User's and Administrator's Manual

AudioCodes 400HD IP Phone Series

C430HD IP Phones

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: October-21-2025

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
C430HD 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
13456	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
13462	Updated to Ver. 2.7.M2; AudioCodes Smart button configure for redial. Dim screen functionality updated; 802.1x authentication parameters added

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 Overview 1

Specifications 1
Migration to Android Open Source Project (AOSP) 5
Allowing URLs, Ports (Security) 5
Security Guidelines for Android-based Native Teams Devices 6

2 Setting up the Phone 7

Unpacking 7
Device Description 8
Front View 8
Rear View 12
Cabling 13
Mounting the Phone 13
Before Using AudioCodes Devices 13

3 Starting up 14

Accessibility 14
Configuring Device Settings 15
Configuring VLAN via DHCP Option when CDP-LLDP isn't Allowed 30
Restoring the Phone to Default Settings 31
Performing a Hard Restore 31
Performing a Soft Restore 32
Performing User Data Reset 33
Recovery Mode 33
Locking and Unlocking the Phone 33
Automatic Lock 33
Unlock 33

4 Teams Application 35

Signing In 35
Multi-Cloud Sign-in 39
Remote Provisioning and Sign-in from Teams admin center 40
Getting Acquainted with the Phone Screen 44
Setting Status 45
Changing Presence Status 46
Enabling Power Saving 47
Configuring Teams Application Settings 48
Using the People Screen 51
Accessing Voicemail 51
Using Audio Devices 52
Transferring Calls and Meetings across Devices 53
Signing Out 53

5 Performing Teams Call Operations 55

Making a Call 55
Dialing a Missed Call 57
Select to Dial 57
Transferring a Call 57
Making an Emergency Call 57
Answering Calls 58
Ending an Established Call 58
Managing Calls 59
Paging to a Group of Phones (Multicast) 59
Transferring a Call to Frequent Contacts 61
Transferring a Call to Work Voicemail 62
Viewing and Playing Voicemail Messages 62
Rejecting an Incoming Call, Sending it Directly to Voicemail 62
Adjusting Volume 62
Adjusting Ring Volume 63
Adjusting Tones Volume 63
Adjusting Handset Volume 63
Adjusting Speaker Volume 63
Adjusting Headset Volume 64
Playing Incoming Call Ringing through USB Headset 64
Assigning a Line Key for Speed Dial or Features 64
6 Performing Administrator-Related Operations 70
Setting up an E911 Emergency Location using TAC 70
Setting up Automatic Provisioning 75
Enabling Users to Make Calls even if Teams is Unavailable 76
Applying a Partial Configuration Profile 79
Configuring an Option to Force Users to Change their Device Lock PIN 79
Configuring Minimum and Maximum Ringer Volumes via the Phone's Configuration File 81
Updating Phone Firmware Manually 82
Loading Certificates to Phones 85
AudioCodes Android Device Utility 85
Certificate Enrollment using SCEP 87
Manually Performing Recovery Operations 89
Enrolling a Device with Intune Policies 90
Creating a Dynamic Group 90
Creating an Exclusion Group 90
Removing Devices from Intune admin center 91
Updating Microsoft Teams Devices Remotely 94
Defining Password Complexity 94
Disabling a Device's USB Port 95
Disabling the Phone's Speaker Hard Key 96
Enabling AudioCodes Smart Button for Redial Functionality 97
Managing Phones with the Device Manager 98

Configuring a Periodic Provisioning Cycle 99
Managing Devices with HTTPS 99
Supported Parameters 100
Configuring Time Zone on Teams Devices 101
Configuring QoS on PC Port 102
Configuring Admin Login Timeout 102
Monitoring Phone Process Statuses 103
7 Troubleshooting 104
DSCP 104
Users 105
Exporting Logs to USB when Phone is in Recovery Mode 106
Network Administrators 106
Android Device Utility 106
Capturing the Phone Screen 108
Running Tcpdump 109
Getting Information about Phones 110
Remote Logging (Syslog) 111
Getting Diagnostics 113
Getting Logs 114
Activating DSP Recording 115
Deactivating DSP Recording 116
SSH 117
Getting the Phone IP Address 118
Installing the APK using SSH 118
Updating Phones using SSH Commands 118
Microsoft Teams Admin Center 120
Collecting Logs 120
Getting Audio Debug Recording Logs 122
Collecting Media Logs (*.blog) from the Phone 123
Encountering an ANR Error - Core Dump 123
Retrieving Bug Report Automatically Produced if 'Boot Reason' is FATAL or PANIC 123
Return to Previous Version 124

1 Overview

The AudioCodes C430HD IP phones are Microsoft Teams-native entry level/common area phones designed to support the next generation of enterprise collaboration technologies with a large LCD screen and full UC integration for the Native Microsoft Teams Online market.

The phones can be managed by the Microsoft Teams & Skype for Business Admin Center. For more information, see here.

Feature highlights:

- Native support for Microsoft Teams
- Color screen 4.3": Graphic, 480x272 resolution
- Multi-lingual support
- Full duplex speakerphone and headset connectivity
- Dual GbE support
- USB headset support
- PoE or external power supply
- Calendar and click-to-join support
- 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.

Specifications

The following table summarizes the phone's specifications.

Table 1-1: Specifications

Feature	Details
Media Processing	■ Voice Coders: G.711, G.729, G.722, SILK, Opus ■ Acoustic Echo Cancelation: G.168-2004 compliant, 64-msec tail length ■ Adaptive Jitter Buffer ■ Voice Activity Detection ■ Comfort Noise Generation ■ Packet Lost Concealment ■ RTP/RTCP Packetization (RFC 3550, RFC 3551), SRTP (RFC 3711)
Microsoft Teams phones feature set	■ Authentication (Sign in with user credentials; Sign in using PC/Smartphone; Modern Authentication; Phone lock/unlock) ■ Calling (Incoming/Outgoing P2P calls; In-call controls via UI (Mute, hold/resume, transfer, end call); PSTN calls; Visual Voicemail; 911 support ■ Calendar and Presence (roadmap feature) (Calendar Access ; Presence Integration; Exchange Calendar Integration; Contact Picture Integration; Corporate Directory Access)
Configuration and Management	■ Teams admin center (TAC) ■ OVOC / Device Manager
Debugging Tools	■ AudioCodes' Android Device Utility (see Android Device Utility on page 106) ■ Log upload to Microsoft server (certification for 3rd party Skype for Business clients) ■ Remote logging via Syslog ■ SSH Access ■ Capturing the phone screen ■ TCPdump ■ Audio Debug recording logs ■ Media logs (*.blog) ■ Remote Packet Capture network sniffer application
Localization	■ Multi-lingual support; the language pack list is not yet final and is

Feature	Details
Support	subject to modification.
Hardware	■ Graphic 4.3" color screen, 480x272 resolution ■ Wired connectivity: ✓ Two RJ-45 [Gigabit Ethernet (GbE)] (10/100/1000BaseT Ethernet) ports: LAN and PC port ✓ USB port for USB headset. Note that **C430HD-R** (**TEAMS-C430HD-R**) is a PoE Class 2 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. ✓ RJ-11 interface ■ Power: ✓ 12V DC jack ✓ Power supply AC 100 ~ 240V ✓ PoE Class 2: IEEE802.3af (optional) ■ Keys: ✓ Illuminated VOICE MAIL message hotkey ✓ 4-way navigation button with OK key ✓ MENU ✓ HOLD ✓ Illuminated MUTE hotkey ✓ TRANSFER ✓ VOLUME control key ✓ Illuminated HEADSET hotkey ✓ Illuminated SPEAKER hotkey ✓ BACK ✓ CONTACTS ✓ Teams home key

Table 1-2: Teams Features Supported by theC430HD Phone

Teams Feature	C430HD
Call Transfer	√
Consultative Transfer	√
Escalate P2P call to Teams Meeting / Conference (Add-hoc Conference)	√
Call Queue	√
Contacts / People	√
Speed Dials dedicated keys	√
Visual VM (when C430HD is used as a CAP, it's supported only after enabling 'Advanced calling')	√
Calendar	Not supported
Click to join meeting	Not supported
Hot Desking	√
Common Area Phone (CAP)	√
CAP: Advanced calling	√
CAP: Voice Mail (only applicable when 'CAP: Advanced calling' is enabled)	√
Music on Hold (MoH)	√
Call Forward via phone UI	√
Teams self presence publish	√
Teams co-workers presence display	√
Call Park	√
Favorites list for speed dial	√
Delegation	Supported but configured from Teams client
Meet Now	Not supported

Teams Feature	C430HD
Better Together (over wireless)	Not supported
AudioCodes Device Duo	Roadmap
Survivable Branch Appliance (SBA)	√
Talkback	Not supported

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.

An *AOSP Migration Guide* for Android AOSP Management for Microsoft Teams Android devices can now be obtained on Microsoft Learn here.

The guide provides customers with detailed instructions and best practices for a smooth migration. It also shows 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.

Allowing URLs, Ports (Security)

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.

Table 1-3: 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	Android NTP	123	UDP	-

Server Role	Service Name	Port	Protocol	Notes
timeserver				
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

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

2 Setting up the Phone

The following instructions show how to set up the phone.

Unpacking

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).

Device Description

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

Front View

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

Figure 2-1: Front View

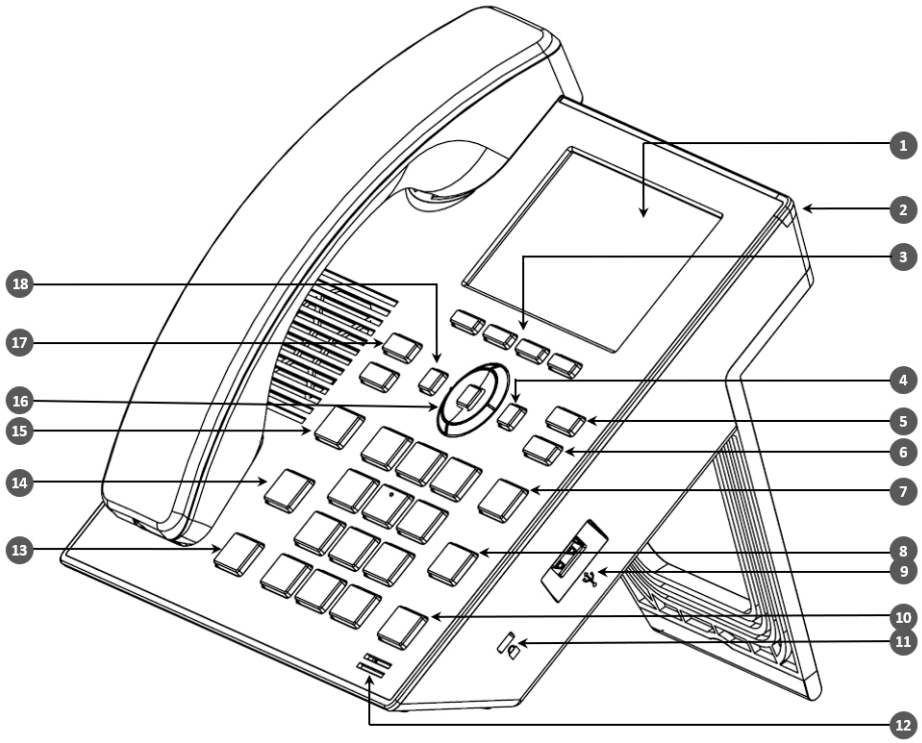


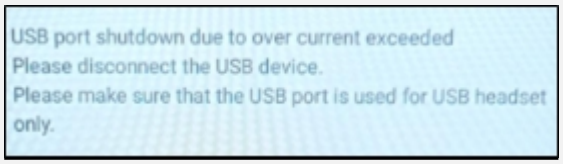
Table 2-1: Font View Description

Item #	Label Name	Description
1	LCD screen	Liquid Crystal Display interactive screen which displays calling information.
2	Ring LED	Indicates phone status: ■ Green: Idle state ■ Flashing red: Incoming call (ringing) ■ Red: Answered call

Item #	Label Name	Description
3	Four softkeys	Enable the user to open (from left to right) the Calls menu, the Voicemail menu, the Contacts menu and the Lock menu.
4	Menu	Opens and provides access to the phone's menu.
5	Voicemail	Retrieves voicemail messages.
6	CONTACTS	Accesses the People screen.
7	Smart Button 	General purpose key. Can be configured to function as a redial button (see Enabling AudioCodes Smart Button for Redial Functionality on page 97).
8	TRANSFER	Transfers a call to another party.
9	USB port	For a USB headset. See also the note below.
10	HOLD	Places an active call on hold.
11	Kensington lock	Allows locking the device.
12	Microphone	Allows talking and listening. The network administrator can disable it if necessary.
13	Speaker	Activates the speaker, allowing a hands-free conversation.

Item #	Label Name	Description
14	Headset	Activates a call using an external headset.
15	Mute	Mutes a call.
16	Navigation Control / OK	■ Press the button's upper rim to scroll up menus / items. ■ Press the button's lower rim to scroll down. ■ Press the button's left or right rim to move the cursor left or right (when editing a contact number for example). ■ Press **OK** to select a menu/item/option.
17	▲ VOL ▼ VOL	Increases or decreases the volume of the handset, headset, speaker, ring tone and call progress tones.
18	'Back' key	Returns you back to the previous screen.

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.



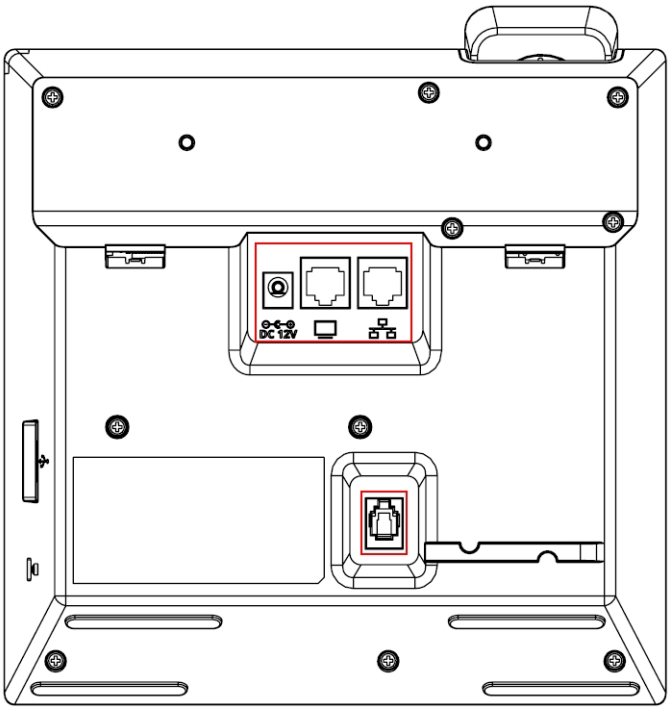


Navigate to menus and select menu items by:

- Pressing the rim of the control button (upper, lower, left or right)
- Pressing the **OK** key on the control button

Rear View

The ports located on the rear of the phone are described from right to left in the table below.



Ports (from right to left)	Description
	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).
	RJ-45 port to connect the phone to a PC (10/100/1000 Mbps downlink).
DC12V	12V DC power jack that connects to the AC power adapter.
AUX	[RJ-11 port] Used as a serial console port to access the phone's terminal.
(Not seen in the image | Located at the bottom of the device)	RJ-9 port used to connect the phone’s handset.

Cabling

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).



Please use only the supplied Ethernet (LAN) cable, which is shorter than 3 meters, to connect the IP Phone's LAN port to the PC.

Mounting the Phone

You can desktop or wall mount the phone. For detailed information on how to mount 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).

To a view a video showing *the principle* of how to mount an AudioCodes IP phone, click here. The principle is the same across all AudioCodes IP phone models.

Before Using AudioCodes Devices

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:**

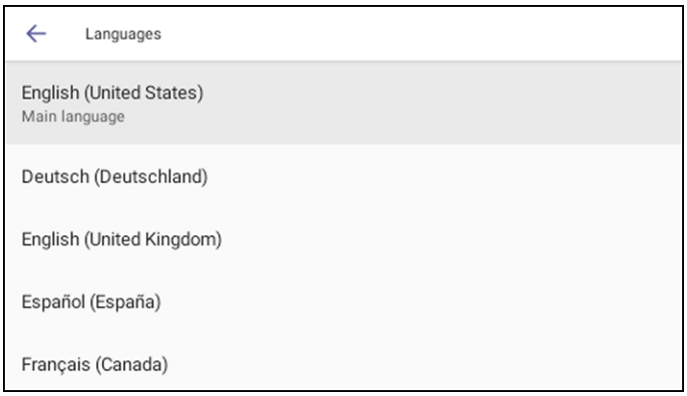
1. Disconnect all cables.
2. Spray onto a clean, dry, microfiber duster a medicinal isopropyl alcohol and water solution of 70:30. Don't oversaturate the duster. If it's wet, squeeze it out.
3. Lightly wipe the screen of the device.
4. Wait for the screen to dry before reconnecting cables.

3 Starting up

Here's how to start up the phone.

➢ **To start up:**

1. Connect the phone to the network (or reset it); the language selection screen is displayed by default.



2. Select the language of your choice and then configure device settings to suit specific requirements.

It will be necessary to repeat this only if the phone is restored to default settings.

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**

  Teams phones support high contrast display modes to improve readability for users with visual impairments.

- **Large Touchscreen Displays**

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

- **Hard Button Mapping**

  Phones support customizable hard button mapping, which can be helpful for users who rely on tactile feedback.

- **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.

- **Camera Shutter and Mute Switch**

  For privacy and accessibility, some models include physical camera shutters and microphone mute switches.

- **Localization and Language Support**

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

- **Device Duo Mode**

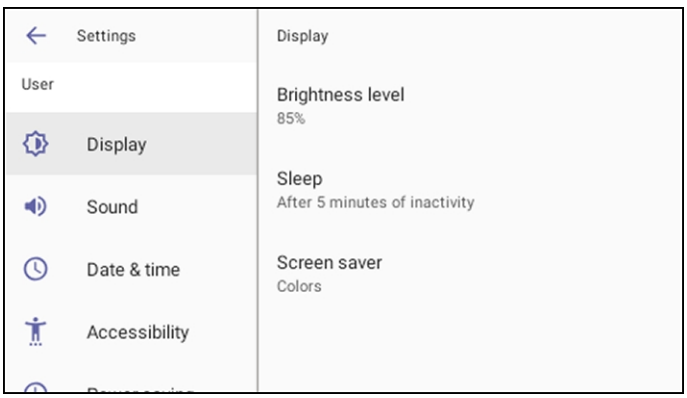
  This feature allows the phone to act as a smart audio device for PC-based UC apps, offering flexibility for users who prefer or require alternative input/output setups.

Configuring 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.

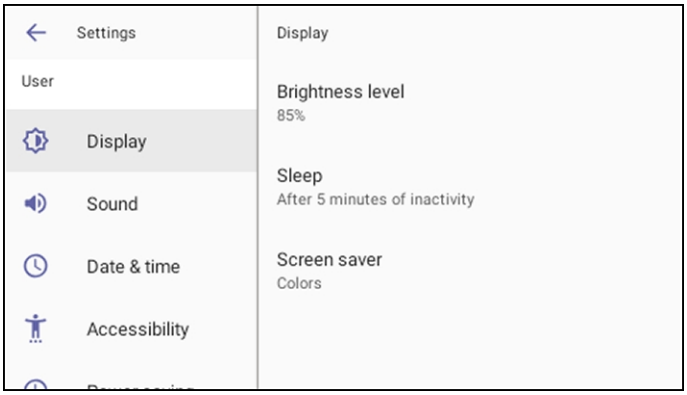
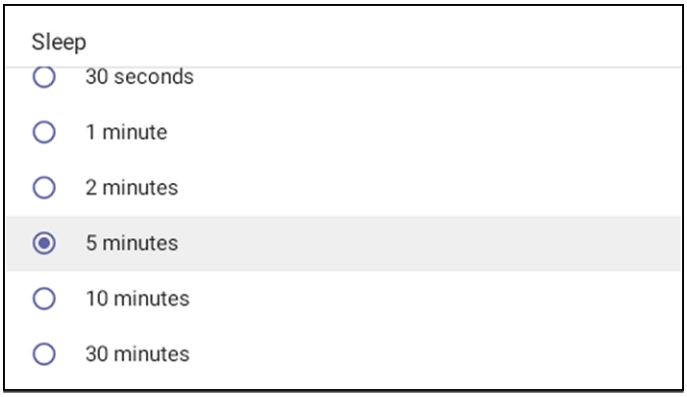
➢ To access device settings:

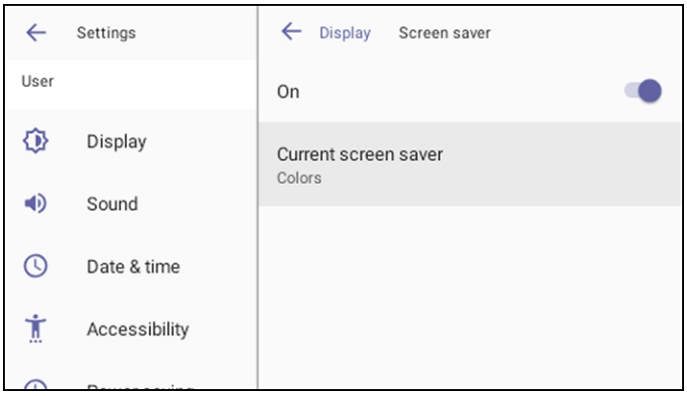
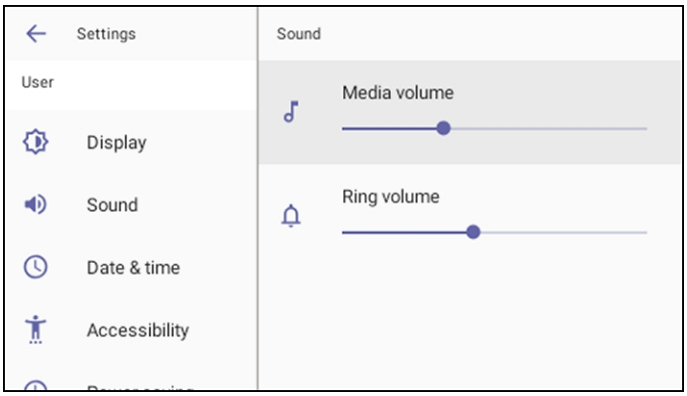
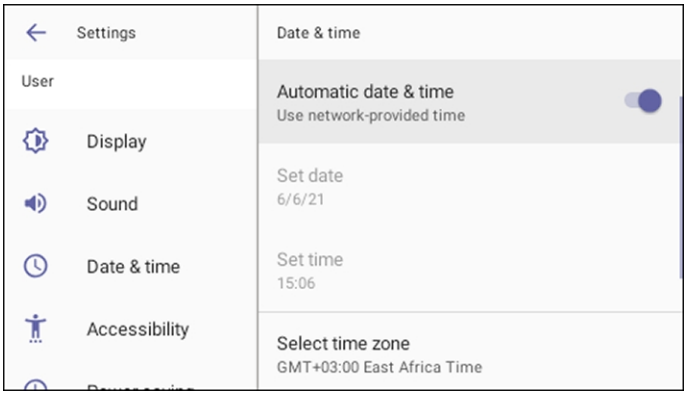
1. In the home screen, select , select **Settings** and then press the **Settings** softkey.

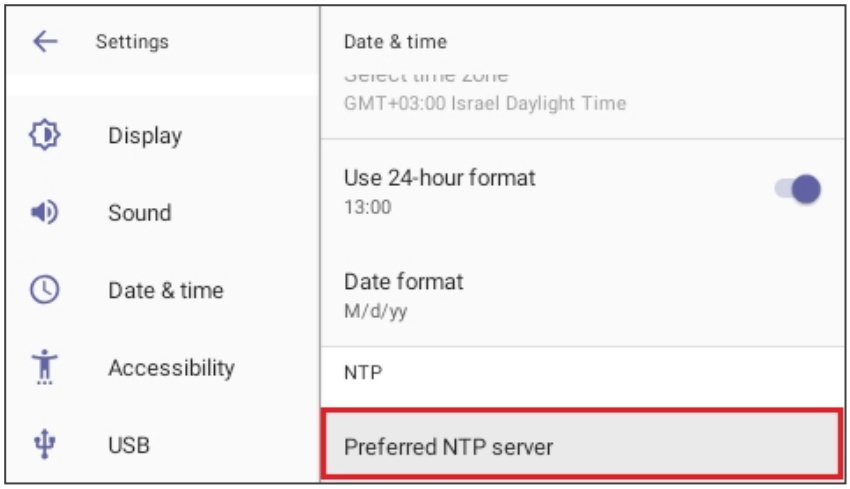
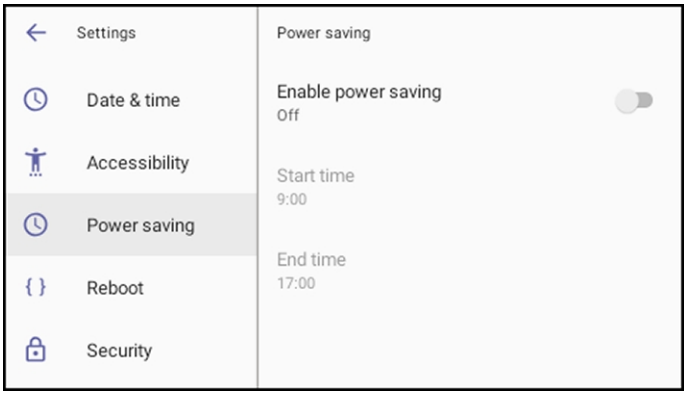


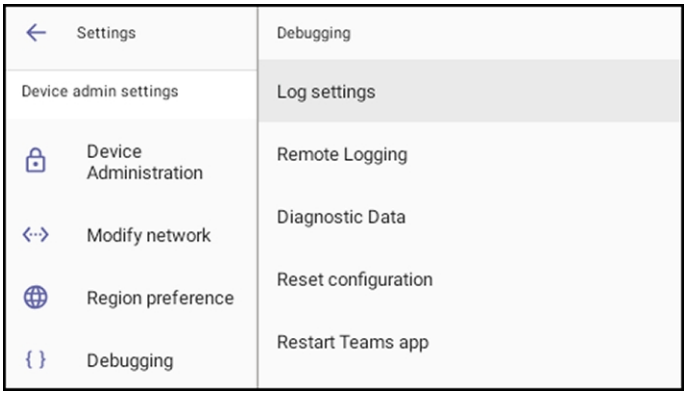
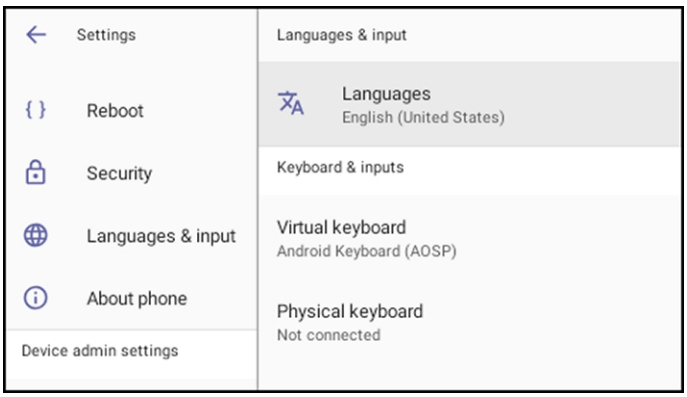
2. View the settings under 'User'. Select a setting to open it. Use the table following as reference. [To view settings related to the network administrator, scroll down and open 'Device Administration'].

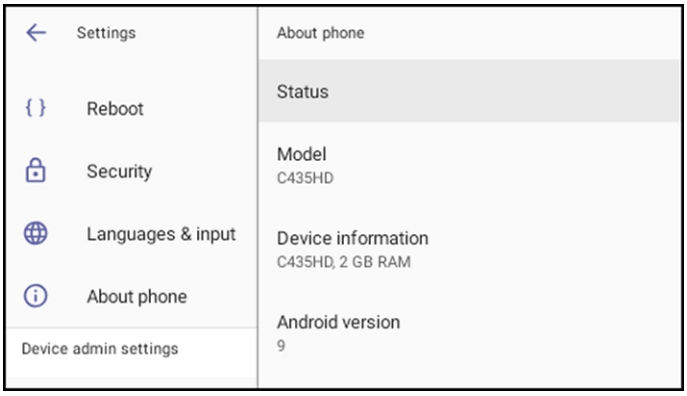
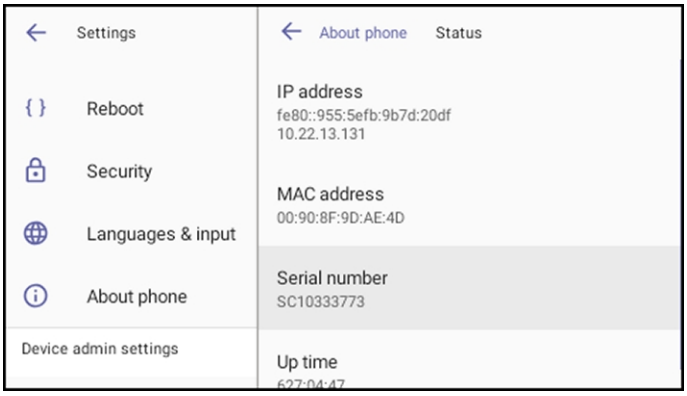
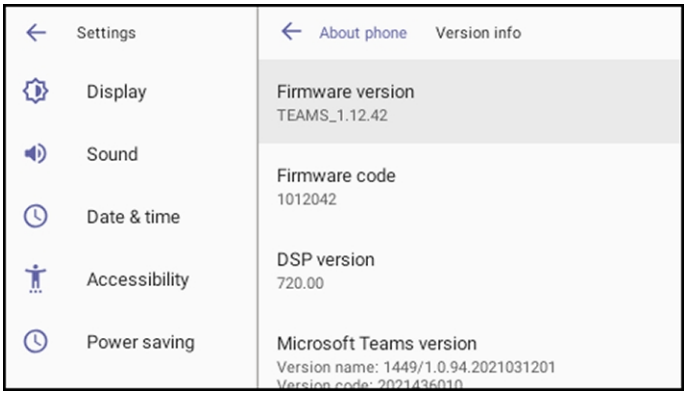
Table 3-1: Device Settings

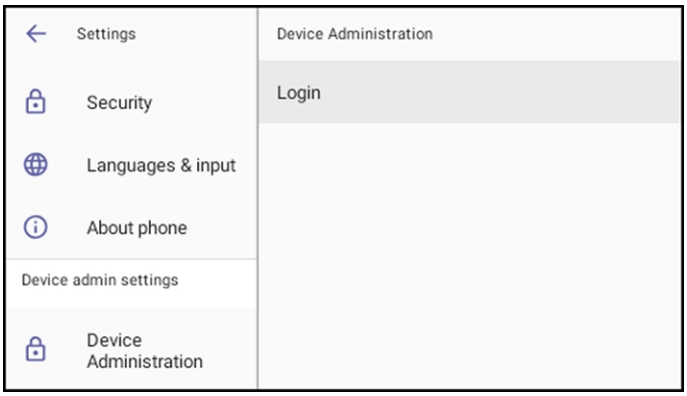
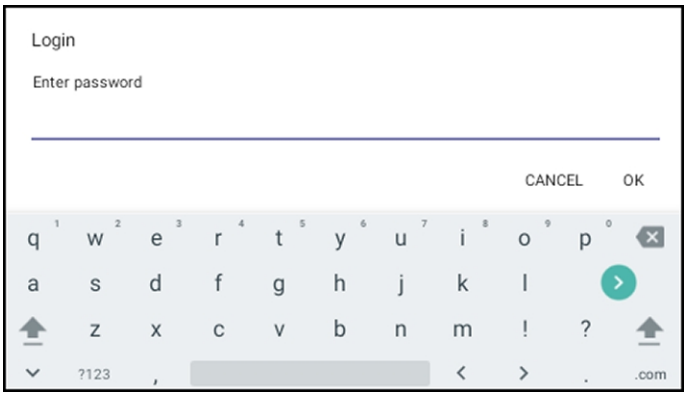
Setting	Description
User	
Display	Opens the 'Display' screen [Brightness level].  The phone's screen supports different brightness levels. Choose the level that suits your requirements. ■ Sleep  ■ Screen saver

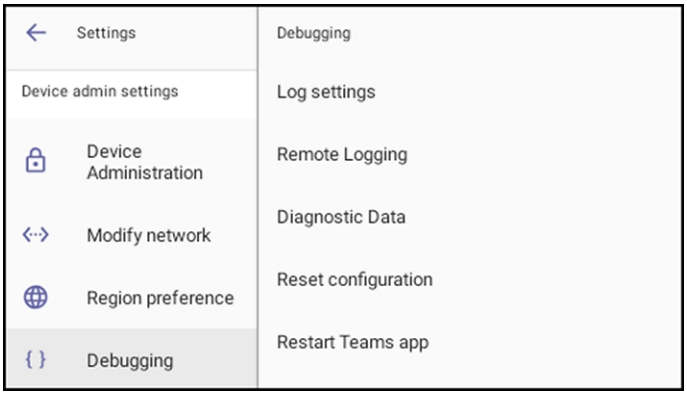
Setting	Description
	
Sound	Allows you to customize phone volume for a friendlier user experience. **Ring volume at n%** 
Date & time	Date and time are automatically retrieved from the deployed Network Time Protocol (NTP) server.  Use 24-hour format [Allows you to select the Time format] Also supported 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.

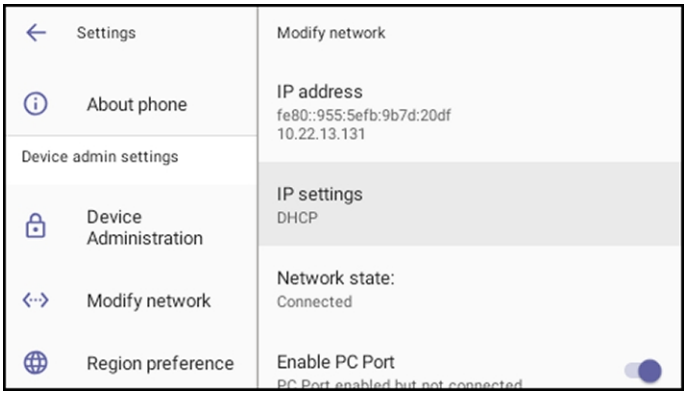
Setting	Description
NTP Preferred NTP server	Admins can use this parameter to *manually* define the NTP server, to comply with enterprise security requirements if those requirements preclude using DHCP Option 42. Manual configuration takes precedence over DHCP Option 42 and the time servers. Two ways to manually define the NTP server are available: ■ Admins can define it in the phone's GUI.  ■ Admins can alternatively use the newly added parameter 'date_time/ntp/server_address' in the phone's .cfg configuration file. See also under Signing In on page 35.
Power Saving	Allows users to contribute to power saving in the enterprise.  Enable power saving Start time [The device consumes minimal energy before the user arrives at the office] End time [The device consumes minimal energy after the user leaves the office]
Debugging	Enables users to reboot the device.

Setting	Description
	 Log in as Administrator for more debugging settings to be available.
Security	Helps secure the enterprise telephony network against breaches. Screen lock [The phone automatically locks after a configured period to secure it against unwanted use. If left unattended for 10 minutes (default), it automatically locks and is inaccessible to anyone who doesn't know its lock code.] Make passwords available See 'Lock Screen & PIN' under Configuring Teams Application Settings on page 48
Languages & input	Allows users to customize inputting to suit personal requirements. 
About	Provides users with device information.

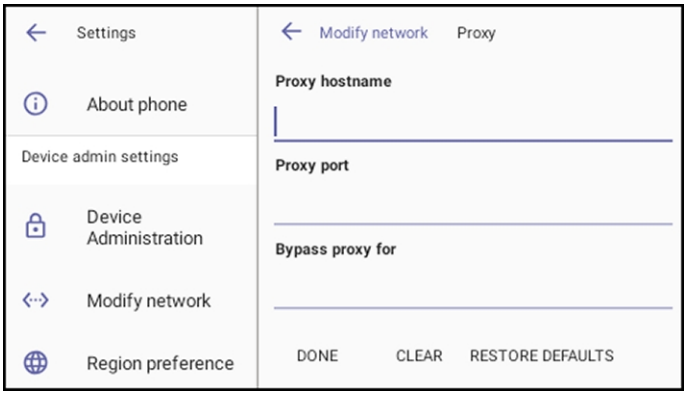
Setting	Description
	 To determine the device's IP address, select the 'Status' option.  To get information about the version, select 'Version info'.  To get information about the Android version, select 'Android version'.

Setting	Description
	
Device Administration	
Device administration	Allows the user to log in as Administrator, necessary for some of the debugging options. It is password protected. Default password: 1234 (or 1111 in early versions). After logging in as an Administrator, the user can log out | change password.  Select **Login** and then in the Login screen that opens, select the 'Enter password' field and use the virtual keyboard to enter the password (**1234** or **1111**). 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. 

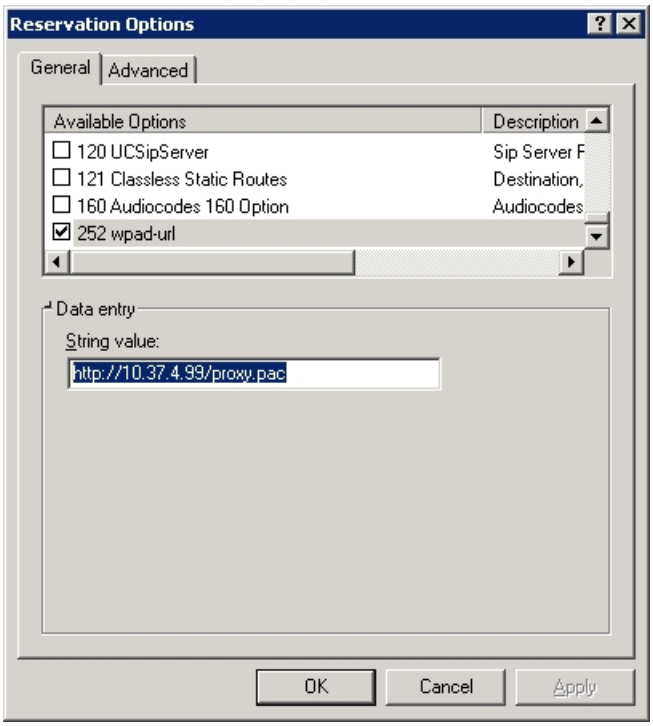
Setting	Description
	 • The phone support a strong password check in order to log in as Administrator. The feature strengthens security. Note that the default password: ✓ must be changed before accessing the device via SSH ✓ can be changed per device from the phone screen (the user first enters the default 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. • 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. The virtual keyboard is also displayed when the network administrator needs to enter an IP address to debug, or when they need to enter their PIN lock for the security tab. After logging in, scroll down in the Settings screen to the section 'Device Administration'. 
Modify network	Enables the Admin user to determine network information and to modify network settings.

Setting	Description
	 IP Address [Read Only] IP Settings [DHCP or Static IP] Network state [Read Only] Enable PC port Enable PC port mirror Proxy 802.1x Settings VLAN Settings. Allows you to configure the VLAN mode **Manual**, **CDP only** or **LLDP only**. Note that **LLDP** switch information is retrieved (for location purposes) when 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 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 select **Modify network**. b. Select the **Proxy** option and then configure the proxy host name and port:

Setting	Description



- **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.

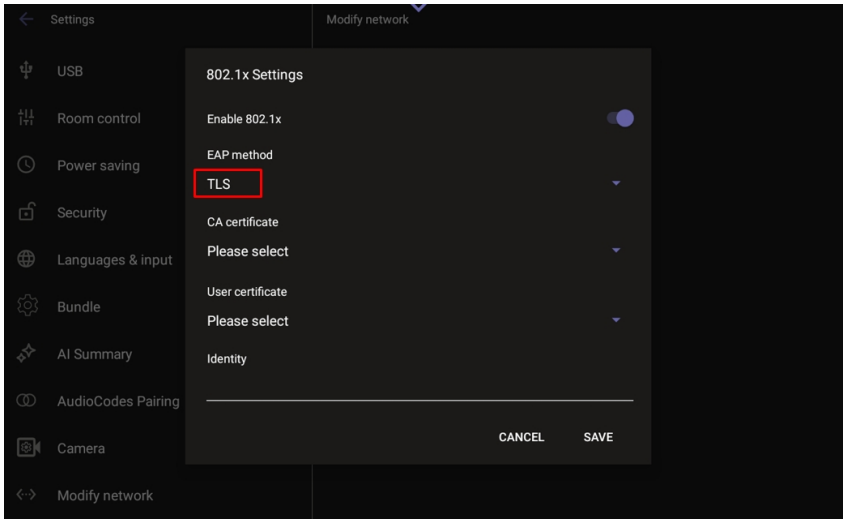
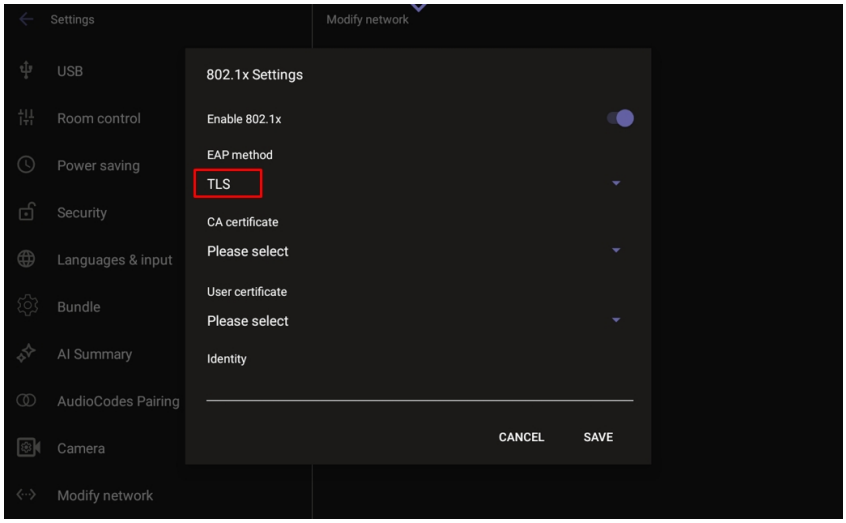
Example of a basic PAC file:

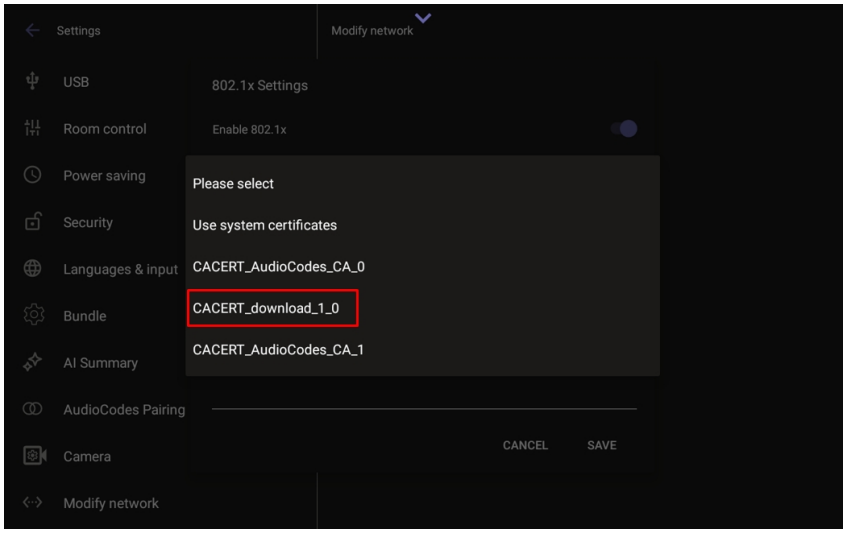
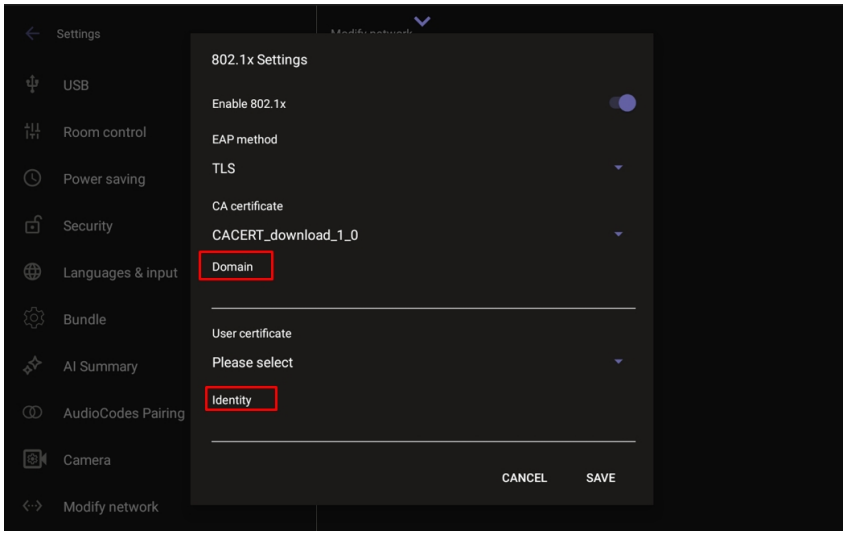
```
function FindProxyForURL(url, host)
{
return "PROXY 10.13.2.40:3128";
```

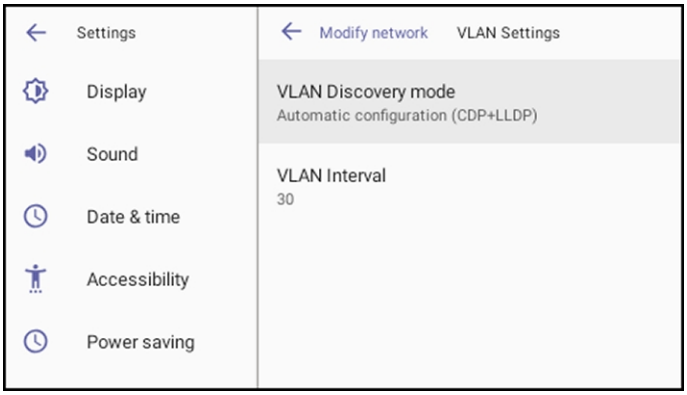
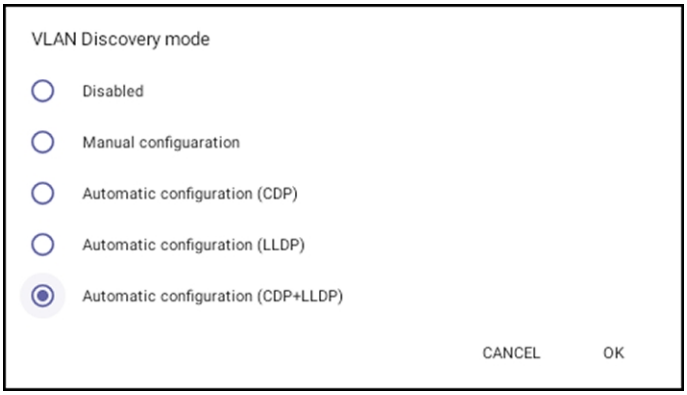
Setting	Description

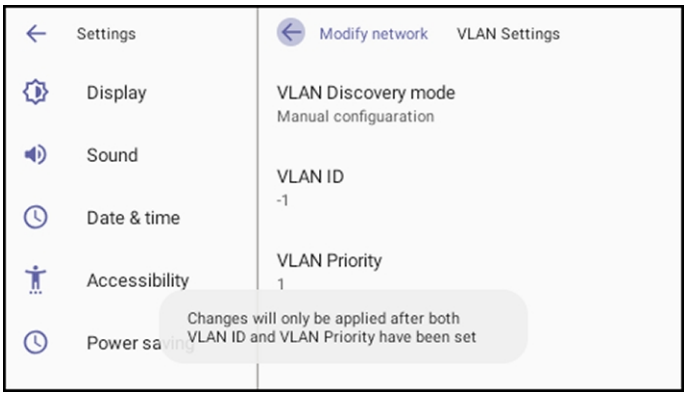
	}
	If the enterprise features a proxy server that requires user authentication, the network administrator can use the PAC file and DHCP Option 252 to configure it. Alternatively, the administrator can configure it using the following parameters:
	`http_client/fwd_proxy/ip=0.0.0.0`
	`http_client/fwd_proxy/password=`
	`http_client/fwd_proxy/port=8080`
	`http_client/fwd_proxy/username=`

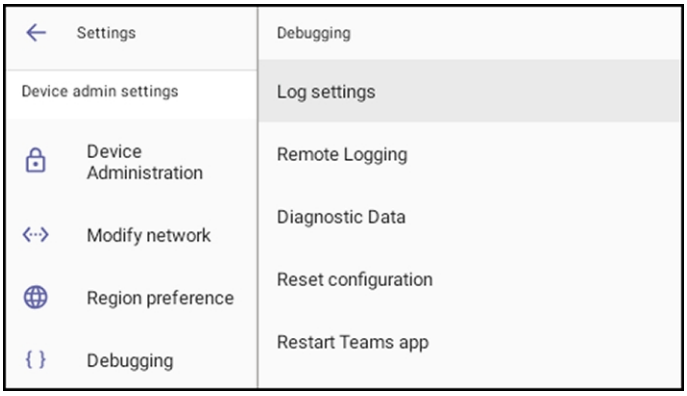
802.1x Settings	802.1x Authentication is the IEEE Standard for Port-based Network Access Control (PNAC). See https://1.ieee802.org/security/802-1x/ for more information.
	
	Instead of performing the following steps, 802.1x Authentication can be enabled and predefined via provisioning, by setting the 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 Admin, go to 'Modify Network' screen, access the 802.1x Settings screen.
	
	
	2. Tap **Enable 802.1x** toggle switch and then tap **Save**.
	3. Once enabled - the admin needs to choose the security method and strength. Commonly used is EAP-TLS

Setting	Description
	 4. Next is to choose which certificates to use - a. the device can use the system certificates  b. Or certificates that has been loaded by the admin - which will look as follows -

Setting	Description
	 5. After choosing which certificate file to use, the admin needs to set the Identity and the Domain the device is intended to enter -  6. Tap **Save** after finished defining all the above. 7. From the 'EAP method' drop-down, select 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

Setting	Description
	✓ root certificate (not required for every method) ✓ device certificate (not required for every method) 9. Select the **Save** softkey The 802.1x settings are not only available via the phone screen, they're also supported in the device Configuration File, enabling network administrator's 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	Select the menu option **VLAN Settings**.  Select **VLAN Discovery mode**.  ■ Cisco Discovery Protocol (**CDP**) is a Cisco proprietary Data Link Layer protocol ■ Link Layer Discovery Protocol (**LLDP**) is a standard, layer two discovery protocol

Setting	Description
	Select the mode you require and then select **OK**. If you select **Manual configuration**, this screen opens:  Select **VLAN ID**.  Select **VLAN Priority**. 
Debugging	Allows the Admin user to perform debugging for troubleshooting purposes. Available after logging in as Admin.

Setting	Description
	 Log settings Remote Logging (see under Remote Logging (Syslog) on page 111 for more information) Diagnostic Data (see under Getting Diagnostics on page 113 for more information) Reset configuration (see here for more information) User data reset Restart Teams app Company portal login Debug Recording (for Media/DSP debugging) (see under Remote Logging (Syslog) on page 111 for more information) Erase all data (factory reset) (the equivalent of restore to defaults; including logout and device reboot) Screen Capture. By default, this setting is enabled. If it's disabled, the phone won't allow its screens to be captured.

Configuring VLAN via DHCP Option when CDP-LLDP isn't Allowed

AudioCodes Android devices can configure VLAN via a DHCP Option when CDP/LLDP isn't 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.

Admins must configure 'VLAN Discovery Mode' to CDP/LLDP/CDP+LLDP to get VLAN via a DHCP Option. 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 LLDP/CDP 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.

DHCP Option syntax is as follows:

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

Restoring 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:

- Performing a Hard Restore below
- Performing a Soft Restore on the next page

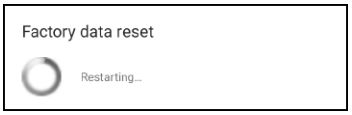
Performing a Hard Restore

You can either:

- perform a hard restore while the phone is up and running (see below)
- restore the phone's settings to their defaults when the phone is not connected (see below)

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

1. Long-press the HOLD key on the phone (more than 15 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 Signing In on page 35 for more information).

➢ **To restore the phone's settings to their defaults when the phone is not connected:**

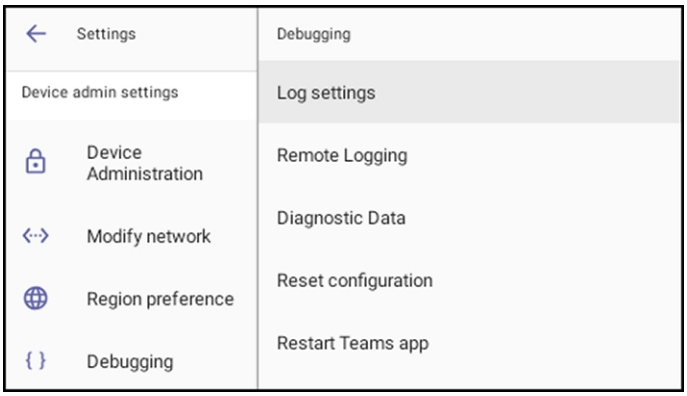
1. Press the OK + MENU keys simultaneously and keeping them pressed, unplug the power cable.
2. Plug the power cable back into the phone continuing to press the OK + MENU keys for +-5 seconds.
3. Release the OK + MENU keys; the phone' settings are restored to their defaults.

Performing a Soft Restore

Users must log in as Administrator (**Settings** > **Device Administration** > **Login** and then use the virtual keyboard to enter the default password of **1234**) in order to perform a soft restore. The soft restore is then performed in the Debugging screen.

➢ **To perform a soft restore:**

1. After logging in as Administrator, you'll have Admin privileges to configure settings. Under Device Admin Settings, select the **Debugging** option.



2. Select the **Reset configuration** option; the device performs a restore to default factory settings.

Performing 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:**

- Navigate to **Device administration** > **Debugging** > **User data reset**.

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

Recovery Mode

If a phone goes into recovery mode, you can boot it using its hard keys as shown in Performing a Hard Restore on page 31.

Locking and Unlocking the Phone

As a security precaution, the phone can be locked and unlocked. The feature includes:

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

Automatic Lock

Users can lock their phones as a security precaution. Configure the phone with any of the lock options before attempting to lock it. If an option isn't configured, the action won't function.

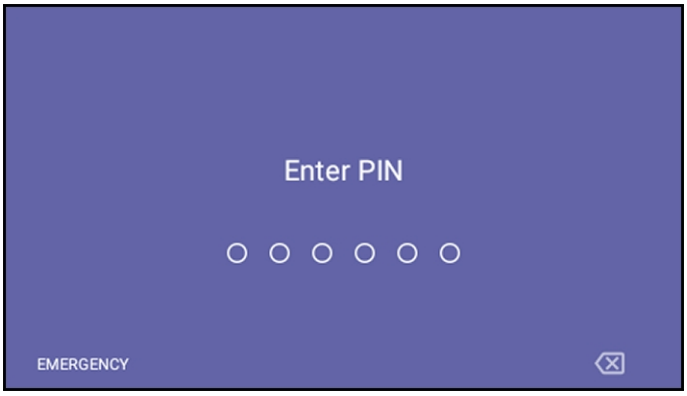
➢ **To lock the phone:**

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

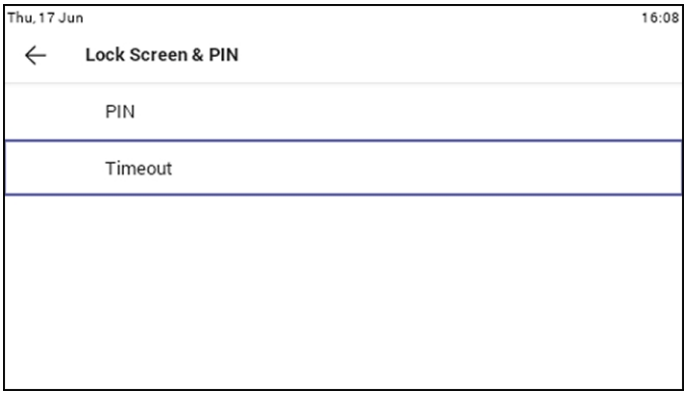
Unlock

➢ **To unlock the phone:**

1. When you interact with the phone, the screen shown in the figure below is displayed.



2. Press the hard keys on the phone to enter the PIN. When the phone detects the unlock code, it unlocks and displays the Lock Screen & PIN screen.



3. Optionally reconfigure the 'Timeout' if it's too short (or too long). Optionally redefine the PIN.

4 Teams Application

The following describes functions related to the phone's Microsoft Teams application.

Signing In



Using TeamsIPPhonePolicy, network administrators can create the following users who can then sign in to the phone:

- UserSignin: All features are available, i.e., calls, meetings and voicemail
- MeetingSignIn: Only meetings are available
- Common Area Phone (CAP) users who can sign in to the device with a CAP account (as a CAP user) using TeamsIPPhonePolicy as follows:
  - ✓ CAP SignIn (SearchOnCommonAreaPhoneMode=Enabled): The user has calling and searching capability
  - ✓ CAP SignIn (SearchOnCommonAreaPhoneMode=Disabled): The user has calling capability

Before using the phone (after setting it up), you need to sign in for security purposes. You can sign-in with user credentials locally on your IP phone, or remotely with your PC / smart phone.

'Modern Authentication' is also supported.

Before signing in, the network administrator must make sure the phone gets the local time, using either:

- **DHCP Option 42 (NTP)**. If DHCP Option 42 (NTP) is opted for, the network administrator must specify the server providing NTP for the network.
- **time.android.com**. NTP server option for Android phones.
- **time.windows.com**. The phones' default NTP server is sometimes not configured in DHCP Option 42. If not, the phones will attempt the Google NTP server. If DHCP Option 42 is not configured and the Google NTP server is blocked (for example), the phones will use this server and if it's unavailable, the server **time.nist.gov**, described next.
- **time.nist.gov**. The phones' default NTP server is sometimes not configured in DHCP Option 42. If not, the phones will attempt the Google NTP server. If DHCP Option 42 is not configured and the Google NTP server is blocked (for example), the phones will use this server (**time.nist.gov**) if the server **time.windows.com** described previously is unavailable.
- Admins 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 parameter 'date_time/ntp/server_address'

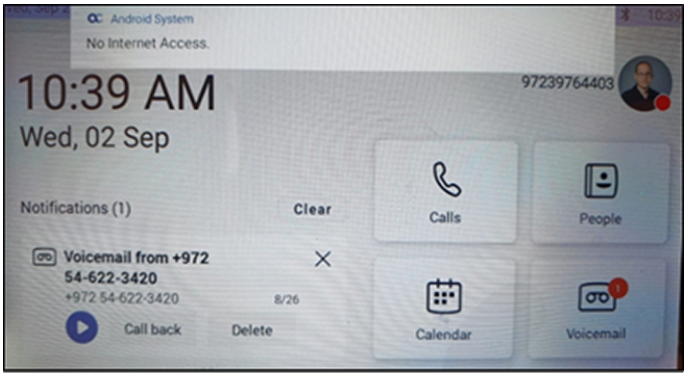
  See also under here for more information.

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.

If the internet connectivity check fails, a 'No Internet Access' warning pops up on the phone screen.

Figure 4-1: Internet Connectivity Check - No Internet Access



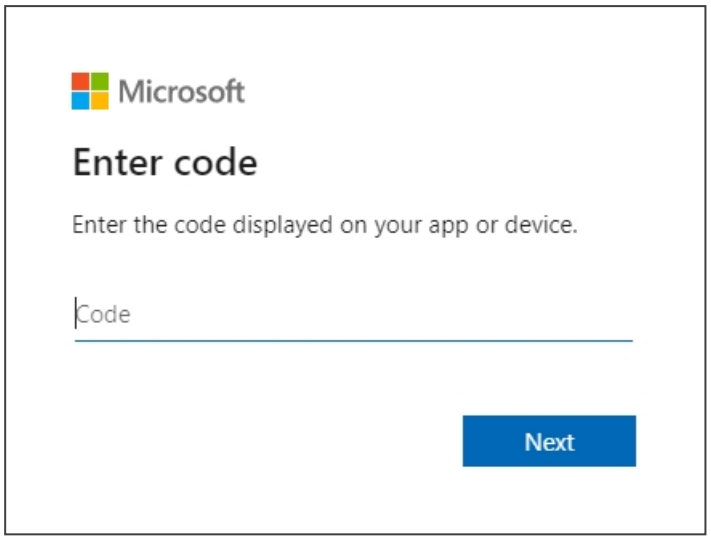
This can point to a problem that is preventing the phone from fully functioning in a Teams environment. The user can ignore the message if the Teams application is fully functioning, or can report a problem if the Teams application is not fully functioning.

➢ To sign in:

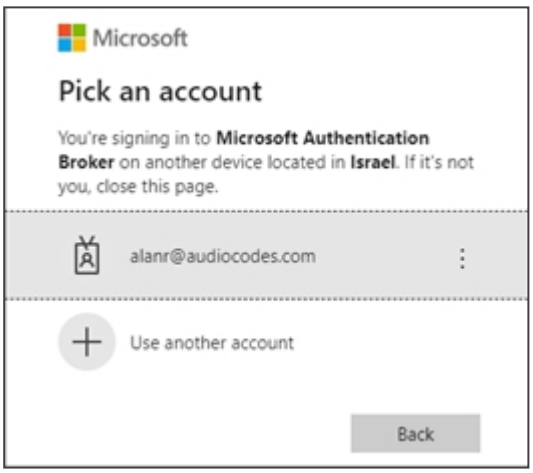
1. Connect the device to the network; this screen is then displayed:



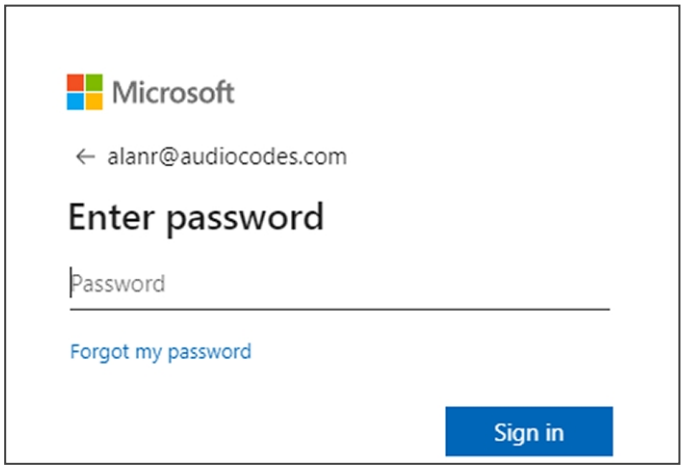
2. Open your browser and point it to **https://microsoft.com/devicelogin** as instructed in the preceding screen.



3. Enter the code and then click **Next**.



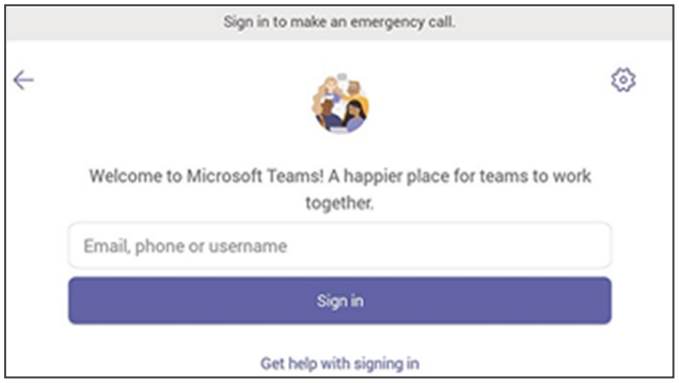
4. Click the account.



5. Enter your password (it's the same password as the Windows password on your PC) and then click **Sign in**.



6. Close the window shown in the preceding figure.
7. Observe that the phone returns to the initial code screen. In that screen, select **Sign in on this device**.

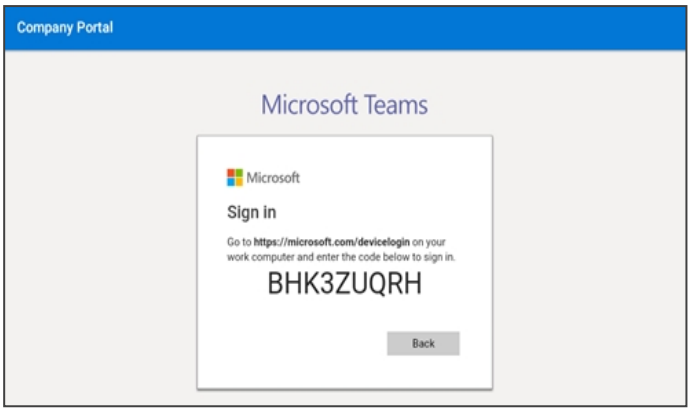


8. Select the 'Email, phone or username' field; a virtual keyboard pops up. Enter one of them and then choose **Sign in**. The 'home' screen opens.
   - If you opt to **Sign in from another device**, complete authentication from your PC or smart phone. This is recommended if you're using Multi Factor Authentication (MFA).

The phone supports a strong password check in order to log in as Administrator. The feature strengths security. The default password:

- must be changed before accessing the device via SSH
- can be changed per device in 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
- Criteria required for a strong password are provided: The password must:
  - ✓ be greater than or equal to 8 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

Figure 4-2: Sign-in from PC / Smart Phone

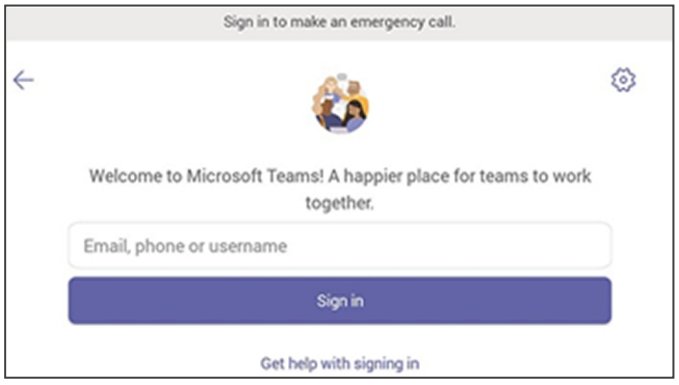


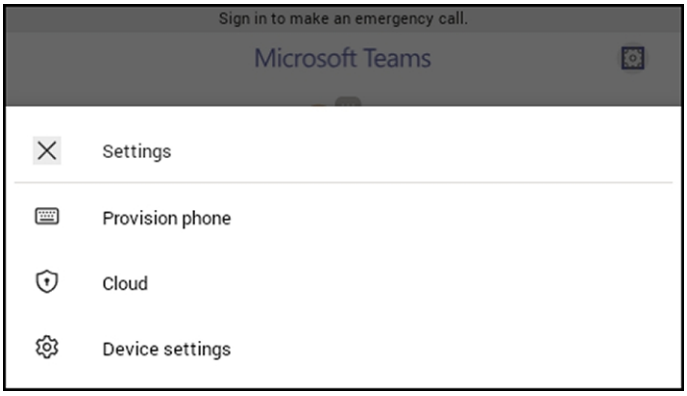
- In the browser on your PC or smart phone, enter the URL indicated in the preceding screen and then in the phone's Web interface that opens, perform sign-in (as noted previously, this option is recommended if using MFA).

LLDP-MED (Link Layer Discovery Protocol – Media Endpoint Discovery) 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. Teams devices connected to the network via Ethernet will dynamically update location information for emergency calling services based on changes to network attributes including chassis ID and port ID.

Multi-Cloud Sign-in

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





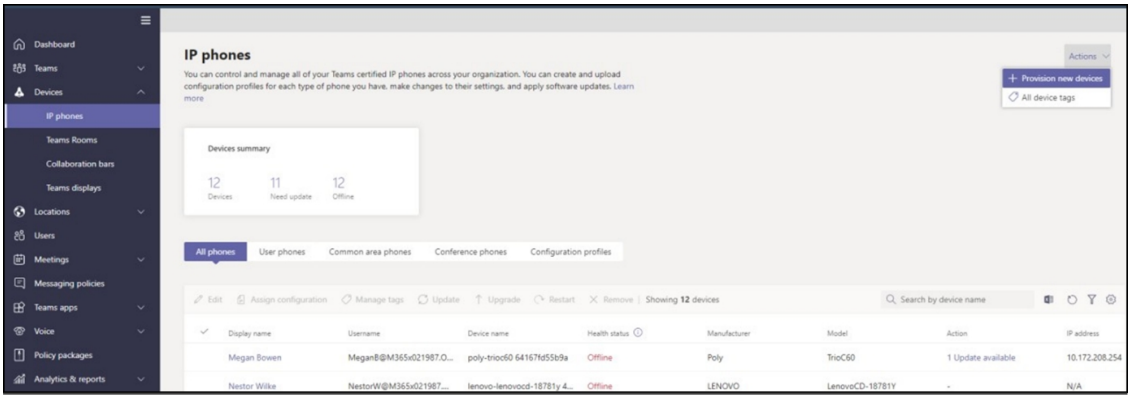
Remote Provisioning and Sign-in from Teams admin center

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

➢ Step 1: Add a device MAC address

Provision the device by imprinting a MAC address on it.

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



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

Manually add a device MAC address

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

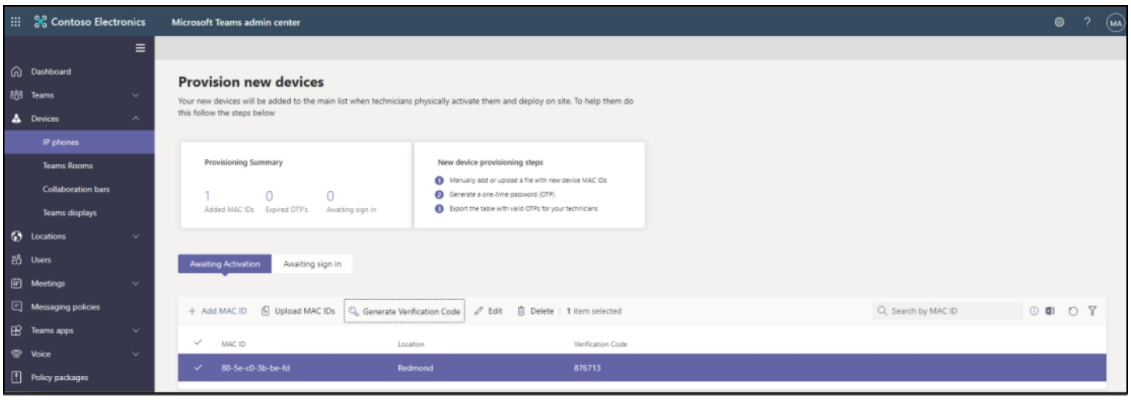
Upload a file to add a device MAC address

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

Step 2: Generate a verification code

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

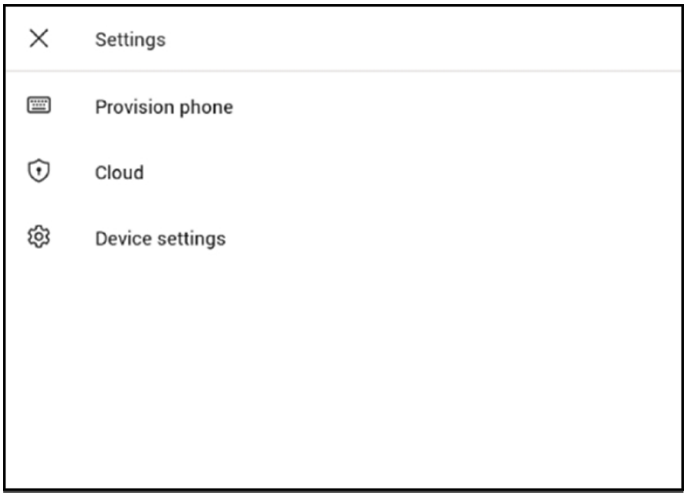
From the **Awaiting Activation** tab, select an existing MAC ID. A password is created for the MAC address and is shown in the **Verification Code** column.



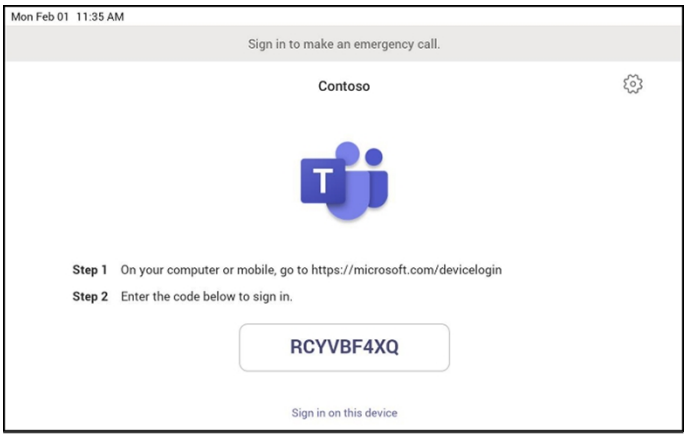
You'll need to provide the list of MAC IDs and verification codes to the field technicians. You can export the detail directly in a file and share the file with the technician who is doing the actual installation work.

Step 3: Provisioning on the device

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



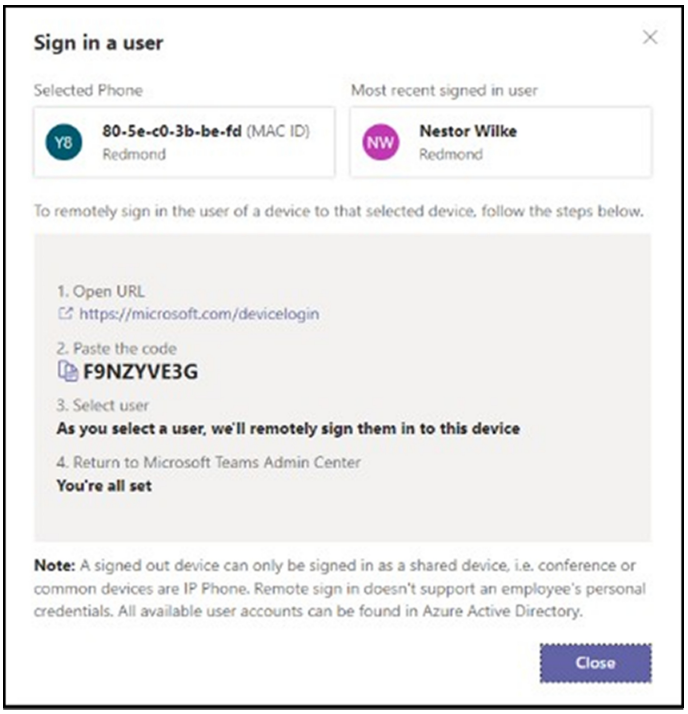
The technician is then expected to enter the device-specific Verification code that was provided in the Teams admin center on the phone's user interface. Once the device is provisioned successfully, the tenant name will be available on the sign in page.



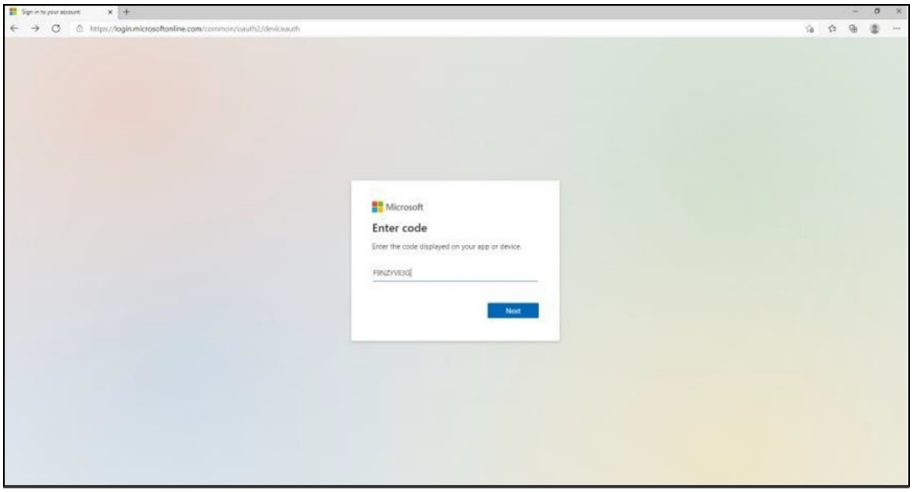
Step 4: Sign in remotely

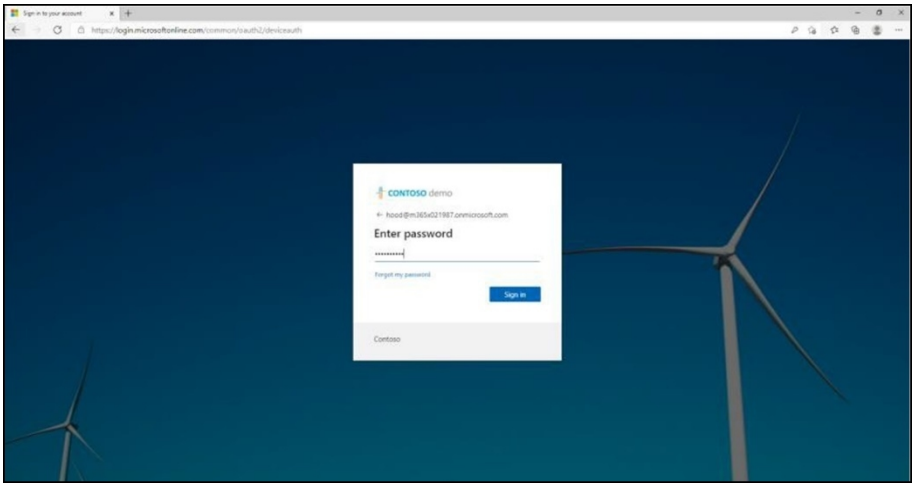
The provisioned device appears in the Awaiting sign in tab. Initiate the remote sign-in process by selecting the individual device.

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

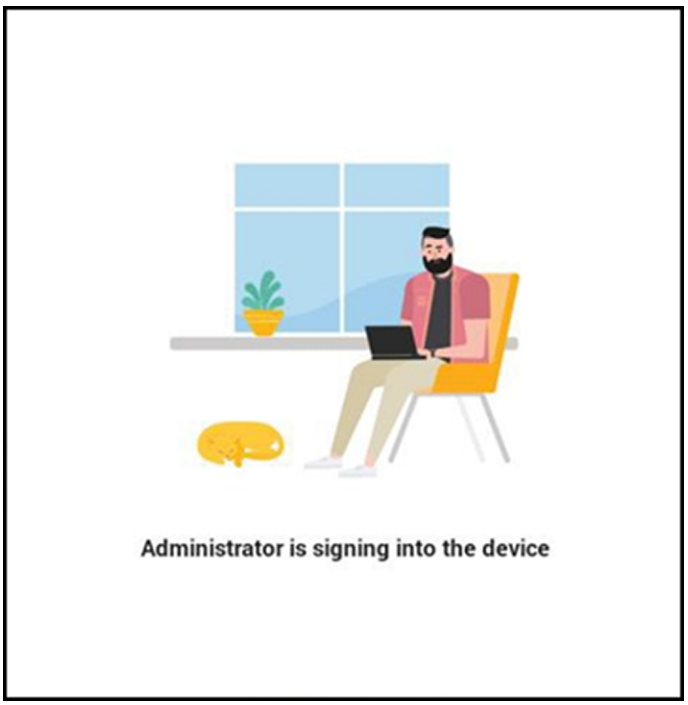


The tenant admin is expected to complete authentication on the device from any browser or smartphone.



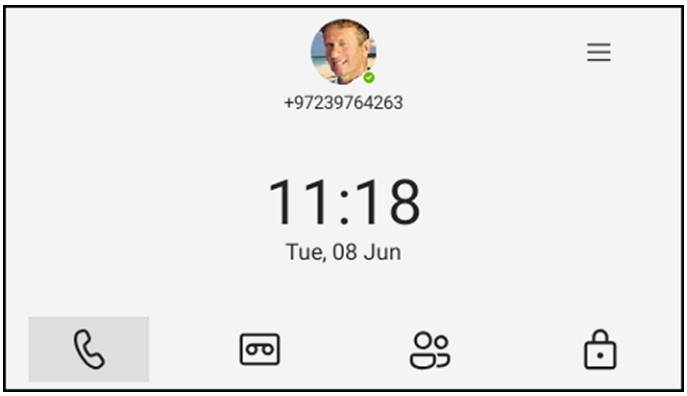


When the tenant admin is signing in from Teams Admin Center, the user interface on the device is blocked to prevent other actions on the phone.

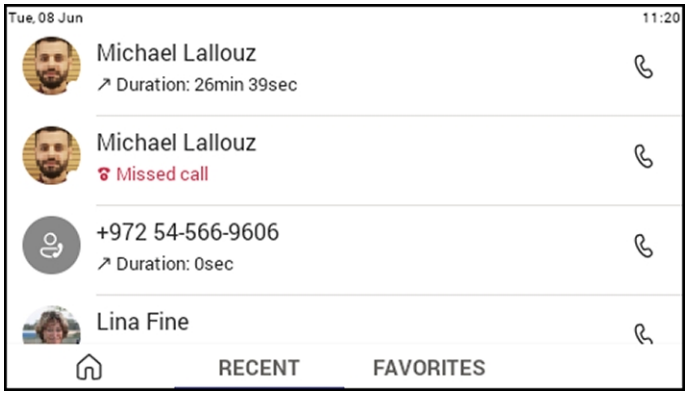


Getting Acquainted with the Phone Screen

The following gets you acquainted with the phone's user interface. The figure below shows the phone's 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	Select the tab to open the Calls screen. The screen shown in the figure preceding this table opens.
People	Select the tab to open the People, shown under Using the People Screen on page 51 opens. 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	Select to open the Calendar screen, shown under Setting up a Meeting opens.
Voicemail	Select the tab to open the Voicemail screen, shown under Accessing Voicemail on page 51 opens.

The following figure shows the user's presence status screen.



Use this table as reference.

Item	Description
Presence status	See Changing Presence Status on the next page for more information.
Settings	See Configuring Teams Application Settings on page 48 for more information.

Setting Status

You can set a presence status such as 'Available' for others in the network to see.

➢ **To set presence status:**

1. In the home screen, select ☰.



2. Select the status displayed; in the preceding figure, 'Available' is displayed.



3. From the drop-down, select the status to set and then press the **OK** button.

Changing 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 presence status:**

1. In the home screen, select ☰.



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

Table 4-1: Presence Statuses

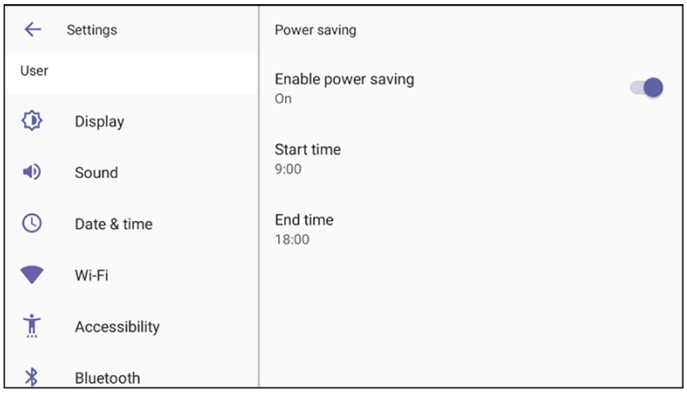
Icon	Presence Status	Description
	Available	You're online and available for other contacts to call.
	Busy	You’re busy and don’t want to be interrupted.
	Do not disturb	You don’t want to be disturbed. Stops the phone from ringing when others call you. If DnD is activated, callers hear a tone indicating 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.

Enabling 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** > **Enable power saving**.



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

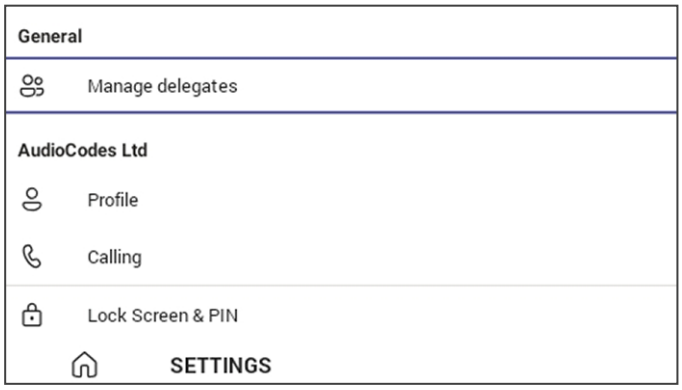
The Configuration File parameters below also support the feature. They can be synchronized with the settings in the phone screen.

- general/power_saving (Used to enable or disable power saving) (Default: 1)
- 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.

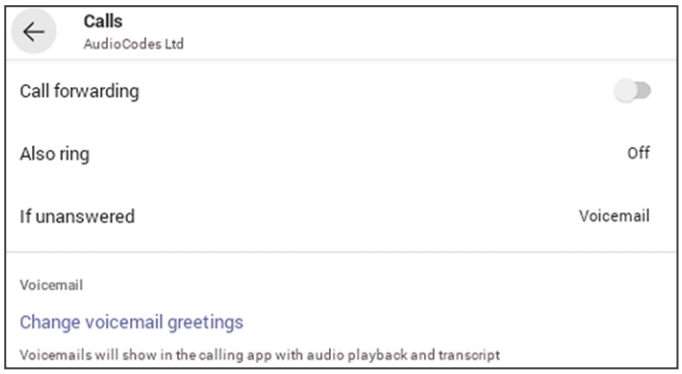
Configuring Teams Application Settings

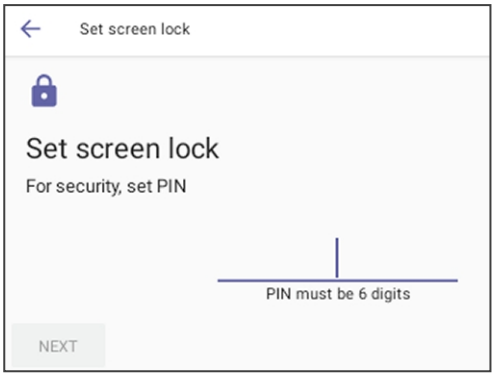
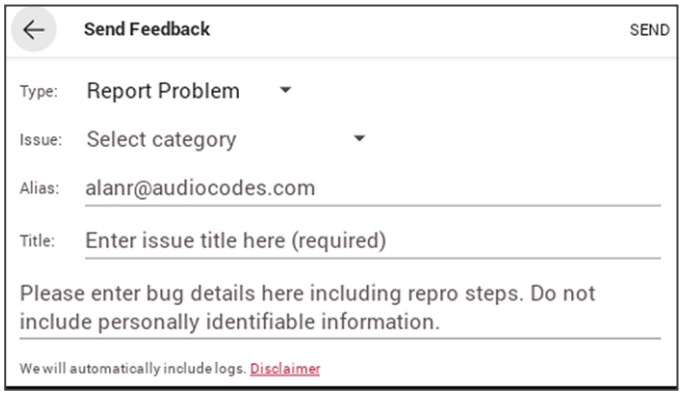
The following describes the Teams application's settings. In the home screen, select .



Use this table as reference:

Table 4-2: Idle Screen Description

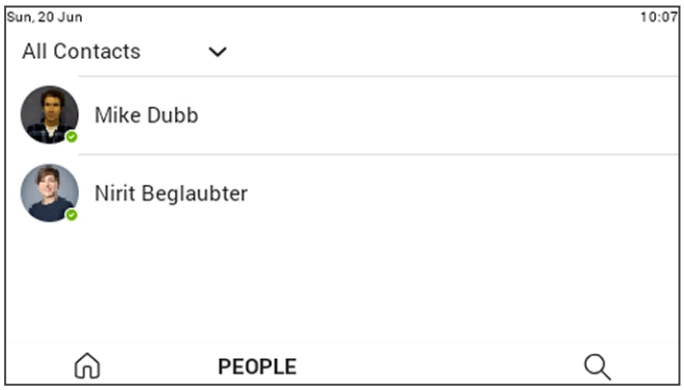
Item	Description
Profile	Opens the user's email address and photo / avatar picture.
Calling	Opens the Calls screen.  **Incoming Calls** ■ **Call forwarding**. Enables automatically redirecting an incoming call to another destination. ■ **Forward to**. Only displayed if the previous setting is enabled. Defines the destination to which to forward incoming calls. ■ **Also ring**. Only displayed if 'Call forwarding' is disabled. Select 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. Select either **Off**, **Voicemail**, **Contact or number**, or Call group. **Caller ID** ■ Hide your phone number when dialing people who are outside of Microsoft Teams **Block Calls** **Block calls with no caller ID**. Enables blocking calls that do not have a Caller ID.
Lock Screen & PIN	You can lock your phone as a security precaution.  Configure a lock option before attempting to lock the phone.

Item	Description
	  If a lock option isn't configured, the lock action won't work. To unlock a locked phone, see Unlock on page 33.
Report an issue	Microsoft Teams application's 'Report an issue' option opens the Send Feedback screen.  'Report an issue' can alternatively be triggered by simultaneously pressing the Vol up + Vol down keys. This can help the user to report an issue even if the application is stuck and does not allow the user to report the issue via the Application > Settings tab.
About	Opens the About screen.

Item	Description
	
Sign out	Lets you sign out of the phone application as one user and optionally sign in again as another user. See Signing Out on page 53 for detailed information.
Device Settings	Opens the [Device] Settings screen. See Configuring Device Settings on page 15 for detailed information.

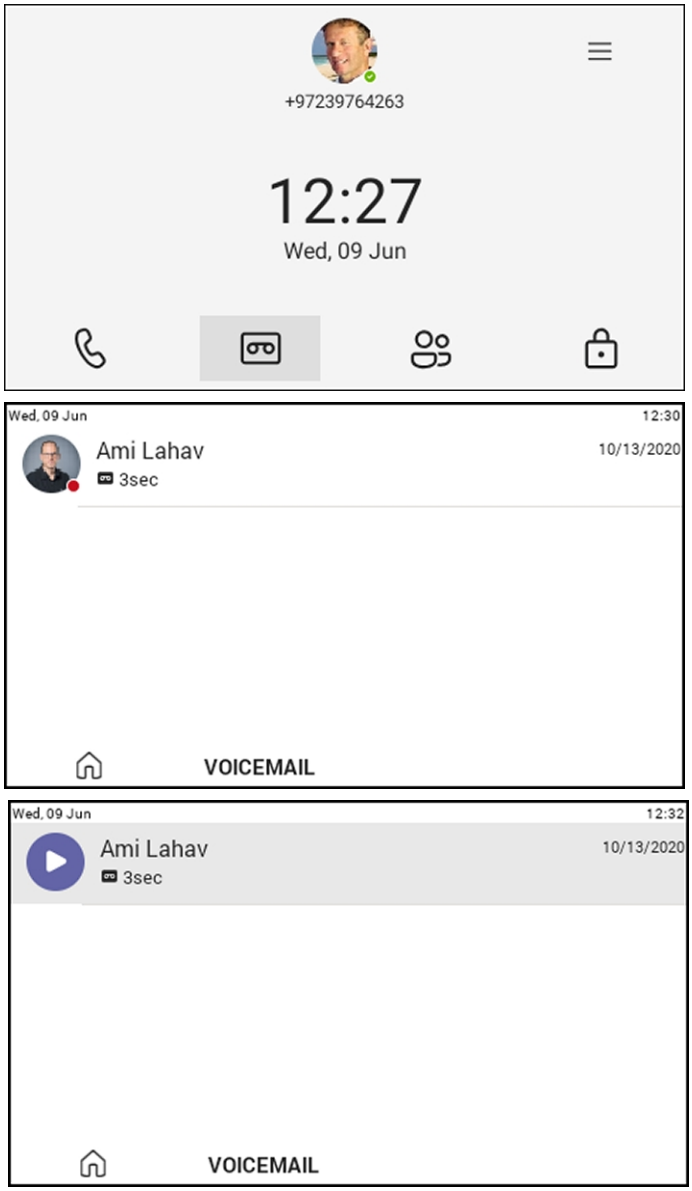
Using the People Screen

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.



Accessing Voicemail

From the phone's home screen, select the **Voicemail** tab.From the phone's home screen, select the voicemail icon and then select the message.



Using Audio Devices

Use one of the following audio devices on the phone for speaking and listening:

- **Handset**: To make a call or answer a call, lift the handset off the cradle.
- **Speaker** (hands-free mode)
  - To activate it, press the speaker key during a call or when making a call.
  - To deactivate it, press the speaker key again.
- **Headset** (hands-free mode). When talking on the phone, you can relay audio to a connected headset.
  - To enable it, press the headset key.
  - To disable it, press it again.

You can easily change audio device during a call.

- **To change from speaker/headset to handset**: Activate speaker/headset and pick up the handset; the speaker/headset is automatically disabled.
- **To change from handset to speaker/headset**: Off-hook the handset and press the speaker/headset key to activate the speaker/headset. Return the handset to the cradle; the speaker/headset remains activated.

Transferring 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.

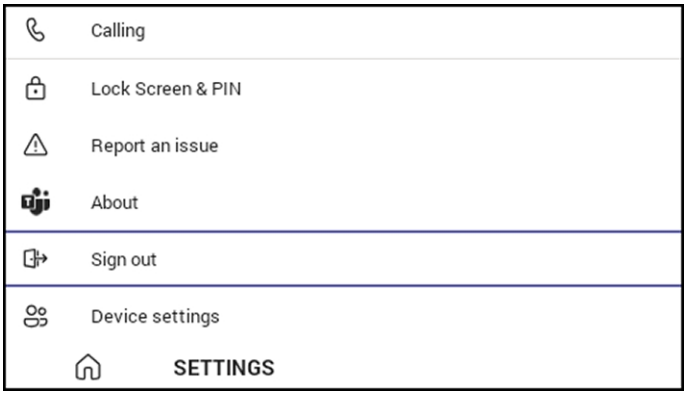
The feature enables the user to move away from their PC while seamlessly staying connected. The phone recognizes the user is in a call on another device and prompts them to transfer or add, letting them start their call from elsewhere and transfer to their desk phone.

Signing Out

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

➢ **To sign out:**

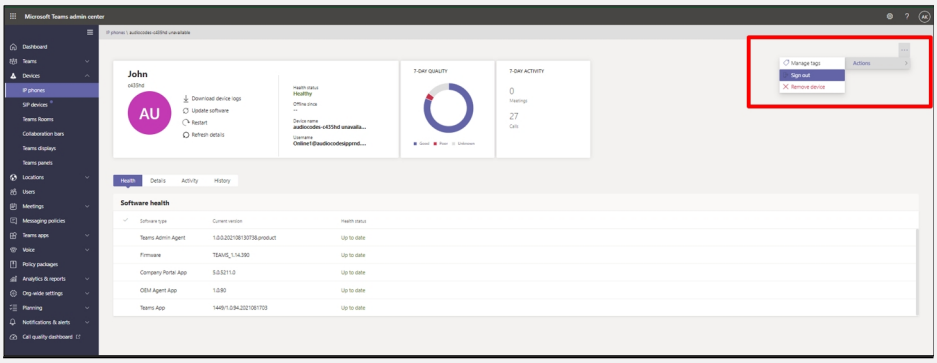
1. Under **Settings**, navigate to and select the **Sign out** option.



2. After selecting the **Sign out** option, you're prompted 'Are you sure you want to sign out? Select **OK**; you're 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.



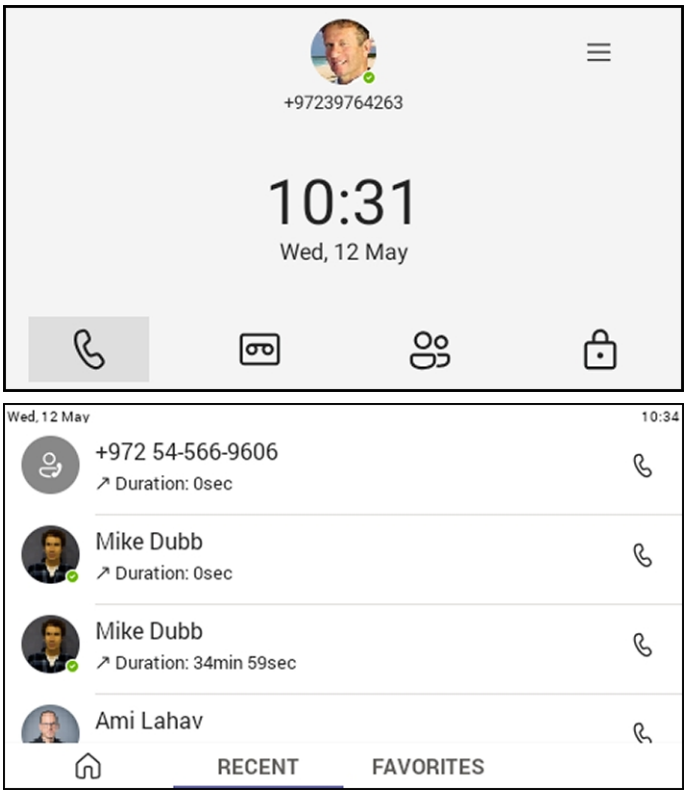
5 Performing Teams Call Operations

The following documentation shows how to perform basic operations with the phone.

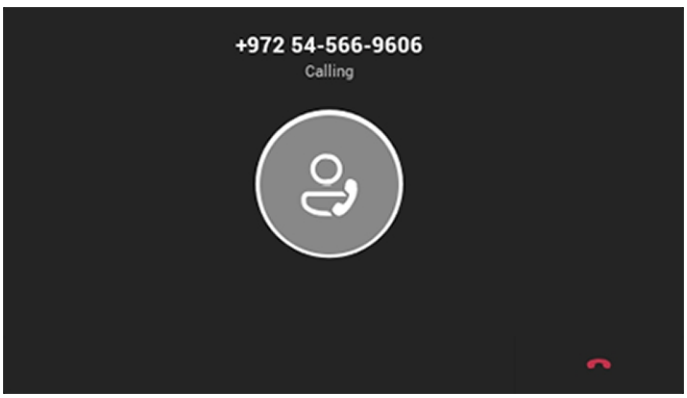
Making a Call

Calls can be made in multiple ways, for example, you can press the digit keys on the phone's dial pad to enter the phone number.

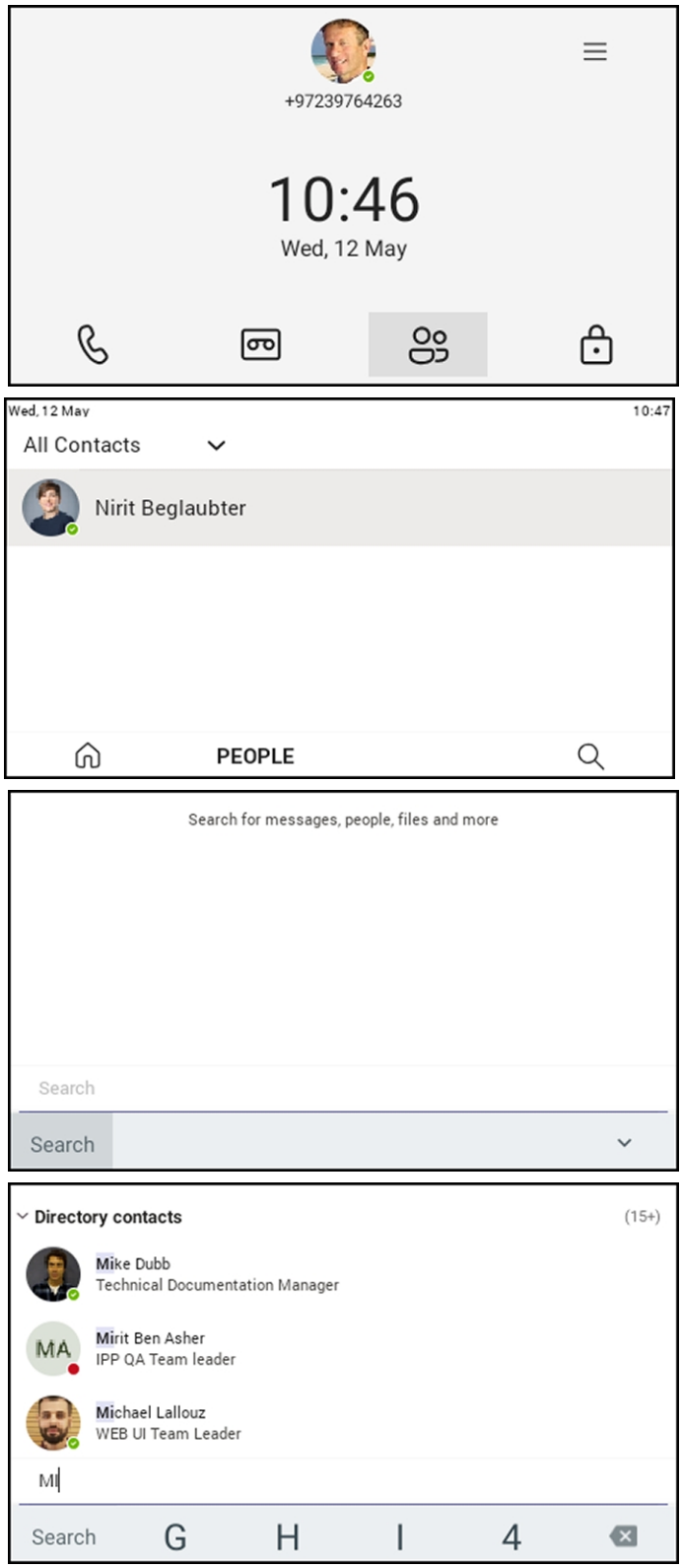
Alternatively, in the home screen you can press the softkey and in the RECENT screen that opens you can navigate to a recent call and then press the **OK** button.



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



You can alternatively make a call using a speed dial from the People screen or from the 'Search people' feature in the People screen.



Dialing 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:**

- In the home screen, select the icon and then in the 'Recent' screen that opens navigate to and select the missed call.

Select to Dial

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

Transferring a Call

During a call, you can also transfer the call using the device's physical **Transfer** button:

- Short press – opens a dialog to select a contact to transfer the call immediately.
- Long press – 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.

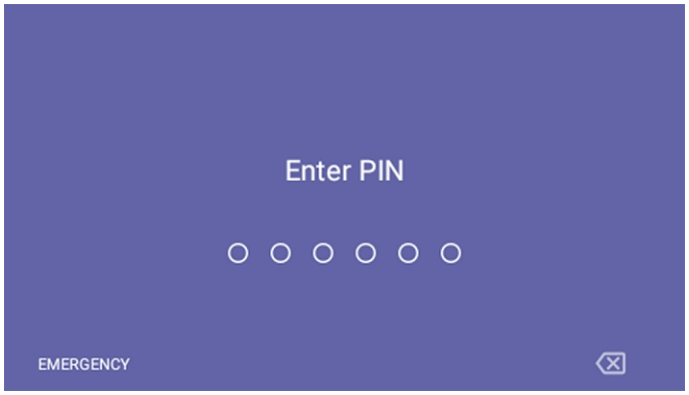
See here for a video clip demonstrating how to immediately transfer a call without verifying with the intended recipient that they want to take the call. The principle is similar across AudioCodes Teams phones.

➢ **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.

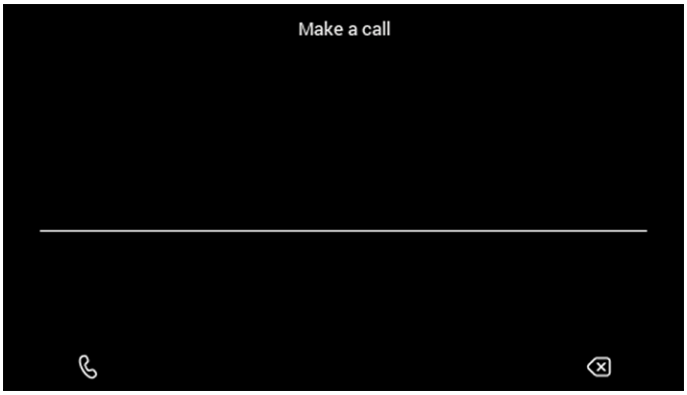
Making an Emergency Call

The phone features an emergency call service. The idle lock screen displays an **Emergency** key.



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

- Select the **EMERGENCY** softkey shown in the preceding figure of the locked idle screen and then enter the emergency number.



Answering Calls

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- select the **Accept** softkey (the speaker is automatically activated).

Ending 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- select the **End** softkey.

Managing Calls

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

> Each device reports every call from | to that user to the server. All devices that a user signs into are synchronized with the server. The Calls screen is synchronized with the server.

➢ **To manage calls:**

1. Select **Calls** and in the Calls screen, select **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. Select a call in the list and then select to call someone back.

Paging 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.

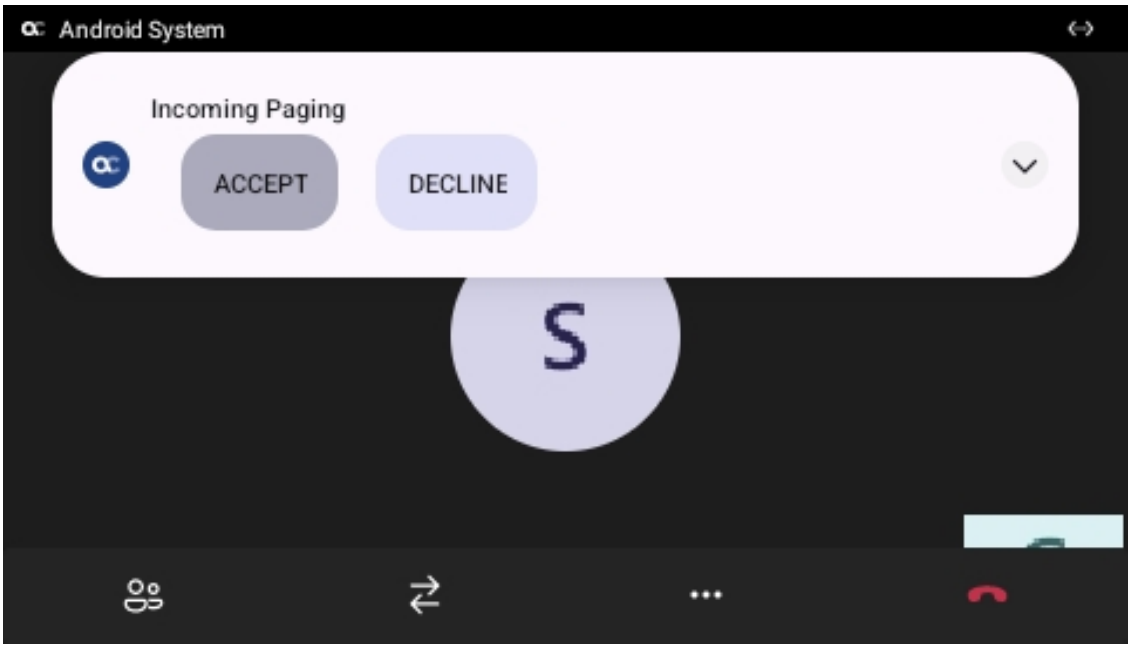
Use the following table as reference.

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 ■ 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

Parameter	Description
	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, the phone *immediately 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 new 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 new 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:



Transferring 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.

Transferring 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.

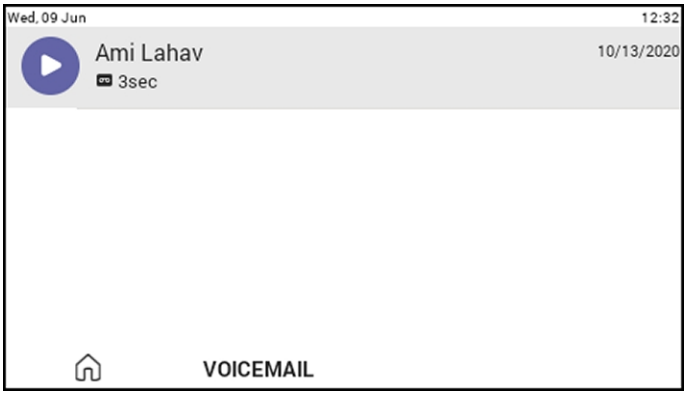
Viewing and Playing Voicemail Messages

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. From the phone's home screen, select the voicemail icon and then select the message.



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.

Rejecting an Incoming Call, Sending 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 ; if you have voicemail, the call will go into voicemail; the Microsoft Teams server performs this functionality.

Adjusting Volume

The phone allows

- Adjusting Ring Volume on the next page

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

For more information about sound and volume, see here.

Adjusting 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, select the VOL▲ or VOL▼ key on the phone.
2. After adjusting, the volume bar disappears from the screen.

Adjusting 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. Select the VOL▲ or VOL▼ key to adjust the volume.
3. After adjusting, the volume bar disappears from the screen.

Adjusting 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. Select the VOL▲ or VOL▼ key; the volume bar is displayed on the screen. After adjusting, the volume bar disappears from the screen.

Adjusting 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. Select the VOL ▲ or VOL ▼ key; the volume bar is displayed on the screen. After adjusting the volume, the volume bar disappears from the screen.

Adjusting 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. the volume bar is displayed on the screen.

Playing Incoming Call Ringing through USB Headset

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

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

■ Configure the following parameter:

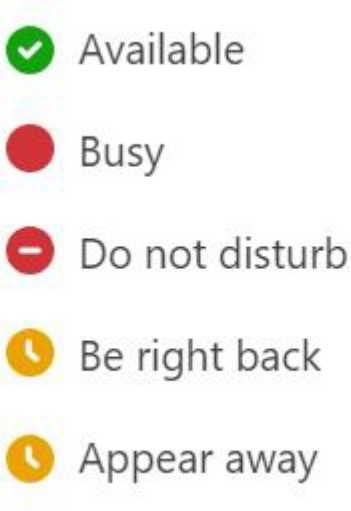
audio/stream/ringer/0/audio_device=**BOTH** (default), **BUILTIN_SPEAKER** or **TYPE_USB**

- **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.

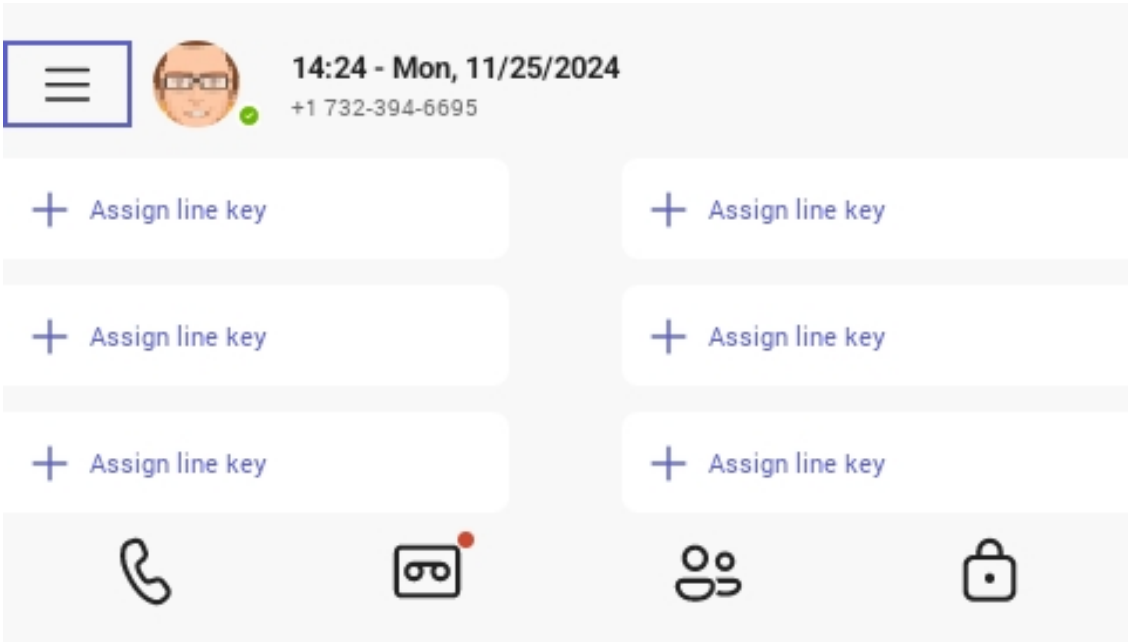
Assigning a Line Key for Speed Dial or Features

Line keys provide quick access to features like redial and voicemail. You can also assign predefined functions or people to line keys and label them for speed dial.

The presence/ status of a contact displays by their name (account avatar) in the LCD home screen:

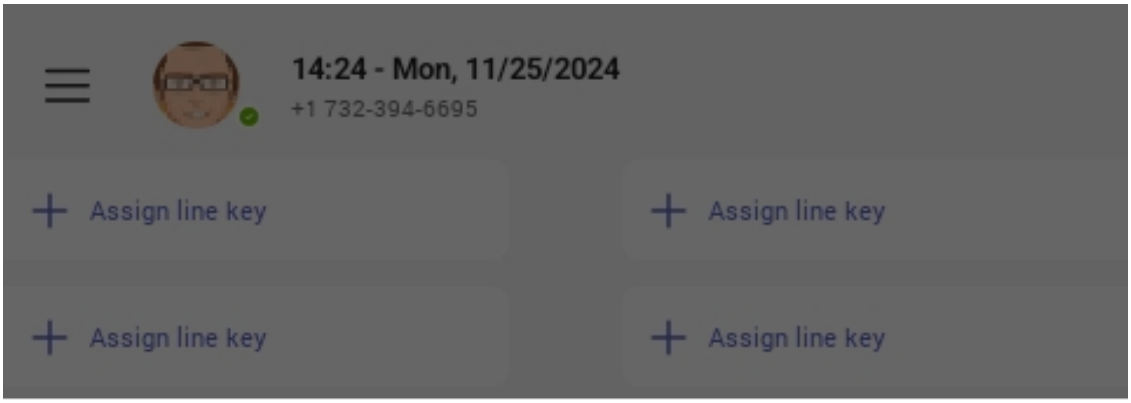


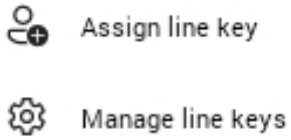
The LCD home screen displays an 'Assign line key' option:



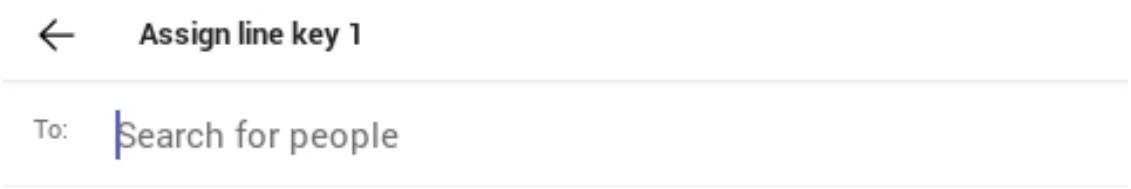
➢ **To assign a line key:**

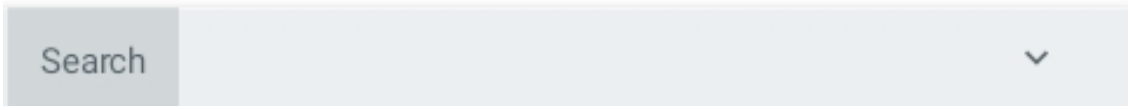
1. Use the navigation control to navigate to the 'Assign line key' you want to associate with a named person.
2. Press the tick button on the navigation control to select; the assign key menu displays:



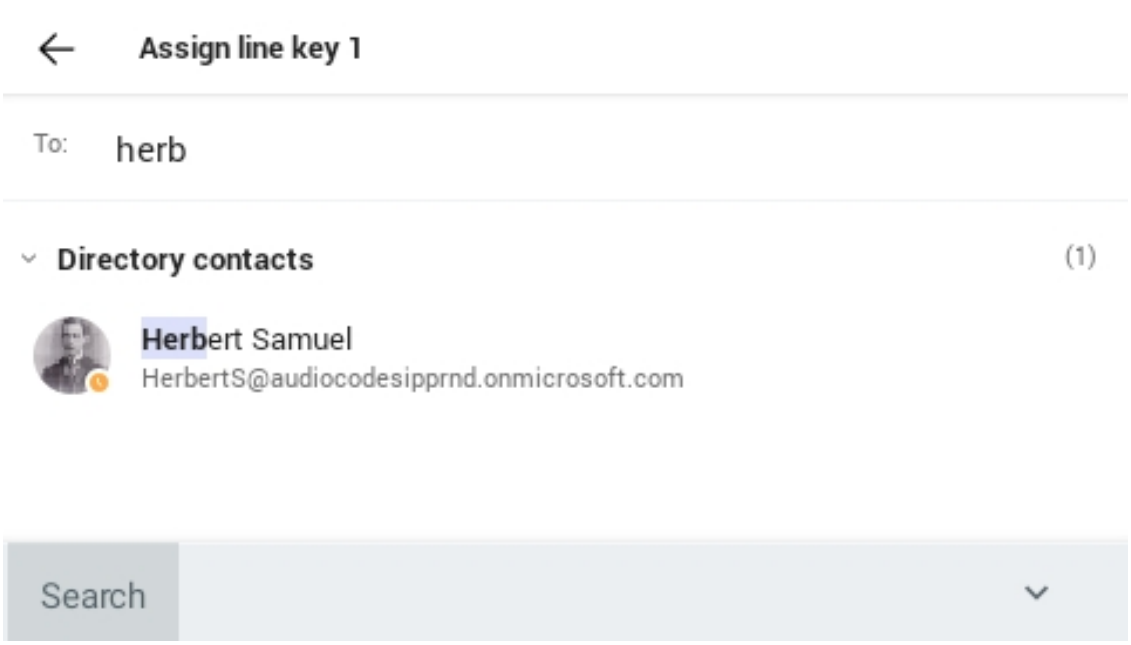


3. Press the tick button again and use the dial pad to spell out the first couple of letters to 'Search for people':

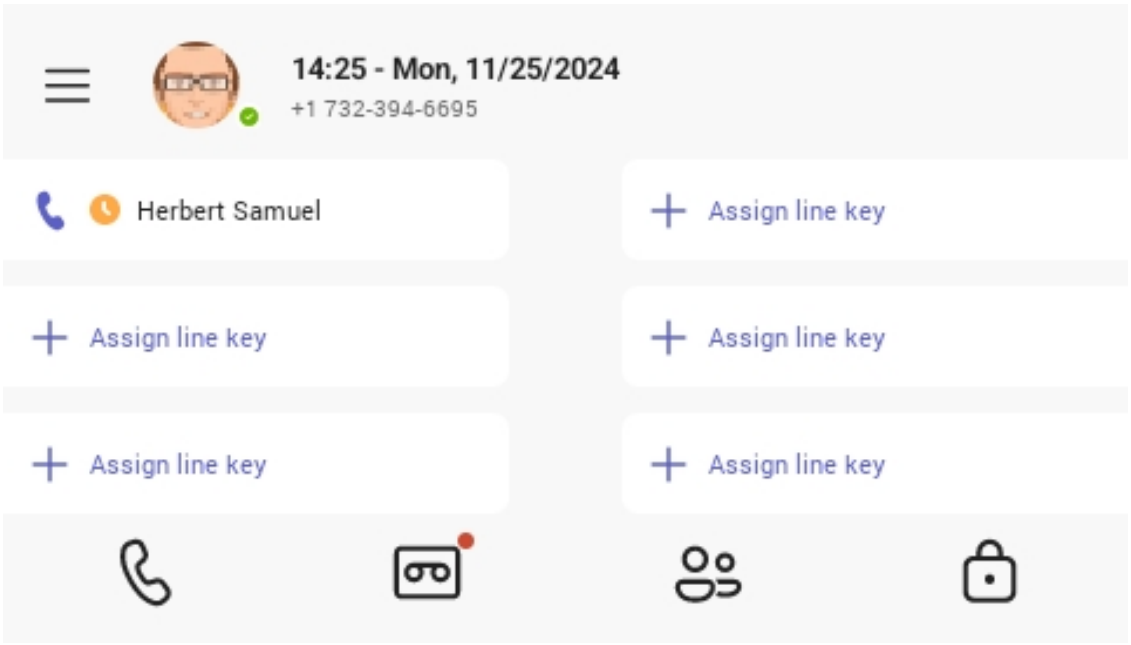




4. Use the navigation control to navigate to the contact you wish to select. Press the tick button. The searched name displays in full:

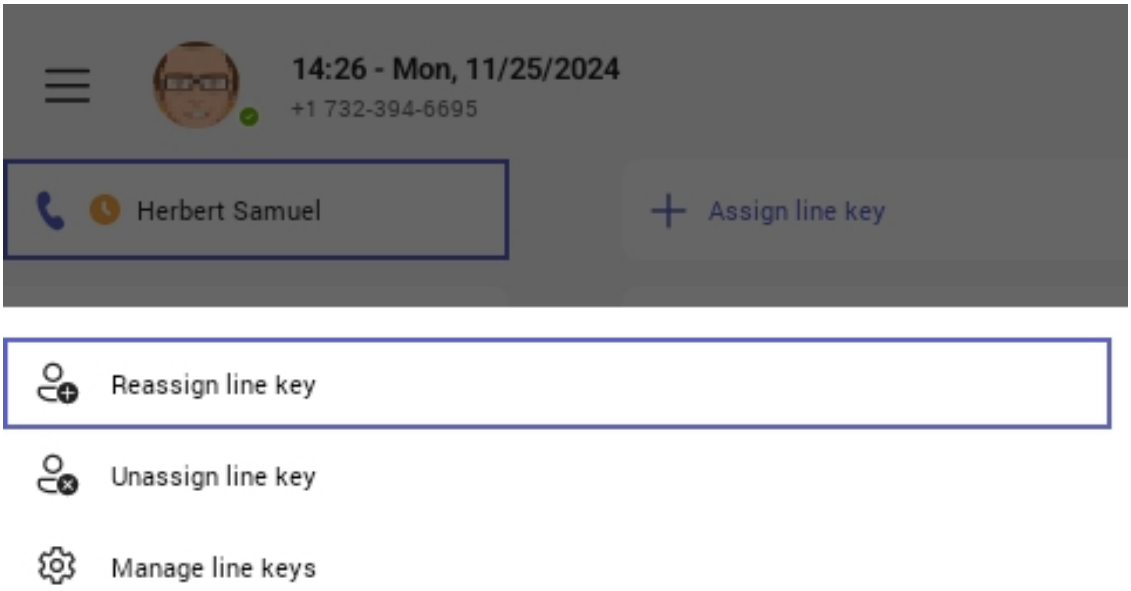


5. Press the navigation control tick button to confirm. The screen displays the assigned line:



➢ **To reassign or unassign a line:**

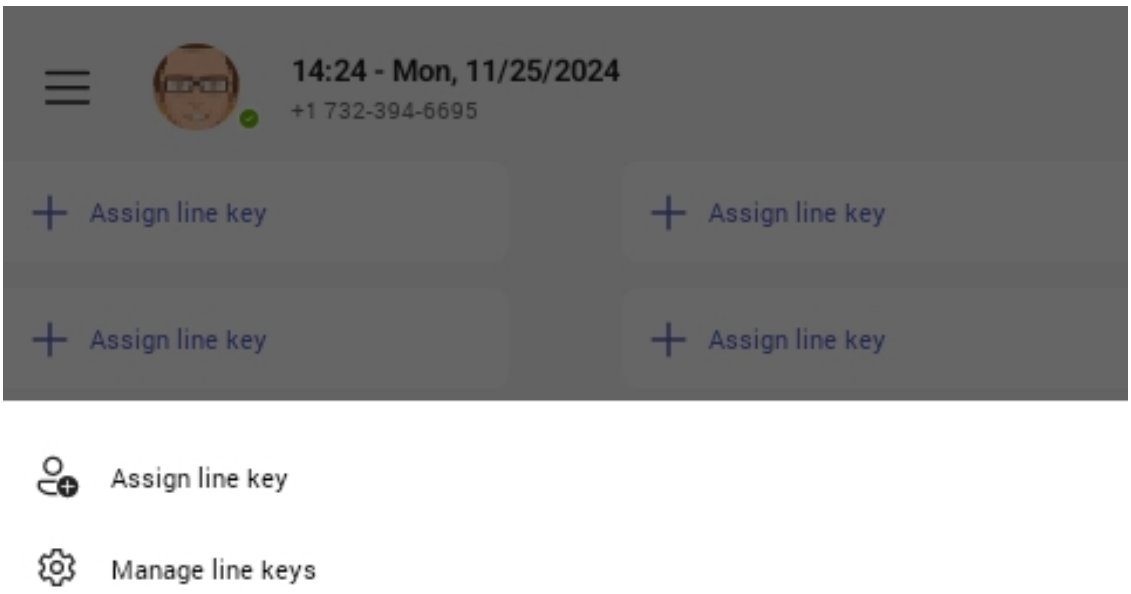
1. Press the softkey to display the menu:



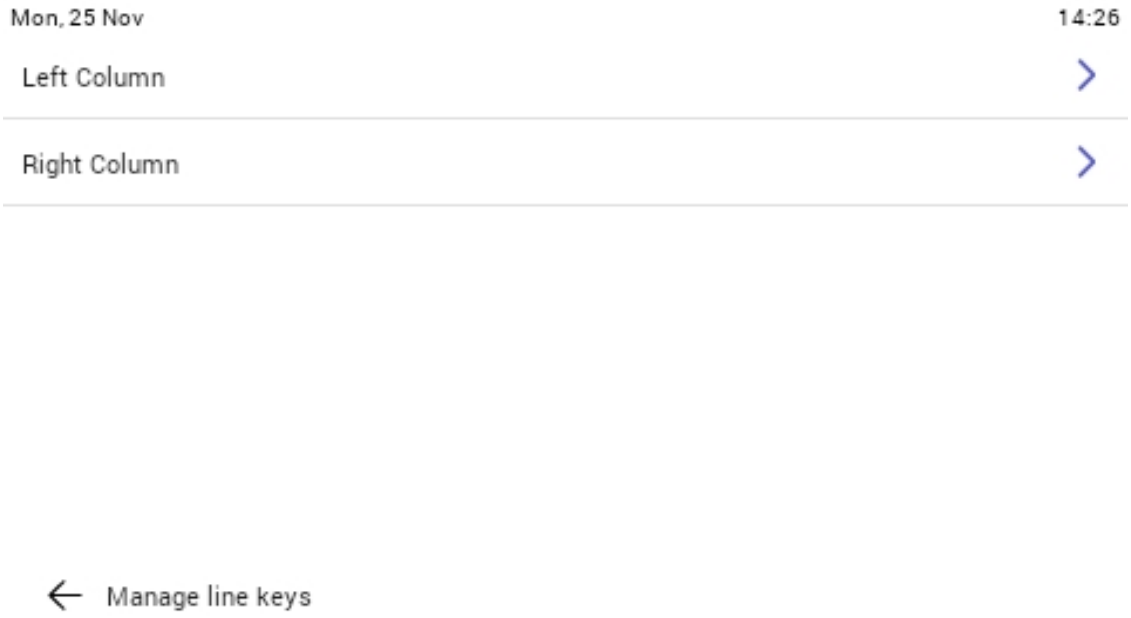
2. Use the navigation control to select 'Reassign line key' or 'Unassign line key'. If you select 'Reassign line key', follow these steps.

➢ **To reformat the LED assign screen:**

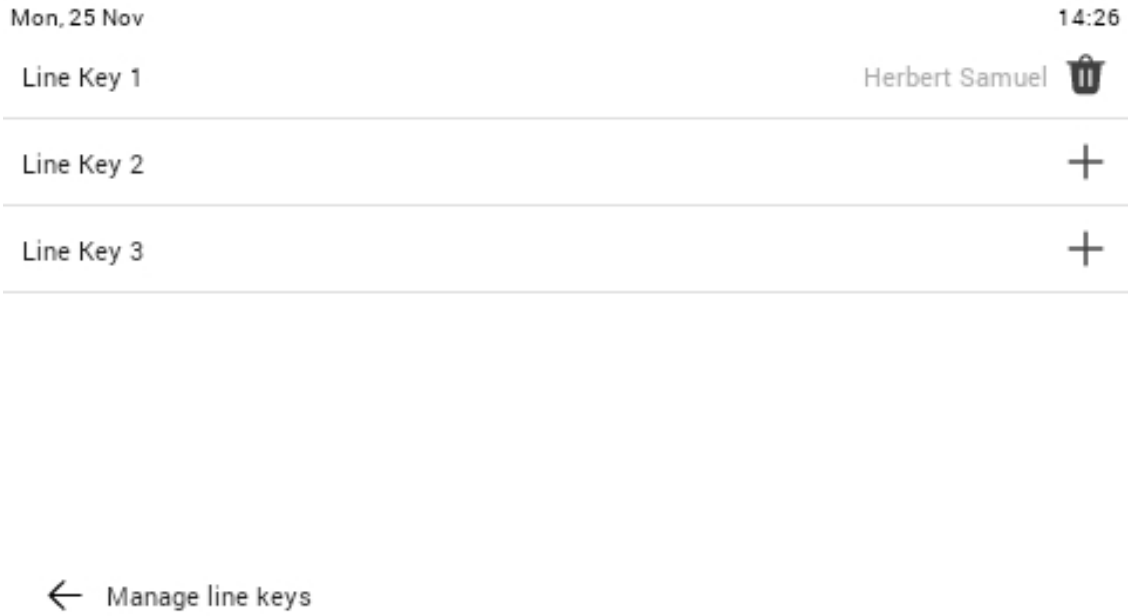
1. Follow these steps and then navigate to 'Manage line keys':



2. Press the tick button. The format options display:



3. Use navigation control to select the field you want to format and then press the tick button.
4. You can now assign a line or delete a contact from a line.



6 Performing Administrator-Related Operations

Network administrators can:

Update phone firmware manually (see Updating Phone Firmware Manually on page 82

Manually perform recovery operations (see Manually Performing Recovery Operations on page 89

Remove devices from Intune management (see Removing Devices from Intune admin center on page 91

Update Microsoft Teams devices remotely (see Updating Microsoft Teams Devices Remotely on page 94

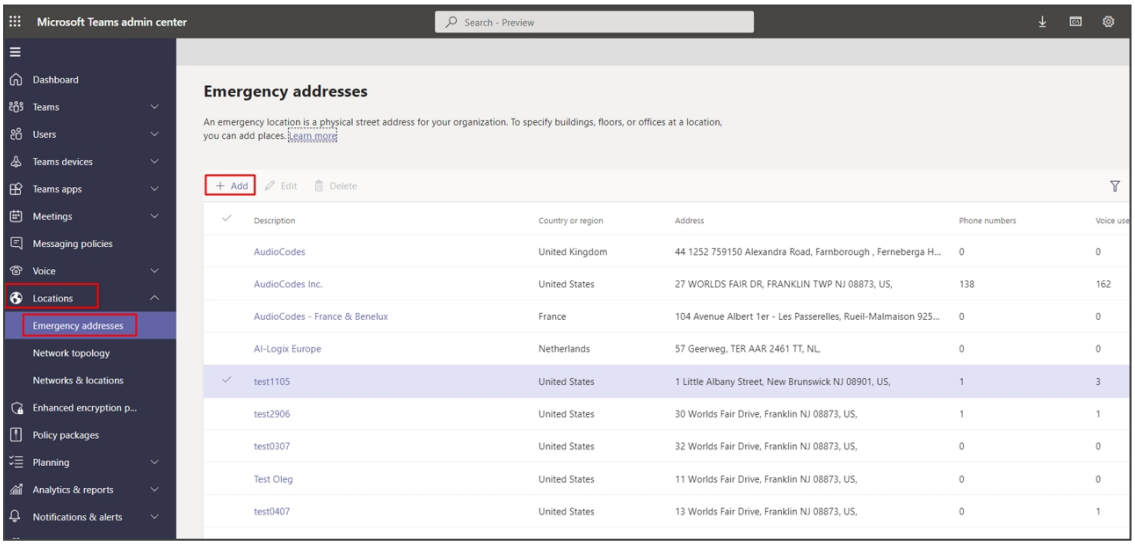
Manage phones with the Device Manager (see Managing Phones with the Device Manager on page 98

Setting up an E911 Emergency Location using TAC

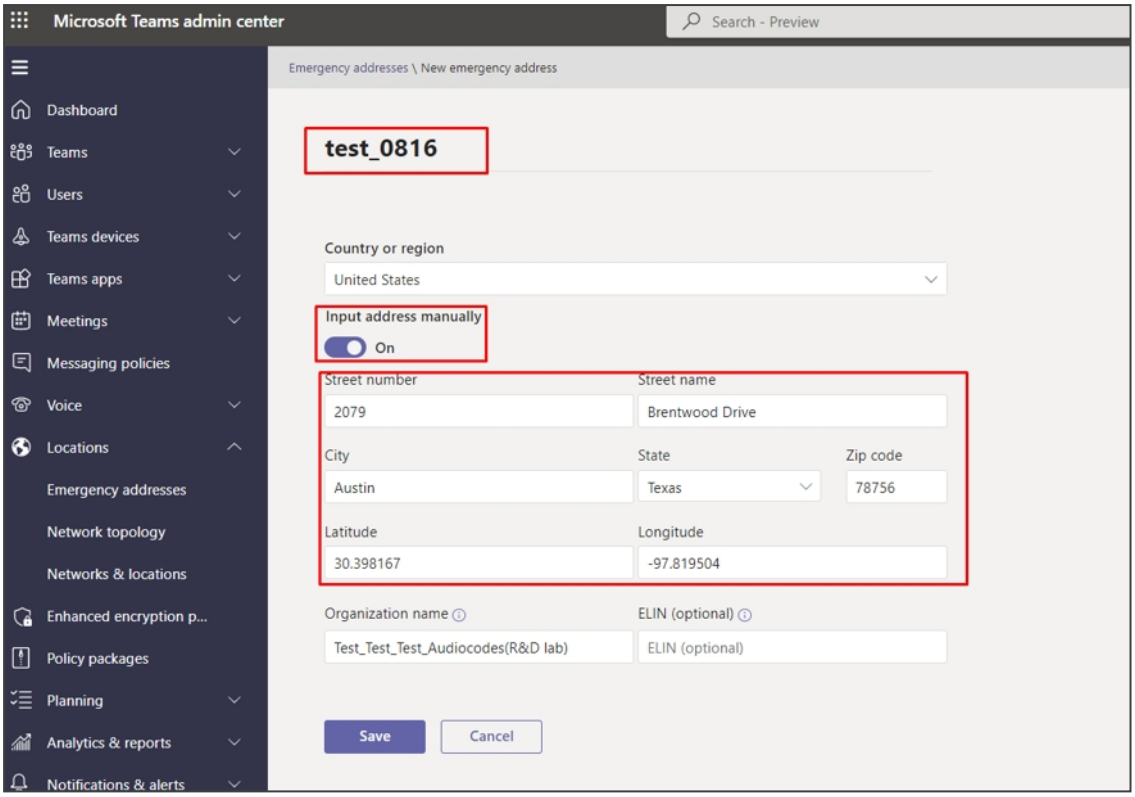
An E911 emergency location can be set up using the Microsoft Teams admin center.

➢ To set up an E911 emergency location:

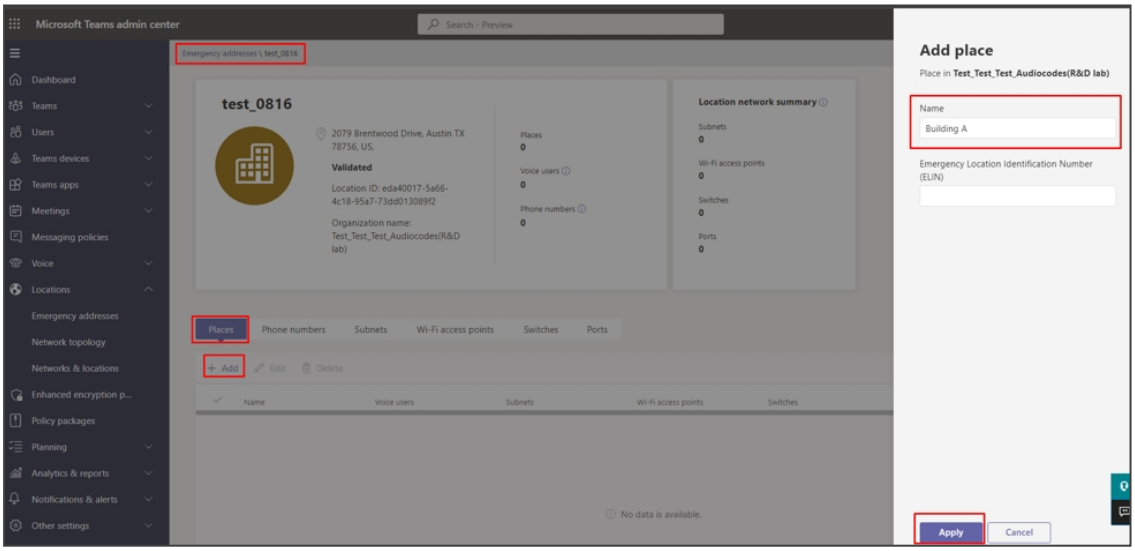
1. In the TAC, go to **Locations** and in the 'Emergency addresses' page, set a new location by clicking **+ Add**.



2. Enter a name for the location, enable **insert address manually**, make sure that all data is filled in correctly and then click **Save**.



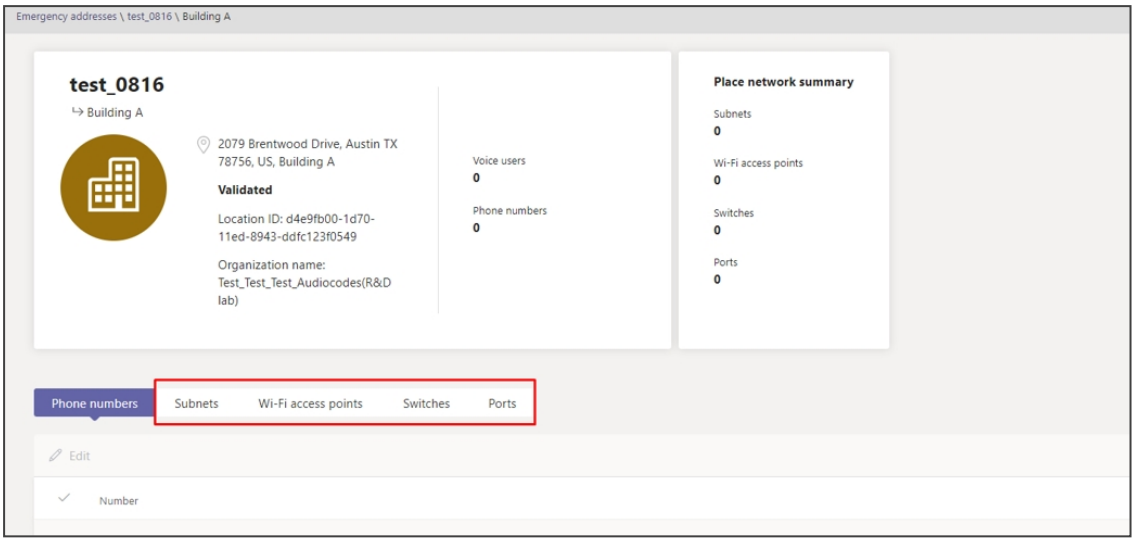
3. After the location has been set, click on the location and add a place (building, etc.). Make sure to maintain the hierarchy. Click **Apply** and verify the place has been set.



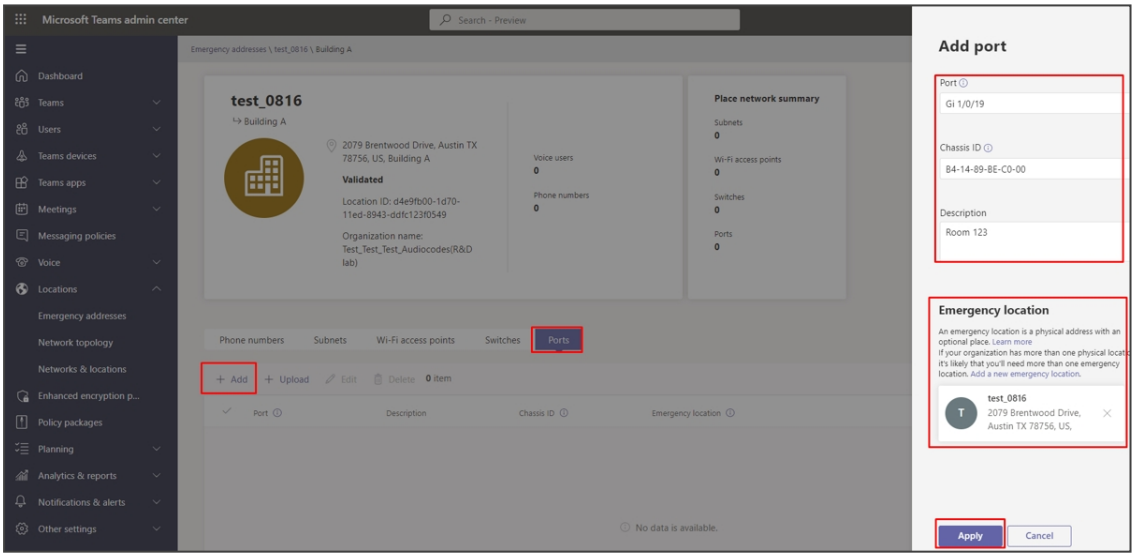
4. Enter the place you've set and define how to determine the emergency location. It can be determined by these values:

- Port ID
- Switch (Chassis) ID
- BSSID (Wi-Fi access points)
- Subnet
- User predefined location (see below for more details).

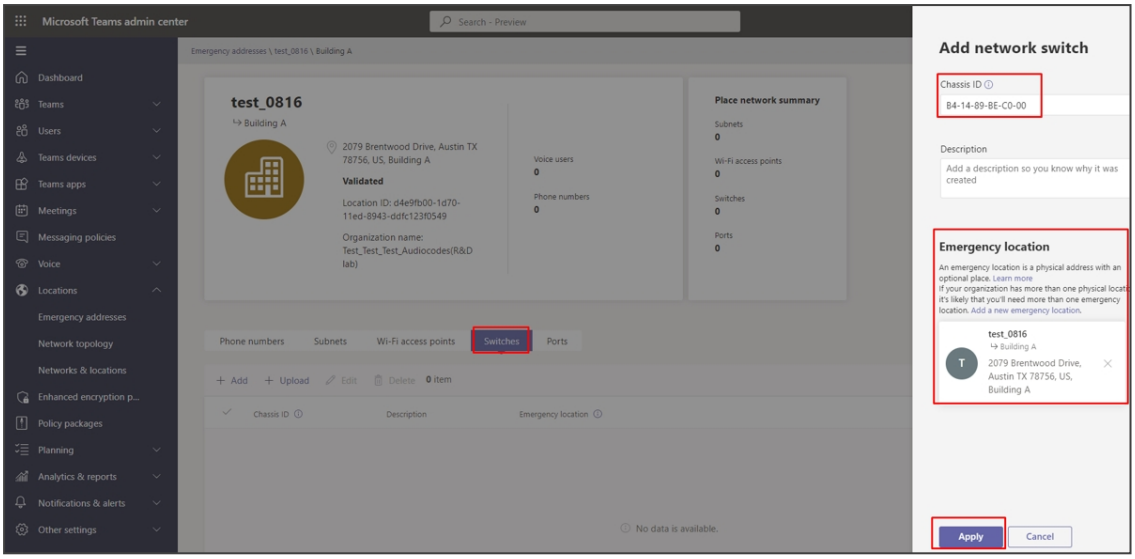
The hierarchy of displaying a location is determined in the same order as above.



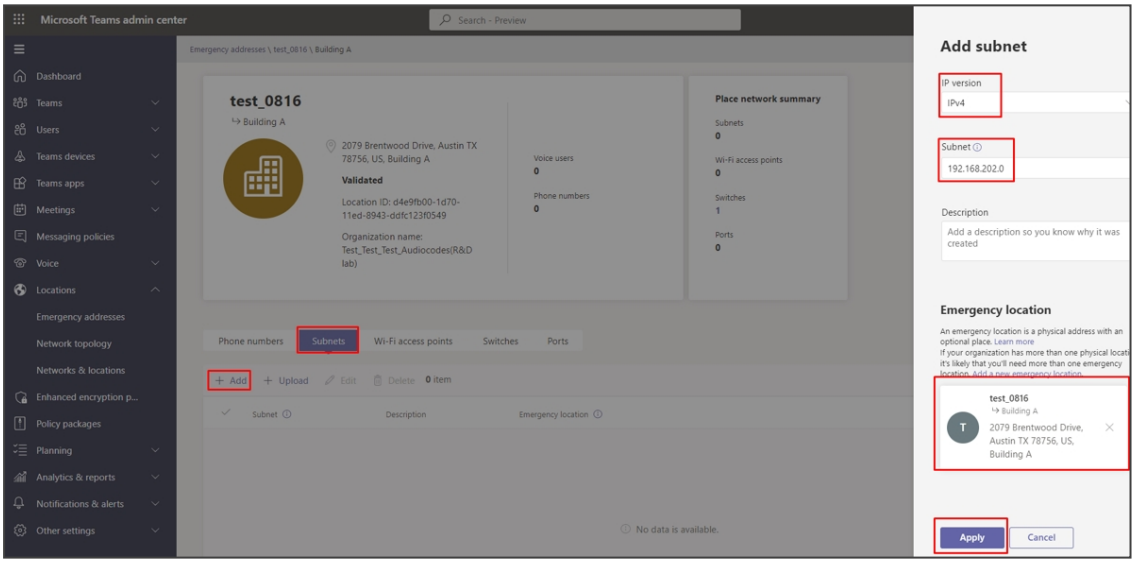
5. Enter a location defined by a specific port ID. Make sure to enter the port description correctly, as delivered from your switch (* the switch must allow LLDP transmit and receive and provide LLDP information).



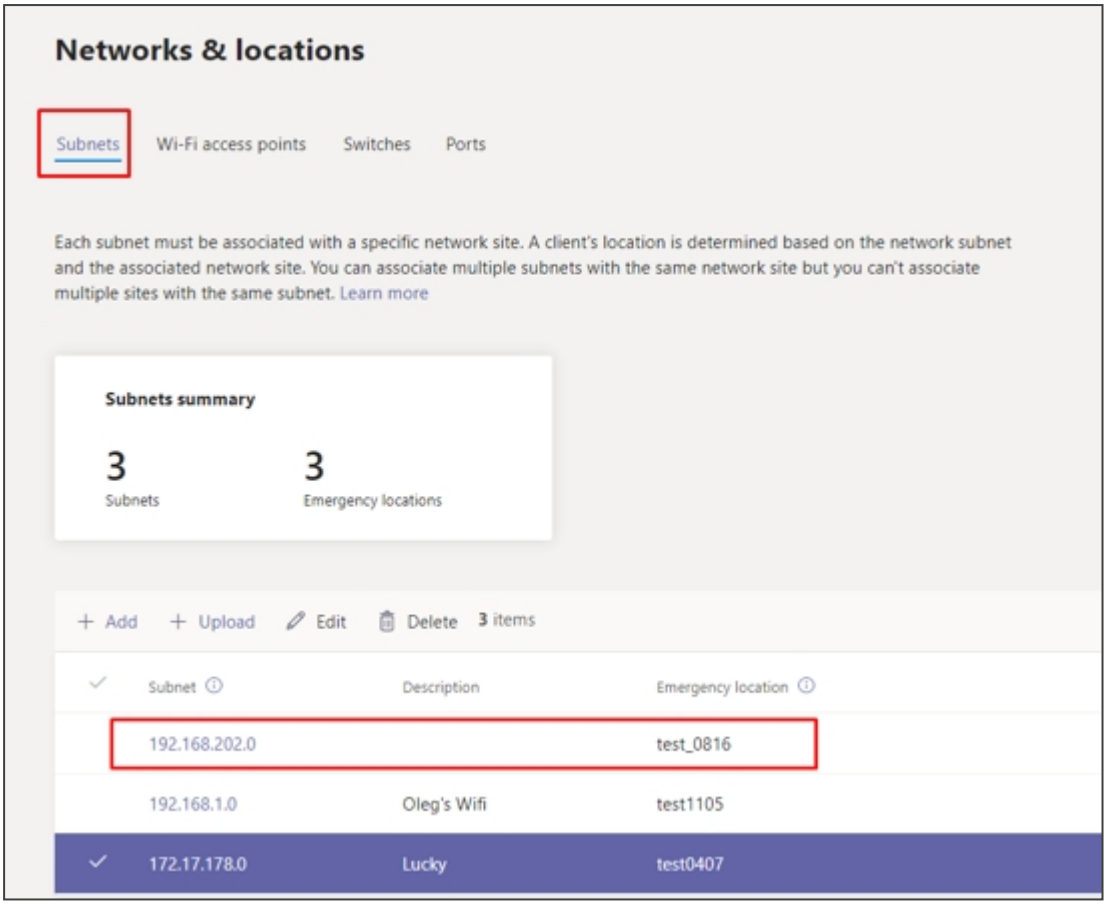
6. Define a location defined by switch (Chassis) ID. The location can be the same since a room defined in the previous step can reflect a room in a building using the same switch).

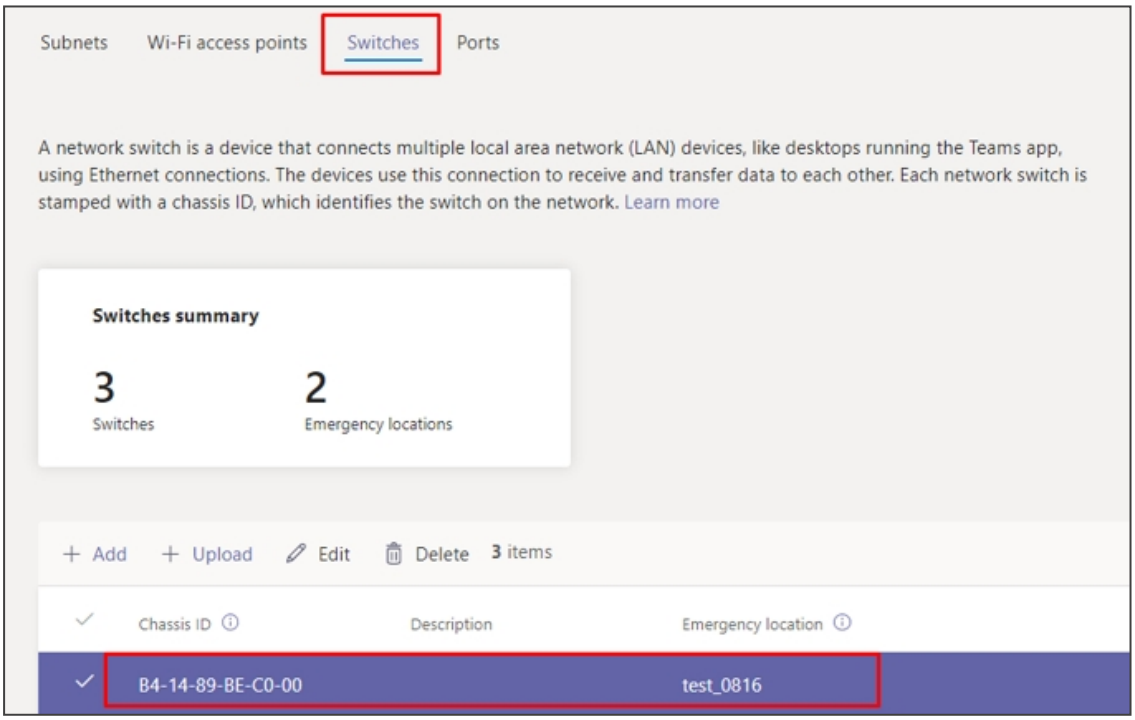


7. Define a location by subnet. The location can be defined like switch ID (if in charge of several buildings, since it reflects a perimeter or an area).

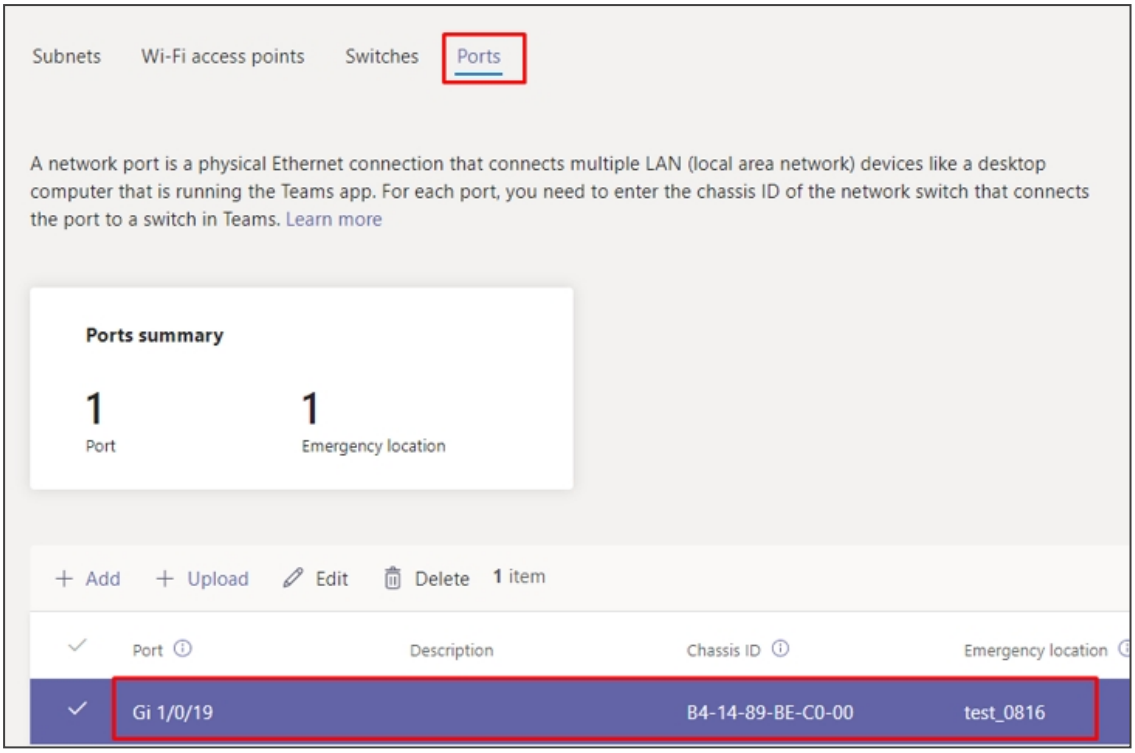


8. Verify all settings have been implemented correctly, under the **Networks & locations** tab.





9. Verify all settings have been implemented correctly, under the **Networks & locations** tab.



After a location has been defined, make sure that:

- AudioCodes' phone runs the latest firmware released.
- AudioCodes' phone runs the Teams app issued June 2022 and later (U3-A and higher).
- 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.

Setting 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.

Enabling 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, admin 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:

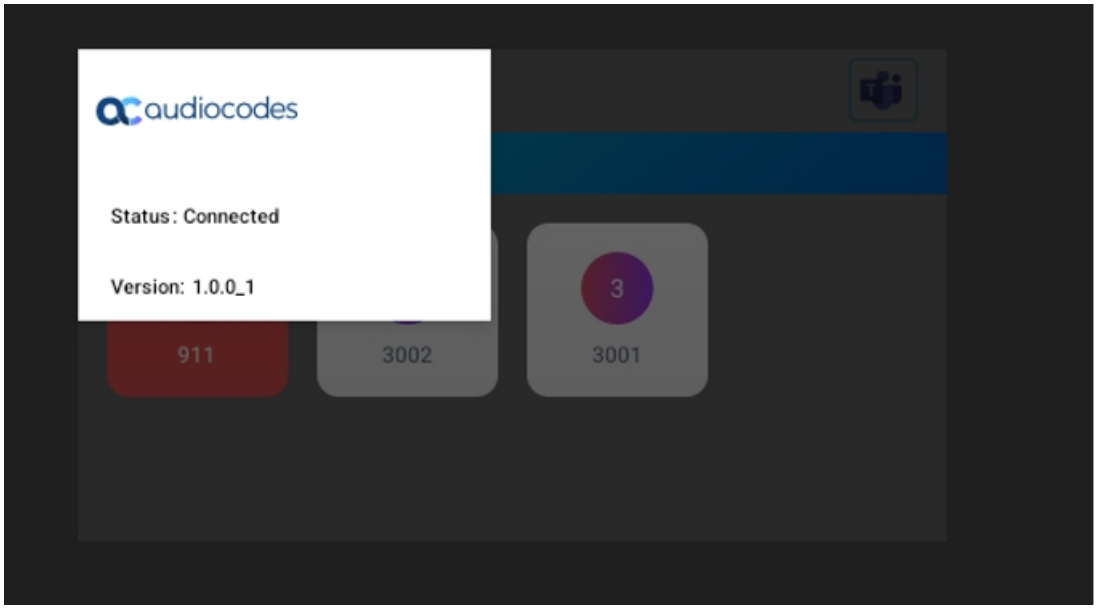


➢ **To register a SIP account (sign in), admin must:**

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 'Connected' if the account status is registered. View 'Not Connected' if the account status is 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.
- Press the **AudioCodes Smart** button on the phone as shown below (only when parameter 'system/ace/minilauncher_enabled' is set to **1**) to switch between Teams and the app.



➢ To add (up to) 41 speed dial keys, admin must:

1. Use the following parameters:
   - personal_settings/functional_key/[0-40]/speed_dial_number= "the 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"

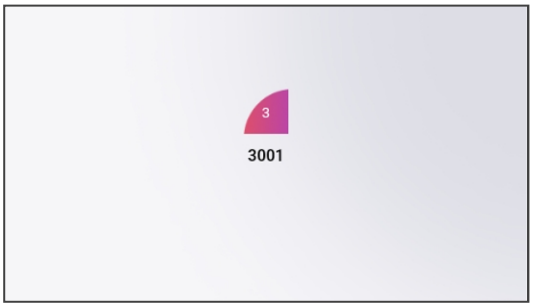


➢ To make a call, the user must:

1. Press the speed dial; the calling screen shows the callee's name. To end the call, on-hook the handset or press the speaker/headset 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.

Applying a Partial Configuration Profile

Configuration profiles enable admin 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.

When admin 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. Admin can change a particular setting without overriding the other setting values defined by the user.

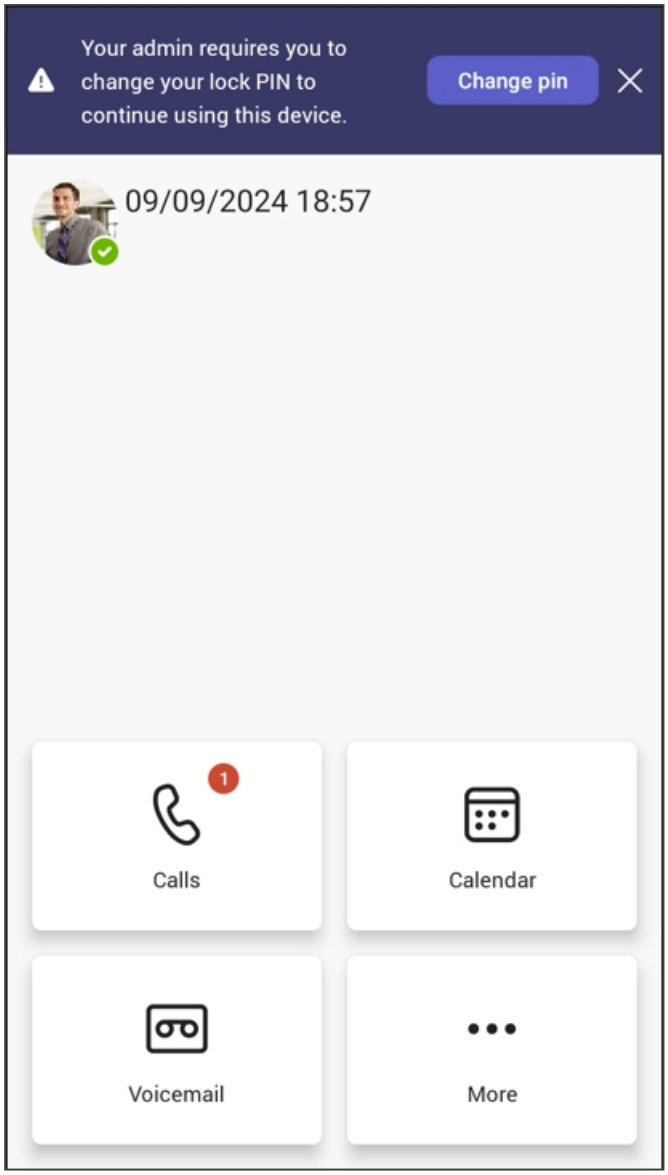
Configuring an Option to Force Users to Change their Device Lock PIN

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

➢ **To force users to update their device lock PIN admin must:**

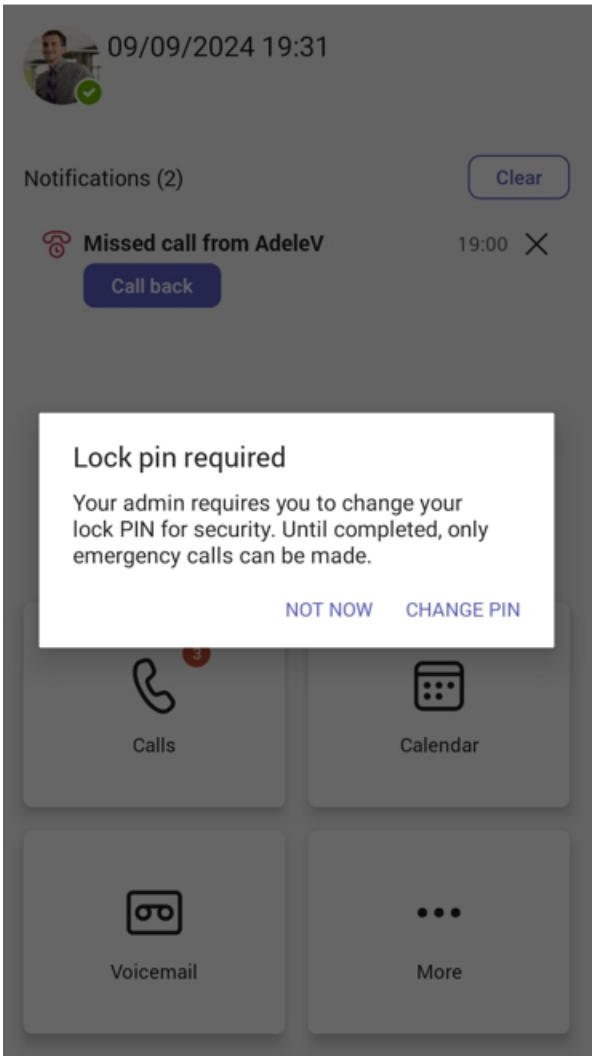
1. Configure the configuration file parameter 'forceChangePIN'.

```
System Config
Lock PIN: 123445
Device Lock Timeout: 600
Date Time Config: test
```



- The same principle applies across all phone models, only the screen dimensions change.
- The configuration option is received as part of the configuration profile settings assigned to the device.
- Once timeout configured by admin lapses, firmware locks the device.

2. When the Teams app detects a PIN lock configuration where a force PIN configuration is toggled, a popup is displayed allowing the user to navigate to device lock settings to change the PIN.



3. If the user clicks 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.

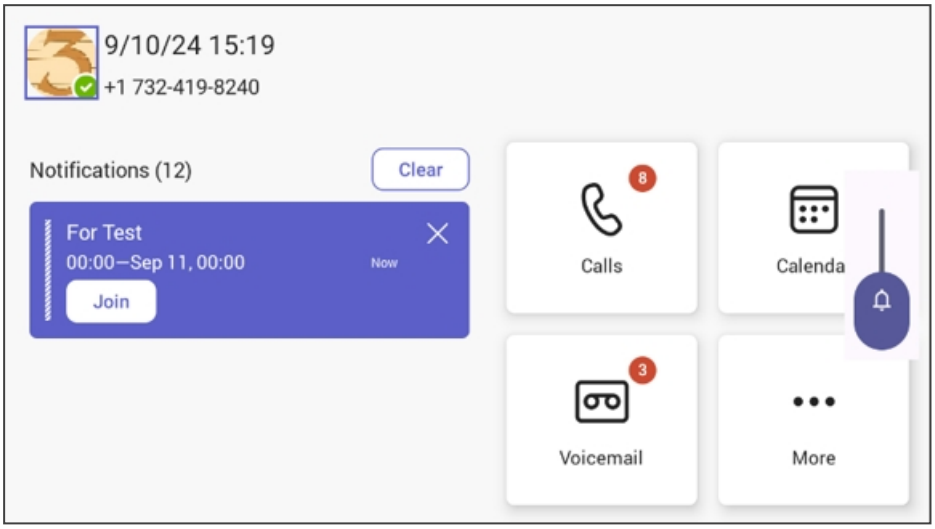
Configuring Minimum and Maximum Ringer Volumes via the Phone's Configuration File

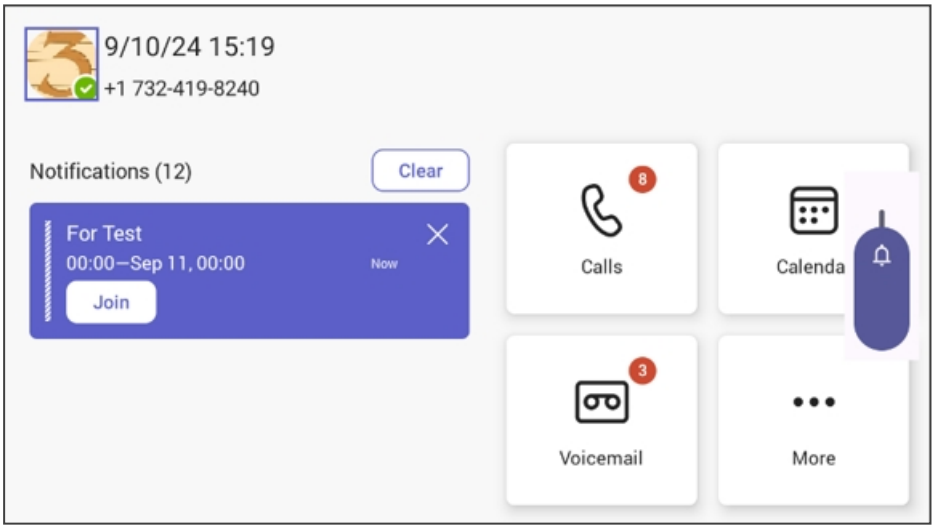
Android phones feature a capability enabling admin to configure minimum and maximum ringer volumes via the phone's configuration file. The feature complies with industrial customers' requirements for phone ringers to be louder and for admin to be able to stop users from reducing ringer volume to too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





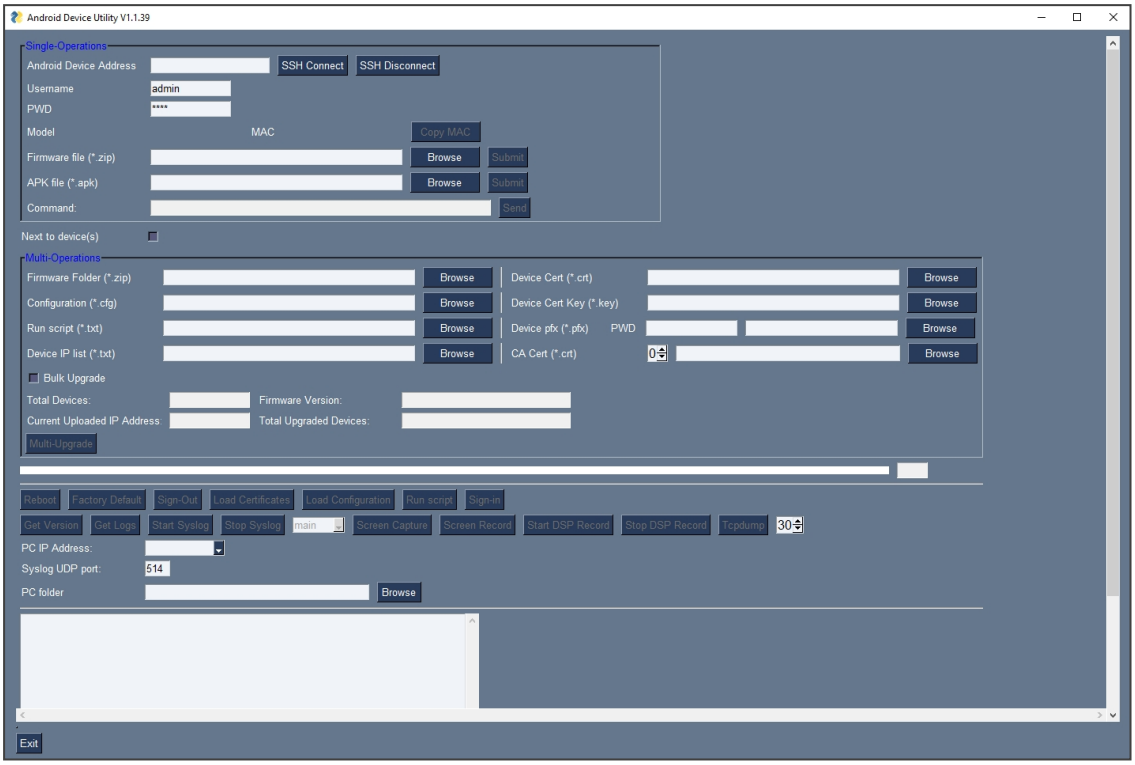
Updating Phone Firmware Manually

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

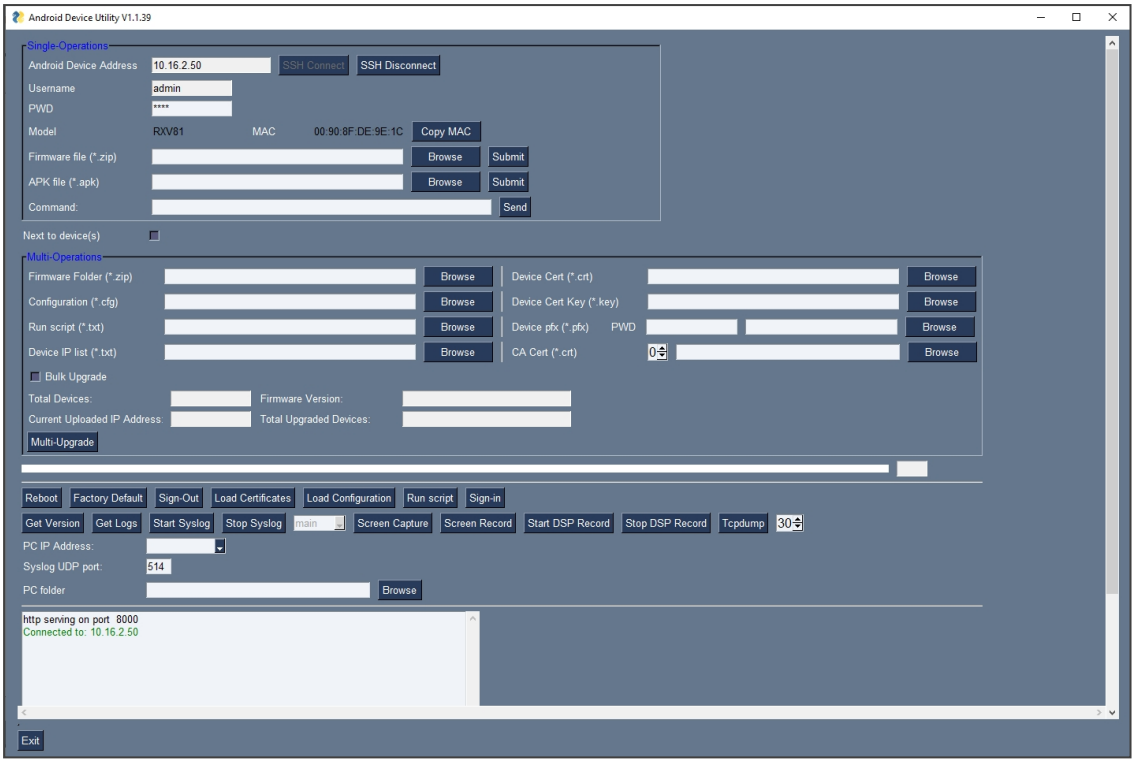
- Firmware downgrade is blocked as of version 2.3.453 to prevent a possible race condition between Microsoft TAC and AudioCodes' OVOC | Device Manager.

➢ 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.

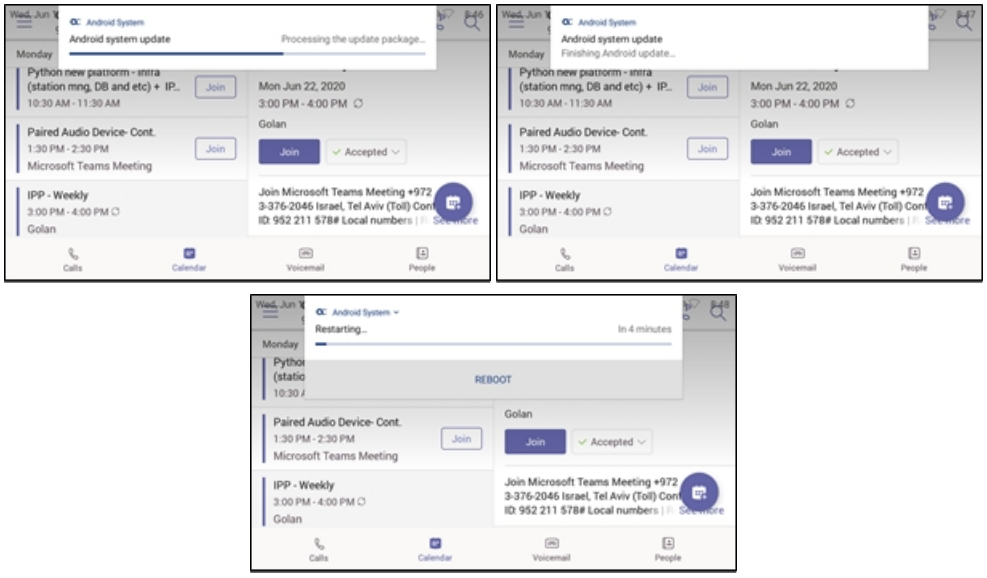


2. In the 'Android Phone Address' field, enter the IP address of the device (get it by pressing the MENU hard key > **About phone** > **Status** > **IP Address**).
3. Click **SSH Connect**; a connection with the device is established.



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.



The above is also displayed when the phone is upgraded remotely from Microsoft Admin Portal or from AudioCodes' Device Manager.

Loading Certificates to Phones

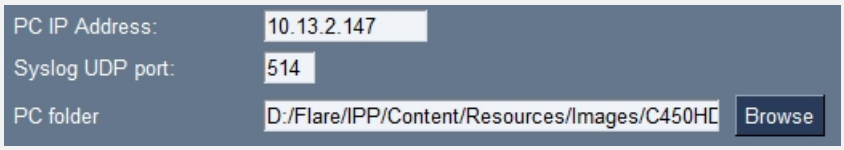
The following shows how to load user certificates to a single device and to multiple devices. Before loading certificates, put the certificate files in a designated folder.

Certificates can be downloaded using:

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



- 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 _

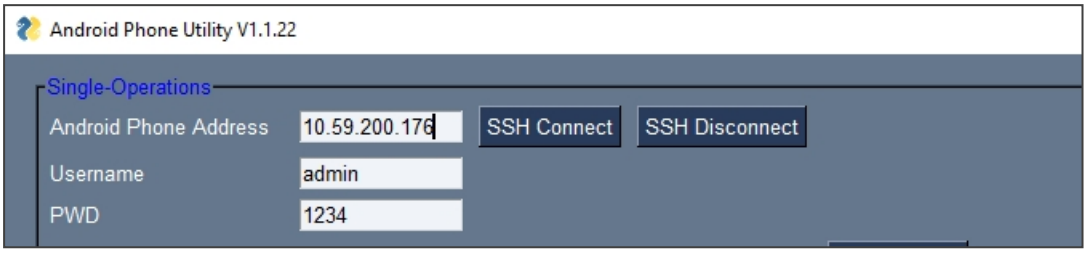
- The CA certificate (ca_cert) can also be loaded to devices using AudioCodes' Device Manager, in the 'Template' screen.
- Certificate loading is performed using HTTP. Prior to version 1.19, it was performed using SCP. The HTTP port is 8000. Make sure the port is not blocked by the organization's firewall.

AudioCodes Android Device Utility

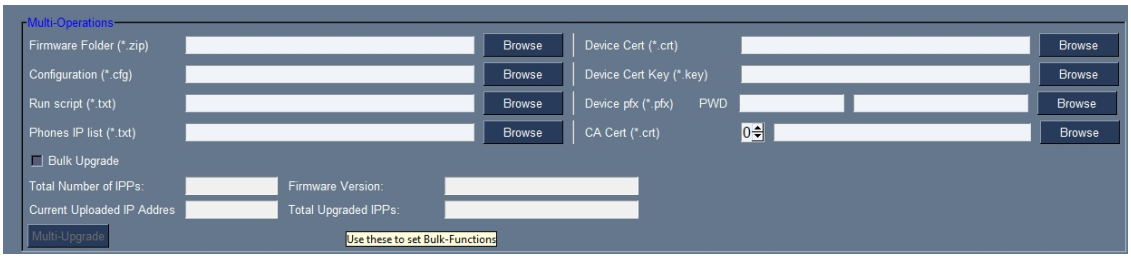
Certificates can be loaded to a phone or to multiple phones using AudioCodes' Android Device Utility.

➢ To load certificates to a single device:

1. In the Android Device Utility (see Android Device Utility on page 106 for detailed information about the application), enter the phone's IP address and click **SSH Connect** shown in the next figure.

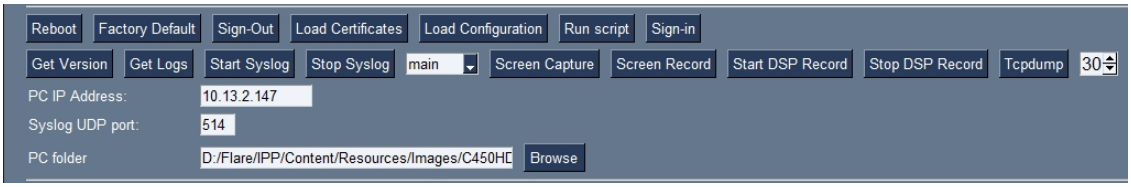


2. Click the**Browse** button next to the field 'Device Cert' shown in the next figure and then navigate to and select the certificate file to download.



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

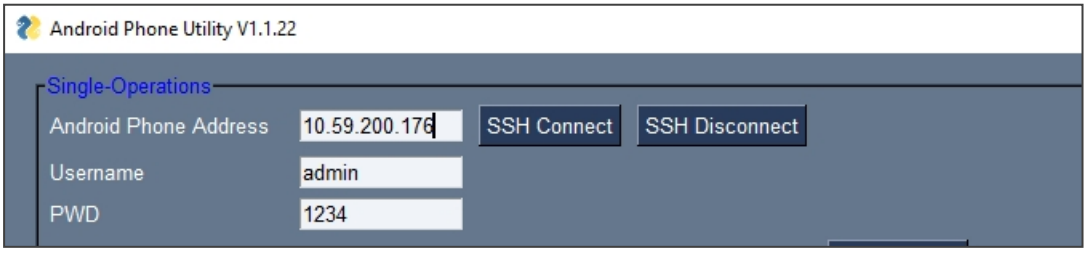
3. Click the **Load Certificates** button shown in the next figure, to add the certificate.



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

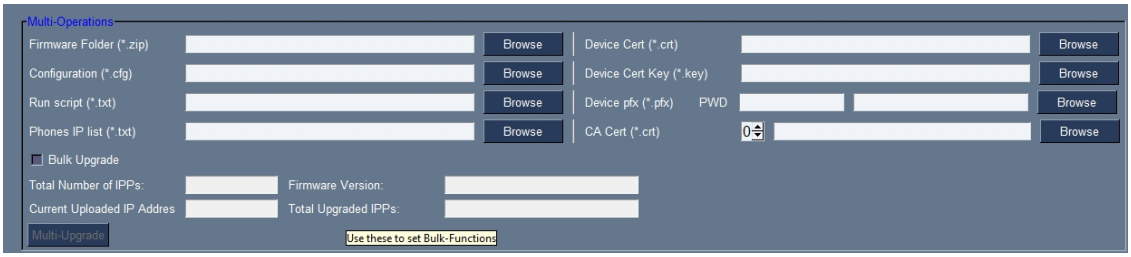
➢ To load certificates to multiple devices:

1. In the Android Device Utility (see Android Device Utility on page 106 for more information), enter the phone's IP address and click **SSH Connect**.



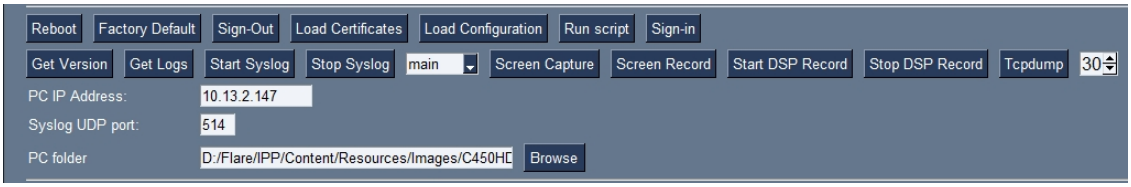
The loaded certificate's file name must be without spaces. Spaces between words can be created using an underscore _

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. Network admins must set its value to (for example): 3EBE50003ABF1DF5E6B5A3230B02B856
security/SCEPEnroll/password_ challenge	Define the enrollment challenge password. Default value: NULL. Network admins must set its value to (for example): 7A7F9FC4BB7625F0935E67EA6D6322ED
security/SCEPServerURL	Define the 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 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

Parameter	Description
security/CSR/Country	Define the name of the country used to generate the certificate signing request (CSR). Note: The ISO (International Organization for Standardization) code of the country / region in which the organization is located.
security/CSR/Email	Optionally, define the email address used to generate the CSR.
security/CSR/Organization	Optionally, define the legal name of the organization used to generate the CSR.
security/CSR/State	Optionally, define the name of the state / province used to generate the CSR.

Manually Performing 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.

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

When?	Action	Press key combination	LED flashes 3x after release
Start pressing immediately after power up (on U-Boot / Universal Boot Loader)	Switch slots A / B	**4** key + **6** key (3 seconds)	Green
	Loader	**1** key + **3** key (3 seconds)	Blue / Yellow

When?	Action	Press key combination	LED flashes 3x after release
	Switch Skype for Business to Android (and vice versa)	Back key + **OK** key (3 seconds)	Red + Green
	Restore defaults	**OK** key + **MENU** key (3 seconds)	Green + blue / Green + yellow
When successfully booted (on Android)	Reboot	From the 'Admin' menu	-
	Restore defaults	Long-press **Hold** key for ~15 seconds	Flashes white once after release

Enrolling a Device with Intune Policies

Two ways to enroll an AudioCodes Teams Android-based device in Intune:

- Create a dynamic group - see here
- Create an exclusion group - see here

Creating a Dynamic Group

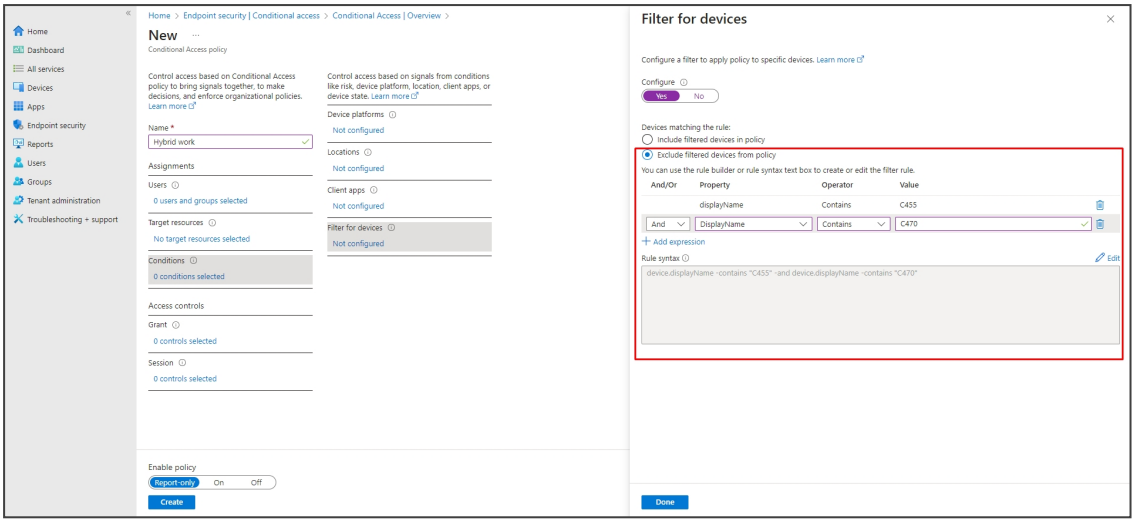
See here how to create dynamic groups in Intune for enrolling AudioCodes Android-based Teams devices.

Creating an Exclusion Group

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

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

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

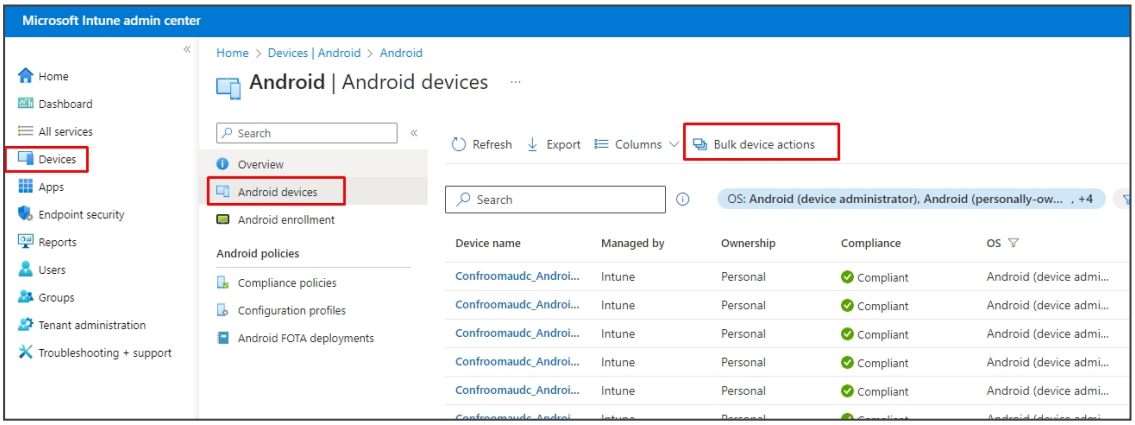


Removing Devices from Intune admin center

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

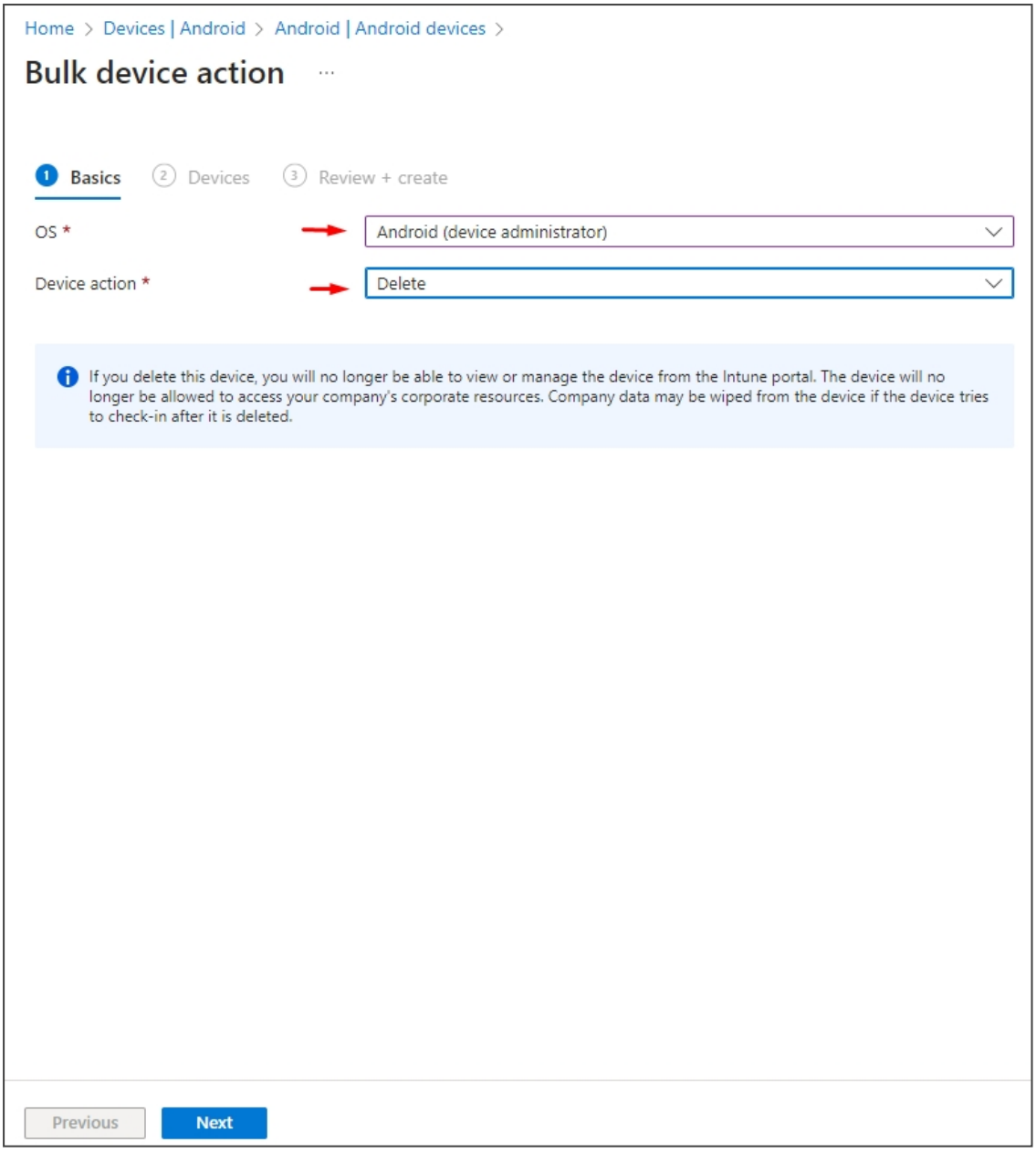
➢ To remove devices from Intune admin center:

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

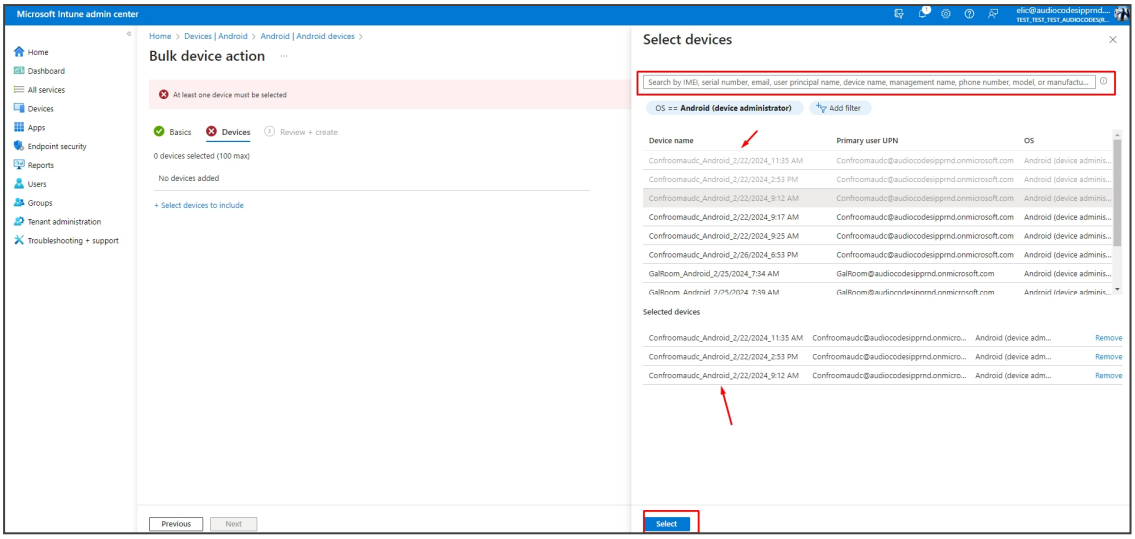


> The Intune admin center service is licensed according to the terms of individual licenses so not all network admins will be able to navigate to it. Check if the license you're using includes the service or not.

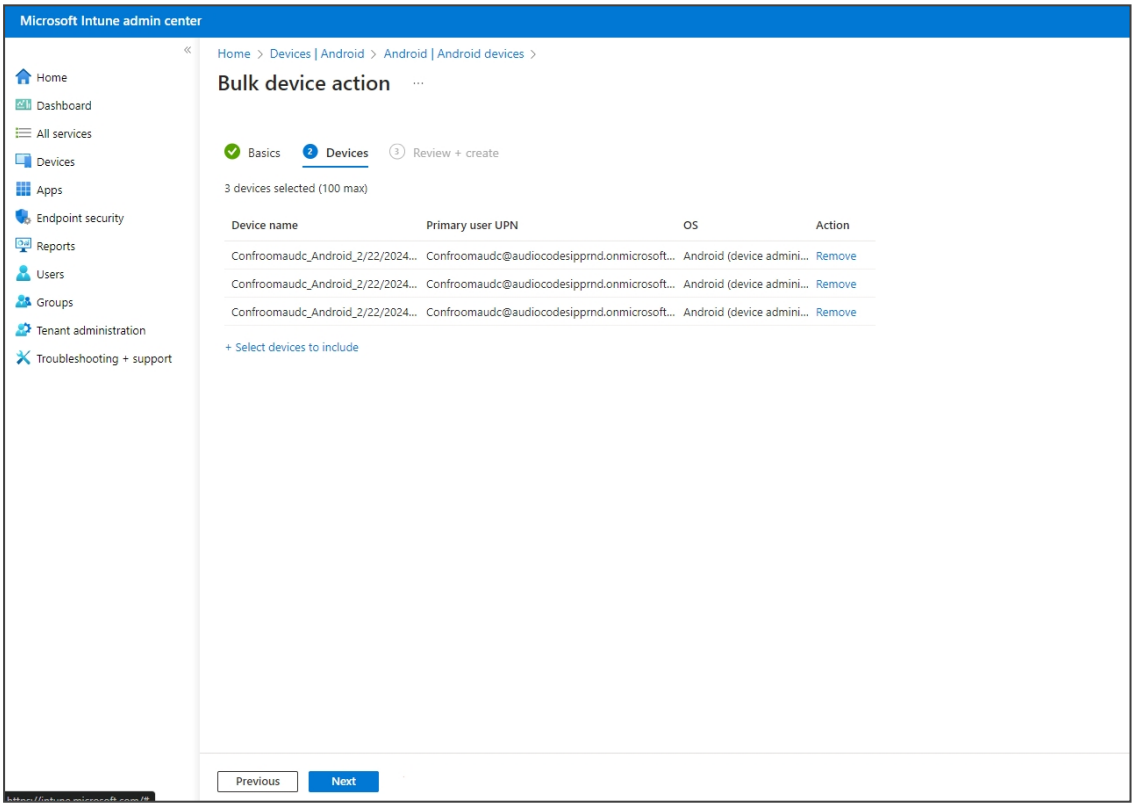
3. Click **Bulk device actions**.



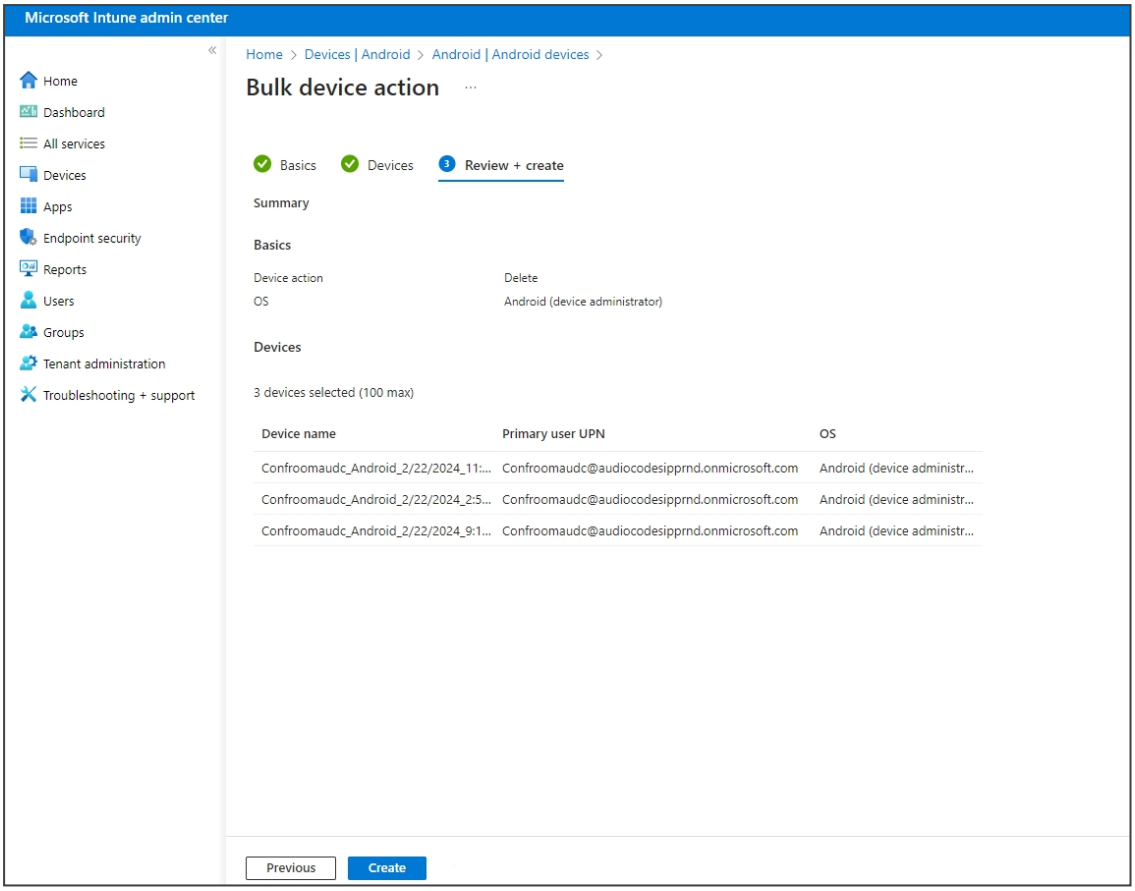
4. From the 'OS' drop-down under the ❶ **Basics** tab, select **Android (device administrator)**. From the 'Device action' drop-down, select **Delete**. Click **Next**.



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



6. Under the 2 **Devices** tab, click **Next**.



7. Under the 3 **Review + Create** tab, make sure your definitions are correct and then click **Create**; admin receives a notification that a delete action from Intune was successfully initiated on all devices and that *n* devices were removed.

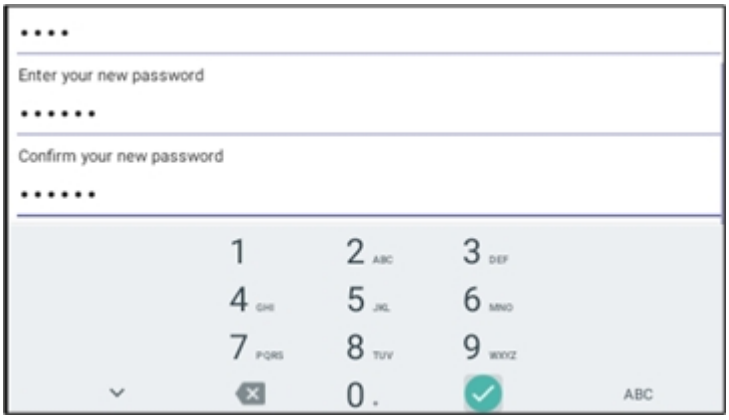
> It may take some time to completely sync the devices with the account so after deleting the devices wait for 30 minutes before signing in.

Updating Microsoft Teams Devices Remotely

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

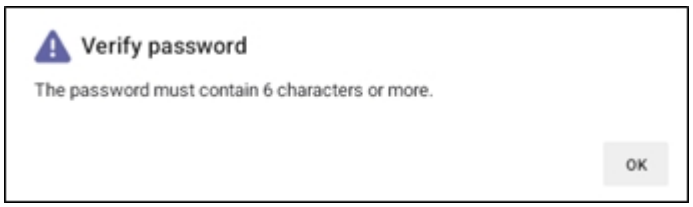
Defining Password Complexity

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 admin with the capability to finely adjust password complexity, ensuring that customers using low-cost phones (LCPs) can easily input passwords using the phone's hard keys.

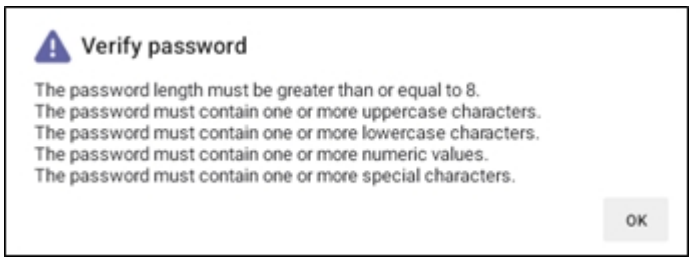


Admin can set password complexity using the cfg configuration file parameter 'system/admin_password/strength'.

- 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.
- Admin can optionally change it to a *non-complex* password.

Disabling 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 admins can 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.

Disabling 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.

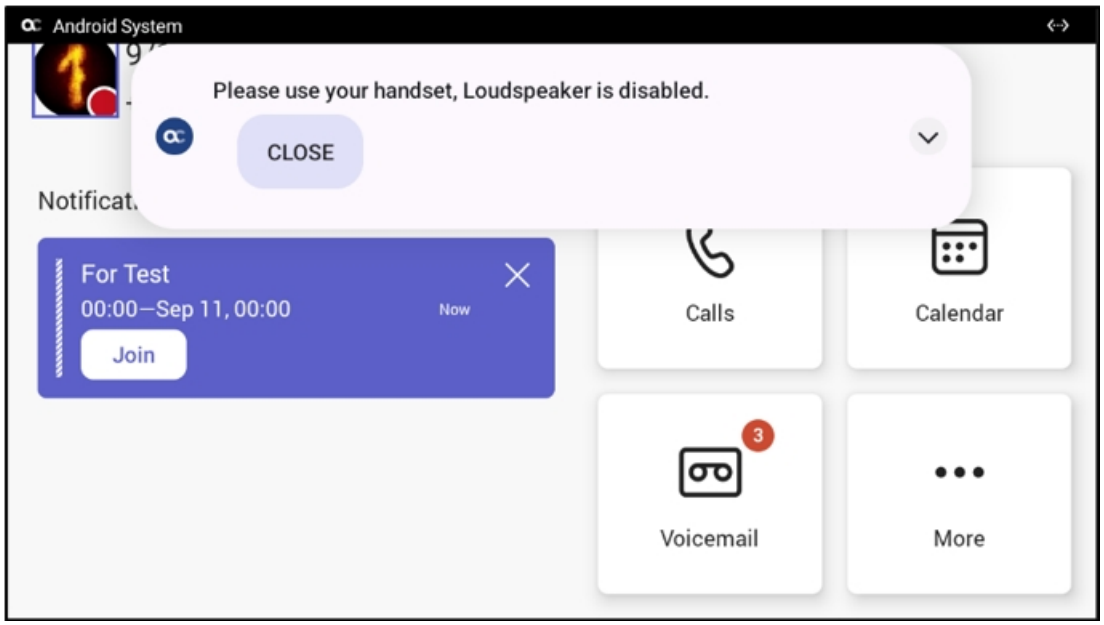
The feature complies with requests from customers in whose offices discretion is important (e.g., government).

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

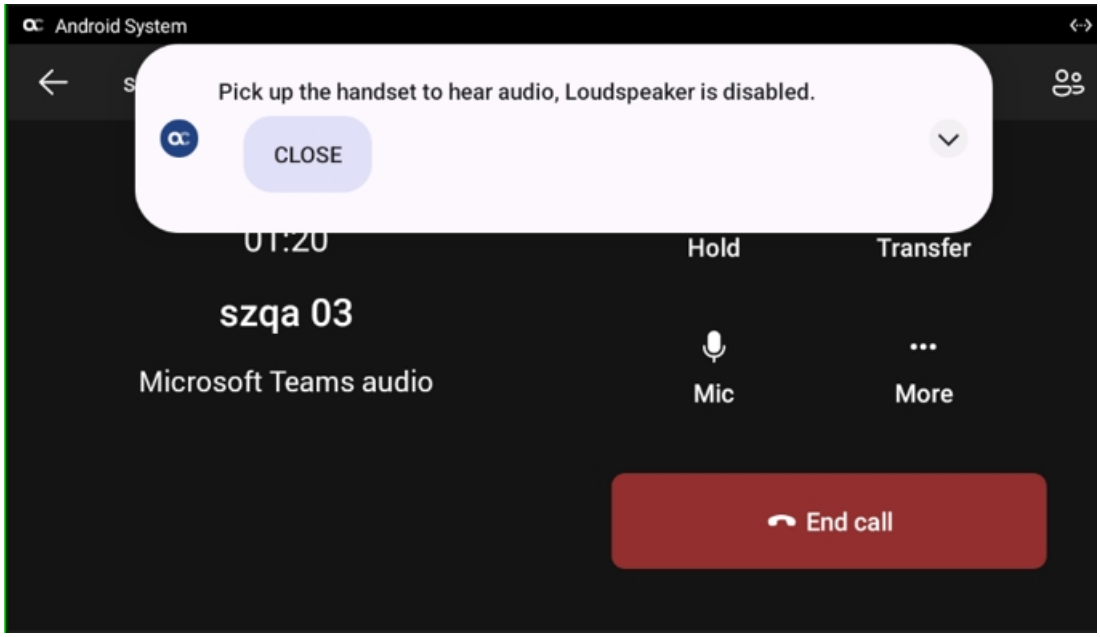
1. Configure the configuration file parameter 'audio/speakerphone/enable' to:
   - **0** = Disable (default)
   - **1** = Enable

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.

Enabling AudioCodes Smart Button for Redial Functionality

The phone's **AudioCodes Smart** button is programmable to function as a redial button.

Enabling this functionality is done through SSH, using the following command:

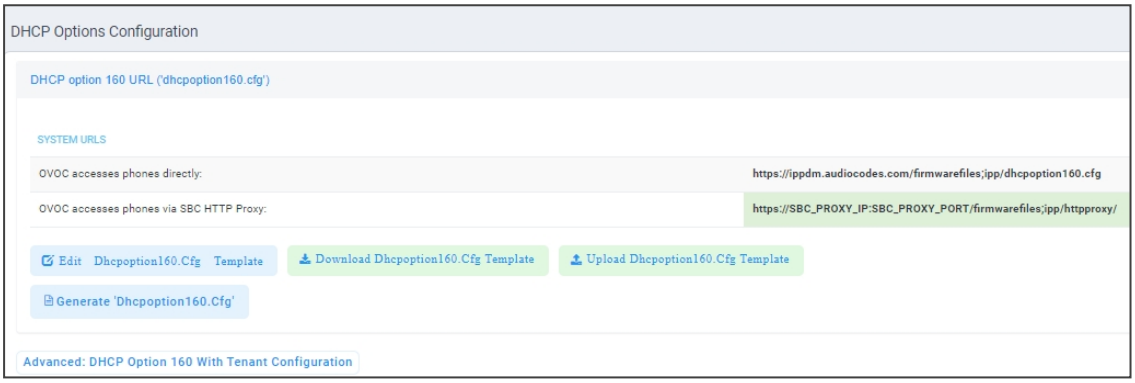
```
personal_settings/audiocodes_key_to_redial/enabled=1
```

Managing 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 6-1: 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, they're allocated to tenants by selecting **Change Tenant** in the 'Actions' menu. Unless already used, it's recommended to leave the default tenant as a 'lobby' for the new devices. 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

Actions that go beyond the devices' periodic provisioning cycle will be supported in next releases. The **Check Status** option is irrelevant for Android-based Teams devices therefore it's omitted from the 'Actions' menu.



- 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.

Configuring 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 6-2: 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 (see Supported Parameters on the next page) that further defines the selected frequency.

Managing 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**

Supported Parameters

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

- general/silent_mode = 0 (default)/1
- general/power_saving = 0 (default)/1
- phone_lock/enabled = 0 (default)/1
- phone_lock/timeout = 900 (default) (in units of seconds)
- phone_lock/lock_pin = 123456
- display/language = English (default)
- display/screensaver_enabled = 0/1
- display/screensaver_timeout = 1800 (seconds)
- display/backlight = 80 (0-100)
- display/high_contrast = 0 (default) /1
- date_time/timezone = 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

Configuring Time Zone on Teams Devices

- AudioCodes recommends using Geolocation as the time zone configuration method.
- Geolocation is the default setting, 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)**:
  - Configuration is obtained from DHCP server.
- **Admin Provisioning**:

  Use one of the following:
  - Teams Admin Center, created under configuration profile.
  - Device Manager, created in configuration parameters setup.

The supported parameters for Device Manager configuration can be found in product specific Admin and User guides. For Teams Admin Center refer to Microsoft documentation > Configuration profile.

Configuring QoS on PC Port

QoS settings for the PC port are supported (VLAN for PC port). Admin can configure PC port QoS via the device's cfg configuration file which can be loaded to the device via (for example) AudioCodes' 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
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.

Configuring Admin Login Timeout

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

settings/admin_logout_timeout,values=3

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



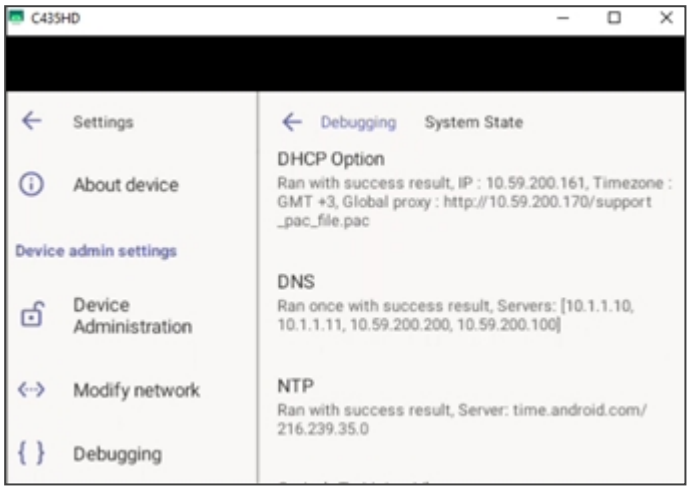
- The cfg file can be loaded to the device using Device Manager.
- Timing begins when exiting the 'Device Settings' menu.
- When the timeout expires, the device logs out automatically.
- The functionality works for both registered and unregistered devices.

Monitoring Phone Process Statuses

Admin can monitor process statuses in the phone's System State screen.

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

The figure below shows the System State screen (**Settings** > **Debugging** > **System State**).



7 Troubleshooting

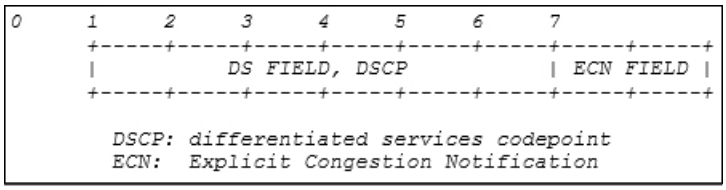
The information presented here shows how to troubleshoot AudioCodes devices.

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 7-1: DS Field, DSCP



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

See also Microsoft's website for more information.

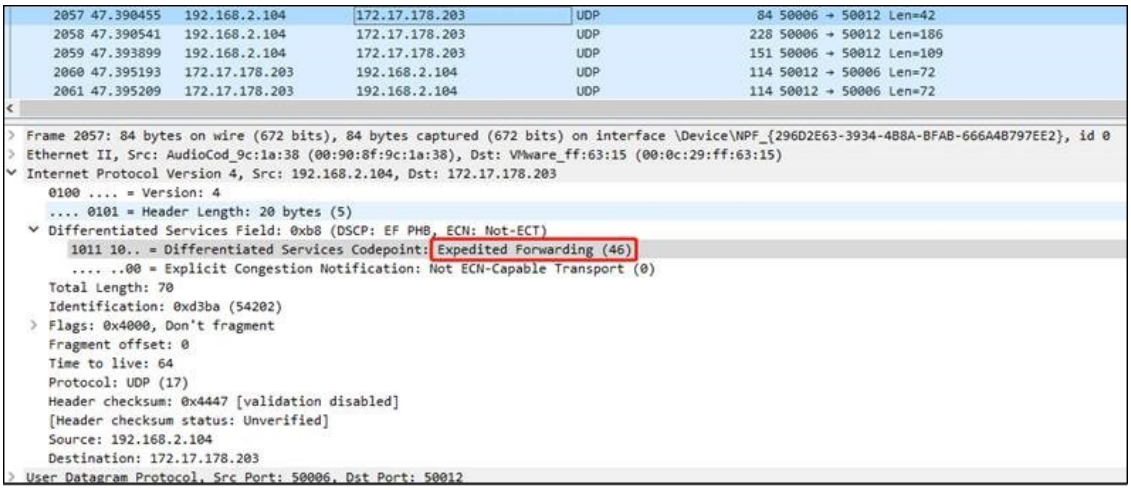
> The DSCP value can be adjusted *on the server*; it cannot be adjusted on the client. See the figures below for recommended values.

Figure 7-2: 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 7-3: Audio



Users

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

Table 7-1: Troubleshooting

Symptom	Problem	Corrective Procedure
Phone is off (no screen displays and LEDs)	Phone is not receiving power	■ 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. ■ If using Power over Ethernet (PoE), contact your network administrator to check that the switch is powering the phone.
Phone is not ringing	Ring volume is set too low	■ Increase the volume (see Adjusting Ring Volume on page 63)
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 of the phone. ■ Make sure the headset volume level is adjusted adequately (see Adjusting Headset Volume on page 64).

Exporting 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.

Network Administrators

Network admins can troubleshoot telephony issues in their IP networks using the following as reference.

Android Device Utility

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



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

AudioCodes provides admins with an SSH-based Android Device Utility.

➢ **To sign in to the utility:**

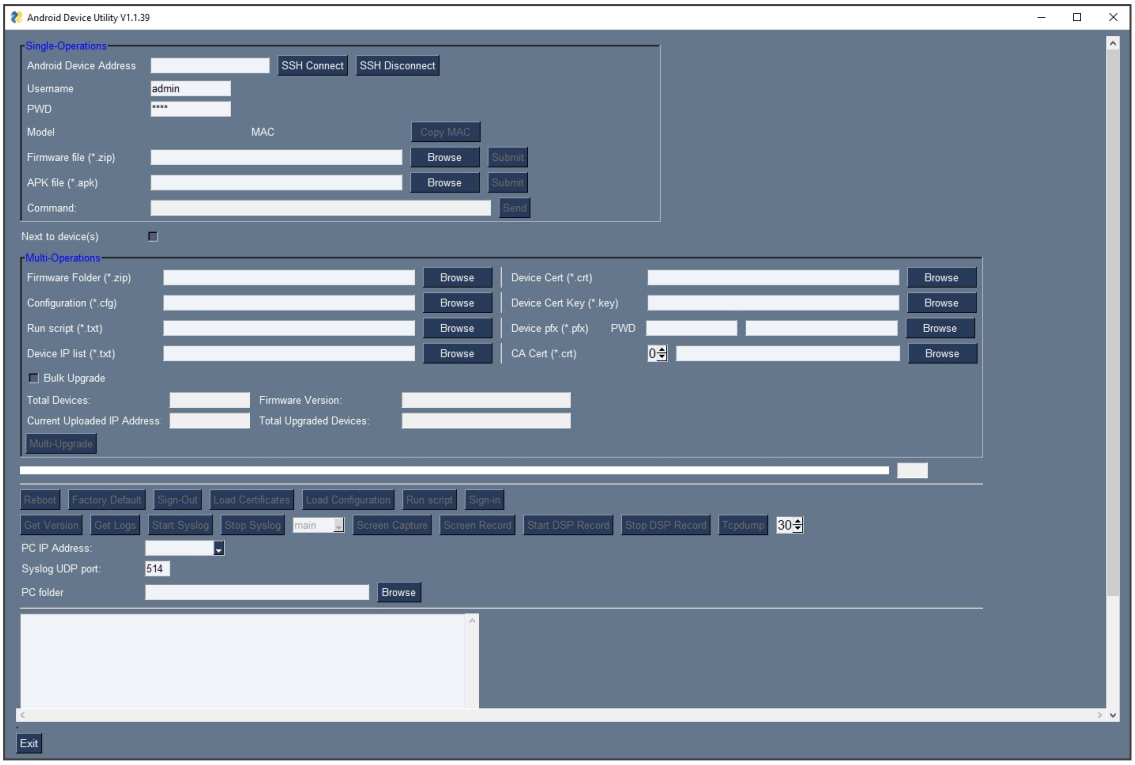
- Enter your username and password; **admin** and **1234** are the defaults.

The application gives network administrators the following debugging capabilities:

- Capturing the Phone Screen on page 108
- Running Tcpdump on page 109
- Getting Information about Phones on page 110
- Remote Logging (Syslog) on page 111
- Getting Diagnostics on page 113
- Getting Logs on page 114
- Activating DSP Recording on page 115
- Deactivating DSP Recording on page 116
- Getting Information about Phones on page 110

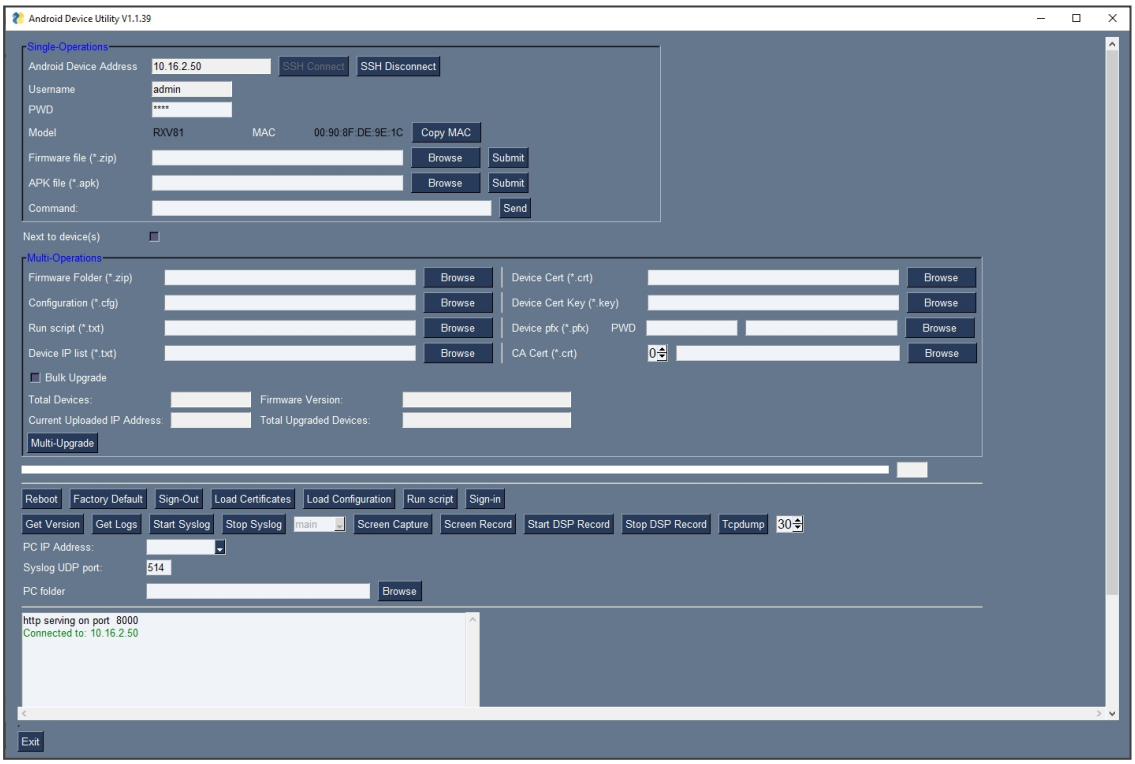
➢ **To open the utility:**

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 pressing the MENU hard key > **About phone** > **Status** > **IP Address**).

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



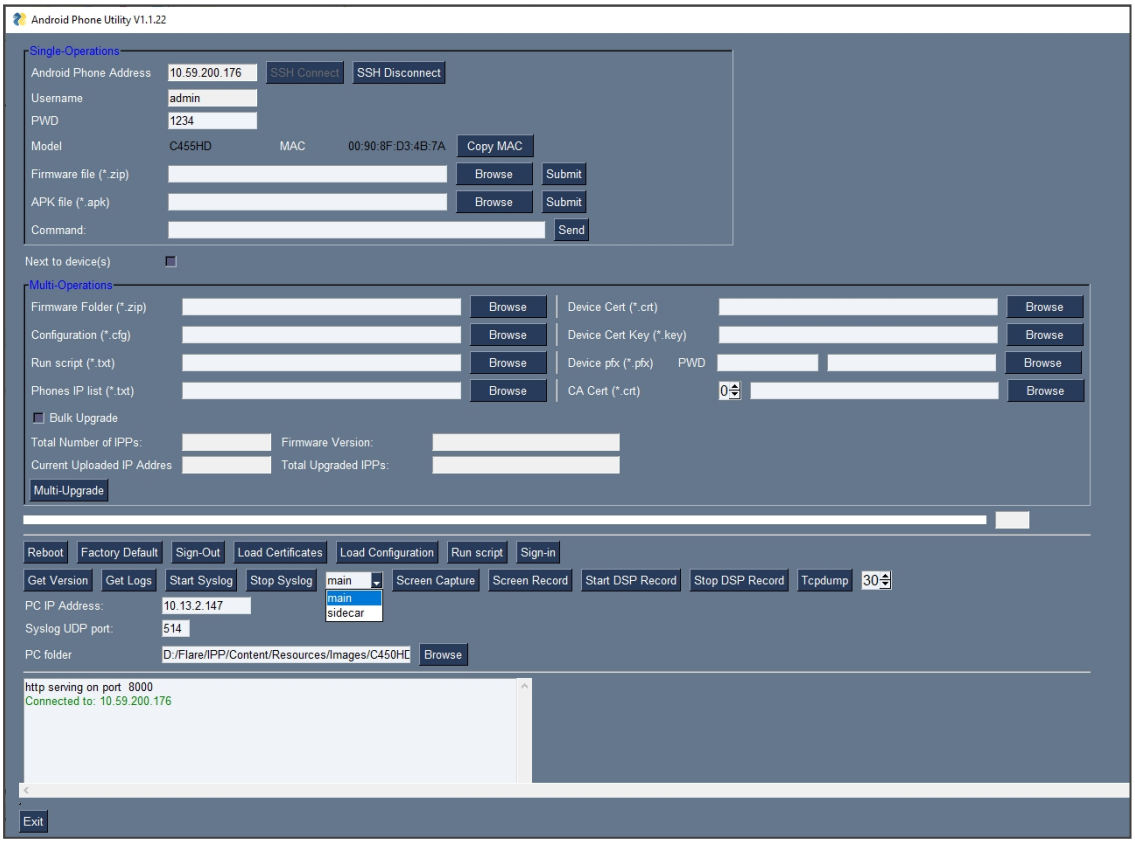
4. Next to the field 'PC folder', click the **Browse** button and navigate to and select the folder to which to send data to use for debugging.

Capturing the Phone Screen

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 pressing the MENU hard key > **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.

Running 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 106 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%
```

Getting 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 106 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
```

Remote Logging (Syslog)

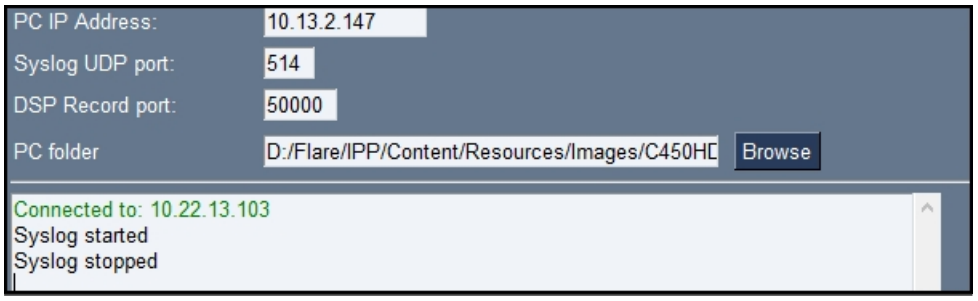
Remote Logging via Syslog provides the same log level as Device Diagnostics (performed via the Microsoft Teams Admin Center) with some additional information that may be relevant to device issues (not Teams application issues). Device Diagnostics via the Microsoft Admin Center are saved to the device 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

- Android Device Utility on page 106
- on the next page

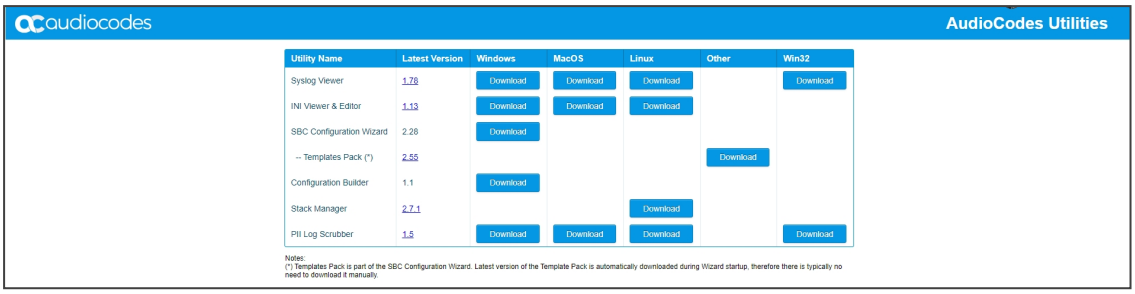
➢ To enable Remote Logging via Syslog from the utility:

1. In the Android Device Utility (see Android Device Utility on page 106 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.



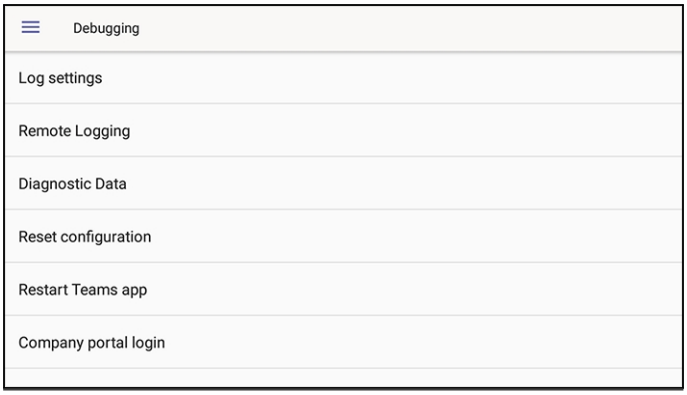
3. Open the folder on the PC to which you commanded the application to send the information, and then locate the Syslog file.

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**.



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 ""
```

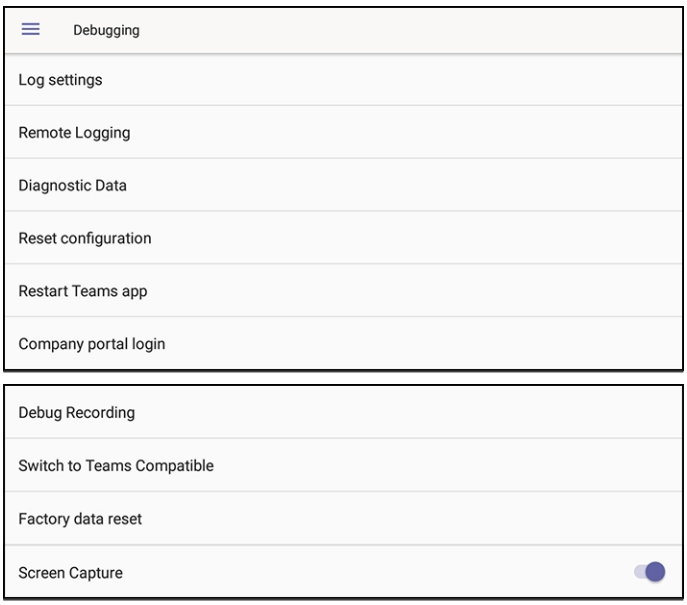
Getting Diagnostics

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:

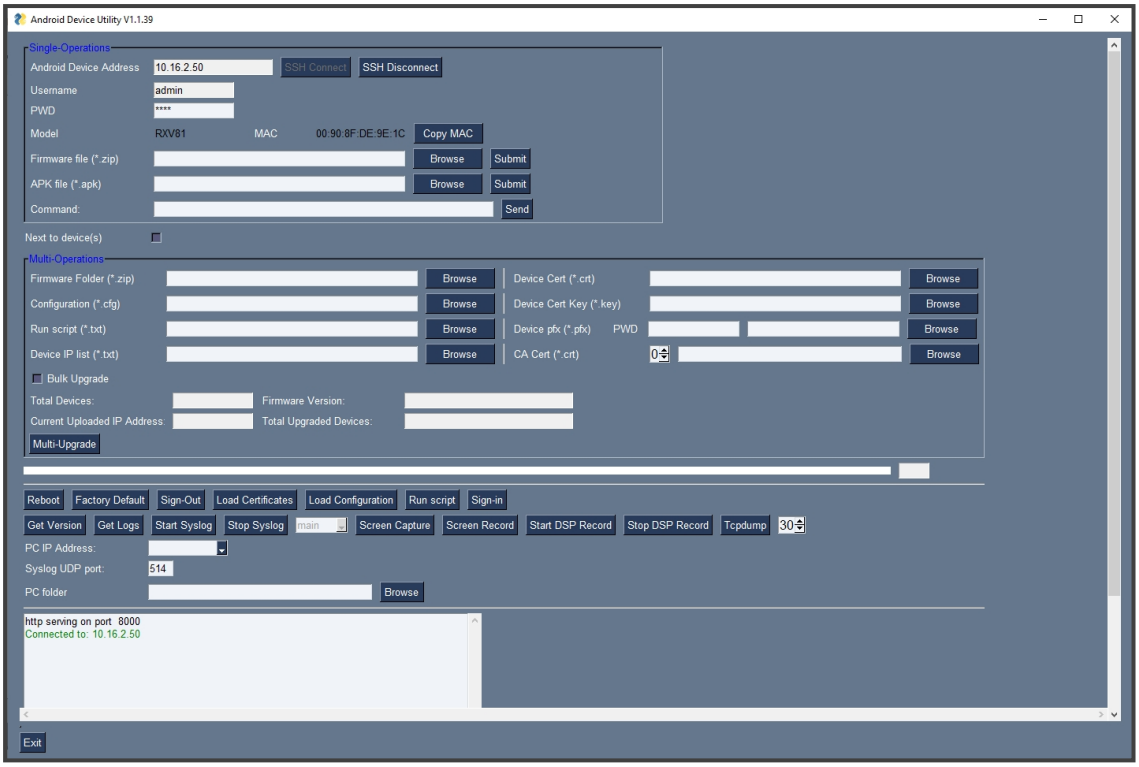
- dmesg.log
- dumpstate-c470hd-1.18.117_58793-41-undated-dumpstate_log-3458.txt
- dumpstate-c470hd-1.18.117_58793-41-undated.txt
- dumpstate-stats.txt
- logcat.log

Getting Logs

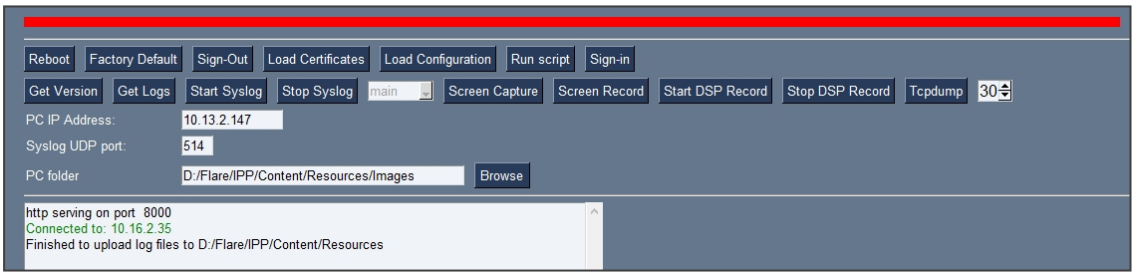
Network administrators can get bug report logs, including a logcat file and a configuration file, to expedite debugging.

➢ To get logs:

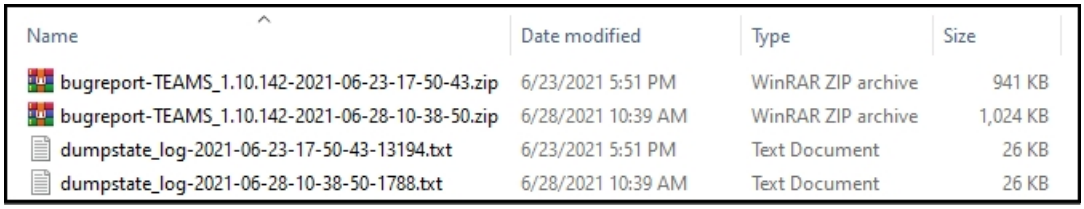
1. In the AudioCodes Android Device Utility (seeAndroid Device Utility on page 106 for more information about the application), enter the phone's IP address, click **SSH Connect** and browse to a folder on the PC to which to send the information.



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.



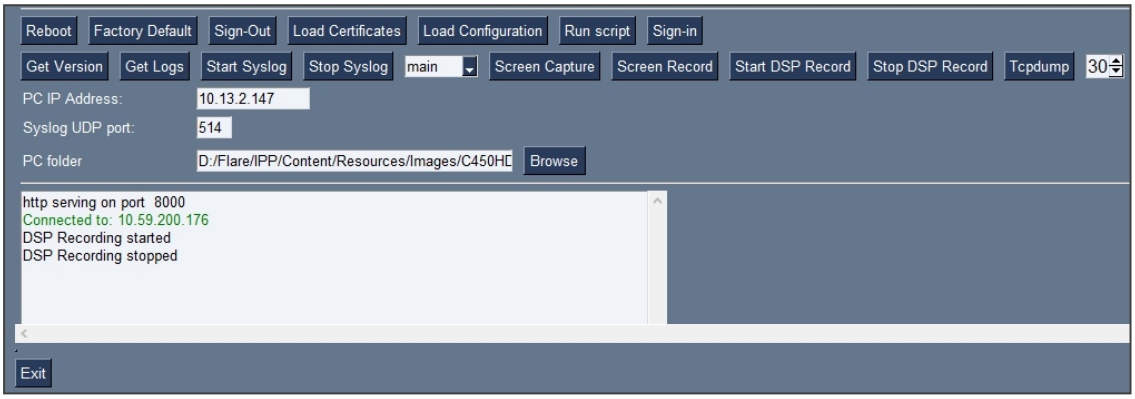
4. Unzip the zipped files and open the txt files to view the report.

Activating DSP Recording

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

➢ **To activate DSP Recording:**

1. In the AudioCodes Android Device Utility (see Android Device Utility on page 106 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 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:**

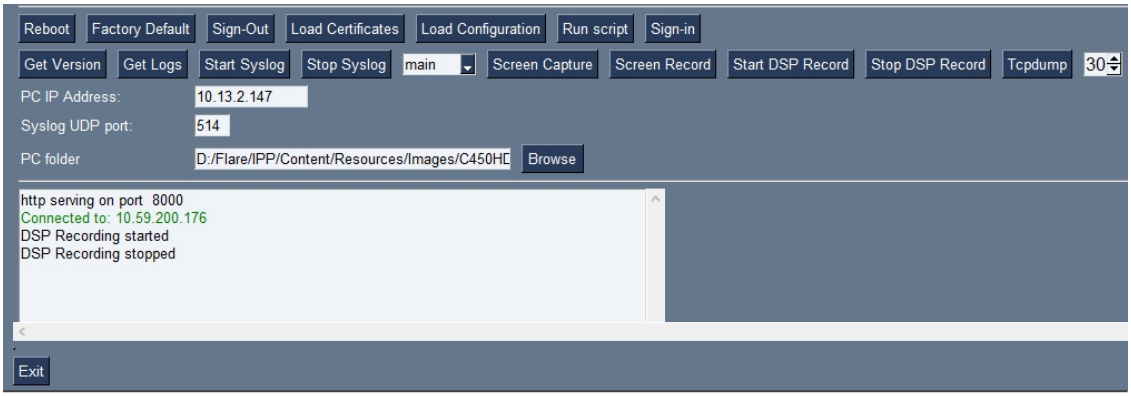
DSP recording can be activated on the fly without requiring the network administrator to reset the phone.

Deactivating DSP Recording

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

➢ **To deactivate DSP Recording:**

1. In the utility (see Android Device Utility on page 106 for more information about the application), click **Stop DSP Record** after a period of recording (see Activating DSP Recording on the previous page for information on how to start DSP recording).



2. View the DSP recording in the PC folder you configured when Activating DSP Recording on page 115.

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

➢ **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 deactivated on the fly without requiring the network administrator to reset the phone.

SSH

The phone can be accessed via Secure Shell (SSH) cryptographic network protocol after the network administrator signs in.

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

To sign in, the administrator needs to know their username and password; **admin** and **1234** are the defaults.

- The default password must be changed before access to the device via SSH is allowed.
- The default password can be changed per device in the phone screen, or via bulk configuration of multiple devices using Microsoft's TAC or AudioCodes' Device Manager.
- After entering a password, the user is prompted to verify it. Criteria required for a strong password are provided: The password length must be greater than or equal to 8. The password must contain one or more uppercase characters. The password must contain one or more lowercase characters. The password must contain one or more numeric values. The password must contain one or more special characters.

SSH access allows administrators debugging capabilities such as:

- Getting the Phone IP Address below
- Pulling files from the phone sdcard (using the curl command)
- Activating DSP Recording on page 115
- Deactivating DSP Recording on page 116
- Installing the APK using SSH below

Getting the Phone IP Address

Network administrators can get a phone's IP address using SSH protocol.

➢ **To get the phone's IP address using SSH protocol, type the following at the shell prompt:**

```
ifconfig
```

Installing the APK using SSH

Network administrators can install the Teams Android Application Package using SSH protocol.

Updating Phones using SSH Commands

➢ **To upgrade firmware:**

1. Download the required firmware version to **sdcard/update_image.zip**.

   For example, use the following:

   ```
   SCP <file name> admin@<DeviceIP>:/sdcard/update_image.zip
   ```

2. Update the firmware using the following:

   ```
   setprop ctl.start local_update
   ```

3. Track progress using the following:

```
logcat | grep  update_engine_client_android
```

➢ To upgrade the Android Package Kit (APK):

1. Download the required APK to sdcard/teams.apk

   For example use the following:

```
SCP <file name> admin@<DeviceIP>>:/sdcard/teams.apk
```

2. Update the APK using the following:

```
pm install -r -g /sdcard/<filename>
```

3. Delete the old APK using the following:

```
pm uninstall com.microsoft.skype.teams.ipphone
```



If the new APK is older than the existing one, delete the existing APK before installing the new one.

➢ To collect logs:

1. Collect logs using the following:

```
param_tool scp command/bugreport 1
```

2. Wait until the logs are created (see in /sdcard/logs/bugreports/ that there is a .gz file)
3. Get the logs from the "/sdcard/logs/bugreports/" folder.

   For example, use the following:

```
SCP admin@<DeviceIP>:/sdcard/logs/bugreports/<log file name>
C:\<destination Directory>
```

➢ To install the Client Certificate:

1. Download certificates to /sdcard/devcert/
2. Install the certificate using the following:

```
setprop ctl.start sdcard_certs_install.
```

Microsoft Teams Admin Center

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

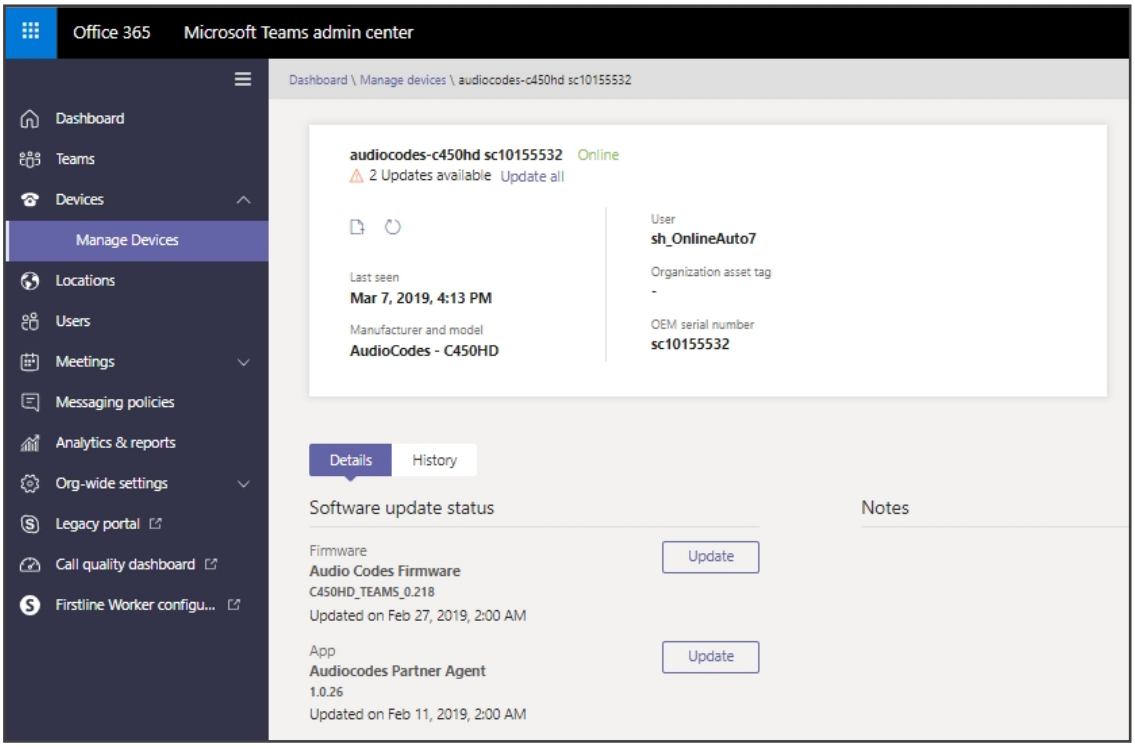
Collecting Logs

Network administrators can download *all logs* from the Microsoft Teams admin center. 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.

➢ **To collect logs:**

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

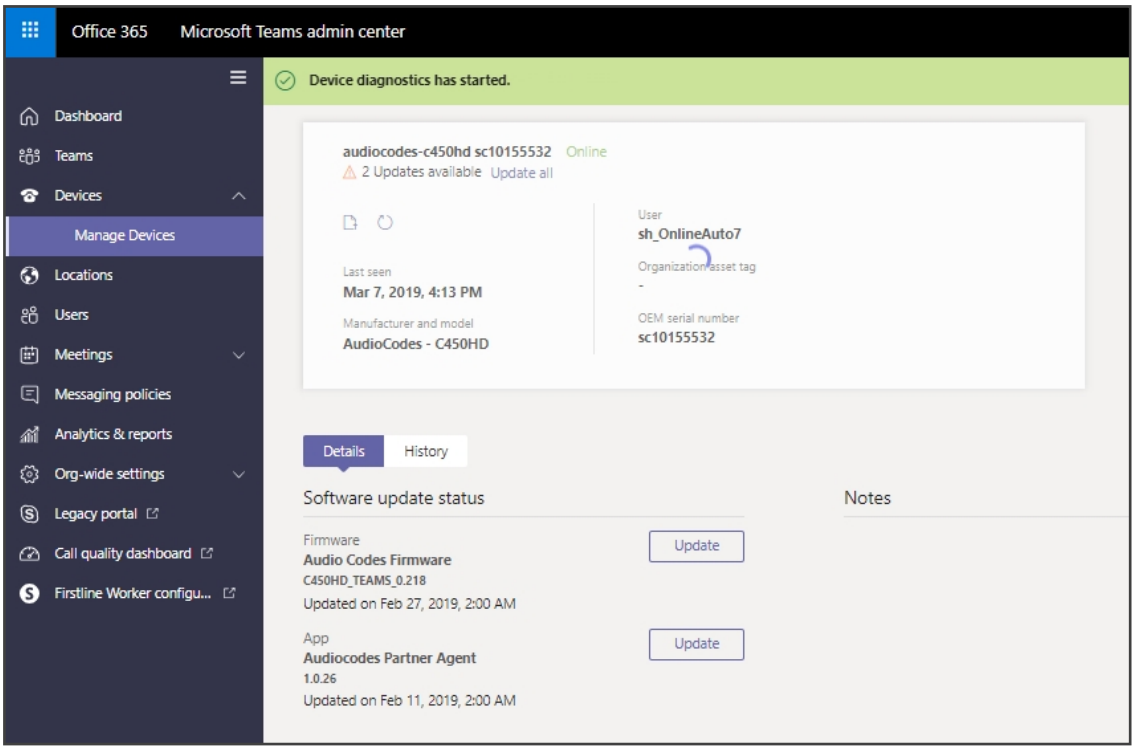
Figure 7-4: Microsoft Teams Admin Center - Diagnostics



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

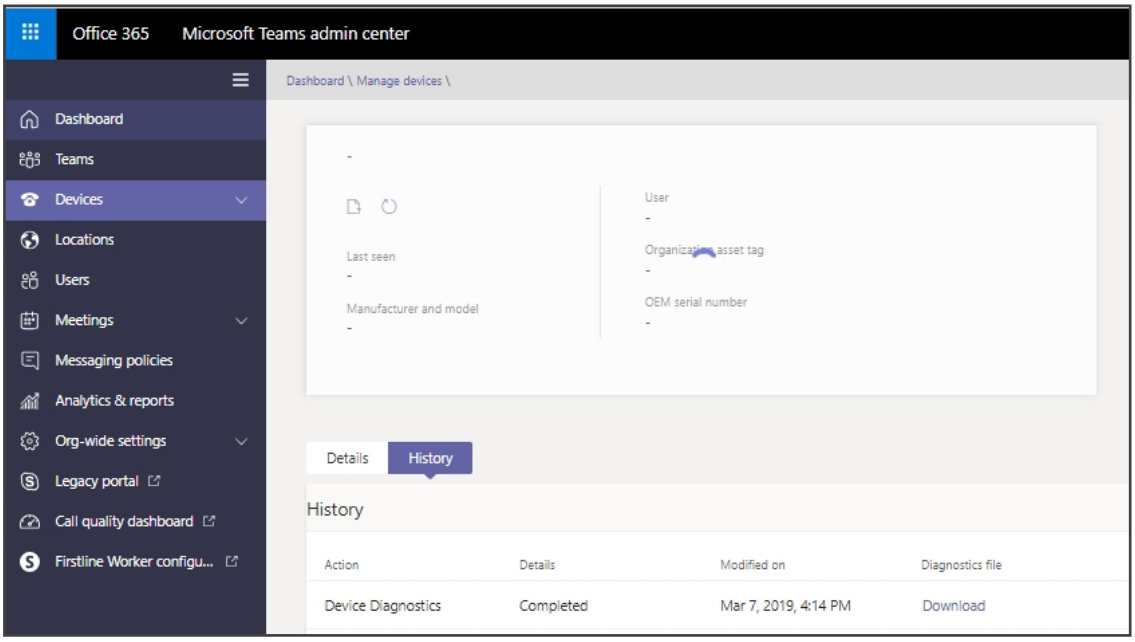
3. Click the **Diagnostics** icon and in the 'Device diagnostics' prompt that pops up, click **Proceed**; log files are retrieved from the devices and uploaded to the server.

Figure 7-5: Microsoft Teams Admin Center – Logs Upload to Server



4. Click the **History** tab.

Figure 7-6: 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 (TAC). 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*.

Getting Audio Debug Recording Logs

Network admins 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. Log in as Administrator.
2. Open the Settings screen and scroll down to **Debug**.



3. Select **Debug** and then scroll down to **Debug Recording**.



4. Configure the remote IP address and port.

5. Enable 'Voice record'.
6. Start Wireshark on your PC to capture the Audio traffic.

Collecting Media Logs (*.blog) from the Phone

Network administrators can collect Media Logs (*.blog) from the phone.

➢ **To collect Media Logs (*.blog) from the phone**

1. Access the phone via SSH.

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

2. Set the phone to the screen to capture.
3. Run the following command:

```
scp -r admin@hosp_
ip:/sdcard/android/data/com.microsoft.skype.teams.ipphone/cache/ .
```

Encountering an ANR Error - Core Dump

If an Application Not Responding (ANR) error / core dump occurs, logging capability helps admin 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.

Retrieving 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.

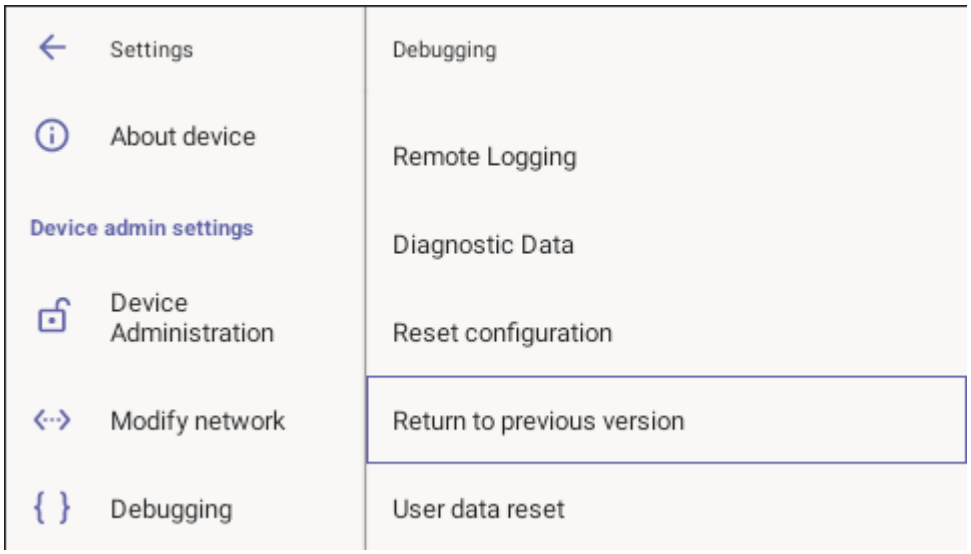
Return to Previous Version

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

- Select **Return to previous version** in the **Debugging** menu:



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

©2025 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-13462