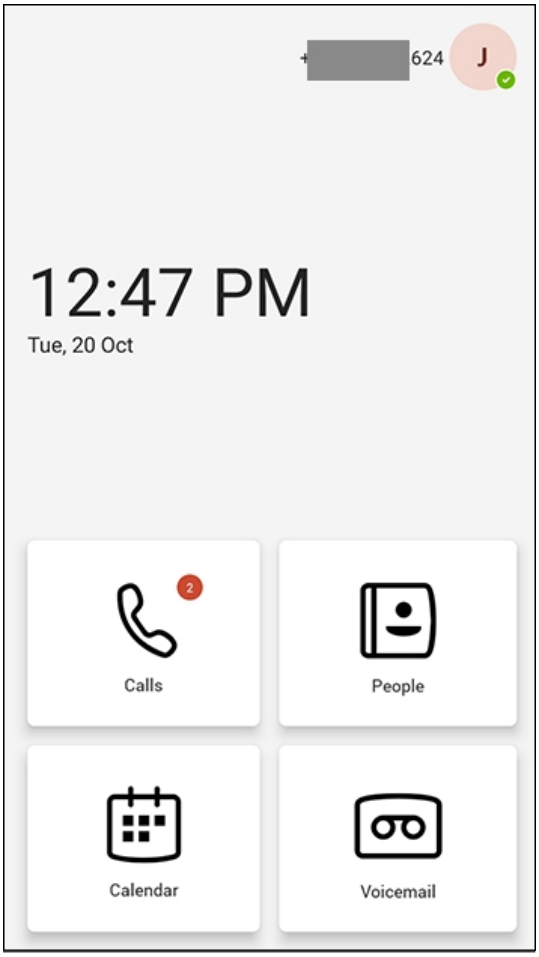
- Get Acquainted with the Phone Screen below
- Change Your Presence Status on page 60
- Configure Teams Application Settings on page 62
- Make and Manage Calls on page 67
- Answer Calls on page 78
- Create and Manage Contacts from the People Screen on page 83
- Manage Speed Dial and Line Keys on page 84
- Manage Meetings on page 93
- Manage Voicemail on page 97
- Other Operations on page 99
- Sign Out on page 103



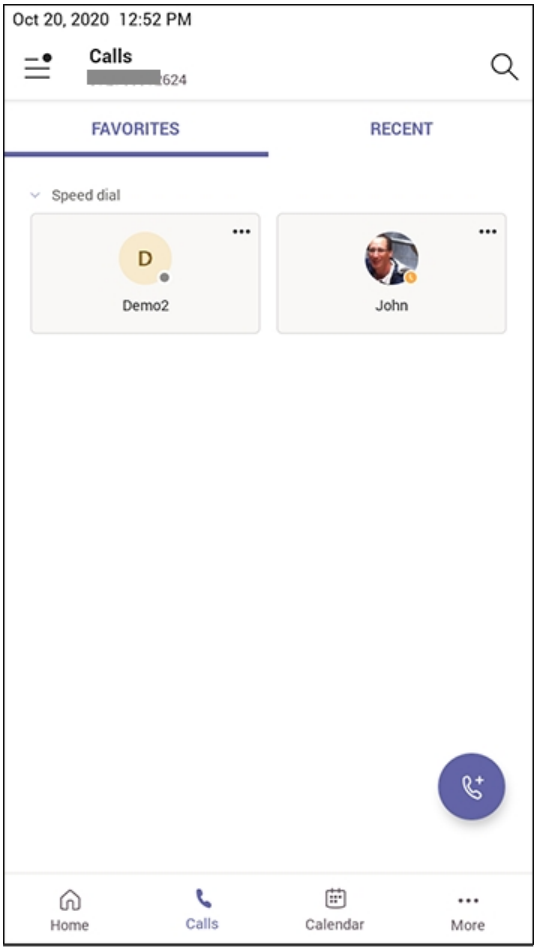
This manual describes a Microsoft Teams IP phone. The above phone operations are implemented Microsoft Teams functions.

Get Acquainted with the Phone Screen

The following gets you acquainted with the phone’s user interface. The figure below shows the phone's default home screen, aka the phone's idle screen.



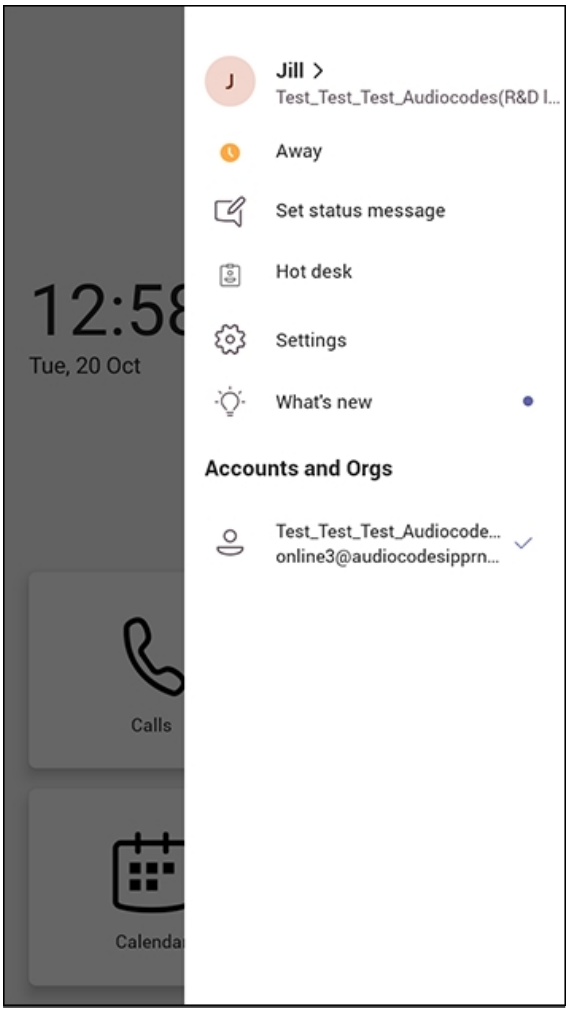
The following figure shows the phone's Calls screen.



The following table describes the phone's home screen.

Item	Description
Calls	Tap the tab to open the Calls screen. The screen shown in the figure preceding this table opens.
People	Tap the tab to open the People, shown under Create and Manage Contacts from the People Screen on page 83. Allows you to easily connect and collaborate with teammates, colleagues, friends and family. Through this screen, you can see all your contacts and create and manage contact groups to organize your contacts. The screen provides a simple user experience and aligns with the contacts on the Teams desktop client. If a contact has multiple numbers, the phone screen allows the user to select from a drop-down menu the intended contact method.
Calendar	Tap to open the Calendar screen, shown under Setting up a Meeting.
Voicemail	Tap the tab to open the Voicemail screen (see View and Play Voicemail Messages on page 97).

The following figure shows the user's presence status screen. To access this screen, tap your avatar.



Use this table as reference.

Item	Description
Presence status	See Change Your Presence Status below.
Set status message	See Set a Status Message on the next page.
Connect a device	See Connect a Device on page 102.
Hot desk	See Set up a Phone for Hot Desking on page 72.
Settings	See Configure Teams Application Settings on page 62.
Lock	See Lock or Unlock the Phone on page 47.

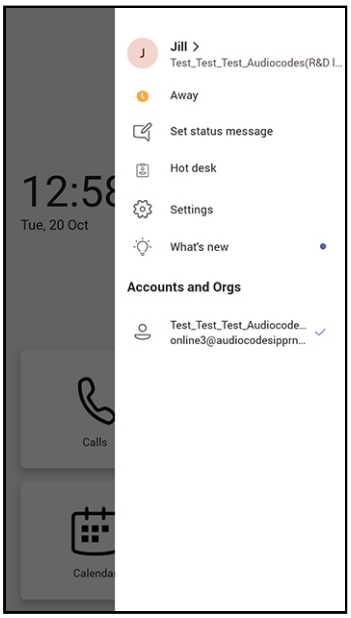
Change Your Presence Status

You can assign a presence status to control whether you want people to contact you or not. By default, your status is based on your Microsoft Teams server.

- After *n* minutes (configured in the Teams server by your administrator), presence status automatically changes to 'Inactive'.
- *n* minutes after this (also configured in the Teams server by your administrator), presence status automatically changes to 'Away'; all calls are then automatically forwarded to the Response Group Service (RGS) if it is configured.

➢ To change your presence status:

1. In the home screen, tap the user (avatar) picture.



2. Tap the current status displayed and from the drop-down list of statuses then displayed, tap the status to change to. Use this table as reference.

Table 4-1: Presence Statuses

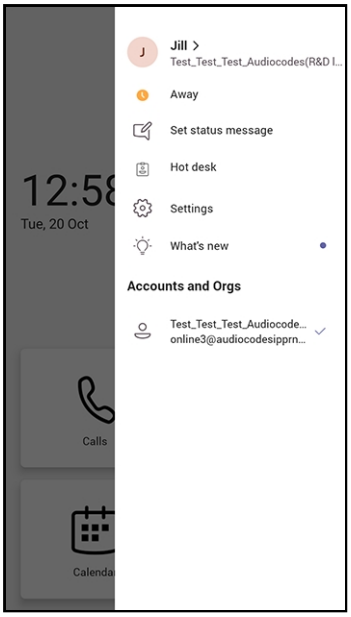
Icon	Presence Status	Description
	Available	You're online and available for other contacts to call.
	Busy	You’re busy and don’t want to be interrupted.
	Do not disturb	You don’t want to be disturbed. Stops the phone from ringing when others call you. If DnD is activated, callers hear a tone indicating that your phone is busy; the call is blocked and your phone's screen indicates 'Missed Calls'.
	Be Right Back	You'll be away briefly and you'll return shortly.
	Away	You want to hide your status and appear to others you're currently away.
	Offline	You're going on vacation (for example).
	Reset status	Resets the status.

Set a Status Message

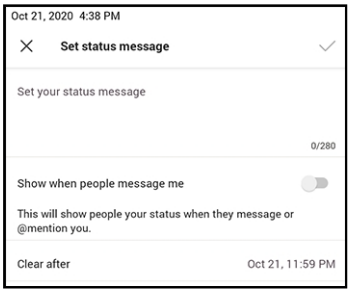
You can set a status message to add more substance to your presence status. For example, a status message such as 'Working from home' adds more substance to the presence status of 'Available'.

➢ **To set presence status:**

1. In the home screen, tap the user (avatar) picture.



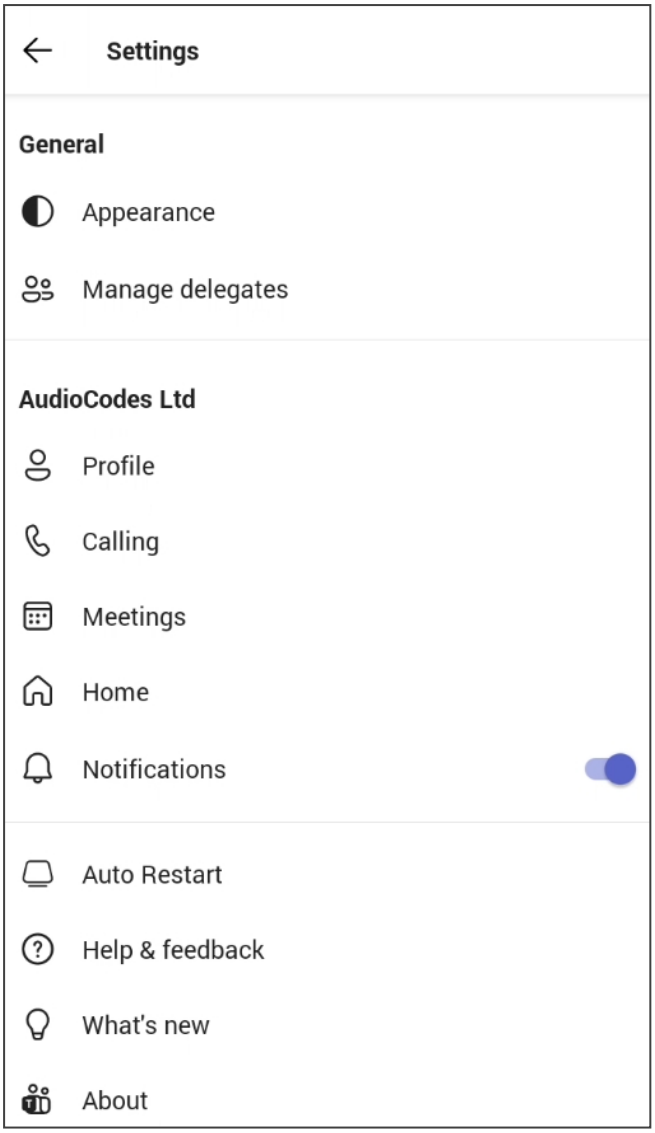
2. Tap **Set status message**.



3. Tap the field under **Set status message** and in the Virtual Keypad that pops up, type in the message you want to show other people, for example, **Working from home**. The text you type in will replace 'Set status message' in the screen shown in the preceding figure.
4. Optionally, switch on **Show when people message me**. When people message or @mention you, they'll view the status message you set.
5. Tap **Clear after** and choose when you want the message to stop displaying. Options are:
   - Never clear
   - 1 hour
   - 4 hours
   - Today
   - This week
   - Custom (set a date and time in the calendar that pops up)

Configure Teams Application Settings

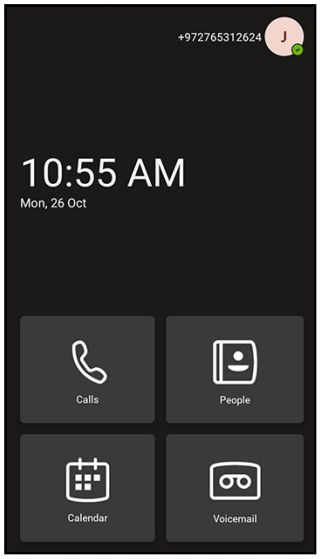
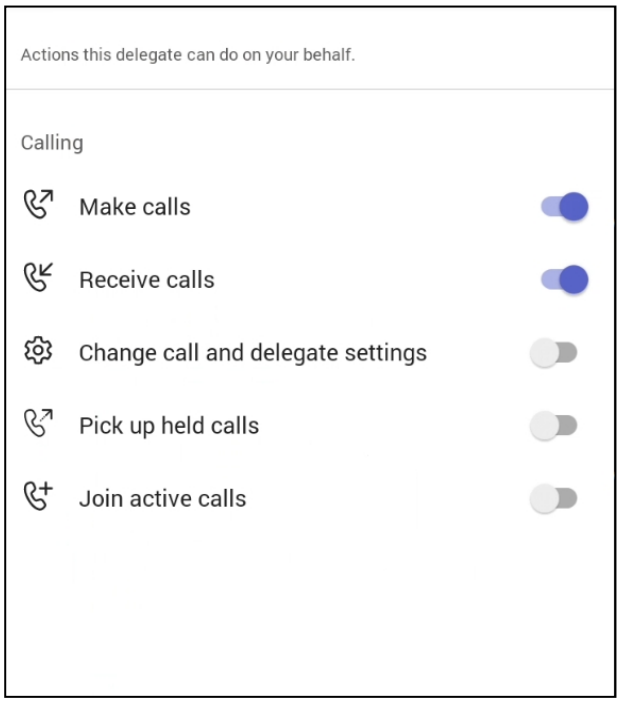
The following describes the Teams application's settings. To access them, tap the avatar and then tap **Settings**.

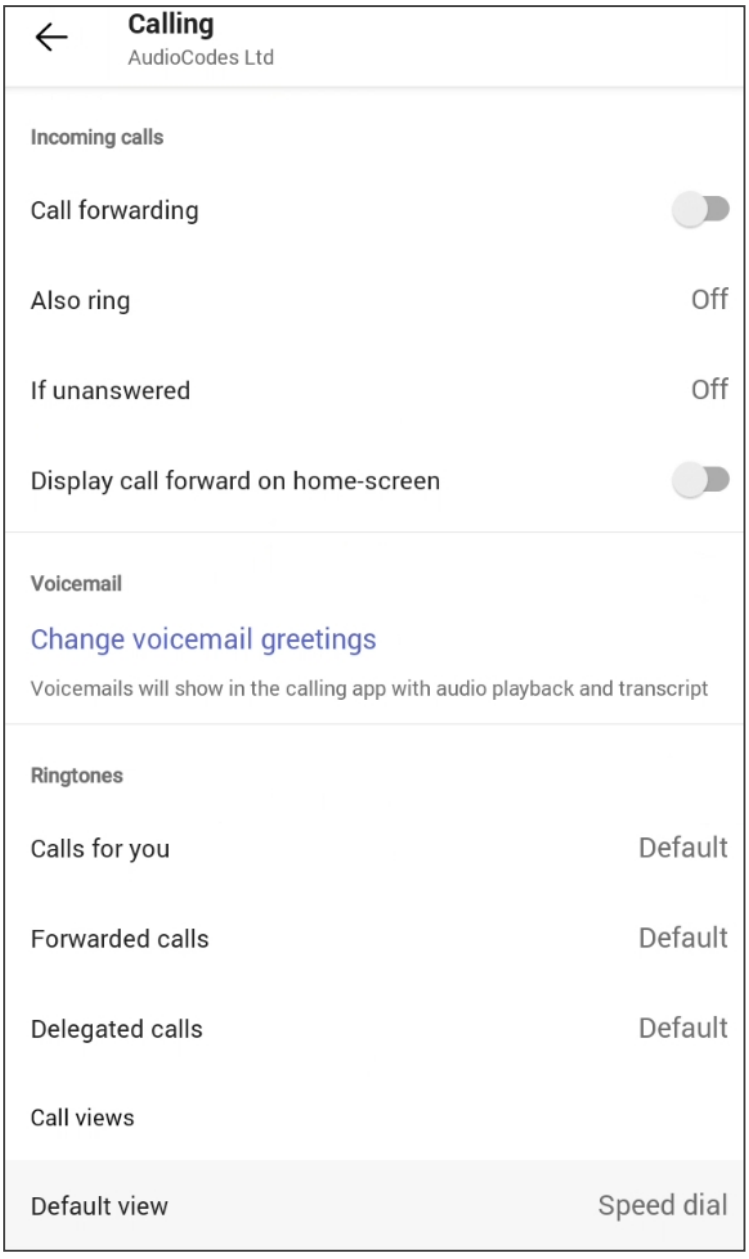


Use this table as reference:

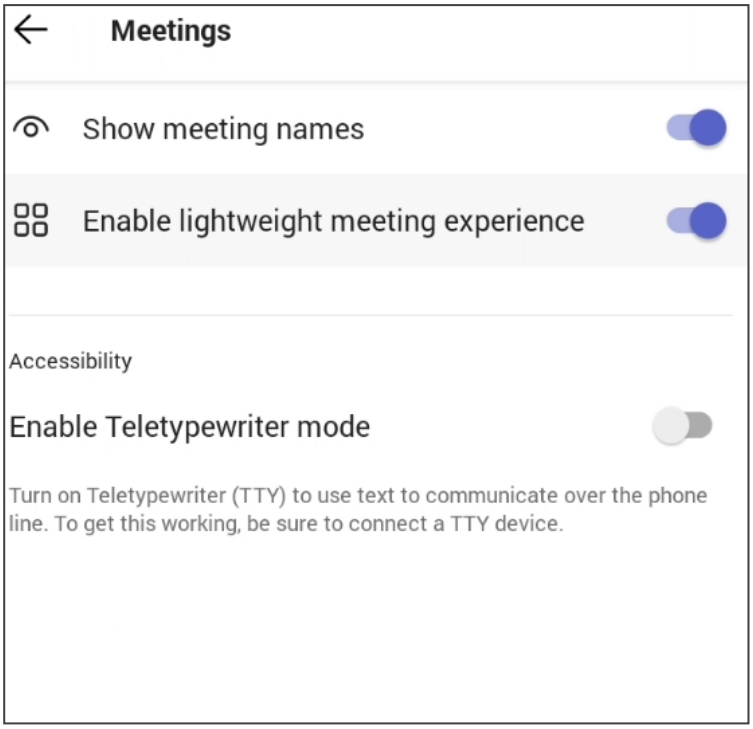
Table 4-2: Idle Screen Description

Item	Description
Appearance	Dark Theme can be enabled to suit user preference (default is Light Theme). To enable Dark Theme: 1. Under 'Themes', tap **Dark**; the following prompt is displayed:  2. Choose **Restart** and then verify after the Teams application restarts that all screens (Teams application and Device Settings) are dark themed:

Item	Description
	
Manage Delegates	Delegates are users allowed to make and receive calls on the phone on the behalf of the phone owner. Delegates are used in boss-delegate configurations (see Use Boss-Admin on page 72). To add a delegate: 1. Under 'Manage delegates', search for and tap the requested contact. 2. Enable or disable the actions that the delegate is allowed to perform, as required, then tap the checkmark. The delegate is added to the list under 'Manage delegates'. 

Item	Description
Profile	Opens the user's email address, phone numbers, and photo / avatar picture.
Calling	Opens the Calls screen.  **Incoming Calls** ✓ **Call forwarding**. Enables automatically redirecting an incoming call to another destination. ✓ **Forward to**. Only displayed if 'Call forwarding' (the previous setting) is enabled. Defines the destination to which to forward incoming calls. ✓ **Also ring**. Only displayed if 'Call forwarding' is disabled.

Item	Description
	Tap either **Off**, **Contact or number**, or **Call group**. ✓ **If unanswered**. Only displayed if 'Call forwarding' is disabled. Defines the destination to which to forward unanswered incoming calls. Tap either **Off**, **Voicemail**, **Contact or number**, or **Call group**. ✓ **Display call forward on home-screen**. If enabled, displays a dropdown on the home screen, allowing you to specify the requested call forward action (**Don't forward calls**, **Forward to voicemail**, or **Forward to contact or number**). ■ **Voicemail > Change voicemail greetings**. Lets you record a message for voicemail, before the caller's message is recorded. ■ **Ringtones**: Set the requested ringtones for personal calls, forwarded calls, and delegated calls. ■ **Call Views > Default view**. Specify if the Calls screen should display the Speed Dial list or the recent call history. ■ **Line Keys > Line keys settings**. Manage line keys and set line key behavior. ■ **Enable voice quality recording**. Activate to attach a recording of the call when you report a problem to Microsoft Support. ■ **Emergency location**. Set a location where responders can reach you in the case of an emergency. ■ **Accessibility** ✓ **Enable Teletypewriter mode.** Enable to communicate over the phone line using text. ✓ **Answer on Pickup.** Automatic answer of calls when the handset is lifted or the speaker button is pressed.
Meetings	Opens the Meetings screen, from which you can configure meeting settings.

Item	Description
	
Home	Select what the home screen should display by default: Default view, favorites, recent call history, or line keys.
Notifications	Default: On (enabled). Allows notifications to be displayed. Slide left to switch off (disable); notifications will not be displayed.
What's new	Links to the 'What's new' page of Microsoft Teams devices.
About	Opens the About screen of Microsoft Teams.
Sign out	Lets you sign out of the phone application as one user and optionally sign in again as another user. See Sign Out on page 103 for detailed information.
Device Settings	Opens the [Device] Settings screen. See Configure C470HD Device Settings on page 23 for detailed information.

Make and Manage Calls

You can:

- Make a Call on the next page
- Make an Emergency Call on page 69
- End an Established Call on page 71
- Manage Call History on page 71

- Park a Call on the next page
- Set up a Phone for Hot Desking on page 72
- Use Boss-Admin on page 72
- Page to a Group of Phones (Multicast) on page 73

Make a Call

Calls can be made in multiple ways. In the phone's home screen, for example, tap **Calls**.

In the Calls screen that opens, tap .

In the 'Make a call' screen, tap the field 'Search for people' and use the virtual keyboard to input the name of person to call -OR- tap **?123** in the lower left corner and input the phone number of the person to call.

After dialing a destination number, the phone displays the Calling screen while playing a ring-back tone.

➢ To toggle between mute and unmute:

- Tap  on the phone. Tap it again to revert.

  You can mute the phone during a call so that the other party cannot hear you. While the call is muted, you can still hear the other party. Muting can also be performed during conference calls.

➢ To toggle between device and speaker:

- Tap  on the phone.

➢ To end a call before it's answered at the other end:

- Touch 

➢ To dial a URL:

1. Press the speaker key or lift the handset.
2. Use the virtual keyboard to input the URL address. To delete (from right to left), tap the clear key.

Dial a Missed Call

The phone logs all missed calls. The screen in idle state displays the number of missed calls adjacent to the Calls softkey.

➢ **To dial a missed call:**

- On the home screen, tap **Calls** and then in the Calls screen under the **RECENT** tab, tap the missed call to dial.

Select to Dial

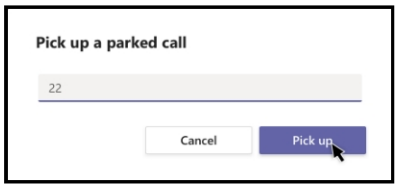
All phone numbers that are part of meeting invites or user contact cards can be dialed out directly by tapping them via the phone screen.

Park a Call

The phone allows a user to park a call, i.e., transfer a call to a "parking lot" for it to be picked up on any other phone in the enterprise by a party who must enter a code to retrieve it.

➢ **To park a call:**

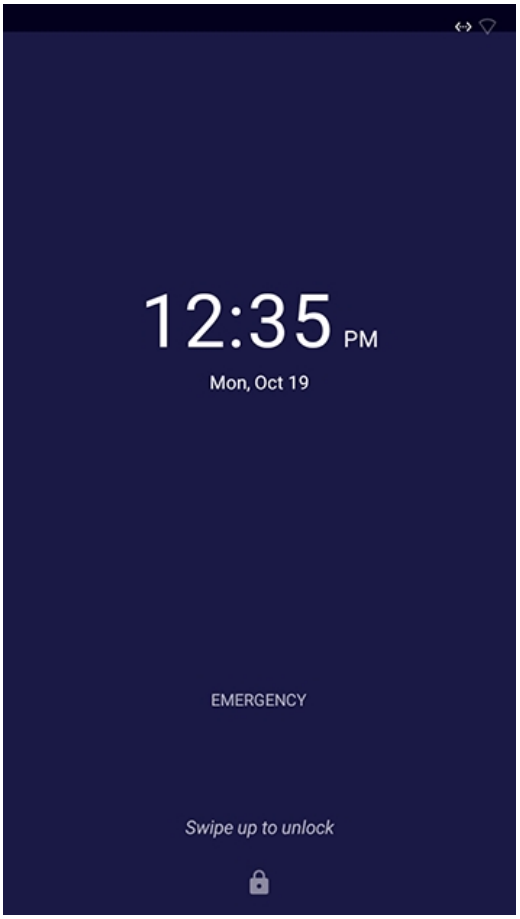
1. Put the call on hold and park it; you'll receive a unique code from the Teams application.
2. Communicate the code to another user who can then pick up the call on their device. The user on the other device taps the call park icon displayed in their device's Calls screen.



3. The user on the other device enters the code communicated to them and then taps the **Pick up** button to pick up the call.

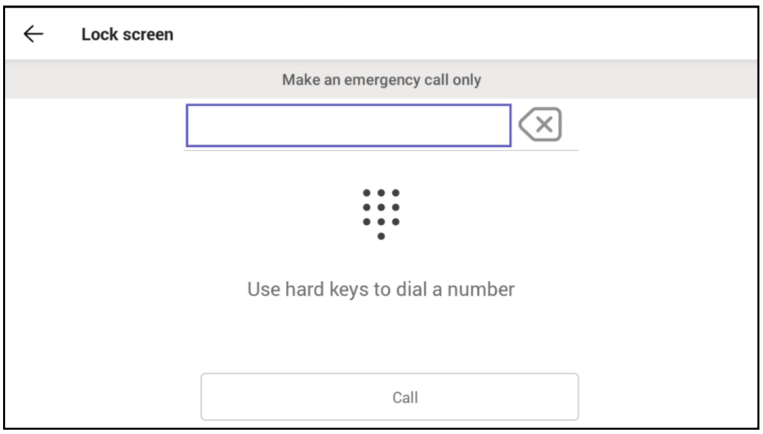
Make an Emergency Call

If your user is assigned an emergency calling policy (configured from the Teams Admin Center), the phone allows you to make an emergency call without unlocking the phone first. The idle lock screen displays an **EMERGENCY** button.



➢ **To dial the service from the locked idle screen:**

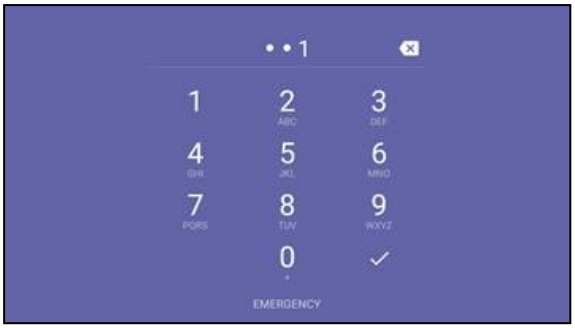
- Tap **EMERGENCY** in the locked idle screen and then enter the emergency number.



-OR-

- Dial from the dial pad without needing to use the **EMERGENCY** key:

  a. Dial **911**.



b. Activate the speaker button on the phone.

c. View the 'Emergency call' screen displaying the dialed emergency number.

- When the phone detects that 911 has been entered or dialed, it automatically calls that number.
- If you enter or dial a number that is not an emergency number, a message is displayed indicating that only emergency numbers can be called.

End an Established Call

You can end an established call in a few ways.

➢ **To end an established call:**

■ Return the handset to the phone cradle if it was used to take the call -or- activate the headset key on the phone -or - activate the speaker key on the phone -or- tap the **End** softkey.

Manage Call History

You can view a history of missed, received and dialed calls.

Each device reports every call from or to that user to the server. All devices that a user signs into and the Calls screen are synchronized with the server.

➢ **To manage calls:**

1. Tap **Calls** and in the Calls screen, tap **Recent**.

- Calls are listed from newest to oldest.
- Missed call indicates a call that was not answered.
- Incoming and outgoing calls are differentiated by their icon.

2. Tap a call in the list to call someone back.

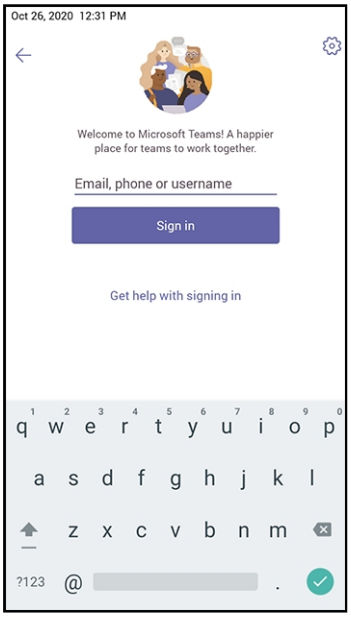
Set up a Phone for Hot Desking

The hot desk feature allows a user to sign in to a phone that is already signed in to by another user without signing out the original user to whom the phone was assigned for primary use.

Any phone in the enterprise network that is enabled with this feature allows any user in the enterprise to temporarily sign into it, make calls, attend meetings and access their calendar and call log. After finishing using these phone functions, the user can sign out to end their hot desk session; call logs and history will automatically be removed from the device.

➢ To set up a phone as a shared device for hot desking:

1. Tap the user's photo or avatar picture, and then from the menu, tap the **Hot desk** option.



2. Tap the field **Email, phone or username**, use the Virtual Keyboard to type in your email, phone or user name and then tap **Done**; the phone is enabled for hot desk.

Use Boss-Admin

Bosses can share their phone line with their assistants|delegates to make and receive calls on their behalf. To set up delegates, see *Manage Delegates* in Configure Teams Application Settings on page 62.

See here a video clip showing how to set up the feature. The principle is the same across all Teams phone models.

A boss can:

- View and join active calls handled by delegates as a boss
- Grant delegates permission to join active calls and resume calls

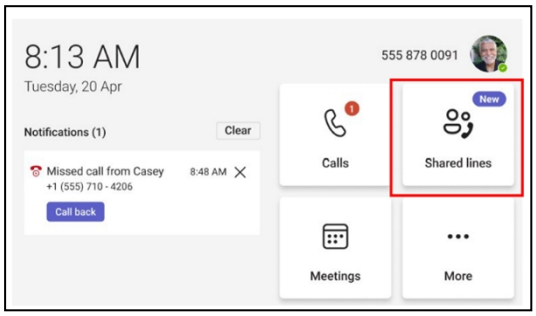
A delegate can:

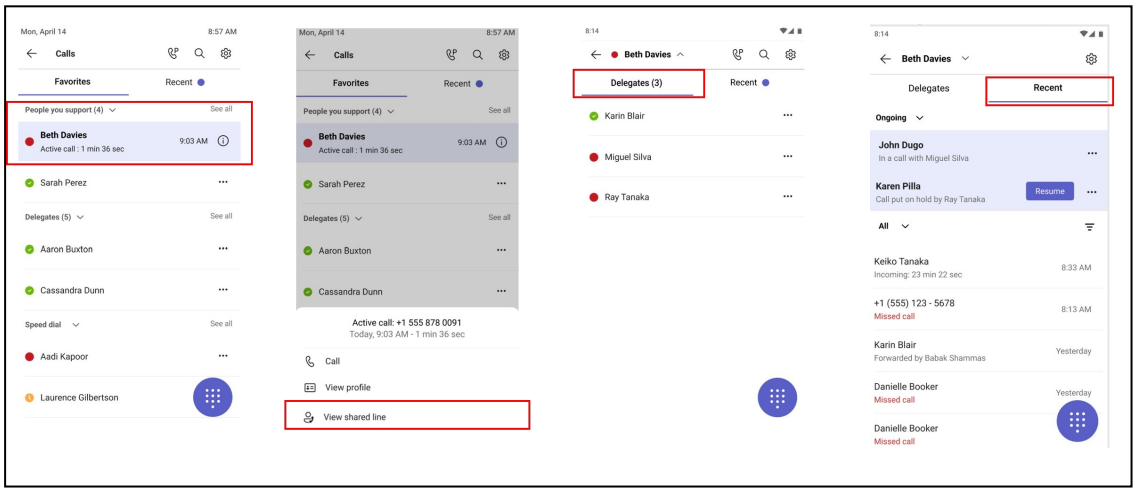
- View shared call history per boss' line

- Switch between different lines easily
- View other delegates managing a boss

➢ **To set up the feature:**

- Use the screenshots below as reference.





Page to a Group of Phones (Multicast)

AudioCodes Android-based phones support multicast paging (including barge-in). The feature allows a call to be paged to a group of phones to notify a team about (for example) the time and place at which a meeting will commence. The paging call is multicast via a designated group IP address, in real time, on all phones in the group.

Barge-in enables paging to interrupt (barge in on) phone conversations that are in progress. The feature is configured in the phone's cfg configuration file. Default: Disabled. When enabled, a paging call overrides an ongoing regular call/meeting due to emergency. When disabled, those who are in regular calls when a paging call comes in are prompted in the phone screen to accept or reject the paging call. If it's accepted, the regular call is put on hold and the paging is heard.

Related paging parameters in the cfg configuration file are:

```
/voip/services/group_paging/enabled
/voip/services/group_paging/codec
/voip/services/group_paging/group/*/activated
```

```
/voip/services/group_paging/group/*/multicast_addr
/voip/services/group_paging/group/*/port
/voip/services/group_paging/allow_barge_in/enabled
```



The values of these parameters can be changed on the fly. Paging behavior is immediately affected.

Use the following table as reference.

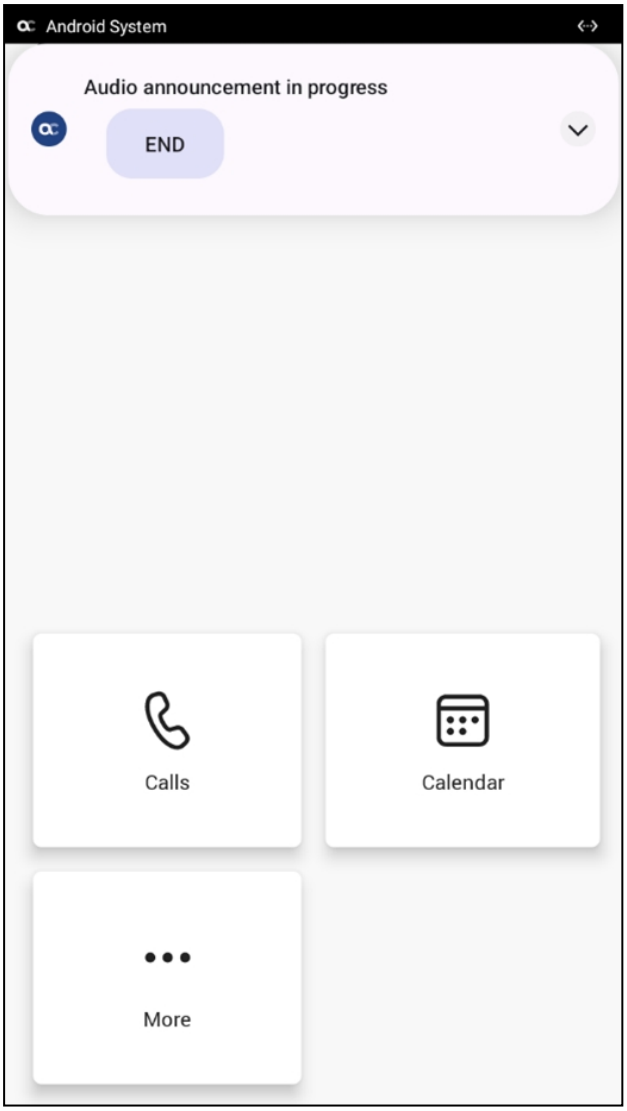
Parameter	Description
voip/services/group_ paging/allow_barge_ in/enabled=0	Allows | disallows the barge-in feature. ■ 0 = disabled ■ 1 = enabled
voip/services/group_ paging/codec=PCMU	Defines the codec. Three available options: ■ PCMU (default) ■ PCMA ■ G722
voip/services/group_ paging/enabled=0	Enables | disables the group paging feature. ■ 0 = disabled ■ 1 = enabled
voip/services/group_ paging/group/0-4/activated=0	Activates| deactivates a group. ■ 0 = deactivated ■ 1 = activated Five groups labeled 0-4 are available.
voip/services/group_ paging/group/0-4/multicast_ addr=224.0.1.0	Defines the paging group's multicast IP address. Must be in the range: 224.0.0.0 - 239.255.255.255 Default: 224.0.1.0. **Important**: For phones to be in a group, all must be configured with the identical multicast address and port. The following three IP addresses (for example) denote three different paging groups: ■ 224.0.1.1:8888

Parameter	Description
	■ 224.0.1.1:2222 ■ 233.2.2.2:8888
voip/services/group_ paging/group/0-4/port=8888	Defines the port through which paging is received. Must be in range: 1-65535 Default: 8888 **Important**: For phones to be in a group, all must be configured with the identical multicast address and port. Port 9998 and 9999 should not be used as they are used by the application.



- AudioCodes Android-based phones currently support incoming paging calls (listening).
- Outgoing paging calls (broadcasting) will be supported in the future.

■ When an incoming call is received on a phone that is in idle state, the phone *immediately and automatically* answers it, irrespective of whether barge-in is enabled or not.



- When the phone is in a Teams call/meeting (active or on-hold):
  - If barge-in is enabled, i.e., if the cfg configuration file parameter 'voip/services/group_paging/allow_barge_in/enabled'=**1**, then the phone will *automatically immediately* display the **Audio announcement in progress** screen with an option to END the announcement.



- If barge-in is *disabled*, i.e., if the cfg configuration file parameter 'voip/services/group_paging/allow_barge_in/enabled'=**0**, then the phone will display the **Incoming audio announcement** screen with an option to ACCEPT or DECLINE it.



Answer Calls

You can answer or manage incoming calls and configure related settings:

- Answer a Call below
- Transfer a Call on the next page
- Reject an Incoming Call and Send It Directly to Voicemail on page 80
- Adjust Volume on page 80
- Play Incoming Call Ringing through USB Headset on page 82
- Opt in or out of Call Queues on page 82

Answer a Call

The phone indicates an incoming call by ringing and displaying **Caller X is calling you**. The LED located in the upper right corner of the phone flashes red, alerting you to the incoming call.

➢ **To answer:**

- Pick up the handset -OR - activate the headset key on the phone (make sure the headset is connected to the phone) -OR- activate the speaker key on the phone -OR- tap the **Accept** softkey (the speaker is automatically activated).

Transfer a Call

When an incoming call arrives or during a call, you can transfer the call:

- Tap **Transfer**, then tap **Transfer now** – opens a dialog to select a contact to transfer the call immediately.
- Tap **Transfer**, then tap **Consult first** – opens a dialog to select a contact for consultation before completing the transfer.

See here for a video clip demonstrating how to use the call transfer feature while checking with the intended recipient that they want to take the call. The principle is similar across AudioCodes Teams phones.

See here for a video clip demonstrating how to immediately transfer a call without verifying with the intended recipient that they want to take the call. The principle is similar across AudioCodes Teams phones.

➢ **To transfer a call received for another person:**

1. When the incoming call arrives, choose whether to transfer it immediately or not; you can transfer it directly right away, or you can decide to consult the intended recipient of the call to verify that they want to receive it.
2. To consult the intended recipient, select **Consult first** and search for the contact you want to transfer the call to. While you consult with the intended recipient about whether they want to take the incoming call, the caller will hear hold music and will not be a party to your discussion.
3. If the recipient decides to take the call, click the phone icon on the top-right of the screen and then confirm the transfer; the call is then transferred smoothly to the intended recipient.



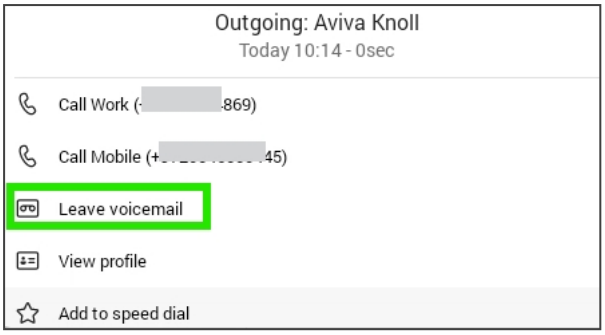
If the recipient does not answer the call, turn on the Safe Transfer toggle button to have Teams ring you back and transfer the call to someone else.

Transfer a Call to Frequent Contacts

To transfer your calls efficiently to frequent contacts, the phone presents frequent contacts in the transfer screen for a single operation transfer. Contacts not shown in the list can be searched for using the search bar.

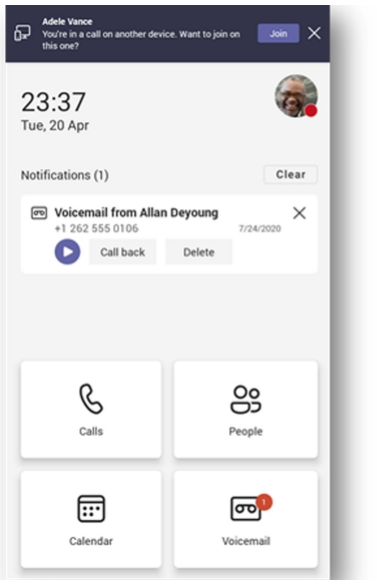
Transfer a Call to Work Voicemail

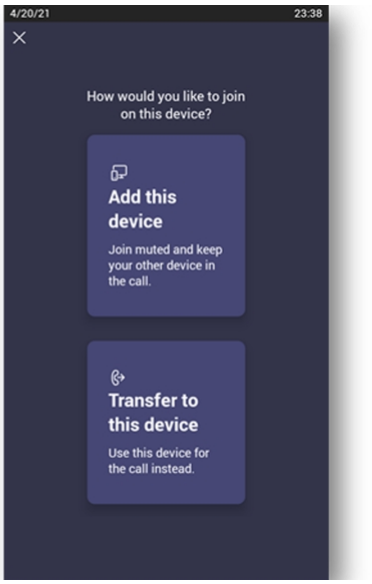
Users can directly transfer a call into someone's work voicemail without needing to ring the far-end user. This allows them to discreetly leave voicemails for users without interrupting them.



Transfer Calls and Meetings across Devices

If a user joins a meeting on their PC, they'll view a prompt suggesting adding their Teams device to split the audio and video, or transferring completely.





The feature enables the user to move away from their PC while seamlessly staying connected. The phone recognizes the user is in a call on another device and prompts them to transfer or add, letting them start their call from elsewhere and transfer to their desk phone.

Reject an Incoming Call and Send It Directly to Voicemail

You can send an incoming call directly to voicemail if time constraints (for example) prevent you from answering it. The caller hears a busy tone from your phone.

➢ **To send an incoming call directly to voicemail:**

- When the phone rings to alert to a call, select **Decline**; if you have voicemail, the call will go into voicemail. The Microsoft Teams server performs this functionality.

Adjust Volume

The phone allows the following volume adjustment actions:

- Adjust Ring Volume on the next page

- Adjust Tones Volume below (e.g., dial tone)
- Adjust Handset Volume below
- Adjust Speaker Volume below
- Adjust Headset Volume on the next page

For more information about sound and volume, see here.

Adjust Ring Volume

The volume of the phone's ring alerting you to an incoming call can be adjusted to suit personal preference.

➢ **To adjust ring volume:**

1. When the phone is in idle state, tap **+** or **-** on the phone..
2. After adjusting, the volume bar disappears from the screen.

Adjust Tones Volume

The phone's tones, including dial tone, ring-back tone and all other call progress tones, can be adjusted to suit personal preference.

➢ **To adjust tones volume:**

1. Off-hook the phone (using handset, speaker or headset).
2. Tap **+** or **-** on the phone.
3. After adjusting, the volume bar disappears from the screen.

Adjust Handset Volume

Handset volume can be adjusted to suit personal preference. The adjustment is performed during a call or when making a call. The newly adjusted level applies to all subsequent handset use.

➢ **To adjust handset volume:**

1. During a call or when making a call, make sure the handset is off the cradle.
2. Tap **+** or **-** on the phone;the volume bar is displayed on the screen. After adjusting, the volume bar disappears from the screen.

Adjust Speaker Volume

The volume of the speaker can be adjusted to suit personal preference. It can only be adjusted *during a call*.

➢ **To adjust the speaker volume:**

1. During a call, activate the speaker key on the phone.
2. Tap **+** or **-**; the volume bar is displayed on the screen. After adjusting the volume, the volume bar disappears from the screen.

Adjust Headset Volume

Headset volume can be adjusted *during a call* to suit personal preference.

➢ **To adjust the headset volume:**

1. During a call, activate the headset key on the phone.
2. Tap **+** or **-** on the phone; the volume bar is displayed on the screen.

Play Incoming Call Ringing through USB Headset

The phone features the capability to ring via a USB headset in addition to via the phone speaker.

Click here to view a video clip demonstrating how to connect a USB headset to the phone.

➢ **To play the ringing of incoming calls via the USB headset:**

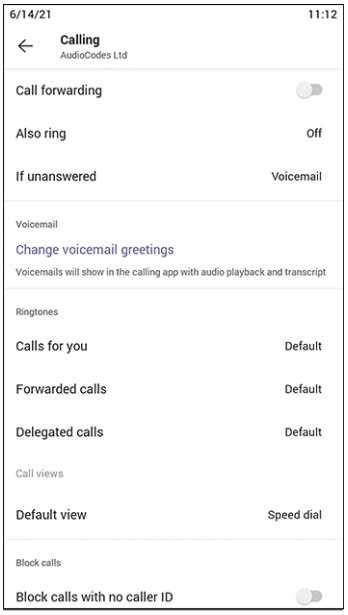
■ Configure the following parameter:

`audio/stream/ringer/0/audio_device=`**`BOTH`** (default), **`BUILTIN_SPEAKER`** or **`TYPE_USB`**

- **`BOTH`**: Incoming calls play through both the USB headset and the phone's speaker.
- **`BUILTIN_SPEAKER`**: Incoming calls play through the phone's speaker.
- **`TYPE_USB`**: Incoming calls play through the USB headset.

Opt in or out of Call Queues

Call queue agents can opt out of call queues or opt in based on settings available on the Teams phones.



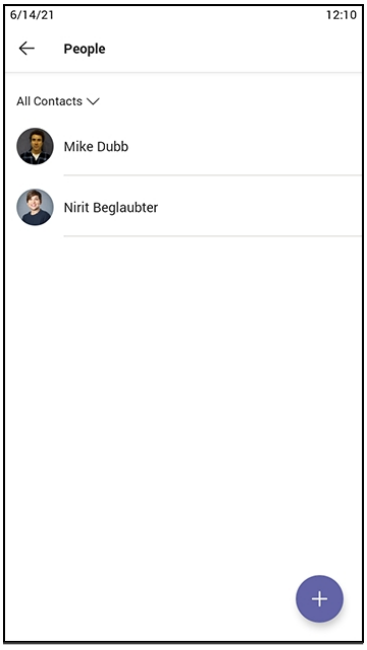
Create and Manage Contacts from the People Screen

The 'People' screen allows users to easily connect and collaborate with teammates, colleagues, friends and family. Through the screen, users can see all their contacts and create and manage contact groups to organize their contacts. The screen provides a simple user experience and aligns with the contacts on the Teams desktop client. In addition to accessing the People screen from the menu, the screen can also be accessed from the hard CONTACTS button on the phone.

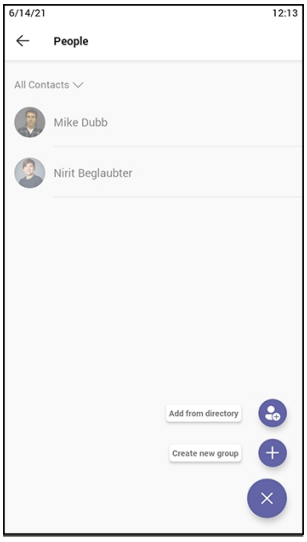
> If a user creates a contact within Microsoft Outlook, their information appears under the People app on the phone screen. Contacts in Microsoft Outlook are available in read-only mode. While only phone numbers currently appear, users can search on the phone for contacts and easily call the people they may email or meet with, using Outlook.

➢ **To access the 'People' screen:**

- On the home screen, tap **More**, then tap **People**.



To add a contact or create a new contact group, tap the + icon .



Manage Speed Dial and Line Keys

This section describes how to make calling and handling incoming calls more efficient using Speed Dial and Line Keys.

Speed Dial is a feature that allows you to call a specific contact by pressing a dedicated button, such as a line key. *Line Keys* are programmable buttons that can be assigned functions, such as speed dialing a contact or transferring incoming calls to a specific person.

- Add a Speed Dial on the next page
- Add a Speed Dial Group on page 88
- Assign a Line Key for Speed Dial or Feature on page 88

Add a Speed Dial

The feature expands the phone's functional capabilities and increases user productivity in the workplace:

- Speed-dial users are listed in a Favorites list for easy access.
- The feature also allows the user to easily transfer a call to a speed dial contact.

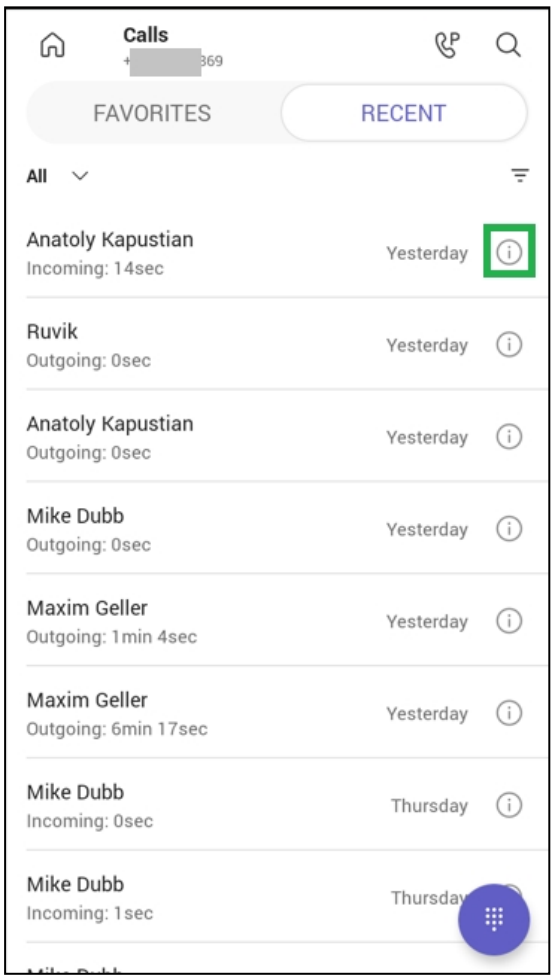
To add a speed dial:

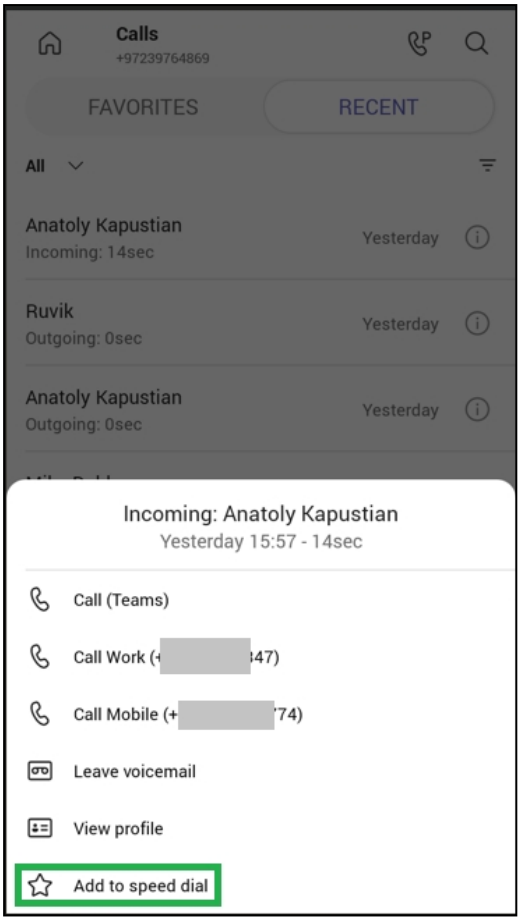
- Add it from the Teams PC client; adding a speed dial from the PC client will be reflected on the sidecar as well.

  -OR-

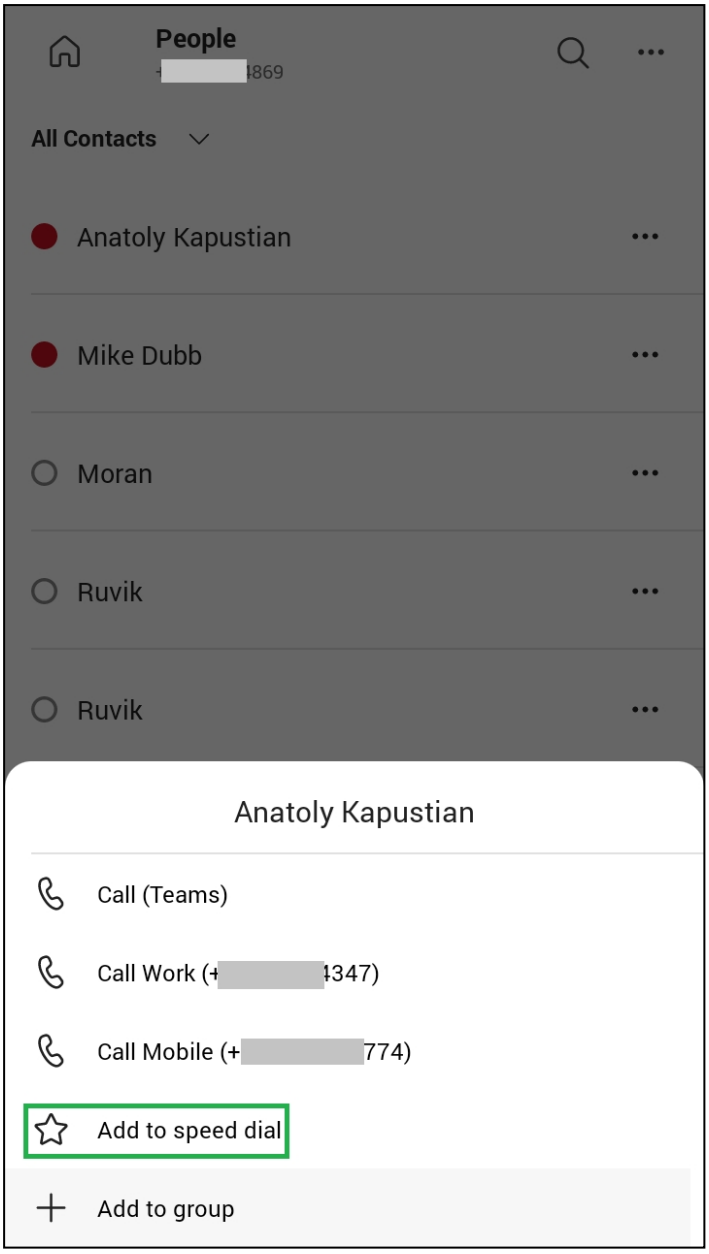
- Add it from the phone using one of the following options:

  a. Via the **Calls** > **RECENT** tab. Tap the information icon of the relevant user and then tap 'Add to speed dial'. The user is added to the **FAVORITES** tab.





b. Via the **People** tab.



c. On the Line Key screen, by assigning speed dial to a free line key:

   i. Tap a free line key.

   ii. Tap **Assign line key**, then **Speed dial**.

   iii. Tap the requested contact from the list.

Remove a Speed Dial

You can remove an assigned speed dial from a favorite contact or a line key.

➢ **To remove a speed dial from a favorite contact:**

1. Access the 'Calls' screen and the **FAVORITES** tab, or access the 'People' screen.

2. In the 'Speed dial' list, locate the relevant contact and tap the three dots next to this contact, then tap **Remove from speed dial**.

➢ **To remove a speed dial from a line key:**

1. On the 'Line Keys' screen, tap any unassigned line key, then tap **Manage line keys**.
2. Navigate to the relevant **page > Line Key** and tap the Delete icon next to it.

Add a Speed Dial Group

Administrators can create a speed dial group and add contacts to the new group.

See here for a video clip demonstrating how to create a speed dial group.

➢ **To create a speed dial group:**

1. Navigate to the **People**screen.
2. From the list, select the contact you want to add to your new group.
3. Tap **Add to group**.
4. In the 'Select a group to edit' screen, tap **Speed dial**. Alternatively,tap Create new group, enter a name for the group, and tap **Create**.
5. After adding the new contact, view them displayed.

Assign a Line Key for Speed Dial or Feature

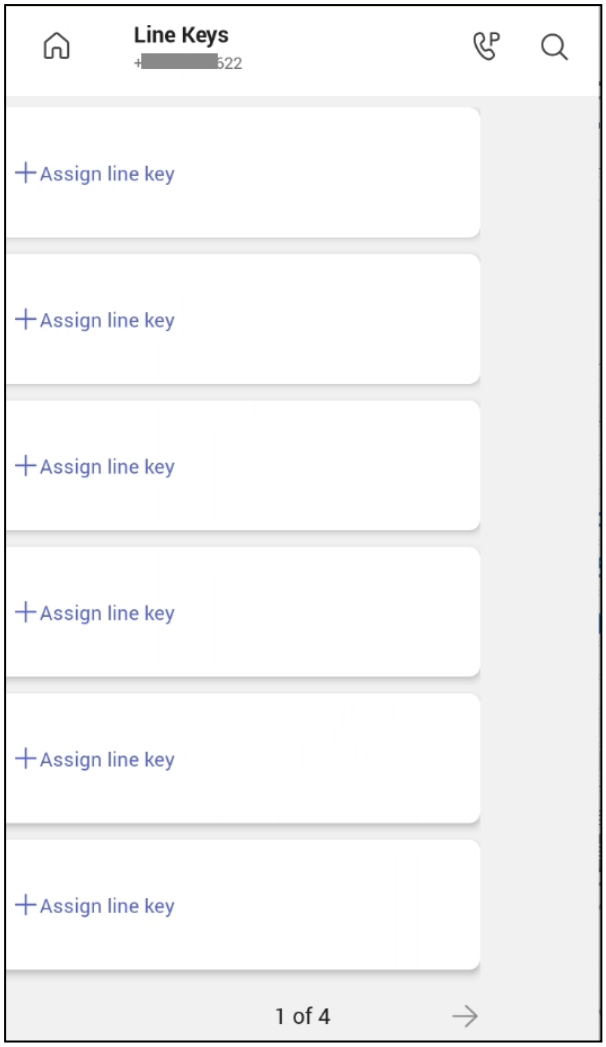
Line keys provide quick access to calling features like speed dial, blind transfer, consult transfer, shared line, and call queue. You can assign people to line keys and label them for any of these features. See here for a detailed description.

The presence/status of an assigned contact displays by their name (account avatar) on the phone's home screen:

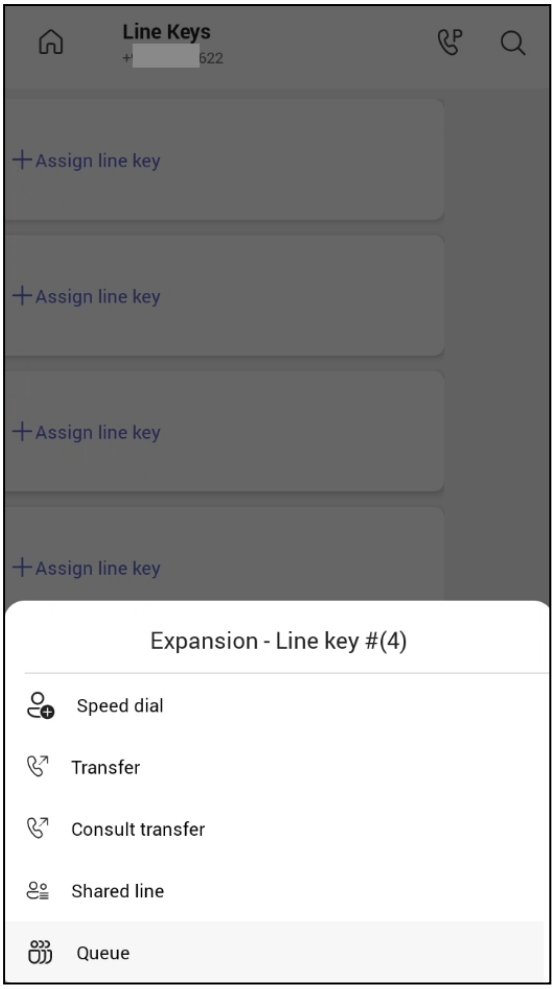


➢ **To assign a line key for speed dial (or other feature):**

1. From the phone's home screen, tap the **More** button, then tap **Line Keys**.



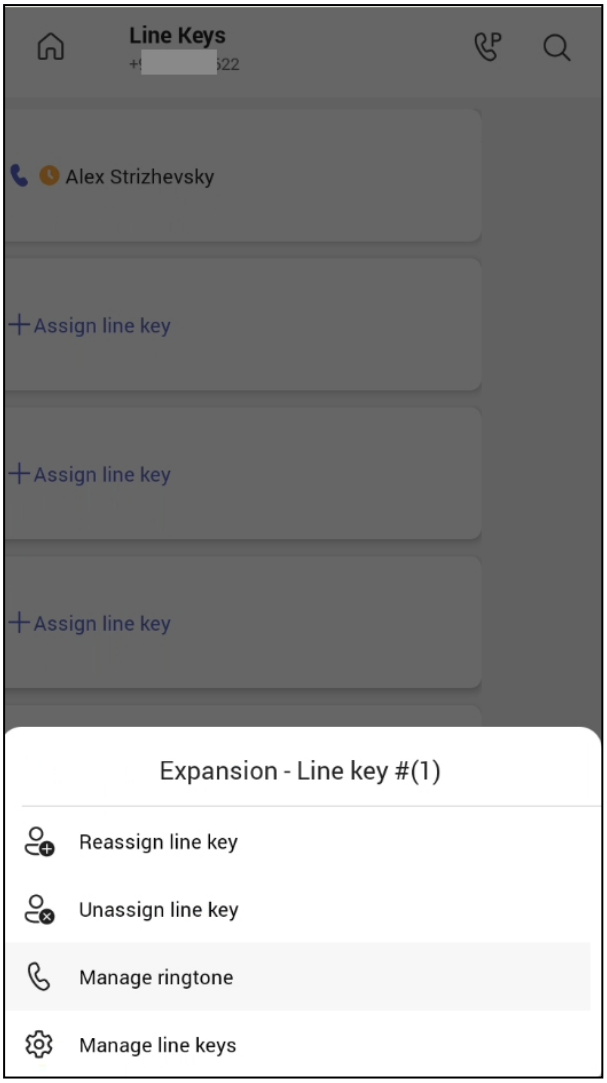
2. Tap the **Assign line key** you want to associate with a named person, then tap again **Assign line key**. The Line Key menu displays the available line key options:



3. To assign the line key to a person, tap **Speed dial**.
4. In the list of contacts, tap the Plus sign next to the relevant contact. If the requested contact does not appear, search and select it instead. The line key is assigned.

➢ To reassign or unassign a line:

1. Long-tap the assigned line key to display the line key menu:

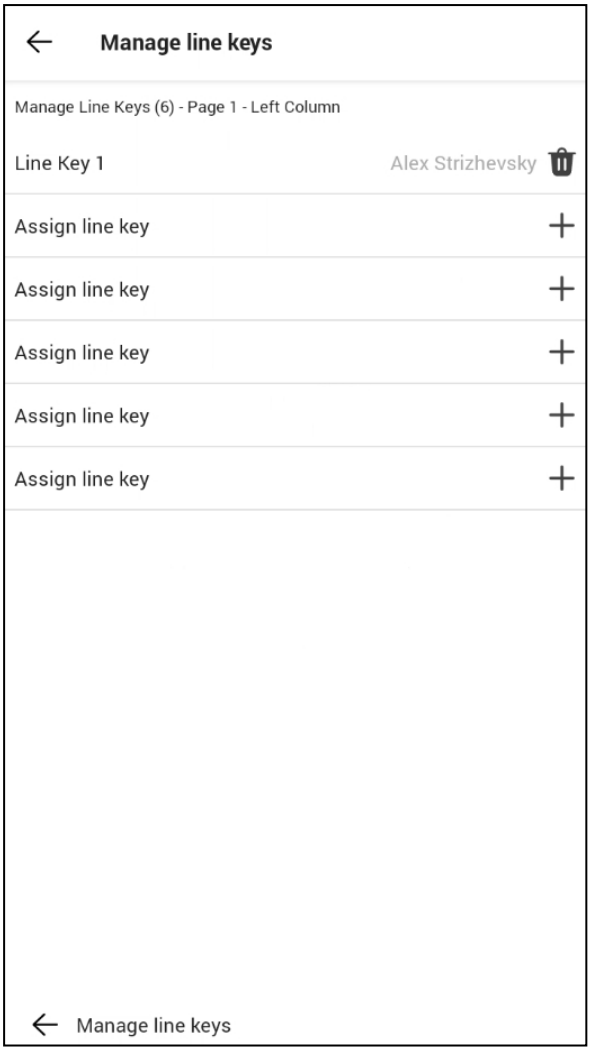


2. Tap **Reassign line key** and reassign the key to a feature or speed-dial as described above, or tap **Unassign line key**.

➢ To manage the LED assign screen:

1. Long-tapthe assigned line key to display the line key menu, then tap 'Manage line keys'.
2. Navigate to the **Line Key** you wish to manage. You can assign a line or delete a contact from a line.


Manage line keys
Manage Line Keys (6)
Page 1
Page 2
Page 3
Page 4
Manage line keys



Manage Meetings

Teams meeting related actions include:

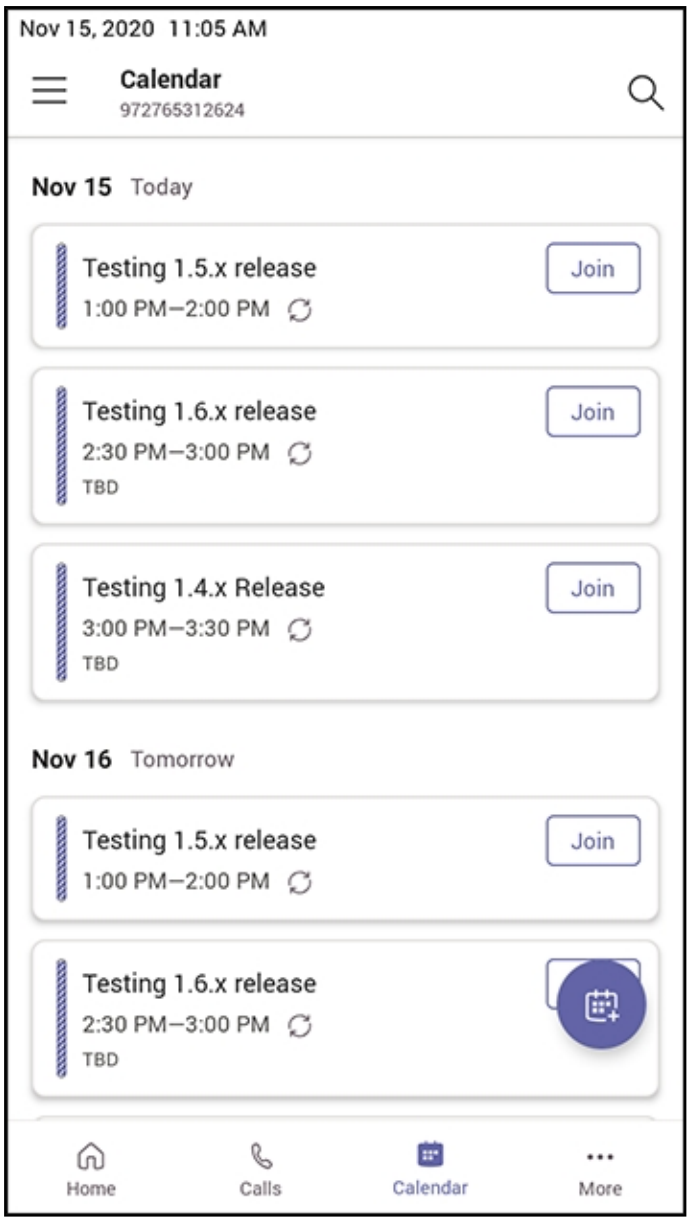
- Schedule a Meeting below
- View and Join Meetings on page 95
- Use Live Captions on page 97
- Hide Names and Meeting Titles for Individual Devices on page 97
- React during a Meeting on page 97

Schedule a Meeting

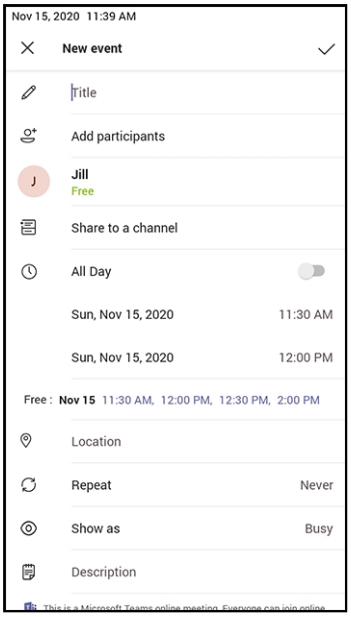
Multi-party conference meetings based on the Teams server (remote conference) can be calendered and initiated from the phone.

➢ **To schedule a meeting:**

1. On the phone's home screen, tap **Calendar**.



2. Tap the icon to add a new event.



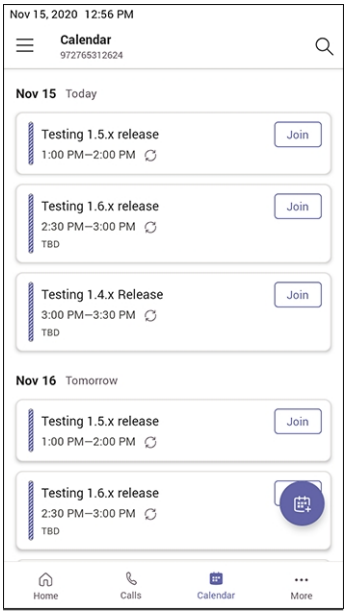
3. In the 'New event' screen, tap the 'Title' field and then use the virtual keyboard that launches to enter a title for the meeting.
4. Tap **NEXT**, then tap **Add participants**. To add a participant:
   a. Tap the 'To' field and then use the soft keyboard to enter the first letter of the name of the participant to add. If you're searching for **Alex** (for example), tap the letter **A** on the soft keyboard, then l, etc.; the name you're searching for will be promoted to the top of the list of Corporate Directory entries displayed.

      The feature lets you quickly and easily navigate to any employee listed in the Corporate Directory.

   b. Tap an entry in the list and then tap ; the participant is added to the meeting.
5. Define 'Share to a channel', date and time, 'Location', 'Show as' and provide a 'Description' of the meeting to facilitate effective management later.
6. Tap the icon; the meeting is calendarized.

View and Join Meetings

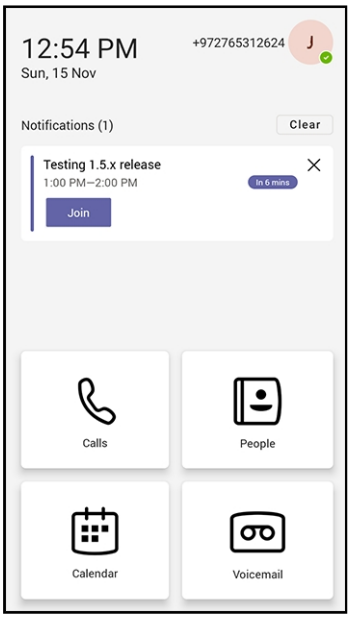
Scheduled meetings can be viewed and joined by selecting the **Calendar** icon in the phone's home screen. See here for a video clip demonstrating how to join a scheduled meeting.



➢ To view the details of a meeting:

1. Scroll down if necessary to the meeting whose details you want to view and select it.
2. View the details of the meeting under 'Notifications'.

For an upcoming meeting, a notification is displayed on the phone's home screen.



➢ To join a meeting:

- In the details of the meeting you want to join, select **Join**.

Use Live Captions

The phone can detect what is said in a meeting, group call or 1:1 call and present the text on the screen in real-time (live) captions.

- Captions are currently only available in English (US).
- Captions are currently unavailable for phones within government clouds.

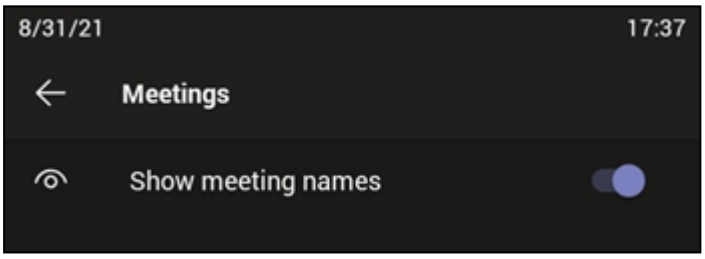
For more information, see here.

Hide Names and Meeting Titles for Individual Devices

Names and meeting titles can be hidden for individual devices.

➢ **To hide names and meeting titles per device:**

1. On the Home screen, tap your avatar, then navigate to **Settings** > **Meetings**).



2. Switch off the **Show meeting names** option.

React during a Meeting

To include silent participants in meetings, *participant reactions* during meetings are supported.

Users can convey their sentiments without hesitation or interruption to participate in the meeting, or they can raise their virtual hands. Everyone in the meeting will see the reaction.

For more information, see here.

Manage Voicemail

To use voicemail:

- View and Play Voicemail Messages below
- Enable Voicemail Support on CAP Users on the next page

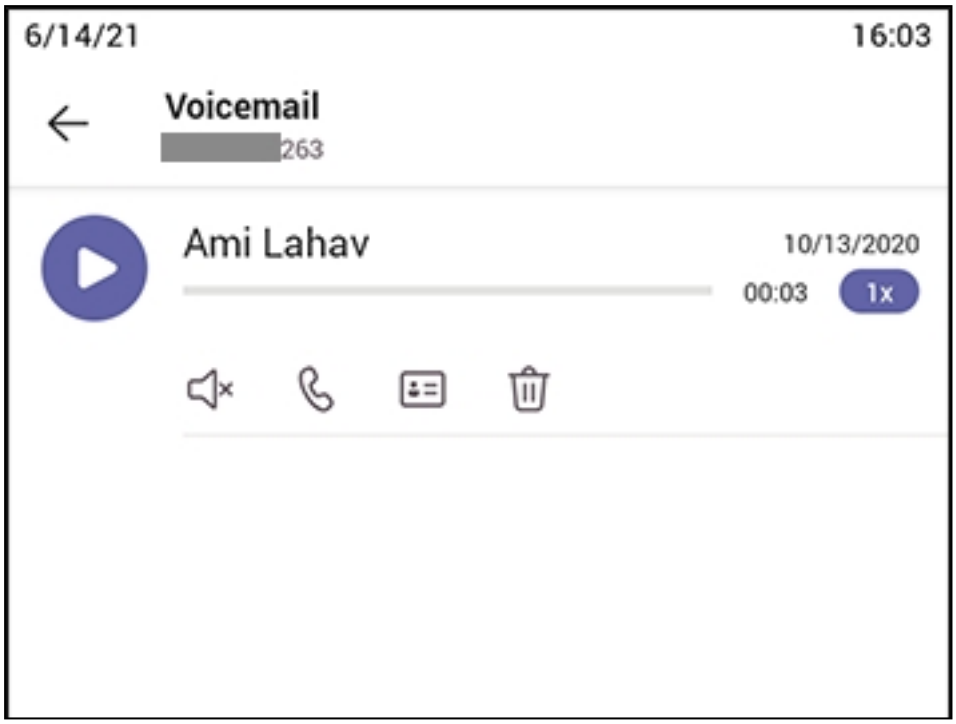
View and Play Voicemail Messages

If you hear a stutter dial tone when you pick up the handset, new messages are in your voicemail box. The phone also provides a visual indication of voicemail messages.

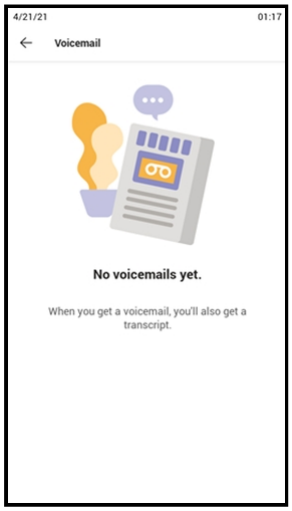
See here for a video clip demonstrating how to view and play voicemail messages.

➢ **To view a list of your voicemail messages:**

1. On the home screen, tap the Voicemail button .



2. Scroll down to select from the list of messages (if there are voicemail messages in your box) which message to **Play**, **Call** or **Delete**.
3. You'll view the following screen if you don't yet have any voicemail messages:



For more information, see here.

Enable Voicemail Support on CAP Users

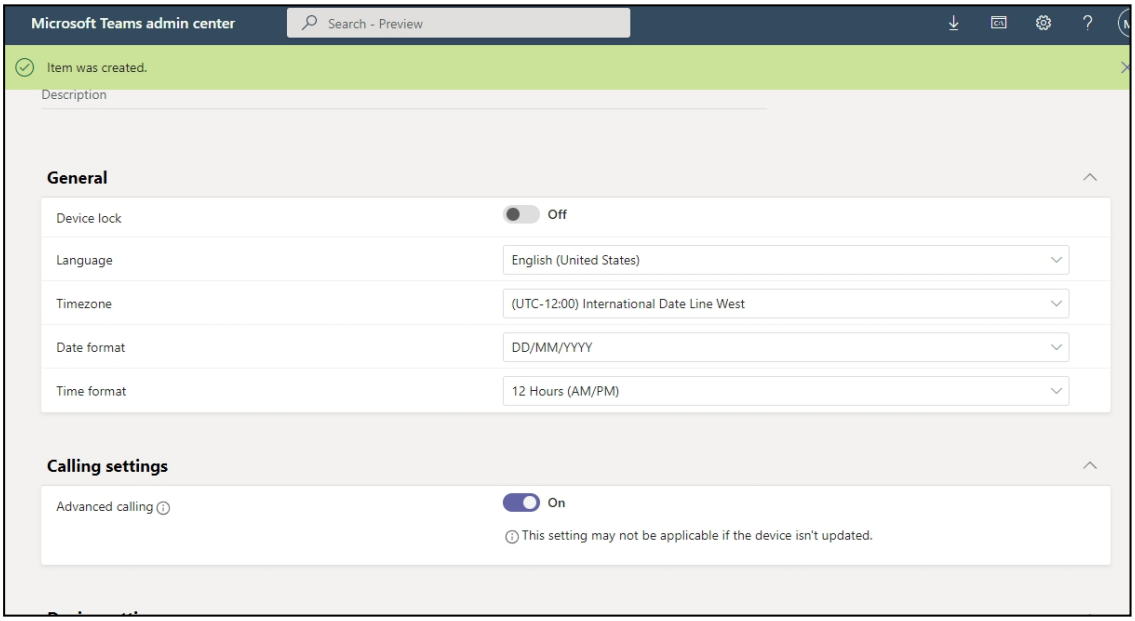
The instructions here show how to enable voicemail on common area phone users. Voicemail can be enabled from the phone or from the TAC. The **Advanced calling** setting must be enabled.

➢ **To enable voicemail from the phone:**

1. In the phone screen, tap the avatar, then tap **Settings**.
2. Navigate to **Device Settings** > **Device administration**.
3. Enter the password (default is **1234**).
4. Access 'Teams Admin Settings' and tap **Calling**.
5. Enable **Advanced calling**.
6. Restart the Teams app as prompted.

➢ **To enable voicemail from the TAC:**

1. Under 'Teams Devices' in the Microsoft Teams Admin Center, select **Phones**.
2. Go to **Configuration Profiles**; in the profiles there is an option under 'Calling settings' to enable **Advanced calling**.



Other Operations

The following is a list of advanced operations that may be available on your phone:

- Configure Better Together over Bluetooth below
- Connect a Device on page 102

Configure Better Together over Bluetooth

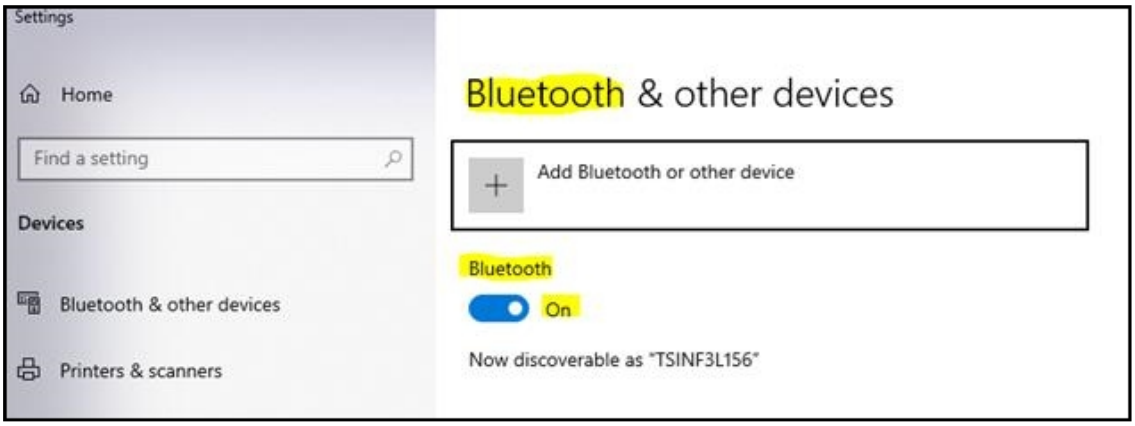
This feature is only supported for phones with integrated Bluetooth and Wi-Fi, i.e., phones with DBW suffix flavor.

Read here about how to configure Better Together over Bluetooth with support for:

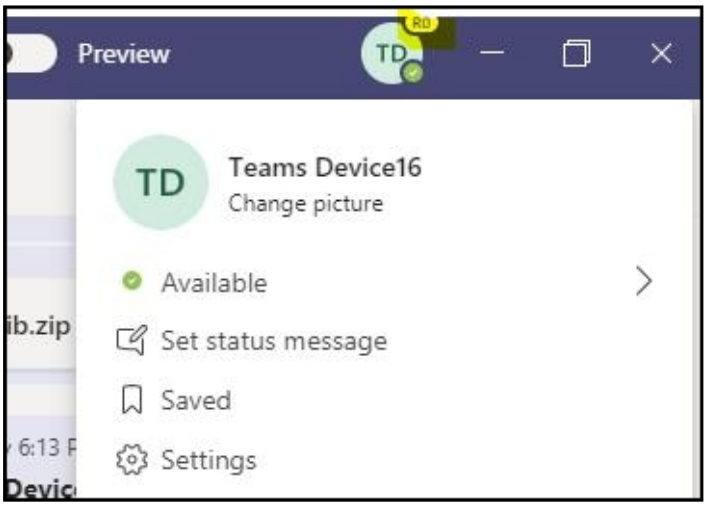
- Pairing with the Teams PC Client
- Lock/unlock synchronization
- [As a feature in preview] Use of the phone as the Teams audio device for calls / meetings

➢ **To set up Bluetooth on the PC side:**

1. Enable Bluetooth on your PC.

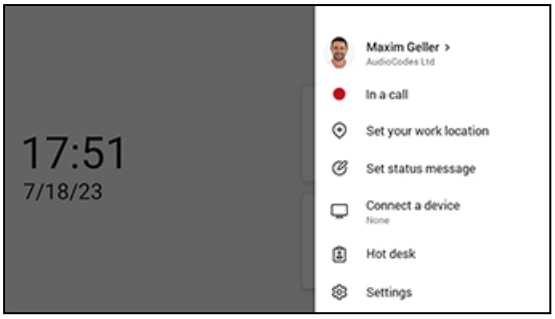


2. Install Teams PC Client on the PC.
3. Sign in to the Teams PC Client with your account (it's necessary to sign in with the same accounts to both the Teams PC Client and to the device).

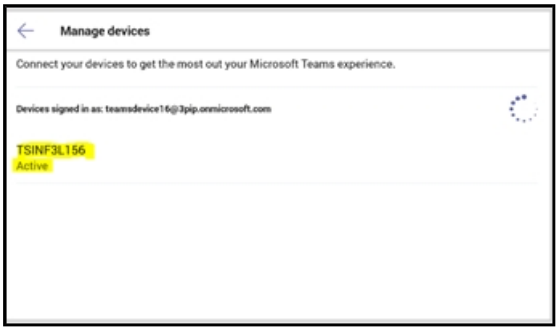


➢ **To set up Bluetooth on the device side:**

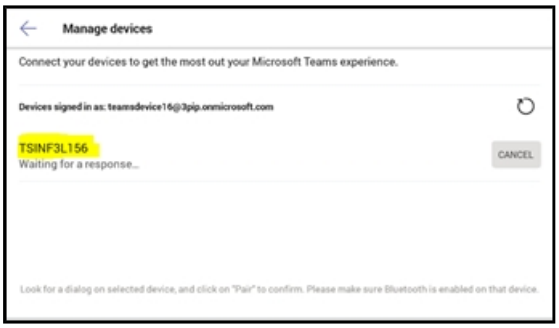
1. Sign in to the Teams application with your account (it's necessary to sign in with the same accounts to both the Teams PC Client and to the device).
2. Tap the avatar and then tap **Connect a device**.



3. View the displayed available device to connect to.



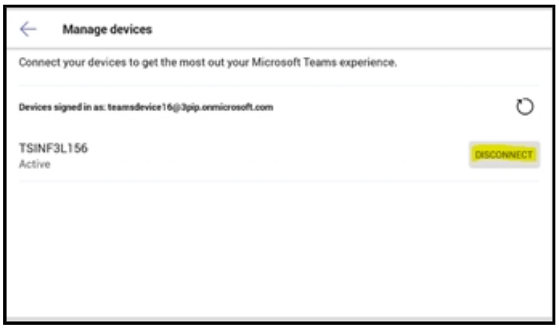
4. Pair the device with your PC.



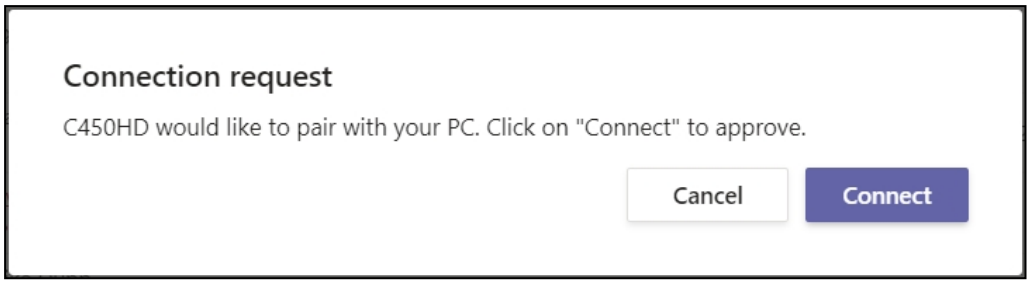
5. View on your PC a notification it gets to accept the connection:



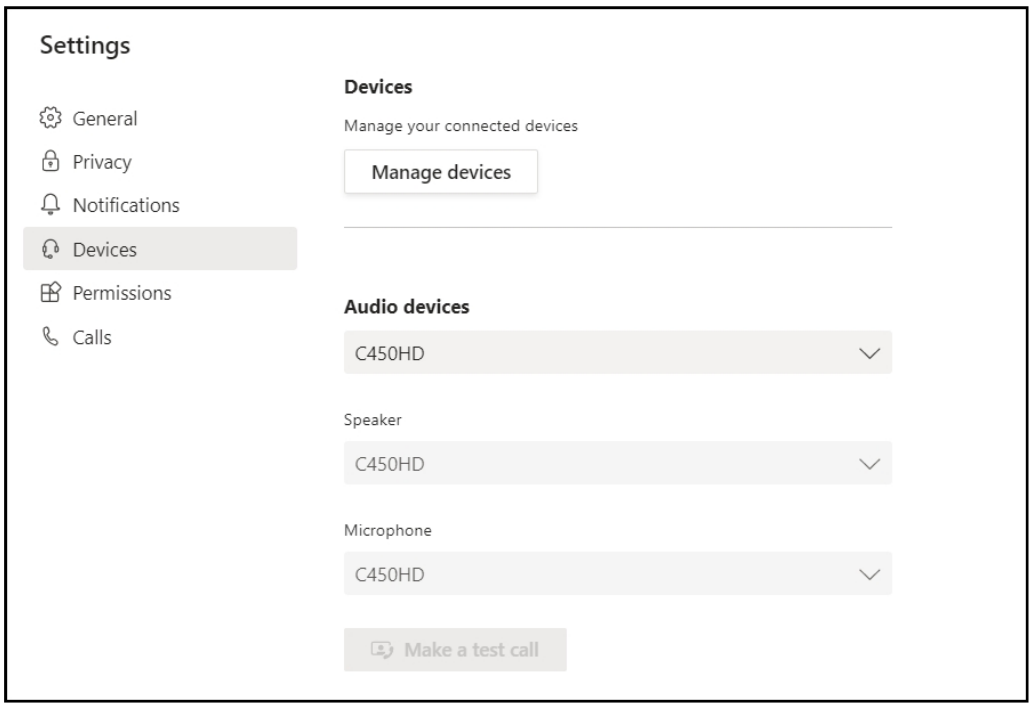
6. Accept the notification from PC.
7. Check the device and make sure pairing was successful:



8. When pairing the phone with the PC Client, the PC Client presents the following request for approval:



Once connected, the phone will be presented as a default Teams PC Client Audio device:



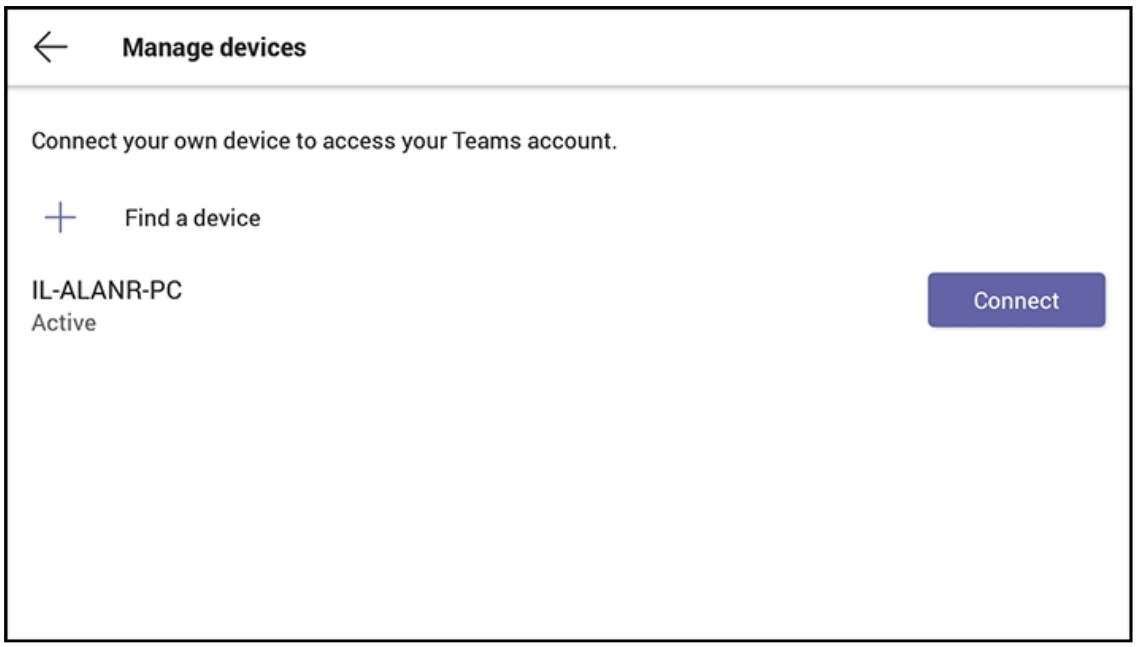
Connect a Device

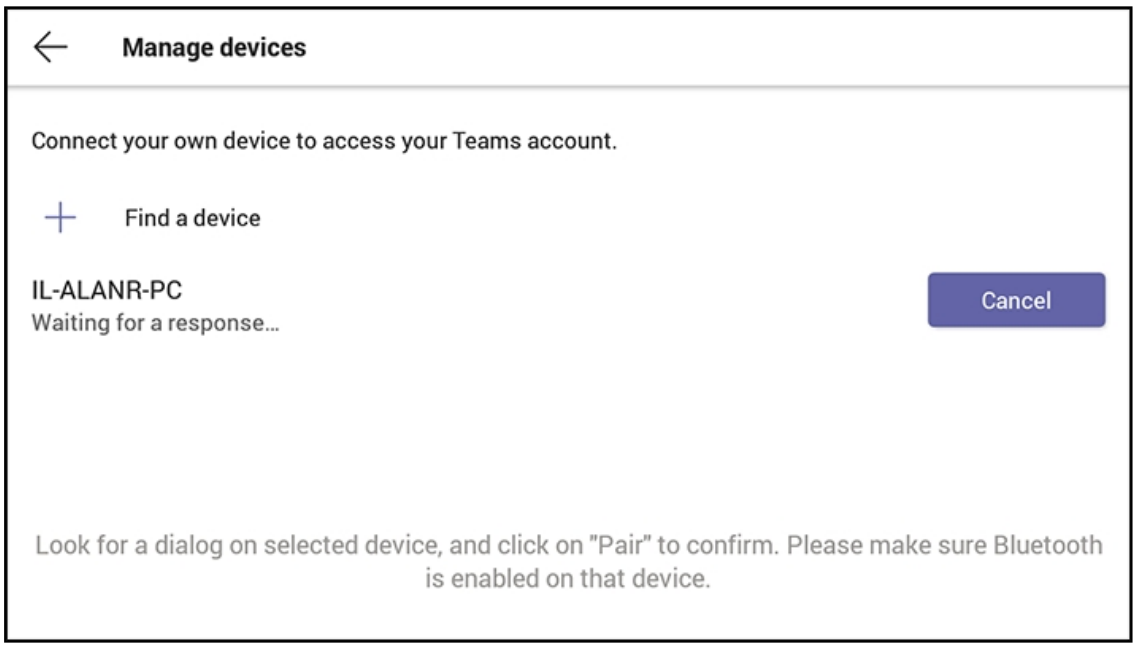
This feature is only supported for phones with integrated Bluetooth and Wi-Fi, i.e., phones with DBW suffix flavor.

You can find a device to connect to, to access your Teams account.

To connect to a device:

1. In the 'Calls' screen (or 'People' screen, 'Calendar' screen or 'Voicemail' screen), tap the phone menu and then tap **Connect a device**.
2. Tap **+** to find a device or if a device is already found, tap the **Connect** button.





3. In the screen displayed by the selected device, tap **Pair**. Make sure wireless is enabled on that device.

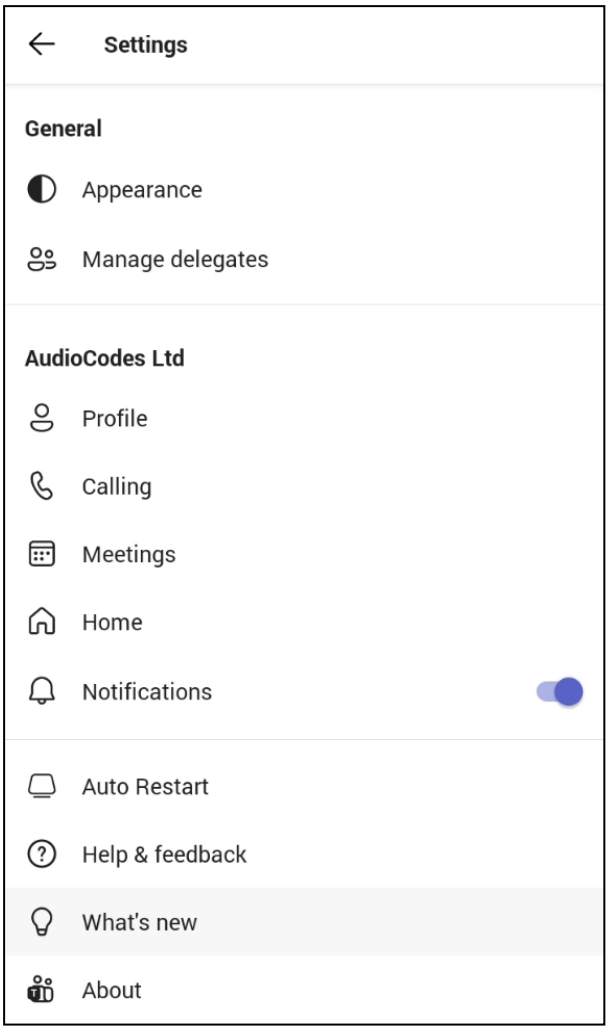
Sign Out

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

➢ **To sign out:**

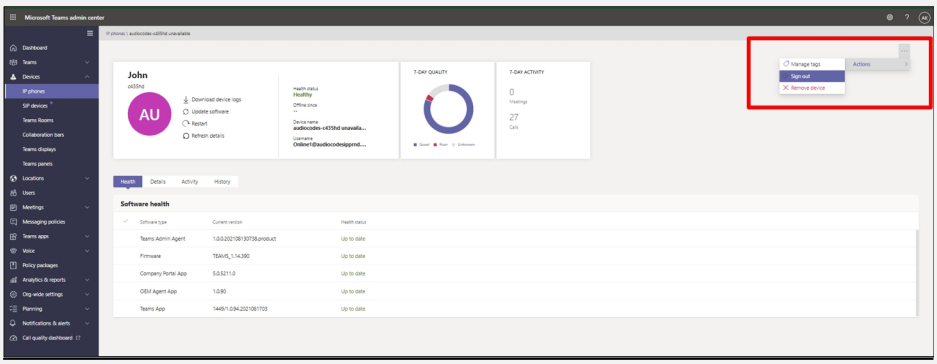
1. Tap your avatar, then tap **Settings**.

Alternatively, in the Calls screen (or People screen, Calendar screen or Voicemail screen), press the MENU key.



2. Tap **Sign out** and confirm. You are signed out and returned to the **Sign in** screen.

Network administrators can alternatively sign out from devices using Microsoft Teams Admin Center (TAC). Network administrators can also remotely sign in and provision devices from Microsoft's TAC.



5 Perform Administrator-Related Operations

The following is a list of operations performed by network administrators:

- Configure Time on Teams Devices below
- Set up Automatic Provisioning on the next page
- Log in as Administrator on page 107
- Perform Password and Security Related Actions on page 108
- Manage Phones with the Device Manager on page 116
- Configure Phone Behavior on page 121
- Set up Emergency Handling on page 132

Configure Time on Teams Devices



- AudioCodes recommends using Geolocation (the default setting) as the time zone configuration method. With this configuration, if no other changes to the time zone settings are made, the device retrieves the time from it's 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 devices public IP address to obtain it's location. If the devices are behind NAT they are using 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)**:
  - Time is obtained from DHCP server.
- **Admin Provisioning**:

  Use one of the following:
  - Teams Admin Center, created under configuration profile. For details refer to the relevant Microsoft documentation.
  - Device Manager, created in configuration parameters setup. The following parameters are available for time setup:

- `date_time/time_dst` – enable or disable daylight saving time validation (see below).
- `date_time/time_format` and `date_time/date_format` – set date and time display format.
- `date_time/timezone_id`, `date_time/timezone`, `date_time/time_zone_retrieval_mechanism`, `date_time/time_zone_region` – automate time zone retrieval or set up the time zone.

See Date & time on page 25 for more information.

- Administrators can **manually define the NTP server** to comply if necessary with enterprise security requirements, if those requirements preclude using DHCP Option 42.

  Manual configuration takes precedence over DHCP Option 42 and the time servers.

  Two ways to manually define the NTP server are available:

  - in the phone's user interface
  - in the phone's .cfg configuration file, using the parameter 'date_time/ntp/server_address'

  See Preferred NTP server on page 25 for more information.

In most regions, Daylight Saving Time changes the regional time twice a year. DST Validation allows maintaining accurate time. Two options for phones to get the correct time are:

- [Recommended] If the DHCP server offers Timezone Options (100/101), the phone will set the obtained time zone and display the correct time on the screen; the time will be calculated based on an embedded Time Zone database, factoring in DST.
- If the DHCP server offers Time Offset Option only (2) and if the Timezone priority mechanism is determined to be on DHCP and not on GEOLOCATION, the phone will assign the obtained time offset to the first matched region in the list but there is a good chance it won't reflect the actual geographical location, therefore the displayed time might be incorrect in some cases. For example, if the given time offset is GMT-5 and the phone is located in Mexico, the phone will get the time (and the DST setting) from central time and not from Mexico because in GMT-5 there is also Central Daylight Time.

Set up Automatic Provisioning

Phones can be directed to a provisioning server using DHCP Option 160 or AudioCodes' HTTPS Redirect Server, to automatically load configuration (cfg) and firmware (img) files.

After the phone is powered up and network connectivity established, it automatically requests provisioning information; if it doesn't get via DHCP Option 160 provisioning method, it sends an HTTPS Request to the Redirect Server which responds with an HTTPS Redirect Response containing the URL of the provisioning server where the firmware and configuration files are located. When the phone successfully connects to the provisioning server's URL, an Automatic Update mechanism begins.

➢ **To set up DHCP Option 160, use this syntax:**

- `<protocol>://<server IP address or host name>/<firmware file name>;<configuration file name>`
- `<protocol>://<server IP address or host name>`
- `<protocol>://<server IP address or host name>/<firmware file name>`
- `<protocol>://<server IP address or host name>/;<configuration file name>`

Where `<protocol>` can be **ftp**, **tftp**, **http** or **https**

➢ **To set up AudioCodes' HTTPS Redirect Server, use this syntax:**

- `<protocol>://<server IP address or host name>`
- `<protocol>://<server IP address or host name>/<firmware file name>`
- `<protocol>://<server IP address or host name>/<firmware file name>;<configuration file name>`
- `<protocol>://<server IP address or host name>/;<configuration file name>`



The Redirect Server's default URL is:
provisioning/redirect_server_url=https://redirect.audiocodes.com
It can be reconfigured if required.

Configure the Model Name in DHCP Option 60

For devices using DHCP Option 60 (Vendor Class Identifier), the model name can be configured, using the `network/model_name_as_venid` parameter. This parameter can receive either of the following values:

- `1` (default) – uses the device's Model Name in DHCP Option 60.
- `2` – uses the fixed string **CPE-OCPHONE** in DHCP Option 60.

Log in as Administrator

You need to be logged in as Administrator to:

- Set up and modify networking parameters
- Troubleshoot (except for basic troubleshooting actions that are also available to regular users)

For details see the Device admin settings section in Configure C470HD Device Settings on page 23.

➢ **To log in as Administrator:**

1. Navigate to the phone's Device Settings screen:
   a. On the phone's home screen, tap the avatar, then tap **Settings**.
   b. On the 'Settings' screen, scroll down and tap **Device Settings**.
2. Scroll down and tap **Device Administration**.
3. Tap **Login** and then in the Login screen that opens, tap the **Enter password** field and use the virtual keyboard to enter the password. 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.



- For enhanced security, the phone supports a strong password check for Administrator login. Note that the default password:
  - ✓ can be changed per device from the phone screen (the user first enters the default password and is then prompted to modify it to a more complete password) or via bulk configuration of multiple devices using Microsoft's TAC or AudioCodes' Device Manager (through the configuration parameter `/admin/default_password`).
  - ✓ must be changed before accessing the device via SSH
- Criteria required for a strong password are provided. The password must:
  - ✓ be greater than or equal to 8 characters in length.
  - ✓ contain one or more uppercase characters.
  - ✓ contain one or more lowercase characters.
  - ✓ contain one or more numeric values.
  - ✓ contain one or more special characters.

Perform Password and Security Related Actions

Define Password Complexity below

Configure Admin Login Timeout on the next page

Force Users to Change their Device Lock PIN Using TAC Configuration Profile on page 110

Load Certificates to Phones on page 111

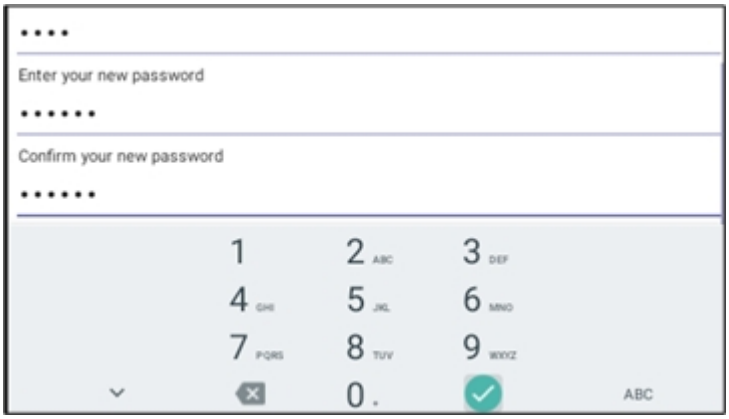
Disable a Device's USB Port on page 115

Disable or Re-enable Wi-Fi and Bluetooth via Device Manager on page 119

Define Password Complexity

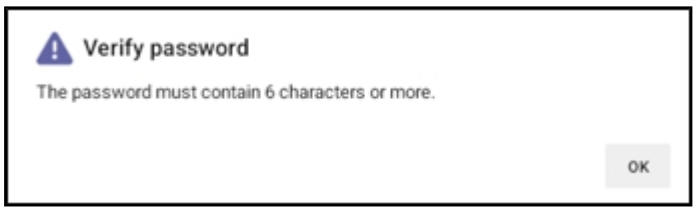
Admin-defined password complexity is designed mainly for non-touch screen phones but it can also be applied to touch-screen phones. The feature provides administrators with the capability

to finely adjust password complexity.

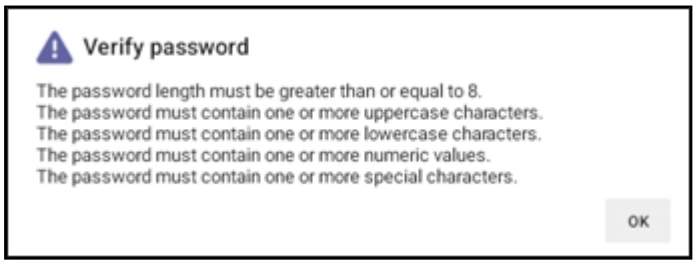


The administrator can set password complexity using the cfg configuration file parameter 'system/admin_password/strength'.

- When updating LCPs to the current version, the parameter is by default set to COMPLEXITY_MEDIUM. Password complexity rule: At least six characters and/or digits must be used.



- When updating non-LCP touch-screen phones to the current version, the parameter default is COMPLEXITY_HIGH. Password complexity rules are as follows:



- If a phone was configured with a *complex* password in earlier versions, it *preserves* that password.
- The administrator can optionally change it to a *non-complex* password.

Configure Admin Login Timeout

The administrator login can be configured to time out. The timeout's value can be configured using a cfg configuration file parameter:

`settings/admin_logout_timeout`

- Default value: 3 (minutes)

- Valid values: 1-10 (minutes)

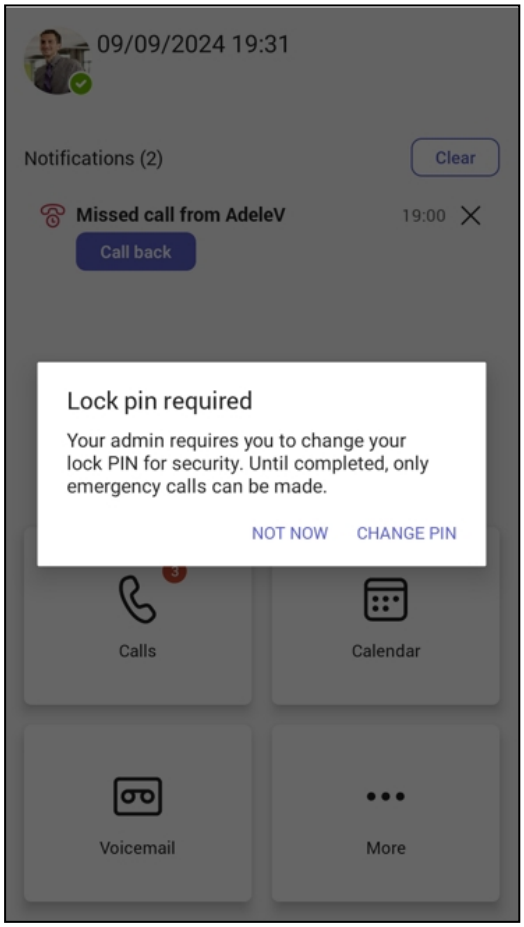
- The cfg file can be loaded to the device using Device Manager.
- Timing begins when exiting the 'Device Settings' menu.
- When the timeout expires, the device logs out automatically.
- The functionality works for both registered and unregistered devices.

Force Users to Change their Device Lock PIN Using TAC Configuration Profile

Historically, users have always been provided with an option to lock their device, but in addition, the *administrator* can configure an option to *force users to change their device lock PIN*.

➢ **The workflow for forcing users to update their device lock PIN admin is as follows:**

1. Set up **Enforce Device Lock** in the Microsoft Teams Admin Center (TAC) Configuration Profile.
2. When the Teams app detects a PIN lock configuration where a force PIN configuration is toggled, a popup is displayed instructing the user to navigate to device lock settings to change the PIN.



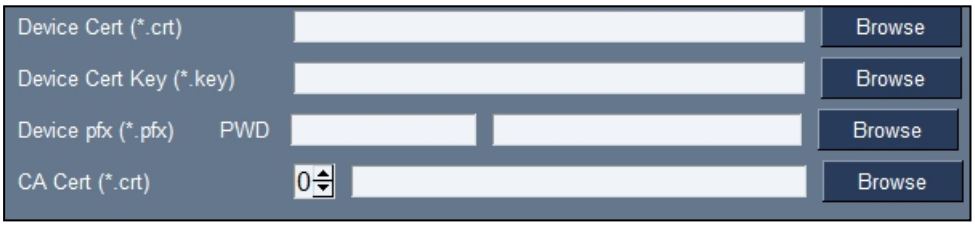
3. If the user taps **CHANGE PIN**, they can navigate to Device Settings to reset the PIN.
4. If the reset PIN configuration times out and the user has not changed their PIN, the device is locked by the Teams app and the user is restricted to emergency calls along with the set PIN notification.

Load Certificates to Phones

The following shows how to load user certificates to a single device and to multiple devices. Before loading certificates, put the certificate files in a designated folder.

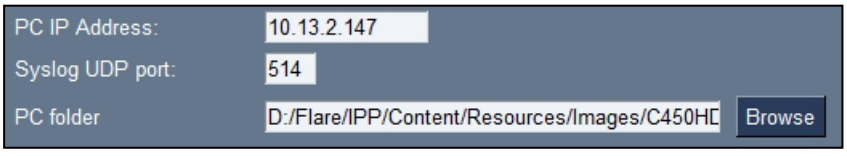
Certificates can be downloaded using:

- Device Manager (see the *Device Manager Administrator's Manual*)
- Android Device Utility as shown here:



Guidelines:

- The extension of the device certificate file must be **.crt**
- The extension of the private key must be **.key**
- Device certificates can be provisioned in **.pfx** file format (combining **.crt** and **.key**). The following parameter values can 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 extension of the CA certificate file must be .crt. It's possible to load up to 5 CA certificates to the phone using the placement selector (0-4) (Default: 0).
- The IP address of the PC on which the certificate files are stored must be entered as shown here:



- The loaded certificate's file name must be without spaces. Spaces between words can be created using an underscore _

- The CA certificate (ca_cert) can also be loaded to devices using AudioCodes' Device Manager, in the 'Template' screen.
- 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.

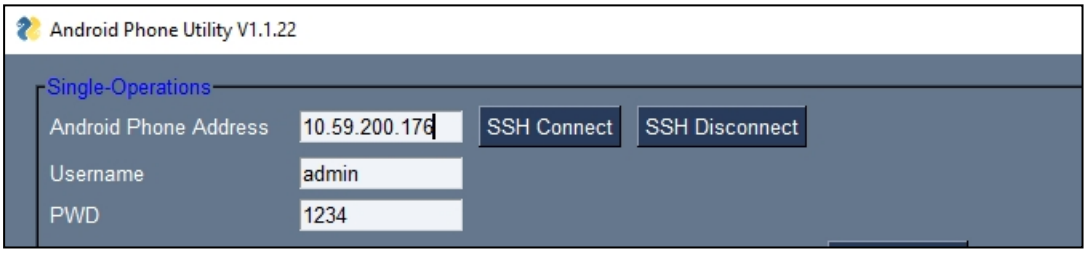
Load Certificates using AudioCodes Android Device Utility

Certificates can be loaded to a phone or to multiple phones using AudioCodes' Android Device Utility.

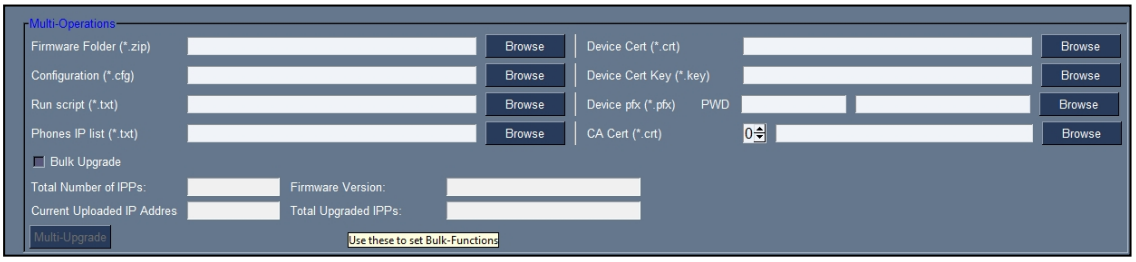
See Android Device Utility on page 144 for detailed information about the application.

To load certificates to a single device:

1. In the Android Device Utility, enter the phone's IP address and click **SSH Connect**.

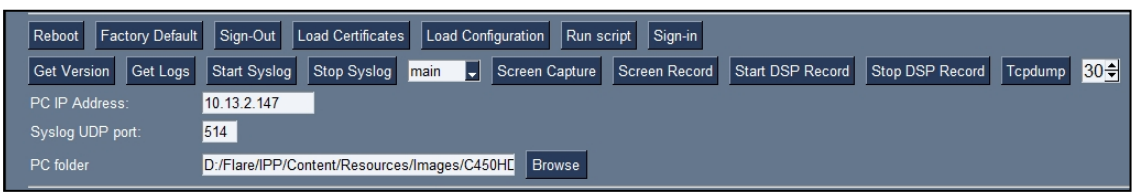


2. Click the**Browse** button next to the field **Device Cert** and then navigate to and select the certificate file to download.



The loaded certificate's file name must be without spaces. Spaces between words can be created using an underscore _

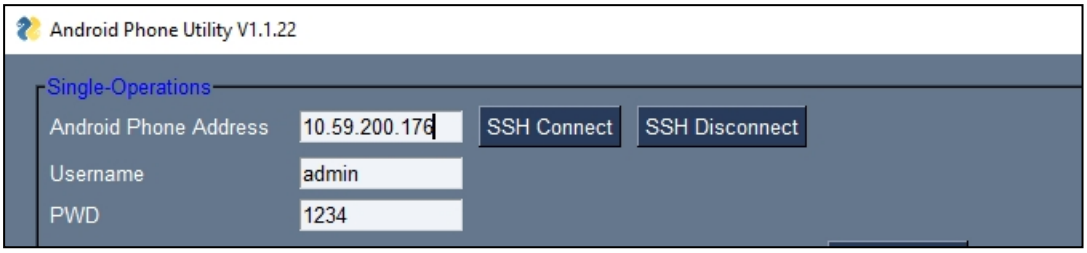
3. Click the **Load Certificates** button to add the certificate.



4. After a short period, view in the results pane "Cert Successfully Installed".

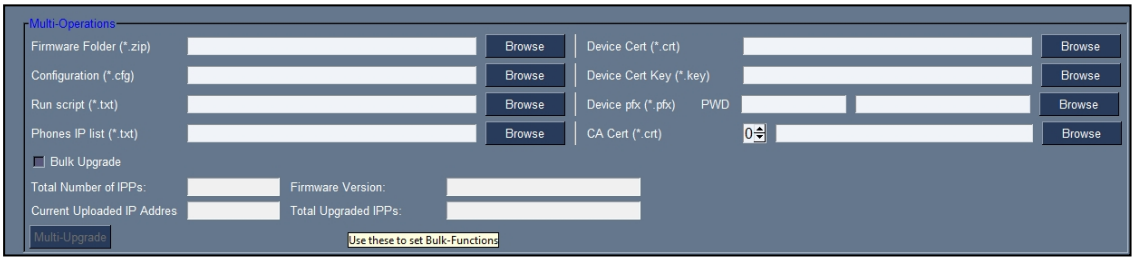
➢ To load certificates to multiple devices:

1. In the Android Device Utility (see Android Device Utility on page 144 for more information), enter the phone's IP address and click **SSH Connect**.



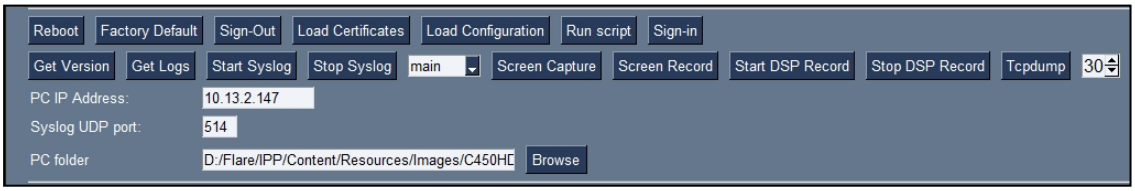
> The loaded certificate's file name must be without spaces. Spaces between words can be created using an underscore _

2. Click the **Browse** button next to the field **Device Cert** under 'Multi Operations' and then navigate to and select the certificate file to download.



3. Adjacent to the field **Phones IP list** under 'Multi Operations', click the **Browse** button and then navigate to and select the txt file listing the IP addresses of the phones to which to download the certificates. The IP addresses are listed one under the other. Each occupies its own line. No notation between them is required.

4. Click the now activated **Load Certificates** button shown in the next figure, to add the certificates to the phones.



5. After a short period, view in the results pane "Certs Successfully Installed".

Certificate Enrollment using SCEP

[Available from version 1.19] The device supports certificate enrollment using Simple Certificate Enrollment Protocol (SCEP) using Microsoft's Network Device Enrollment Service (NDES) server, 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, issue a Certificate Signing Request (CSR) to the NDES and receive a device certificate signed by the CA certificate (the one that the device received from NDES).

Configure the following three parameters:

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

The next table shows the descriptions of the SCEP parameters.

Parameter	Description
security/SCEPEnroll/ca_fingerprint	Define the thumbprint (hash value) for the CA certificate. Default value: NULL. The network administrator must set its value to (for example): 3EBE50003ABF1DF5E6B5A3230B02B856
security/SCEPEnroll/password_ challenge	Define the enrollment challenge password. Default value: NULL. The network administrator must set its value to (for example): 7A7F9FC4BB7625F0935E67EA6D6322ED
security/SCEPServerURL	Define the SCEP server URL. Default: NULL. If you use Microsoft NDES server, use: https://<NDES server IP address/Hostname>/certsrv/mscep/mscep.dll/pkiclient.exe
security/SCEPEnroll/renewal/advancethreshold	Define the renewal advance threshold of the device certificate. Configure between 50 and 100 (in units of percentage) Default: 80 This indicates that a renewal of the certificate (device.crt) will be initiated when 80 percent of its validity is reached.
security/SCEPEnroll/rollover/advancethreshold	Specify the threshold of the CA Root certificate's validity at which to initiate a renewal. Configure between 50 and 100 (in units of percentage). Default: 90

Parameter	Description
	This indicates a renewal of the certificate (CAROOT.crt.) will be initiated when 90 percent of its validity is reached.
security/CSR/CommonName	Define a value according to the following 'wild-card' format: {mac} – the device's MAC address {IP} – the device's IP address {model} – the device model
security/CSR/Country	Define the name of the country used to generate the certificate signing request (CSR). Use the ISO (International Organization for Standardization) code of the country / region in which the organ-ization is located.
security/CSR/Email	Optionally, define the email address used to gen-erate the CSR.
security/CSR/Organization	Optionally, define the legal name of the organ-ization used to generate the CSR.
security/CSR/State	Optionally, define the name of the state / province used to generate the CSR.
security/SCEPEnroll/otp_server_url	Optionally, set the One-Time Password and Certificate server URL
security/SCEPEnroll/otp_password	Optionally, set the One-Time Password and Certificate Thumbprint
security/SCEPEnroll/otp_username	Optionally, set the One-Time Password and Certificate server username

Disable a Device's USB Port

Applies to all AudioCodes' Teams phones.

This functionality complies with the physical security requirements of some customers, specifically, customers who are in the government space.

Customer administrators can enable or disable a phone's USB port with the following parameter available in the phone's .cfg configuration file:

```
admin/usb_enabled=1
admin/usb_enabled=0
```

The parameter can be configured via the AudioCodes One Voice Operations Center (OVOC) Device Manager module used to manage AudioCodes' Teams phones, as well as via SSH command.

The parameter is also available in the template which can be applied to multiple phones via the Device Manager.

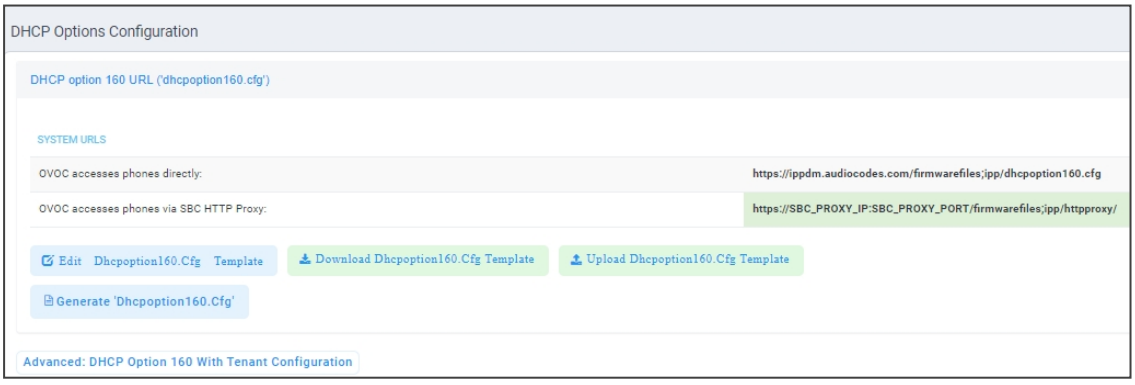
- After setting the parameter to 0, the phone cannot under any circumstances detect a plugged-in USB device.
- Additionally, all USB-related settings are removed from the phone's user interface.

Manage Phones with the Device Manager

AudioCodes' Device Manager manages Android-based Teams phones in a similar way to UC-type phones. Teams phones' configuration parameters are in the same format as UC phones. A .cfg configuration file is defined for each device. Device Manager version 7.8.2000 and later supports Android-based Teams devices.

Zero Touch Provisioning is supported in a non-tenant aware manner; each local DHCP Option 160 must be configured with a fully-specified URL pointing to **dhcpoption160.cfg** as shown here:

Table 5-1: DHCP Option 160 URL



This URL is displayed in the Device Manager page under **Setup** > **DHCP Options Configuration**. After devices are added to the Device Manager (which allocates them to the default tenant), they can be re-allocated by selecting **Change Tenant** in the 'Actions' menu. The above URL can also be configured in AudioCodes' Redirect Server. Android-based Teams devices currently support:

- Provisioning of configuration
- Provisioning of firmware
- Switching to UC / Teams

- Monitoring (based on periodic Keep-Alive messages sent from devices)
- Resetting the device

The Device Manager's 'internal' functions (which don't involve devices) are:

- Change tenant
- Change template
- Show info
- Generate Configuration
- Delete device status
- Nickname



- To change a device's configuration, see the *Device Manager Administrator's Manual*. Changing a device's configuration using the Device Manager is the same for Android-based Teams devices as for UC devices.
- To commit a change made at the template/tenant/site/group/user level, perform **Generate Configuration**. The change can be validated in the device's .cfg file. The Android-based endpoint pulls the updated configuration when the next periodic provisioning cycle occurs.

Configure a Periodic Provisioning Cycle

Network administrators can configure how often periodic provisioning cycles will occur, to suit enterprise management preference.

➢ **To configure how often periodic provisioning cycles will occur:**

- Use the following table as reference.

Table 5-2: Periodic Provisioning Cycle

Parameter	Description
provisioning/period/type	Defines the frequency of the periodic provisioning cycle. Valid values are: ■ HOURLY ■ DAILY (default) ■ WEEKLY ■ POWERUP ■ EVERY5MIN ■ EVERY15MIN Each value type is accompanied by additional parameters

Parameter	Description
	that further defines the selected frequency: ■ provisioning/period/daily/time. ■ provisioning/period/hourly/hours_interval ■ provisioning/period/weekly/day ■ provisioning/period/weekly/time ■ provisioning/random_provisioning_time

Manage Devices with HTTPS

Android-based Teams devices support an HTTPS connection.

➢ **To establish an HTTPS connection:**

- The server certificate must be signed by a well-known Certificate Authority .

  -OR-

- A root/intermediate CA certificate must be loaded to the device's trust store via Configuration File parameter '/security/ca_certificate/[0-4]/uri'.

➢ **To maintain backward compatibility with devices previously running UC versions:**

- Configure parameter '/security/SSLCertificateErrorsMode' to **Ignore**

Configure QoS on PC Port

QoS settings for the PC port are supported (VLAN for PC port). Administrators can configure PC port QoS via the device's cfg configuration file which can be loaded to the device via AudiocCodes' Device Manager. The following three cfg configuration file parameters are available configuring the feature:

Parameter	Description
network/lan/vlan/pc_port_ tagging/enable=0	Defines the PC port VLAN as enabled / disabled. ■ 0 = PC port VLAN disabled ■ 1 = PC port VLAN enabled Default: 0
network/lan/vlan/pc_port_id=0	Defines the PC port VLAN ID. Range: 0-4096 Default: 0

Parameter	Description
network/lan/vlan/pc_port_priority=0	Defines PC port VLAN priority. Range: 0-7 Default: 0

The feature provides PC port QoS for AudioCodes' Android-based phones which feature settings for VLAN *and* VLAN Priority (802.1p) for the PC port.

Disable or Re-enable Wi-Fi and Bluetooth via Device Manager

For AudioCodes IP phones that include Wi-Fi and Bluetooth capacities, administrators can enforce a wireless lockdown, by turning on a dedicated flag in Device Manager. When this flag is turned on:

- The Wi-Fi and Bluetooth options are removed from the phone's Device Settings.
- Wi-Fi and Bluetooth related configuration parameters have no effect.

End users cannot re-enable these wireless interfaces while the restriction is in effect.

➢ **To disable Wi-Fi and Bluetooth:**

- Enable the following configuration parameter for the relevant phones in Device Manager:

```
admin/restrict_wireless=1
```

➢ **To re-enable Wi-Fi and Bluetooth:**

- Disable the following configuration parameter for the relevant phones in Device Manager:

```
admin/restrict_wireless=0
```



- By default, the `restrict_wireless` flag is disabled, meaning Wi-Fi and Bluetooth are available and unrestricted.
- For more information refer to the Device Manager documentation.

Supported Parameters

Listed here are some of 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 = Asia/Jerusalem
- 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, SILENT
- admin/default_password = 1234
- admin/ssh_enabled=0/1 (default)
- security/SSLCertificateErrorsMode = IGNORE, NOTIFICATION, DISALLOW (default)
- security/ca_certificate/[0-4]/uri
- 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

- admin/restrict_wireless

Configure Phone Behavior

- Configure Minimum and Maximum Ringer Volumes via the Phone's Configuration File below
- Configure Noise Reduction on the next page
- Disable the Phone's Speaker Hard Key on the next page
- Enable a Phone to be used as an Audio Device on page 124
- Update Phone Firmware Manually on page 125
- Update Microsoft Teams Devices Remotely on page 127
- Apply a Partial Configuration Profile on page 128
- Enroll a Device with Intune Policies on page 128
- Configure Time on Teams Devices on page 105
- Restore the Phone to Default Settings on page 51

Configure Minimum and Maximum Ringer Volumes via the Phone's Configuration File

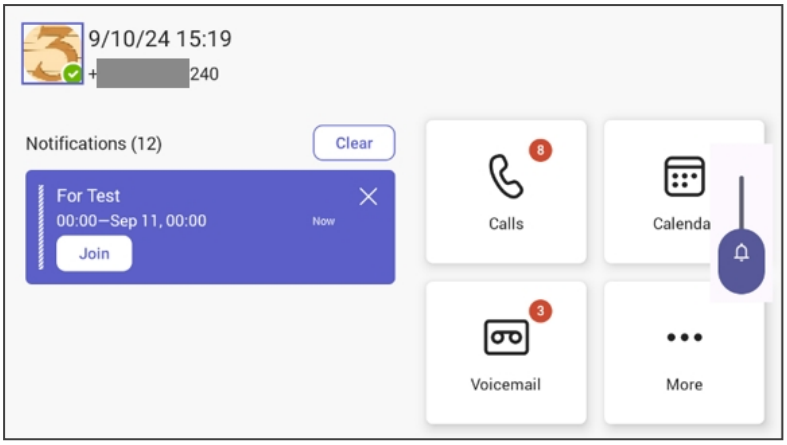
Android phones feature a capability enabling administrators to configure minimum and maximum ringer volumes via the phone's configuration file. The feature complies with industrial customers' requirements for phone ringers to be louder and for administrators to be able to stop users from reducing ringer volume to too low.

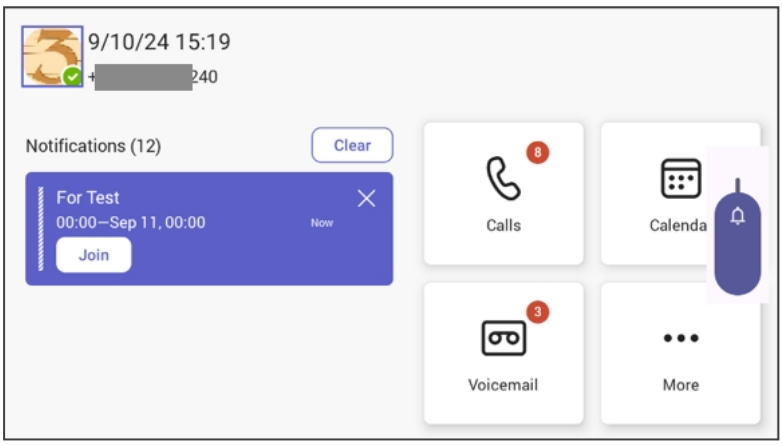
➢ **To configure maximum and minimum volume:**

1. Set the configuration file parameter `audio/ringer/volume_max` to **10**.
2. Set the configuration file parameter `audio/ringer/volume_min` to **0**.



- Ringer volume by default has a range of **0-10**, where **0** is mute.
- The capability allows administrators to define a *new minimum* | *maximum range* of **3-7** so that the user will be able to reach a minimum of **30%** and a maximum of **70%** of the original **0-100%** range as shown in the figures below. The same principle applies to all phone models. Only screen dimensions vary.





Configure Noise Reduction

The phone supports a noise reduction mechanism designed to improve call clarity in open-space environments. This mechanism minimizes background noise, such as machinery, chatter, and ambient sounds, heard by remote participants when the local user is not speaking.

By default, the system intelligently suppresses most background noise without compromising voice quality. For high-noise environments, an advanced configuration option is available:

- **Parameter:** `dsp/audio/reduce_open_space_noise`
- **Default Value:** `2`
- **Optional Value:** `3` (for more aggressive noise reduction, with slight impact on voice quality)

Disable the Phone's Speaker Hard Key

The speaker hard key on the phone can be configured to be disabled so that in an office environment, the user won't have the option to use the speaker. Speaker functionality will then be disabled during calls. Pressing the hard key will have no impact and its light will not illuminate. Only use of the handset and headset will be enabled.

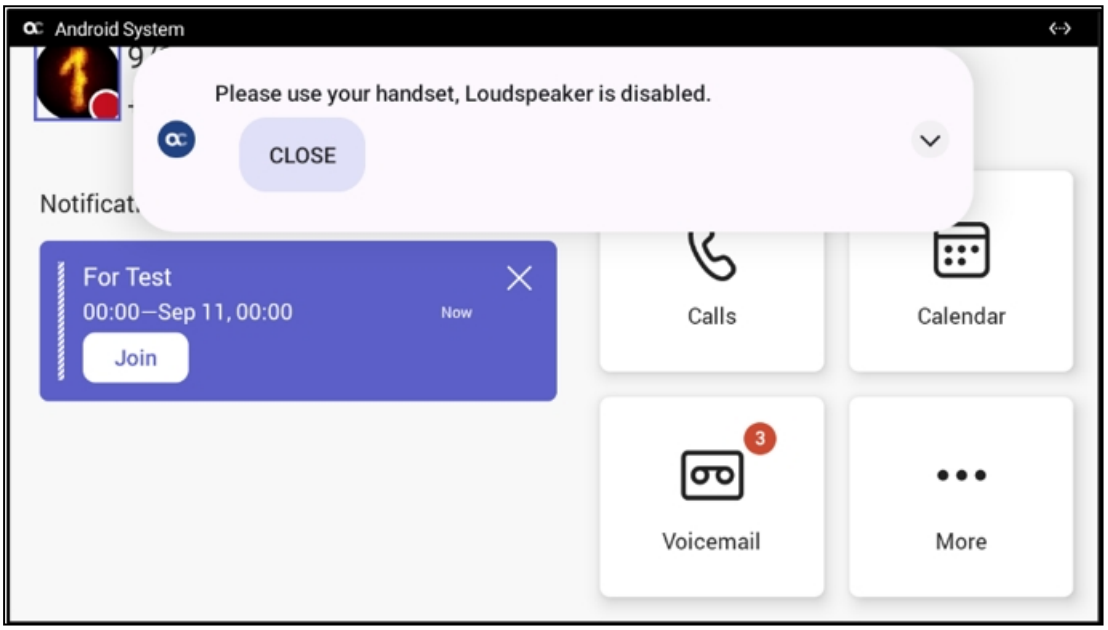
The feature complies with requests from customers in whose offices discretion is important (e.g., government).

➢ **To configure the speaker hard key on the phone to be disabled:**

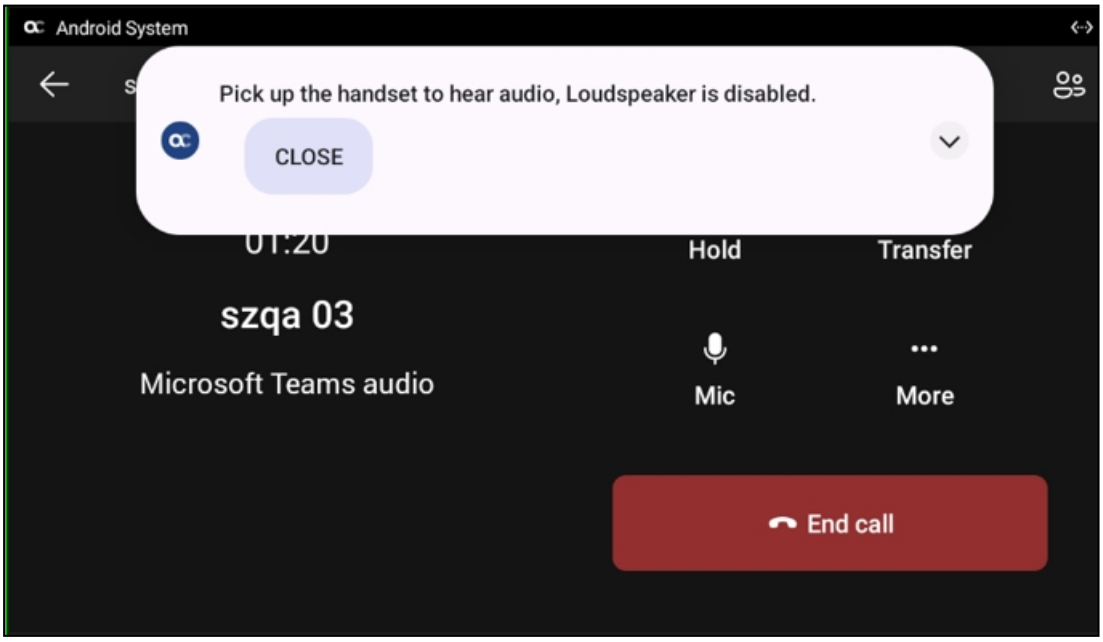
1. Configure the configuration file parameter `audio/speakerphone/enable` to:
   - `0` = Disable (default)
   - `1` = Enable

> ⚠ Ring to speaker still functions.

2. If after the feature is enabled the user presses the 'Speaker' button in the idle screen, the following popup message is displayed in the phone screen:



3. If after the feature is enabled the user presses the 'Accept' softkey or the speaker hard key, the following popup message is displayed in the phone screen:



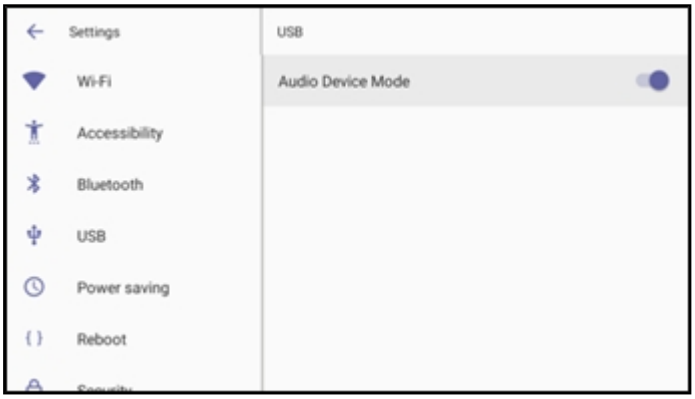
4. The user can then answer by picking up the handset or by putting on the headset if a USB headset is connected. The popup indication then disappears.

Enable a Phone to be used as an Audio Device

USB host mode is supported, i.e., the phone can be connected to a PC via a USB-A Male – USB-A Male cable, allowing it to be used as the PC's audio device such as an external speaker. Click here to view a video clip demonstrating how to use the phone in Audio Device Mode. The principle is the same across all AudioCodes Teams phone models.

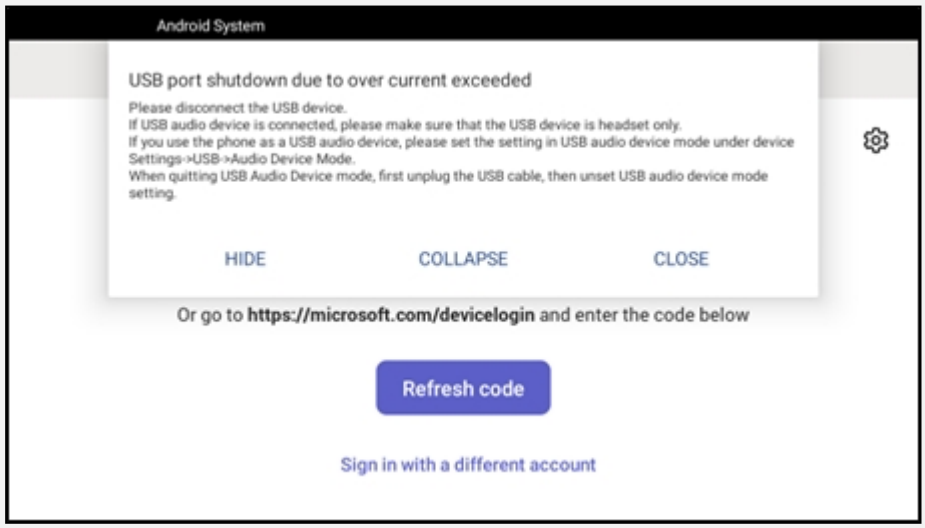
➢ To set up the feature:

1. In the phone's Device Settings > USB, enable **Audio Device Mode**.



2. Connect the the USB-A - USB-A cable from the phone to the PC.

- It is important to set the feature up *in this order* (i.e., first enable USB mode and then connect the USB cable).
- If the cable is connected before enabling the mode, you'll get this message:



3. On a PC running Windows OS, navigate to **Settings** > **Devices** > **Audio** and make sure the phone is set to be the PC's default audio device.
4. Play media such as YouTube and Windows Media Player via the phone speaker.

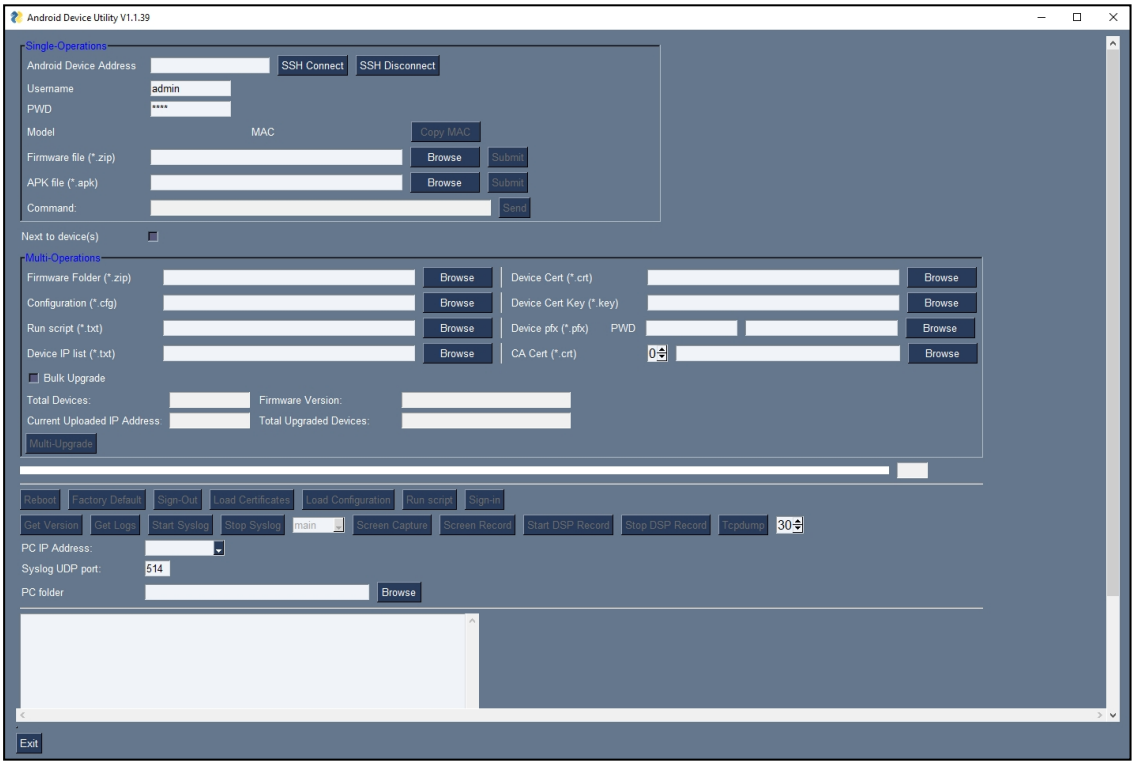
Update Phone Firmware Manually

AudioCodes' Android Device Utility allows network administrators to manually update a phone's firmware.

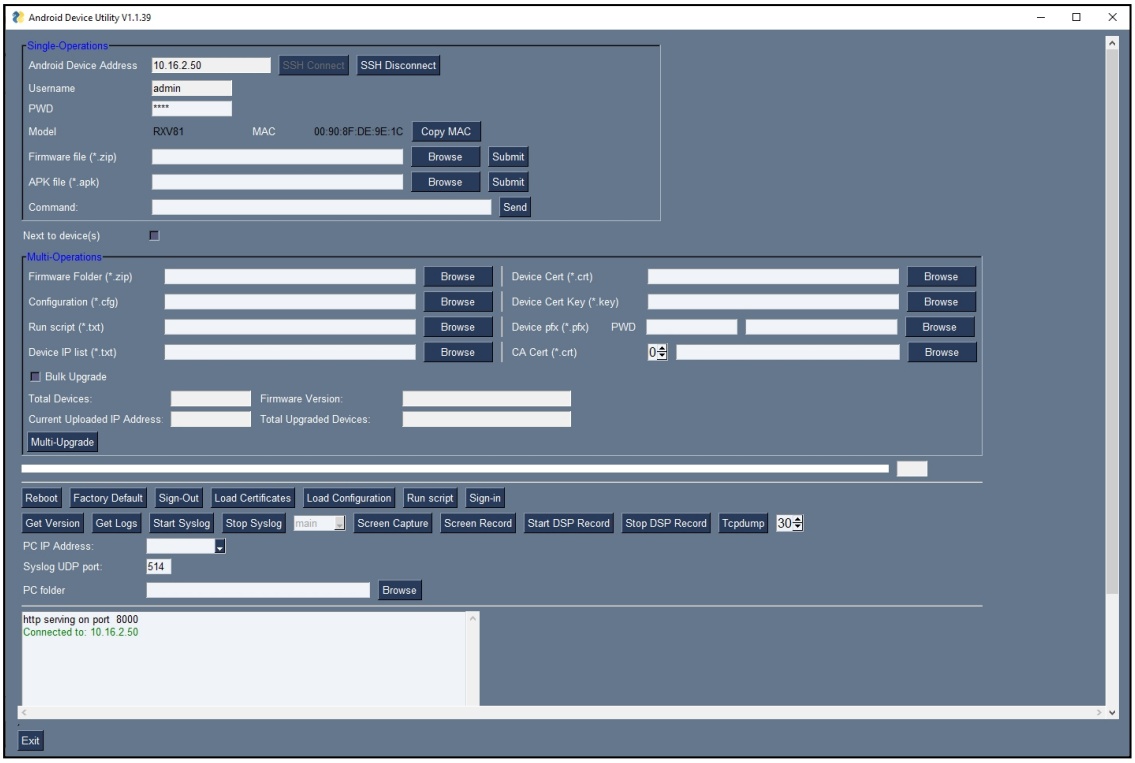
- Firmware downgrade is blocked as of version 2.3.453 to prevent a possible race condition between Microsoft TAC and AudioCodes' OVOC | Device Manager.
- After an upgrade is completed and the popup of 'Reboot now or Later' appears, wait for about 30 seconds before pressing the **Reboot** button.

To manually update a phone's firmware:

1. From the PC's **Start** menu, select the app icon or click the application's exe file in the folder in which you saved it.

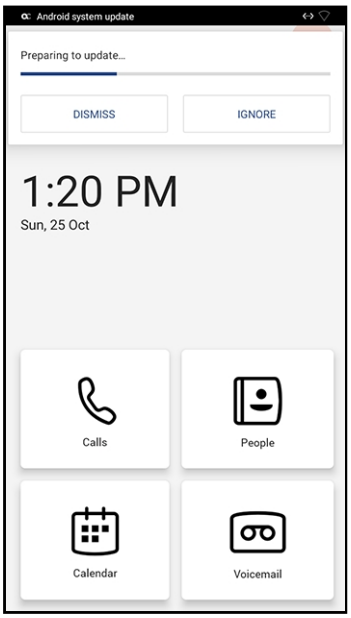


2. In the 'Android Phone Address' field, enter the IP address of the device (get it by tapping the user's picture | avatar in the home screen > **Settings** > **Device Settings** > **About phone** > **Status** > **IP Address**).
3. Click **SSH Connect**; a connection with the device is established.



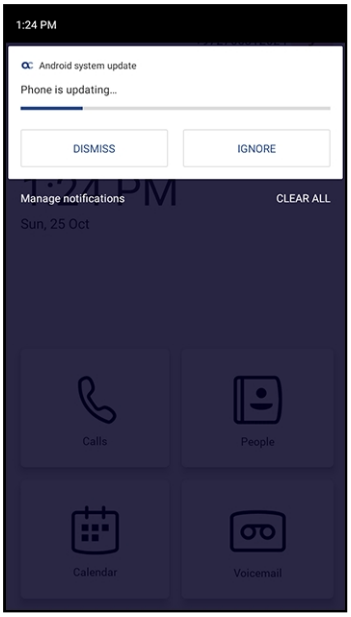
4. Under the 'Single Operations' section of the screen next to the field 'Firmware file', click the **Browse** button and navigate to and select the candidate image file.
5. Click the **Submit** button; a firmware upgrade process starts; the phone is automatically rebooted; a notification pops up when the process finishes. The phone notifies you that it's being updated and rebooted.

> Upgrade notifications are also displayed when the phone is upgraded remotely from Microsoft Admin Portal or from AudioCodes' Device Manager.

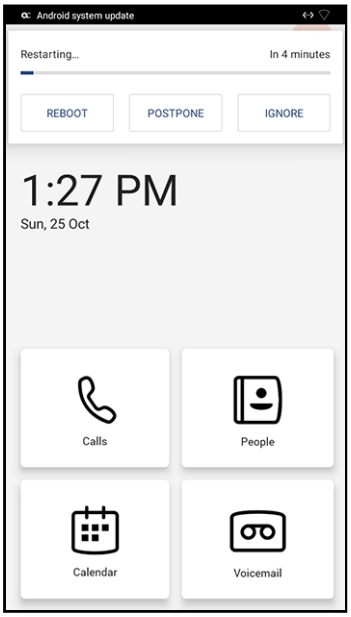


➢ **To manage notifications during an upgrade:**

1. Swipe down twice in rapid succession to present the **Manage notifications** option.



2. Tap **Manage notifications**; the screen that is then displayed allows viewing notifications such as:
   - Upgrade state (Preparing, updating, etc.)
   - Internet access issues
3. After the update is completed, the phone reboots.



Update Microsoft Teams Devices Remotely

For instructions on how to update Microsoft Teams devices remotely, see here.

Apply a Partial Configuration Profile

Configuration profiles enable administrators to simultaneously assign several settings to multiple Android devices. Different types of settings are supported, e.g., general settings, device settings, network settings applied to the device through a partner agent, and meeting settings applied on the Teams app via the Microsoft Teams Admin Center (TAC).

When the administrator assigns a configuration profile to a device, not all settings that are part of that profile are applied to the device. Settings on the device that were configured by the user are not overridden. Administrators can change a particular setting without overriding the other setting values defined by the user.

For more details and instructions, click here.

Enroll a Device with Intune Policies

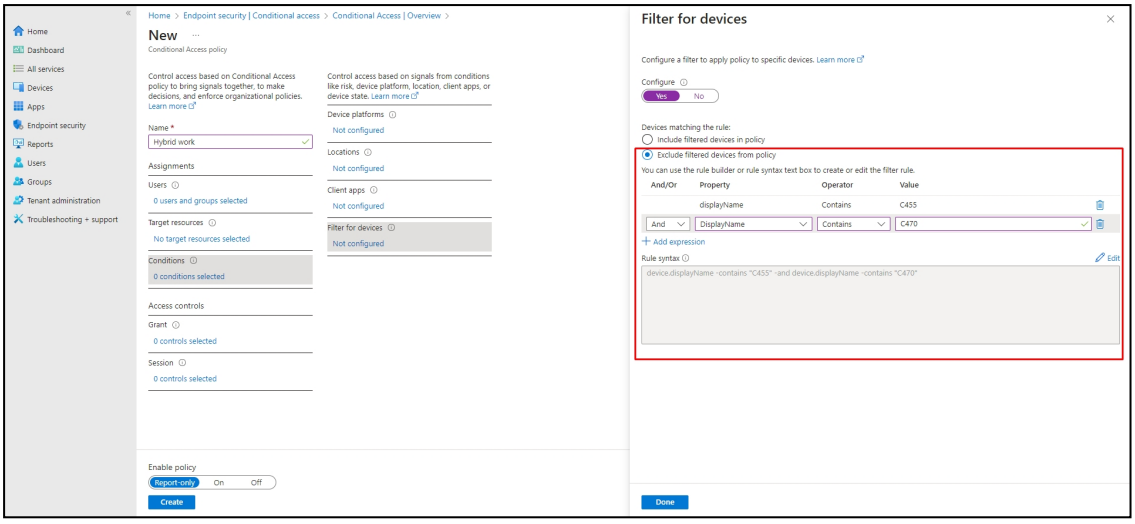
- To learn about Intune conditional access and Intune device policies for Microsoft Teams devices, click here.
- For more information about AOSP device management , refer to official MS documentation. In addition, refer to the AOSP Migration Guide.
- See also the following sections for detailed instructions:
  - Create an Exclusion Group below
  - Remove Devices from Intune Admin Center on the next page

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 previous configured:
  - Access Microsoft Azure Government Portal **Home > Conditional Access Policies > Require Hybrid Joined or Intune to Access Cloud Resources Conditional Access policy** as shown in the figure below.
  - Exclude the device from Intune policies and replace **displayName -contains <C4xxHD>** where **<C4xxHD>** is the name of the device model (**device.model**).

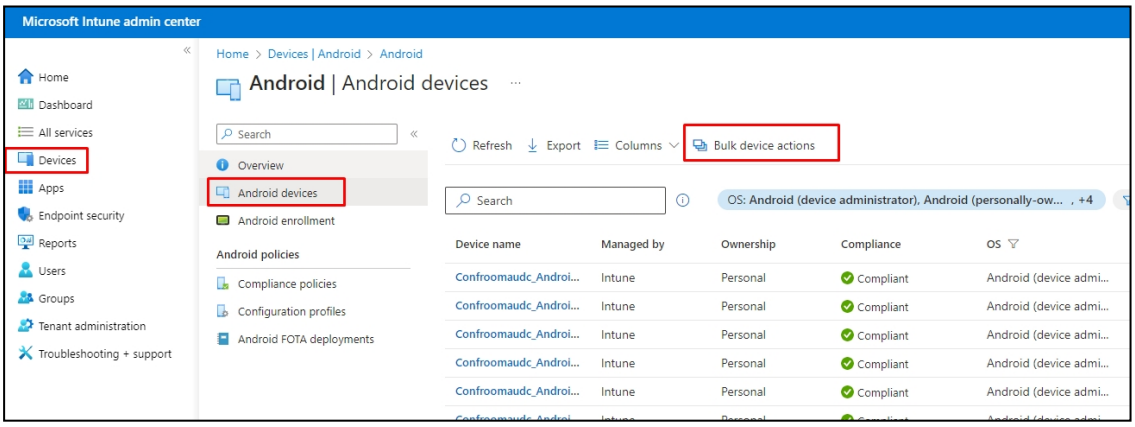


Remove Devices from Intune Admin Center

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

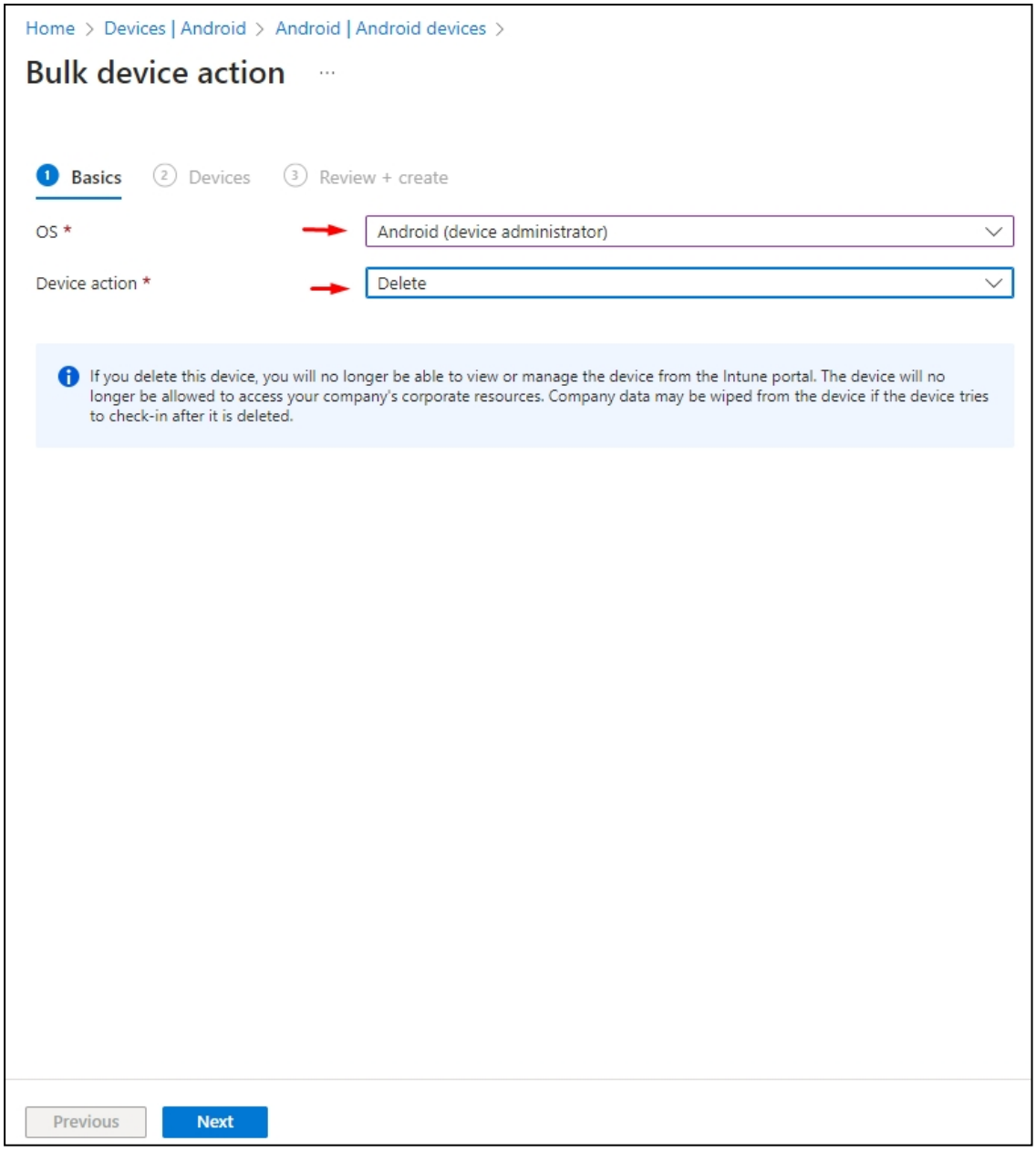
➢ To remove devices from Intune Admin Center:

1. Go to Microsoft 365 Admin Center [portal.office.com] and log in with an Administration account.
2. Navigate to **Devices** > **Android devices**.

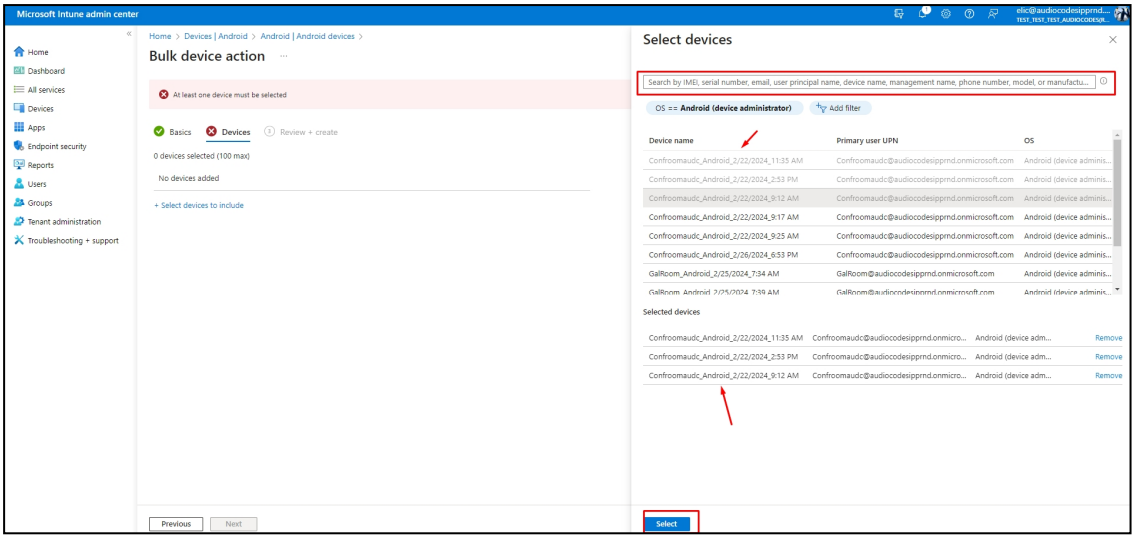


> The Intune Admin Center service is licensed according to the terms of individual licenses so not all network administrators will be able to navigate to it. Check if the license you're using includes the service or not.

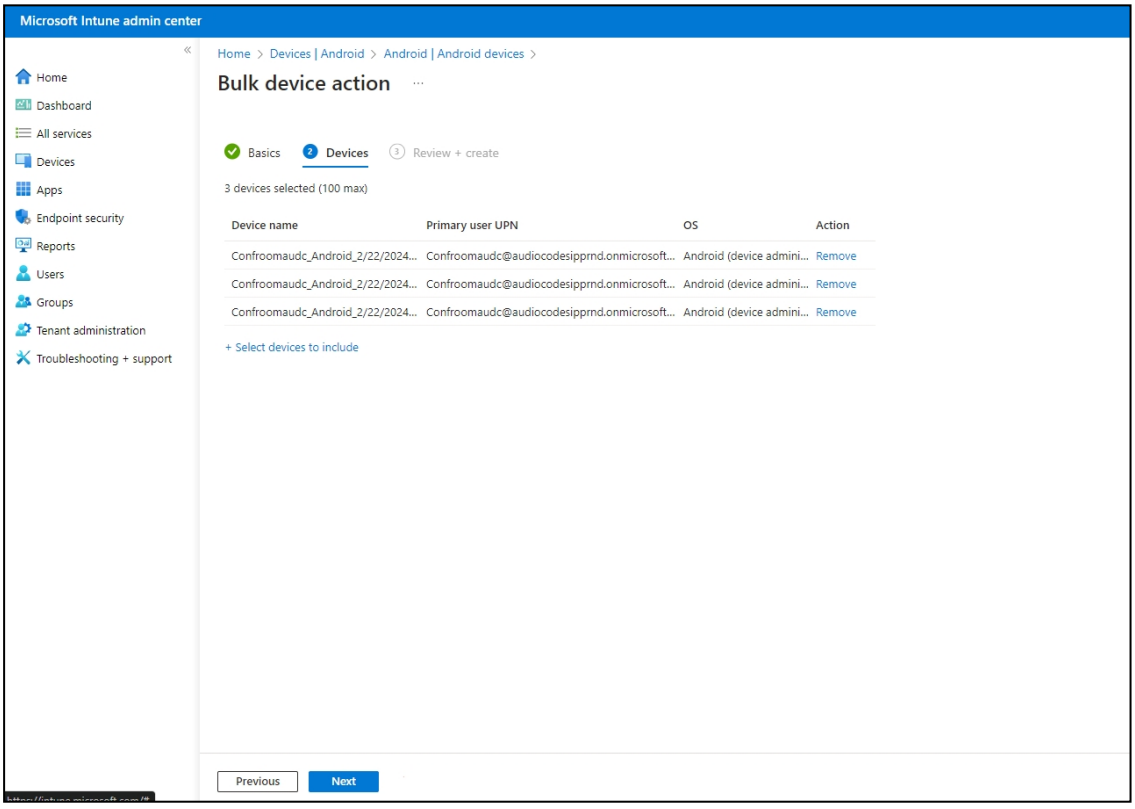
3. Click **Bulk device actions**.



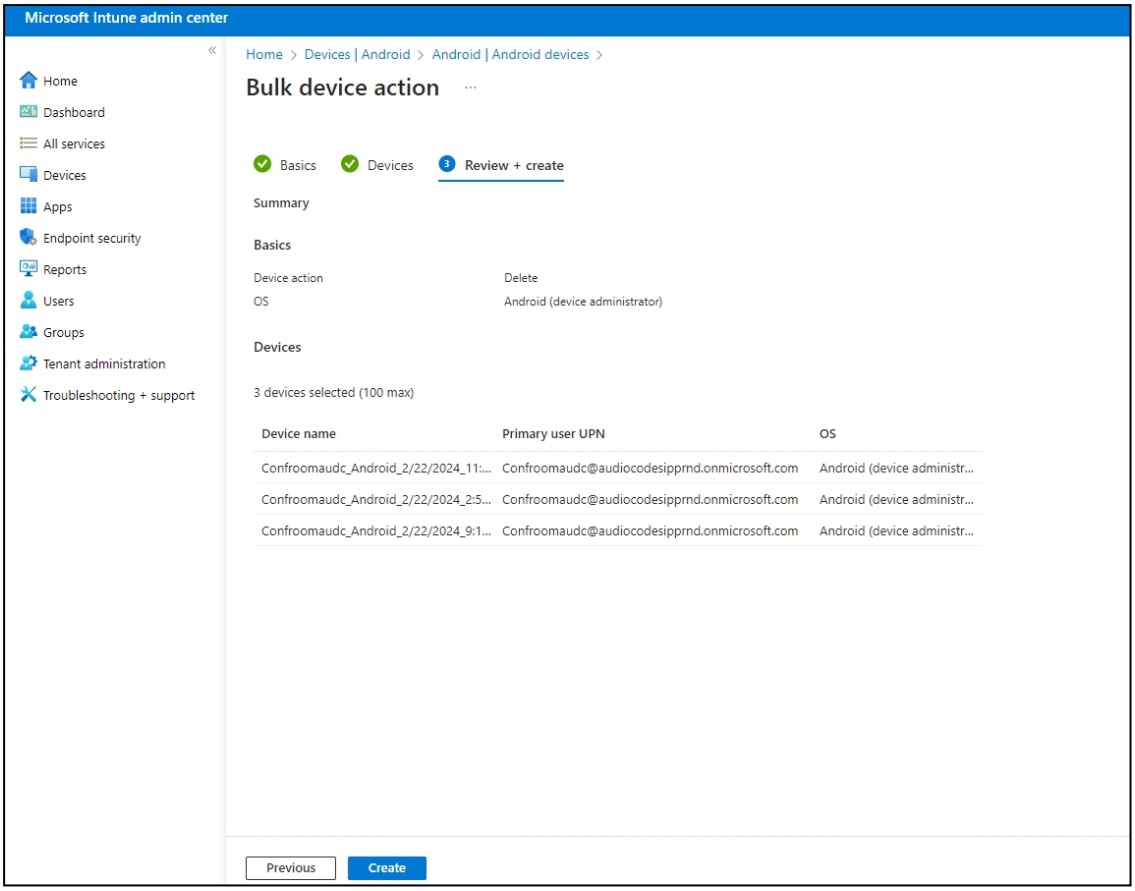
4. From the 'OS' drop-down under the ❶ **Basics** tab, select **Android (device administrator)**. From the 'Device action' drop-down, select **Delete**. Click **Next**.



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



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



7. Under the 3 **Review + Create** tab, make sure your definitions are correct and then click **Create**; the administrator 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 so after deleting the devices wait for 30 minutes before signing in.

Set up Emergency Handling

- Set up an E911 Emergency Location below
- Enable Users to Make Calls even if Teams is Unavailable on the next page

Set up an E911 Emergency Location

An E911 emergency location can be set up using the Microsoft Teams Admin Center (TAC). For details and instructions, click here.

After a location has been defined, make sure that:

- AudioCodes' phone runs the latest firmware released.
- E911 information is displayed on the phone screen 30-120 minutes after the location is set (time estimated under laboratory conditions).
- To trigger information to be shown before that time period, dial a 933-test call and check if the location has been accepted, displayed and vocalized by the announcer.

Enable Users to Make Calls even if Teams is Unavailable

A fallback feature enables users to make calls even if Teams is unavailable. If Teams is unavailable, the device will still have connectivity to the internet via the SBC using a SIP-based application.

For this feature to work, the SBC must be configured for WebRTC. For details, refer to the *WebRTC* section in the Mediant Software (VE-CE-SE) SBC User's Manual.

➢ To enable it, the administrator must:

1. Set parameter 'system/ace/shortcut_enabled' to **1** (default = **0**); an AC soft button is then displayed in the lower right corner of the phone screen (if Teams is unavailable) as shown here:



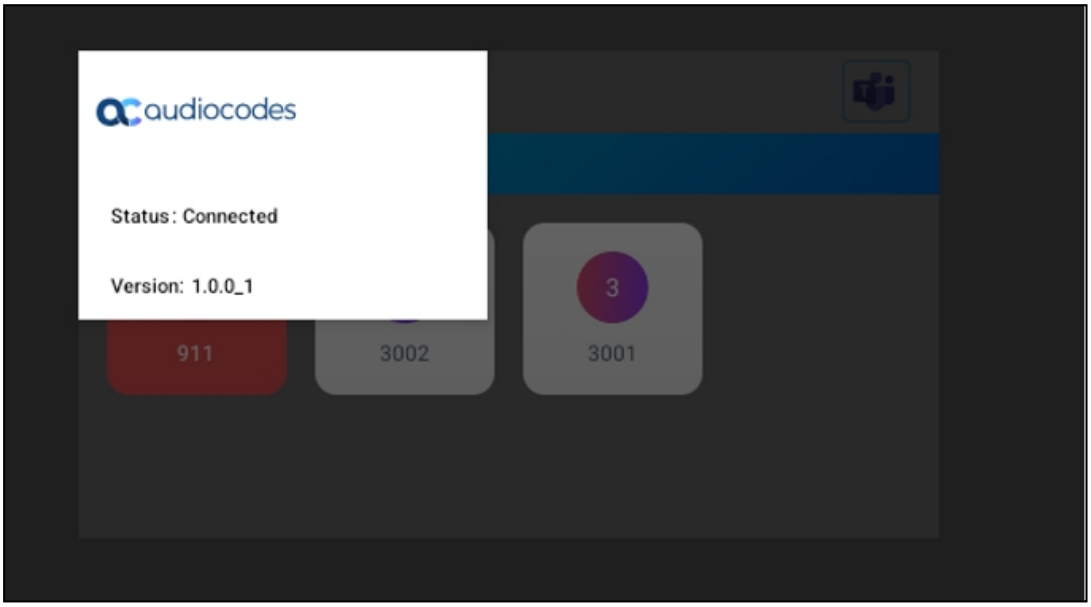
2. Set the parameter 'system/ace/minilauncher_enabled' to **1** (default = **0**) to enable the app to be launched if Teams is available.

➢ To register a SIP account (sign in), the admin must:

1. Set the following parameters:
   - `personal_settings/sip/server =wss://<SBC URL>`

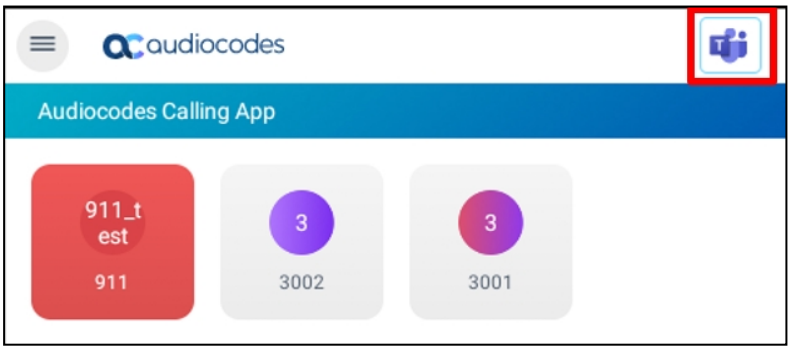
- `personal_settings/sip/port =<SBC server port>`, e.g., **443**
- `personal_settings/sip/domain =<domain name>`
- `personal_settings/sip/username=<account name>`
- `personal_settings/sip/password=<account password>`

2. View the account status: **Connected** if registered, **Not Connected** if not registered.



➢ **To enter the app, the user must:**

■ Press the **AC** button to switch to the app. To switch back to Teams, press the Teams button as shown in the figure below the next.



➢ **To add up to 41 speed dial keys, the administrator must:**

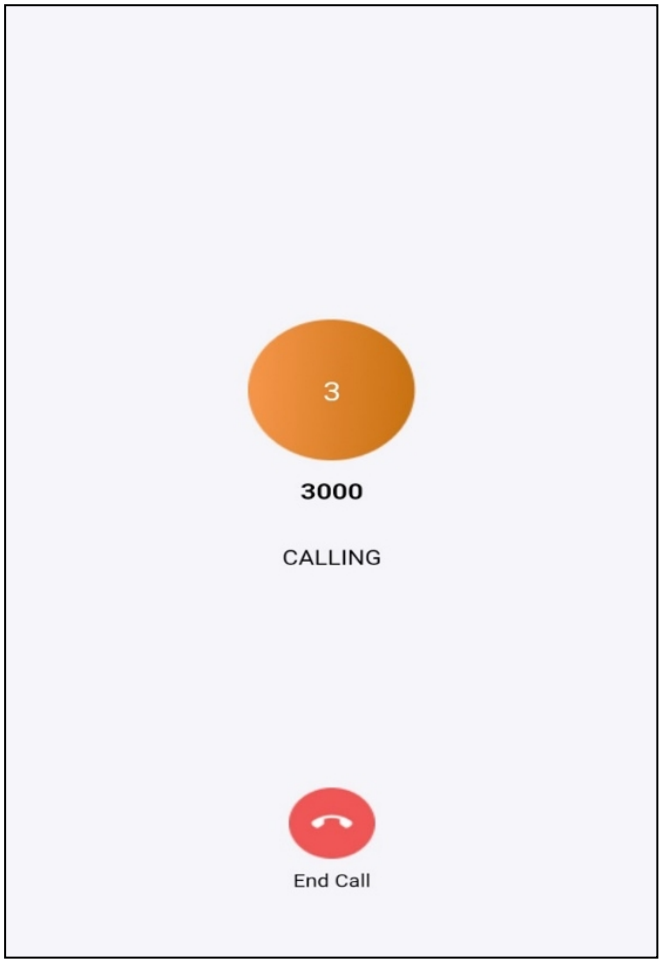
1. Use the following parameters:

- `personal_settings/functional_key/[0-40]/speed_dial_number=< destination>`
- `personal_settings/functional_key/[0-40]/type = DEFAULT` (button retains its Teams color) -or- `EMERGENCY` (button is colored red)

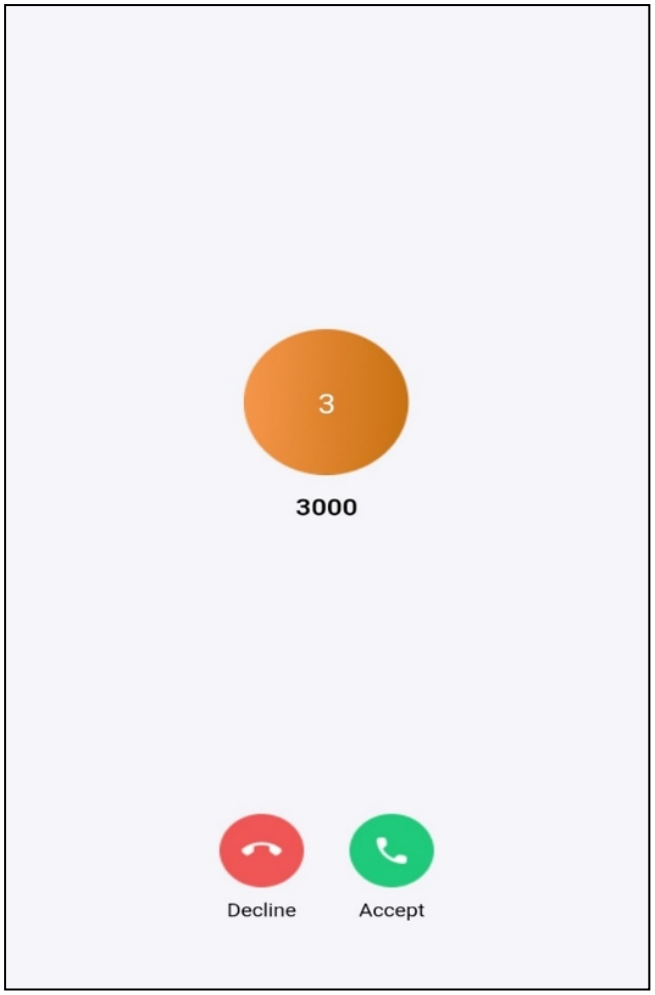
- `personal_settings/functional_key/[0-40]/display_name=<destination display name>`

➢ **To make a call, the user must:**

1. Tap the speed dial; the calling screen shows the callee's name. To end the call, tap the 'End Call' button.
2. View the phone's calling screen:



3. View the phone's incoming call screen:



4. [Optionally] During the call, the user can adjust the volume, mute, unmute, DTMF, switch audio source, etc.

- The app blocks incoming calls when Teams is in the foreground.
- When Teams is available and the app is in the foreground in idle state, the phone cannot get an incoming Teams call.
- After rebooting, the device always displays the Teams home screen.

6 Troubleshooting

The information presented here shows how to troubleshoot AudioCodes devices:

- Basic Phone Troubleshooting for Users below
- Device Troubleshooting Options on page 139
- Android Device Utility on page 144
- SSH based Debugging on page 157
- Microsoft Teams Admin Center on page 157
- DSCP on page 160
- Additional Debugging Options on page 161

Basic Phone Troubleshooting for Users

Read the following if an issue with your phone occurs. Contact your network administrator if necessary. Network administrators can also use this documentation as reference.

Table 6-1: Troubleshooting

Symptom	Problem	Corrective Procedure
Phone is off (no screen displays and LEDs)	Phone is not receiving power	■ If using Power over Ethernet (PoE), contact your network administrator to check that the switch is powering the phone. ■ Make sure the AC/DC power adapter is attached firmly to the DC input on the rear of the phone. ■ Make sure the AC/DC power adapter is plugged into the electrical outlet. ■ Make sure the electrical outlet is functional.
Phone is not receiving incoming calls (No flashing red LED; no Incoming Call message displayed on screen)	Presence status is set to **Do Not Disturb**	Check your presence status (see Change Your Presence Status on page 60). If it is set to **Do Not Disturb**, change it to **Available**
	Calls are automatically forwarded	Check the **Incoming callls > Call forwarding** settings on the **Calls** screen (see Configure Teams Application Settings on page 62). Verify that: ■ **Call forwarding** is **OFF** or **Forward to** is not redirecting calls. ■ **Also ring** is configured as expected.

Symptom	Problem	Corrective Procedure
		■ **If unanswered** is not forwarding unexpectedly.
	No Internet access	If the device is not connected to the Internet, a **No Internet Access** message is displayed. Check the following: ■ The Ethernet LAN cable supplied by AudioCodes is properly plugged into the phone's RJ-45 port and the LAN outlet. ■ Alternatively, if the phone supports Wi-Fi, verify that it is connected to an available Wi-Fi network (see Configure Wi-Fi on page 39). ■ Verify there are no Internet issues in your area. Check with your Internet provider if needed.
	Teams sign-in problem	Make sure you are signed in to the phone. If you are signed in, sign out (see Sign Out on page 103), then sign back in (see Sign In to Your device Teams Phone on page 15). See also Migration to Android Open Source Project (AOSP) on page 6.
	None of the above	Reboot the phone (**Device settings > Reboot**). If this does not help, contact your administrator.
Phone is not ringing	Ring volume is set too low	■ Increase the volume (see Adjust Ring Volume on page 81).
Screen display is poor	Screen settings	■ Adjust the phone’s screen brightness.
Headset has no audio	Headset not connected properly	■ Make sure your headset is securely plugged into the headset port located on the side or the rear side of the phone. ■ Make sure the headset volume level is adjusted adequately (see Adjust Headset Volume on page 82).

Device Troubleshooting Options

The phone's Device Settings screen contains a multitude of status monitoring and debugging tools.



You need to be logged in as Administrator to access most troubleshooting tools (see Log in as Administrator on page 107).

Debugging options include:

- Monitor Phone Process Statuses below
- Get Audio Debug Recording Logs on the next page
- Capture Traffic Using 'rpcapd' on page 141
- Restore the Phone to Default Settings on page 51
- Return to Previous Version on page 144

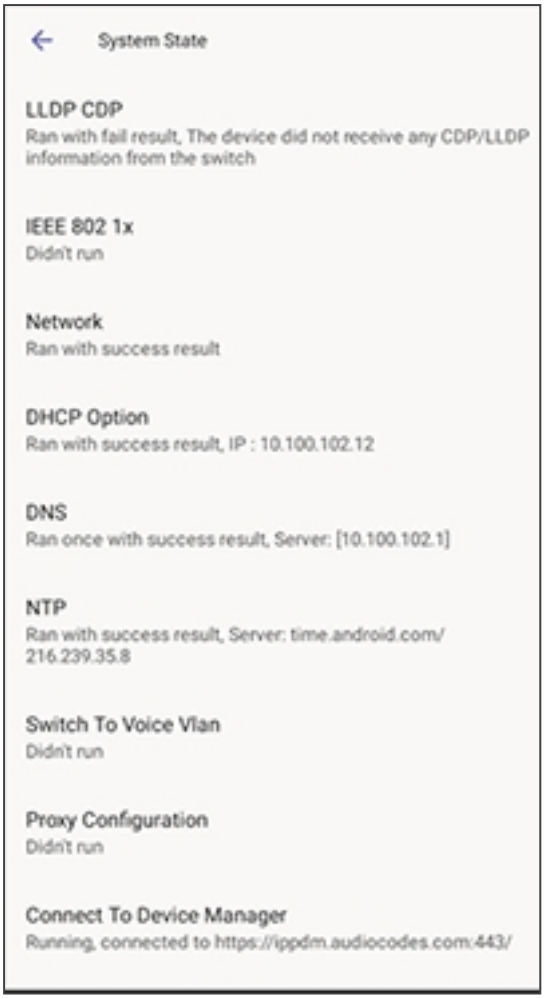
Monitor Phone Process Statuses

Administrators can monitor process statuses on the phone's System State screen.

If initial provisioning is unsuccessful or if the administrator encounters an issue related to the network / connection to Device Manager, this feature gives an indication as to why. The feature enables debugging via the phone screen without requiring external systems. The administrator can check connectivity independently of external apps.

➢ **To monitor the process statuses:**

1. Log in as Administrator on page 107.
2. On the phone's Device Settings screen, scroll down and tap **Debugging**, then **System State**.

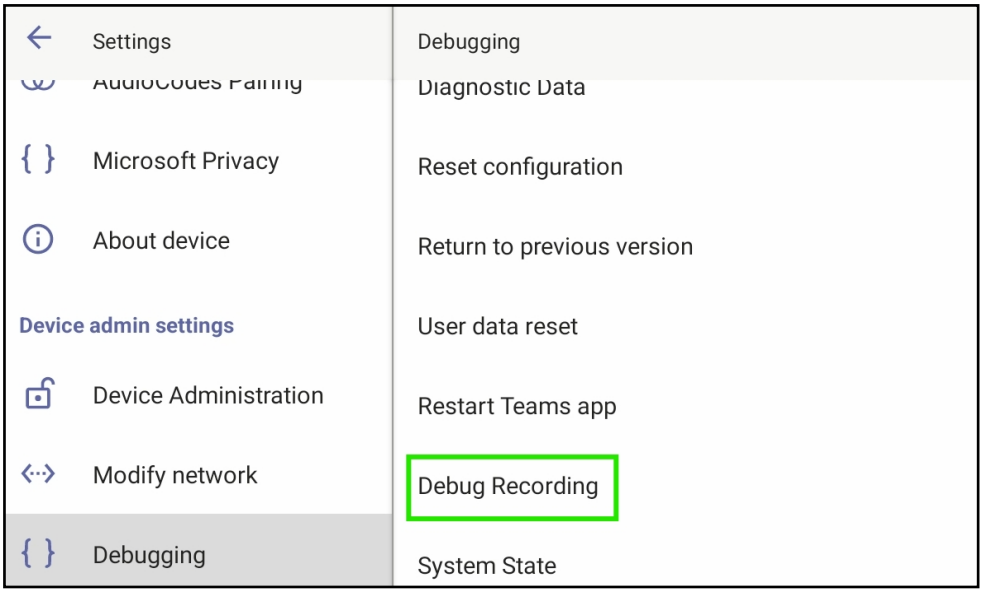


Get Audio Debug Recording Logs

Network administrators can opt to get Audio Debug Recording logs from the phone screen. The purpose of these logs is for issues related to media.

➢ **To enable Audio Debug Recording logs:**

1. Navigate to Device Settings and log in as Administrator.
2. Scroll down and navigate to **Debugging > Debug Recording**.



3. Configure the remote IP address and port.
4. Enable 'Voice record'.
5. Start Wireshark on your PC to capture the Audio traffic.

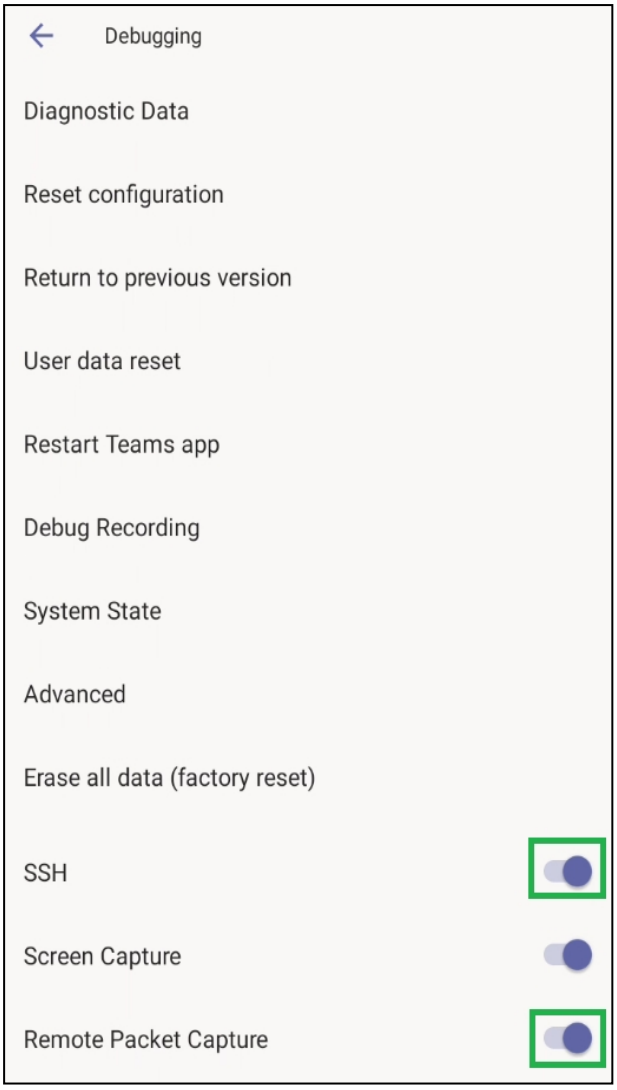
Capture Traffic Using 'rpcapd'

The 'rpcapd' (Remote Packet Capture) network sniffer application enables network administrators to analyze and debug Android traffic on their desktop PC using the app's integral SSH server.

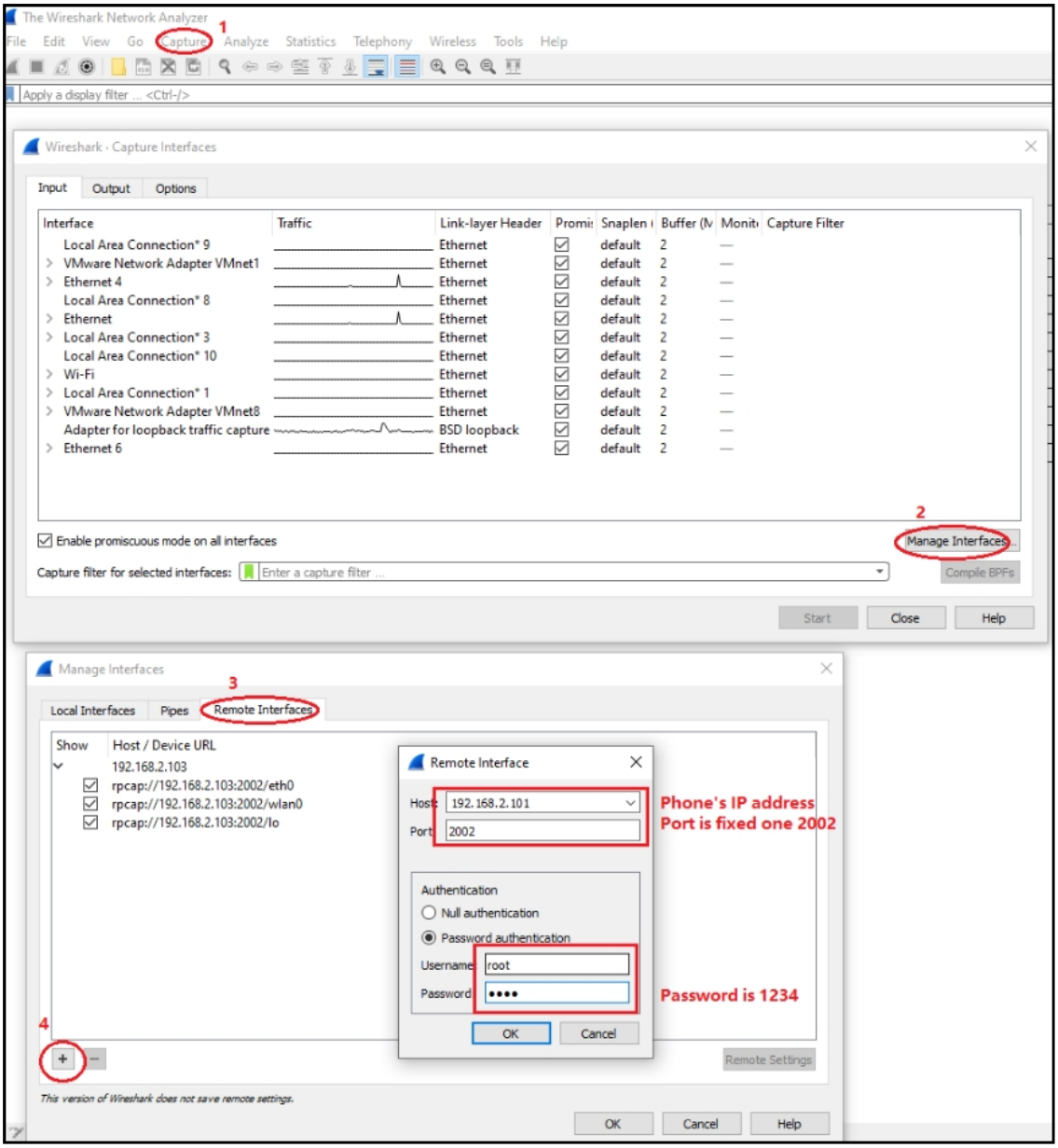
SSH is by default disabled and needs to enabled for the feature to work.

➢ **To capture traffic using 'rpcapd':**

1. Log in as Administrator on page 107.
2. Scroll down and tap **Debugging**.
3. Turn on **SSH** and **Remote Packet Capture**.



4. After 'rpcapd' is enabled on the phone, use Wireshark to connect with it. Follow **the steps below** to connect to the phone.



5. View all the interfaces on the phone and choose your preferred interface with which to capture packets.

Enable Port Mirroring Network Monitoring

The phone supports the port mirroring network monitoring technique of copying and sending network packets transmitted as input from a phone port, to another port of a monitoring device for enhanced analysis and debugging capability.

➢ To enable the feature:

- Open the phone's 'Modify network' screen (**Settings** > **Device admin settings** > **Modify network**) and select the option 'Enable PC Port Mirror' to enable it if it isn't already enabled.

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 Global Availability (GA) build running on the device. The user needs to change the active firmware slot and perform a factory reset.

➢ **To switch back to previous firmware:**

1. Log in as Administrator on page 107.
2. On the phone's Device Settings screen, scroll down and tap **Debugging**, then **Return to previous version**.

Android Device Utility

AudioCodes' IP phone is by default accessed via Secure Shell (SSH) cryptographic network protocol after the administrator signs in.



SSH is by default disabled and can be enabled with Administrator permissions in the phone screen (**Device Administration** > **Debugging** > **SSH**).

AudioCodes provides administrators with an SSH-based Android Device Utility. For a detailed description on how to install and use the utility, see the Android Device Utility User's Manual.

➢ **To sign in to the utility:**

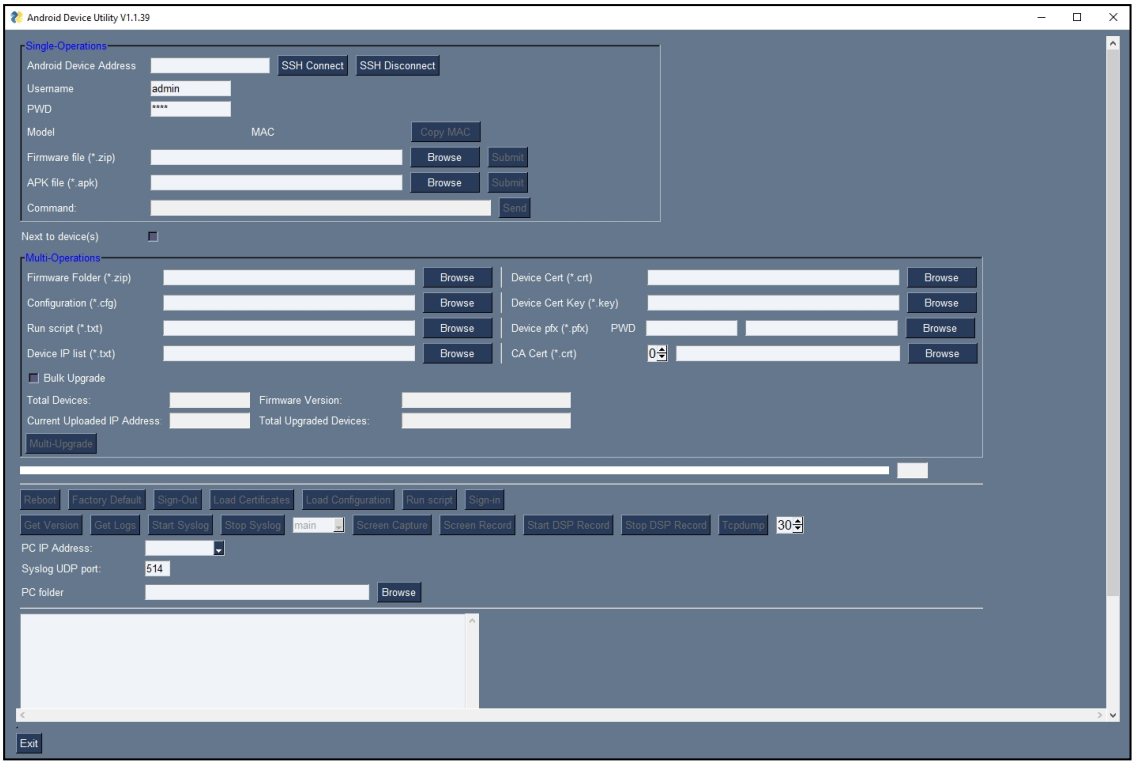
- Enter your username and password; **admin** and **1234** are the defaults.

The application gives network administrators the following debugging capabilities:

- Capture the Phone Screens on page 146
- Run Tcpdump on page 147
- Get Information about Phones on page 148
- Perform Remote Logging (Syslog) on page 150
- Get Diagnostics on page 153
- Get Logs on page 154
- Activate and Deactivate DSP Recording on page 155

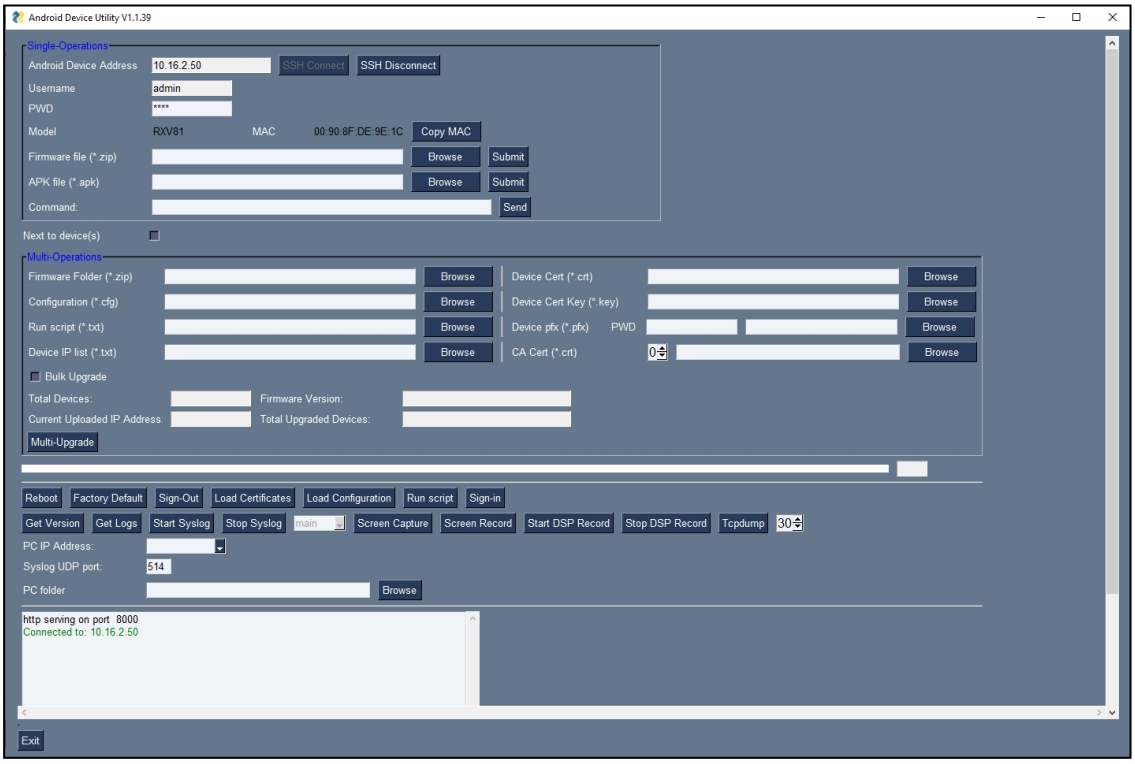
➢ **To open the utility:**

1. From the PC's **Start** menu, select the app icon or click the application's exe file in the folder in which you saved it.



2. In the 'Android Phone Address' field, enter the IP address of the device (get it by tapping the user's picture | avatar in the home screen > **Settings** > **Device Settings** > **About phone** > **Status** > **IP Address**).

3. Click **SSH Connect**; a connection with the device is established.



4. Next to the field 'PC folder', click the **Browse** button and navigate to and select the folder to which to send data to use for debugging.

Capture the Phone Screens

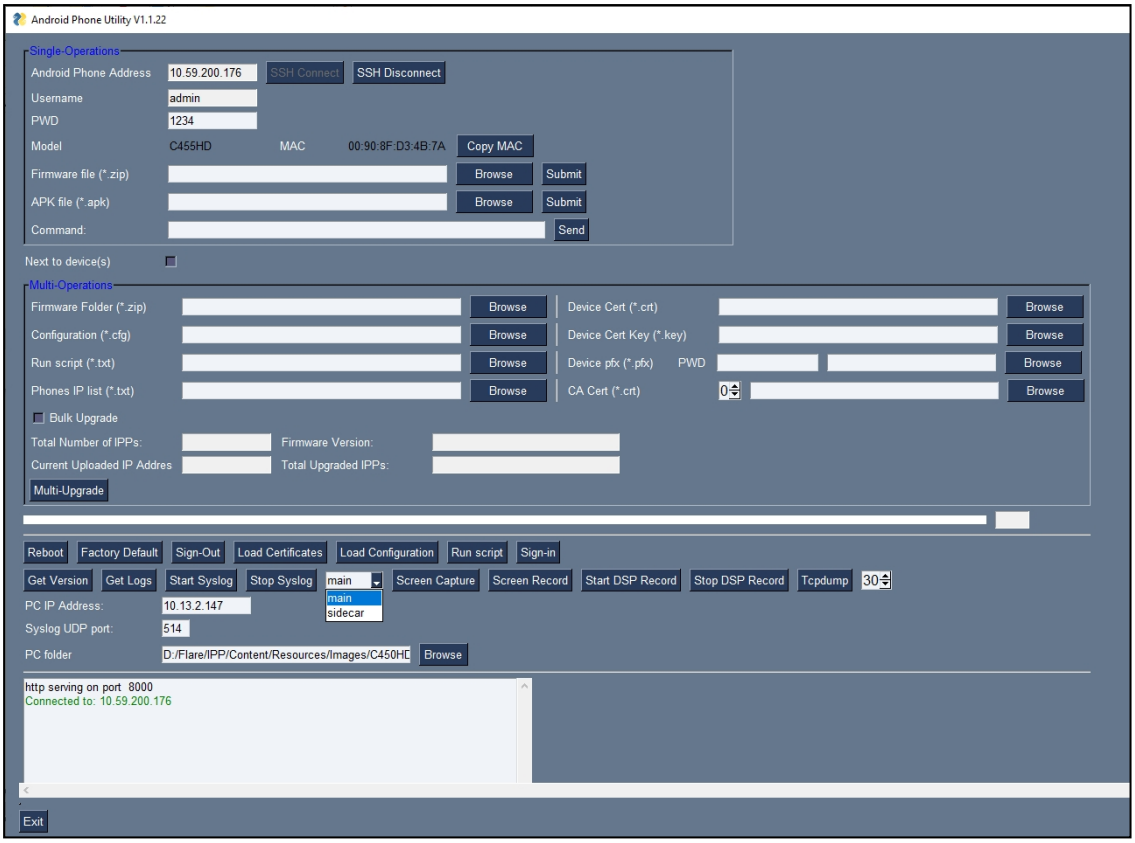


For this feature to work, screen capture must be enabled in the phone's device settings (**Device Administration** > **Debugging** > **Screen capture**). **Screen capture** is enabled by default.

AudioCodes' Android Device Utility allows network administrators to effectively collaborate and debug issues using the screen-capturing feature. The feature enables capturing the phone's main screen.

➢ **To capture the phone screen:**

1. Open the Android Device Utility: From the PC's **Start** menu, select the app icon or click the application's exe file in the folder in which you saved it.
2. In the 'Android Phone Address' field, enter the IP address of the device (get it by tapping the user's picture | avatar in the home screen > **Settings** > **Device Settings** > **About phone** > **Status** > **IP Address**).
3. Click **SSH Connect**; a connection with the device is established.
4. Next to the field 'PC folder', click the **Browse** button and navigate to and select the folder to which to send the screen captures.
5. Make sure that the drop-down menu next to the **Screen Capture** button shows **main**.
6. Click the **Screen Capture** button; the phone's screen is captured and the screenshot is saved and sent to the folder.



7. On your PC, navigate to the folder and retrieve the screenshot. Default file name: **screencap.png**. Rename it to a name related to the screen you captured. If you don't rename it, it will be overwritten the next time you take a screenshot.

Run Tcpdump

Tcpdump is a common packet analyzer that allows network administrators to display TCP/IP and other packets transmitted or received over the IP telephony network, for debugging purposes.

➢ To run Tcpdump:

1. In the Android Device Utility (see Android Device Utility on page 144 for more information about the application), enter the phone's IP address, click **SSH Connect** and browse to a folder on the PC to which to send the information.
2. Next to the **Tcpdump** button, set the time period or leave it at the default. Default: **30** seconds.
3. Click the **Tcpdump** button and then after the progress indicator reaches the end you'll view in the results pane a 'Finished' indication.



4. Open the folder on the PC to which you commanded the application to send the information and locate and open the file 'net.pcap'.

Alternatively, run Tcpdump *without* the utility.

➢ **To run tcpdump without the utility:**

1. Access the phone via SSH and run the following commands:

```
setprop ac.ac_tcpdump.timeout <seconds>
```

2. After defining the capturing time as shown in the preceding command, start the capture:

```
setprop ac.ac_tcpdump 1
```

3. Tcpdump capture file will appear in this location:

```
/sdcard/recording/net.pcap
```

4. After running Tcpdump, reproduce the issue.
5. Execute the following command from your PC command prompt (cmd):

```
scp -r admin@%deviceIp%:/sdcard/recording/ %FolderOnPc%
```

Get Information about Phones

Network administrators can get information about phones using AudioCodes' SSH protocol based Android Device Utility.

➢ **To get information about the phone:**

1. Open the Android Device Utility (see Android Device Utility on page 144 for more information about the application), enter the phone's IP address, click the adjacent **SSH Connect** button and browse to a folder on the PC to which to send the information.
2. Click the **Get Version** button.



3. View the information in the pane.
4. Alternatively:

- To get *firmware information*, in the **Command** field enter the following and then click **Send**:

```
getprop ro.build.id
```

- To get *Bootloader information* using SSH protocol, in the utility's **Command** field enter the following and then click **Send**:

```
getprop ro.bootloader
```

- To get *DSP information* using SSH protocol, in the utility's **Command** field enter the following and then click **Send**:

```
getprop ro.ac.dsp_version
```

- To get the *Microsoft Teams version* using SSH protocol, in the utility's **Command** field enter the following and then click **Send**:

```
getprop ro.teams.version
```

- To get the *Microsoft Company Portal version* using SSH protocol, in the utility's **Command** field enter the following and then click **Send**:

```
getprop ro.portal.version
```

- To get the *Microsoft Admin version* using SSH protocol, in the utility's **Command** field enter the following and then click **Send**:

```
getprop ro.agent.version
```

Perform Remote Logging (Syslog)

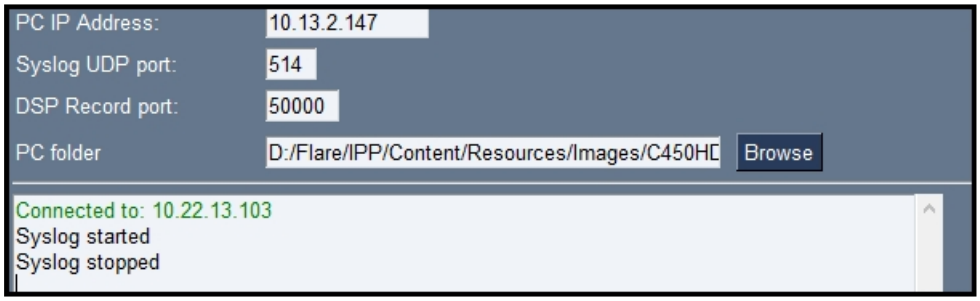
Remote Logging via Syslog provides the same log level as Device Diagnostics (performed via the Microsoft Teams Admin Center) with some additional information that may be relevant to device issues (not Teams application issues). Device Diagnostics via the Microsoft Admin Center are saved to the device sdcard and collected after the event. When performing Remote Logging via Syslog, the logs are collected in real time.

Remote Logging via Syslog can be enabled from the following (see details below):

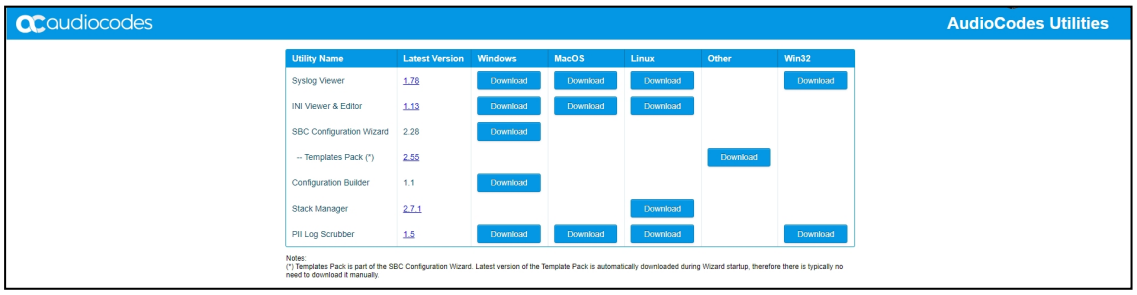
- Android Device Utility
- Phone

➢ To enable Remote Logging via Syslog from the utility:

1. In the Android Device Utility (see Android Device Utility on page 144 for more information), enter the phone's IP address, click **SSH Connect** and browse to a folder on the PC to which to send the information.
2. In the 'PC IP Address' field, enter the IP address of the PC on which the utility is installed and then click the **Start Syslog** button.



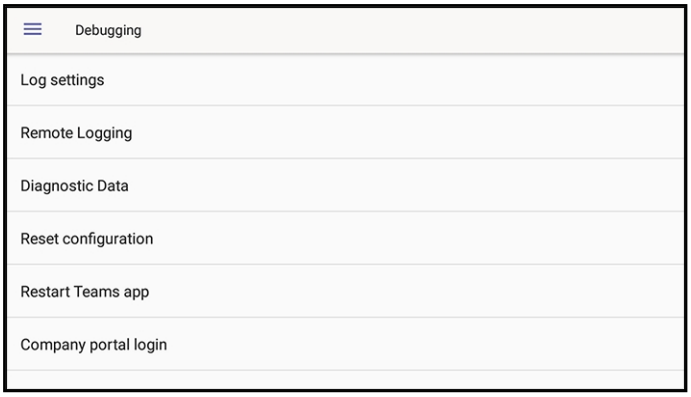
3. Open the folder on the PC to which you commanded the application to send the information, and then locate the Syslog file.
4. To view Syslog, you can optionally download the Syslog Viewer available in AudioCodes' website.

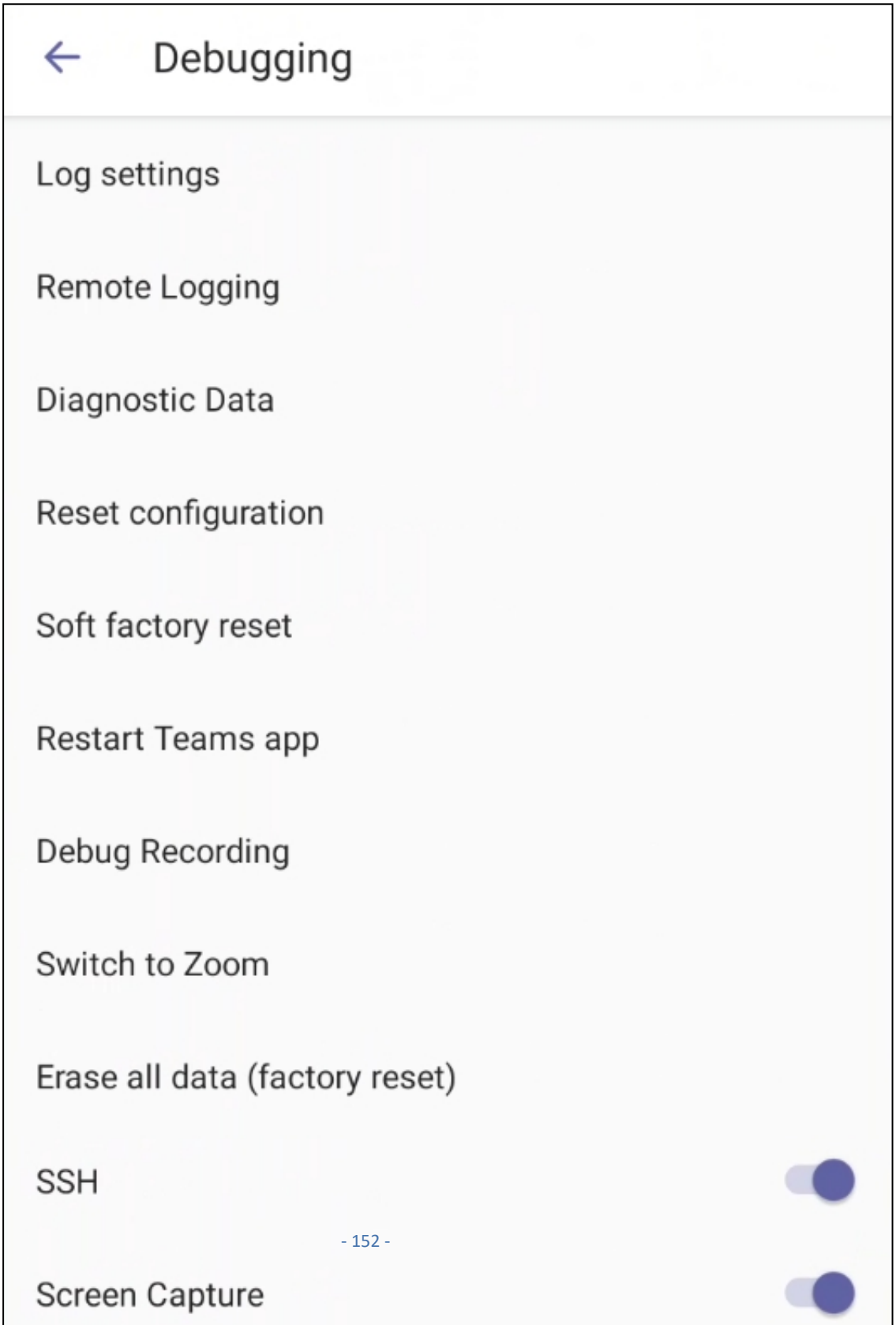


➢ To enable Remote Logging via Syslog from the phone:

1. Log in to the phone as Administrator and go back.
2. In the 'Device administration' screen, select **Debugging**.

3. Select **Remote logging**.


Debugging
Log settings
Remote Logging
Diagnostic Data
Reset configuration
Restart Teams app
Company portal login


Debugging
Log settings
Remote Logging
Diagnostic Data
Reset configuration
Soft factory reset
Restart Teams app
Debug Recording
Switch to Zoom
Erase all data (factory reset)
SSH
Screen Capture

4. Configure the 'Remote IP address' and 'Remote port' and enable 'Remote Logging'; the device starts sending logs to the Syslog server.

> 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 ""
```

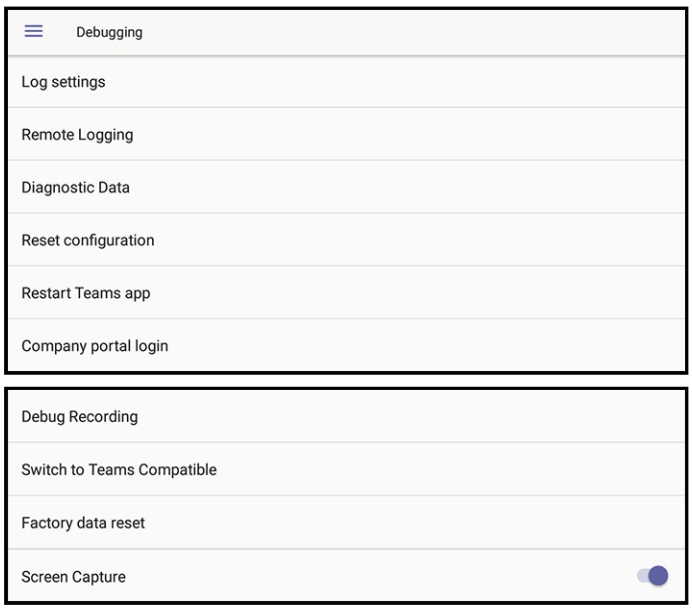
Get Diagnostics

Network administrators can get diagnostics information to facilitate debugging.

> Network administrators who need to get diagnostics info 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 administrator can dump the logs into the SD Card.

➢ **To get diagnostics info:**

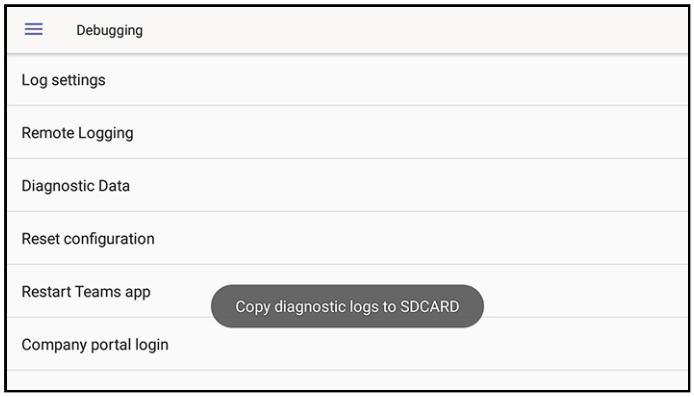
1. Log in to the phone as an Admin user.
2. Open the Debugging screen (**Device Administration** > **Debugging**).



3. Select the **Diagnostic Data** option.



4. Select **OK** to confirm.



5. Wait until the screen shown in the preceding figure disappears; the phone creates all necessary logs and copies them to the its SD Card / Logs folder.
6. Get the logs using SCP notation as follows:

```
scp -r admin@host_IP:/sdcard/logs/ .
```

The following diagnostics files are then received from the phone:

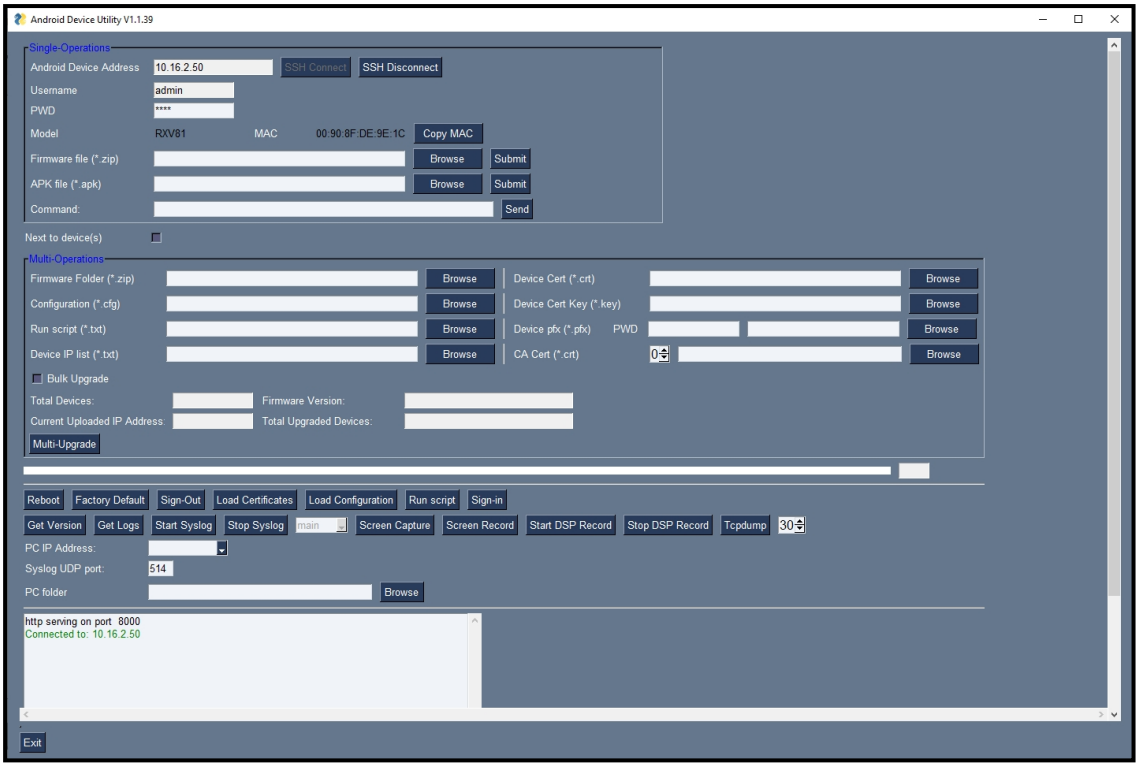
- dmesg.log
- dumpstate-c470hd-1.18.117_58793-41-undated-dumpstate_log-3458.txt
- dumpstate-c470hd-1.18.117_58793-41-undated.txt
- dumpstate-stats.txt
- logcat.log

Get Logs

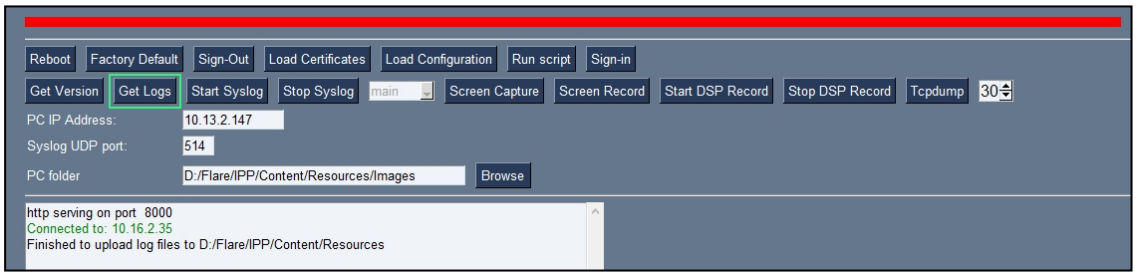
Network administrators can get bug report logs, including a logcat file and a configuration file, to expedite debugging.

➢ To get logs:

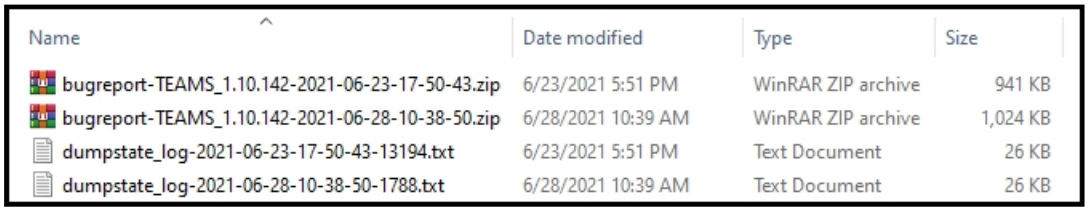
1. In the AudioCodes Android Device Utility (seeAndroid Device Utility on page 144 for more information about the application), enter the phone's IP address, click **SSH Connect** and browse to a folder on the PC to which to send the information.



2. Click **Get Logs**; after a short period, view a 'Finished' indication in the results pane.



3. Open the folder on the PC to which you commanded the application to send the information.



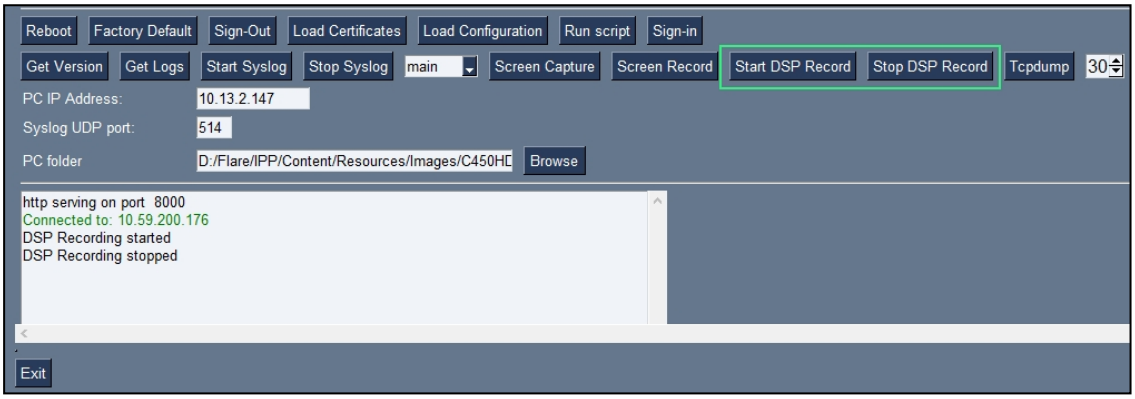
4. Unzip the zipped files and open the txt files to view the report.

Activate and Deactivate DSP Recording

Network administrators can activate DSP recording using AudioCodes' SSH protocol based Android Device Utility.

➢ **To activate or deactivate DSP Recording:**

1. In the AudioCodes Android Device Utility (see Android Device Utility on page 144 for more information about the application), enter the phone's IP address, click **SSH Connect** and then click the **Browse** button next to the field 'PC folder' to configure a folder on the PC to which to send the information.
2. In the 'PC IP Address' field, enter the IP address of the PC on which the utility is installed and then click the **Start DSP Record** button.
3. After a period of recording, click **Stop DSP Record**.



4. View the DSP recording in the PC folder you configured.

Network administrators can alternatively activate and deactivate a DSP recording using SSH protocol *without* the Android Device Utility, as shown next.

➢ **To activate DSP recording using SSH protocol *without* the utility, type the following at the shell prompt:**

```
setprop ac.dr_voice_enable true
setprop ac.dr_ipaddr <ip_address>
setprop ac.dr_port 50000

setprop persist.ac.dr_voice_enable true
setprop persist.ac.dr_ipaddr <local host ip address>
setprop persist.ac.dr_port <50030> //default is 50030
```

➢ **To deactivate DSP recording using SSH protocol *without* the utility, type the following at the shell prompt:**

```
setprop ac.dr_voice_enable false
```

DSP recording can be activated or deactivated on the fly without requiring the network administrator to reset the phone.

SSH based Debugging

The phone can be accessed via Secure Shell (SSH) cryptographic network protocol after the network administrator logs in (see Log in as Administrator on page 107).

SSH is by default disabled and can be enabled with Administrator permissions in the phone screen (**Device Administration** > **Debugging** > **SSH**) or via the phone's configuration file (`admin/ssh_enabled=1`).

SSH access allows administrators debugging capabilities such as:

- Get the phone's IP address (using the `ifconfig` command)
- Install the Teams APK (or any other APK)
- Pull files from the phone sdcard (using the `curl` command)

Microsoft Teams Admin Center

The Microsoft Teams Admin Center allows network administrators to troubleshoot issues encountered with the phone.

Collect Logs

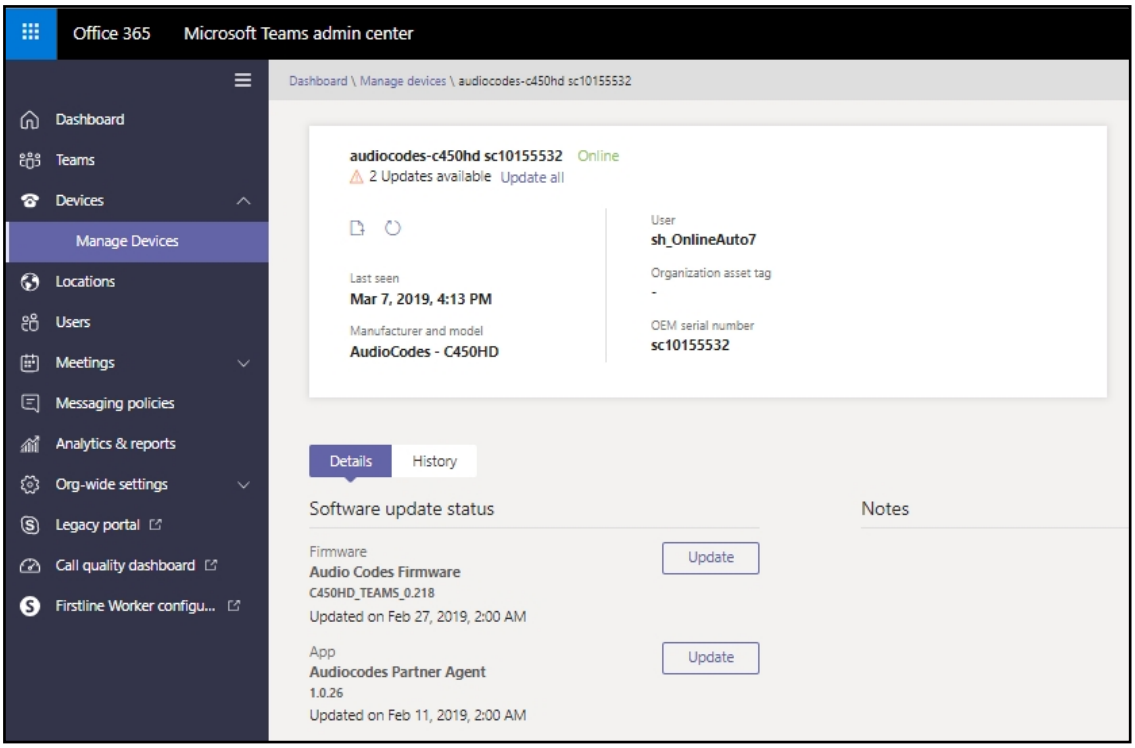
Network administrators can download *all logs* from the Microsoft Teams Admin Center (TAC). Logs that administrators can download include device diagnostics (Logcat), dumpsys, ANRs, Client Log, Call Policies File, Call Log Info File, Sky lib Log Files, Media Log Files, and CP. The logs can help debug Teams application issues and also for issues related to the device.

For details click here.

➢ **To collect logs:**

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

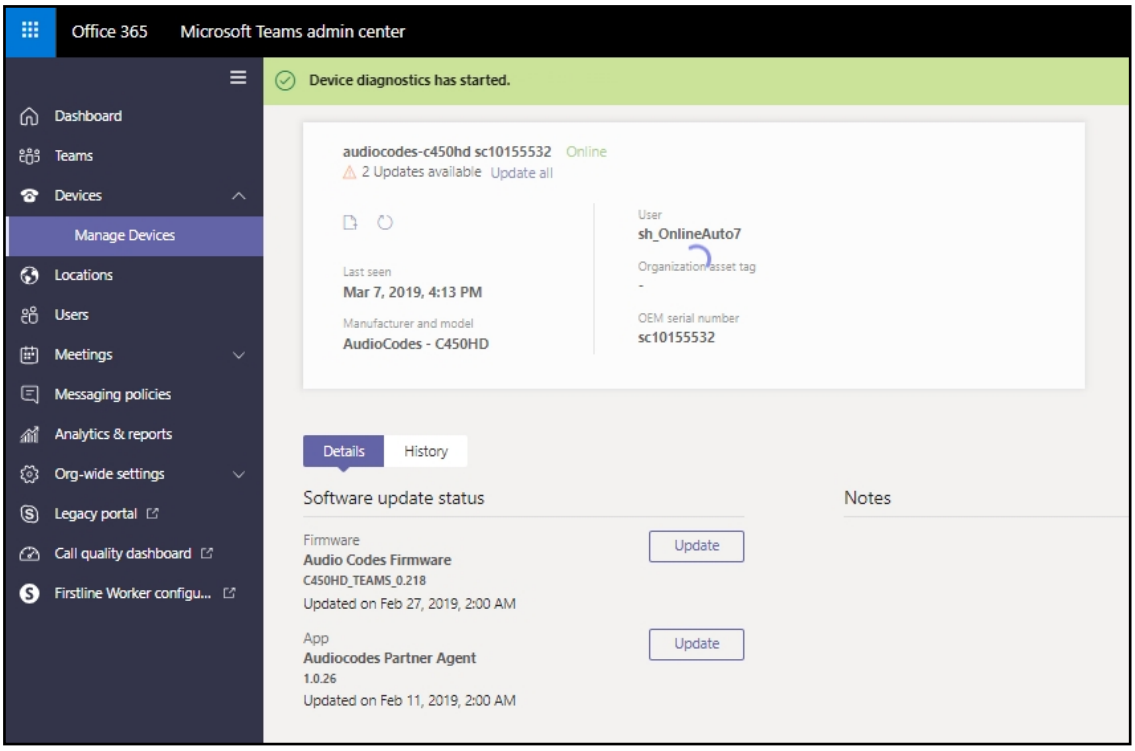
Figure 6-1: Microsoft Teams Admin Center - Diagnostics



Applies to all AudioCodes phones for Microsoft Teams even though a specific model is shown in the figures here.

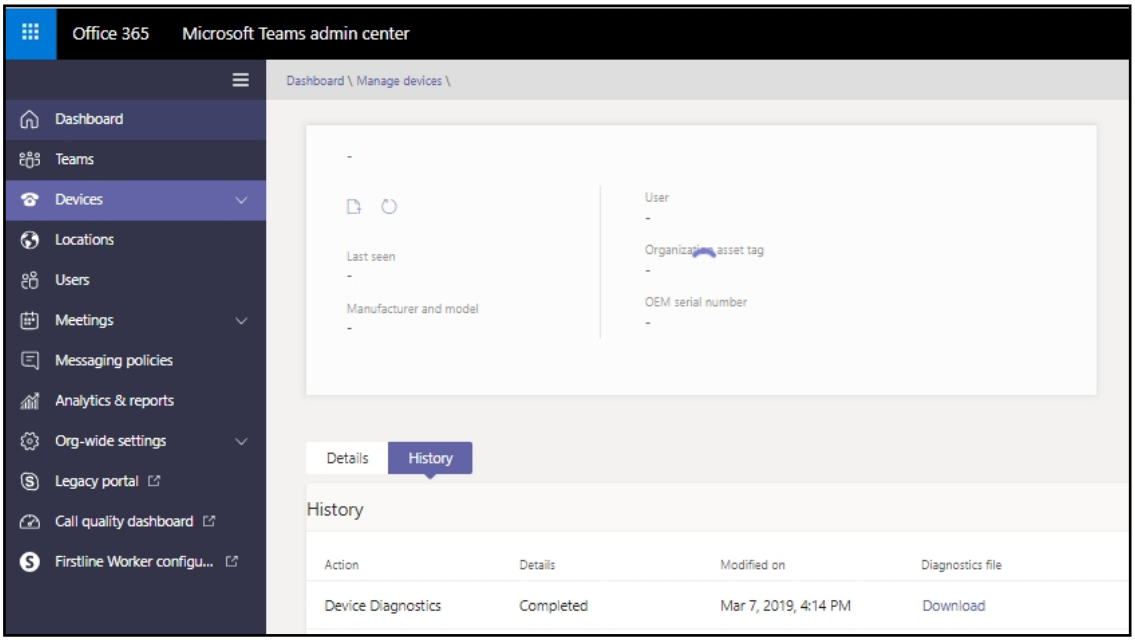
3. Click the **Diagnostics** icon and in the 'Device diagnostics' prompt that pops up, click **Proceed**; log files are retrieved from the devices and uploaded to the server.

Figure 6-2: Microsoft Teams Admin Center – Logs Upload to Server



4. Click the **History** tab.

Figure 6-3: History - Download



Click **Download** to download the logs.

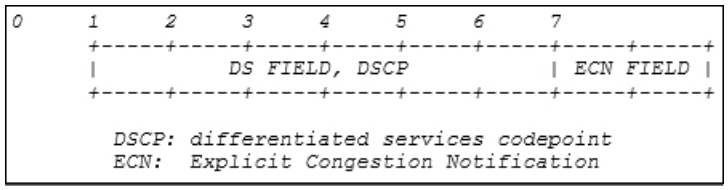
- AudioCodes Device Manager's 'Collect Logs' action also includes all information collected by Microsoft Teams Admin Center. The .zip file includes the following files:
  - ✓ Android BugReport
  - ✓ AdminAgentLogs.zip - includes logcat collected by the OVOC/Device Manager.
  - ✓ blog files (media logs)
  - ✓ Skylib-XXX.blog
  - ✓ app_process32.XXX.blog
  - ✓ config.cfg & status.cfg - Device configuration and status
  - ✓ ac_config.xml and ac_status.xml - Device configuration and status for internal use.
  - ✓ dmesg - Diagnostic messages command useful for debugging hardware-related issues.
  - ✓ SessionID_For_Company_Portal_Logs.txt (this is the CP SSDI, not the logs; the logs are sent to the OVOC / Device Manager server).
- See also the *Device Manager Administrator's Manual*.

DSCP

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

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

Figure 6-4: DS Field, DSCP



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

See also Microsoft's website for more information.

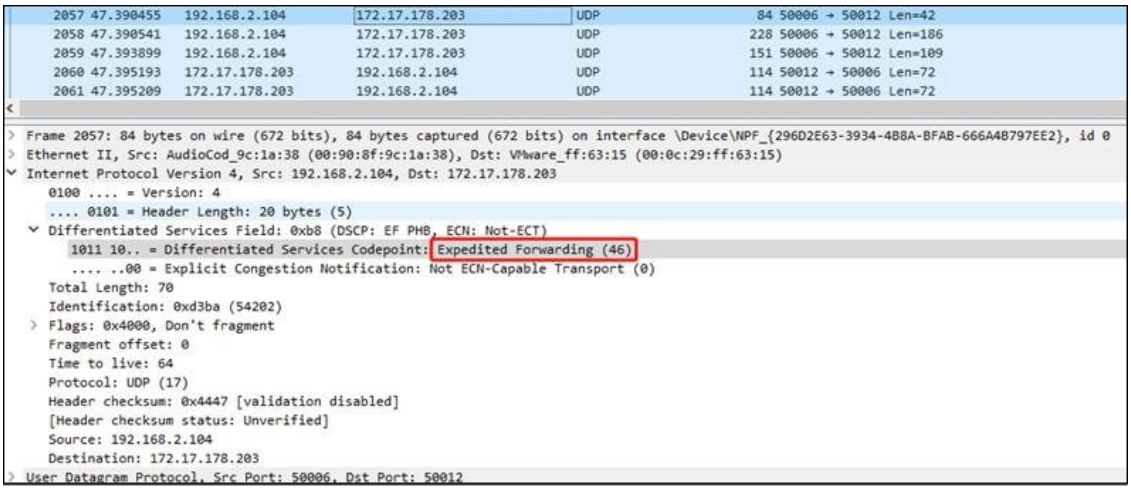
The DSCP value can be adjusted *on the server*; it cannot be adjusted on the client. See the figures below for recommended values.

Figure 6-5: Recommended Values

Table 1. Recommended initial port ranges

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

Figure 6-6: Audio



Additional Debugging Options

- Export Logs to USB when Phone is in Recovery Mode below
- Encounter an ANR Error - Core Dump below
- Retrieve Bug Report Automatically Produced if 'Boot Reason' is FATAL or PANIC on the next page

Export Logs to USB when Phone is in Recovery Mode

This feature empowers users to seamlessly save logs while their phone is in recovery mode. In Android recovery mode, the system automatically mounts a partition, enabling users to connect a USB stick. By simply clicking the 'Export logs to USB disk' option, all logs are efficiently copied to the USB stick, providing a convenient and reliable method for log management during recovery procedures.

Encounter an ANR Error - Core Dump

If an Application Not Responding (ANR) error / core dump occurs, logging capability helps administrators ensure a high level of customer experience (CX). The logging feature automatically stores the logs (as a Bugreport file) when an application or service in Android crashes (including FATAL/PANIC) or gets stuck. When this happens, it takes the logs from the event and saves them under **sdcard/logs**.

When a device does not encounter an ANR error / core dump, log files don't appear.

- The feature is available for all devices running Android 10 or Android 12 operating system.
- Only the last 10 logs are stored on the device. If this number is exceeded, the previous logs are deleted.

Retrieve Bug Report Automatically Produced if 'Boot Reason' is FATAL or PANIC

A bug report is automatically produced if the 'boot reason' after the device is booted up is **FATAL** or **PANIC** (or anything that falls in the FATAL category). The trigger is included in the bug report.

The report is stored in the **sdcard/logs** folder.

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

©2026 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, AudioCodes One Voice, AudioCodes Meeting Insights, and AudioCodes Room Experience are trademarks or registered trademarks of AudioCodes Limited. All other products or trademarks are property of their respective owners. Product specifications are subject to change without notice.

Document #: LTRT-13479