

C470HD IP Phone

Microsoft Teams Application

Version 1.19



Notice

Information contained in this document is believed to be accurate and reliable at the time of printing. However, due to ongoing product improvements and revisions, AudioCodes cannot guarantee accuracy of printed material after the Date Published nor can it accept responsibility for errors or omissions. Updates to this document can be downloaded from <https://www.audiocodes.com/library/technical-documents>.

This document is subject to change without notice.

Date Published: March-20-2024

WEEE EU Directive

Pursuant to the WEEE EU Directive, electronic and electrical waste must not be disposed of with unsorted waste. Please contact your local recycling authority for disposal of this product.

Customer Support

Customer technical support and services are provided by AudioCodes or by an authorized AudioCodes Service Partner. For more information on how to buy technical support for AudioCodes products and for contact information, please visit our 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
Android Device Utility User's Manual
IP Phones How To . A selection of video clips explaining how to perform a variety of frequently needed actions on AudioCodes IP phones quickly and easily.

Document Name
C470HD IP Phone for Microsoft Teams Quick Guide
C470HD IP Phone for Microsoft Teams Release Notes
Device Manager Administrator's Manual
Device Manager Deployment Guide
https://docs.microsoft.com/en-us/MicrosoftTeams/phones-for-teams

Table of Contents

1	Overview	1
	Specifications	2
	Allowing URLs, Ports (Security)	4
	Security Guidelines for Android-based Native Teams Devices	4
	Android-Level Security Hardening	5
	Google Play Services	6
	Running Android in Kiosk Mode	6
	Screen Lock	6
	AudioCodes Private Key	6
	Android Debug Bridge (ADB)	7
	App Signing	7
	Web Browser	7
	Remote Configuration Management	7
	AudioCodes Device Manager Validation	7
	Sandboxing	8
	Device File System	8
	Keystore	8
	Device Certificate	8
	Data Protection	8
	Debugging Interface	8
	SSH Access: Reduced File System Privileges	9
	Android Security Updates	9
	AudioCodes Root CA Certificate	9
2	Setting up the Phone	12
	Unpacking	12
	Device Description	13
	Front View	13
	Rear View	16
	Cabling	17
	Mounting the Phone	17
	Before Using AudioCodes Devices	17
3	Starting up	18
	Configuring Device Settings	18
	Configuring Wi-Fi	33
	Connecting to an Available Wi-Fi Network	33
	Manually Connecting to a Wi-Fi Network	36
	Configuring VLAN via DHCP Option when CDP-LLDP isn't Allowed	41
	Restoring the Phone to Default Settings	42
	Performing a Hard Restore	42
	Performing a Soft Restore	42
	Performing User Data Reset	43

Recovery Mode	44
Locking and Unlocking the Phone	45
Automatic Lock	45
Unlock	45
4 Teams Application	48
Signing In	48
Multi-Cloud Sign-in	53
Remote Provisioning and Sign-in from Teams admin center	54
Getting Acquainted with the Phone Screen	58
Enabling Google Talkback	61
Opting in or out of Call Queues	64
Setting Status	64
Hot Desking	65
Changing Presence Status	66
Power Saving	68
Enabling Voicemail Support on CAP Users	68
Configuring Teams Application Settings	69
Setting up a Meeting	72
Using the People Screen	72
Accessing Voicemail	73
Using Audio Devices	74
Transferring Calls and Meetings across Devices	74
Signing Out	75
5 Performing Teams Call Operations	77
Making a Call	77
Microsoft Lightweight Calling Experience	78
Dialing a Missed Call	79
Select to Dial	79
Transferring a Call	79
Making an Emergency Call	80
Answering Calls	81
Ending an Established Call	82
Managing Calls	82
Using Boss-Admin	82
Parking a Call	83
Managing Teams Meetings	84
Using Live Captions	85
Raising a Hand During a Meeting	86
Hiding Names and Meeting Titles for Individual Devices	86
Reacting During a Meeting	86
Transferring a Call to Frequent Contacts	87
Transferring a Call to Work Voicemail	87

Viewing and Playing Voicemail Messages	87
Rejecting an Incoming Call, Sending it Directly to Voicemail	88
Adjusting Volume	89
Adjusting Ring Volume	89
Adjusting Tones Volume	89
Adjusting Handset Volume	89
Adjusting Speaker Volume	90
Adjusting Headset Volume	90
Playing Incoming Call Ringing through USB Headset	90
Using the Phone as a USB Speaker	90
Viewing and Joining Meetings	91
Better Together over Bluetooth	92
Adding a Speed Dial	95
Adding a Speed Dial Group	97
6 Performing Administrator-Related Operations	98
Setting up Automatic Provisioning	98
Setting up an E911 Emergency Location using TAC	99
Updating Phone Firmware Manually	104
Loading Certificates to Phones	107
AudioCodes Android Device Utility	108
Certificate Enrollment using SCEP	110
Manually Performing Recovery Operations	112
Enrolling a Device with Intune Policies	113
Creating a Dynamic Group	113
Creating an Exclusion Group	113
Removing Devices from Intune admin center	114
Updating Microsoft Teams Devices Remotely	117
Applying Firmware to a Phone from a USB Disk	117
Disabling a Device's USB Port	118
Enabling a Phone to be used as an Audio Device	119
Managing Phones with the Device Manager	120
Configuring a Periodic Provisioning Cycle	121
Configuring TimeZone and Daylight Savings	122
Managing Devices with HTTPS	123
Supported Parameters	123
7 Troubleshooting	125
DSCP	125
Users	126
Network Administrators	127
Android Device Utility	127
Capturing the Phone Screen	129
Running Tcpdump	130
Getting Information about Phones	131

Remote Logging (Syslog)	132
Getting Diagnostics	135
Getting Logs	136
Activating DSP Recording	137
Deactivating DSP Recording	138
SSH	139
Getting the Phone IP Address	140
Installing the APK using SSH	140
Updating Phones using SSH Commands	140
Microsoft Teams Admin Center	142
Collecting Logs	142
Getting Audio Debug Recording Logs	144
Collecting Media Logs (*.blog) from the Phone	145
Capturing Traffic Using 'rpcapd'	145

1 Overview

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

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

C470HD Features:

- Native support for Microsoft Teams
- Graphical portrait 5.5" color touch screen (1280 x 720) with multi-lingual support
- GbE support
- USB headset support
- Bluetooth 5.0 support

400HD IP Phone Series Highlights:

- Superior voice quality
- Full duplex speaker phone
- Robust security mechanisms
- PoE or external power supply
- Centralized management supported by AudioCodes Device Manager (available for download free of charge)



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 software specifications.

Table 1-1: Software Specifications

Feature	Details
Media Processing	<ul style="list-style-type: none"> ■ Voice Coders: G.711, G.729, G.722, SILK, Opus ■ Acoustic Echo Cancellation: 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	<ul style="list-style-type: none"> ■ 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 and Meeting Details; Presence Integration; Exchange Calendar Integration; Contact Picture Integration; Corporate Directory Access) ■ Meetings (roadmap feature) (One-click Join for Meetings; Join Skype for Business meetings; Meeting Call controls [Mute/unmute, hold/resume, hang up, add/remove participant]; Meeting Details. See also here for related Microsoft documentation.
Configuration and Management	<ul style="list-style-type: none"> ■ Teams admin center (TAC) ■ OVOC / Device Manager
Debugging Tools	<ul style="list-style-type: none"> ■ AudioCodes' Android Device Utility (see Android Device Utility on page 127) ■ Log upload to Microsoft server (certification for 3rd party Skype for Business clients) ■ Remote logging via Syslog ■ SSH Access

Feature	Details
	<ul style="list-style-type: none"> ■ Capturing the phone screen ■ TCPdump ■ Audio Debug recording logs ■ Echo Canceler (EC) debug recording ■ Media logs (*.blog) ■ Remote Packet Capture network sniffer application
Localization Support	<ul style="list-style-type: none"> ■ Multi-lingual support; the language pack list is not yet final and is subject to modification.
Hardware	<ul style="list-style-type: none"> ■ Graphical portrait 5.5" color touch screen, 1280 x 720 resolution, with multi-lingual support ■ Wired connectivity: <ul style="list-style-type: none"> ✓ Two RJ-45 [Gigabit Ethernet (GbE)] (10/100/1000BaseT Ethernet) ports: LAN and PC port ✓ USB port ✓ RJ-11 interface ✓ Survivable Branch Appliance (SBA) ■ Wireless connectivity: <ul style="list-style-type: none"> ✓ Dual band 2.4GHz/5GHz, 802.11b/g/n Wi-Fi support ✓ Wi-Fi supported protocols: WEP, WPA-PSK/WPA2-PSK and WPA/WPA2 Enterprise (802.1X) PEAP only ■ Bluetooth support; integrated; optional <ul style="list-style-type: none"> ✓ Max. # of Bluetooth devices that can connect simultaneously to C470HD: 1 ■ Power: <ul style="list-style-type: none"> ✓ DC jack adapter 12V ✓ Power supply AC 100 ~ 240V ✓ PoE Class 2: IEEE802.3af (optional) ■ Keys: <ul style="list-style-type: none"> ✓ Hold ✓ Mute ✓ Transfer

Feature	Details
	<ul style="list-style-type: none"> ✓ Volume ✓ Headset (including LED) ✓ Speaker (including LED) ✓ Back ✓ Home

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. See also [Microsoft's guide to the ports the phone uses](#).

Table 1-2: URLs / Ports to Allow when Deploying Teams Phones (Security)

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

Security Guidelines for Android-based Native Teams Devices

AudioCodes' Android-based Native Teams devices are purpose-built and customized for Microsoft Teams calling and meeting. Customers might perceive Android-based products as

vulnerable to security issues but security is *less* of an issue on devices purpose-built and customized for Microsoft Teams calling and meeting. Security is in fact *enhanced* on these devices *as part of their default use*.

When analyzing device security, two levels must be addressed:

- Authentication and security with respect to Teams connectivity and use
- Android level / system of the device

AudioCodes recommends the following:

- Use the sign-in mode **Sign-in with other device option**. In this mode, users do not type the password on the device but instead obtain a code on their PC / laptop to be used to sign-in; the phone obtains a private token that enables it to access Teams cloud; this token, unlike a password, allows only that device which obtained it to reuse it. The token is stored on the secured file system.
- Leverage Multi-Factor-authentication (MFA) to improve sign-in security.
- Reduce the expiration time of the sign-in for devices which are connected remotely (outside the organization's network) versus devices inside the organization's premises.

AudioCodes recommends visiting Microsoft's technical pages for more security guidelines and policies for Microsoft Teams adoption:

- [Overview of security and compliance - Microsoft Teams | Microsoft Docs](#)
- [Identity models and authentication for Microsoft Teams - Microsoft Teams | Microsoft Docs](#)
- [Sign in to Microsoft Teams - Microsoft Teams | Microsoft Docs](#)

Android-Level Security Hardening

Major Android-level system-level developments have been incorporated into AudioCodes' devices to improve security:

- See [Google Play Services](#) on the next page
- See [Running Android in Kiosk Mode](#) on the next page
- See [Screen Lock](#) on the next page
- See [AudioCodes Private Key](#) on the next page
- See [Android Debug Bridge \(ADB\)](#) on page 7
- See [App Signing](#) on page 7
- See [Web Browser](#) on page 7
- See [Remote Configuration Management](#) on page 7
- See [AudioCodes Device Manager Validation](#) on page 7
- See [Sandboxing](#) on page 8
- See [Device File System](#) on page 8

- See [Keystore](#) on page 8
- See [Device Certificate](#) on page 8
- See [Data Protection](#) on page 8
- See [Debugging Interface](#) on page 8
- See [SSH Access: Reduced File System](#)
- See [Android Security Updates](#) on page 9

Google Play Services

Google Play services were removed from AudioCodes devices software. Access to any Google store or Play service is not allowed.

- Updating the AudioCodes device's Android software and application is performed via special software components that either connect to the Teams Admin Center or to AudioCodes' Device Manager over a secured channel.

Running Android in Kiosk Mode

Android Kiosk Lockdown software 'locks down' Android devices to only allow essential apps by disabling access to the Home / Launcher. Using Android Kiosk Lockdown software, Android devices can be converted into public kiosk terminals or secured work devices.

- Only specific Microsoft apps and AudioCodes-signed apps that were certified and approved in the certification process can run in Kiosk mode; even if a malicious user manages to install a new unauthorized app on the file system, the launcher on the device will only run those specific approved apps and this cannot be changed in run time (only with a new software code provided by AudioCodes).

Screen Lock

AudioCodes devices use a screen lock mechanism to prevent any malicious user/users from gaining access to Calendar information and / or Active Directory list of employees and / or triggering unauthorized calls from the device. After enabling screen lock, the device automatically locks after a preconfigured period; a code is required to unlock the device and resume full operation.

AudioCodes Private Key

The system software on AudioCodes devices is signed with AudioCodes' private key. Users can replace the complete software only with new software that is also signed by AudioCodes' private key.

This prevents users from replacing the complete over-the-air (OTA) package of the device with any new system software, unless the software is fully signed by AudioCodes.

Android Debug Bridge (ADB)



The device does not allow access to ADB.

AudioCodes disabled the Android Debug Bridge (ADB) application and keeps the Teams app running in the front all the time. As a result, it's impossible to install other apps from unknown sources, and to sideload apps.

App Signing

Android requires all apps to be digitally-signed with a developer key before installation; currently, the AudioCodes devices verify that apps are signed by Microsoft.

App signing prevents malicious user/users from replacing a Microsoft-signed app with an app that "pretends" to be Microsoft but which lacks the private key that is known only to Microsoft.

Web Browser

The AudioCodes device does not include a Web browser. Users cannot browse to the public internet or internal intranet. All Web services are customized to connect to Office 365 services and AudioCodes' managed services such as the One Voice Operations Center (OVOC).

Without a Web browser, malicious user/users will not be able to access the device and browse from it as a trusted device into the customer network.

Remote Configuration Management

AudioCodes devices do not have an embedded Web server. Configuration and management are performed using one of the following remote interfaces:

- Microsoft Teams Admin Center (for Native Teams devices) over HTTPS protocols, enabled after a successful sign-in authentication process.
- AudioCodes Device Manager (part of AudioCodes' OVOC suite) over HTTPS.
- Debugging interface over SSH. Note that SSH must be disabled by default and enabled only per specific case for debugging purposes only.

AudioCodes Device Manager Validation

The AudioCodes Native Teams devices validate the AudioCodes Device Manager identity using a known trusted certificate:

- The device is shipped with known trusted certificate installed. See [AudioCodes Root CA Certificate](#) on page 9.
- For the initial connection, the AudioCodes Device Manager accesses devices using a known trusted certificate.

- Once a successful secured connection has been established between the device and the Device Manager, the user can replace the trusted certificate on the Device Manager and on the phone, and re-establish the connection leveraging any Private Trusted Certificate.

Sandboxing

AudioCodes devices use Android Application Sandbox so that each application can access its own data and is isolated from other applications. This prevents a malicious app from accessing the code or the data of other applications in the system.

Device File System

The AudioCodes device's file system is encrypted on C470HD devices. Customers may enforce a policy of device encryption via Microsoft's cloud-based Intune service.

Keystore

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

Device Certificate

AudioCodes devices are shipped with a unique certificate which is signed by AudioCodes Root CA. Network administrators can install a third-party certificate on the phone in the customer's trusted environment. Network administrators should follow the following guidelines when replacing the existing device certificate:

- The device certificate URL will only be valid if no SCEP server URL is present
- Use the following two parameters to set the device certificate in the phone's configuration file:
 - `security/device_certificate_url=http://<server-ip>/device.crt`
 - `security/device_private_key_url=http://<server-ip>/device.key`



- Trusted certificates are provisioned by parameter `security/ca_certificate/[0-4]/`
- The loaded certificate's file name must be without spaces. Spaces between words can be created using an underscore `_`

Data Protection

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

Debugging Interface

- AudioCodes devices leverage SSH as a debugging interface.
- AudioCodes recommends that customers disable SSH on devices via AudioCodes' Device Manager (OVOC).

- AudioCodes recommends changing the Admin password from the default, via the Teams Admin Center or AudioCodes' Device Manager (OVOC).
- When a device - or multiple devices - needs to be debugged, users can enable SSH on it / them, access SSH with the new Admin password for the debugging phase, and disable SSH once debugging is finished.



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

SSH Access: Reduced File System Privileges

Administrator users who access SSH have reduced file system privileges. For example, files cannot be deleted, and some parts of the file system cannot be reviewed. This prevents malicious actions or unintended errors that might cause damage to the device.

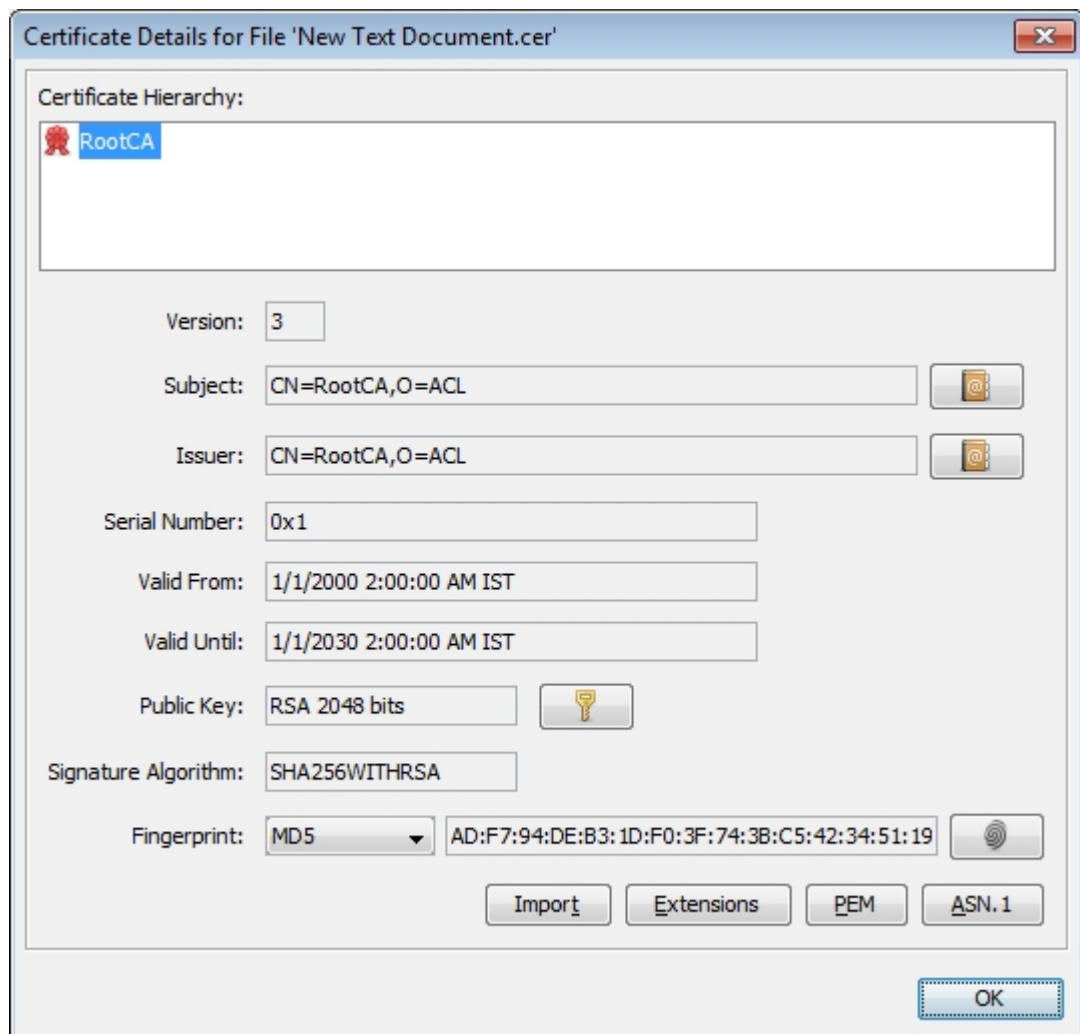
Android Security Updates

AudioCodes regularly adopts and integrates Android security updates.

For reference, see [here](#).

AudioCodes Root CA Certificate

The following figure shows the AudioCodes Root CA Certificate.



-----BEGIN CERTIFICATE-----

MIIDMTCCAhmGAWIBAgIBATANBgkqhkiG9w0BAQsFADAFMQwwCgYDVQQKEwNBQ0wx

DzANBgNVBAMTBiJvb3RDQTAeFw0wMDAxMDEwMDAwMDBaFw0zMDAxMDEwMDAwMDBa

MB8xDDAKBgNVBAoTA0FDTDEPMA0GA1UEAxMGUm9vdENBMIIBIjANBgkqhkiG9w0B

AQEFAAOCAQ8AMIIBCgKCAQEA6GK495KUCXAm/UE17G4/cjnZN4LNaxYIEYzbfZL0a

EhgSKYt/LQ+iUcDhojsneusNgrcGkpwKkIKsGsvGWmSRNULV01CW+TX2VJN73+hh

V0uzhyOIYAUhbDaoqNM6Kp5b7sJ1ew4lg9kfd/ma9Czl5koESLlw/inLj/r+rD96

mUcPEIWkKspv7Qy4I14fsK/yMArixRopTL1munVVPpSFM9Jh8IY3JHyr5CQJXKK
S

EhGAJsnHaRqsR2Su3X/WtslgEF+cvP34pxhIhFL29nMfnaFATSS3rgGaFISvl1ZS

esLMqkWjp9cqGYrvt7K61sYnvMMb+o/KbWqVokXb+Fr7bwIDAQABo3gwdjAMB
gNV

HRMEBTADAQH/MB0GA1UdDgQWBbQDXySn9hz15IDraZ+iXddZGReB+zBHB
gNVHSME

QDA+gBQDXySn9hz15IDraZ+iXddZGReB+6EjpCEwHzEMMAoGA1UEChMDQU
NMMQ8w

DQYDVQQDEwZSb290Q0GCAQEwDQYJKoZIhvcNAQELBQADggEBAI0rUywo
mmWWJnH3

JOfKiS3+VnX5hJITZymvWanMXUz/6FonHccPXEBYTrUYwhiWx3dwELAFXDFK
kxMp

0KKWZ4F39cAOLRjqhzya+xUeeJ9HQZCXAJ6XgvTfN2BtyZk9Ma8WG+H1hNv
vTZY

QLbWsjQdu4eFniEufeYDke1jQ6800LwMIFlc59hMQCeJTEnRx4HdJbJV86k1gBU
E

A7fJT1ePrRnXNDRz6QtADWoX3OmN7Meqen/roTwwLpEP22nYwvB28dq3JetlQ
Kwu

XC4gwl/o8K2wo3pySLU9Y/vanxXCr0/en5I3RDz1YpYWmQwHA8jJlu8rxdhr+VNQ
Zv6R/Ys=

-----END CERTIFICATE-----

2 Setting up the Phone

The instructions following 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, see the phone's *Quick Guide* shipped with the device or available from AudioCodes.

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

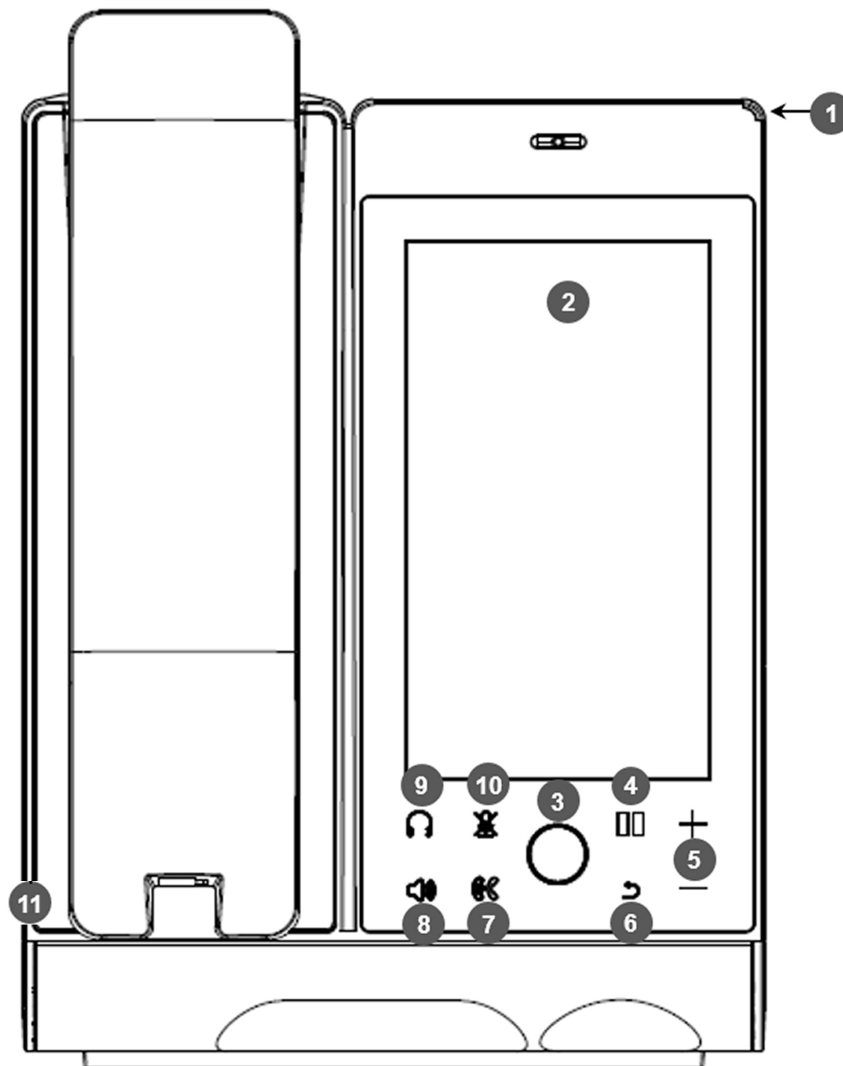


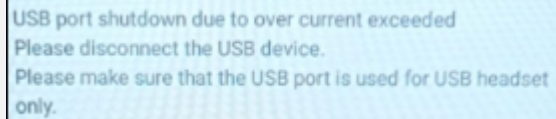
Table 2-1: Font View Description

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

Item #	Label/Name	Description
		<ul style="list-style-type: none"> ■ Flashing red: Incoming call (ringing) ■ Red: Answered call
2	TFT touch screen	Thin Film Transistor touch screen, a type of LCD (Liquid Crystal Display) interactive screen which displays calling information and lets you configure phone features by touching the glass.
3	Home	<ul style="list-style-type: none"> ■ Touch the key to return to the phone's home (idle) screen from any screen. ■ Long-press the key to open the device Settings screen. ■ Visual indications: <ul style="list-style-type: none"> ✓ If the key is illuminated red (constantly, without flashing), it indicates 'No network'; touching the key then gives the user direct access to the Network menu. ✓ Flashing red indicates a system alert, for example, when a user tries to charge via the device's USB port (see the note after this table). ✓ Flashing yellow indicates that the phone is in the process of a software upgrade.
4	Hold	Touch to place an active call on hold.
5	Volume	Increases or decreases the volume of the handset, headset, speaker, ring tone or call progress tones. See Adjusting Volume on page 89 for detailed information.
6	'Back' key	Touch to return to the previous screen.
7	Call transfer	Touch to transfer a call to a third party.
8	Speaker	Touch to activate the speaker, allowing a hands-free conversation.
9	Headset	Touch to activate a call using an external headset.
10	Mute	Touch to mute an established call.
11	USB port	For a USB headset. See also the note below.



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



USB port shutdown due to over current exceeded
Please disconnect the USB device.
Please make sure that the USB port is used for USB headset
only.

Rear View

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

Figure 2-2: Rear View

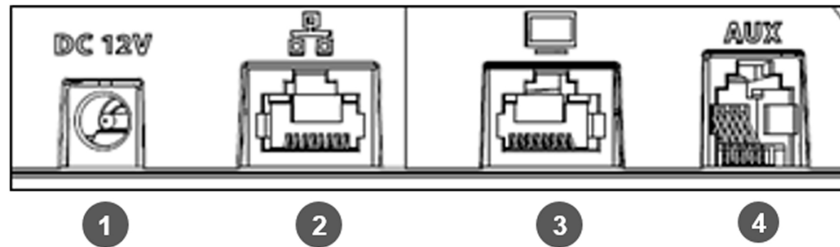


Table 2-2: Rear View Description

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

Cabling

See the phone's *Quick Guide* shipped with the device and also available from AudioCodes for detailed information on how to cable the phone.

Mounting the Phone

The phone can be mounted on a:

- Desk (see Desktop Mounting)

See the phone's *Quick Guide* shipped with the device and also available from AudioCodes for detailed information on how to mount the phone.

See also [here](#) for a clip showing *the principle* of how to mount an AudioCodes IP phone. 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:

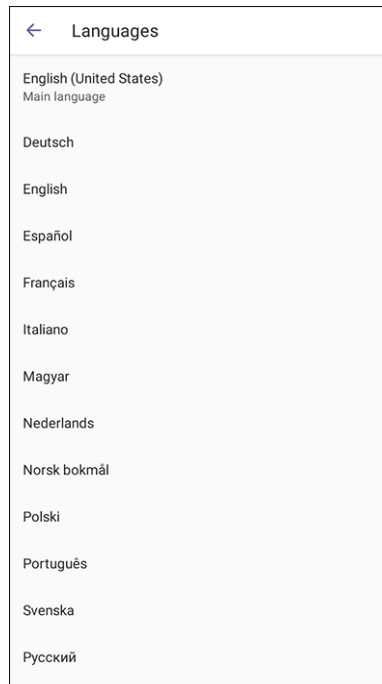
1. Disconnect all cables.
2. Spray onto a clean, dry, microfiber duster a medicinal isopropyl alcohol and water solution of 70:30. Don't oversaturate the duster. If it's wet, squeeze it out.
3. Lightly wipe the screen of the device.
4. Wait for the screen to dry before reconnecting cables.

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.



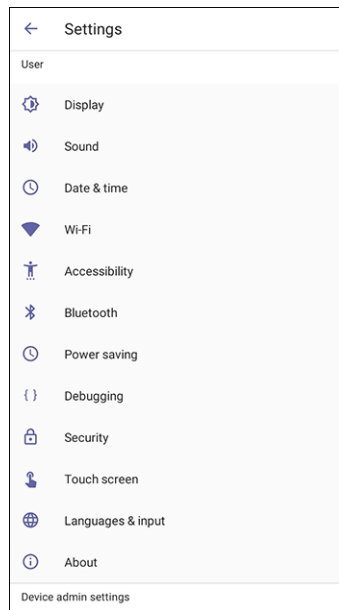
It will be necessary to repeat this only if the phone is restored to default settings.

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 the user (avatar) picture and then select the **Settings** option and then **Device settings**.

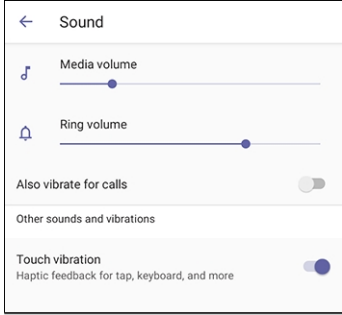
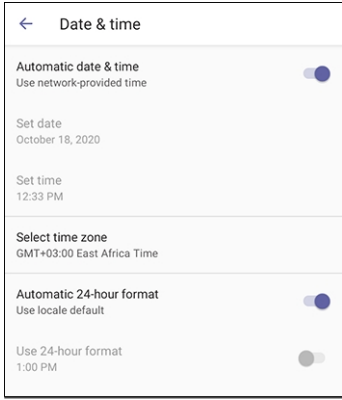


- View the settings under 'User'. Select a setting to open it. Use the table following as reference. [To view settings related to the network administrator, scroll down and open 'Device admin settings'].

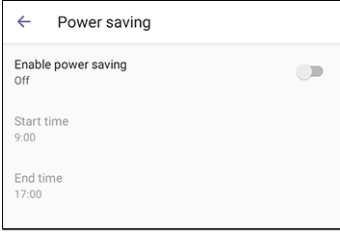
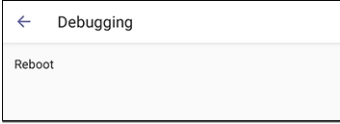
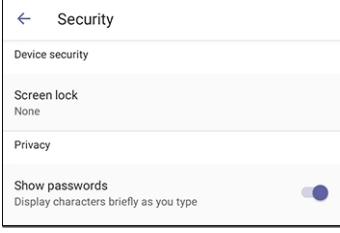
Table 3-1: Device Settings

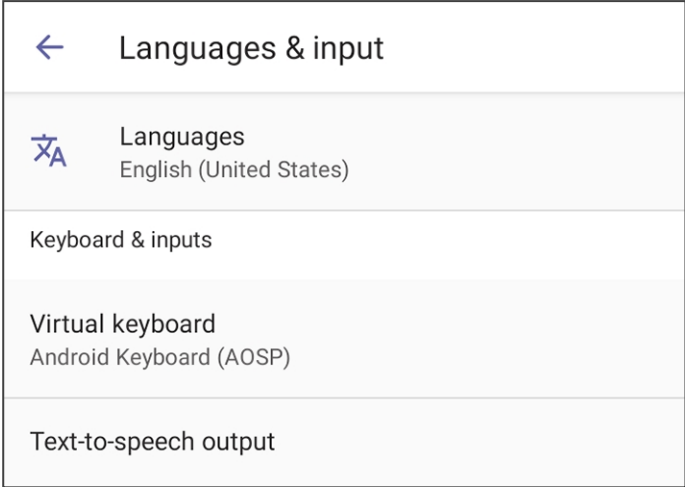
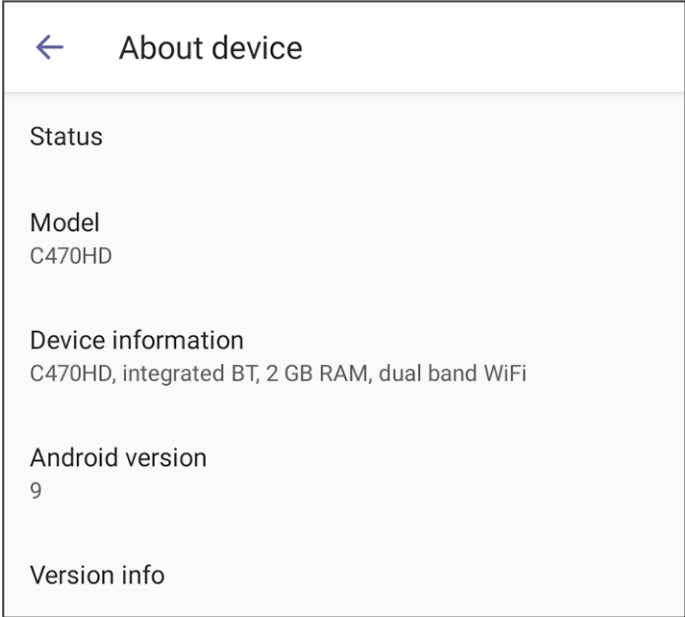
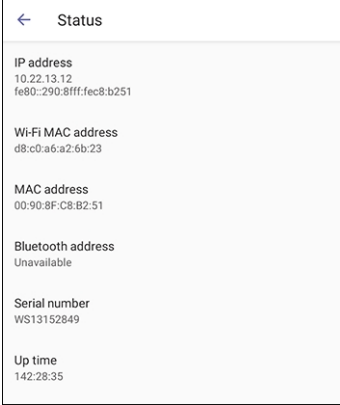
Setting	Description
User	
Display	<p>Opens the 'Display' screen [Brightness level].</p> <div data-bbox="665 1205 1278 1659" style="border: 1px solid black; padding: 5px; margin: 10px 0;"> </div> <p>The phone's screen supports different brightness levels. Choose the level that suits your requirements.</p> <ul style="list-style-type: none"> Sleep

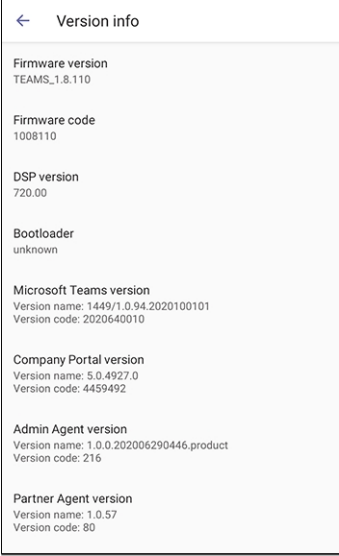
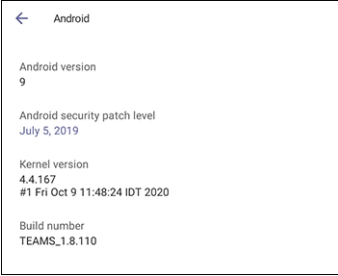
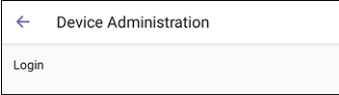
Setting	Description
	<div data-bbox="719 264 1225 719" style="border: 1px solid black; padding: 5px; margin-bottom: 10px;"> <p>← Sleep</p> <ul style="list-style-type: none"> <input type="radio"/> Never <input type="radio"/> 30 seconds <input type="radio"/> 1 minute <input type="radio"/> 2 minutes <input type="radio"/> 5 minutes <input checked="" type="radio"/> 10 minutes <input type="radio"/> 30 minutes </div> <p>■ Screen saver</p> <div data-bbox="678 808 1264 1037" style="border: 1px solid black; padding: 5px; margin-bottom: 10px;"> <p>← Screen saver</p> <hr/> <p>On <input checked="" type="checkbox"/></p> <p>Current screen saver ⚙️</p> <p>Clock</p> </div> <p>■ Font size</p> <div data-bbox="801 1111 1144 1715" style="border: 1px solid black; padding: 5px;"> <p>← Font size</p> <hr/> <p>Sample text</p> <p>The Wonderful Wizard of Oz</p> <p>Chapter 11: The Wonderful Emerald City of Oz</p> <p>Even with eyes protected by the green spectacles Dorothy and her friends were at first dazzled by the brilliancy of the wonderful City. The streets were lined with beautiful houses all built of green marble and studded everywhere with sparkling emeralds. They walked over a pavement of the same green marble, and where the blocks were joined together were rows of emeralds, set closely, and glittering in the brightness of the sun. The window panes were of green glass; even the sky above the City had a green tint, and the rays of the sun were green.</p> <p>There were many people, men, women and children, walking about, and these were all dressed in green clothes and had greenish skins. They looked at Dorothy and her strangely assorted company with wondering eyes, and the children all ran away and hid behind their mothers when they saw the Lion; but no one spoke to them. Many shops stood in the street, and Dorothy saw that everything in them was green. Green candy and green pop-corn were offered for sale, as well as green shoes, green hats and green clothes of all sorts. At one place a man was selling green lemonade, and when the children bought it Dorothy could see that they paid for it with green pennies.</p> <p>There seemed to be no horses nor animals of any kind; the</p> <p>Preview</p> <div style="text-align: center;"> <p>Default</p> <p>A A A ● </p> <p>Make the text on screen smaller or larger.</p> </div> </div>

Setting	Description
	
<p>Date & time</p>	<p>Date and time are automatically retrieved from the deployed Network Time Protocol (NTP) server.</p>  <p>Use 24-hour format [Allows you to select the Time format]</p> <p>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.</p>
<p>NTP Preferred NTP server</p>	<p>Admins can use this parameter to <i>manually</i> 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:</p> <ul style="list-style-type: none"> Admins can define it in the phone's GUI.

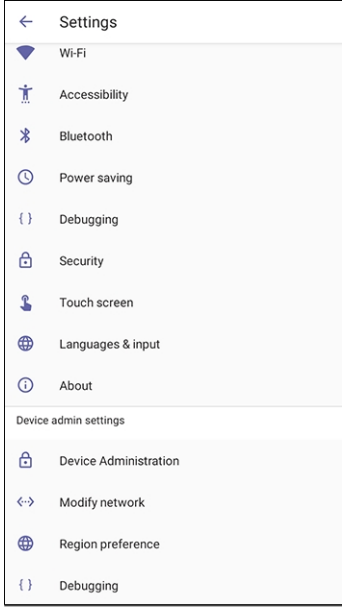
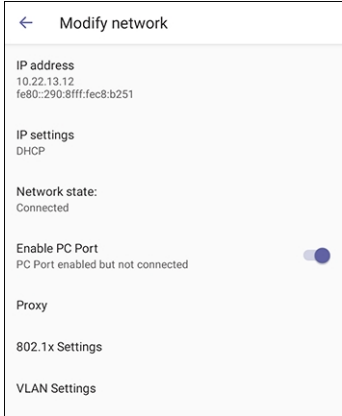
Setting	Description
	<div data-bbox="804 264 1150 891" data-label="Image"> </div> <p data-bbox="555 927 1358 999">■ Admins can alternatively use the newly added parameter 'date_time/ntp/server_address' in the phone's .cfg configuration file.</p> <p data-bbox="555 1025 1002 1057">See also under Signing In on page 48.</p>
<p data-bbox="312 1099 376 1131">Wi-Fi</p>	<p data-bbox="555 1099 1374 1245">The phone can connect to an Access Point via Wi-Fi. See the phone's <i>Quick Guide</i> for detailed information on setting up Wi-Fi. See also Configuring Wi-Fi on page 33 in this document for information about configuring the feature.</p>
<p data-bbox="312 1292 456 1323">Accessibility</p>	<p data-bbox="555 1292 1374 1357">Allows making the screen reader-friendlier. See also Enabling Google Talkback on page 61.</p> <div data-bbox="804 1368 1145 1626" data-label="Image"> </div>
<p data-bbox="312 1682 432 1713">Bluetooth</p>	<p data-bbox="555 1682 1353 1747">Hands free profile where the phone is able to connect to Bluetooth headset or speaker.</p> <p data-bbox="555 1765 1353 1830">See the phone's <i>Quick Guide</i> for detailed information on setting up Bluetooth.</p>
<p data-bbox="312 1883 472 1915">Power Saving</p>	<p data-bbox="555 1883 1273 1915">Allows users to contribute to power saving in the enterprise.</p>

Setting	Description
	 <p>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]</p>
Debugging	<p>Enables users to reboot the device.</p>  <p>Log in as Administrator for more debugging settings to be available.</p>
Security	<p>Helps secure the enterprise telephony network against breaches.</p>  <p>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</p>
Touch screen	<p>Allows users to disable the phone's touch screen.</p>
Languages & input	<p>Allows users to customize inputting to suit personal requirements.</p>

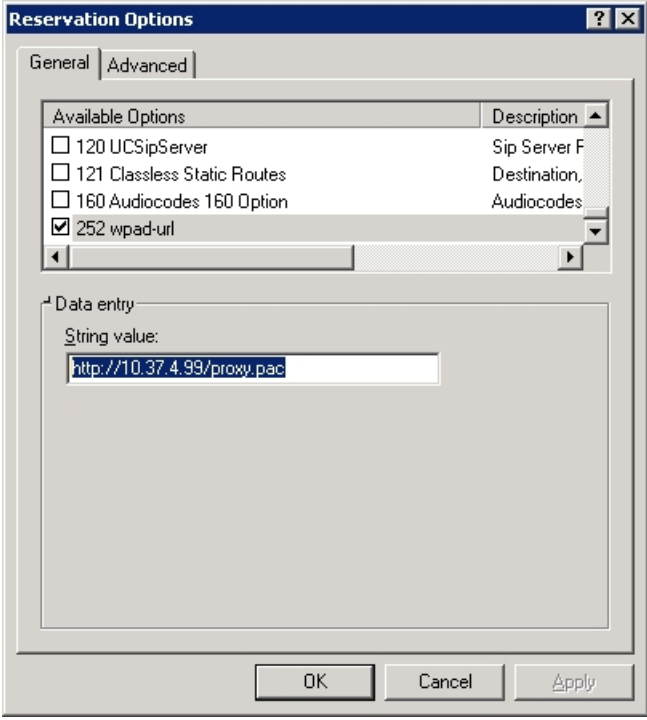
Setting	Description
	
<p>About</p>	<p>Provides users with device information.</p>  <p>To determine the device’s IP address, select the ‘Status’ option.</p> 

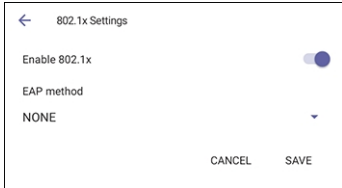
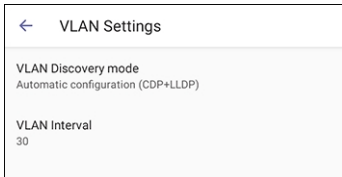
Setting	Description
	<p>To get information about the version, select 'Version info'.</p>  <p>To get information about the Android version, select 'Android version'.</p> 
Device admin settings	
<p>Device administration</p>	<p>Allows the user to log in as Administrator, necessary for some of the debugging 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.</p>  <p>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.</p>

Setting	Description
	<div data-bbox="799 264 1142 869" style="border: 1px solid black; padding: 5px; margin-bottom: 10px;"> </div> <div data-bbox="555 904 1394 1608" style="background-color: #f0f0f0; padding: 10px; border-radius: 10px;"> <ul style="list-style-type: none"> ! <ul style="list-style-type: none"> • The phone support a strong password check in order to log in as Administrator. The feature strengthens security. Note that the default password: <ul style="list-style-type: none"> ✓ 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: <ul style="list-style-type: none"> ✓ 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. </div> <p>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.</p> <p>After logging in, scroll down in the Settings screen to the section 'Device admin settings'.</p>

Setting	Description
	
<p>Modify network</p>	<p>Enables the Admin user to determine network information and to modify network settings.</p>  <p>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</p>

Setting	Description
	<p>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.</p>
Proxy	<p>The phone can be configured with an HTTP Proxy server by an Admin user in two ways:</p> <ul style="list-style-type: none"> ■ Manually. The Admin user can use this method to configure HTTP proxy server parameters through the Teams application: <ul style="list-style-type: none"> a. Log in as Administrator and select Modify network. b. Select the Proxy option and then configure the proxy host name and port: <div data-bbox="799 763 1142 1368" style="border: 1px solid black; padding: 5px; margin: 10px 0;"> </div> <ul style="list-style-type: none"> ■ 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:

Setting	Description
	 <p>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.</p> <p>Example of a basic PAC file:</p> <pre>function FindProxyForURL(url, host) { return "PROXY 10.13.2.40:3128"; }</pre> <p>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:</p> <pre>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=</pre>
802.1x Settings	<p>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.</p> <p>To configure an 802.1X Authentication method:</p>

Setting	Description
	<p>1. From the 'Modify Network' screen (as an Admin), access the 802.1x Settings screen.</p>  <p>2. From the 'EAP method' drop-down, select the method: MD5 or TLS (for example).</p> <p>3. Enter this information:</p> <ul style="list-style-type: none"> ✓ Identity: User ID ✓ Password ✓ root certificate (not required for every method) ✓ device certificate (not required for every method) <p>4. Select the Save softkey</p> <p>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:</p> <ul style="list-style-type: none"> ■ Enable/Disable ■ EAP method ■ Identity ■ Password
VLAN Settings	<p>Select the menu option VLAN Settings.</p>  <p>Select VLAN Discovery mode.</p>

Setting	Description
	<div data-bbox="799 264 1142 521" style="border: 1px solid black; padding: 5px; margin-bottom: 10px;"> <p>← VLAN Discovery mode</p> <p><input type="radio"/> Disabled</p> <p><input type="radio"/> Manual configuration</p> <p><input type="radio"/> Automatic configuration (CDP)</p> <p><input type="radio"/> Automatic configuration (LLDP)</p> <p><input checked="" type="radio"/> Automatic configuration (CDP+LLDP)</p> <p style="text-align: right;">CANCEL OK</p> </div> <ul style="list-style-type: none"> <li data-bbox="552 555 1334 629">■ Cisco Discovery Protocol (CDP) is a Cisco proprietary Data Link Layer protocol <li data-bbox="552 651 1310 725">■ Link Layer Discovery Protocol (LLDP) is a standard, layer two discovery protocol <p data-bbox="552 748 1374 822">Select the mode you require and then select OK. If you select Manual configuration, this screen opens:</p> <div data-bbox="799 846 1142 1451" style="border: 1px solid black; padding: 5px; margin-bottom: 10px;"> <p>← VLAN Settings</p> <p>VLAN Discovery mode Manual configuration</p> <p>VLAN ID -1</p> <p>VLAN Priority 1</p> <p style="text-align: center; font-size: small;">Changes will only be applied after both VLAN ID and VLAN Priority have been set</p> </div> <p data-bbox="552 1485 735 1518">Select VLAN ID.</p> <div data-bbox="799 1541 1142 1697" style="border: 1px solid black; padding: 5px; margin-bottom: 10px;"> <p>← VLAN ID</p> <p>Enter VLAN ID (range 0 to 4094)</p> <hr style="border: 0; border-top: 1px solid black; margin: 5px 0;"/> <p style="text-align: right;">CANCEL OK</p> </div> <p data-bbox="552 1731 799 1765">Select VLAN Priority.</p> <div data-bbox="799 1787 1142 1944" style="border: 1px solid black; padding: 5px;"> <p>← VLAN Priority</p> <p>Enter VLAN Priority (range 0 to 7)</p> <hr style="border: 0; border-top: 1px solid black; margin: 5px 0;"/> <p style="text-align: right;">CANCEL OK</p> </div>

Setting	Description
	<p>Select VLAN Interval.</p> <div data-bbox="632 322 1315 703" style="border: 1px solid black; padding: 10px; margin: 10px 0;"> <p>VLAN Interval</p> <p>Enter VLAN interval (range 1 to 3600)</p> <hr style="border: 0.5px solid #ccc;"/> <p style="text-align: right;">CANCEL OK</p> </div> <p>The 'VLAN interval' refers to CDP/LLDP advertisements' periodic interval. Default: 30 seconds. You can increase or decrease the intervals between the CDP/LLDP packets that are sent, based on network traffic and topology.</p>
<p>Debugging</p>	<p>Allows the Admin user to perform debugging for troubleshooting purposes. Available after logging in as Admin.</p> <div data-bbox="801 1012 1142 1435" style="border: 1px solid #ccc; padding: 10px; margin: 10px 0;"> <p>← Debugging</p> <hr/> <ul style="list-style-type: none"> Log settings Remote Logging Diagnostic Data Reset configuration Restart Teams app Company portal login Debug Recording Erase all data (factory reset) Screen Capture <input checked="" type="checkbox"/> </div> <p>Log settings Remote Logging (see under Remote Logging (Syslog) on page 132 for more information) Diagnostic Data (see under Getting Diagnostics on page 135 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 132 for more information) Erase all date (factory reset) (the equivalent of restore to defaults;</p>

Setting	Description
	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 Wi-Fi

[Applies to devices whose PN indicates **DBW**] Network administrators can configure Wi-Fi parameters for the phone. The parameters are concealed from the user's view.



- Users can enable|disable Wi-Fi using the phone screen; Wi-Fi cannot be enabled|disabled using SSH command.
- The Wi-Fi connection is transparent to users; which frequency is used, 2.4 GHz or 5 GHz, is made for users by the phone; users cannot disable one or the other.

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

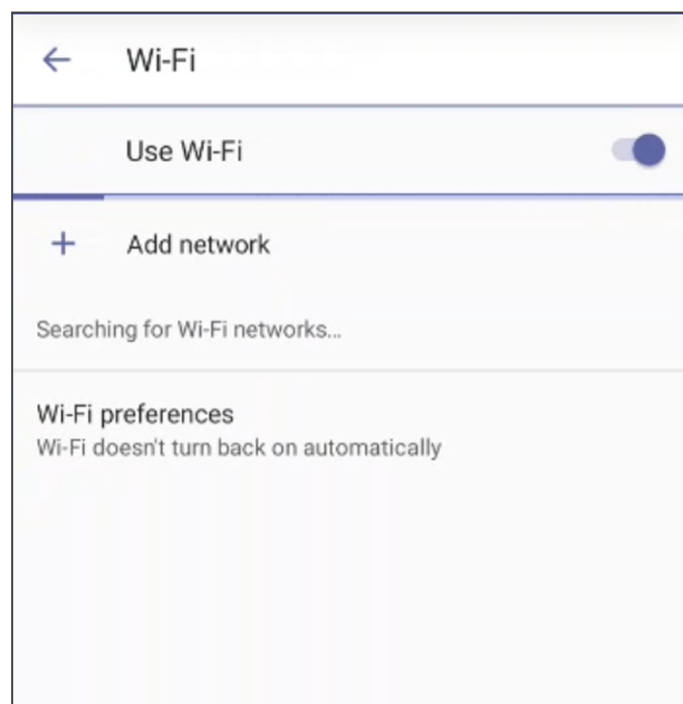
Connecting to an Available Wi-Fi Network

➤ To connect to an available Wi-Fi network:

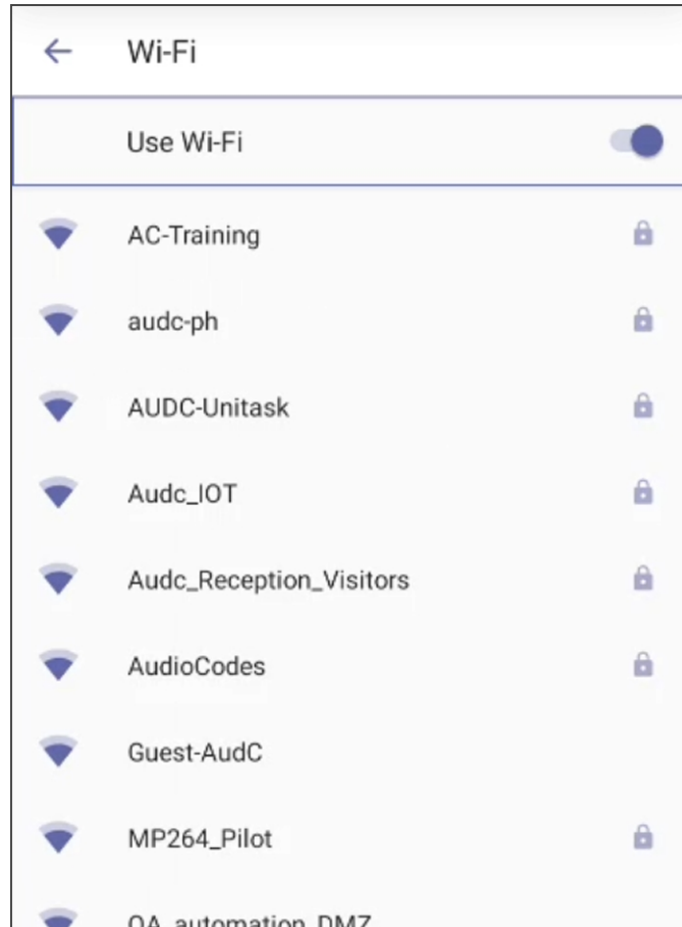


Make sure to first disconnect your Ethernet cable. If it's connected, the device will not be able to connect to a Wi-Fi network.

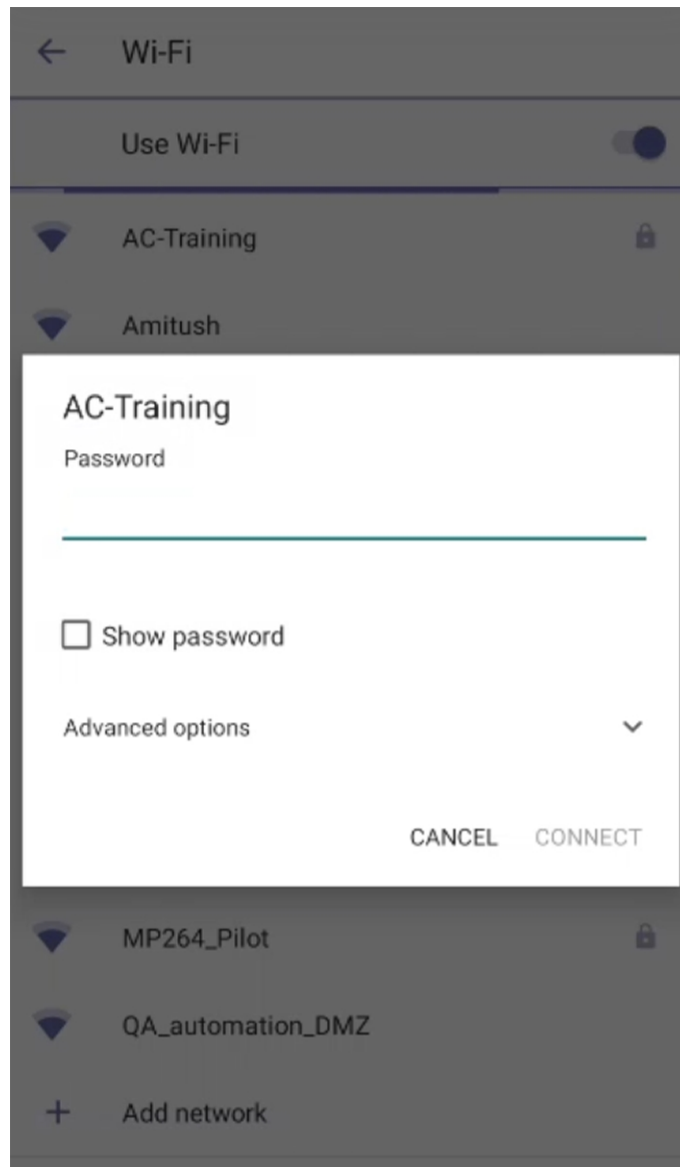
1. In the Wi-Fi screen (**Settings > Wi-Fi**), slide the **Use Wi-Fi** setting to 'on'.



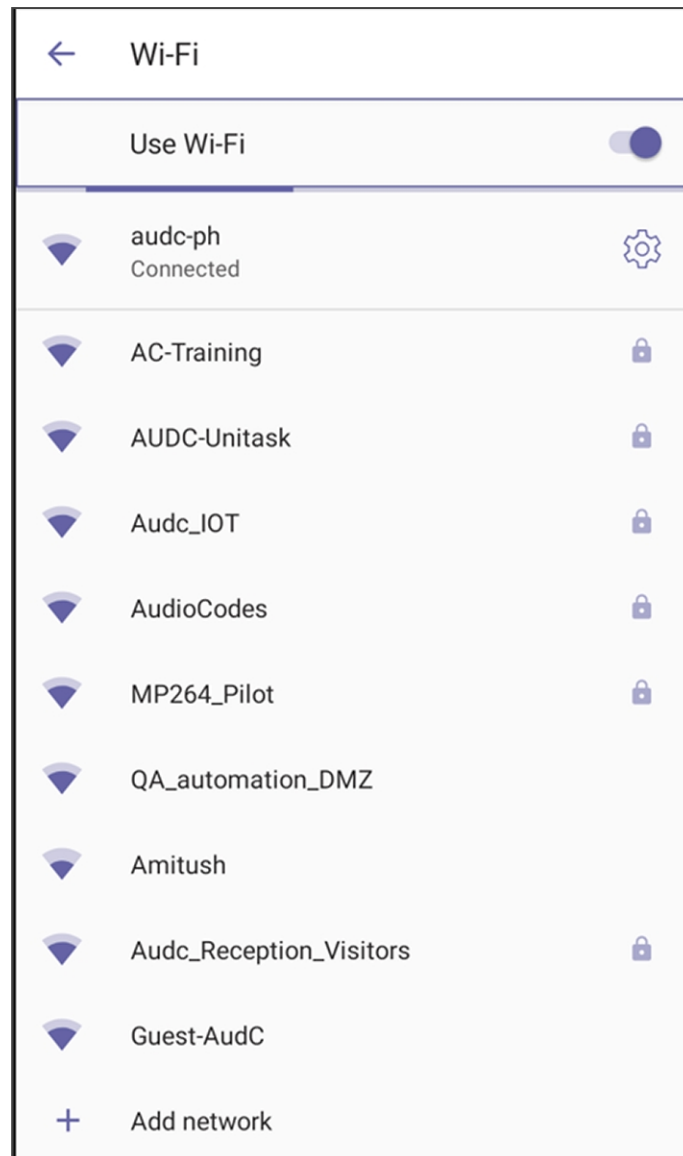
2. View a list of available connections.



3. Select the Wi-Fi network you want and enter the password.



4. View the network you selected 'Connected'.



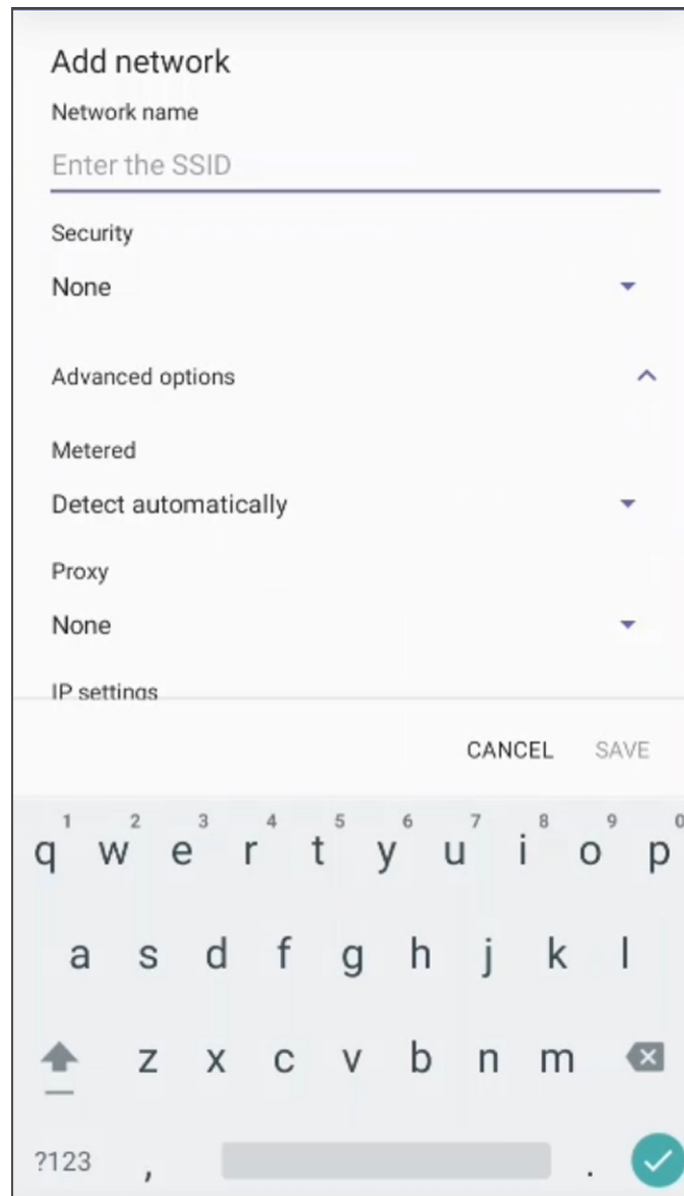
Manually Connecting to a Wi-Fi Network

➤ To manually connect to a Wi-Fi network:



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

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



2. From the 'Security' drop-down, select one of the following security key strengths (encryption methods):

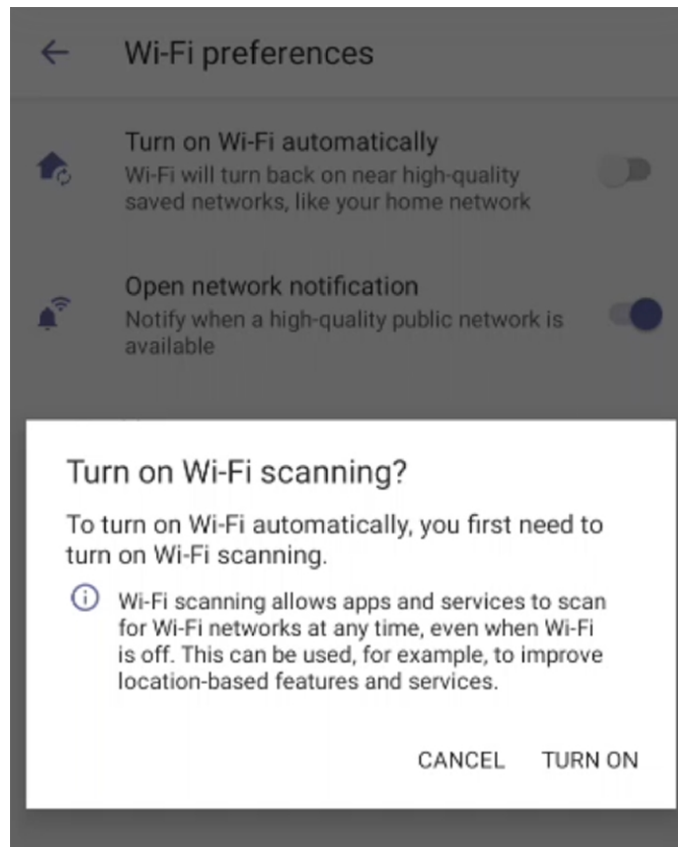
- Optionally meter the selected network. Expand **Advanced Options**. Leave the setting at its default value of **Detect automatically** if you don't want to meter the network. Select a **Metered** option to meter it.



'Proxy' and 'DHCP' shown in the figures below will automatically be configured by the network.



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



As an alternative to manually configuring Wi-Fi settings via the phone's user interface as shown above, you can configure the Wi-Fi settings described in the next table, using the Configuration File. Available from version 1.19.

Table 3-2: Configuration File Wi-Fi Settings

Wi-Fi Setting	Description
network/wireless/advanced_options/dns1	Defines the IP of the wireless DNS1.
network/wireless/advanced_options/dns2	Defines the IP of the wireless DNS2.
network/wireless/advanced_options/gateway	Defines the IP address of the wireless gateway
network/wireless/advanced_options/hidden_network	Defines the name of the wireless hidden network.

Wi-Fi Setting	Description
network/wireless/advanced_options/ip_addr	Defines the IP address of the static Wi-Fi network if you're operating with a static Wi-Fi network.
network/wireless/advanced_options/ip_settings	Used to define DHCP.
network/wireless/advanced_options/network_prefix_length	Defines the network prefix length to be used.
network/wireless/advanced_options/proxy	Defines the proxy wireless server source.
network/wireless/advanced_options/proxy/auto_config/pac_url	Defines the URL of the PAC file.
network/wireless/advanced_options/proxy/manual/exclusion_list	Defines the list of IP addresses that will be blocked.
network/wireless/advanced_options/proxy/manual/proxy_hostname	Defines the name of the proxy host.
network/wireless/advanced_options/proxy/manual/proxy_port	Defines the proxy port.
network/wireless/anon_identity	Defines the anonymous wireless users who won't be seen.
network/wireless/ca_cert	Defines which CA certificate to use.
network/wireless/client_cert	Defines which client certificate to use.
network/wireless/domain	Defines the domain name.
network/wireless/eap_method	Defines the EAP method.
network/wireless/identity	Defines the identity of the user.
network/wireless/password	Defines the password of the network.
network/wireless/phase2_method NONE,MSCHAPV2,GTC,PAP,MSCHAP	Defines the encryption method. Phase 2 applies only to the 802.1x EAP method.
network/wireless/security	Defines the security method (encryption protocol).

Wi-Fi Setting	Description
network/wireless/ssid	Defines the SSID of the network.

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:

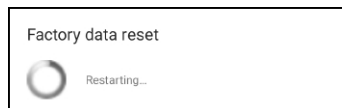
- [Performing a Hard Restore](#) below
- [Performing a Soft Restore](#) below

Performing a Hard Restore

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

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

1. Long-press the HOLD key on the phone (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.

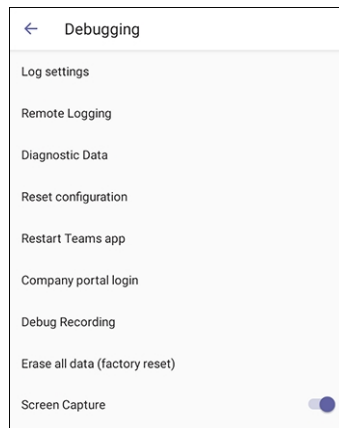
2. Select **OK**; the sign-in screen is displayed (see [Signing In](#) on page 48 for more information).

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.



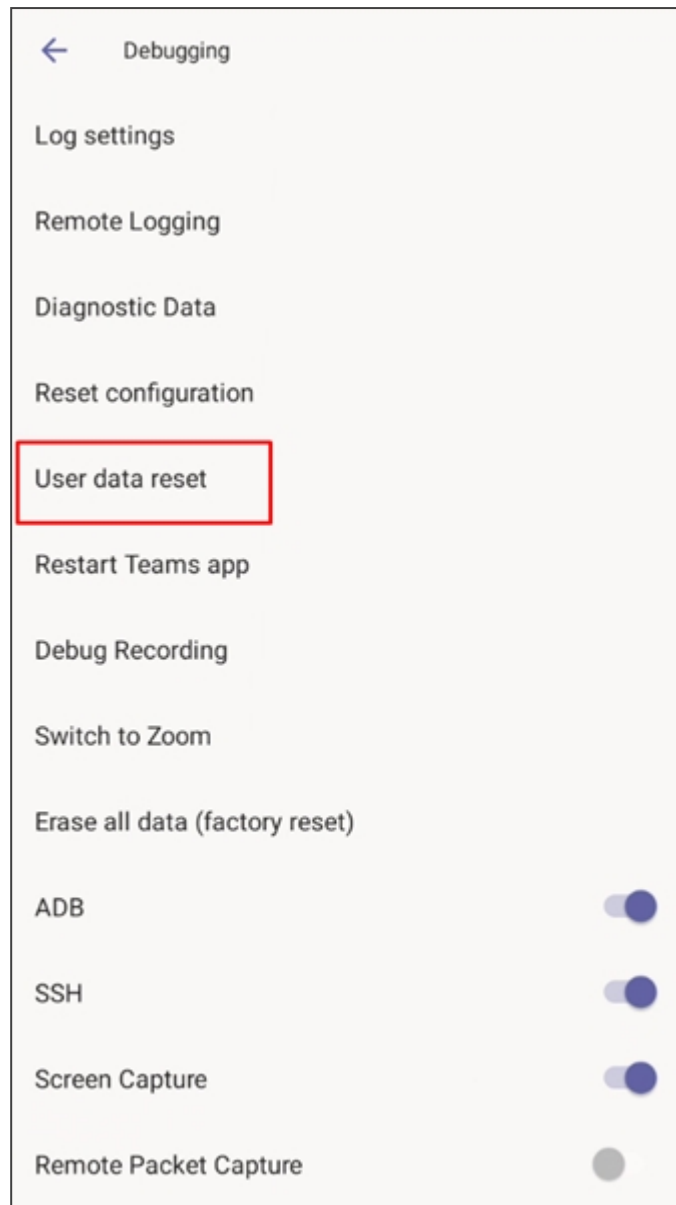
2. Select the **Erase all data (factory reset)** option; the device performs a restore to default factory settings.

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**.



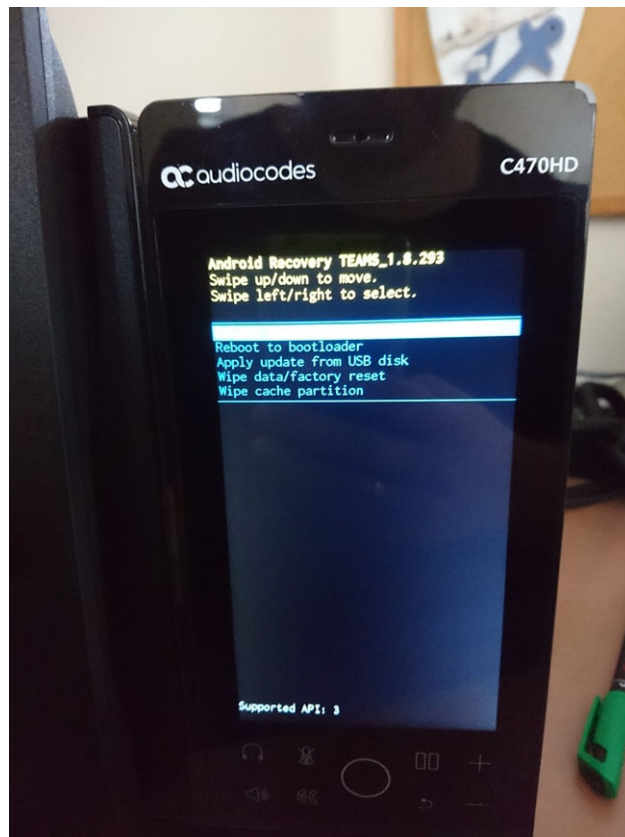
After 'User data reset', network settings are preserved.

Recovery Mode

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

➤ To boot the phone:

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



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

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.

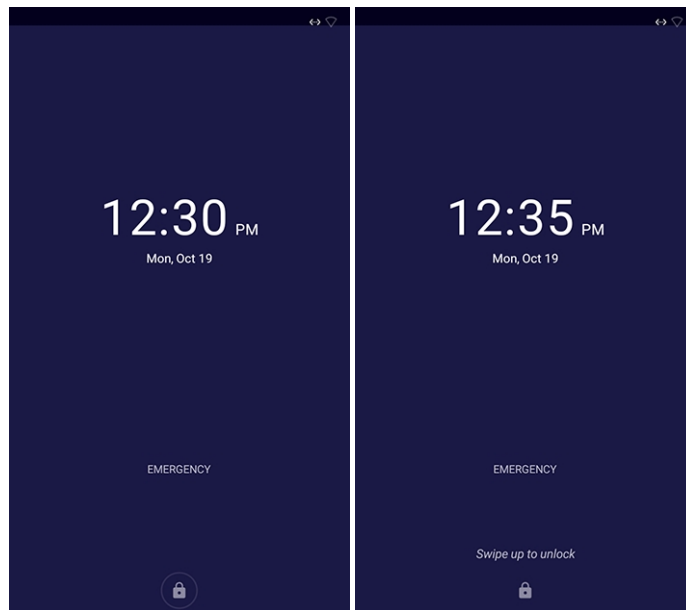
➤ To lock the phone:

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

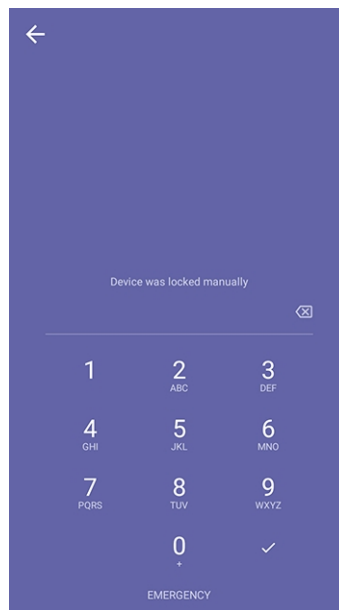
Unlock

➤ To unlock the phone:

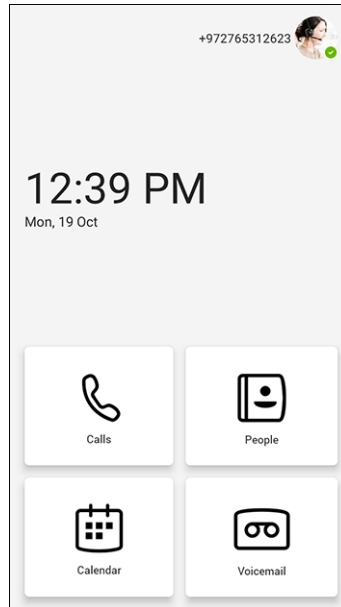
1. When the screen shown in the figure below is displayed, touch the lock icon and swipe up



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



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



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'

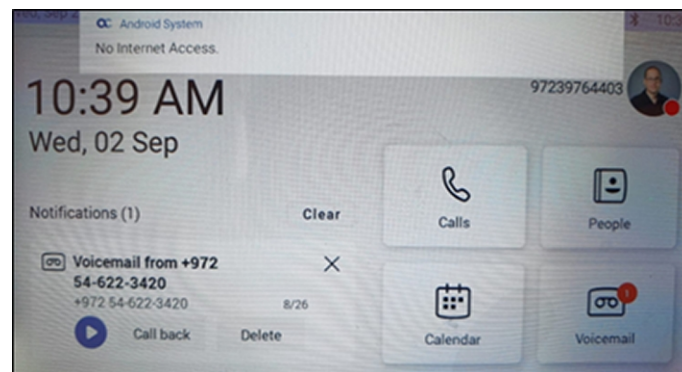
See also under [here](#) for more information.

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), 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.

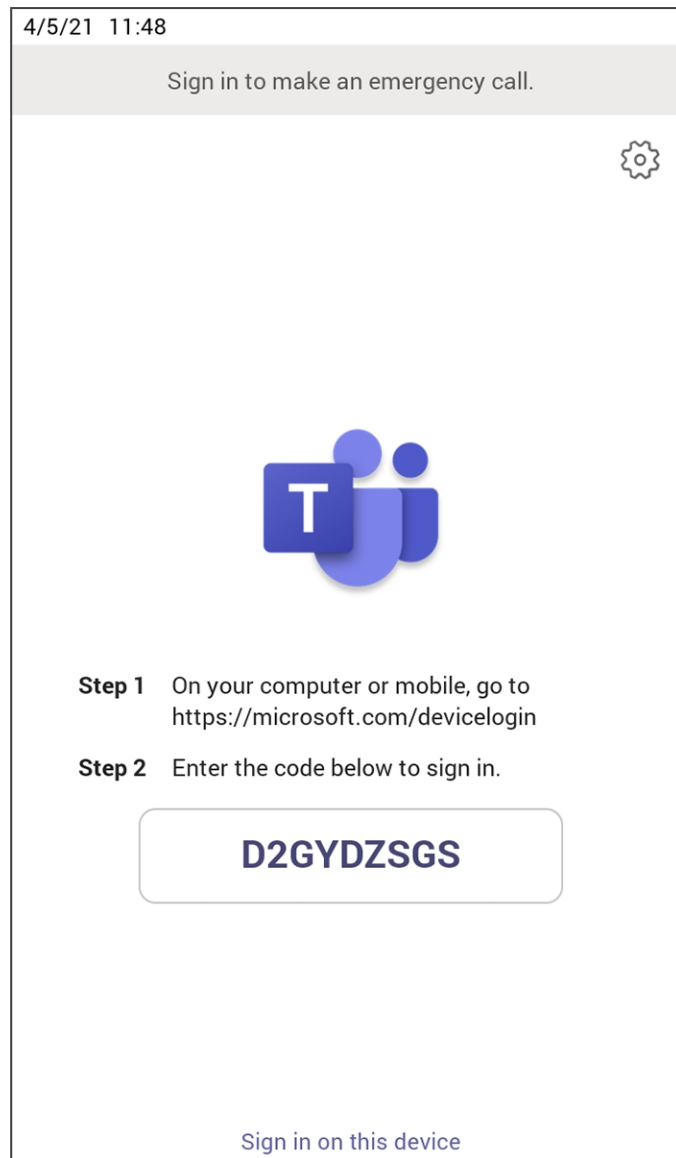
Figure 4-1: Internet Connectivity Check - No Internet Access



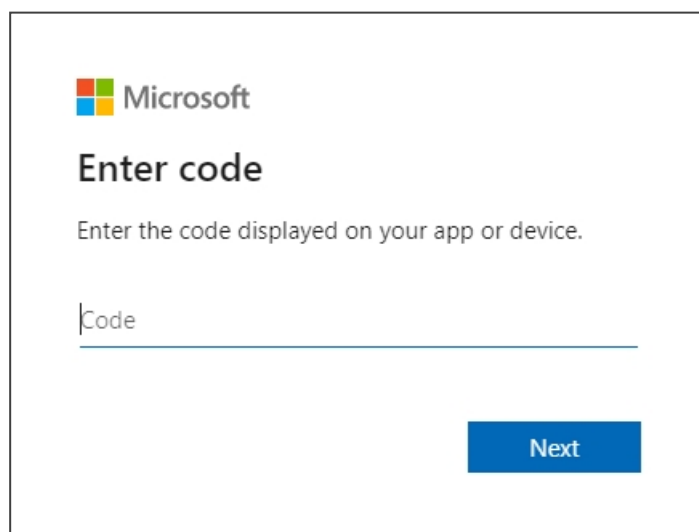
This can point to a problem that is preventing the phone from fully functioning in a Teams environment. The user can ignore the message if the Teams application is fully functioning, or can report a problem if the Teams application is not fully functioning.

➤ **To sign in:**

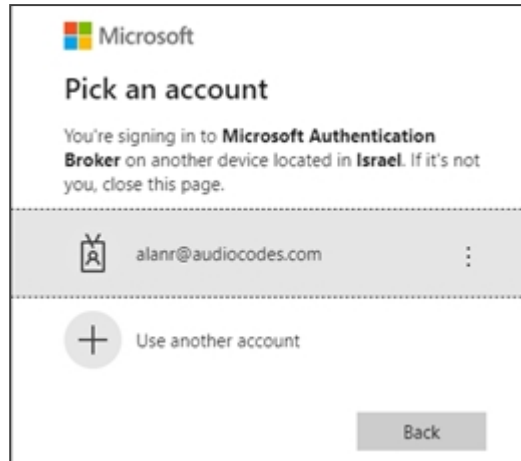
1. Connect the device to the network; this screen is then displayed:



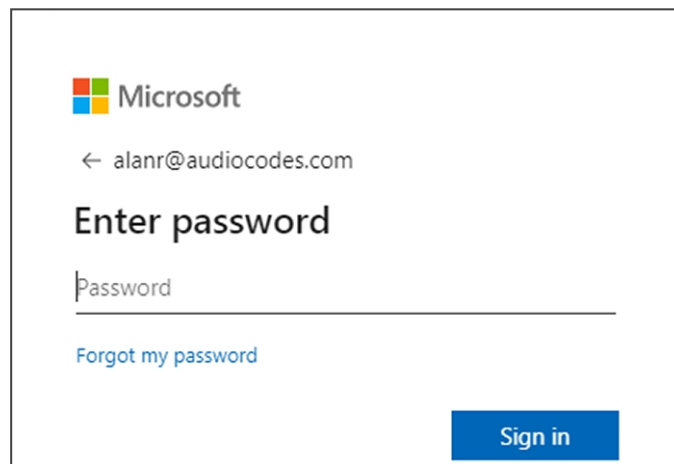
2. Open your browser and point it to <https://microsoft.com/devicelogin> as instructed in the preceding screen.



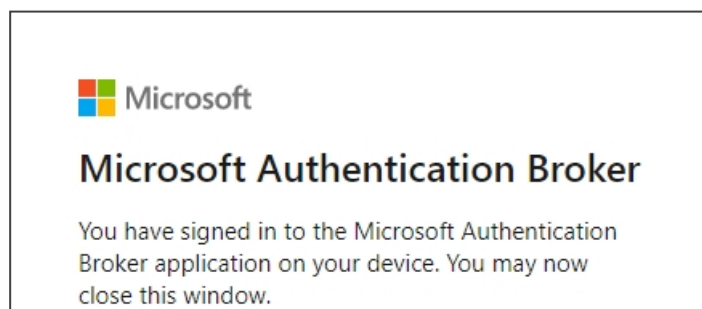
3. Enter the code and then click **Next**.



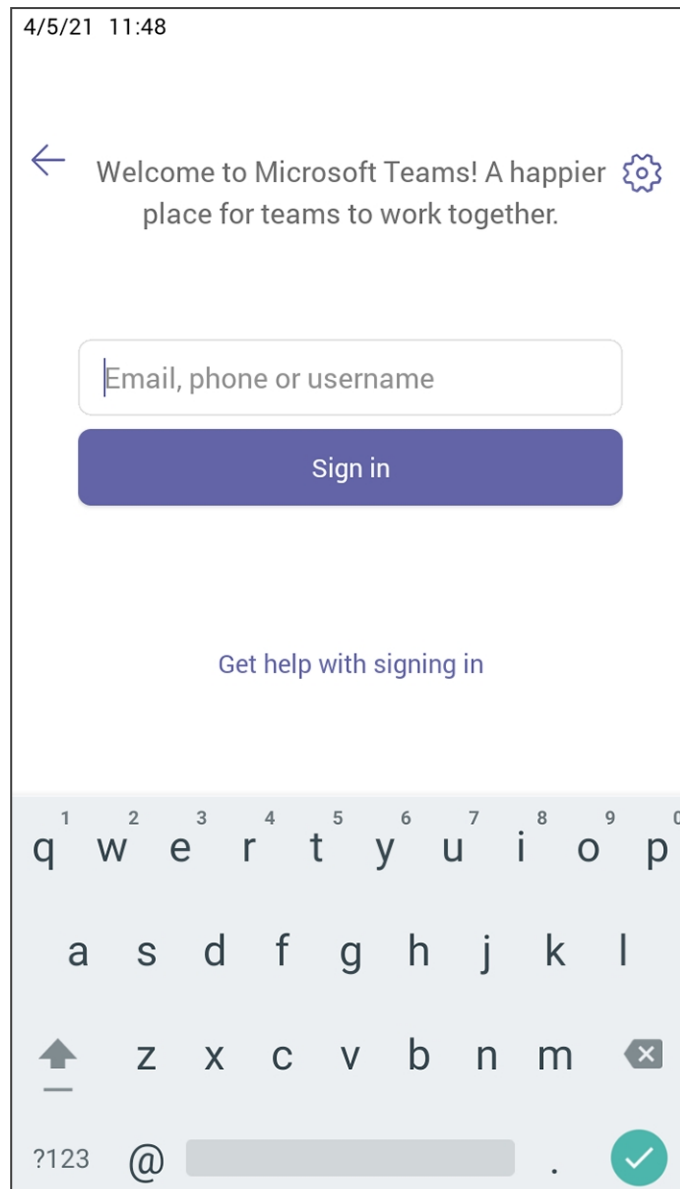
4. Click the account.



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**.



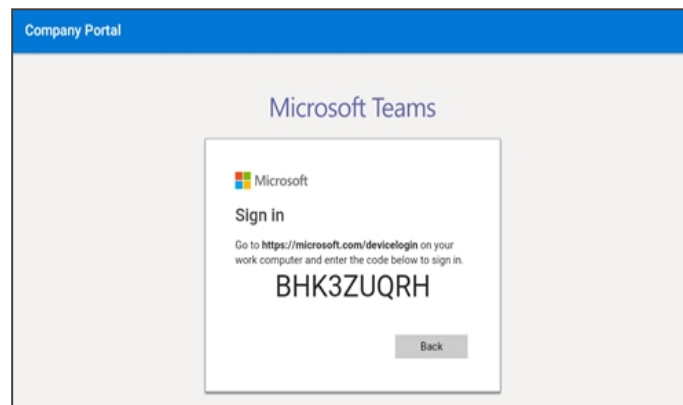
8. Select the 'Email, phone or username' field; a virtual keyboard pops up. Enter one of them and then choose **Sign in**. The 'home' screen opens.
 - If you opt to **Sign in from another device**, complete authentication from your PC or smart phone. This is recommended if you're using Multi Factor Authentication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



The phone supports a strong password check in order to log in as Administrator. The feature strengthens 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



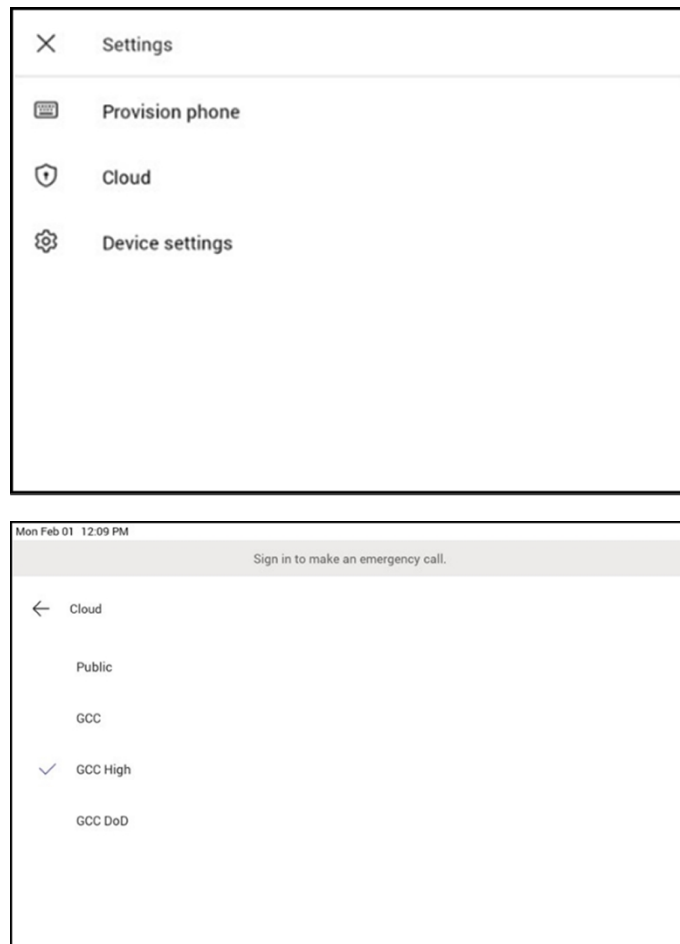
- ◆ In the browser on your PC or smart phone, enter the URL indicated in the preceding screen and then in the phone's Web interface that opens, perform sign-in (as noted previously, this option is recommended if using MFA).



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.



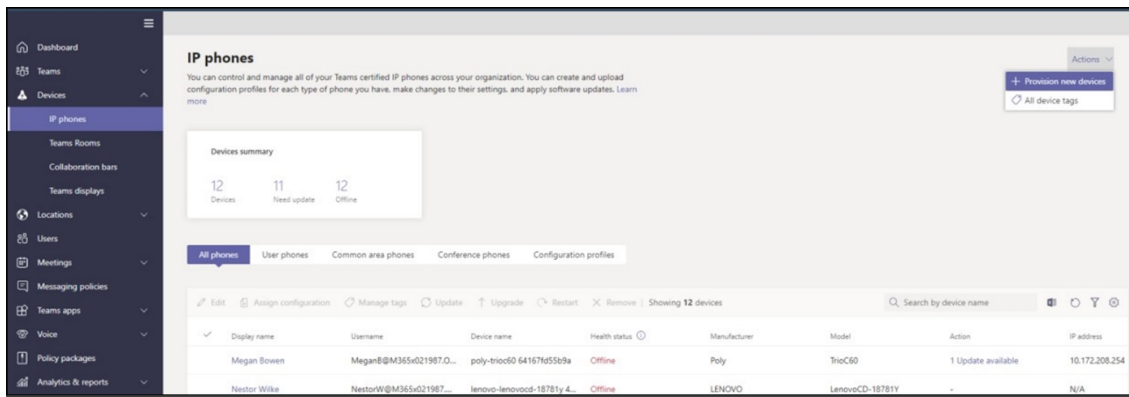
Remote Provisioning and Sign-in from Teams admin center

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.

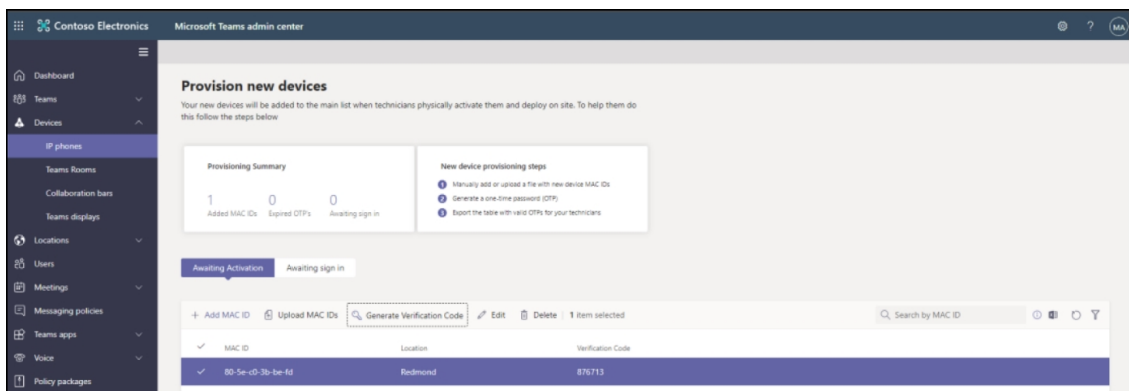
Upload a file to add a device MAC address

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.

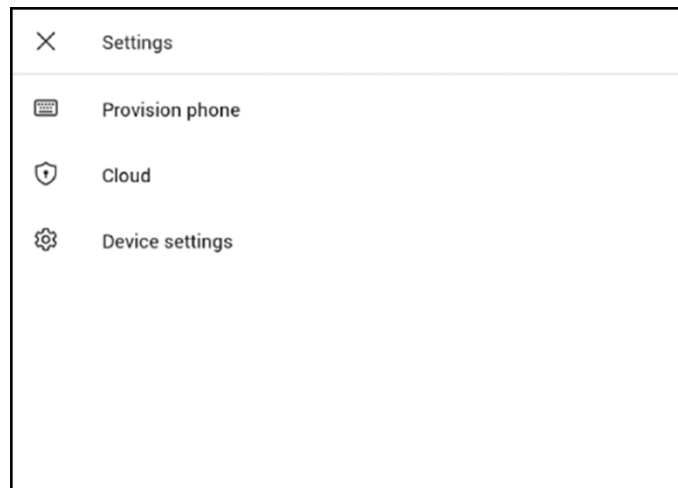
From the **Awaiting Activation** tab, select an existing MAC ID. A password is created for the MAC address and is shown in the **Verification Code** column.



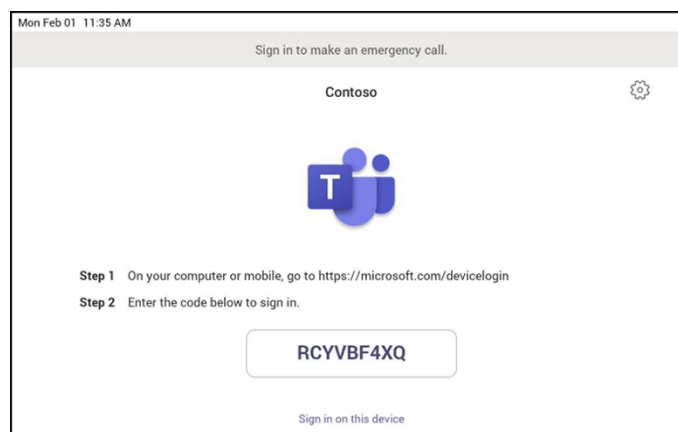
You'll need to provide the list of MAC IDs and verification codes to the field technicians. You can export the detail directly in a file and share the file with the technician who is doing the actual installation work.

➤ **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**.



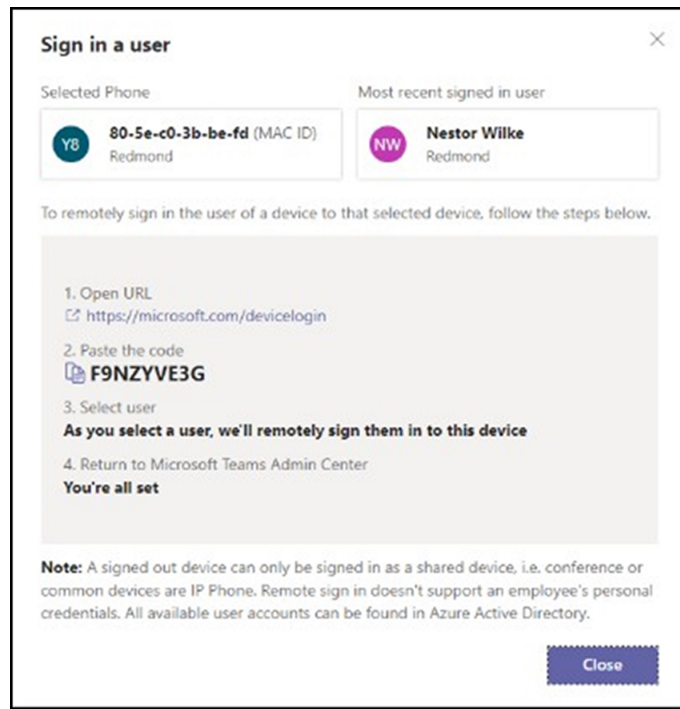
The technician is then expected to enter the device-specific Verification code that was provided in the Teams admin center on the phone's user interface. Once the device is provisioned successfully, the tenant name will be available on the sign in page.



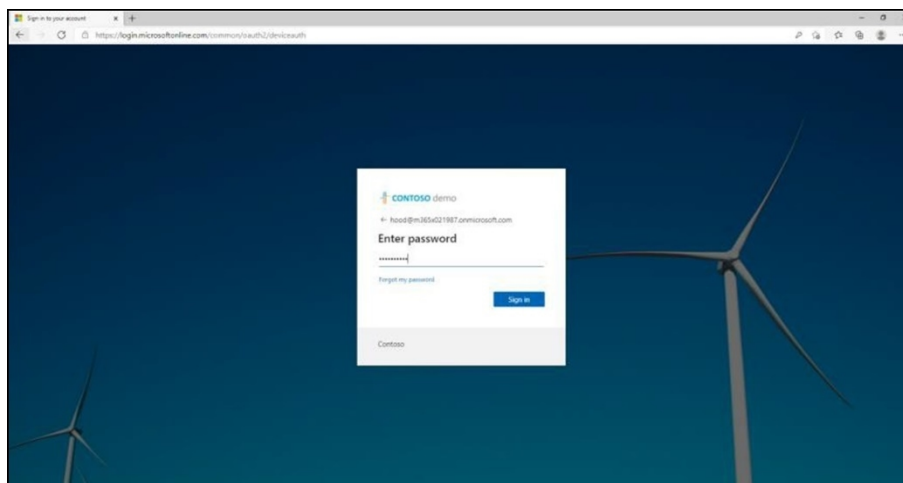
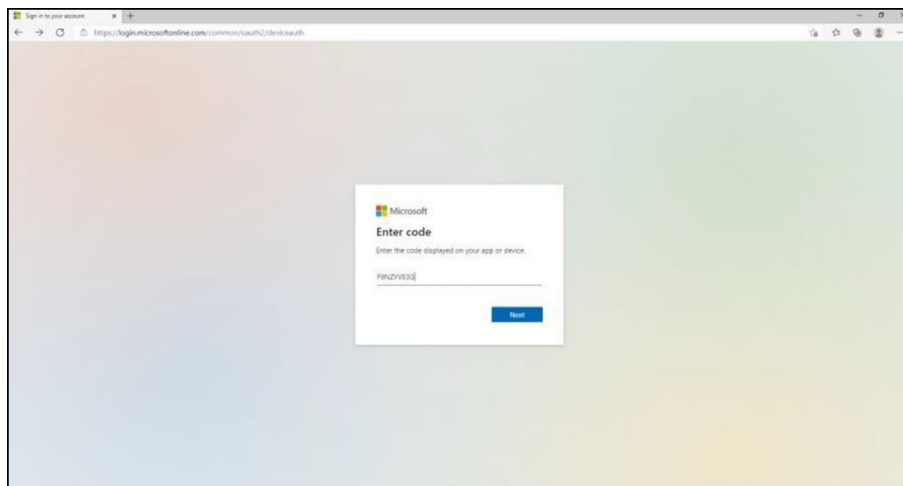
➤ **Step 4: Sign in remotely**

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

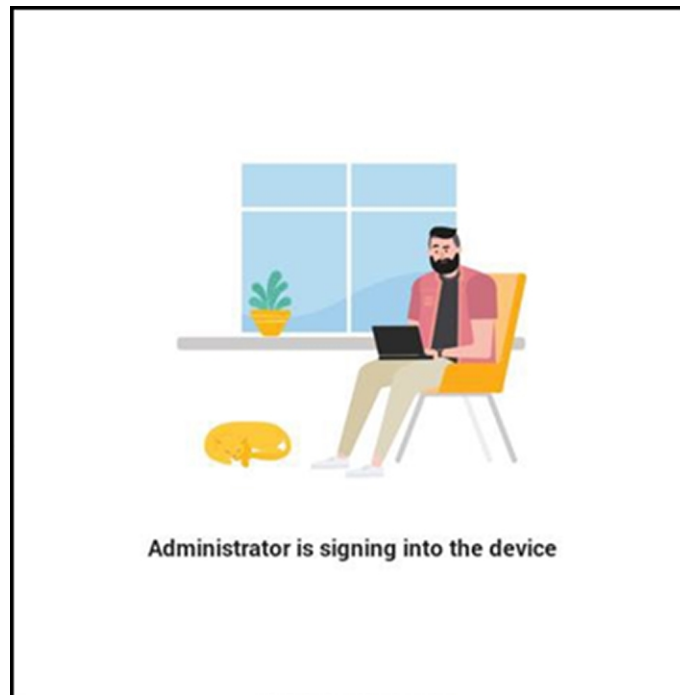
1. Select a device from the **Awaiting sign in** tab.
2. Follow the instructions in **Sign in a user**, and then select **Close**.



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

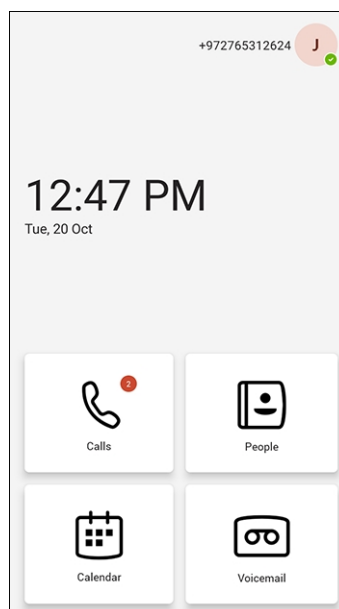


When the tenant admin is signing in from Teams Admin Center, the user interface on the device is blocked to prevent other actions on the phone.

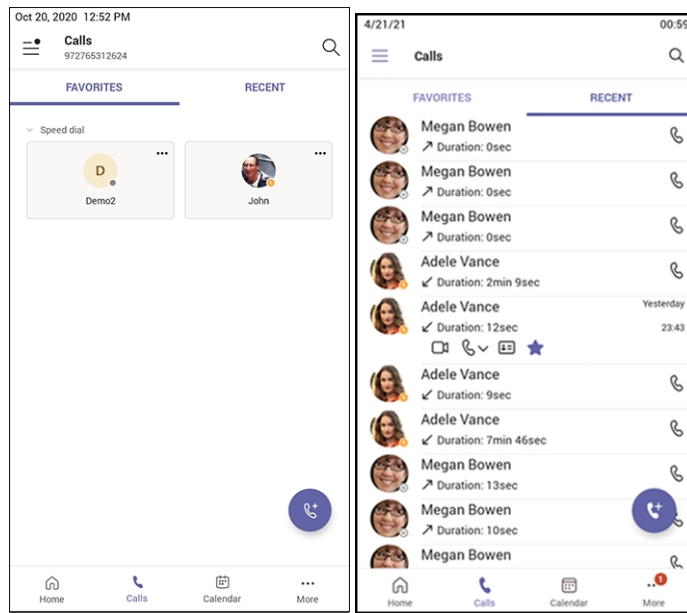


Getting Acquainted with the Phone Screen


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.



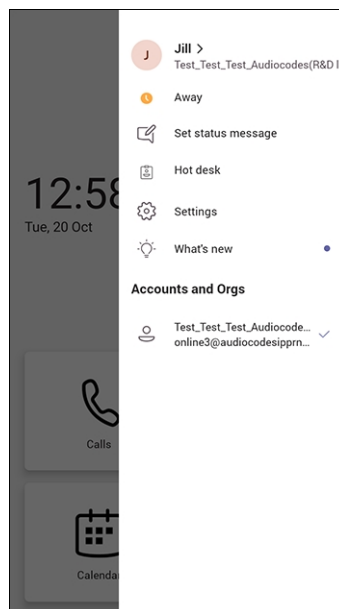
The following figure shows the phone's Calls screen.



The following table describes the phone's home screen.

Item	Description
	The phone menu. Select it to open the menu shown in the figure following this table.
Calls	Select the tab to open the Calls screen. The screen shown in the figure preceding this table opens.
People	<p>Select the tab to open the People, shown under Using the People Screen on page 72 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.</p> <p>If a contact has multiple numbers, the phone screen allows the user to select from a drop-down menu the intended contact method.</p>
Calendar	Select to open the Calendar screen, shown under Setting up a Meeting on page 72 opens.
Voicemail	Select the tab to open the Voicemail screen, shown under Accessing Voicemail on page 73 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 page 66 for more information.

Item	Description
Set status message	See Setting Status on page 64 for more information.
Connect a device	See Connecting a Device for more information.
Hot desk	See Hot Desking on page 65 for more information.
Settings	See Configuring Teams Application Settings on page 69 for more information.
Sign Out	See Signing Out on page 75 for more information.

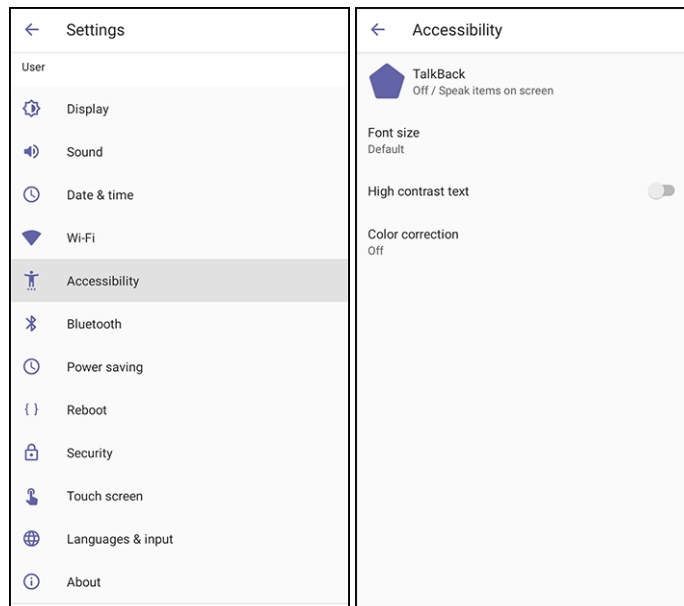
Enabling Google Talkback

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

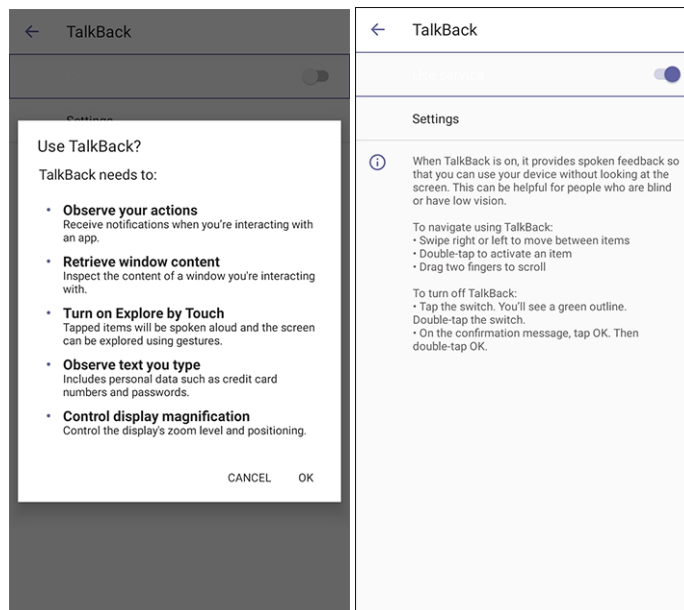
The feature improves the experience of these users.

➤ To enable the feature:

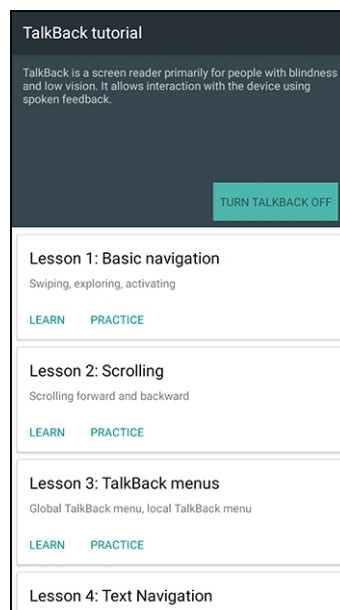
1. Open the Accessibility screen (**Settings > Device settings > Accessibility**).



2. Select the **TalkBack** option shown in the preceding figure.

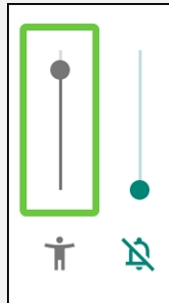


3. Click **OK** to switch the feature on as shown in the preceding figures. Listen to the audio tutorial that begins playing. The tutorial explains how to interact with the device.



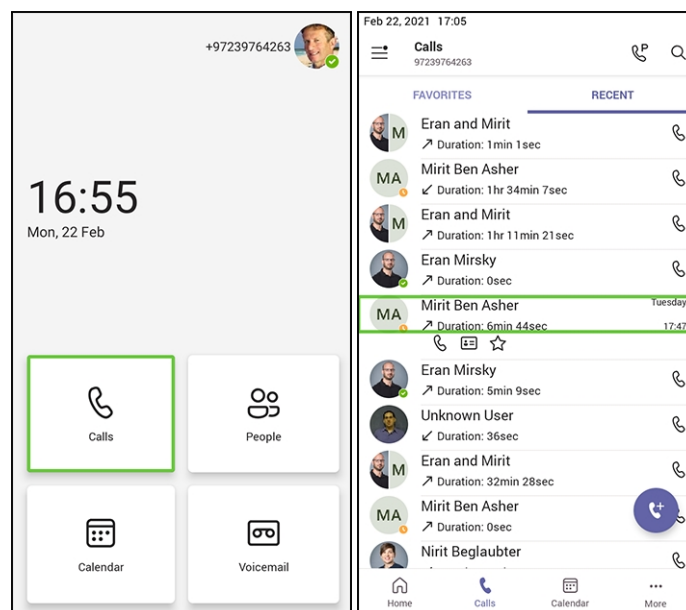


- After TalkBack is switched on, operations are performed by *touching to select* and then *double-touching to activate*.
- To turn up the volume, touch the **+** key on the phone and in the volume pop-up shown in the figure below, touch the slider to select it; audio announces what level you're at.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



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

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



➤ **To interact with the Calls screen:**

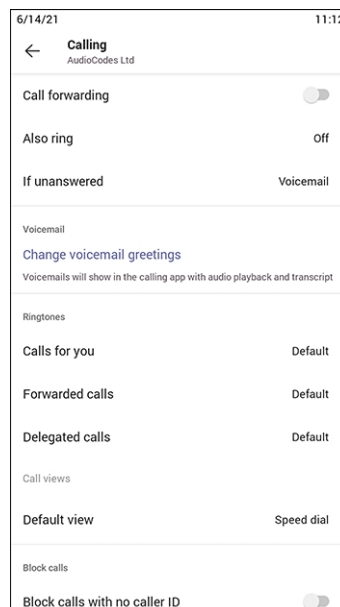
1. In the Calls screen shown in the preceding figure, select the **Recent** tab; audio informs you what you selected.
2. Select a listed call as shown in the preceding figure; audio informs you whether the call was outgoing or incoming and to / from whom it was made and the day on which it was made.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



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

Opting in or out of Call Queues

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

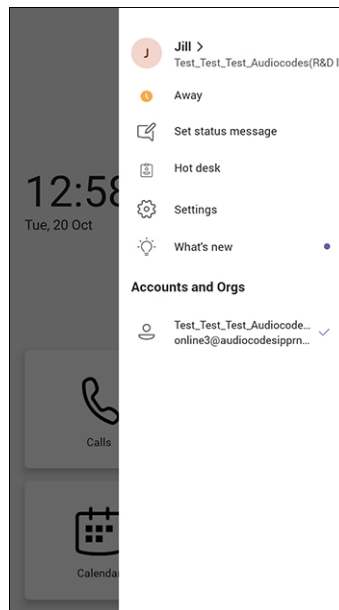


Setting Status

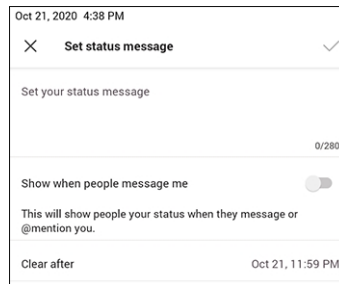
You can set a status message to add more substance to your presence status. For example, a status message such as 'Working from home' adds more substance to the presence status of 'Available'.

➤ To set presence status:

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



2. Select **Set status message**.



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

Hot Desking

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

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

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


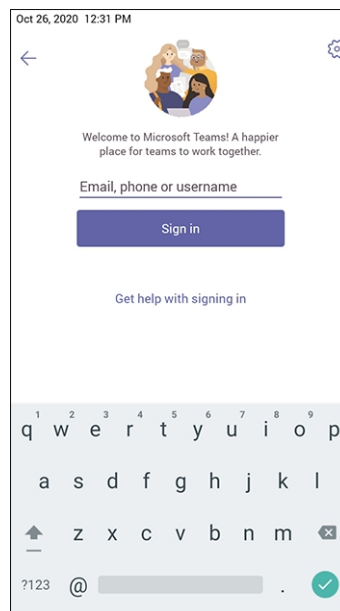
1. Select the user's photo or avatar picture, and then from the menu, select the **Hot desk** option. Alternatively, in the Calls screen (or People screen, Calendar screen or Voicemail screen), select the phone menu  and then select **Hot desk**.

Figure 4-3: Hot desk



2. Use the Virtual Keyboard to type in your email, phone or user name and then select **Done**; the phone is enabled for hot desk.


Changing Presence Status

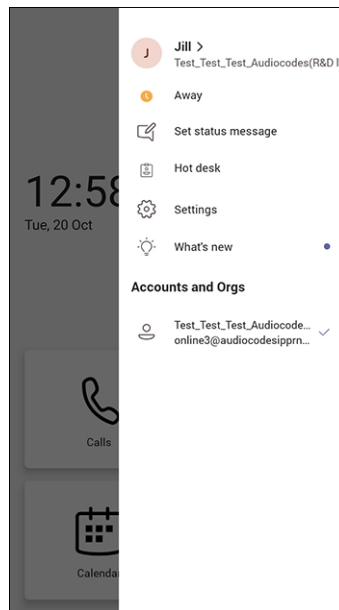
You can assign a presence status to control whether you want people to contact you or not. By default, your status is based on your Microsoft Teams server.



- 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 the user (avatar) picture or in the Calls and Calendar 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

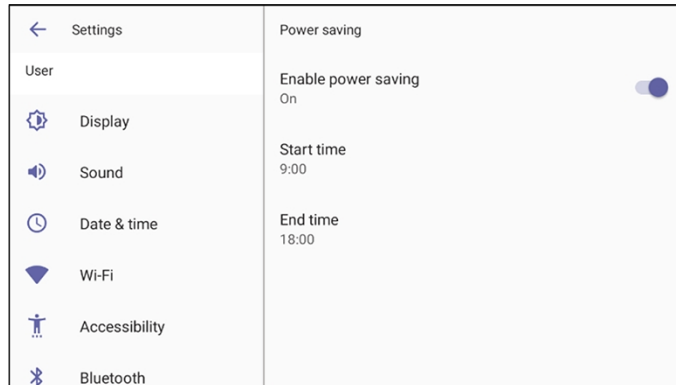
Icon	Presence Status	Description
	Available	You're online and available for other contacts to call.
	Busy	You're busy and don't want to be interrupted.
	Do not disturb	You don't want to be disturbed. Stops the phone from ringing when others call you. If DnD is activated, callers hear a tone indicating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

Power Saving

The phone's Message Waiting Indicator (MWI) shuts down during off hours. During off hours, the device's MWI / Presence LED is switched off and the LCD blacks out.

➤ To enable this feature:

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



- By default, the feature is disabled.
- The feature is based on off work hours and sleep timeout.

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: 0)
- `office_hours/end`
- `office_hours/start`

Enabling Voicemail Support on CAP Users

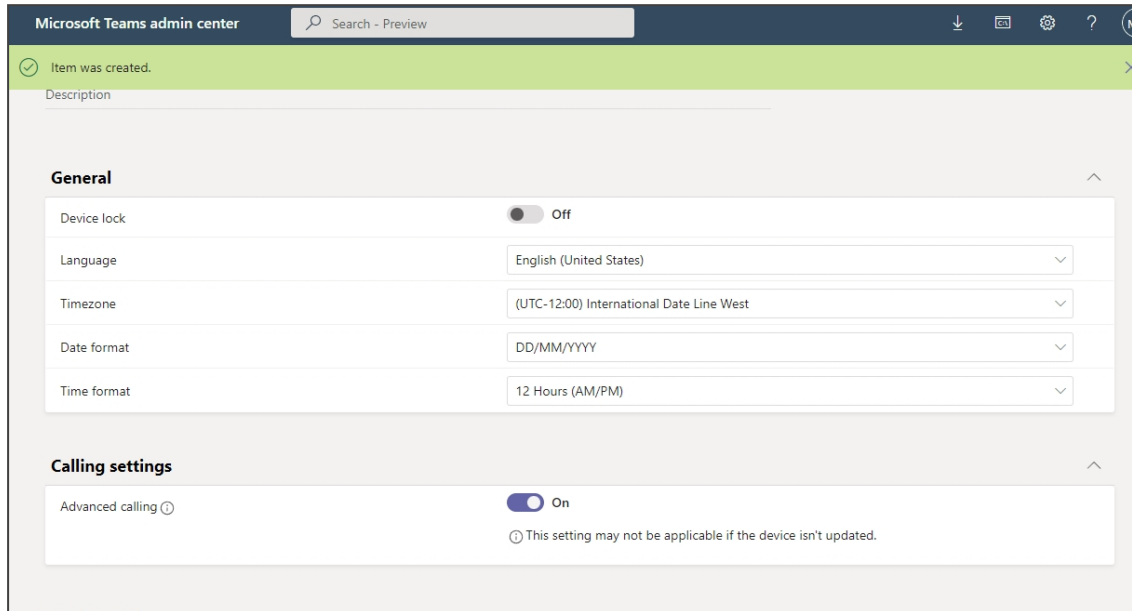
The instructions here show how to enable voicemail on common area phone users. Voicemail can be enabled from the phone or from the TAC. The **Advanced calling** setting must be enabled.

➤ To enable voicemail from the phone:


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

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

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



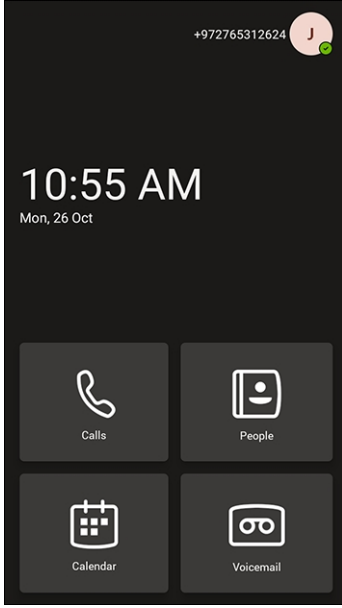
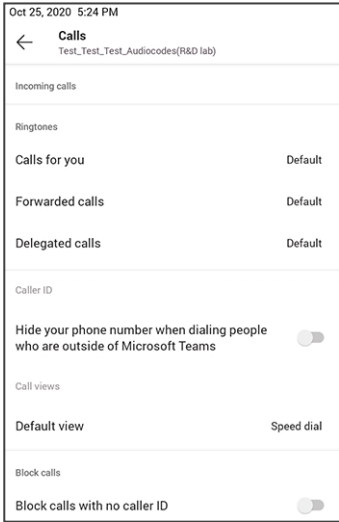
Configuring Teams Application Settings

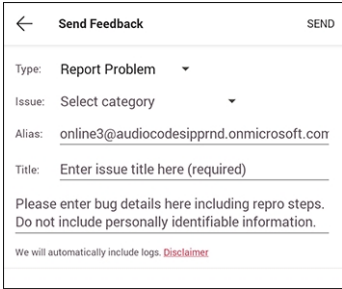
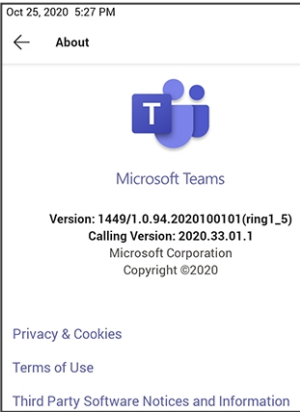
The following describes the Teams application's settings. In the home screen, select the user picture / avatar. Alternatively, in the Calls screen (or People screen, Calendar screen or Voicemail screen), select the phone menu  and then the **Settings** option.

Use this table as reference:

Table 4-2: Idle Screen Description

Item	Description
Dark Theme	<p>Dark Theme can be enabled to suit user preference. To enable Dark Theme:</p> <ol style="list-style-type: none"> 1. Drag the 'Dark Theme' setting slider to the 'on' position; the following prompt is displayed: <div data-bbox="756 1742 1203 1839" style="border: 1px solid black; padding: 5px; margin: 10px 0; text-align: center;"> You'll need to restart the app to switch themes. CANCEL RESTART </div> 2. Choose Restart and then verify after the Teams application restarts that all screens (Teams application and Device Settings) are dark themed:

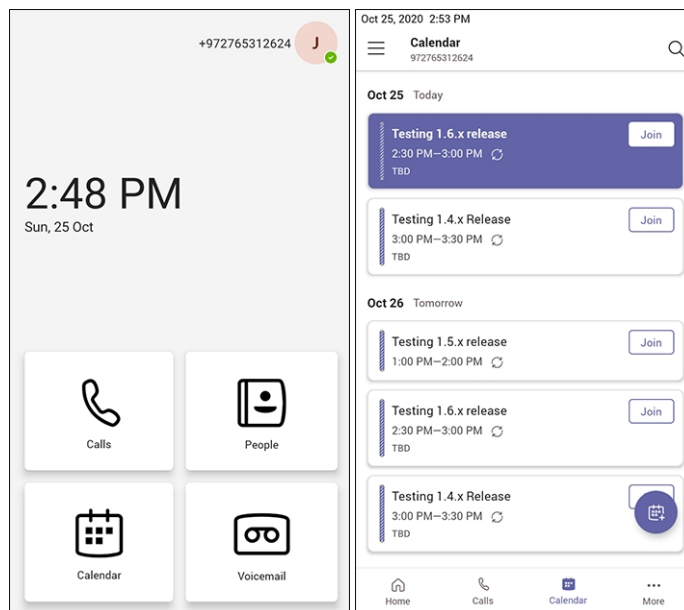
Item	Description
	
Profile	Opens the user's email address and photo / avatar picture.
Calling	<p>Opens the Calls screen.</p>  <p>Incoming Calls</p> <ul style="list-style-type: none"> ■ Call forwarding. Enables automatically redirecting an incoming call to another destination. ■ Forward to. Only displayed 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


Item	Description
	<p>number, or Call group.</p> <p>Caller ID</p> <ul style="list-style-type: none"> ■ Hide your phone number when dialing people who are outside of Microsoft Teams <p>Block Calls</p> <p>Block calls with no caller ID. Enables blocking calls that do not have a Caller ID.</p>
Home screen	Default: On (enabled). Slide left to switch off (disable) and block the home screen from view; the Calendar screen takes its place.
Notifications	Default: On (enabled). Allows notifications to be displayed. Slide left to switch off (disable); notifications will not be displayed.
Report an issue	<p>Microsoft Teams application's 'Report an issue' option opens the Send Feedback screen.</p>  <p>'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.</p>
About	<p>Opens the About screen.</p> 
Sign out	Lets you sign out of the phone application as one user and optionally

Item	Description
	sign in again as another user. See Signing Out on page 75 for detailed information.
Device Settings	Opens the [Device] Settings screen. See Configuring Device Settings on page 18 for detailed information.

Setting up a Meeting

From the phone's home screen, select **Calendar**.



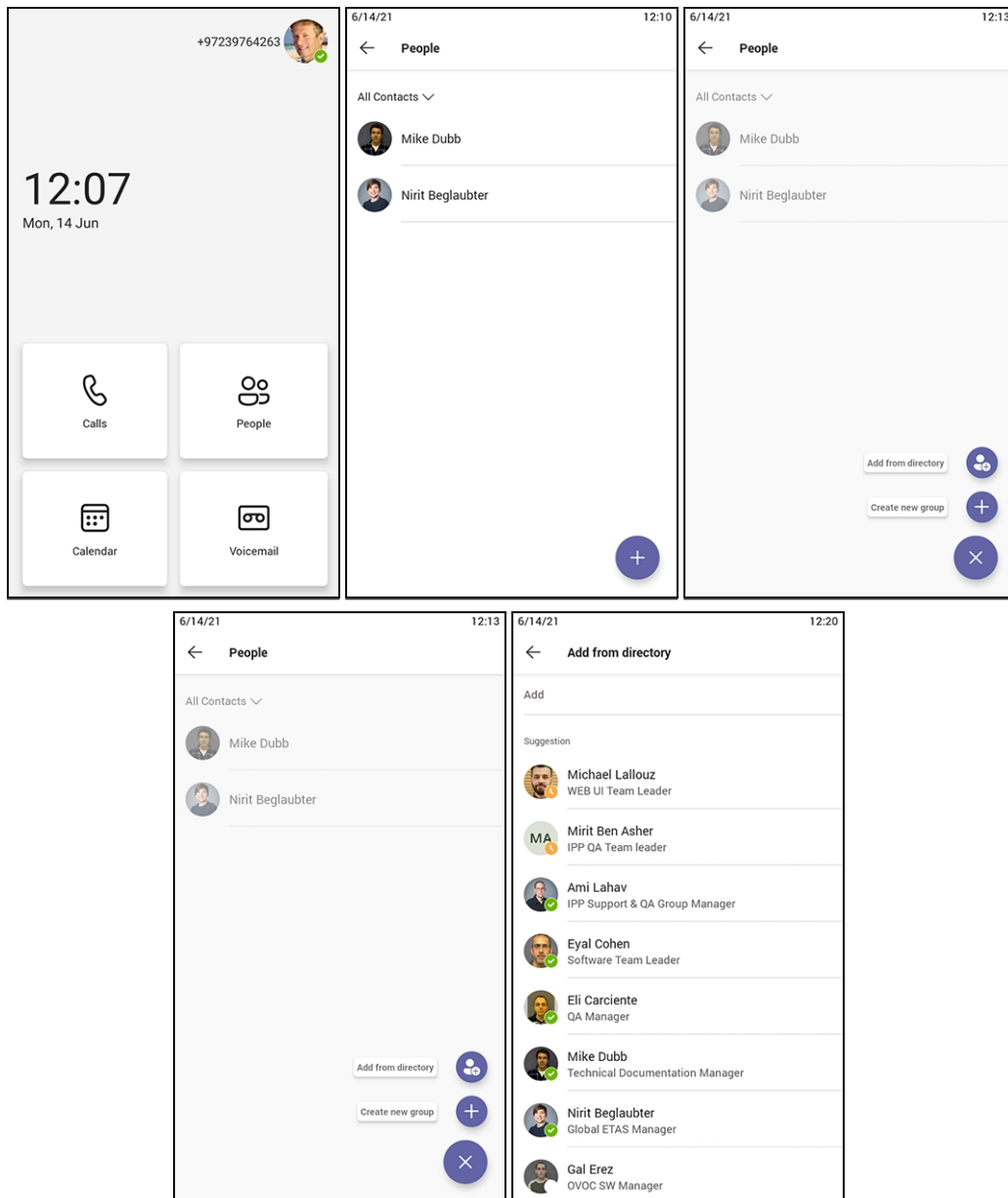
You can join calendered meetings and / or you can select  to add a new event to the calendar. See [here](#) for a video clip demonstrating how to join a scheduled meeting.

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.

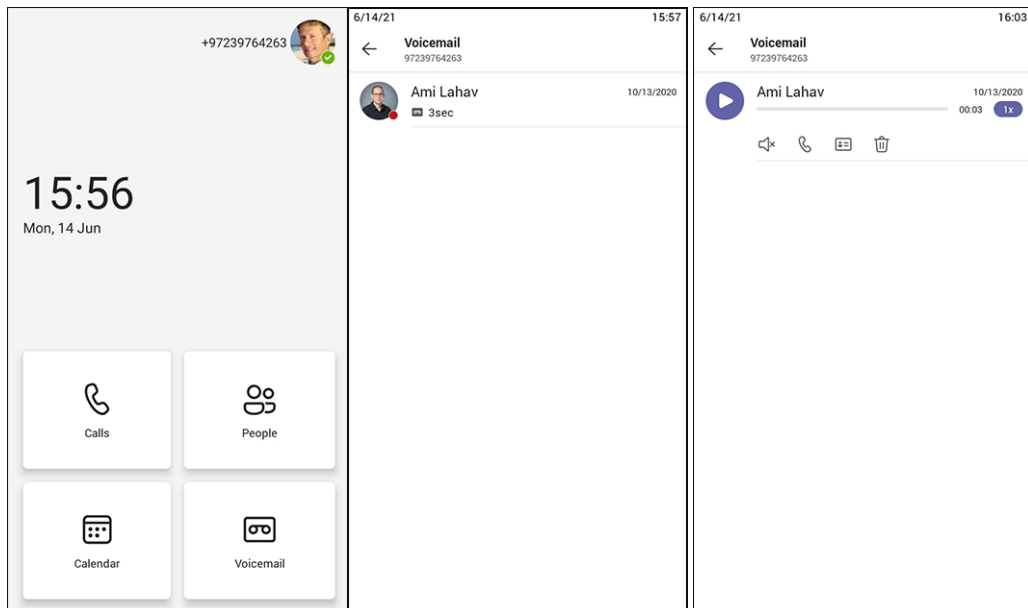


If a user creates a contact within Microsoft Outlook, their information appears under the People app on the phone screen. Contacts in Microsoft Outlook are available in read-only mode. While only phone numbers currently appear, users can search on the phone for contacts and easily call the people they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



Accessing Voicemail

From the phone's home screen, select the **Voicemail** tab.



Using Audio Devices

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

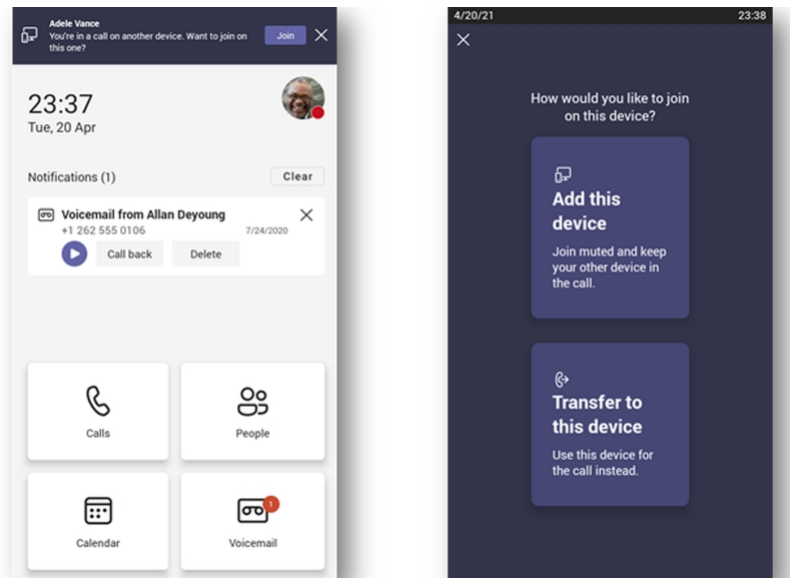
- **Handset:** To make a call or answer a call, lift the handset off the cradle.
- **Speaker (hands-free mode)**
 - To activate it, press the speaker key during a call or when making a call.
 - To deactivate it, press the speaker key again.
- **Headset (hands-free mode).** When talking on the phone,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

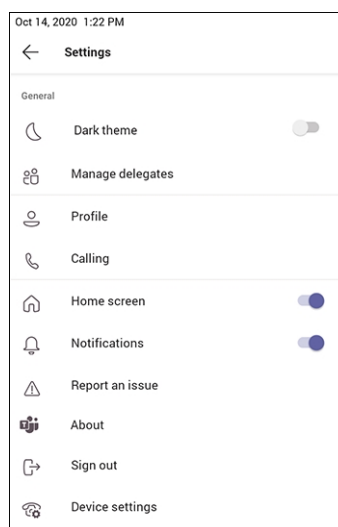
You can optionally sign out of the phone application and sign in as another user.

➤ To sign out:

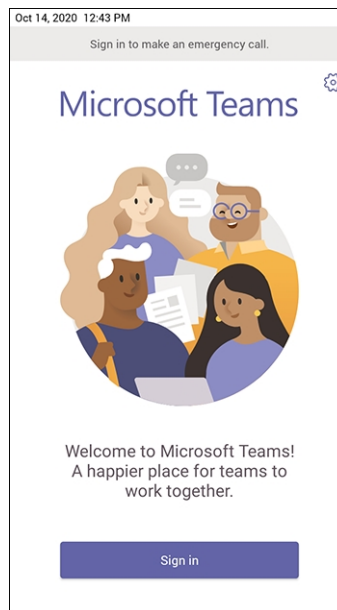
1. Under **Settings**, navigate to and select the **Sign out** option.



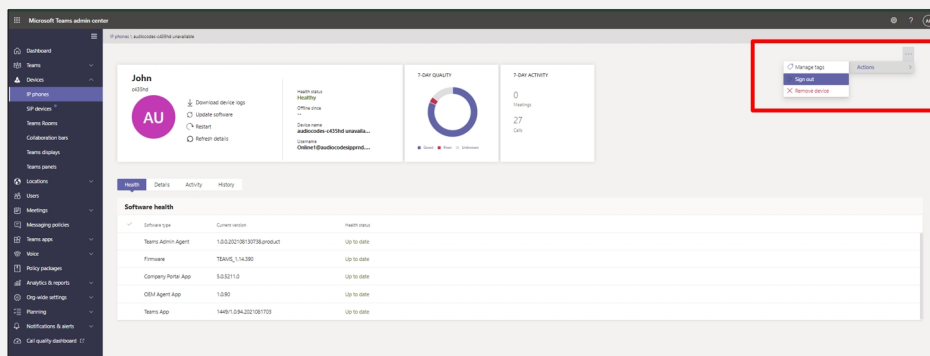
Alternatively, in the Calls screen (or People screen, Calendar screen or Voicemail screen), select the phone menu , select the **Settings** option.



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.

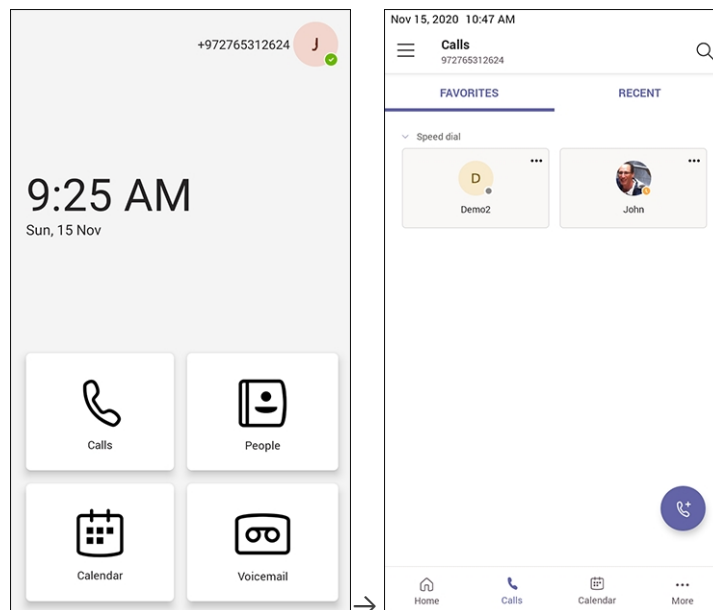



5 Performing Teams Call Operations

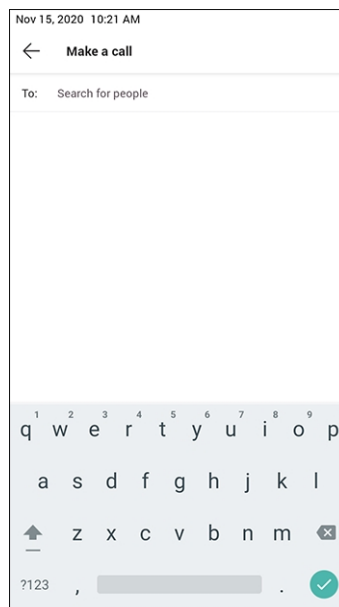
The following documentation shows how to perform basic operations with the phone.

Making a Call

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




In the Calls screen that opens, touch .



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


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

➤ **To toggle between mute and unmute:**

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

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

➤ **To toggle between device and speaker:**

- Touch  on the phone.

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

- Touch .

➤ **To dial a URL:**

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

Microsoft Lightweight Calling Experience

AudioCodes' phones feature a *simplified look and feel* for incoming and outgoing calls, improving phone performance.

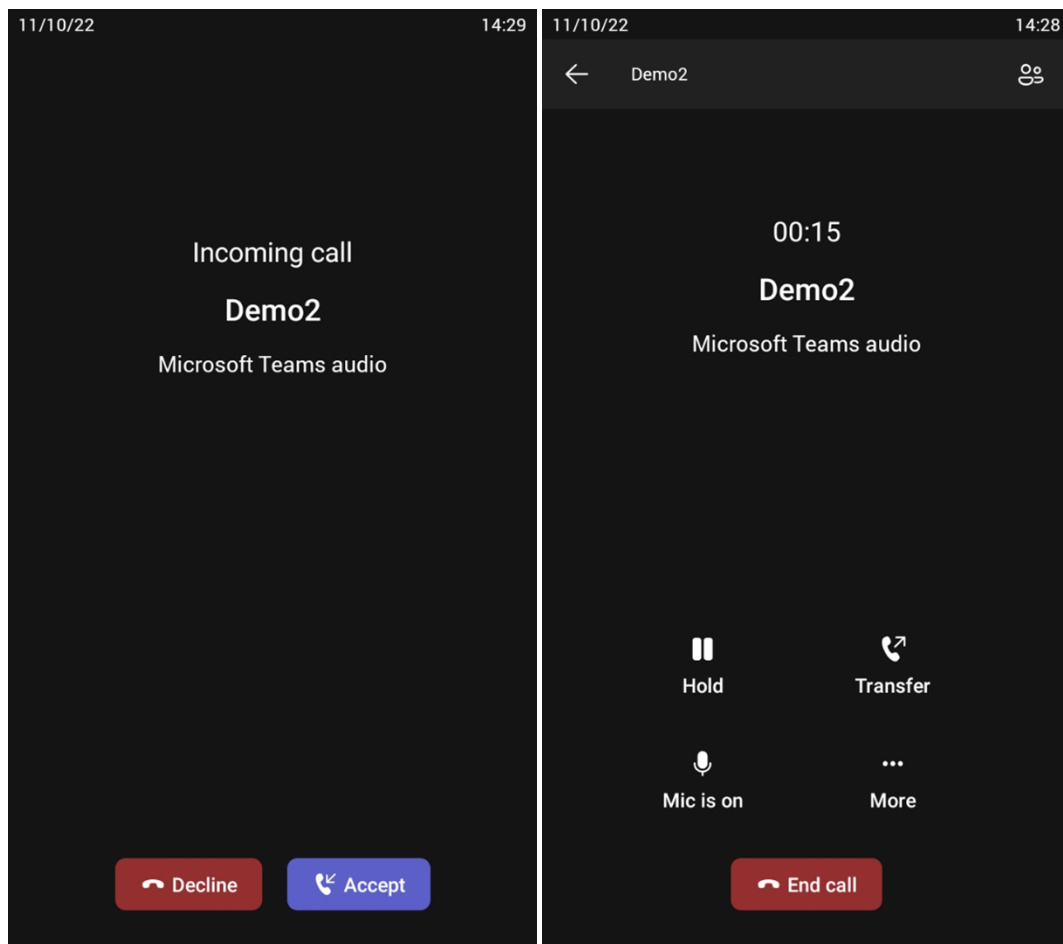


The feature is enabled by default.

➤ **To disable the feature:**

- On the phone, navigate to **Teams Application Settings > Calling > Enable lightweight calling experience** and switch it off.


The figure below shows an incoming call screen when the feature is enabled while the figure below it shows the ongoing call screen when the feature is enabled.



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:

- Select **Calls** and then in the Calls screen under the **Recent** tab, scroll to the missed call to dial if there is more than one listed.
- Select  adjacent to 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

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.

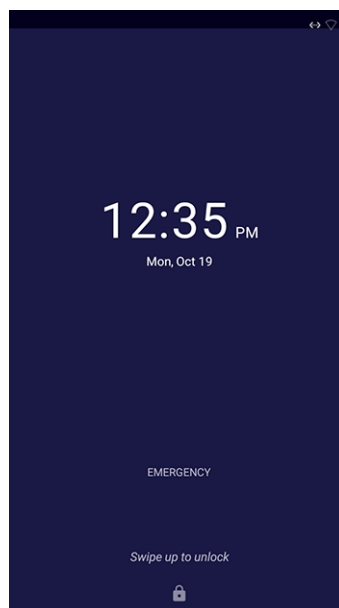
See [here](#) for a video clip demonstrating how to immediately transfer a call without verifying with the intended recipient that they want to take the call. The principle is similar across AudioCodes Teams phones.

➤ **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:**

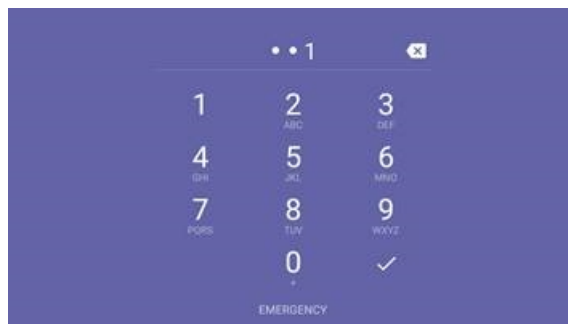
- Select the **EMERGENCY** softkey shown in the preceding figure of the locked idle screen and then enter the emergency number.



-OR-

- Dial from the locked idle screen without needing to use the **EMERGENCY** key:

a. Dial **911**.



- b. Activate the speaker button on the phone.
- c. View the 'Emergency call' screen displaying the dialed emergency number.



When the phone detects that 911 was requested, it automatically dials that 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.

Using Boss-Admin

Bosses can share their phone line with their assistants|delegates to make and receive calls on their behalf.

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

A boss can:

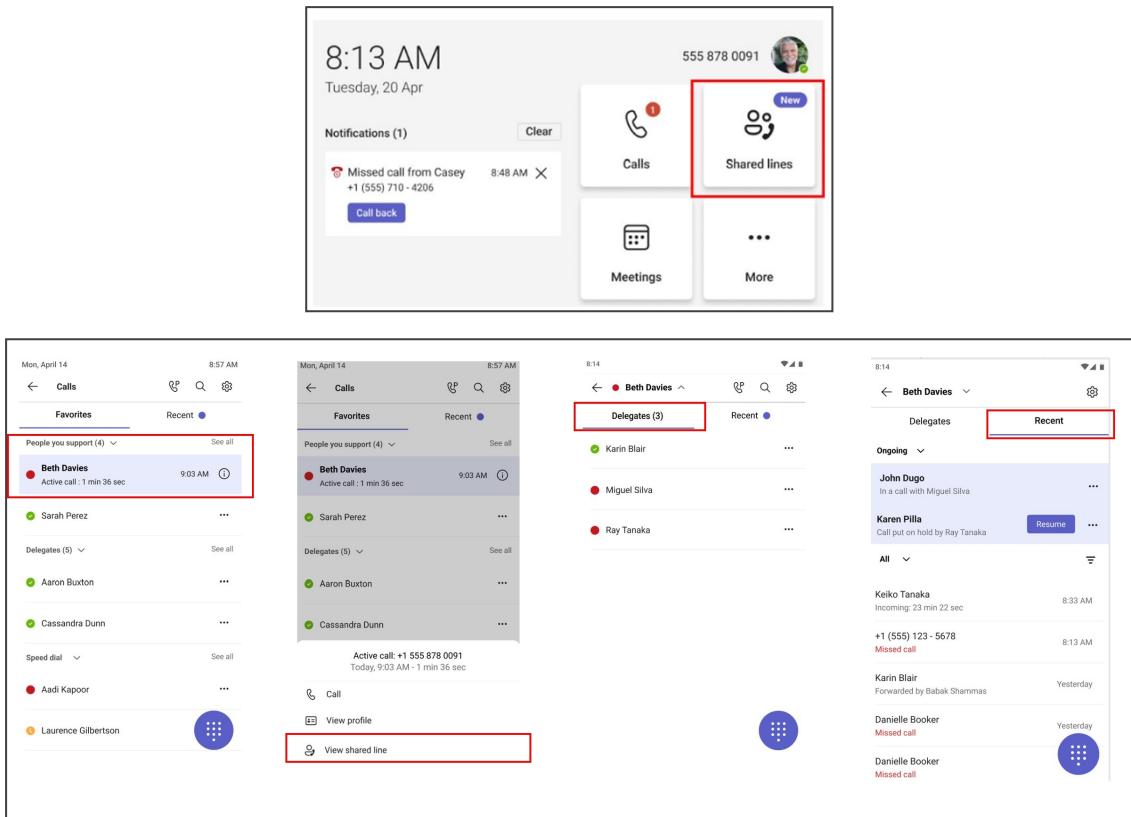
- View and join active calls handled by delegates as a boss
- Grant delegates permission to join active calls and resume calls

A delegate can:

- View shared call history per boss' line
- Switch between different lines easily
- View other delegates managing a boss

➤ **To set up the feature:**


- Use the screenshots below as reference.

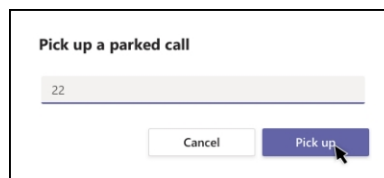


Parking a Call

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

➤ **To park a call:**

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



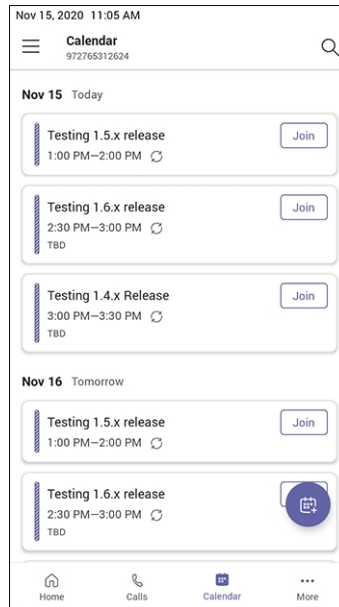
3. The user on the other device enters the code communicated to them and then selects the **Pick up** button to pick up the call.


Managing Teams Meetings

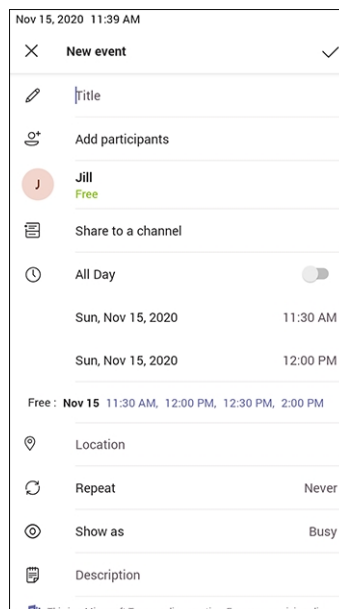
Multi-party conference meetings based on the Teams server (remote conference) can be calendered and initiated from the phone.

➤ **To manage conference meetings:**

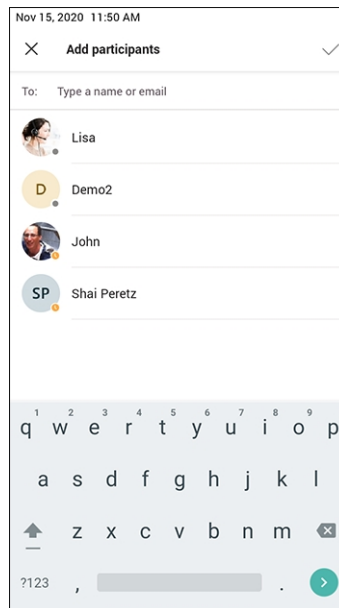
1. In the phone's home screen, select **Calendar**.



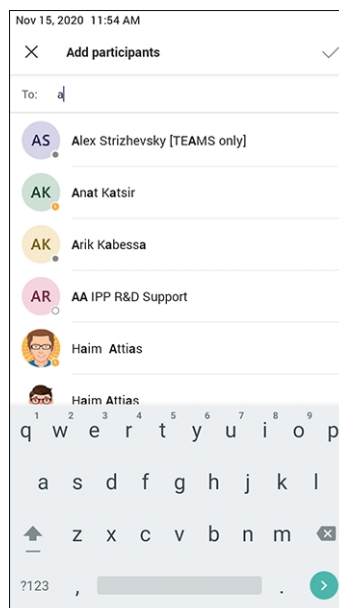
2. Touch the  icon.





3. In the 'New event' screen, touch the 'Title' field and then use the virtual keyboard that launches to enter a title for the meeting.
4. Touch the 'Add participants' field.



5. In the 'Add participants' field, touch the 'To:' field and input the first digit in the name of a participant to add; the names of the employees listed in the Corporate Directory is displayed.



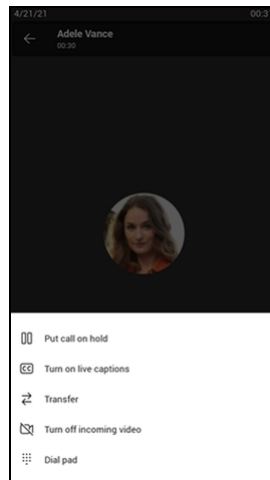
6. Touch an entry in the list and then touch ; the participant is added to the meeting.
7. Define 'Share to a channel', date, date and time, 'Location', 'Show as' and provide a 'Description' of the meeting to facilitate effective management later.
8. Touch the  icon; the meeting is calendarized.

Using Live Captions

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



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



For more information, see [here](#).

Raising a Hand During a Meeting

During a meeting, you can raise a virtual hand from your phone to let people know you want to contribute without interrupting the conversation. Everyone in the meeting will see that you've got your hand up.

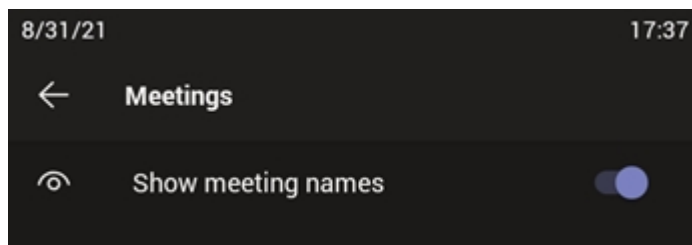
For more information, see [here](#).

Hiding Names and Meeting Titles for Individual Devices

Names and meeting titles can be hidden for individual devices.

➤ To hide names and meeting titles per device:

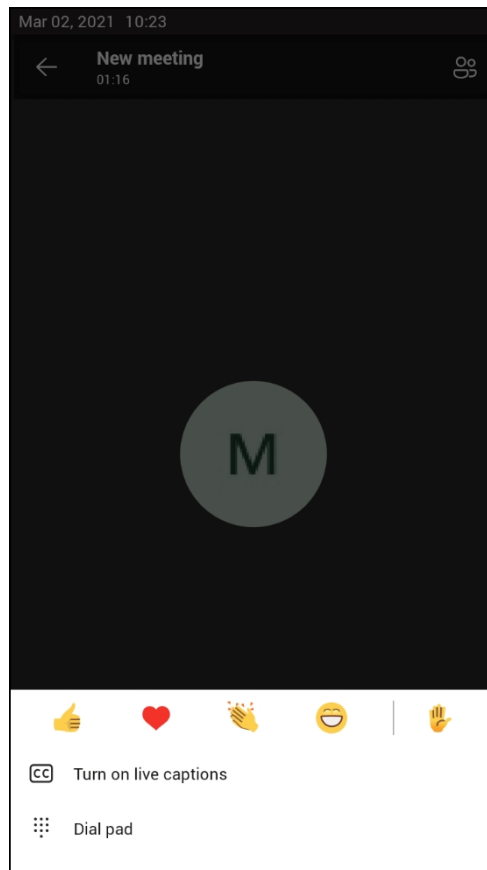
1. Access the Meetings screen (**More > Settings > Meetings**) (the figure is for illustrative purposes only).



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

Reacting During a Meeting

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



Users can convey their sentiments without hesitation or interruption to participate in the meeting, or they can raise their hands.

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.

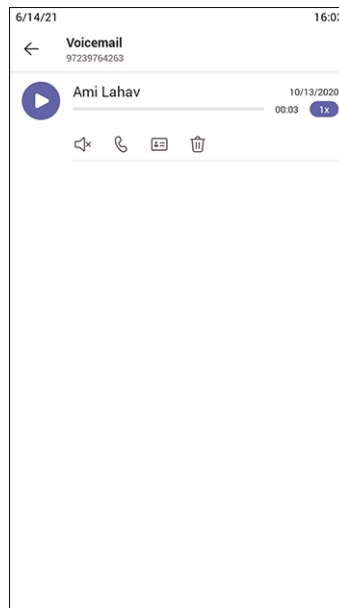
Viewing and Playing Voicemail Messages

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.

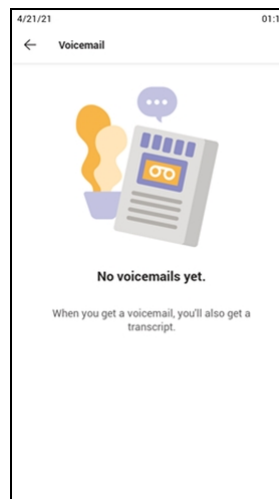
See [here](#) for a video clip demonstrating how to view and play voicemail messages.

➤ To view a list of your voicemail messages:

1. In the phone's home screen, select the **Voicemail** icon .



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](#) below
- [Adjusting Tones Volume](#) below (e.g., dial tone)
- [Adjusting Handset Volume](#) below
- [Adjusting Speaker Volume](#) on the next page
- [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, tap + or - 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. Touch + or - on the phone.
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. Touch + or - on the phone; 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. Touch + or -; 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. Touch + or - on the phone; 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.

Click [here](#) to view a video clip demonstrating how to connect a USB headset to the phone.

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

- Configure the following parameter:

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

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

Using the Phone as a USB Speaker

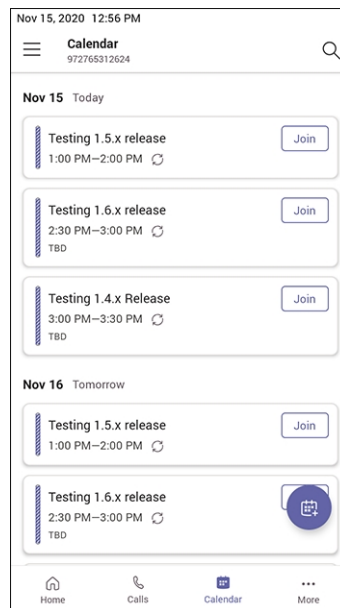
The Device Duo feature enables the phone to be configured as a paired audio device. The feature allows users to use their phone not only as a standalone desk phone but also as a smart audio device for all kinds of UC applications running on the PC. From the Teams app perspective, the phone is like any USB speaker with all controls available in the Teams app on the USB speaker interface.



For more information, see the *Device Duo Application Note*.

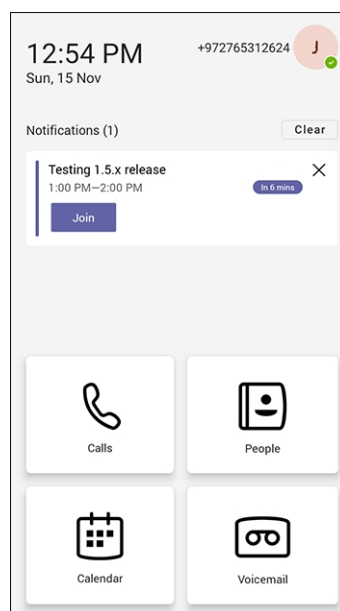
Viewing and Joining Meetings

Scheduled meetings can be viewed and joined by selecting the **Calendar** icon in the phone's home screen.



➤ To view the details of a meeting:

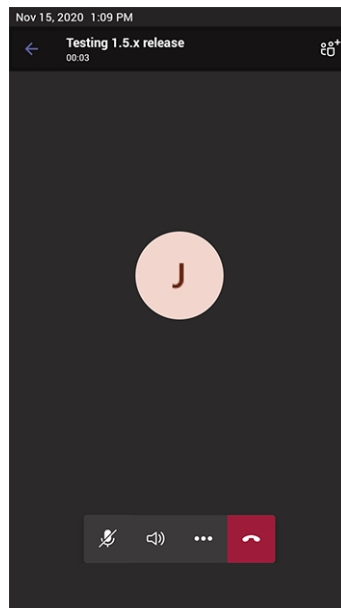
1. Scroll down if necessary to the meeting whose details you want to view and select it.



2. View the details of the meeting under 'Notifications'.

➤ To join a meeting:

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



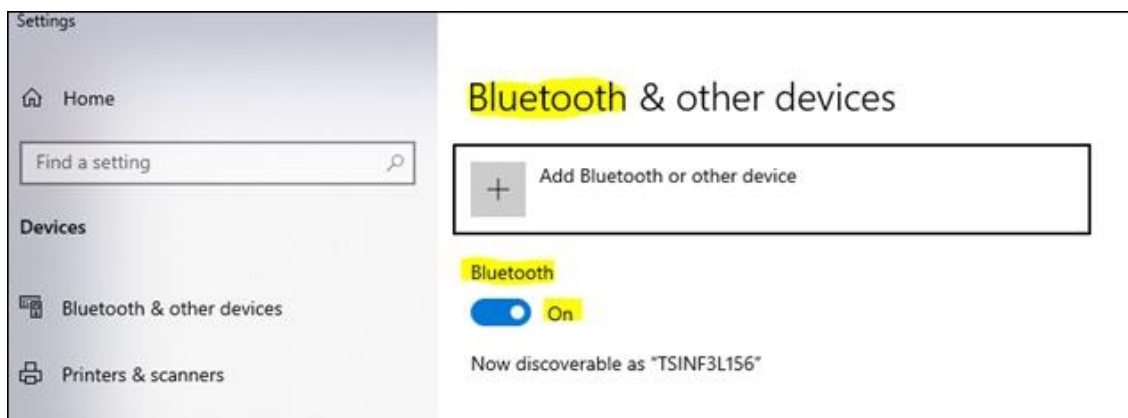
Better Together over Bluetooth

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

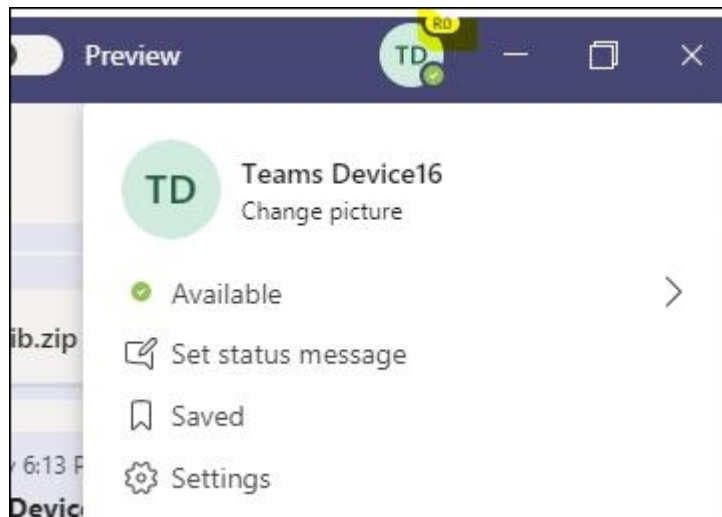
- Pairing with the Teams PC Client
- Lock/unlock synchronization
- [As a feature in preview] Use of the phone as the Teams audio device for calls / meetings

➤ To set up Bluetooth on the PC side:

1. Enable Bluetooth on your PC.

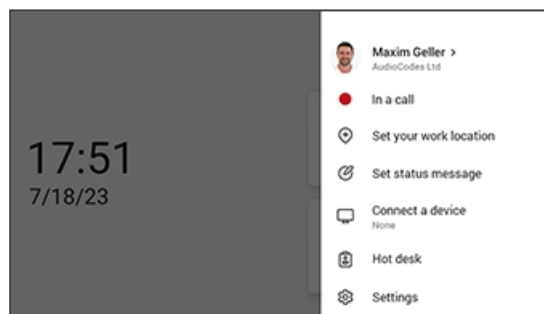


2. Install Teams PC Client on the PC.
3. Sign in to the Teams PC Client with your account (it's necessary to sign in with the same accounts to both the Teams PC Client and to the device).

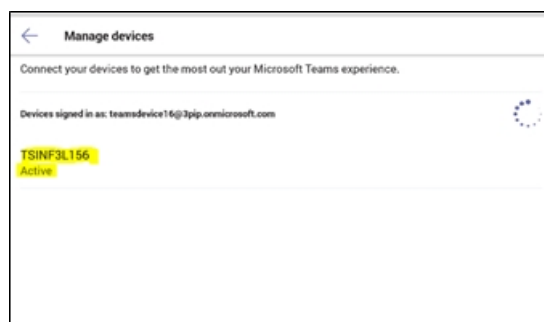


➤ **To set up Bluetooth on the device side:**

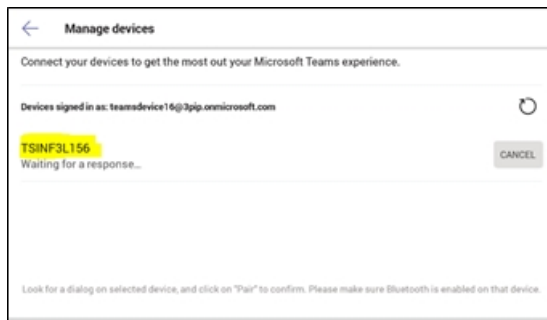
1. Sign in to the Teams application with your account (it's necessary to sign in with the same accounts to both the Teams PC Client and to the device).
2. Touch the avatar and then touch **Connect a device**.



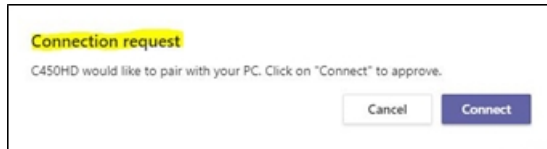
3. View the displayed available device to connect to.



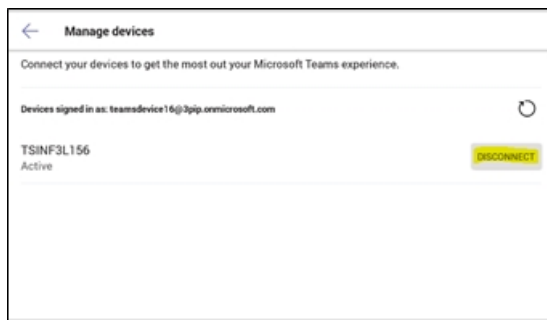
4. Pair the device with your PC.



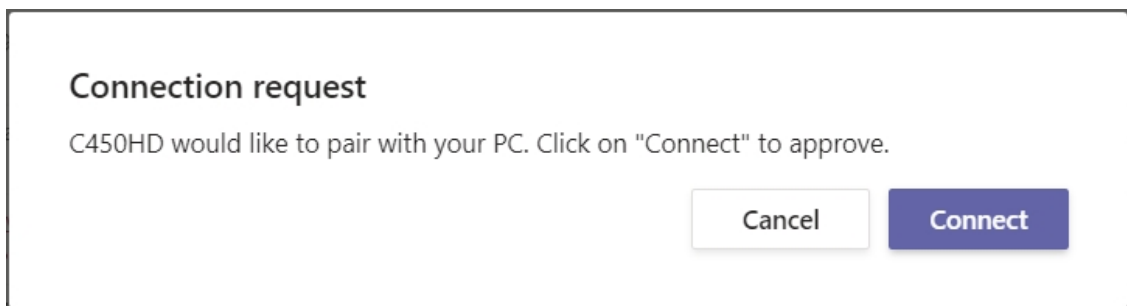
5. View on your PC a notification it gets to accept the connection:



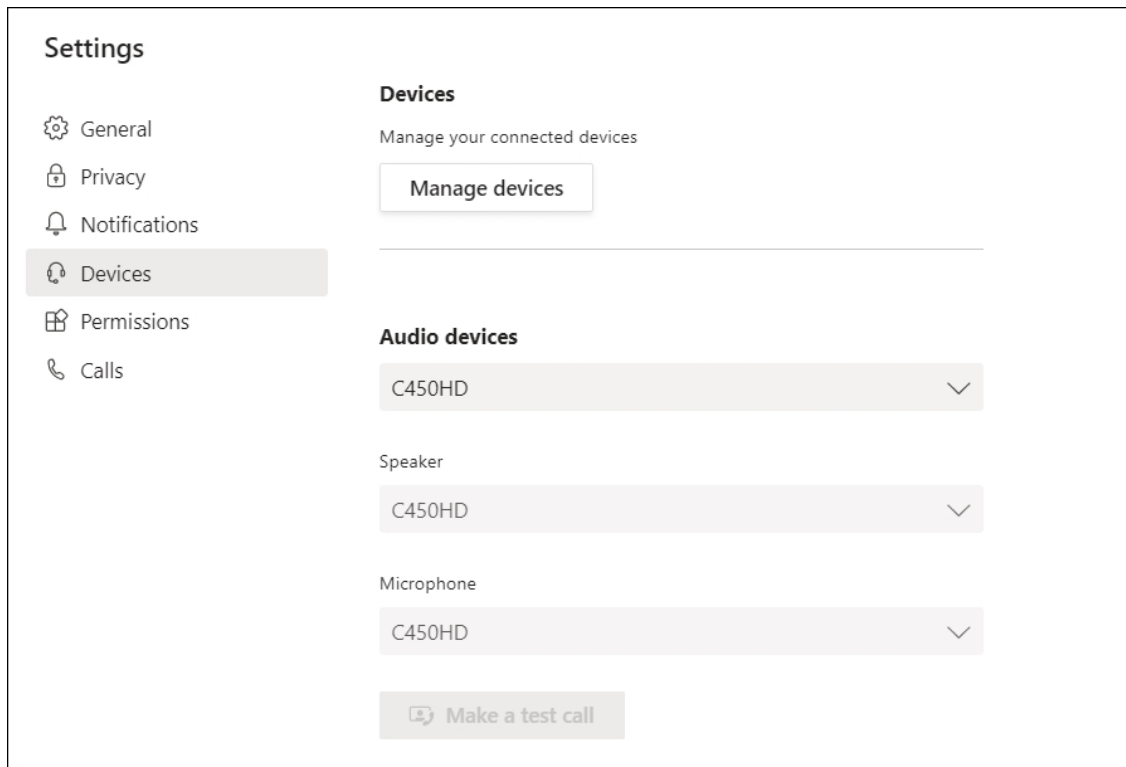
6. Accept the notification from PC.
7. Check the device and make sure pairing was successful:



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



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



Adding a Speed Dial



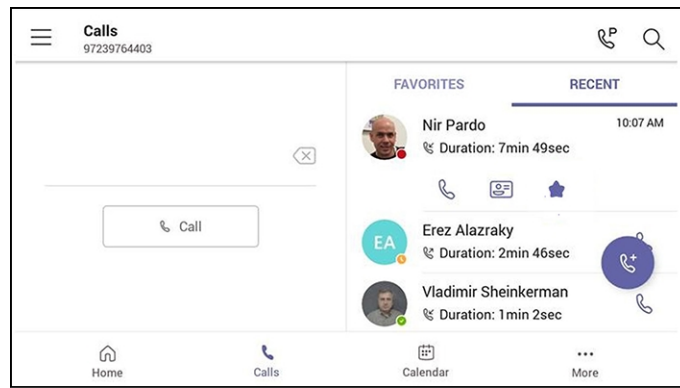
- The feature expands the phone's functional capabilities.
- Users can configure speed dials in the sidecar's BLFs to speed dial frequently-used contacts with the press of a button, determine contacts' presence status from BLF button LEDs, and manage contacts quickly.
- The feature also allows the user to easily transfer a call to a speed dial contact.
- The feature increases user productivity in the workplace.

➤ To add a speed dial:

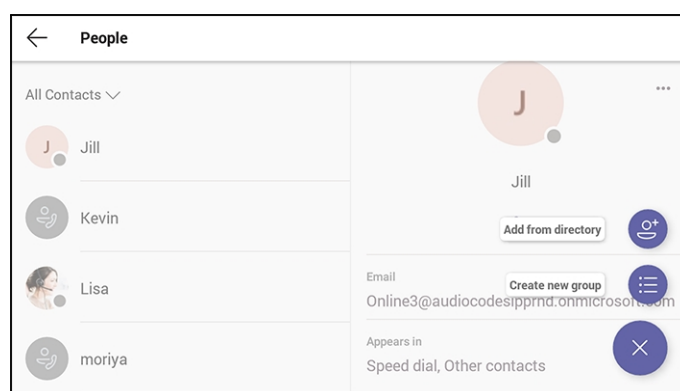
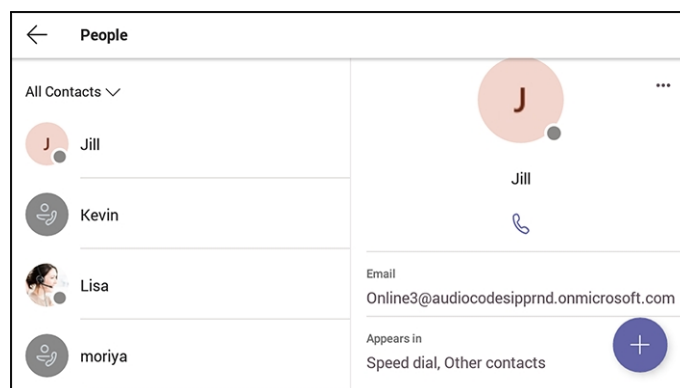
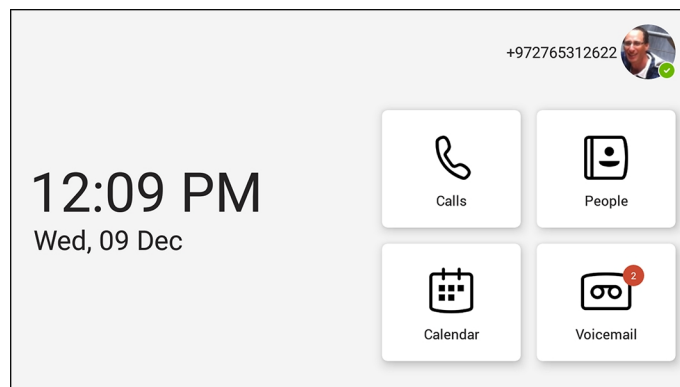
- Add it from the Teams PC client; adding a speed dial from the PC client will be reflected on the sidecar as well.

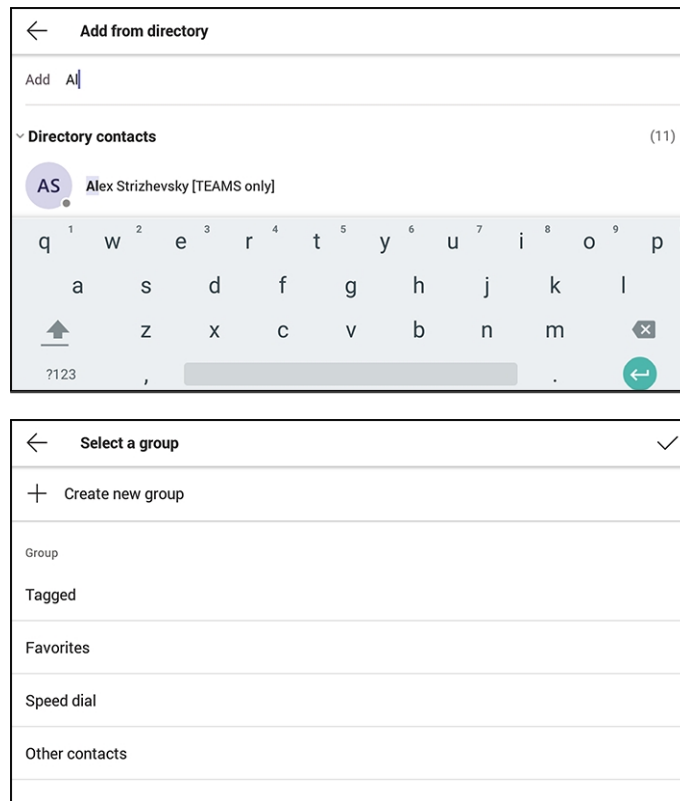
-OR-

- Add it from the phone using one of the following options:
 - a. Via the **Calls > Recent** tab. Select a user and then select the 'star' icon to add them to the speed dial list:



- b. Via the **People** tab using + > **Add from Directory** and then add the users to the speed dial.





The sidecar displays the user's speed dial list. The list is synchronized on all devices under the same user account. The order on the sidecar corresponds to the order of the speed dial list.

Adding a Speed Dial Group

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

See [here](#) for a video clip demonstrating how to create a speed dial group.

➤ To create a speed dial group:

1. Click **People**.
2. From the list, select the contact you want to add to your new group.
3. Select **Add to group**.
4. In the 'Select a group to edit' screen, choose **Speed dial**.
5. After adding the new contact, view them displayed.

6 Performing Administrator-Related Operations

Network administrators can:

Update phone firmware manually (see [Updating Phone Firmware Manually](#) on page 104)

Manually perform recovery operations (see [Manually Performing Recovery Operations](#) on page 112)

Remove devices from Intune management (see [Removing Devices from Intune admin center](#) on page 114)

Update Microsoft Teams devices remotely (see [Updating Microsoft Teams Devices Remotely](#) on page 117)

Manage phones with the Device Manager (see [Managing Phones with the Device Manager](#) on page 120)

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.

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**.

The screenshot shows the Microsoft Teams admin center interface. The left-hand navigation pane is open, with 'Locations' selected and 'Emergency addresses' highlighted. The main content area displays the 'Emergency addresses' page. At the top, there is a '+ Add' button, 'Edit', and 'Delete' icons. Below this is a table with the following data:


Description	Country or region	Address	Phone numbers	Voice use
AudioCodes	United Kingdom	44 1252 759150 Alexandra Road, Farnborough , Ferneberga H...	0	0
AudioCodes Inc.	United States	27 WORLDS FAIR DR, FRANKLIN TWP NJ 08873, US,	138	162
AudioCodes - France & Benelux	France	104 Avenue Albert 1er - Les Passerelles, Rueil-Malmaison 925...	0	0
AI-Logix Europe	Netherlands	57 Geerweg, TER AAR 2461 TT, NL,	0	0
test1105	United States	1 Little Albany Street, New Brunswick NJ 08901, US,	1	3
test2906	United States	30 Worlds Fair Drive, Franklin NJ 08873, US,	1	1
test0307	United States	32 Worlds Fair Drive, Franklin NJ 08873, US,	0	0
Test Oleg	United States	11 Worlds Fair Drive, Franklin NJ 08873, US,	0	0
test0407	United States	13 Worlds Fair Drive, Franklin NJ 08873, US,	0	1

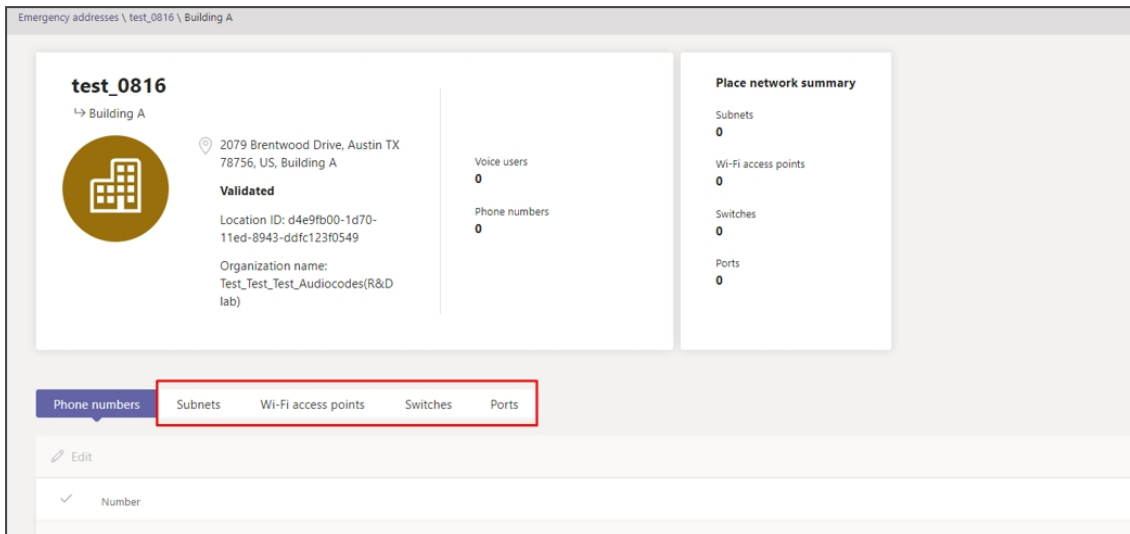
2. Enter a name for the location, enable **insert address manually**, make sure that all data is filled in correctly and then click **Save**.

- 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.

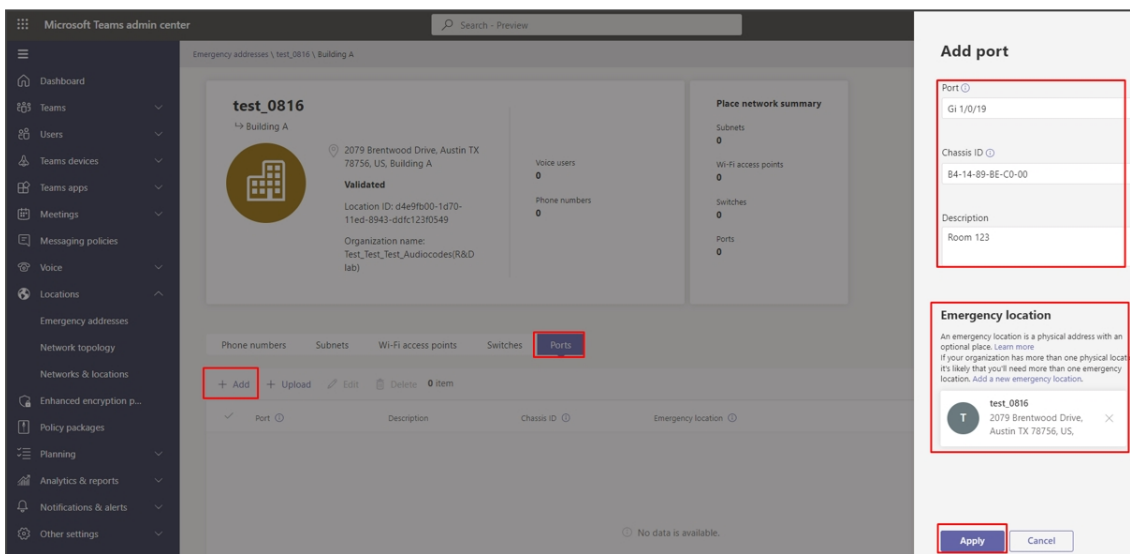
- Enter the place you've set and define how to determine the emergency location. It can be determined by these values:

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

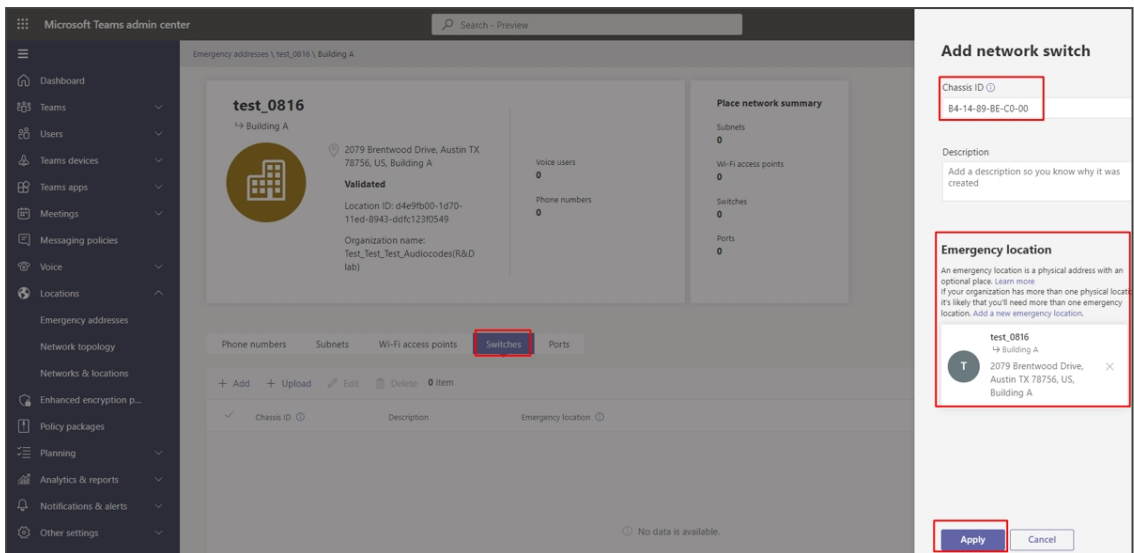
 The hierarchy of displaying a location is determined in the same order as above.



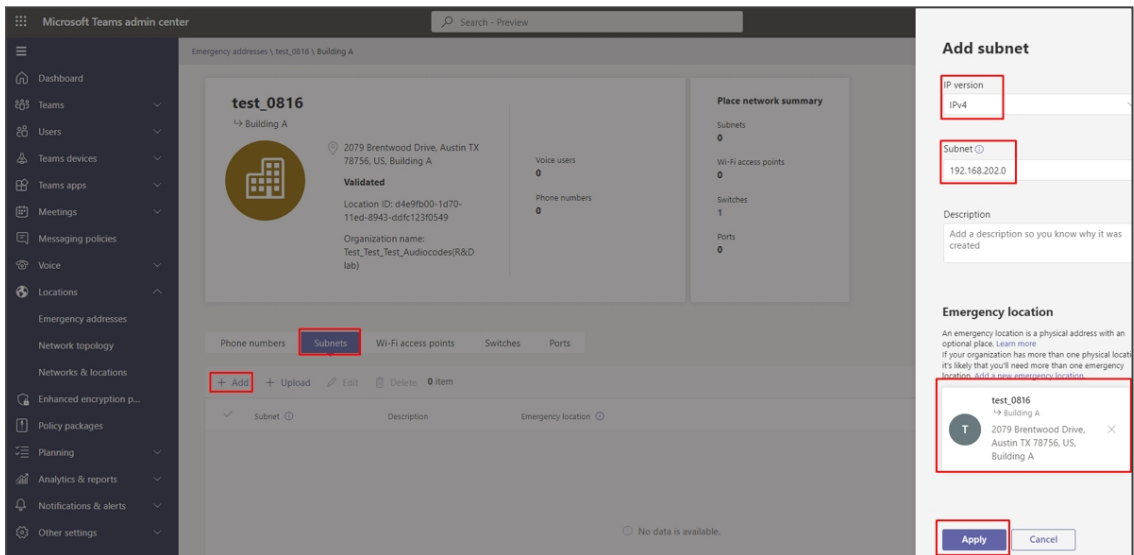
5. Enter a location defined by a specific port ID. Make sure to enter the port description correctly, as delivered from your switch (* the switch must allow LLDP transmit and receive and provide LLDP information).



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.

Networks & locations

Subnets Wi-Fi access points Switches Ports

Each subnet must be associated with a specific network site. A client's location is determined based on the network subnet and the associated network site. You can associate multiple subnets with the same network site but you can't associate multiple sites with the same subnet. [Learn more](#)

Subnets summary

3 Subnets **3** Emergency locations

+ Add + Upload Edit Delete 3 items

Subnet ⓘ	Description	Emergency location ⓘ
192.168.202.0		test_0816
192.168.1.0	Oleg's Wifi	test1105
✓ 172.17.178.0	Lucky	test0407

Subnets Wi-Fi access points **Switches** Ports

A network switch is a device that connects multiple local area network (LAN) devices, like desktops running the Teams app, using Ethernet connections. The devices use this connection to receive and transfer data to each other. Each network switch is stamped with a chassis ID, which identifies the switch on the network. [Learn more](#)

Switches summary

3 Switches **2** Emergency locations

+ Add + Upload Edit Delete 3 items

Chassis ID ⓘ	Description	Emergency location ⓘ
✓ B4-14-89-BE-C0-00		test_0816

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

Subnets Wi-Fi access points Switches **Ports**

A network port is a physical Ethernet connection that connects multiple LAN (local area network) devices like a desktop computer that is running the Teams app. For each port, you need to enter the chassis ID of the network switch that connects the port to a switch in Teams. [Learn more](#)

Ports summary

1 Port **1** Emergency location

+ Add + Upload Edit Delete 1 item

Port	Description	Chassis ID	Emergency location
Gi 1/0/19		B4-14-89-BE-C0-00	test_0816



After a location has been defined, make sure that:

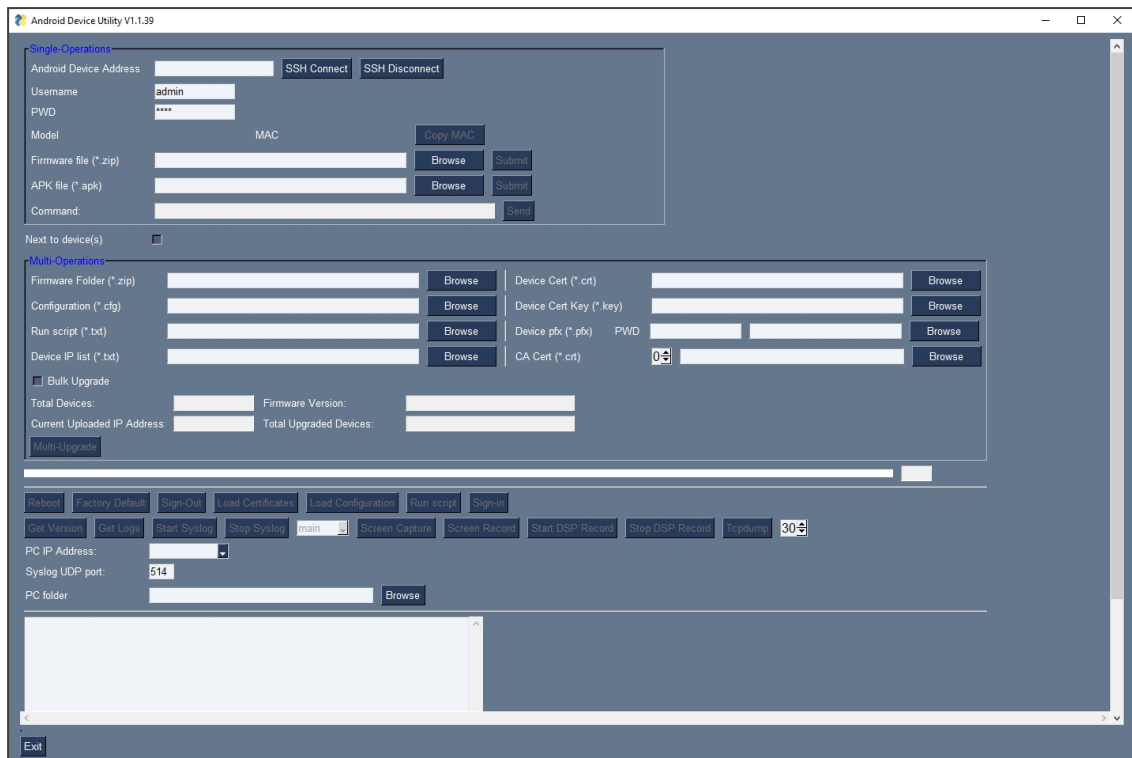
- AudioCodes' phone runs the latest firmware released.
- AudioCodes' phone runs the Teams app issued June 2022 and later (U3-A and higher).
- E911 information is displayed on the phone screen 30-120 minutes after the location is set (time estimated under laboratory conditions).
- To trigger information 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.

Updating Phone Firmware Manually

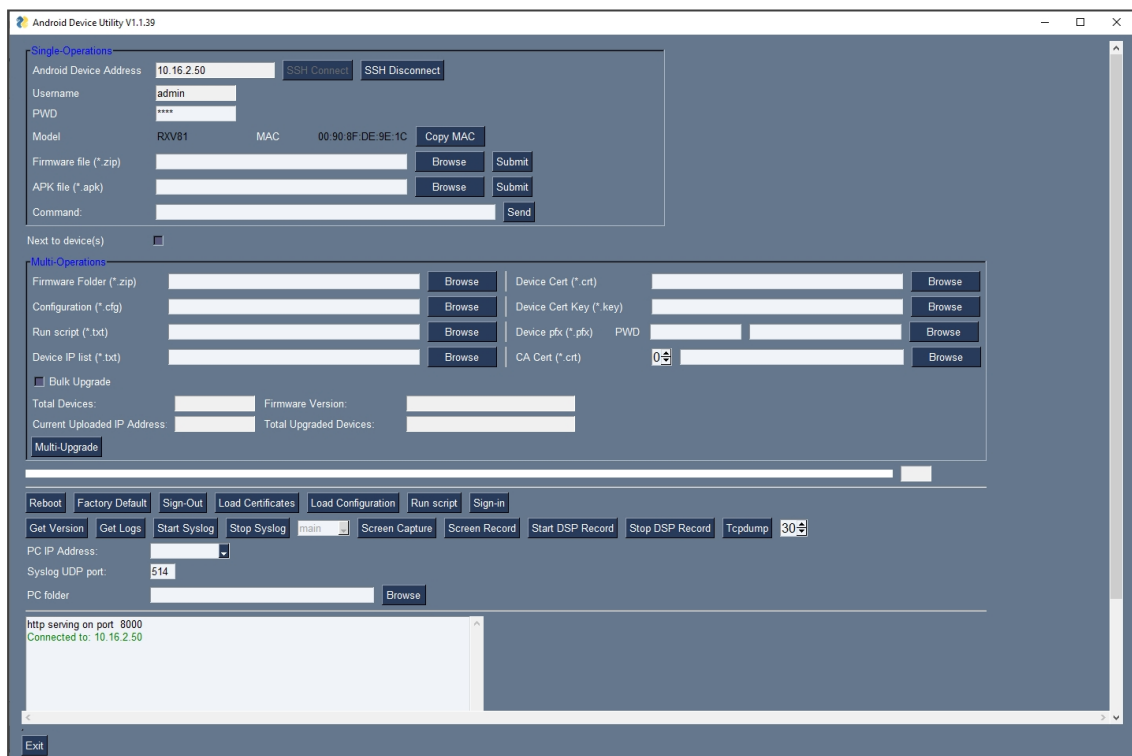
AudioCodes' Android Device Utility allows network administrators to manually update a phone's firmware.

➤ To manually update a phone's firmware:

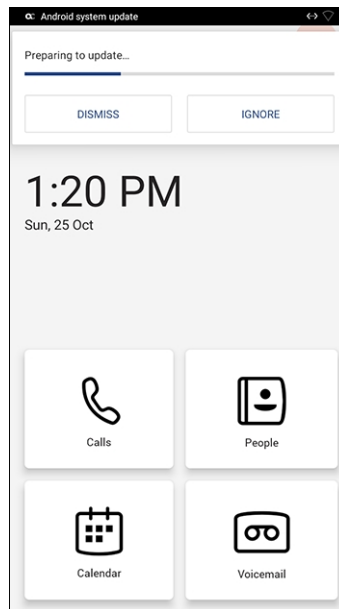
1. From the PC's **Start** menu, select the app icon or click the application's exe file in the folder in which you saved it.



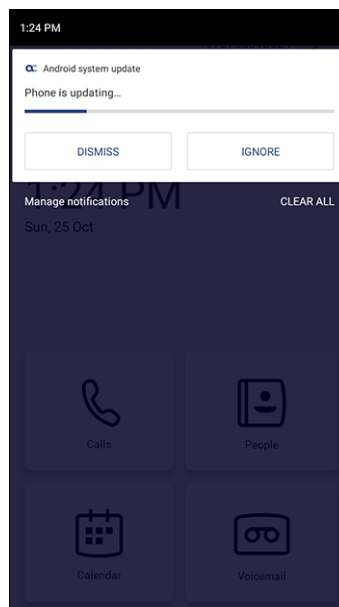
2. In the 'Android Phone Address' field, enter the IP address of the device (get it by touching the user's picture | avatar in the home screen > **Settings** > **Device Settings** > **About phone** > **Status** > **IP Address**).
3. Click **SSH Connect**; a connection with the device is established.



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

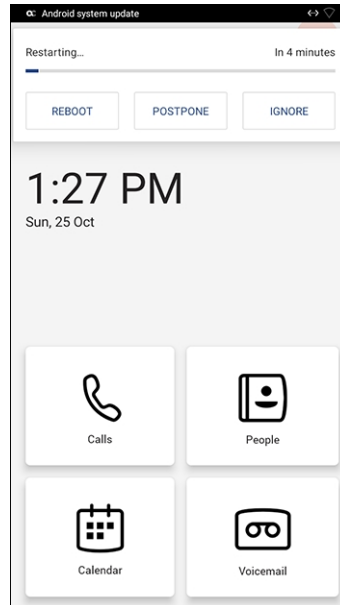


6. Swipe down twice in rapid succession to present the **Manage notifications** option.



7. Touch **Manage notifications**; the screen that is then displayed allows viewing notifications such as:
 - Upgrade state (Preparing, updating, etc.)
 - Internet access issues

8. After the update is completed, the phone reboots.



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:

Device Cert (*.ct)	<input type="text"/>	Browse
Device Cert Key (*.key)	<input type="text"/>	Browse
Device pfx (*.pfx)	PWD <input type="text"/>	Browse
CA Cert (*.ct)	0 <input type="text"/>	Browse



- 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:

PC IP Address:	<input type="text" value="10.13.2.147"/>
Syslog UDP port:	<input type="text" value="514"/>
PC folder	<input type="text" value="D:\Flare\IPP\Content\Resources\Images\C450HC"/> <input type="button" value="Browse"/>

- 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 127 for detailed information about the application), enter the phone's IP address and click **SSH Connect** shown in the next figure.

Android Phone Address		<input type="text" value="10.59.200.176"/>	<input type="button" value="SSH Connect"/>	<input type="button" value="SSH Disconnect"/>
Username		<input type="text" value="admin"/>		
PWD		<input type="text" value="1234"/>		

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 127 for more information), enter the phone's IP address and click **SSH Connect**.



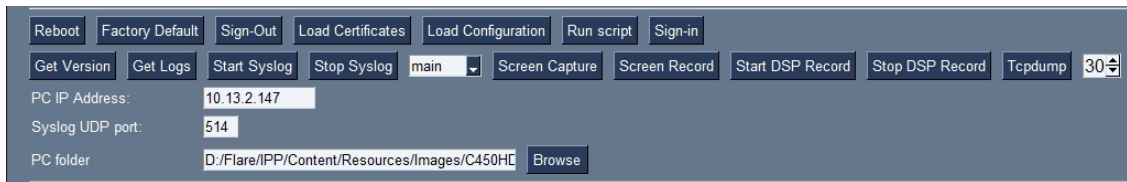
The loaded certificate's file name must be without spaces. Spaces between words can be created using an underscore _

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



- If you use Microsoft NDES server, you need to modify the 'security/SCEPServerURL' (which can be done via OVOC Device Manager):
https://<NDES server IP address/Host-name>/certsrv/mscep/mscep.dll/pkiclient.exe
- For example: http://xxx.xxx.xxx.xxx/certsrv/mscep/mscep.dll/pkiclient.exe

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.

Parameter	Description
	<p>Network admins must set its value to (for example): 7A7F9FC4BB7625F0935E67EA6D6322ED</p>
security/SCEPServerURL	<p>Define the NDES server's URL. Default: NULL.</p> <p>Network admins must set its value to (for example): https://ndes_server</p>
security/SCEPEnroll/renewal/advancethreshold	<p>Define the renewal advance threshold of the device certificate.</p> <p>Configure between 50 and 100 (in units of percentage)</p> <p>Default: 80</p> <p>This indicates that a renewal of the certificate (device.crt) will be initiated when 80 percent of its validity is reached.</p>
security/SCEPEnroll/rollover/advancethreshold	<p>Specify the threshold of the CA Root certificate's validity at which to initiate a renewal.</p> <p>Configure between 50 and 100 (in units of percentage).</p> <p>Default: 90</p> <p>This indicates a renewal of the certificate (CAROOT.crt.) will be initiated when 90 percent of its validity is reached.</p>
security/CSR/CommonName	<p>Define a value according to the following 'wildcard' format:</p> <p>{mac} – the device's MAC address</p> <p>{IP} - the device's IP address</p> <p>{model} - the device model</p>
security/CSR/Country	<p>Define the name of the country used to generate the certificate signing request (CSR). Note: The ISO (International Organization for Standardization) code of the</p>

Parameter	Description
	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.

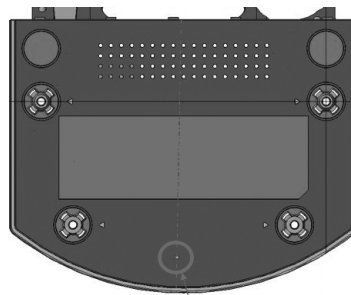
Manually Performing Recovery Operations



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.

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



Tactile switch hole



While a device is powering up, you can perform recovery operations by long-pressing the device's reset key.

When long-pressing the reset key, the device's main LED changes color after every n seconds; each color is aligned with a recovery operation option.

When?	Action	Press for how long?	LED flashes 3x after release
Start pressing immediately after power up (on U-Boot / Universal Boot Loader)	Recovery mode (you can restore defaults from there)	~ 4 seconds	Red
	Switch slots A / B	~ 10 seconds	Green
	Loader	~ 15 seconds	Blue / Yellow
	Restore defaults	~25 seconds	Green + blue / Green + yellow
When successfully booted (on Android)	Reboot	From the 'Admin' menu	-
	Restore defaults	Long-press Hold key for ~15 seconds	Flashes yellow 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:

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

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



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

- Click **Bulk device actions**.

Home > Devices | Android > Android | Android devices >

Bulk device action ...

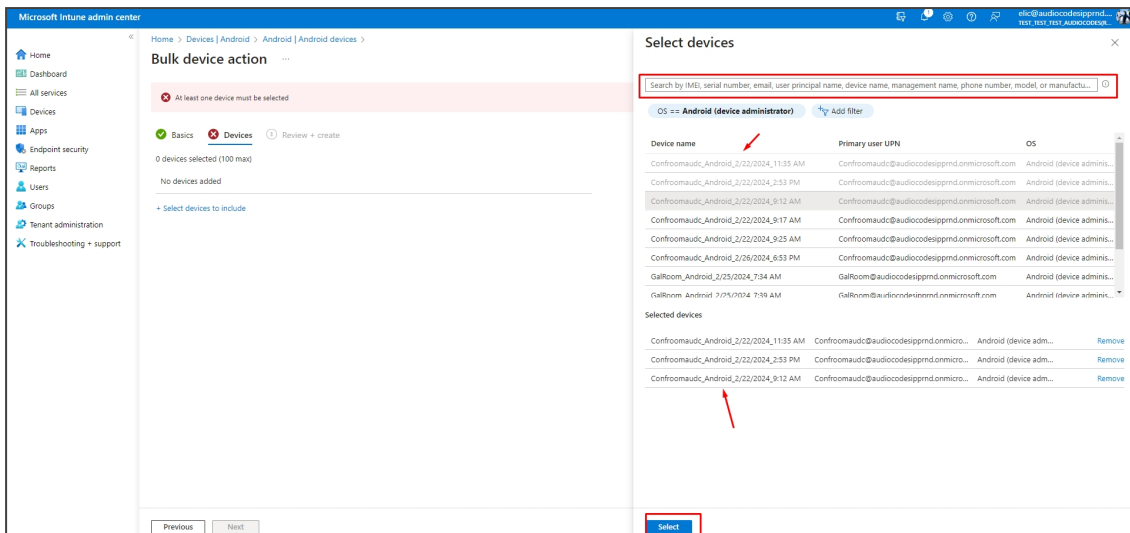
① Basics ② Devices ③ Review + create

OS * →

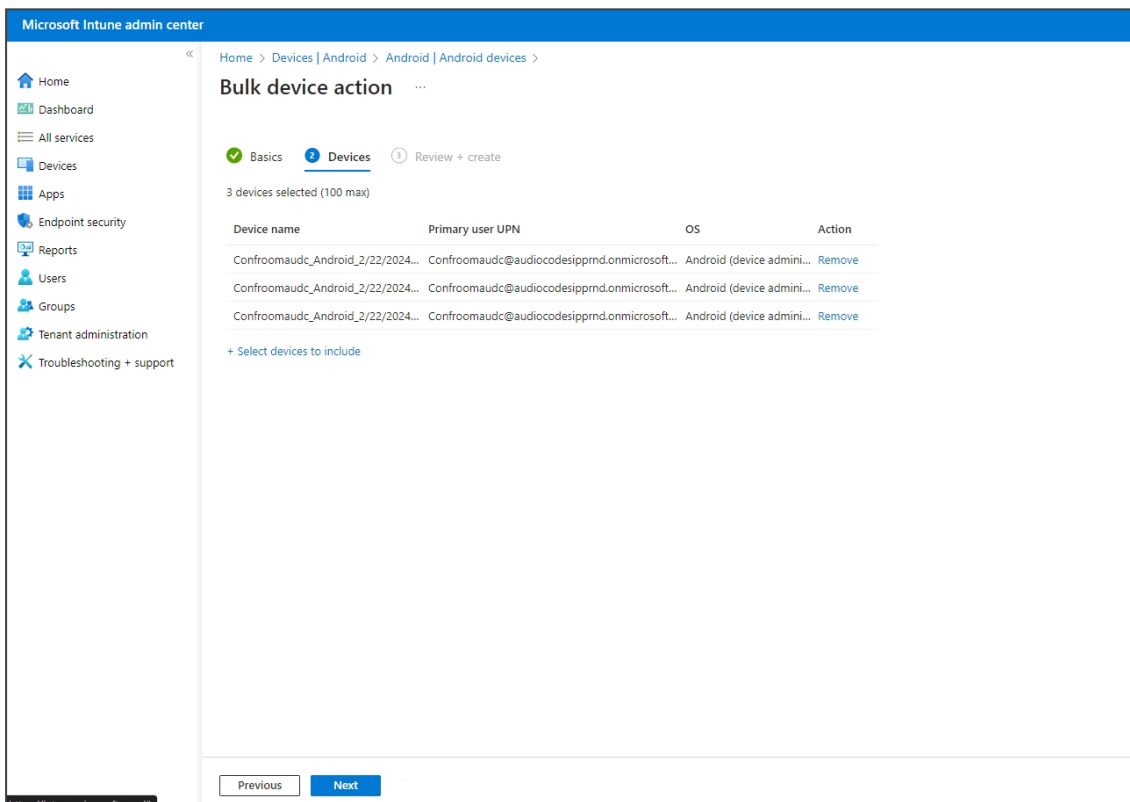
Device action * →

i If you delete this device, you will no longer be able to view or manage the device from the Intune portal. The device will no longer be allowed to access your company's corporate resources. Company data may be wiped from the device if the device tries to check-in after it is deleted.

4. From the 'OS' drop-down under the ① **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**.

Microsoft Intune admin center

Home > Devices | Android > Android | Android devices >

Bulk device action

Basics Devices **3 Review + create**

Summary

Basics

Device action Delete
OS Android (device administrator)

Devices

3 devices selected (100 max)

Device name	Primary user UPN	OS
Confroomauc_Android_2/22/2024_11...	Confroomauc@audiocodesippnd.onmicrosoft.com	Android (device administr...
Confroomauc_Android_2/22/2024_2:5...	Confroomauc@audiocodesippnd.onmicrosoft.com	Android (device administr...
Confroomauc_Android_2/22/2024_9:1...	Confroomauc@audiocodesippnd.onmicrosoft.com	Android (device administr...

Previous Create

- 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

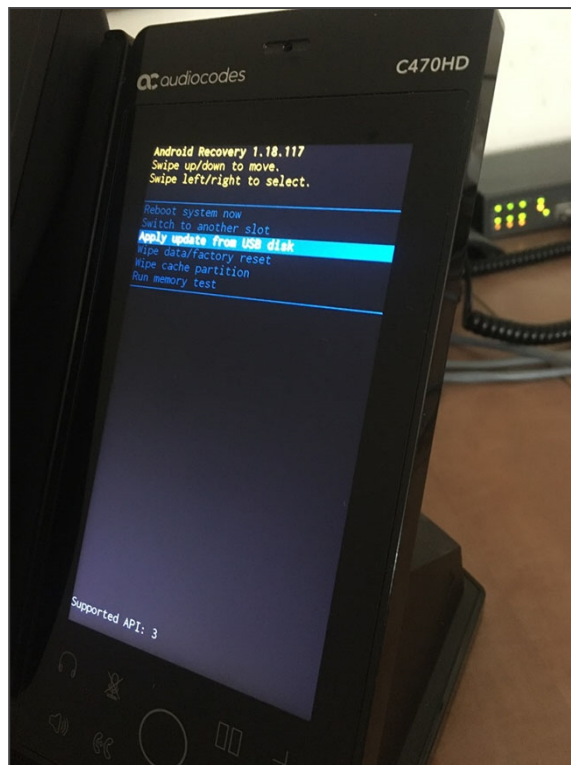
For instructions on how to update Microsoft Teams devices remotely, see [here](#).

Applying Firmware to a Phone from a USB Disk

For recovery purposes, firmware can be applied to a phone from a USB disk.

➤ To apply the firmware from the USB disk:

- Enter recovery mode by pressing for 4 seconds the reset pin located under the base of the device; the device's LED lights up red.
- Insert the USB disk with the target firmware.



3. Select the **Apply update from USB disk** option and then choose the correct firmware image from the disk.

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.

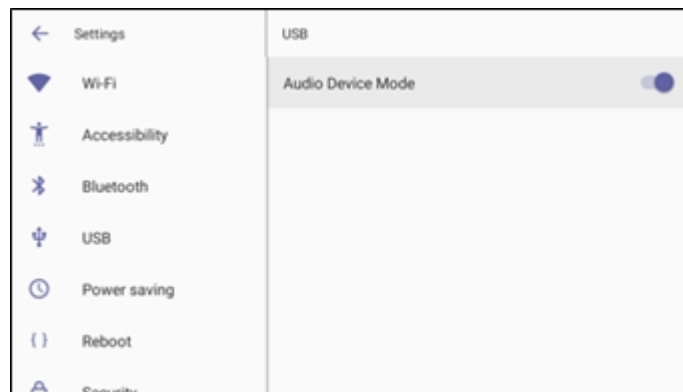
Enabling a Phone to be used as an Audio Device

[Requires an updated 1.19 build] USB host mode is now supported as a feature in preview, i.e., the phone can be connected to a PC via USB, allowing it to be used as the PC's audio device such as an external speaker.


Click [here](#) to view a video clip demonstrating how to use the phone in Audio Device Mode. The principle is the same across all AudioCodes Teams phone models.

➤ To set up the feature:

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



2. Connect a USB cable from the phone to the PC.

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

Android System

USB port shutdown due to over current exceeded

Please disconnect the USB device.
 If USB audio device is connected, please make sure that the USB device is headset only.
 If you use the phone as a USB audio device, please set the setting in USB audio device mode under device Settings->USB->Audio Device Mode.
 When quitting USB Audio Device mode, first unplug the USB cable, then unset USB audio device mode setting.

HIDE COLLAPSE CLOSE

Or go to <https://microsoft.com/devicelogin> and enter the code below

Refresh code

[Sign in with a different account](#)

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

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 **dhcption160.cfg** as shown here:

Table 6-1: DHCP Option 160 URL

DHCP Options Configuration	
DHCP option 160 URL ('dhcption160.cfg')	
SYSTEM URLS	
OVOC accesses phones directly:	https://ppdm.audiocodes.com/firmwarefiles;pp/dhcption160.cfg
OVOC accesses phones via SBC HTTP Proxy:	https://SBC_PROXY_IP:SBC_PROXY_PORT/firmwarefiles;pp/httpproxy/
<div style="display: flex; justify-content: space-between; align-items: center;"> Edit Dhcption160.Cfg Template Download Dhcption160.Cfg Template Upload Dhcption160.Cfg Template </div>	
<div style="display: flex; justify-content: center; align-items: center; margin-top: 5px;"> Generate 'Dhcption160.Cfg' </div>	
<div style="border: 1px solid gray; padding: 2px; margin-top: 5px; font-size: small;">Advanced: DHCP Option 160 With Tenant Configuration</div>	

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

Parameter	Description
	<p>values are:</p> <ul style="list-style-type: none"> ■ HOURLY ■ DAILY (default) ■ WEEKLY ■ POWERUP ■ EVERY5MIN ■ EVERY15MIN <p>Each value type is accompanied by additional parameters (see Supported Parameters on the next page) that further defines the selected frequency.</p>

Configuring TimeZone and Daylight Savings

Network administrators can configure TimeZone and Daylight Savings to suit enterprise requirements.



AudioCodes' Teams phones feature a **Automatic Time Zone Detection** mechanism that allows the device to automatically detect the time zone via geographical location. If time zone is not configured, this feature is implemented.

➤ To configure TimeZone and Daylight Savings:

- Use the following table as reference.

Table 6-3: TimeZone And Daylight Savings

Parameter	Description
date_time/- timezone	<p>Defines the Timezone. Valid values are:</p> <ul style="list-style-type: none"> ■ +00:00 ■ +01:00 ■ +02:00 ■ Etc.
date_time/time_ dst	<p>[Boolean parameter]. Configuring ENABLED adds one hour to the configured time. Valid values are:</p> <ul style="list-style-type: none"> ■ 1 ■ 0

For example, to configure Central European Summer Time (CEST) you can either configure:

```
date_time/timezone=+01:00
```

```
date_time/time_dst=1
```

-OR-

```
date_time/timezone=+02:00
```

```
date_time/time_dst=0
```

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 = +02:00`
- `date_time/time_dst = 0 (default) /1`

- `date_time/time_format = 12 (default) / 24`
- `network/dhcp_enabled = 0/1`
- `network/ip_address =`
- `network/subnet_mask =`
- `network/default_gateway =`
- `network/primary_dns =`
- `network/pecondary_dns =`
- `network/pc_port = 0/1`
- `office_hours/start = 08:00`
- `office_hours/end = 17:00`
- `logging/enabled = 0/1`
- `logging/levels = VERBOSE, DEBUG, INFO, WARN, ERROR, ASSERT, 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`

7 Troubleshooting

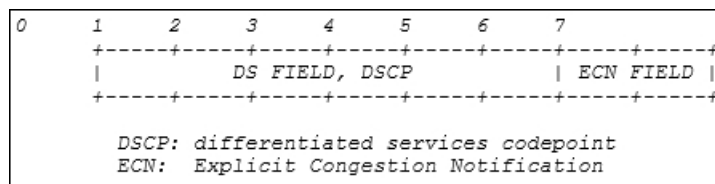
The information presented here shows how to troubleshoot AudioCodes devices.

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

```

2057 47.390455 192.168.2.104 172.17.178.203 UDP 84 50006 → 50012 Len=42
2058 47.390541 192.168.2.104 172.17.178.203 UDP 228 50006 → 50012 Len=186
2059 47.393899 192.168.2.104 172.17.178.203 UDP 151 50006 → 50012 Len=109
2060 47.395193 172.17.178.203 192.168.2.104 UDP 114 50012 → 50006 Len=72
2061 47.395209 172.17.178.203 192.168.2.104 UDP 114 50012 → 50006 Len=72
<
> Frame 2057: 84 bytes on wire (672 bits), 84 bytes captured (672 bits) on interface \Device\NPF_{296D2E63-3934-488A-8FAB-666A48797EE2}, id 0
> Ethernet II, Src: AudioCod_9c:1a:38 (00:90:8f:9c:1a:38), Dst: VMware_ff:63:15 (00:0c:29:ff:63:15)
> Internet Protocol Version 4, Src: 192.168.2.104, Dst: 172.17.178.203
  0100 .... = Version: 4
  .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0xb8 (DSCP: EF PHB, ECN: Not-ECT)
    1011 10.. = Differentiated Services Codepoint: Expedited Forwarding (46)
      .... ..00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)
  Total Length: 70
  Identification: 0xd3ba (54202)
  > Flags: 0x4000, Don't fragment
  Fragment offset: 0
  Time to live: 64
  Protocol: UDP (17)
  Header checksum: 0x4447 [validation disabled]
  [Header checksum status: Unverified]
  Source: 192.168.2.104
  Destination: 172.17.178.203
> User Datagram Protocol, Src Port: 50006, Dst Port: 50012
    
```

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	<ul style="list-style-type: none"> ■ 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	<ul style="list-style-type: none"> ■ Increase the volume (see Adjusting Ring Volume on page 89)
Screen display is poor	Screen settings	<ul style="list-style-type: none"> ■ Adjust the phone’s screen brightness
Headset has no audio	Headset not connected properly	<ul style="list-style-type: none"> ■ 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 90).

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:

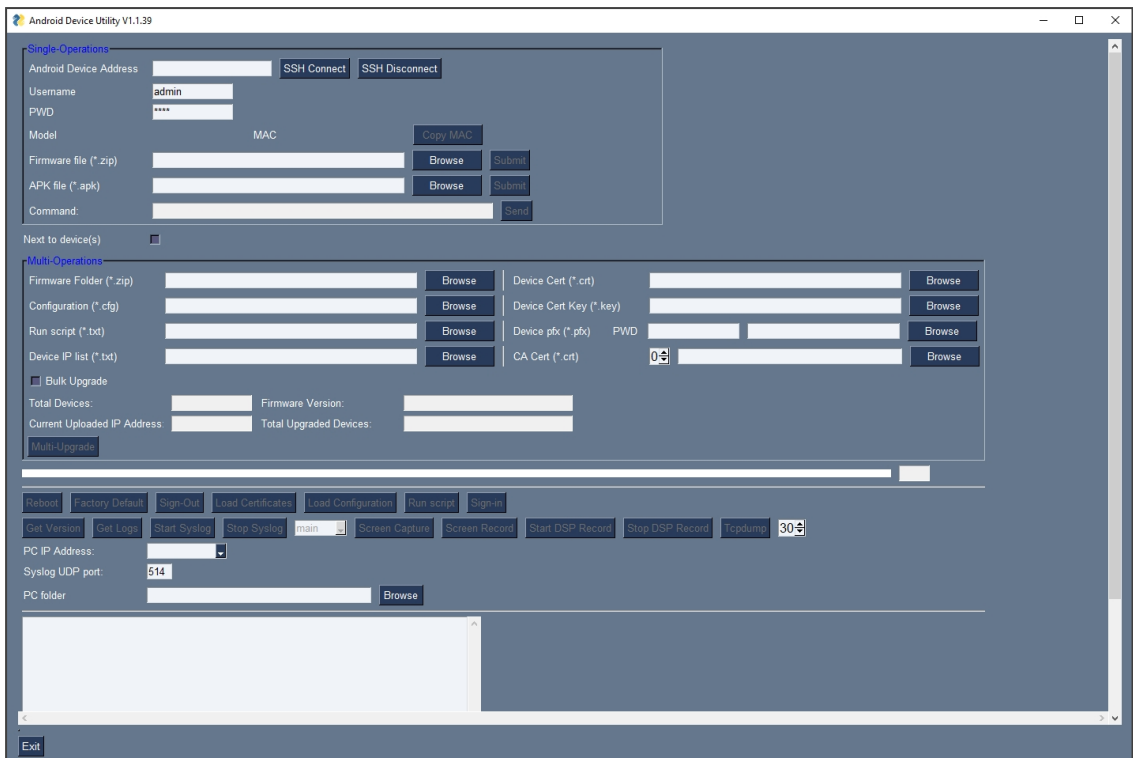
- Enter your username and password; **admin** and **1234** are the defaults.

The application gives network administrators the following debugging capabilities:

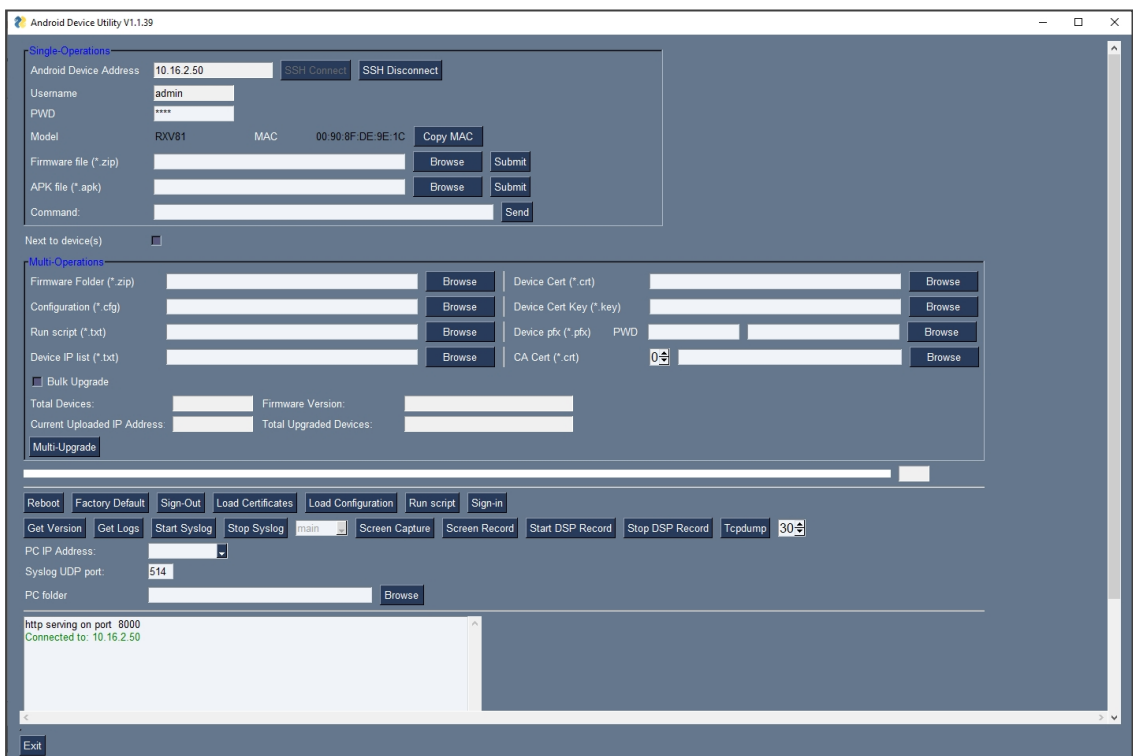
- [Capturing the Phone Screen](#) on page 129
- [Running Tcpdump](#) on page 130
- [Getting Information about Phones](#) on page 131
- [Remote Logging \(Syslog\)](#) on page 132
- [Getting Diagnostics](#) on page 135
- [Getting Logs](#) on page 136
- [Activating DSP Recording](#) on page 137
- [Deactivating DSP Recording](#) on page 138
- [Getting Information about Phones](#) on page 131

➤ 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 touching the user's picture | avatar in the home screen > **Settings** > **Device Settings** > **About phone** > **Status** > **IP Address**).
3. Click **SSH Connect**; a connection with the device is established.



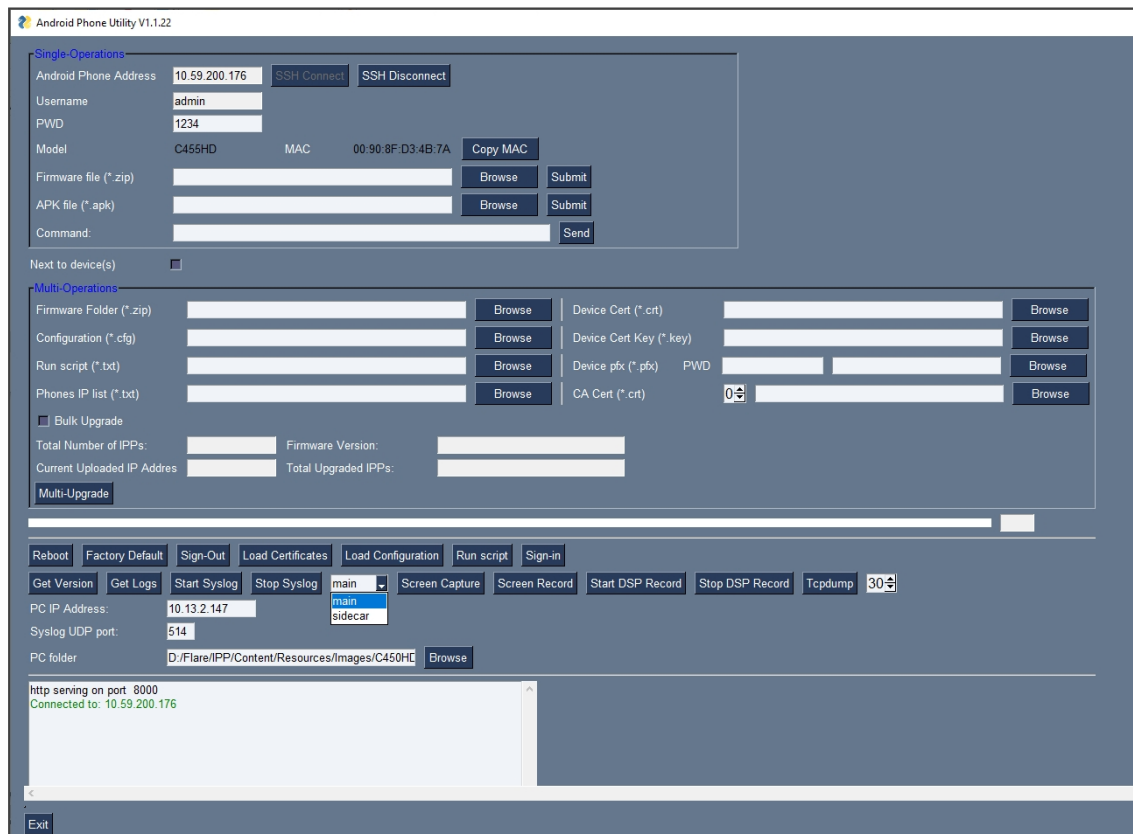
- Next to the field 'PC folder', click the **Browse** button and navigate to and select the folder to which to send data to use for debugging.

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:

- 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.
- In the 'Android Phone Address' field, enter the IP address of the device (get it by touching the user's picture | avatar in the home screen > **Settings** > **Device Settings** > **About phone** > **Status** > **IP Address**).
- Click **SSH Connect**; a connection with the device is established.
- Next to the field 'PC folder', click the **Browse** button and navigate to and select the folder to which to send the screen captures.
- Make sure that the drop-down menu next to the **Screen Capture** button shows **main**.
- Click the **Screen Capture** button; the phone's screen is captured and the screenshot is saved and sent to the folder.



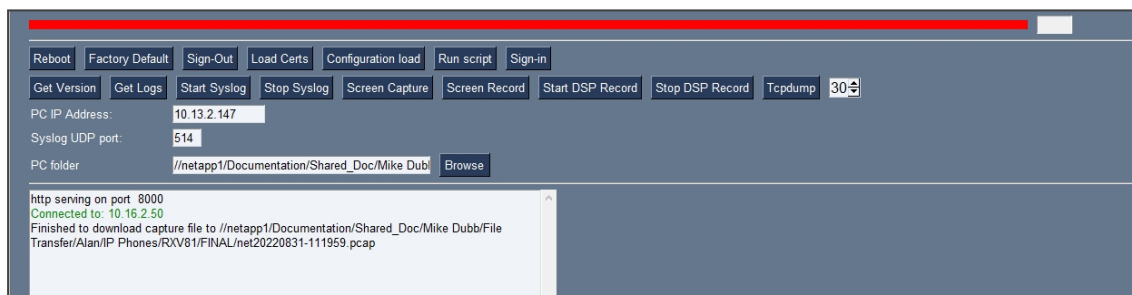
7. On your PC, navigate to the folder and retrieve the screenshot. Default file name: **screencap.png**. Rename it to a name related to the screen you captured. If you don't rename it, it will be overwritten the next time you take a screenshot.

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 127 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 Tcpcmdump, reproduce the issue.
5. Execute the following command from your PC command prompt (cmd):

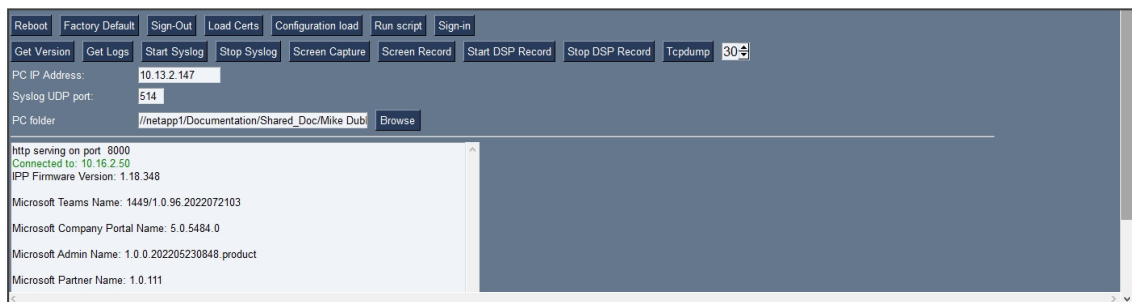
```
scp -r admin@%deviceIp%:/sdcard/recording/ %FolderOnPc%
```

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 127 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)

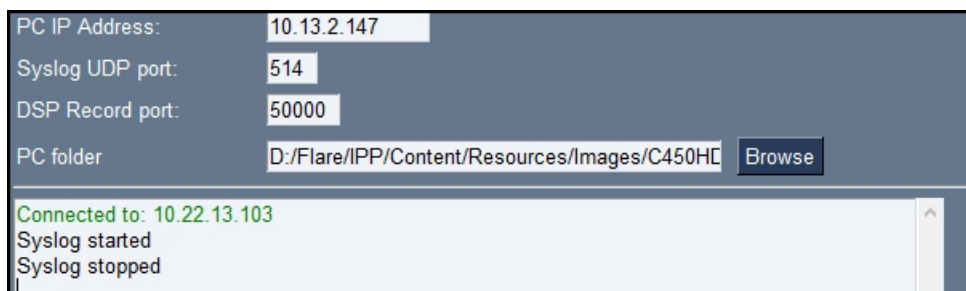
Remote Logging via Syslog provides the same log level as Device Diagnostics (performed via the Microsoft Teams Admin Center) with some additional information that may be relevant to device issues (not Teams application issues). Device Diagnostics via the Microsoft Admin Center are saved to the device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

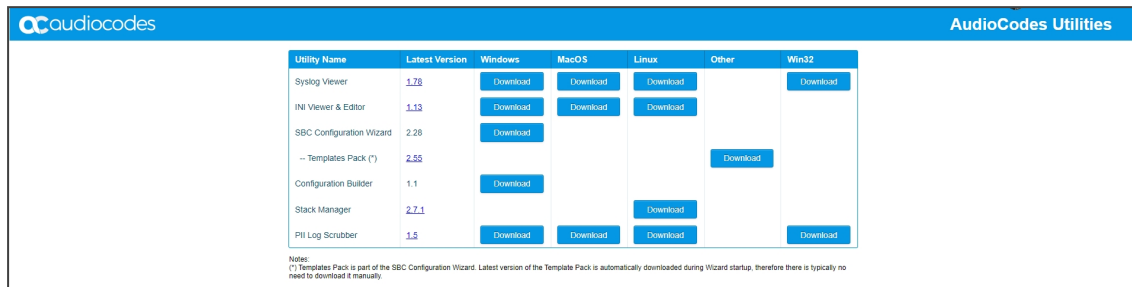
- [Android Device Utility](#) on page 127
- on the next page

➤ To enable Remote Logging via Syslog from the utility:

1. In the Android Device Utility (see [Android Device Utility](#) on page 127 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.

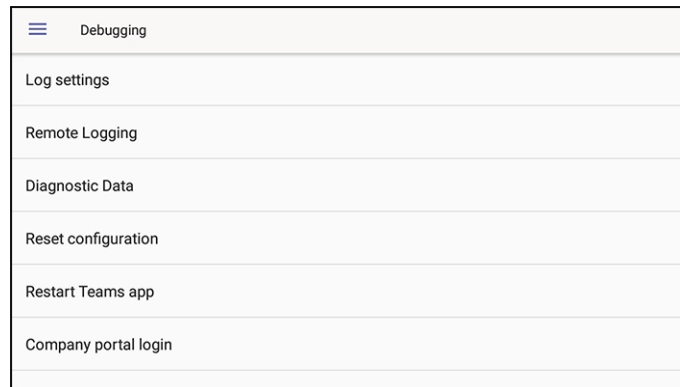


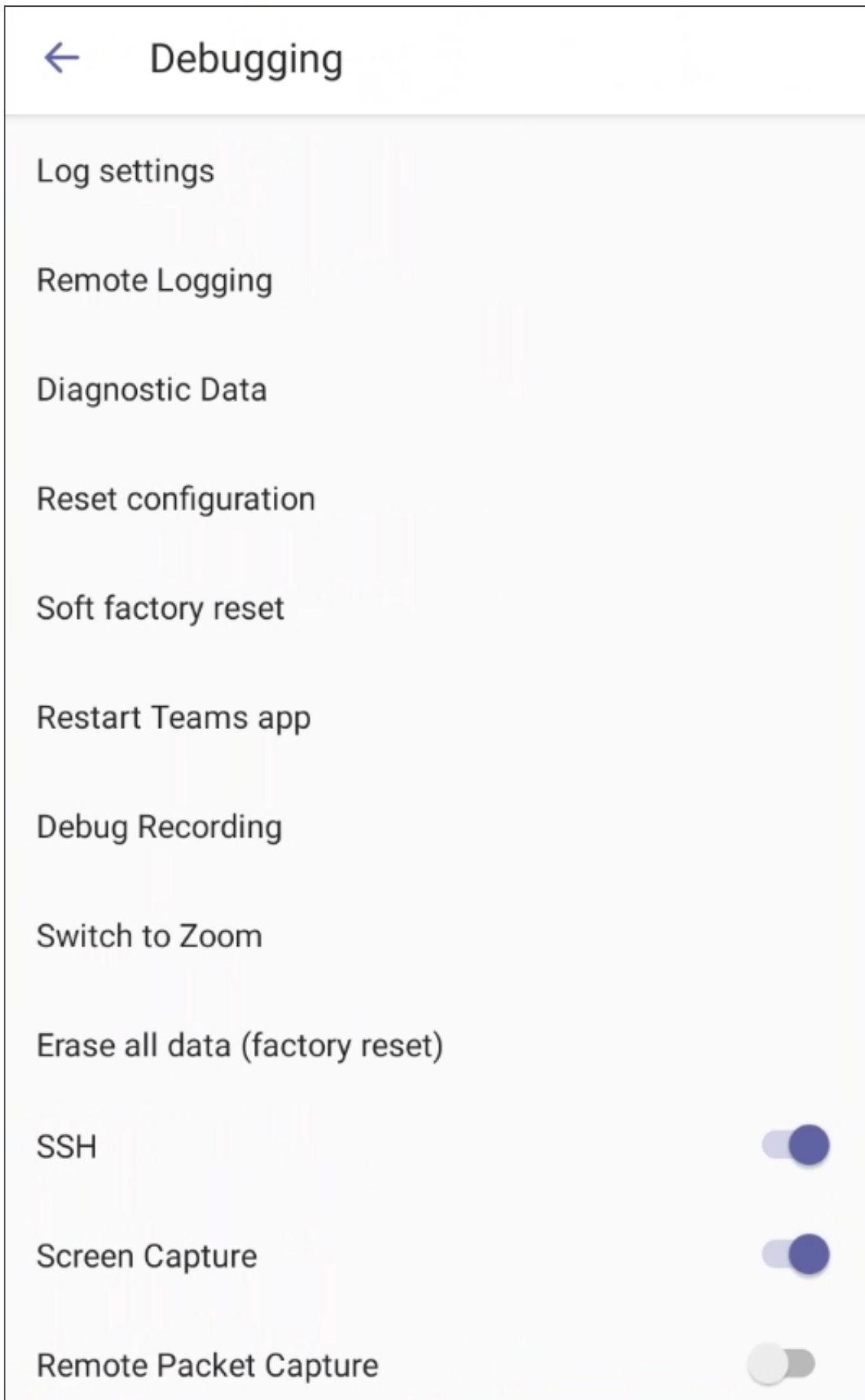
3. Open the folder on the PC to which you commanded the application to send the information, and then locate the Syslog file.
4. To view Syslog, you can optionally download the Syslog Viewer available in AudioCodes' website.



➤ **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

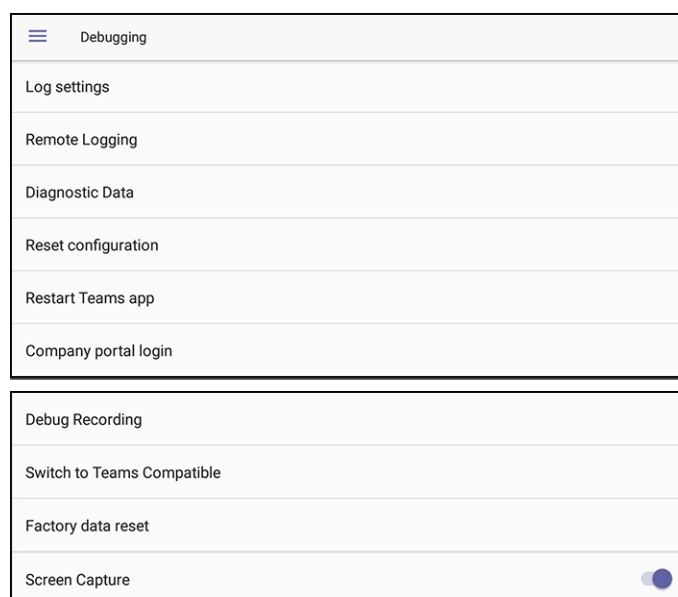
Network administrators can get diagnostics information to facilitate debugging.



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:

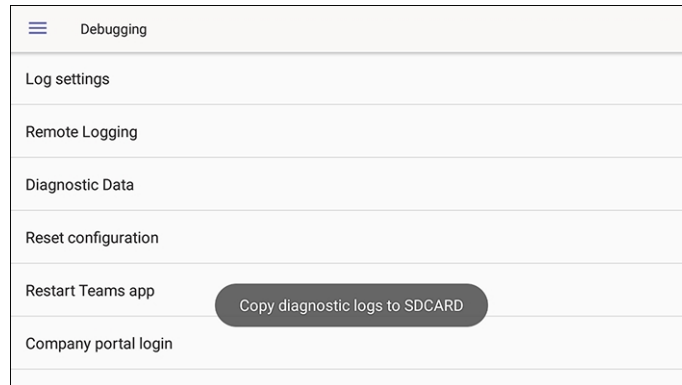
1. Log in to the phone as an Admin user
2. Open the Debugging screen (**Device Administration > Debugging**).



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:

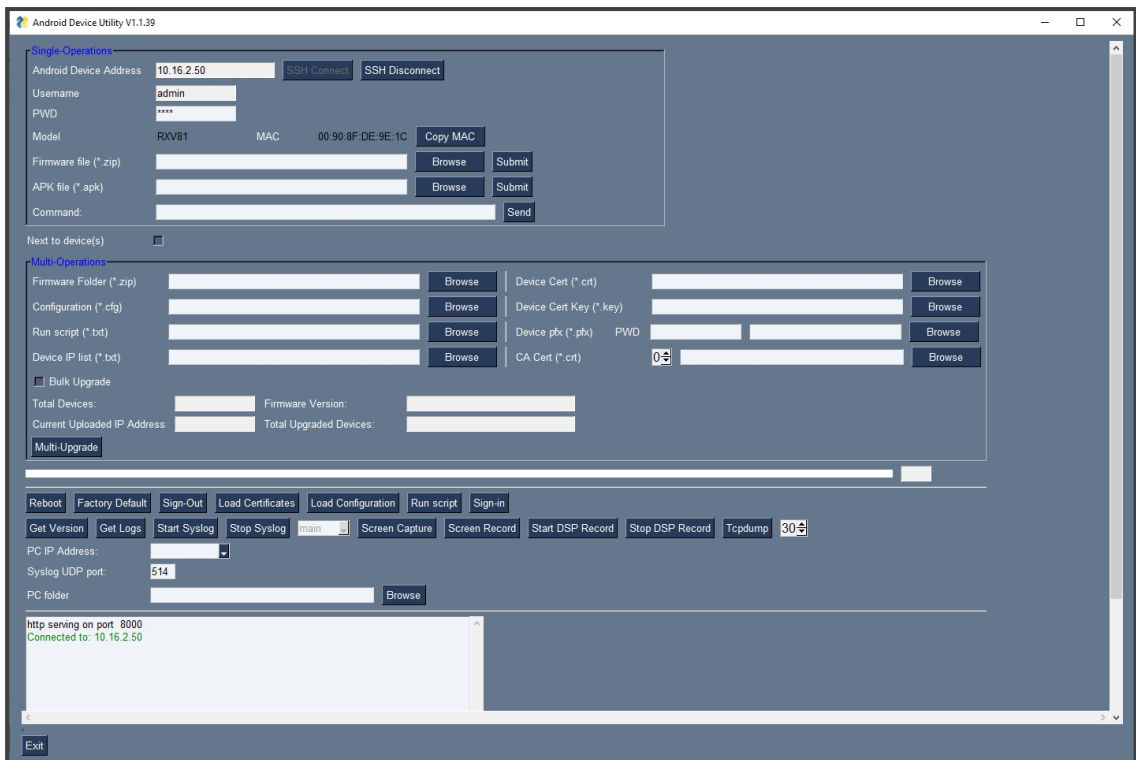
- dmesg.log
- dumpstate-c470hd-1.18.117_58793-41-undated-dumpstate_log-3458.txt
- dumpstate-c470hd-1.18.117_58793-41-undated.txt
- dumpstate-stats.txt
- logcat.log

Getting Logs

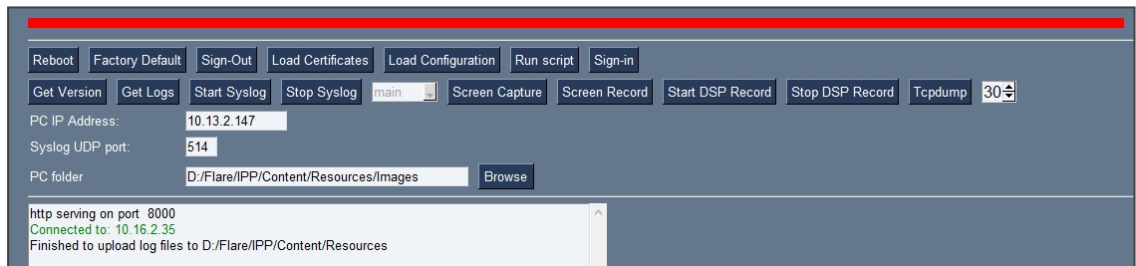
Network administrators can get bug report logs, including a logcat file and a configuration file, to expedite debugging.

➤ To get logs:

1. In the AudioCodes Android Device Utility (see [Android Device Utility](#) on page 127 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.

Name	Date modified	Type	Size
bugreport-TEAMS_1.10.142-2021-06-23-17-50-43.zip	6/23/2021 5:51 PM	WinRAR ZIP archive	941 KB
bugreport-TEAMS_1.10.142-2021-06-28-10-38-50.zip	6/28/2021 10:39 AM	WinRAR ZIP archive	1,024 KB
dumpstate_log-2021-06-23-17-50-43-13194.txt	6/23/2021 5:51 PM	Text Document	26 KB
dumpstate_log-2021-06-28-10-38-50-1788.txt	6/28/2021 10:39 AM	Text Document	26 KB

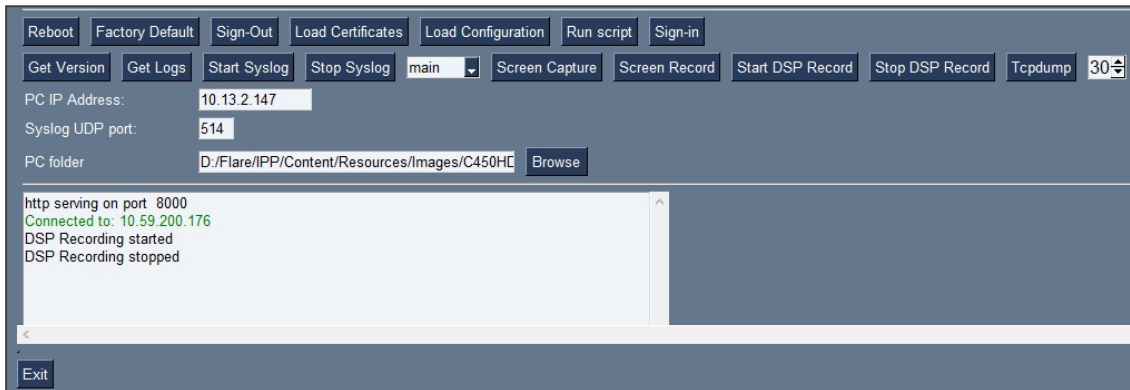
4. Unzip the zipped files and open the txt files to view the report.

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 127 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:**

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



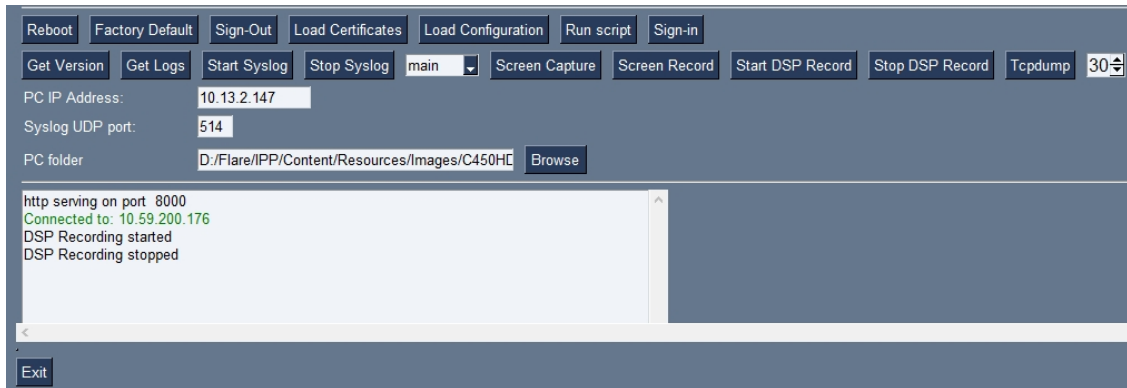
DSP recording can be activated on the fly without requiring the network administrator to reset the phone.

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 127 for more information about the application), click **Stop DSP Record** after a period of recording (see [Activating DSP Recording](#) on page 137 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 137.



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 137
- [Deactivating DSP Recording](#) on page 138
- [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:

```
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 sdcards_certs_install.
```

Microsoft Teams Admin Center

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

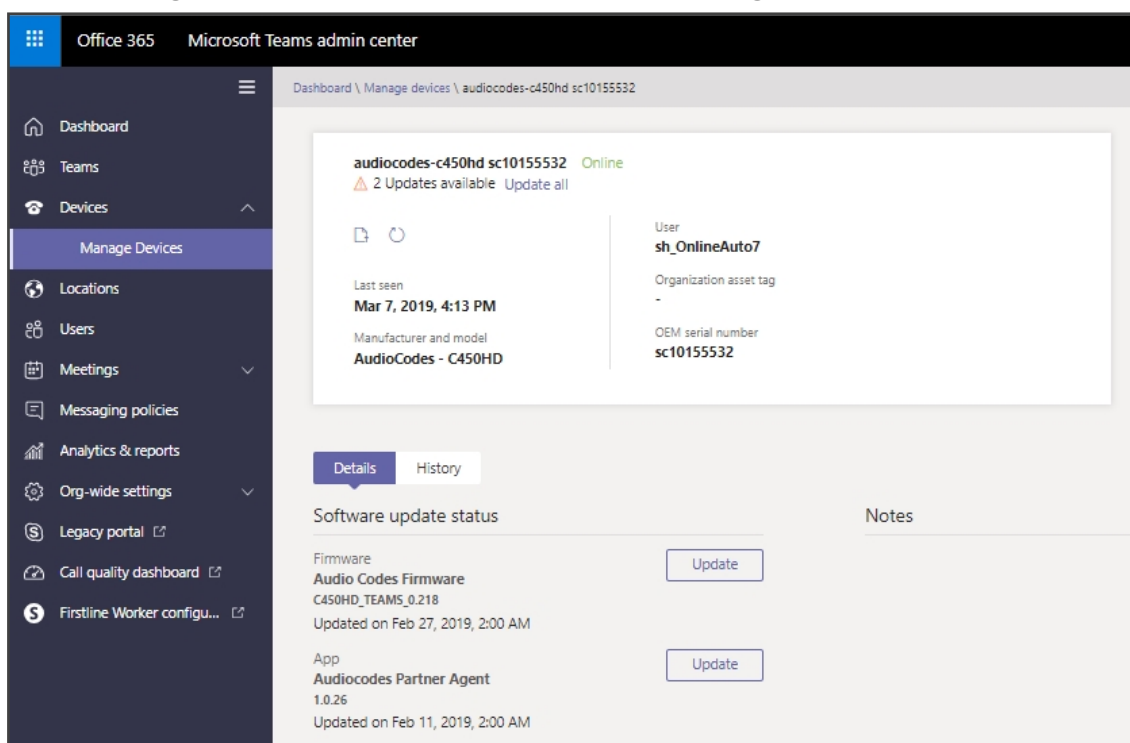
Collecting Logs

Network administrators can download *all logs* from the Microsoft Teams admin center. Logs that administrators can download include device diagnostics (Logcat), dumphsys, 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.


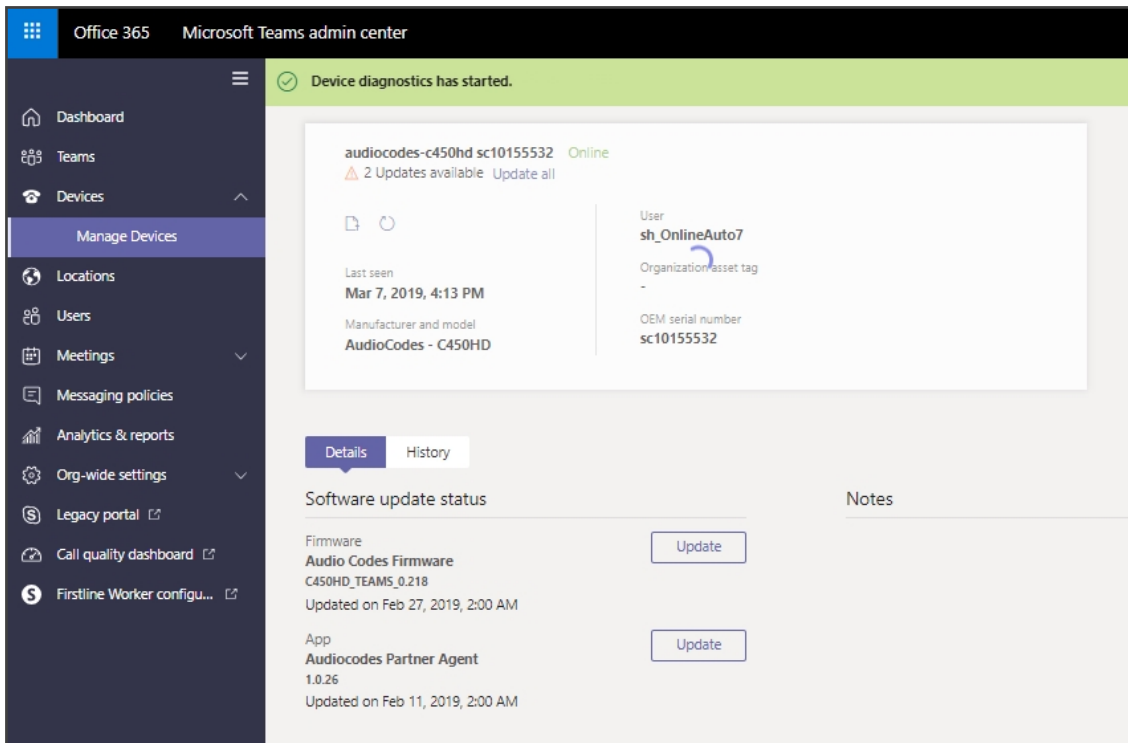
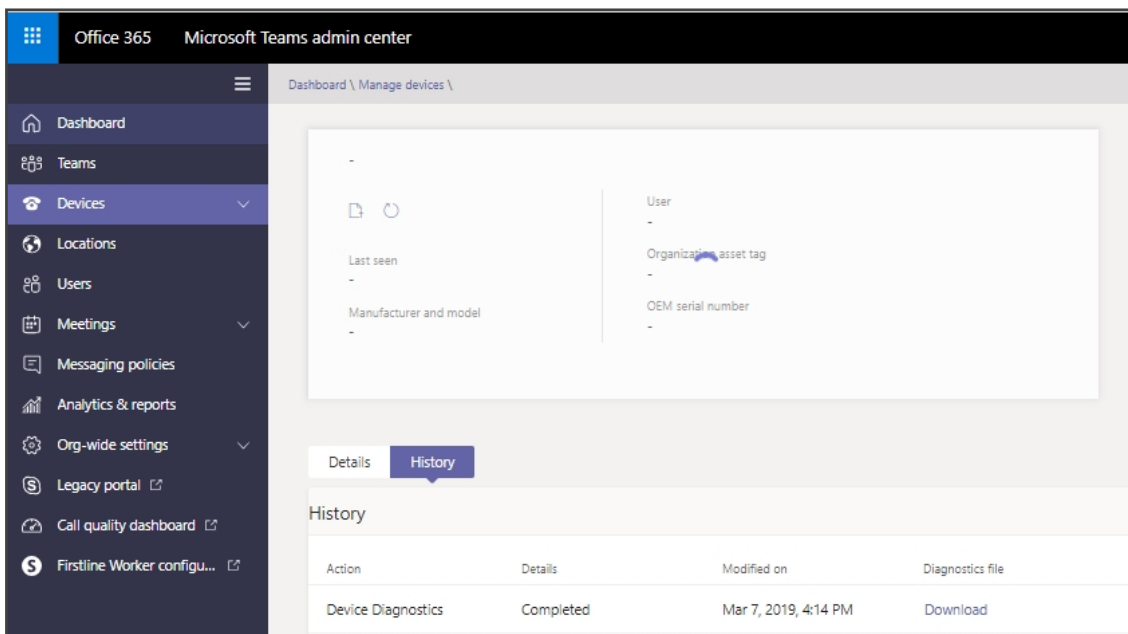
3. Click the **Diagnostics** icon  and in the 'Device diagnostics' prompt that pops up, click **Proceed**; log files are retrieved from the devices and uploaded to the server.

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.



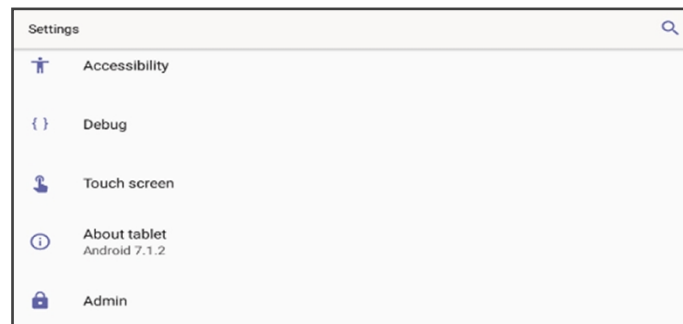
- AudioCodes Device Manager's 'Collect Logs' action also includes all information collected by Microsoft Teams admin center (TAC). The .zip file includes the following files:
 - ✓ Android BugReport
 - ✓ AdminAgentLogs.zip - includes logcat collected by the OVOC/Device Manager.
 - ✓ blog files (media 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/ .
```

Capturing Traffic Using 'rpcapd'

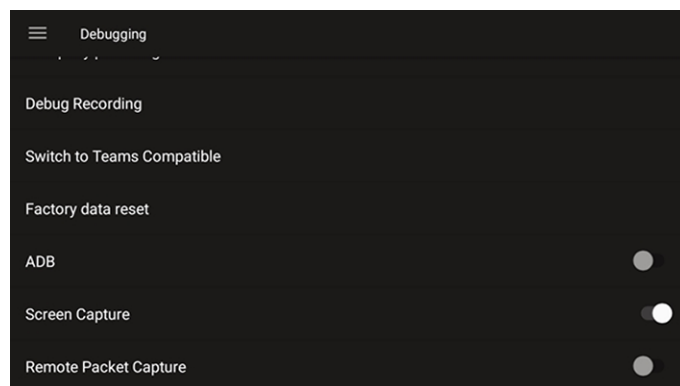
The 'rpcapd' (Remote Packet Capture) network sniffer application enables network admins to analyze and debug Android traffic on their desktop PC using the app's integral SSH server.

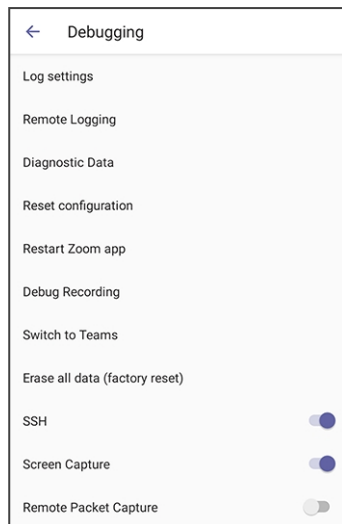


SSH is by default disabled and can be enabled with Administrator permissions in the phone screen (Device Administration > Debugging > SSH).

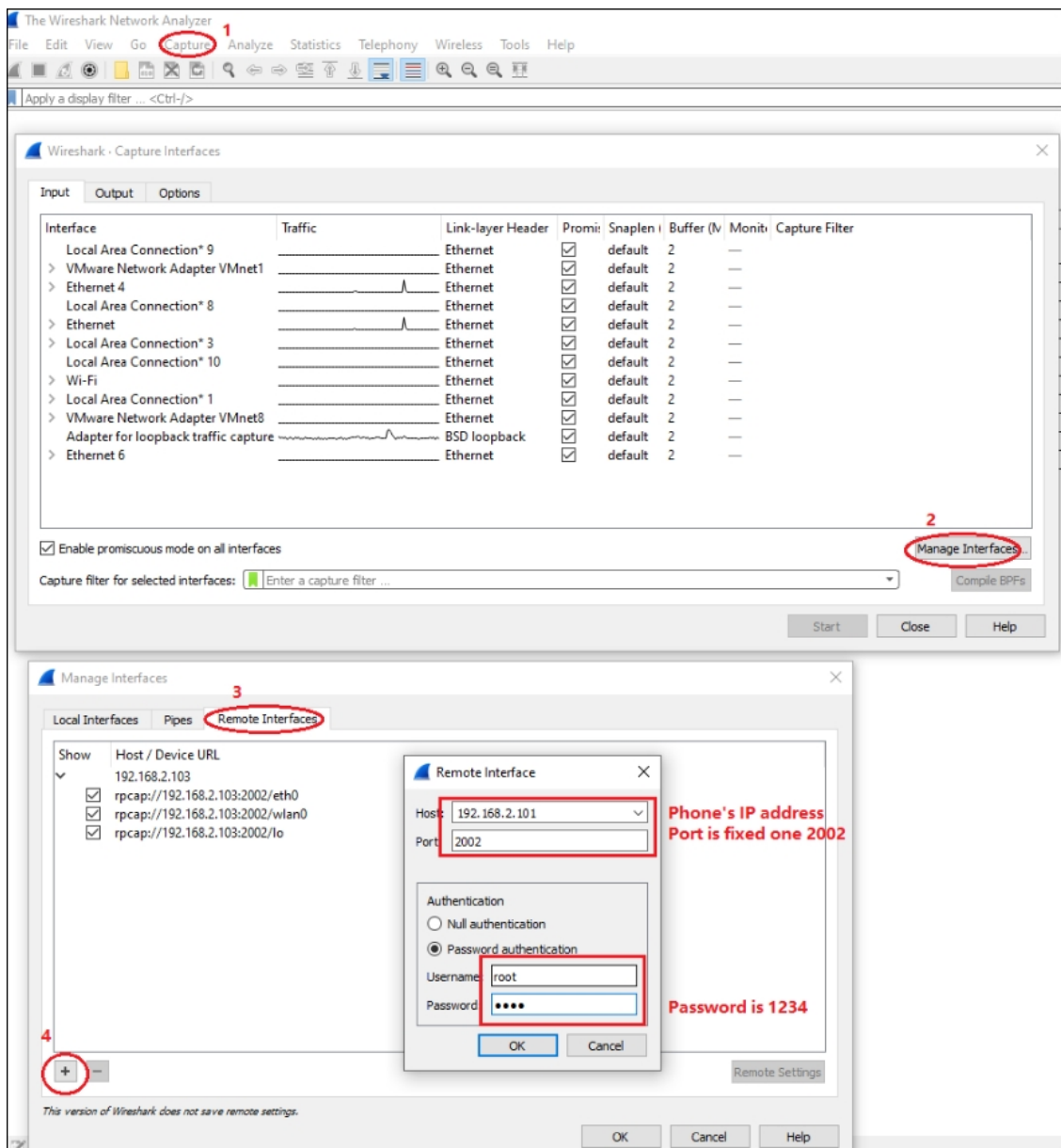
➤ To capture traffic using 'rpcapd':

1. Open the phone's Debugging screen and switch **Remote Packet Capture** on.





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



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

This page is intentionally left blank.

International Headquarters

1 Hayarden Street,

Airport City

Lod 7019900, Israel

Tel: +972-3-976-4000

Fax: +972-3-976-4040

AudioCodes Inc.

80 Kingsbridge Rd

Piscataway, NJ 08854, USA

Tel: +1-732-469-0880

Fax: +1-732-469-2298

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

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

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

©2024 AudioCodes Ltd.. All rights reserved. AudioCodes, AC, HD VoIP, HD VoIP Sounds Better, IPmedia, Mediant, MediaPack, What's Inside Matters, OSN, SmartTAP, User Management Pack, VMAS, VoIPerfect, VoIPerfectHD, Your Gateway To VoIP, 3GX, VocaNom, AudioCodes One Voice, 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-13432

