

C470HD IP Phone

Microsoft Teams Application

Version 1.10



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: April-07-2021

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
C470HD IP Phone for Microsoft Teams Quick Guide
C470HD IP Phone for Microsoft Teams Release Notes
https://docs.microsoft.com/en-us/MicrosoftTeams/phones-for-teams

Table of Contents

1	Overview	1
	Specifications	1
	Security Guidelines for Android-based Native Teams Devices	3
	Android-Level Security Hardening	4
	Google Play Services	5
	Running Android in Kiosk Mode	5
	AudioCodes Private Key	5
	Android Debug Bridge (ADB)	5
	App Signing	5
	Web Browser	5
	Remote Configuration Management	5
	AudioCodes Device Manager Validation	6
	Device File System	6
	Debugging Interface	6
	Android Security Updates	6
	AudioCodes Root CA Certificate	6
2	Setting up the Phone	9
	Unpacking	9
	Device Description	10
	Front View	10
	Rear View	12
	Cabling	13
	Before Using AudioCodes Devices	13
3	Starting up	14
	Configuring Device Settings	14
	Configuring Wi-Fi	27
	Restoring the Phone to Default Settings	29
	Performing a Hard Restore	29
	Performing a Soft Restore	30
	Recovery Mode	30
	Locking and Unlocking the Phone	31
	Automatic Lock	31
	Unlock	32
4	Teams Application	34
	Signing In	34
	Multi-Cloud Sign-in	41
	Remote Provisioning and Sign-in from Teams Admin Center	42
	Getting Acquainted with the Phone Screen	45
	Enabling Google Talkback	47
	Opting in or out of Call Queues	50
	Setting a Status Message	50

Hot Desking	52
Changing Presence Status	52
Configuring Teams Application Settings	54
Setting up a Meeting	57
Using the People Screen	58
Accessing Voicemail	60
Using Audio Devices	61
Signing Out	61
5 Performing Basic Operations	63
Making a Call	63
Dialing a Missed Call	64
Touch to Dial	64
Making an Emergency Call	64
Answering Calls	66
Ending an Established Call	67
Managing Calls	67
Parking a Call	68
Managing Teams Meetings	68
Using Live Captions	71
Raising a Hand During a Meeting	71
Reacting During a Meeting	71
Transferring a Call to Frequent Contacts	72
Transferring a Call to Work Voicemail	72
Viewing and Playing Voicemail Messages	72
Rejecting an Incoming Call, Sending it Directly to Voicemail	74
Adjusting Volume	74
Adjusting Ring Volume	74
Adjusting Tones Volume	74
Adjusting Handset Volume	75
Adjusting Speaker Volume	75
Adjusting Headset Volume	75
Viewing and Joining Meetings	76
Better Together over Bluetooth	77
6 Updating Phone Firmware Manually	81
7 Managing Phones with the Device Manager	84
Configuring a Periodic Provisioning Cycle	85
Configuring TimeZone and Daylight Savings	85
Managing Devices with HTTPS	86
Supported Parameters	86
8 Updating Microsoft Teams Devices Remotely	89
8 Removing Devices from Intune Management	90

9 Troubleshooting	97
Users	97
Network Administrators	97
Collecting Logs	97
Remote Logging	99
Diagnostic Data	100
SSH	102
Capturing the Phone Screen	102
Running the tcpdump Tool	103
Activating DSP Recording	103
Deactivating DSP Recording	103
Getting the Phone IP Address	104
Getting Information about Phones	104
Installing the Teams APK (or Any Other APK) using SSH	105
Getting Company Portal Logs	105
Getting Logs via the Phone	106
Getting Logs using UUID	107
Getting Audio Debug Recording Logs	109
Collecting Media Logs (*.blog) from the Phone	109
Manually Performing Recovery Operations	110

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)

Specifications

The following table summarizes the software specifications of the AudioCodes IP phones for Microsoft Teams.

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

Feature	Details
	<ul style="list-style-type: none"> ■ 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 (Calendar Access and Meeting Details; Presence Integration; Exchange Calendar Integration; Contact Picture Integration; Corporate Directory Access) ■ Meetings (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 https://docs.microsoft.com/en-us/MicrosoftTeams/phones-for-teams).
Configuration and Management	<ul style="list-style-type: none"> ■ Microsoft Teams & Skype for Business Admin Center (Provisioning and Logging) ■ AudioCodes Device Management and AudioCodes Redirect Server for monitoring, upgrading and configuring
Debugging Tools	<ul style="list-style-type: none"> ■ Log upload to Microsoft server (certification for 3rd party Skype for Business clients) ■ Remote logging via Syslog ■ SSH Access ■ Capturing the phone screen ■ TCPdump ■ Company Portal (Intune) logs ■ Audio Debug recording logs ■ Media logs (*.blog) ■ Port mirroring network monitoring (C450HD) ■ 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.

Feature	Details
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 for WAN and LAN ✓ RJ-9 port (jack) for handset ✓ USB port for headset support ✓ RJ-11 interface ■ 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 ■ Integrated optional Bluetooth support (Currently supported at a Beta level) ■ Power: <ul style="list-style-type: none"> ✓ DC jack adapter 12V ✓ Power supply AC 100 ~ 240V ✓ PoE Class 3: IEEE802.3af (optional) ■ Keys: <ul style="list-style-type: none"> ✓ Hold ✓ Mute ✓ Transfer ✓ Volume ✓ Headset (including LED) ✓ Speaker (including LED) ✓ Back ✓ Home

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 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 the devices to improve security:

- See [Google Play Services](#) on the next page
- See [Running Android in Kiosk Mode](#) on the next page
- See [AudioCodes Private Key](#) on the next page
- See [Android Debug Bridge \(ADB\)](#) on the next page
- See [App Signing](#) on the next page
- See [Web Browser](#) on the next page
- See [Remote Configuration Management](#) on the next page
- See [AudioCodes Device Manager Validation](#) on page 6
- See [Device File System](#) on page 6
- See [Debugging Interface](#) on page 6
- See [Android Security Updates](#) on page 6

Google Play Services

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

- Updating the 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).

AudioCodes Private Key

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

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 that all apps are digitally signed with a developer key before installation; the devices currently verify that apps are signed by Microsoft.

Web Browser

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

Remote Configuration Management

Native Teams 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 phones validate the AudioCodes Device Manager identity using a known Root CA:

- The device is shipped with known Root CAs installed. See [AudioCodes Root CA Certificate below](#).
- For the initial connection, the AudioCodes Device Manager accesses devices using a known CA.
- Once a successful secured connection has been established between the device and the Device Manager, the user can replace the Root CA on the Device Manager and on the phone, and re-establish the connection leveraging any Private Root CA.

Device File System

The device's file system is encrypted on the C470HD, C435HD and C450HD-DBW devices. Customers may enforce a policy of device encryption via Microsoft's cloud-based Intune service.

Debugging Interface

- The 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.

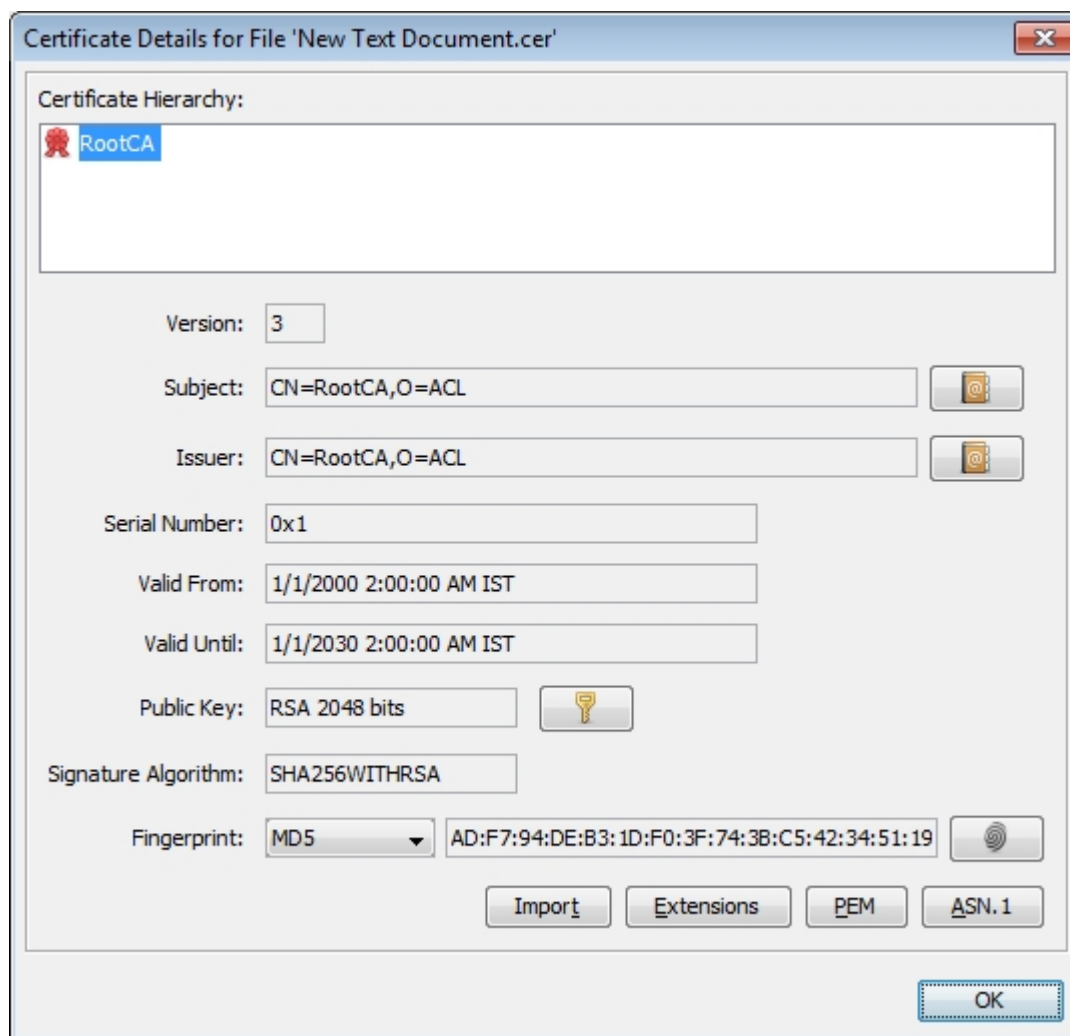
Android Security Updates

AudioCodes regularly adopts and integrates Android security updates.

For reference, see <https://source.android.com/security/bulletin/2019-10-01>.

AudioCodes Root CA Certificate

The following figure shows the AudioCodes Root CA Certificate.



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

MIIDMTCCAhmGAWIBAgIBATANBgqhkiG9w0BAQsFADAFMQwwCgYDVQQKEwNBQ0wx

DzANBgNVBAMTBiJvb3RDQTAeFw0wMDAxMDEwMDAwMDBaFw0zMDAxMDEwMDAwMDBa

MB8xDDAKBgNVBAoTA0FDTDEPMA0GA1UEAxMGUm9vdENBMiIIBjANBgkqhkiG9w0B

AQEFAAOCAQ8AMIIBCgKCAQEA6GK495KUCXAm/UE17G4/cjnZN4LNaxYEZbfZL0a

EhgSKYt/LQ+iUcDhojsneusNgrcGkpwKklKsGsvGWmSRNULV01CW+TX2VJN73+hh
V0uzhyOIYAUhbDaoqNM6Kp5b7sJ1ew4lg9kfd/ma9Czl5koESLw/inLj/r+rD96

mUcPEIWkKspv7Qy4I14fsK/yMArixRopTL1munVVPpSFM9Jh8IY3JHyr5CQJXK
Ks
EhGAJsnHaRqsR2Su3X/WtslgEF+cvP34pxhFL29nMfnaFATSS3rgGaFISvl1ZS
esLMqkWjp9cqGYrvt7K61sYnvMMb+o/KbWqVokXb+Fr7bwIDAQABo3gwdjAMB
gNV
HRMEBTADAQH/MB0GA1UdDgQWBBQDXySn9hz15IDraZ+iXddZGReB+zBH
BgNVHSME
QDA+gBQDXySn9hz15IDraZ+iXddZGReB+6EjpCEwHzEMMAoGA1UEChMDQ
UNMMQ8w
DQYDVQQDEwZSb290Q0GCAQEwDQYJKoZIhvcNAQELBQADggEBAI0rUyw
ommWWJnH3
JOfKiS3+VnX5hJITZymvWanMXUz/6FonHccPXEByTrUYwhiWx3dwELAFXDF
KkxMp
0KKWZ4F39cAOLRjqhzya+xUeeJ9HQZCXYAJ6XgvTfN2BtyZk9Ma8WG+H1hN
vTZY
QLbWsjQdu4eFniEufeYDke1jQ6800LwMIFlc59hMQCeJTEnRx4HdJbJV86k1gBU
E
A7fJT1ePrRnXNDRz6QtADWoX3OmN7Meqen/roTwvLpEP22nYwvB28dq3Jetl
QKwu
XC4gwl/o8K2wo3pySLU9Y/vanXXCr0/en5l3RDz1YpYWmQwHA8jJlu8rxdhr+VN
Q
Zv6R/Ys=
-----END CERTIFICATE-----

2 Setting 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

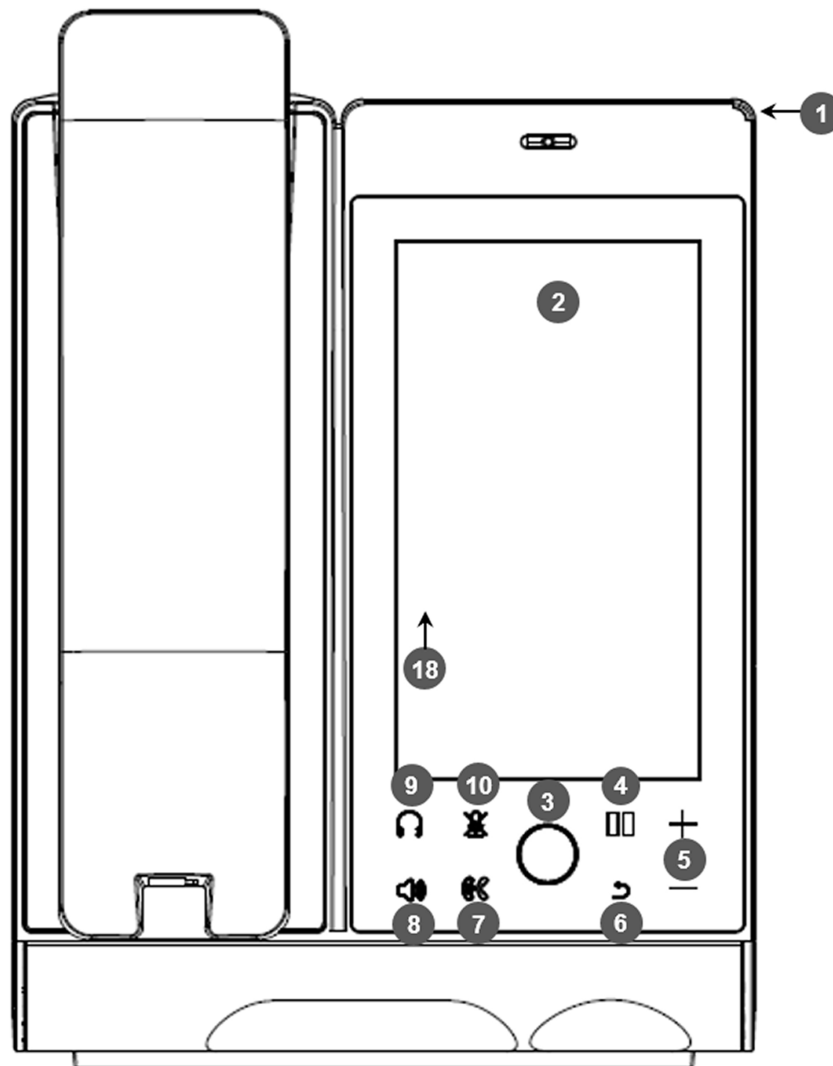


Table 2-1: Font View Description

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

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 it to return to the phone's home (idle) screen from any screen. ■ Long-press it to open the device Settings screen.
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 74 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.

Rear View

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

Figure 2-2: Rear View

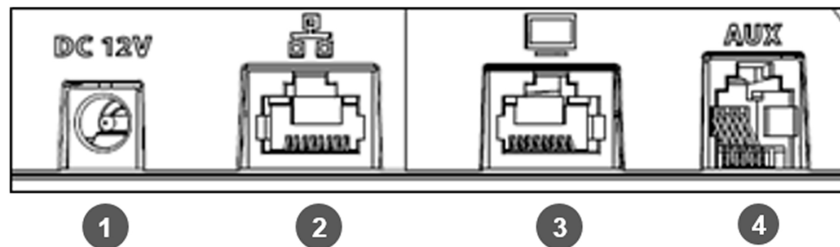


Table 2-2: Rear View Description

#	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.

Before Using AudioCodes Devices

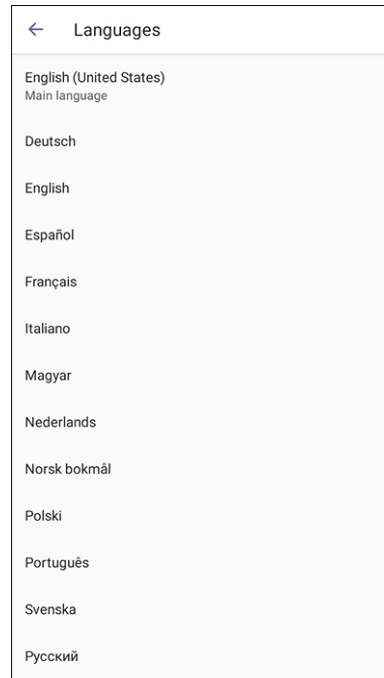
AudioCodes recommends frequently cleaning devices' touch screens especially the screens on devices in common use areas such as conference rooms and lobbies.

➤ To clean a device's touch 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

After connecting the phone to the network (or resetting it), the language selection screen is displayed by default.



Touch the language of your choice and then configure device settings to match specific requirements.



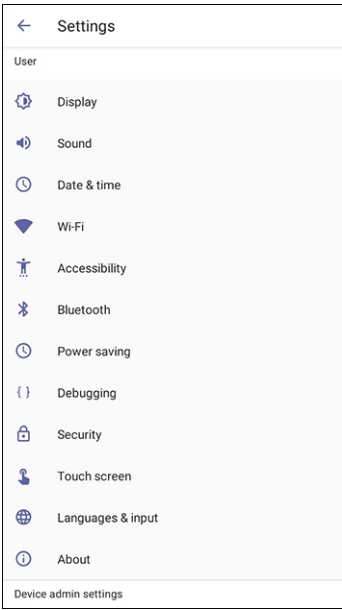
Only if the phone is restored to default settings will it be necessary to repeat this.

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 enterprise requirements.

➤ To access device settings:

1. In the home screen, touch the avatar picture and then touch the option **Settings** and then the option **Device settings**.

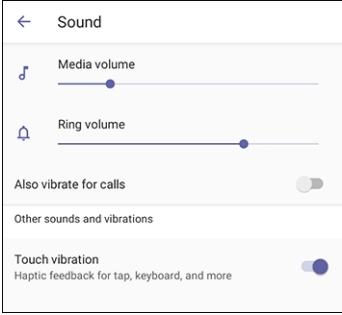
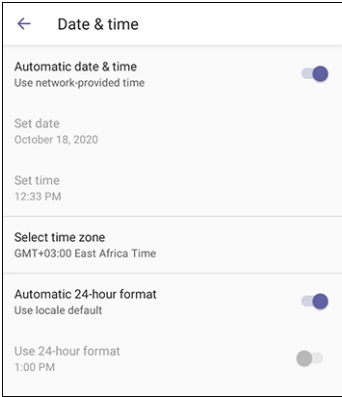
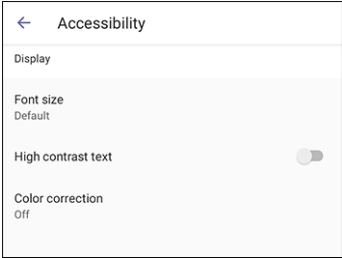


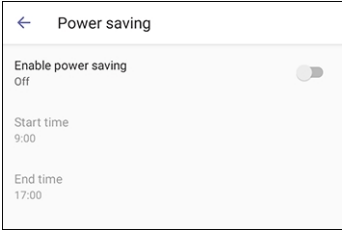
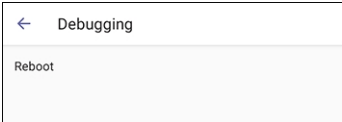
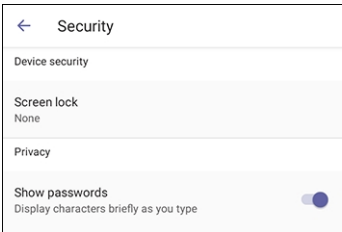
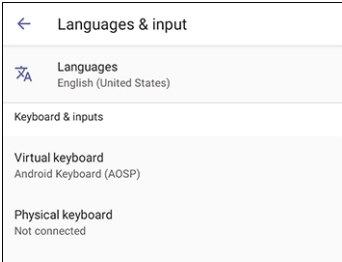
2. Under 'User', view the settings; touch a setting to open it. Scroll down to view the settings under 'Device admin settings'. Use this table as reference.

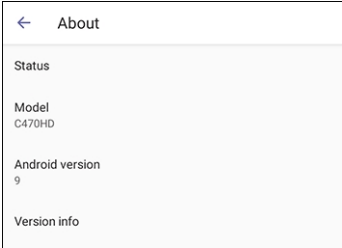
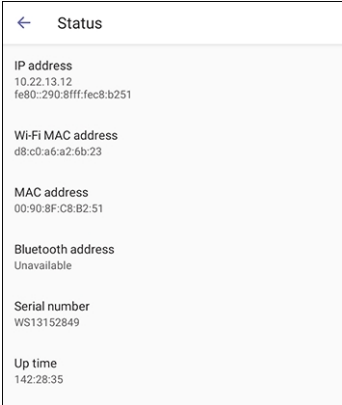
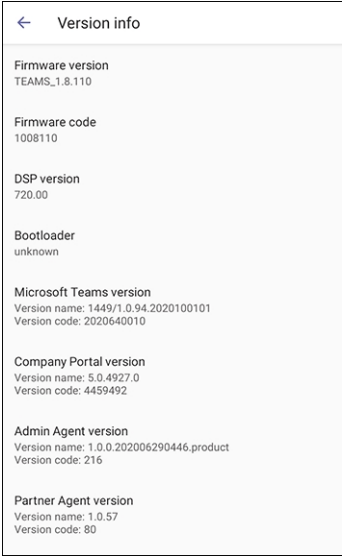
Table 3-1: Device Settings

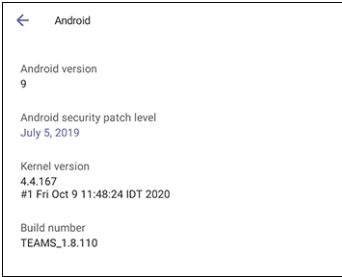
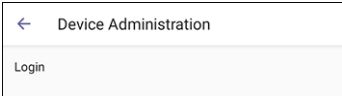
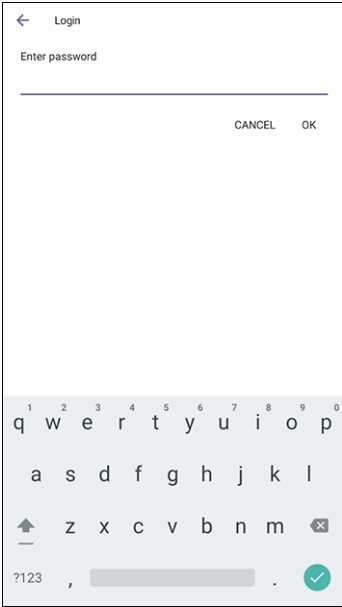
Setting	Description
'User'	
Display	<div>Opens the 'Display' screen [Brightness level].</div> <div></div> <div>The phone's screen supports different brightness levels. Choose the level that best suits your requirements.</div> <div><input checked="" type="checkbox"/> Sleep</div>

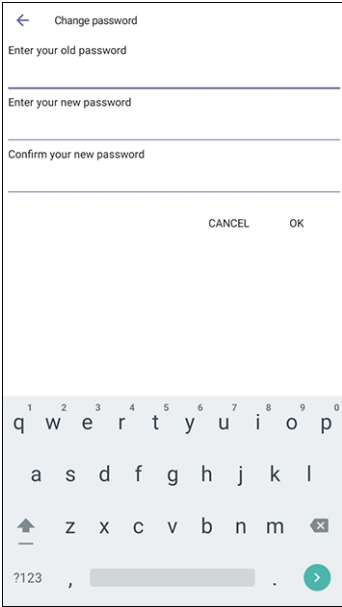
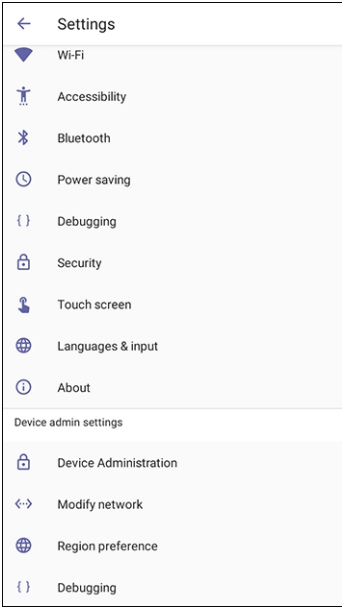
Setting	Description
	<div> <div> <div>←</div> <div>Sleep</div> </div> <div> <div><input type="radio"/></div> <div>Never</div> </div> <div> <div><input type="radio"/></div> <div>30 seconds</div> </div> <div> <div><input type="radio"/></div> <div>1 minute</div> </div> <div> <div><input type="radio"/></div> <div>2 minutes</div> </div> <div> <div><input type="radio"/></div> <div>5 minutes</div> </div> <div> <div><input checked="" type="radio"/></div> <div>10 minutes</div> </div> <div> <div><input type="radio"/></div> <div>30 minutes</div> </div> </div> <div> <div>■</div> <div>Screen saver</div> </div> <div> <div> <div>←</div> <div>Screen saver</div> </div> <div> <div>On</div> <div><input checked="" type="checkbox"/></div> </div> <div> <div>Current screen saver</div> <div>Clock</div> <div>⚙</div> </div> </div> <div> <div>■</div> <div>Font size</div> </div> <div> <div> <div>←</div> <div>Font size</div> </div> <div> <div>Sample text</div> <div>The Wonderful Wizard of Oz</div> <div>Chapter 11: The Wonderful Emerald City of Oz</div> <div>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.</div> <div>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.</div> <div>There seemed to be no horses nor animals of any kind; the</div> <div>Preview</div> <div> <div>Default</div> <div>A <input type="range"/> A</div> <div>Make the text on screen smaller or larger.</div> </div> </div> </div>
Sound	<p>Allows you to customize phone volume for a friendlier user experience.</p> <p>Ring volume at n%</p>

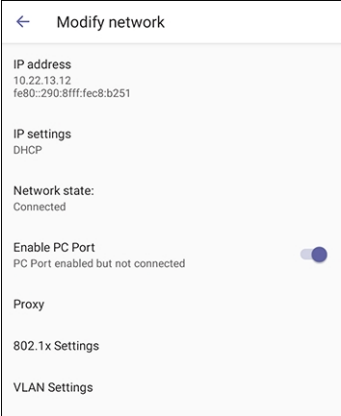
Setting	Description
	
Date & time	<p>Date and time are automatically retrieved from the deployed Network Time Protocol (NTP) server.</p>  <p>Use 24-hour format [Allows you to select the Time format]</p>
Wi-Fi	<p>The phone can connect to an Access Point via Wi-Fi. See the phone's <i>Quick Guide</i> for detailed information on setting up Wi-Fi. See also Configuring Wi-Fi on page 27 in this document for information about configuring the feature.</p>
Accessibility	<p>Allows making the screen reader-friendlier. See also Enabling Google Talkback on page 47.</p> 
Bluetooth	<p>Hands free profile where the phone is able to connect to Bluetooth headset or speaker.</p> <p>See the phone's <i>Quick Guide</i> for detailed information on setting up Bluetooth.</p>

Setting	Description
Power Saving	<p>Allows users to contribute to power saving in the enterprise.</p>  <p>Enable power saving</p> <p>Start time [The device consumes minimal energy before the user arrives at the office]</p> <p>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 untouched for 10 minutes (default), it automatically locks and is inaccessible to anyone who doesn't know its lock code.]</p> <p>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> 

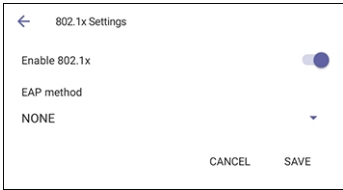
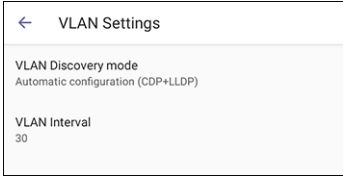
Setting	Description
About [Android 7.1.2]	<p>Enables users to determine device information.</p>  <p>To determine the device's IP address, select the 'Status' option.</p>  <p>To get information about the version, select 'Version info'.</p>  <p>To get information about the Android version, select 'Android version'.</p>

Setting	Description
	
'Device admin settings'	
Device administration	<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>Touch Login and then in the Login screen that opens, touch 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 (shown first below) or QWERTY (shown second below).</p> 

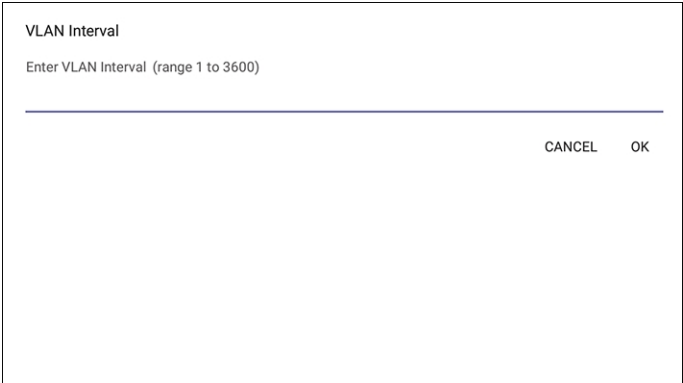
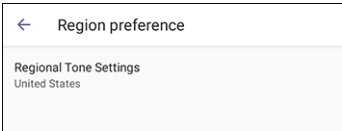
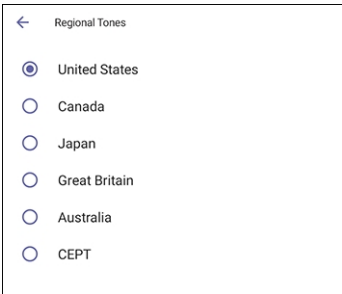
Setting	Description
	 <p>These virtual keyboards are also displayed when network administrators need to enter an IP address to debug, or when they need to enter their PIN lock for the security tab.</p> <p>After logging in, scroll down in the Settings screen to the section 'Device admin settings'.</p> 
Modify network	Enables the Admin user to determine network information and to modify network settings.

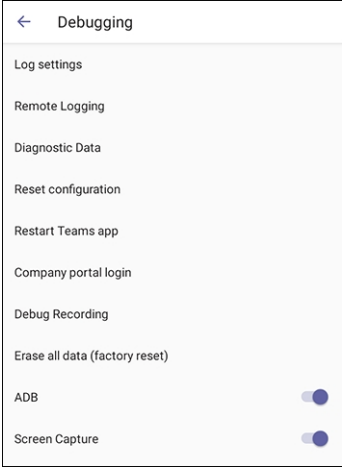
Setting	Description
	 <p>IP Address [Read Only]</p> <p>IP Settings [DHCP or Static IP]</p> <p>Network state [Read Only]</p> <p>Enable PC port</p> <p>Enable PC port mirror</p> <p>Proxy</p> <p>802.1x Settings</p> <p>VLAN Settings. Allows you to configure the VLAN mode Manual, CDP only or LLDP only.</p>
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, touch the Modify network. b. Touch the Proxy option and then configure the proxy host name and port:

Setting	Description
	<div data-bbox="603 264 948 869"> </div> <p>■ 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:</p> <div data-bbox="603 1077 1257 1787"> </div> <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</p>

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

Setting	Description
	<div data-bbox="564 262 906 519"> </div> <p>■ Cisco Discovery Protocol (CDP) is a Cisco proprietary Data Link Layer protocol</p> <p>■ Link Layer Discovery Protocol (LLDP) is a standard, layer two discovery protocol</p> <p>Select the mode you require and then touch OK. If you select Manual configuration, this screen opens:</p> <div data-bbox="564 842 906 1447"> </div> <p>Touch VLAN ID.</p> <div data-bbox="564 1534 906 1691"> </div> <p>Touch VLAN Priority.</p> <div data-bbox="564 1778 906 1935"> </div>

Setting	Description
	<p>Touch VLAN Interval.</p>  <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>
Region preference	<p>Touch the menu option Region preference.</p>  <p>This option allows you to define the country in which the phone is located. The setting determines which regional tone the phone will use. Call Progress Tones (CPTs) are country-specific; the behavior and parameters of analog telephones lines vary from country to country. Touch Regional Tone Settings and select the country in which the phone is located.</p> 
Debugging	Allows the Admin user to perform debugging for troubleshooting purposes. Available after logging in as Admin.

Setting	Description
	 <p>Log settings</p> <p>Remote Logging (see under Remote Logging on page 99 for more information)</p> <p>Diagnostic Data (see under Diagnostic Data on page 100 for more information)</p> <p>Reset configuration</p> <p>Restart Teams app</p> <p>Company portal login</p> <p>Debug Recording (for Media/DSP debugging) (see under Remote Logging on page 99 for more information)</p> <p>Switch to Teams Compatible</p> <p>Factory data reset (the equivalent of restore to defaults; including logout and device reboot)</p> <p>ADB (Android Debug Bridge command-line tool used to debug the Teams app); the setting is disabled by default; leave it unchanged at the default unless there's a real necessity to use it.</p> <p>Screen Capture. By default, this setting is enabled. If it's disabled, the phone won't allow its screens to be captured.</p>

Configuring Wi-Fi

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

Table 3-2: Wi-Fi Parameters

Parameter	Description	Values
network/wifi_enabled	Enables/disables the Wi-Fi feature.	0 (disable, default)

Parameter	Description	Values
		1 (enable)
network/wifi_pc_bridge	Enables network connectivity for the PC behind the phone; for debugging purposes.	0 (disable, default) 1 (enable)
network/wifi_ipv4_method	Defines the Dynamic or Static IP address for Wi-Fi.	DHCP (default) STATIC
network/wifi_channel_mode	Enables the Wi-Fi channel mode: <ul style="list-style-type: none"> <input type="checkbox"/> 2.4G only <input type="checkbox"/> 5G only <input type="checkbox"/> 2.4G+5G 	5G_2_4G (default) 2_4G_ONLY 5G_ONLY

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

Table 3-3: Wi-Fi Parameters per Index

Parameter	Description	Values
network/wifi/[0-15]/ssid	Saves the Access Point's SSID.	-
network/wifi/[0-15]/password	Saves the password for some authentication methods which need it, e.g., WPA PERSONAL, WPA2 PERSONAL	-
network/wifi/[0-15]/security	Saves the Access Point's authentication method: • WPA PERSONAL • WPA2 PERSONAL • WPA ENTERPRISE • WPA2 ENTERPRISE	-
network/wifi/[0-15]/auto_reconnect	Configure this parameter to reconnect this SSID automatically.	1 (default, enable) 0 (disable)
network/wifi/[0-15]/identity	Saves the identity for some authentication methods that need it, e.g., WPA PERSONAL, WPA2 PERSONAL	-
network/wifi/[0-15]/anonymous_identity	Saves the anonymous identity for some authentication methods that need it, e.g., WPA ENTERPRISE, WPA2 ENTERPRISE, etc.	-

Parameter	Description	Values
network/wifi/[0-15]/phase2_authentication	Phase 2 authentication for WPAENTERPRISE, WPA2ENTERPRISE. The phone supports PAP, MSCHAP, MSCHAPV2, CHAP, MD5, GTC	-
network/wifi/[0-15]/pin_code	Defines the PIN code for the WPS PIN code authentication method.	String of up to 64 characters
network/wifi/[0-15]/wps_method	Defines the WPS method. The phone supports PIN and push button.	None ALL (default) PIN AUTH PBC

Restoring the Phone to Default Settings

Users can restore the device to factory default settings at any time. The feature can be used if a user forgets their Admin password, for example. Two kinds of restore are available:

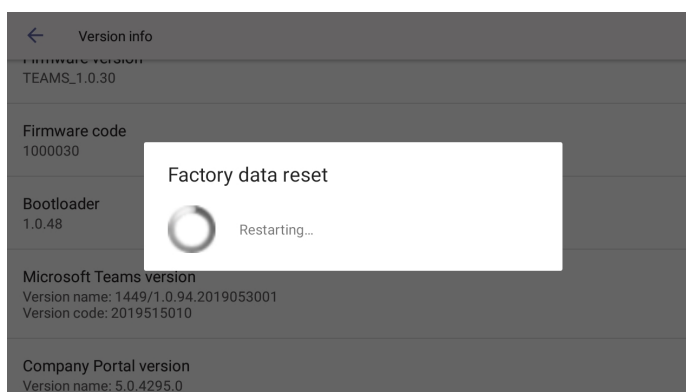
- [Performing a Hard Restore](#) below
- [Performing a Soft Restore](#) on the next page

Performing a Hard Restore

You can restore the phone's settings to their defaults when the phone is up and running (see below)

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

1. Long-press the HOLD key on the phone (more than 15 seconds); the screen shown below is displayed and the device performs a restore to default factory settings.



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

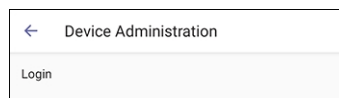
2. Touch **OK**; the sign-in screen is displayed (see [Signing In](#) on page 34 for more information).

Performing a Soft Restore

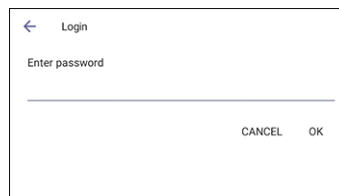
Users must log in as Administrator in order to perform a soft restore. The soft restore is then performed in the 'Debug' screen.

➤ To perform a soft restore:

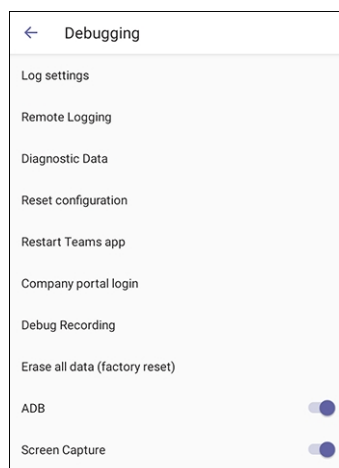
1. In the Settings screen, scroll down and touch the **Device Administration** option.



2. Touch the **Login** menu item.



3. Touch the field for the virtual keyboard to be displayed and then enter the default password of **1234**; you're prompted with 'You are now logged in'; you now have Admin privileges to configure settings.
4. Under 'Device admin settings', select the **Debugging** option.



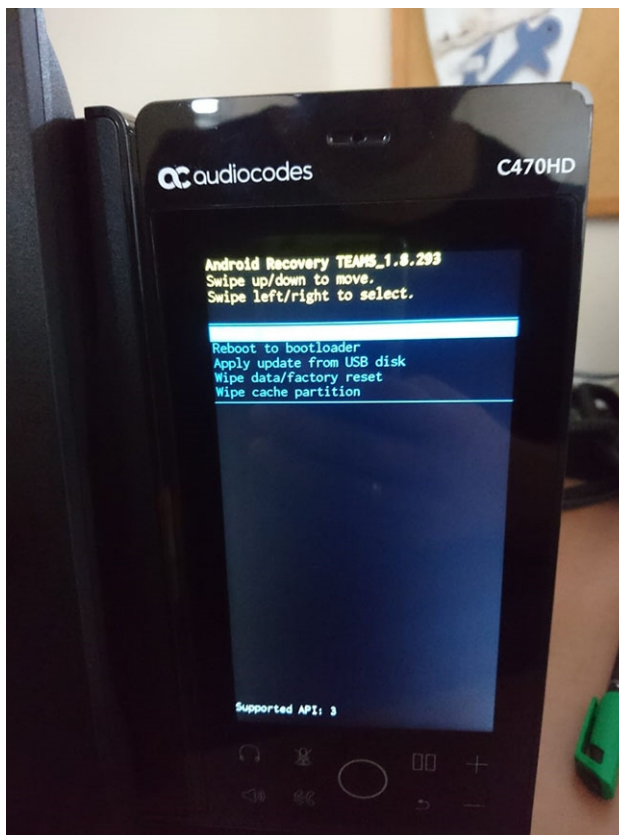
5. Touch the **Erase all data (factory reset)** option; the device performs a restore to default factory settings.

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](#) on the next page)
- Automatic lock ([Automatic Lock](#) below)

Automatic Lock

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

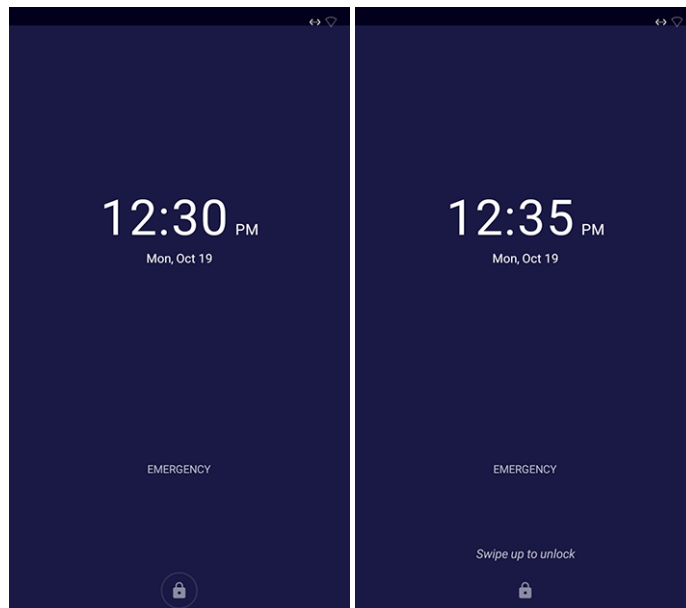
➤ To lock the phone:

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

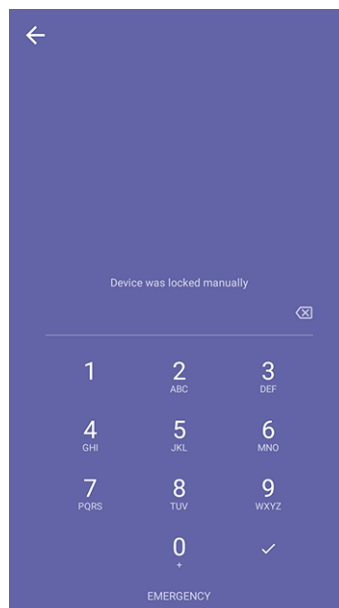
Unlock

➤ To unlock the phone:

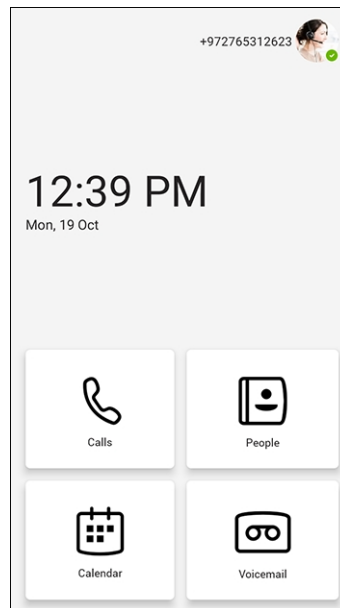
1. When the screen shown in the figure below is displayed, touch the lock icon and swipe up



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 documentation 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:

- NTP Time server **2.android.pool.ntp.org**
- **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.windows.com**. Phones can be configured with this NTP server option when migrating from Skype for Business phones to Native Teams phones. The option accelerates customers' migration process. The Native Teams phones' default NTP server is sometimes not configured in DHCP Option 42. If the default NTP server is not configured in DHCP Option 42, the phones 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.windows.com**) and if it's unavailable, the server **time.nist.gov** described next.
- **time.nist.gov**. Phones can be configured with this NTP server option when migrating from Skype for Business phones to Native Teams phones. The option accelerates customers' migration process. The Native Teams phones' default NTP server is sometimes not configured in DHCP Option 42. If the default NTP server is not configured in DHCP Option 42, the phones 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.

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.

The network administrator must make sure the phone can access the following URLs (to check connectivity with the internet):

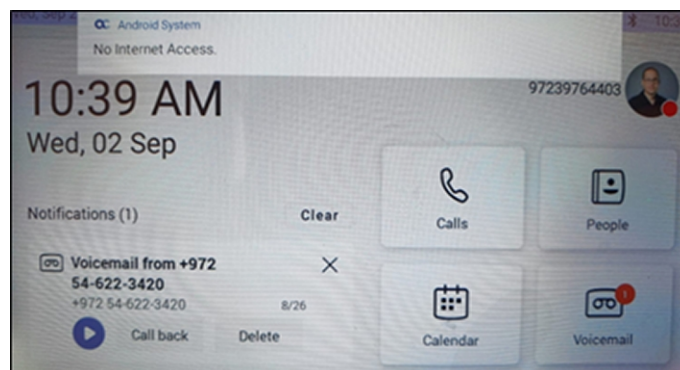
https://www.google.com/generate_204

http://connectivitycheck.gstatic.com/generate_204

http://www.google.com/gen_204

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

4/5/21 11:48

Sign in to make an emergency call.



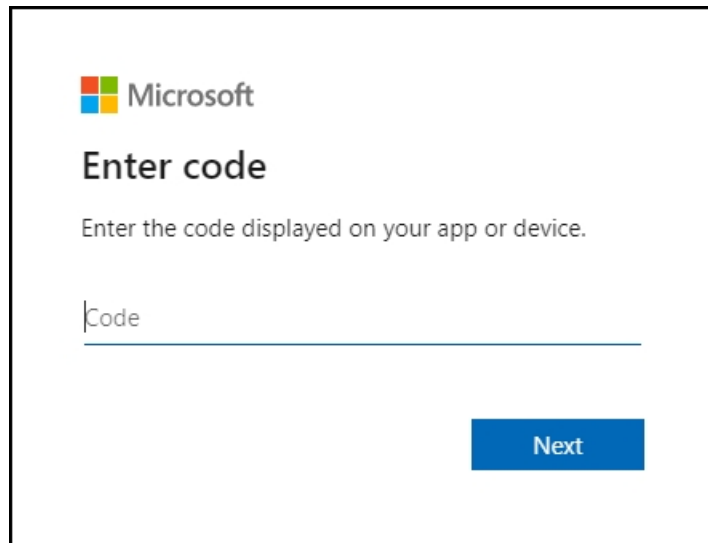
Step 1 On your computer or mobile, go to <https://microsoft.com/devicelogin>

Step 2 Enter the code below to sign in.

D2GYDZSGS

Sign in on this device

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

A screenshot of the Microsoft 'Enter code' login screen. At the top left is the Microsoft logo. Below it, the text 'Enter code' is displayed in a large, bold font. Underneath that, a smaller line of text says 'Enter the code displayed on your app or device.' Below this text is a text input field with the placeholder text 'Code'. At the bottom right of the screen is a blue button with the word 'Next' in white text.

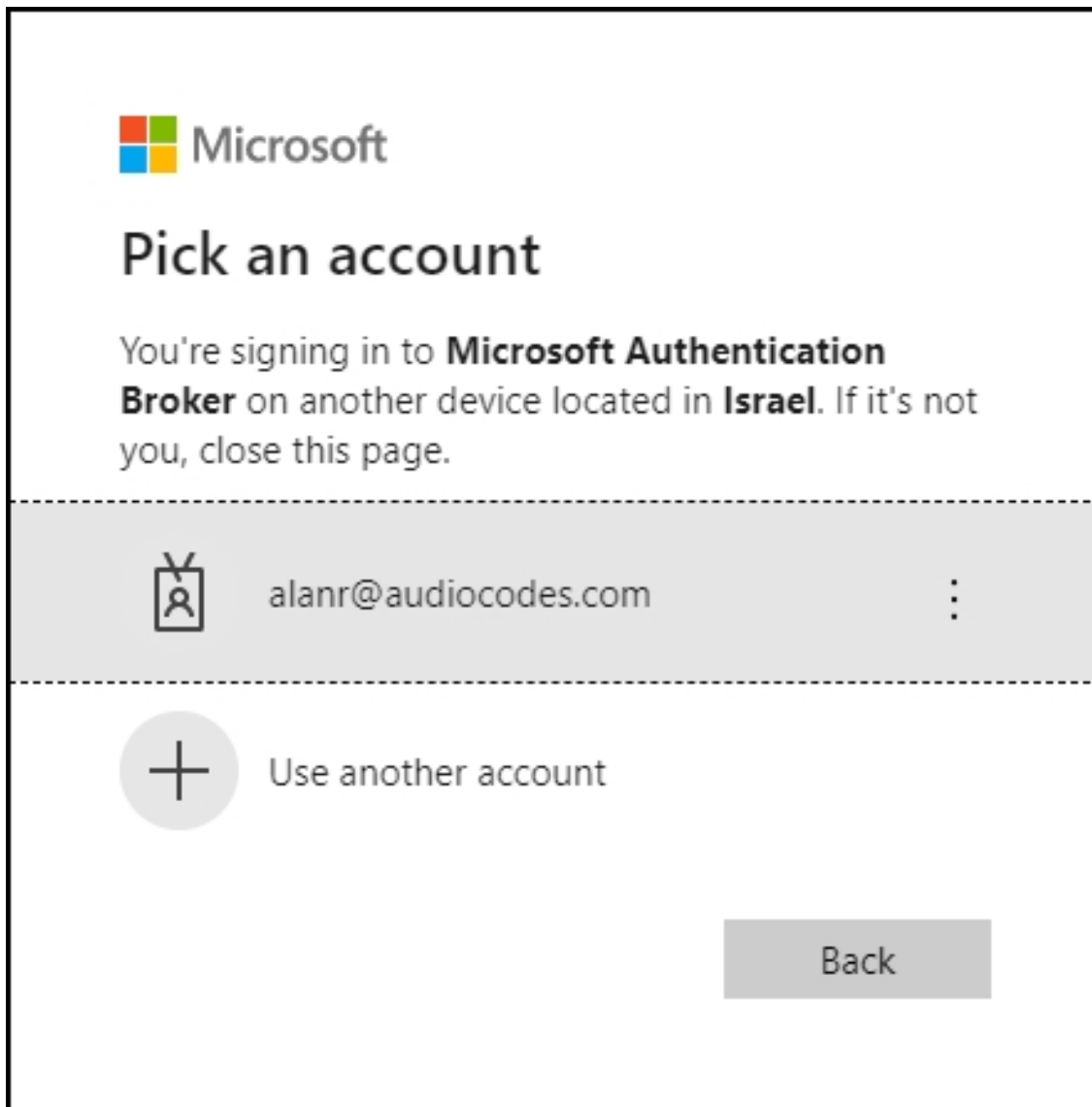
Microsoft

Enter code

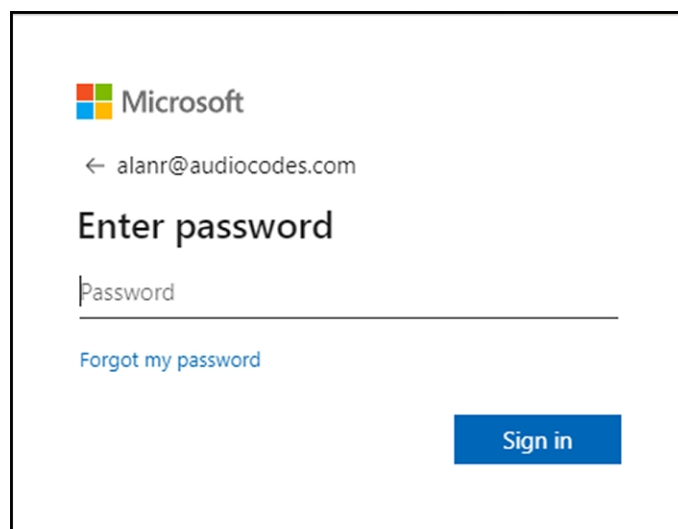
Enter the code displayed on your app or device.

Next

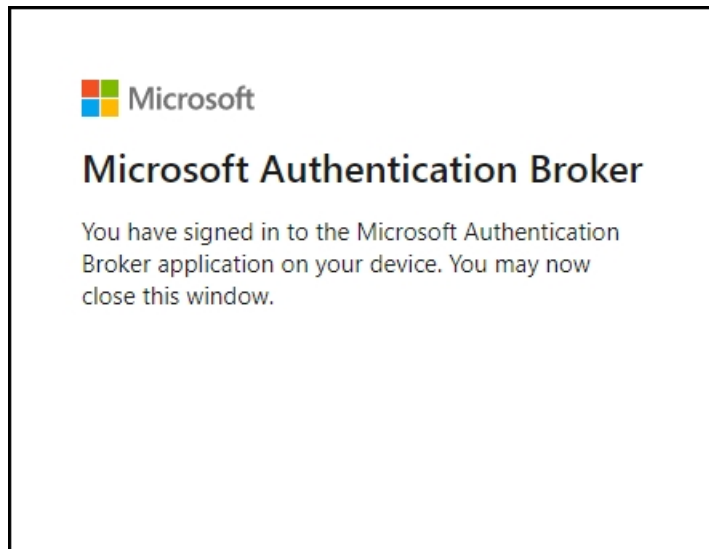
3. Key in the code and then click **Next**.



4. Click the account.



5. Key in 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 your phone returns to the initial code screen. In that screen, touch **Sign in on this device**.

4/5/21 11:48

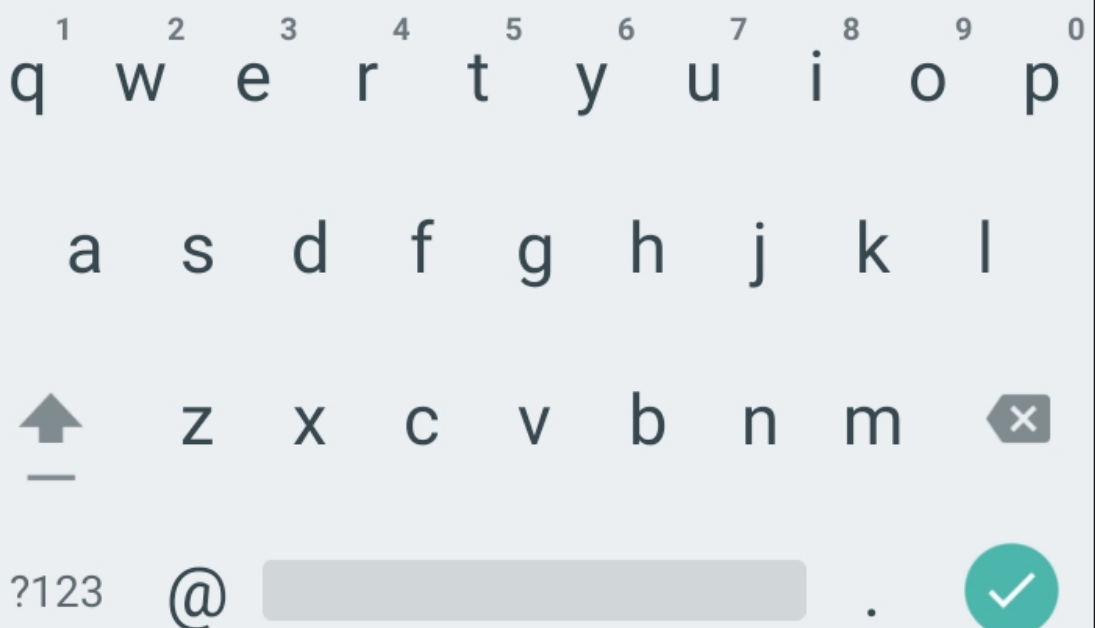


Welcome to Microsoft Teams! A happier
place for teams to work together.



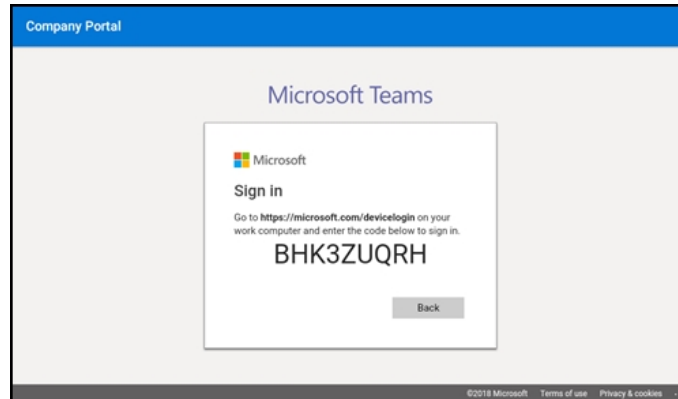
Sign in

[Get help with signing in](#)



8. Touch the 'Email, phone or username' field; a virtual keyboard pops up. Enter one of them and then touch **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).

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



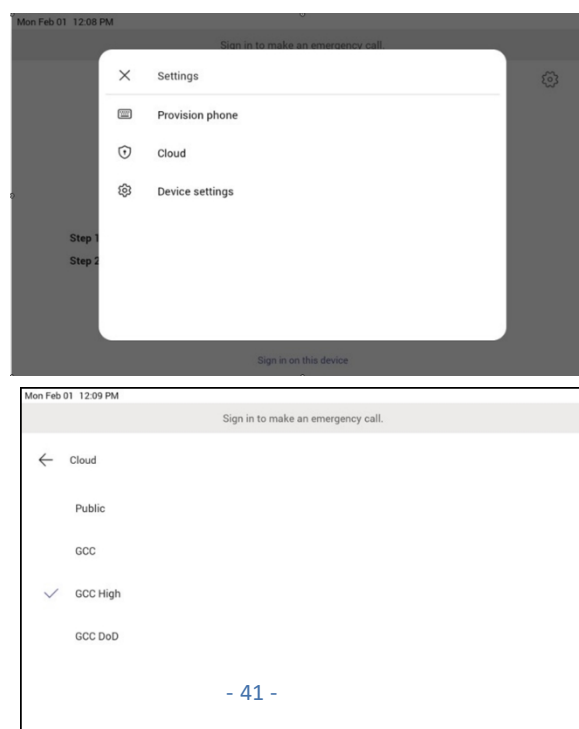
- ◆ In the browser on your PC or smart phone, enter the URL indicated in the preceding screen and then in the phone's Web interface that opens, perform sign-in (as noted previously, this option is recommended if using MFA).



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.



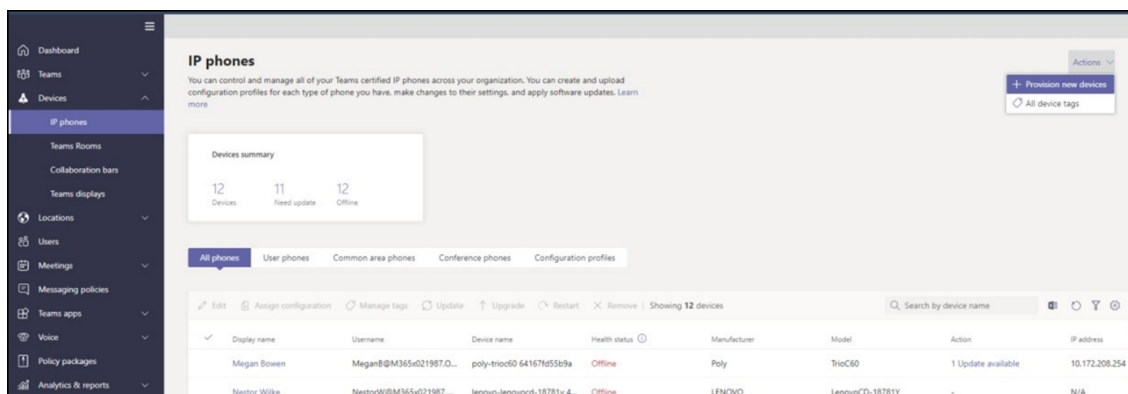
Remote Provisioning and Sign-in from Teams Admin Center

Network administrators 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.

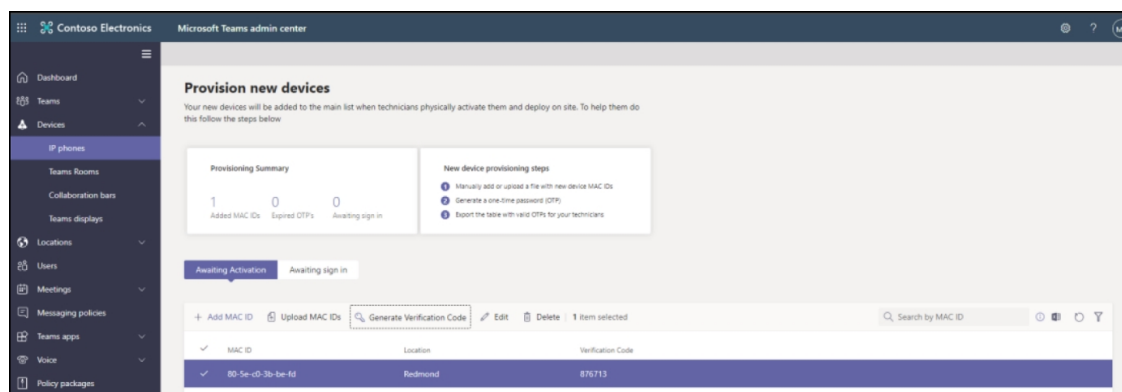
Upload a file to add a device MAC address

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.

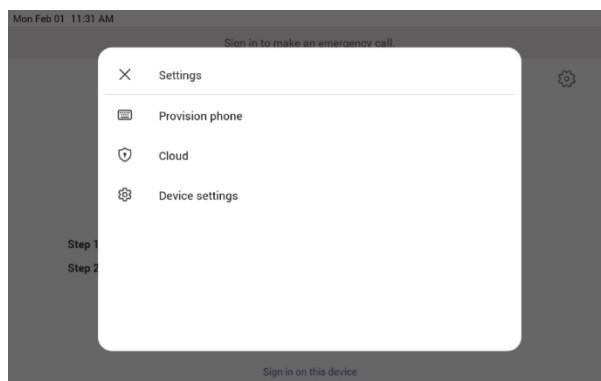
From the **Awaiting Activation** tab, select an existing MAC ID. A password is created for the MAC address and is shown in the **Verification Code** column.



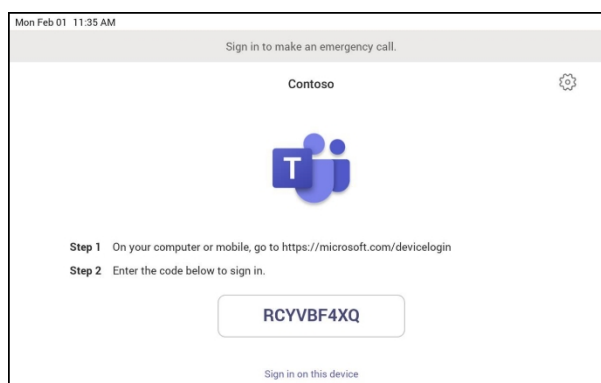
You'll need to provide the list of MAC IDs and verification codes to the field technicians. You can export the detail directly in a file and share the file with the technician who is doing the actual installation work.

➤ 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**.



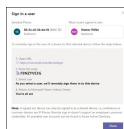
The technician is then expected to enter the device-specific Verification code that was provided in the Teams admin center on the phone's user interface. Once the device is provisioned successfully, the tenant name will be available on the sign in page.



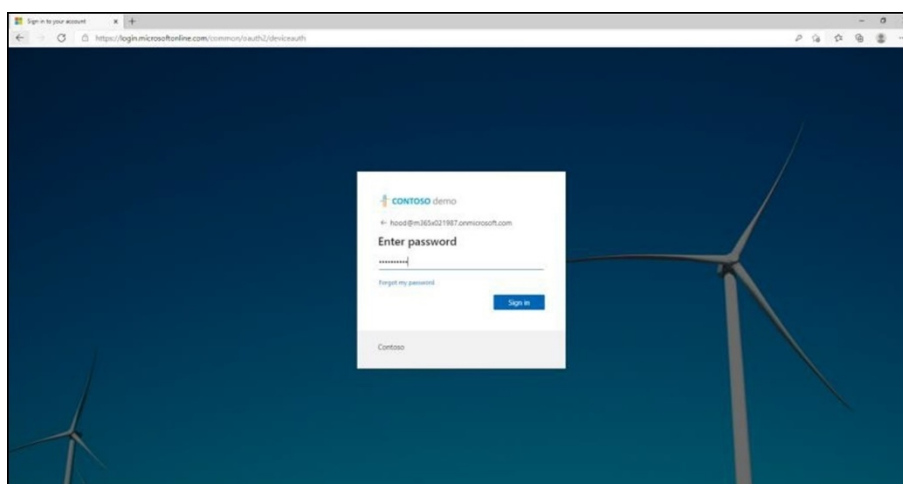
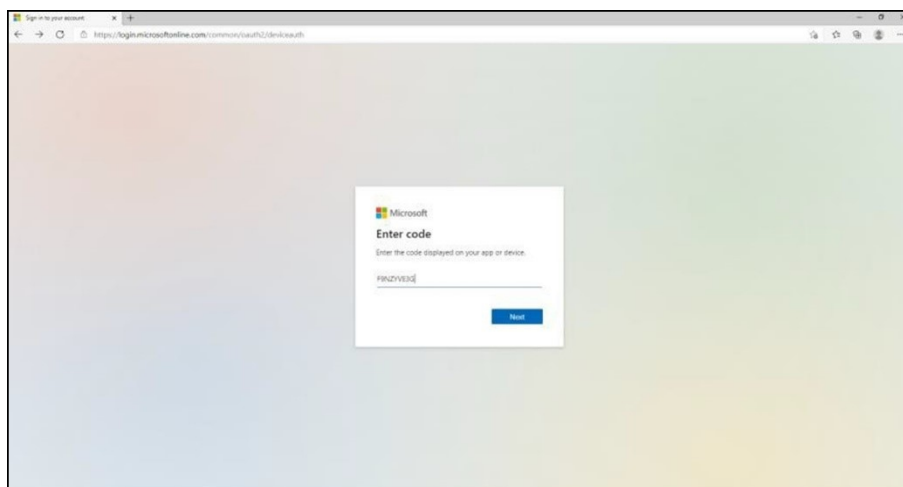
➤ Step 4: Sign in remotely

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

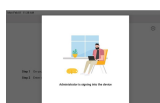
1. Select a device from the **Awaiting sign in** tab.
2. Follow the instructions in **Sign in a user**, and then select **Close**.



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



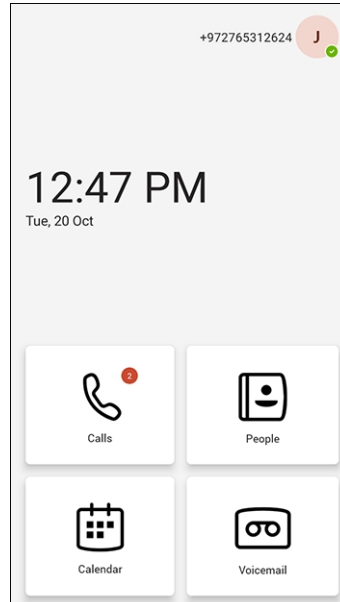
When the tenant admin is signing in from Teams Admin Center, the user interface on the device is blocked to prevent other actions on the phone.



Getting Acquainted with the Phone Screen

The following gets you acquainted with the phone's user interface. The figure below shows the home screen.

Figure 4-3: Home Screen



Touch **Calls**, **People**, **Calendar** or **Voicemail**.

Figure 4-4: Calls Screen

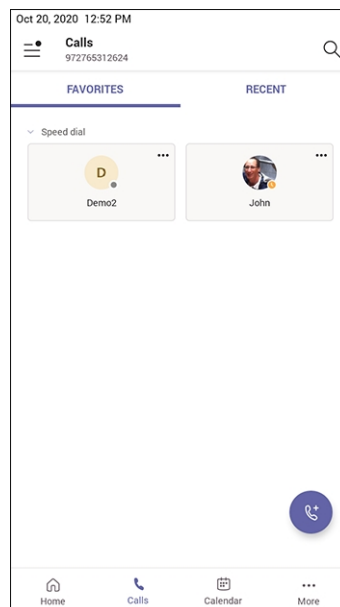


Table 4-1: Calls Screen


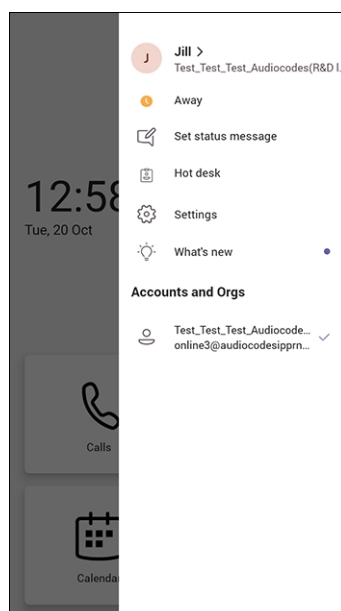
Item	Description
	The phone menu. Touch to open the menu shown in the figure following this table.
Calls	Touch the tab to open the Calls screen. The screen shown in the figure preceding this table opens.
People	Touch the tab to open the People, shown under Using the People Screen on page 58 opens. Allows 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.
Calendar	Touch to open the Calendar screen, shown under Setting up a Meeting on page 57 opens.
Voicemail	Touch the tab to open the Voicemail screen, shown under Accessing Voicemail on page 60 opens.

Figure 4-5: Menu Items

Use this table as reference.

Table 4-2: Menu Item Descriptions

Item	Description
Presence status	See Changing Presence Status on page 52 for more information.

Item	Description
Set status message	See Setting a Status Message on page 50 for more information.
Connect a device	See Connecting a Device for more information.
Hot desk	See Hot Desking on page 52 for more information.
Settings	See Configuring Teams Application Settings on page 54 for more information.
Sign Out	See Signing Out on page 61 for more information.

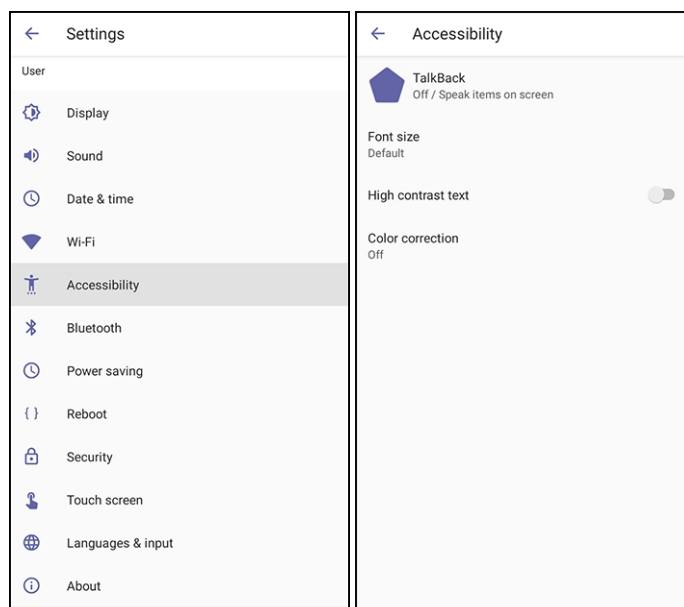
Enabling Google Talkback

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.

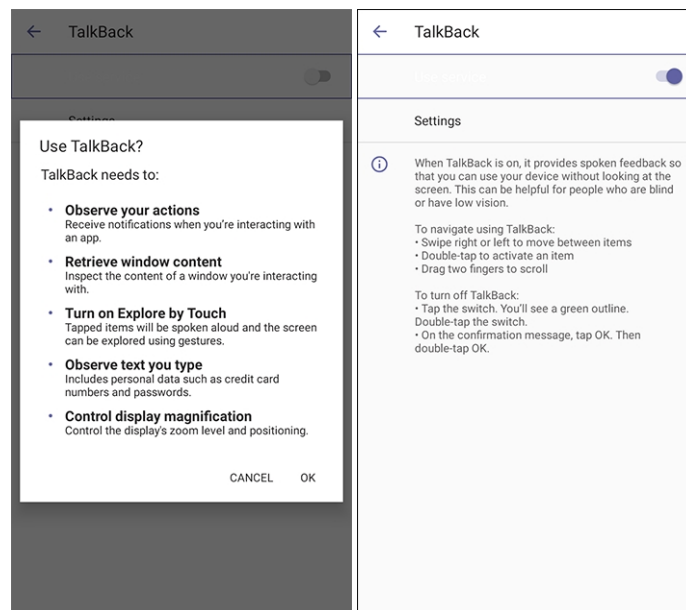
The feature improves the experience of these users.

➤ To enable the feature:

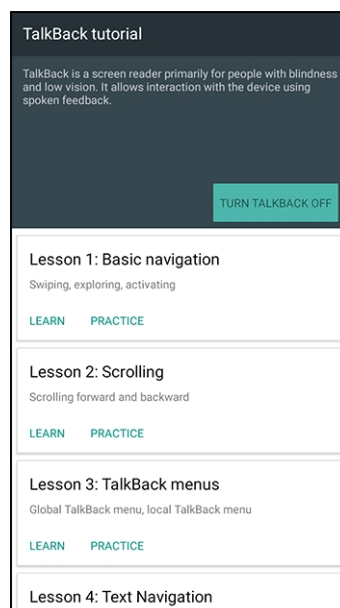
1. Open the Accessibility screen (**Settings > Device settings > Accessibility**).



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

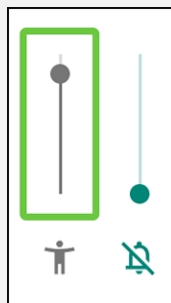


3. Click **OK** to switch the feature on as shown in the preceding figures. Listen to the audio tutorial that begins playing. The tutorial explains how to interact with the device.



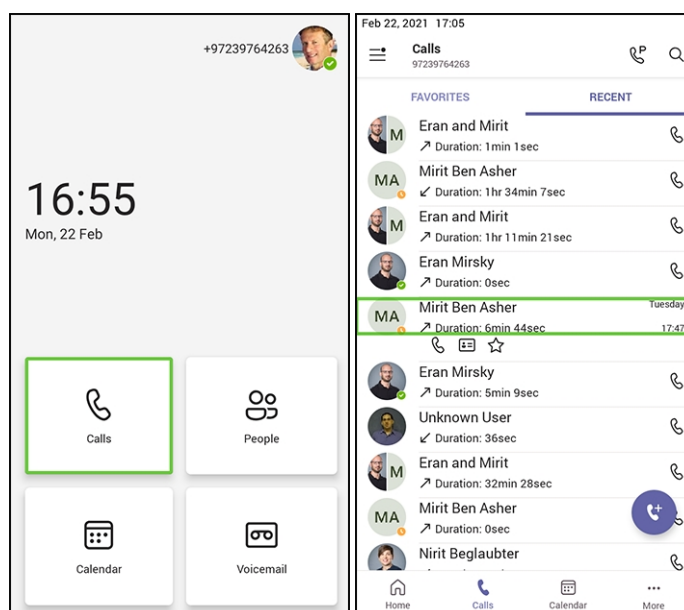


- After TalkBack is switched on, operations are performed by *touching to select* and then *double-touching to activate*.
- To turn up the volume, touch the + key on the phone and in the volume pop-up shown in the figure below, touch the slider to select it; audio announces what level you're at. Double-touch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

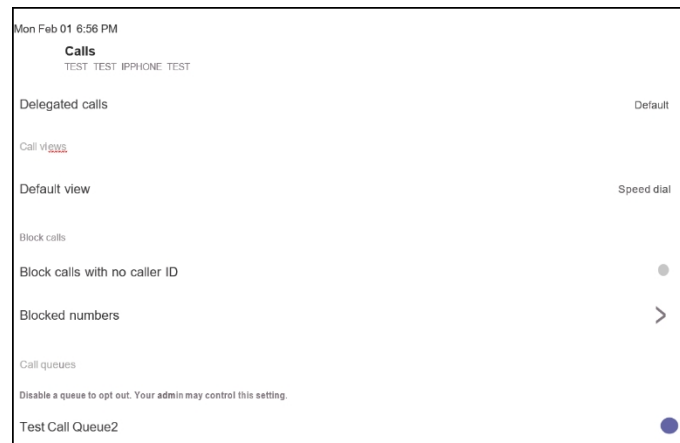
1. In the Calls screen shown in the preceding figure, touch the **Recent** tab; audio informs you what you touched.
2. Touch a listed call as shown in the preceding figure; audio informs you whether the call was outgoing or incoming and to / from whom it was made and the day on which it was made.
3.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



4. Touch 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. Touch 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.

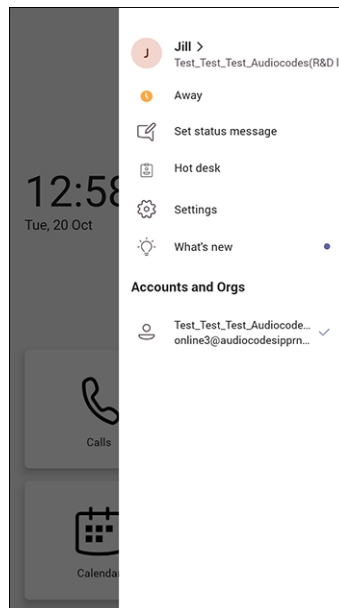


Setting a Status Message

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

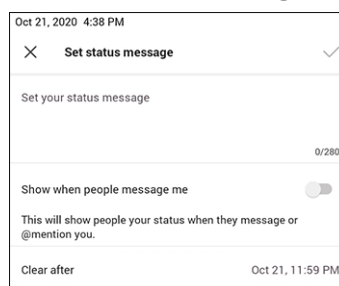
➤ To set a status message:

1. In the home screen, touch the user picture. (In the Calls and Calendar screens, touch ).



2. Touch **Set status message**.

Figure 4-6: Set status message



3. Touch 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. Touch '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:**


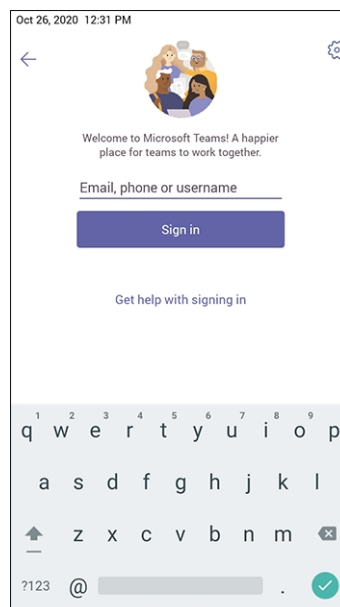
1. Touch the user's photo or avatar picture, and then from the menu touch the option **Hot desk**. Alternatively, in the Calls screen (or People screen, Calendar screen or Voicemail screen), touch the phone menu  and then touch **Hot desk**.

Figure 4-7: Hot desk



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


Changing Presence Status

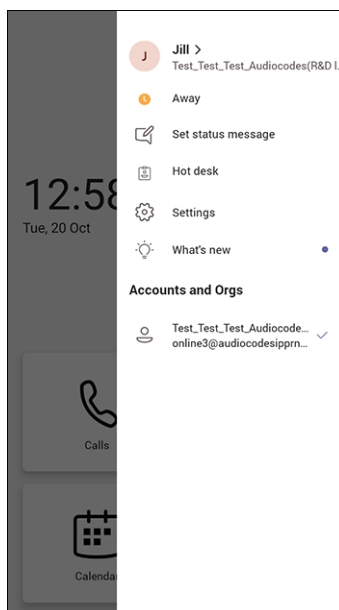
You can assign a presence status to control whether you want people to contact you or not. By default, your status is based on your Microsoft Teams server.



- 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 RGS (Response Group Service) if it is configured.




➤ **To change presence status:**




1. In the home screen, touch the user picture. (In the Calls and Calendar screens, touch ).



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

Table 4-3: 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 touch screen indicates 'Missed Calls'.

Icon	Presence Status	Description
	Be Right Back	You'll be away briefly and you'll return shortly.
	Off Work	You're going on vacation (for example).
	Away	You want to hide your status and appear to others you're currently away.

Configuring Teams Application Settings


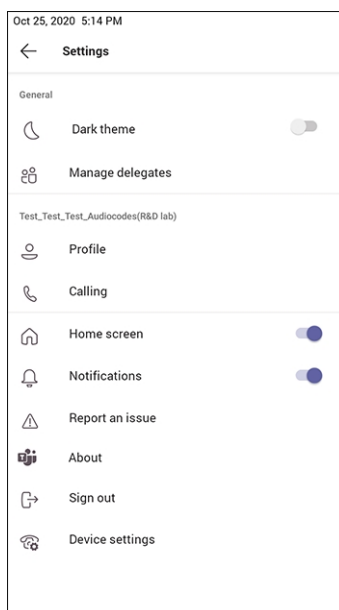
The following describes the Teams application's settings. In the home screen, touch the user picture / avatar. Alternatively, in the Calls screen (or People screen, Calendar screen or Voicemail screen), touch the phone menu  and select the **Settings** option.

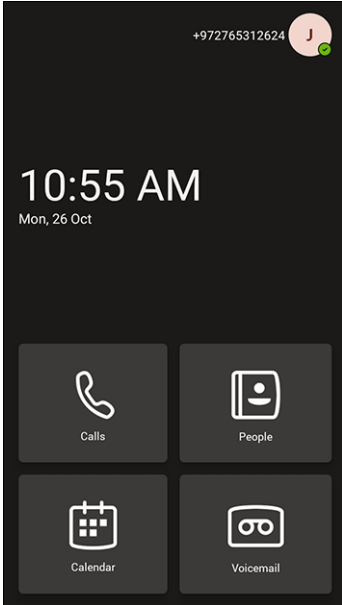
Figure 4-8: Settings



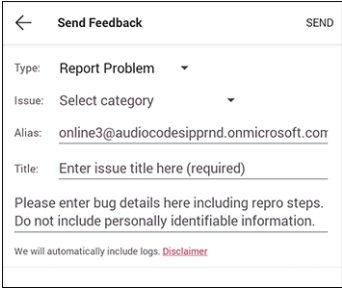
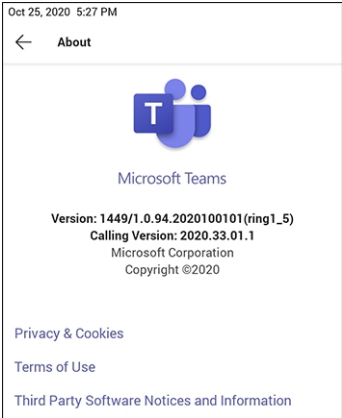
Use this table as reference:

Table 4-4: 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:

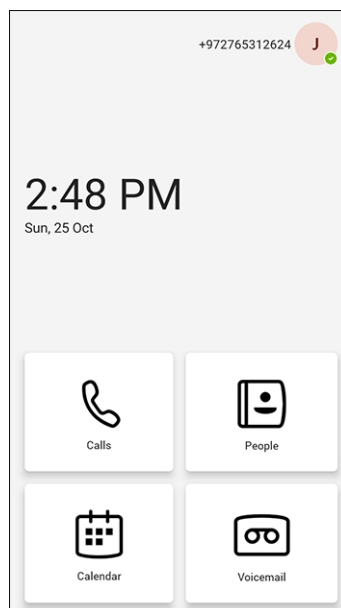
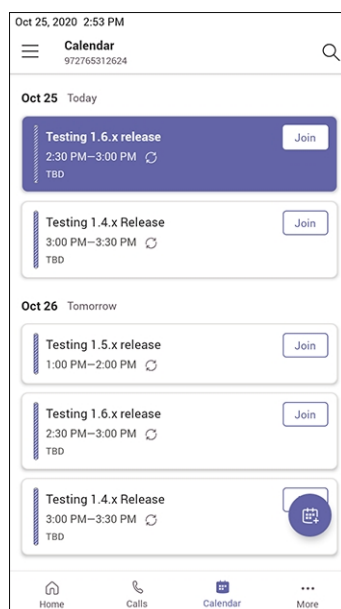
Item	Description
	<div><p>You'll need to restart the app to switch themes.</p><p>CANCEL RESTART</p></div> <p>2. Click Restart and then verify after the Teams application restarts that all screens (Teams application and Device Settings) are dark themed:</p> 
Profile	Opens the user's email address and photo / avatar picture.
Calling	Opens the Calls screen.


Item	Description
	<div data-bbox="568 259 911 864"> <p>Oct 25, 2020 5:24 PM</p> <p>← Calls Test_Test_Test_Audiocodes(R&D lab)</p> <p>Incoming calls</p> <p>Ringtone</p> <p>Calls for you Default</p> <p>Forwarded calls Default</p> <p>Delegated calls Default</p> <p>Caller ID</p> <p>Hide your phone number when dialing people who are outside of Microsoft Teams <input type="checkbox"/></p> <p>Call views</p> <p>Default view Speed dial</p> <p>Block calls</p> <p>Block calls with no caller ID <input type="checkbox"/></p> </div> <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 number, or Call group. <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.

Item	Description
Notifications	Default: On (enabled). Allows notifications to be displayed. Slide left to switch off (disable); notifications will not be displayed.
Report an issue	<p>Opens the Send Feedback screen.</p> 
About	<p>Opens the About screen.</p> 
Sign out	Lets you sign out of the phone application as one user and optionally sign in again as another user. See Signing Out on page 61 for detailed information.
Device Settings	Opens the [Device] Settings screen. See Configuring Device Settings on page 14 for detailed information.

Setting up a Meeting

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

Figure 4-9: Home**Figure 4-10: Calendar**

You can join calendered meetings and / or you can touch  to add a new event to the calendar.

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.

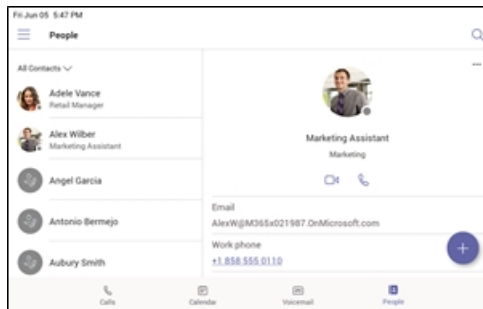
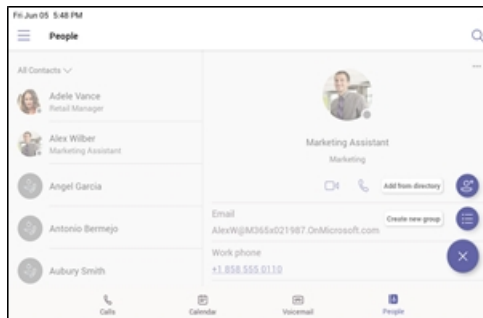
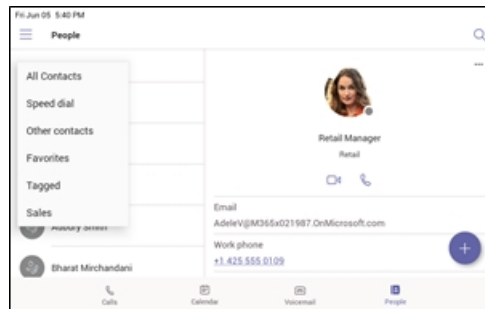
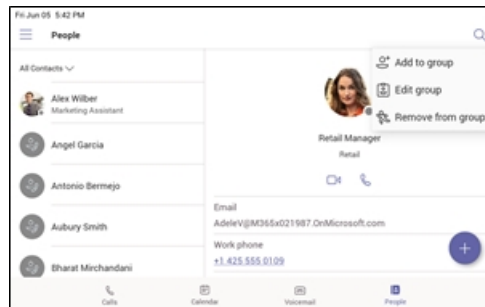
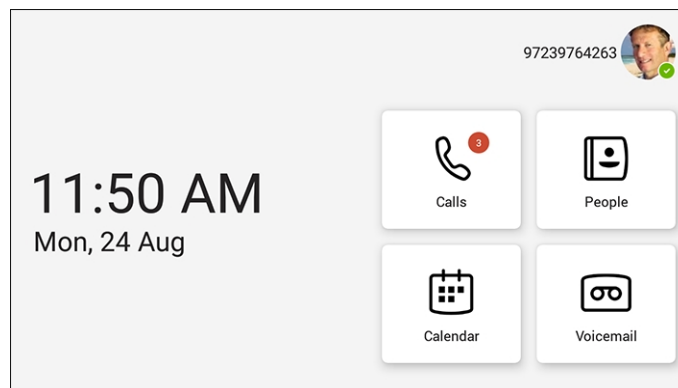
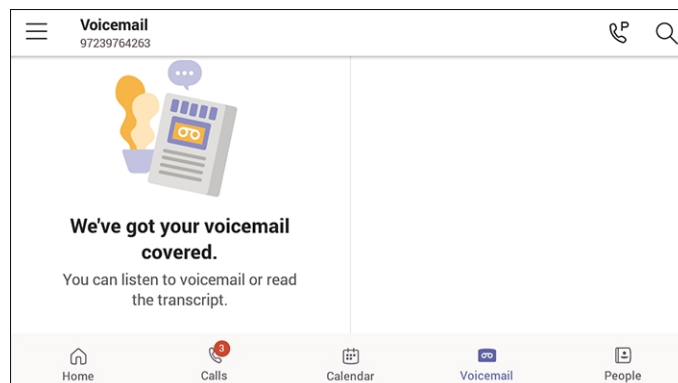
Figure 4-11: Accessing the People screen**Figure 4-12: Creating new group****Figure 4-13: Add from directory****Figure 4-14: Select a group**

Figure 4-15: Select a group**Figure 4-16: Edit group**

Accessing Voicemail

From the phone's Home screen, touch the **Voicemail** tab.

Figure 4-17: Home**Figure 4-18: Voicemail**

Using Audio Devices

You can 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.


Signing Out

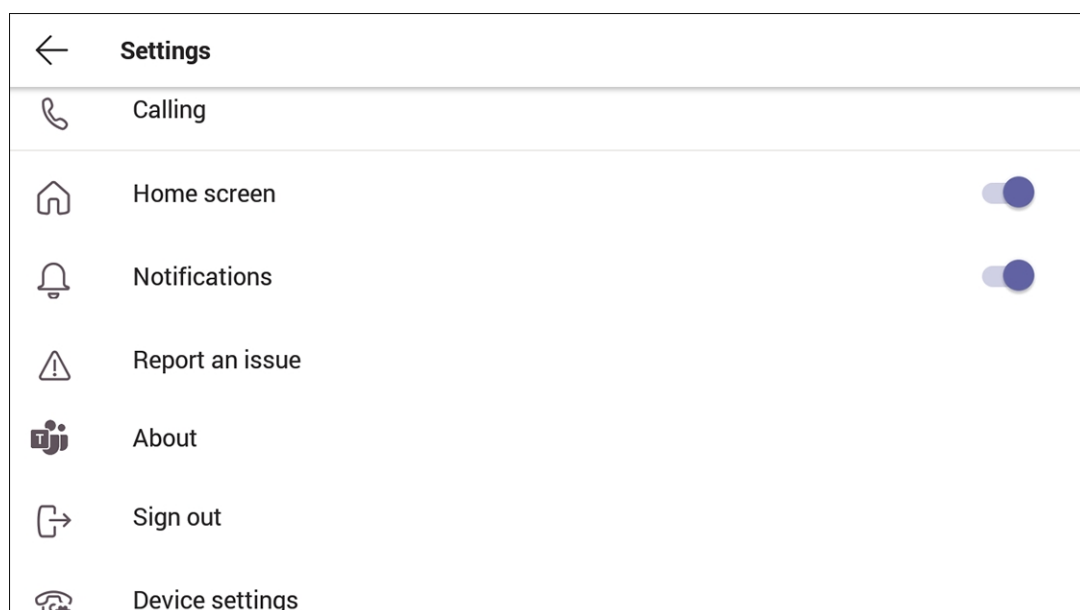
You can sign out of the phone application as one user and optionally sign in as another user.

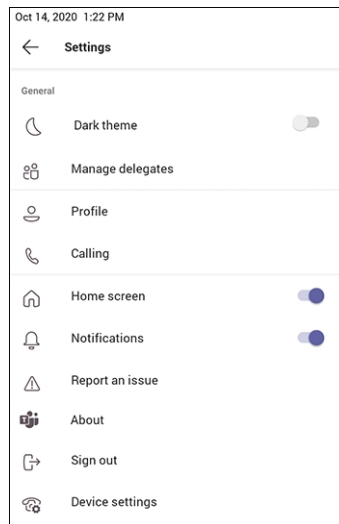
➤ To sign out:

1. In the home screen, touch the user photo / avatar picture, touch the **Settings** option and then touch the **Sign Out** option.

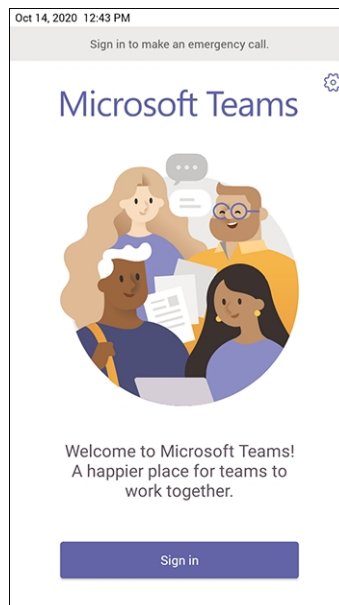


Alternatively, in the Calls screen (or People screen, Calendar screen or Voicemail screen), touch the phone menu , touch the **Settings** option.





2. Touch the **Sign Out** option; you're signed out and returned to the **Sign in** screen.

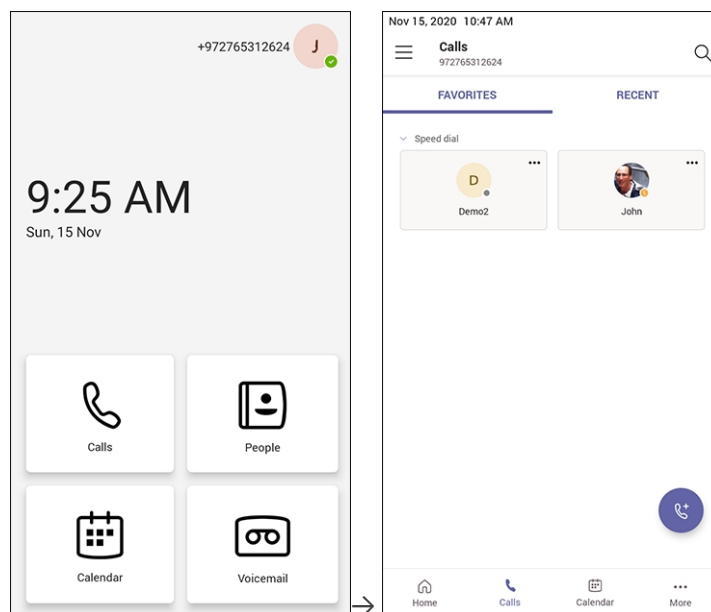


5 Performing Basic Operations

The documentation following shows basic phone operations.

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.

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:**

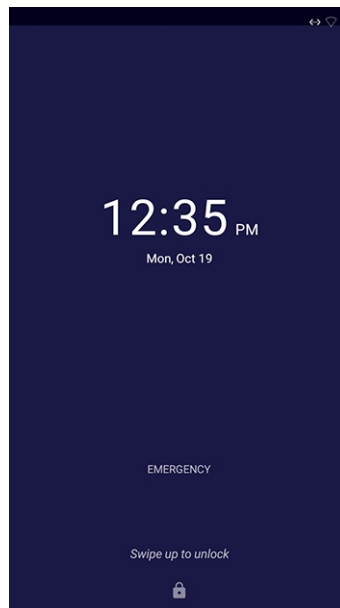
1. Touch **Calls** and then in the Calls screen under the **Recent** tab, scroll to the missed call to dial if there is more than one listed.
2. Touch  adjacent to the missed call.

Touch to Dial

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

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:**

- Touch 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 press the **EMERGENCY** key:
 - a. Dial **911**.



- b. Press the speaker button.
 - 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

Your 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- touch the headset key on the phone (make sure the headset is connected to the phone) -OR- touch the speaker key on the phone -OR- touch the **Accept** softkey (the speaker is automatically activated).

Ending an Established Call

You can end an established call.

➤ To end an established call:

- Return the handset to the phone cradle if it was used to take the call -or- touch the headset key on the phone -or- touch the speaker key on the phone -or- touch 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. Touch **Calls** and in the Calls screen touch **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.

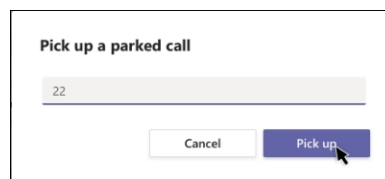
2. Touch a call in the list and then touch  to call someone back.

Parking a Call

The Teams 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 touches the call park icon  displayed in their device's Calls screen.



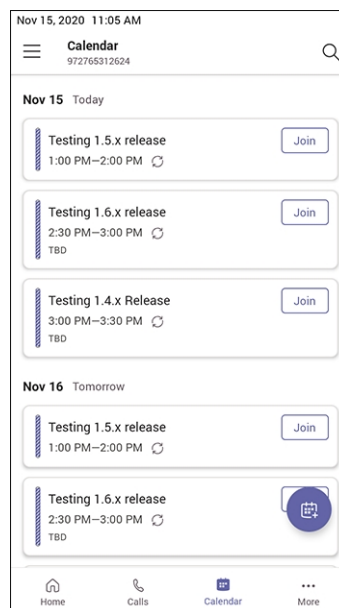
3. The user on the other device enters the code communicated to them and then touches the **Pick up** button to pick up the call.


Managing Teams Meetings

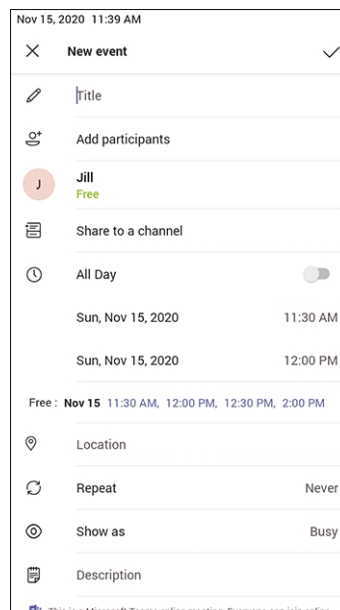
Multi-party conference meetings based on the Teams server (remote conference) can be calendered and initiated from the phone.

➤ To manage conference meetings:

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



2. Touch the  icon.



Nov 15, 2020 11:39 AM

✕ New event ✓

✎ Title

✚ Add participants

J Jill
Free

📄 Share to a channel

🕒 All Day ☐

Sun, Nov 15, 2020 11:30 AM

Sun, Nov 15, 2020 12:00 PM

Free: Nov 15 11:30 AM, 12:00 PM, 12:30 PM, 2:00 PM

📍 Location

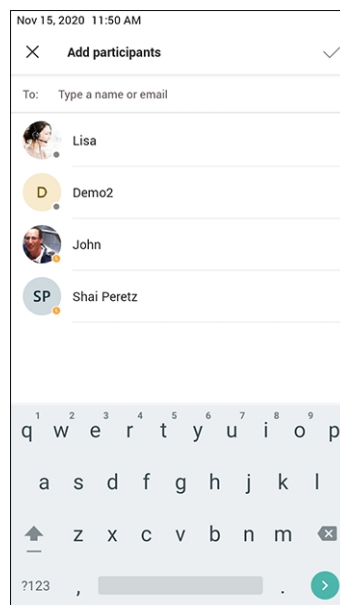
🔄 Repeat Never

👤 Show as Busy

📄 Description

🔗 This is a Microsoft Teams online meeting. Everyone can join online.

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.



Nov 15, 2020 11:50 AM

✕ Add participants ✓

To: Type a name or email

Lisa

D Demo2

John

SP Shai Peretz

1 2 3 4 5 6 7 8 9 0

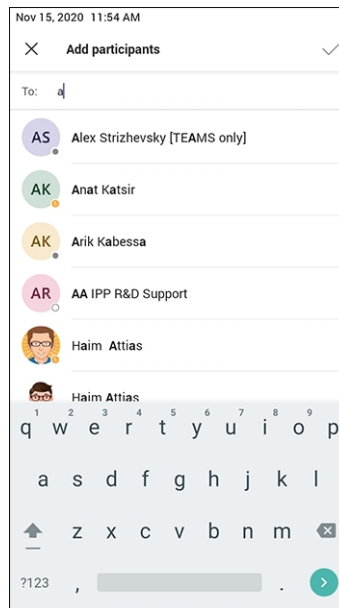
q w e r t y u i o p



a s d f g h j k l

↑ z x c v b n m ✕

?123 , . >

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 Teams phone can detect what's said in a meeting or group call and present real-time captions.

For more information, go to <https://support.microsoft.com/en-us/office/use-live-captions-in-a-teams-meeting-4be2d304-f675-4b57-8347-cbd000a21260#ID0EABAAA=Mobile>

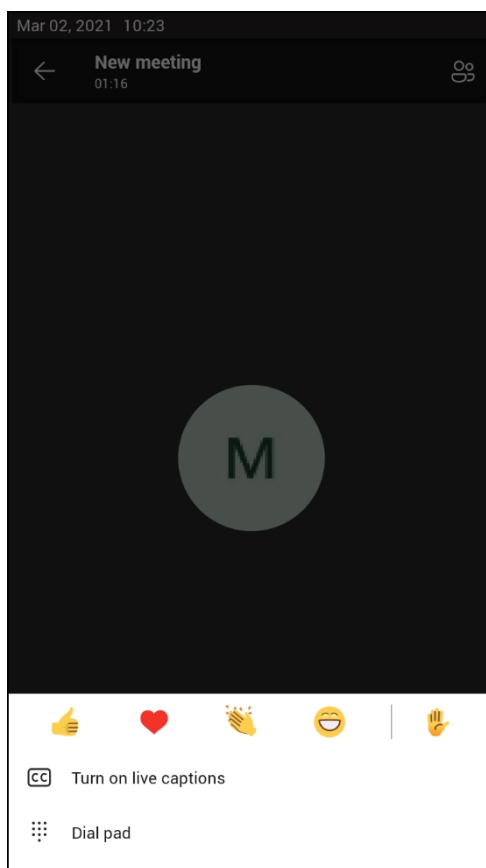
Raising a Hand During a Meeting

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 <https://support.office.com/en-us/article/raise-your-hand-in-a-teams-meeting-bb2dd8e1-e6bd-43a6-85cf-30822667b372>

Reacting During a Meeting

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



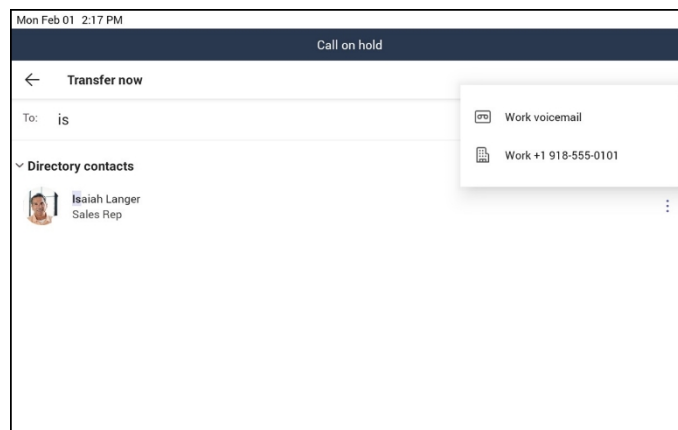
Users can convey their sentiments without hesitation or interruption to participate in the meeting, or they can raise their hands.

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 touch 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.

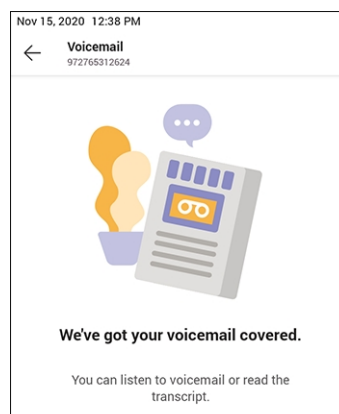


Viewing and Playing Voicemail Messages

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.

➤ To view a list of your voicemail messages:

1. In the phone's home screen, touch 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**.

For more information, see <https://support.microsoft.com/en-us/office/check-your-voicemail-in-teams-f8d568ce-7329-4fe2-a6a2-325ec2e2b419>

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, touch ; 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](#) on the next page
- [Adjusting Speaker Volume](#) on the next page
- [Adjusting Headset Volume](#) on the next page

For more information about sound and volume, see <https://support.microsoft.com/en-us/surface/surface-sound-volume-and-audio-accessories-ec517257-d98b-5a1b-1f94-a410b671a0eb>.

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, touch + 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, touch 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

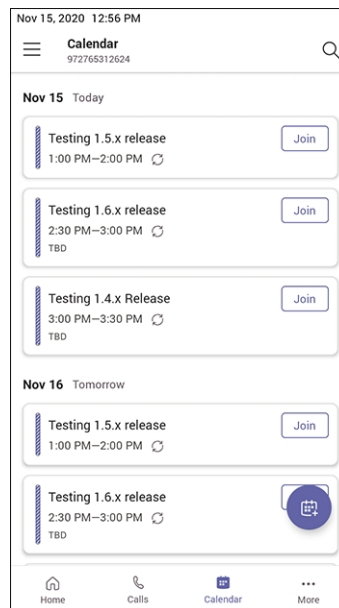
Headset volume can be adjusted *during a call* to suit personal preference.

➤ To adjust the headset volume:

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

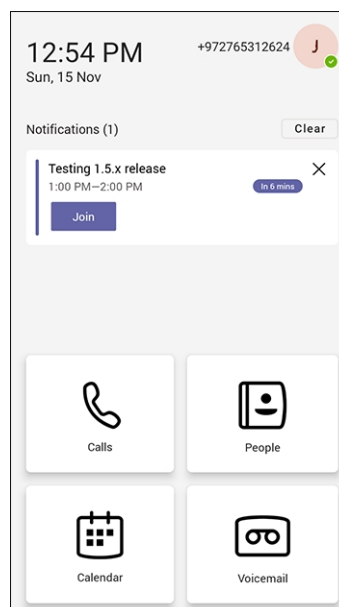
Viewing and Joining Meetings

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



➤ To view the details of a meeting:

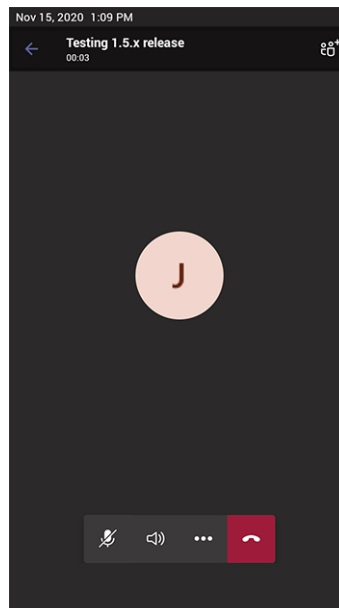
1. Scroll down if necessary to the meeting whose details you want to view and touch it.



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

➤ To join a meeting:

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



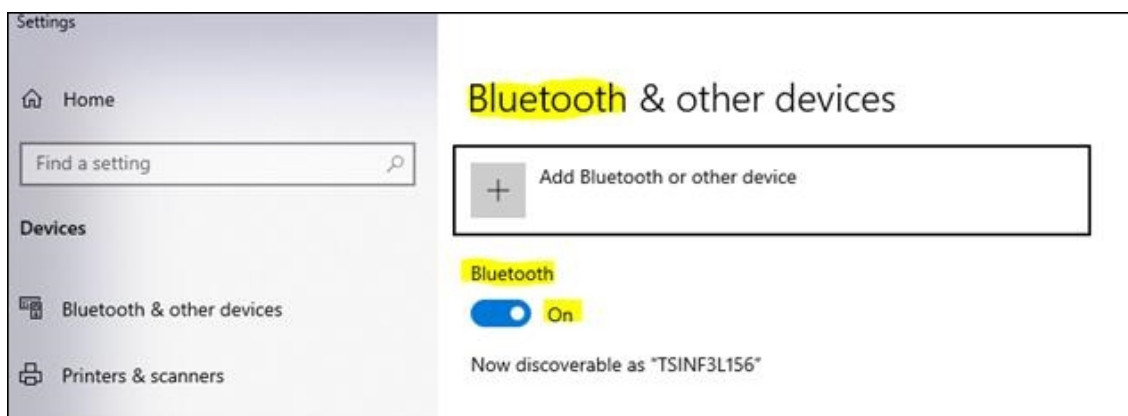
Better Together over Bluetooth

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

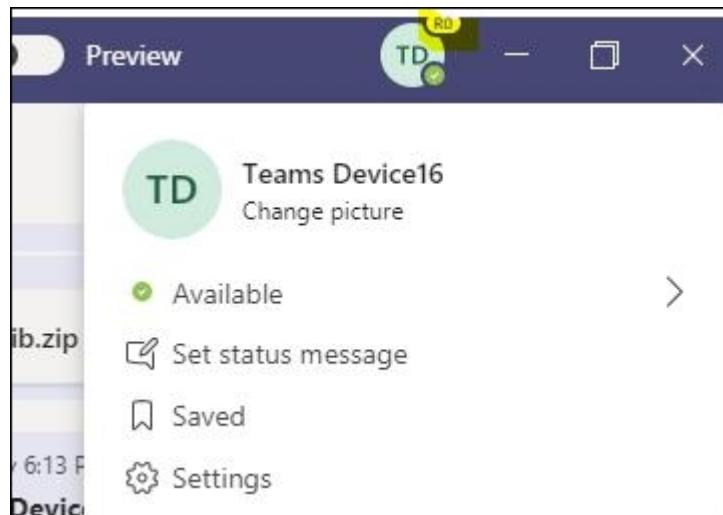
- Pairing with the Teams PC Client
- Lock/unlock synchronization
- [As a feature in preview] Use of the phone as the Teams audio device for calls / meetings

➤ To set up Bluetooth on the PC side:

1. Enable Bluetooth on your PC.

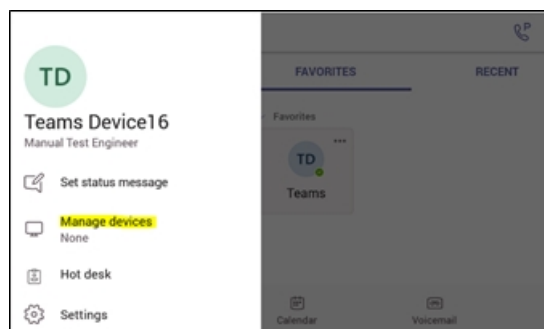


2. Install Teams PC Client on the PC.
3. Sign in to the Teams PC Client with your account (it's necessary to sign in with the same accounts to both the Teams PC Client and to the device).

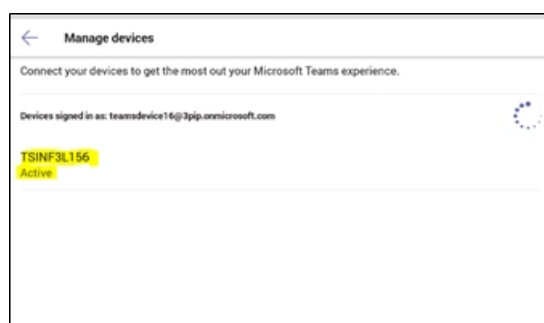


➤ **To set up Bluetooth on the device side:**

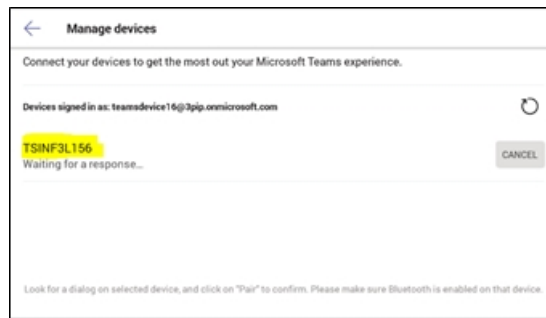
1. Sign in to the Teams application with your account (it's necessary to sign in with the same accounts to both the Teams PC Client and to the device).
2. Go to the hamburger menu on the device and click **Manage devices**.



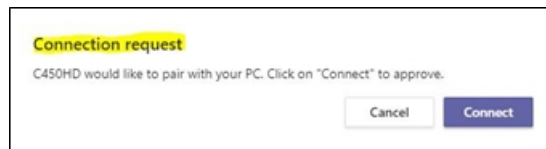
3. View the displayed available device to connect to.



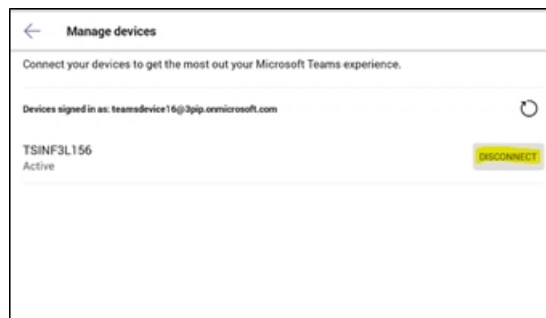
4. Pair the device with your PC.



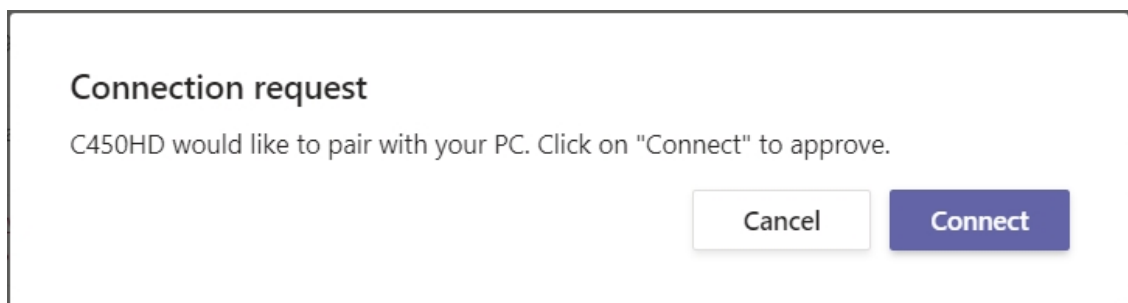
5. View on your PC a notification it gets to accept the connection:



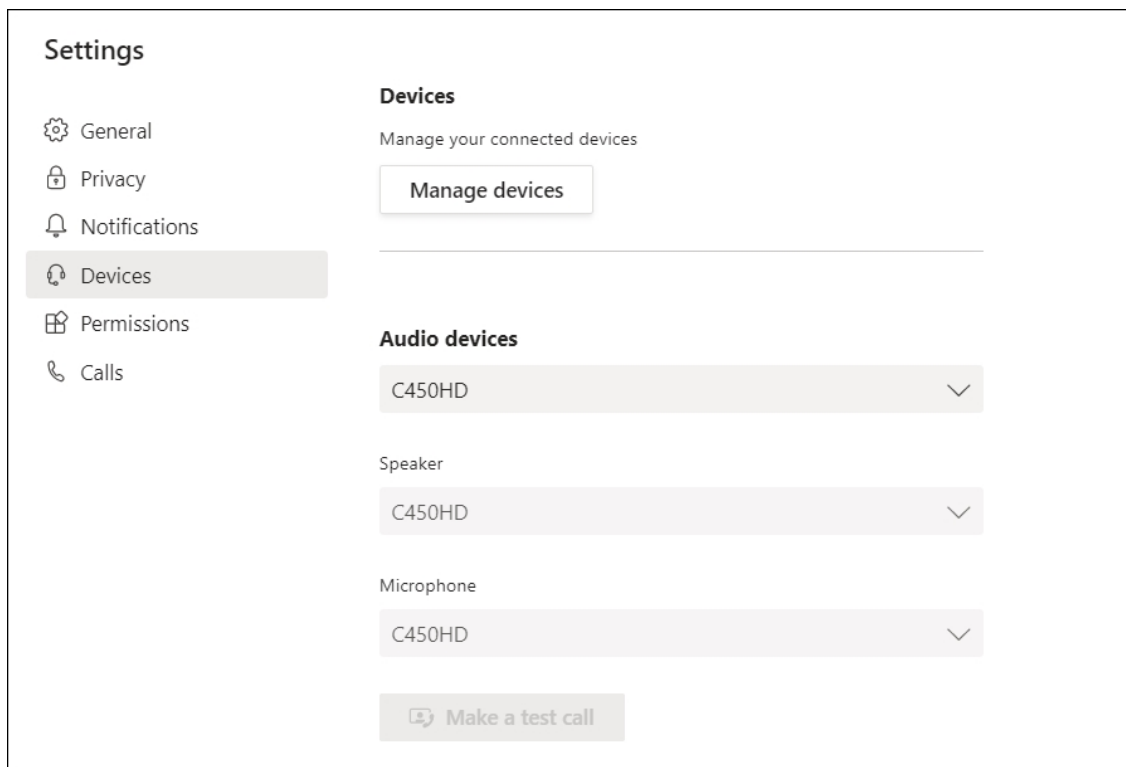
6. Accept the notification from PC.
7. Check the device and make sure pairing was successful:



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:



6 Updating Phone Firmware Manually

The phone's firmware can be upgraded manually via Secure Shell (SSH) cryptographic network protocol.

➤ **To manually upgrade firmware to firmware that does not exist in Microsoft Admin Portal:**



- Make sure you have a command line tool that implements Secure Copy Protocol (SCP).
- Place the firmware file in the same directory from which this command line tool is running.

1. Open the Command prompt.
2. Run the following command:

```
scp C470HD_TEAMS_1.8.zip admin@10.16.2.50:/data/ota_package/update_image.zip
```

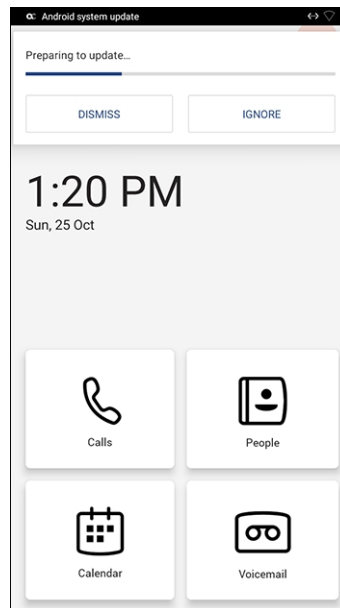


- In the preceding example, the phone's IP address is **10.16.2.50** and the firmware name is **C470HD_TEAMS_1.8.zip**
- The SCP command allows you to copy files over SSH connections.

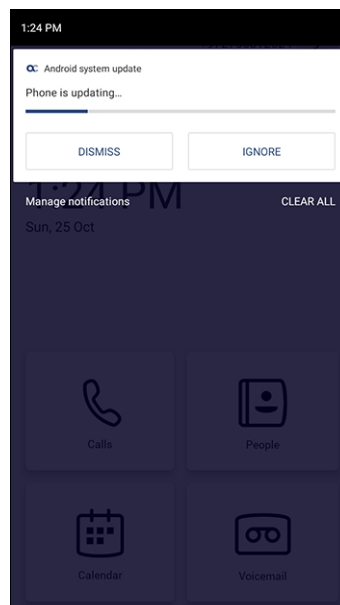
3. Choose **Yes** and enter the phone admin password (default is **1234** or **1111** if you didn't perform restore default yet); the firmware is downloaded to the phone's memory.
4. Run the following command:

```
ssh admin@10.16.2.50 local_update.sh
```

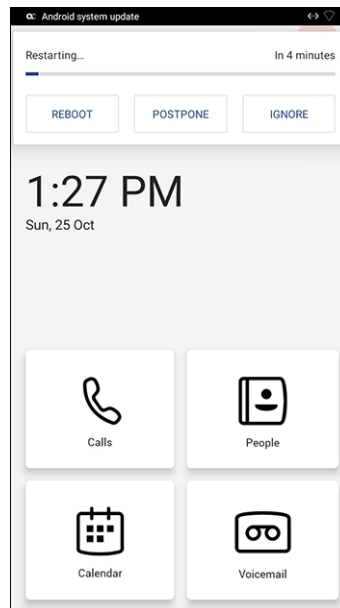
5. Enter the Admin password; the firmware is burnt to the phone and the phone is automatically rebooted.
6. View the notification that is displayed to notify you that the phone is preparing to update.



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



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



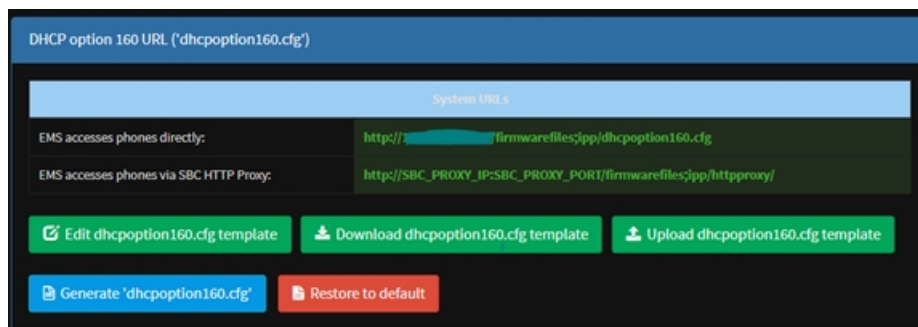
The above notification is also displayed when the phone is upgraded remotely from Microsoft Admin Portal or from AudioCodes' Device Manager.

7 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 (Pro and Express) 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 7-1: DHCP Option 160 URL



This URL is displayed in the Device Manager page under **Setup > DHCP options configuration**. After devices are added to the Device Manager, they're allocated to tenants by selecting **Change Tenant** in the 'Actions' menu. Unless already used, it's recommended to leave the default tenant as a 'lobby' for the new devices. The above URL can also be configured in AudioCodes' Redirect Server. Android-based Teams devices currently support:

- Provisioning of configuration
- Provisioning of firmware
- Switching to UC / Teams
- Monitoring (based on periodic Keep-Alive messages sent from devices)
- Resetting the device

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

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

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



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

Configuring a Periodic Provisioning Cycle

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

➤ To configure how often periodic provisioning cycles will occur:

- Use the following table as reference.

Table 7-2: Periodic Provisioning Cycle

Parameter	Description
provisioning/period/type	<p>Defines the frequency of the periodic provisioning cycle.</p> <p>Valid 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.

➤ To configure TimeZone and Daylight Savings:

- Use the following table as reference.

Table 7-3: TimeZone And Daylight Savings

Parameter	Description
date_time/- timezone	Defines the Timezone. Valid values are: <ul style="list-style-type: none"> ■ +00:00 ■ +01:00 ■ +02:00 ■ Etc.
date_time/time_ dst	[Boolean parameter]. Configuring ENABLED adds one hour to the configured time. Valid values are: <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 either via 802.1x or configuration 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 – uri to download costumer's root-ca`
- `provisioning/period/daily/time`
- `provisioning/period/hourly/hours_interval`
- `provisioning/period/type = HOURLY, DAILY (default), WEEKLY, POWERUP, EVERY5MIN, EVERY15MIN`

- provisioning/period/weekly/day
- provisioning/period/weekly/time
- provisioning/random_provisioning_time

8 Updating Microsoft Teams Devices Remotely

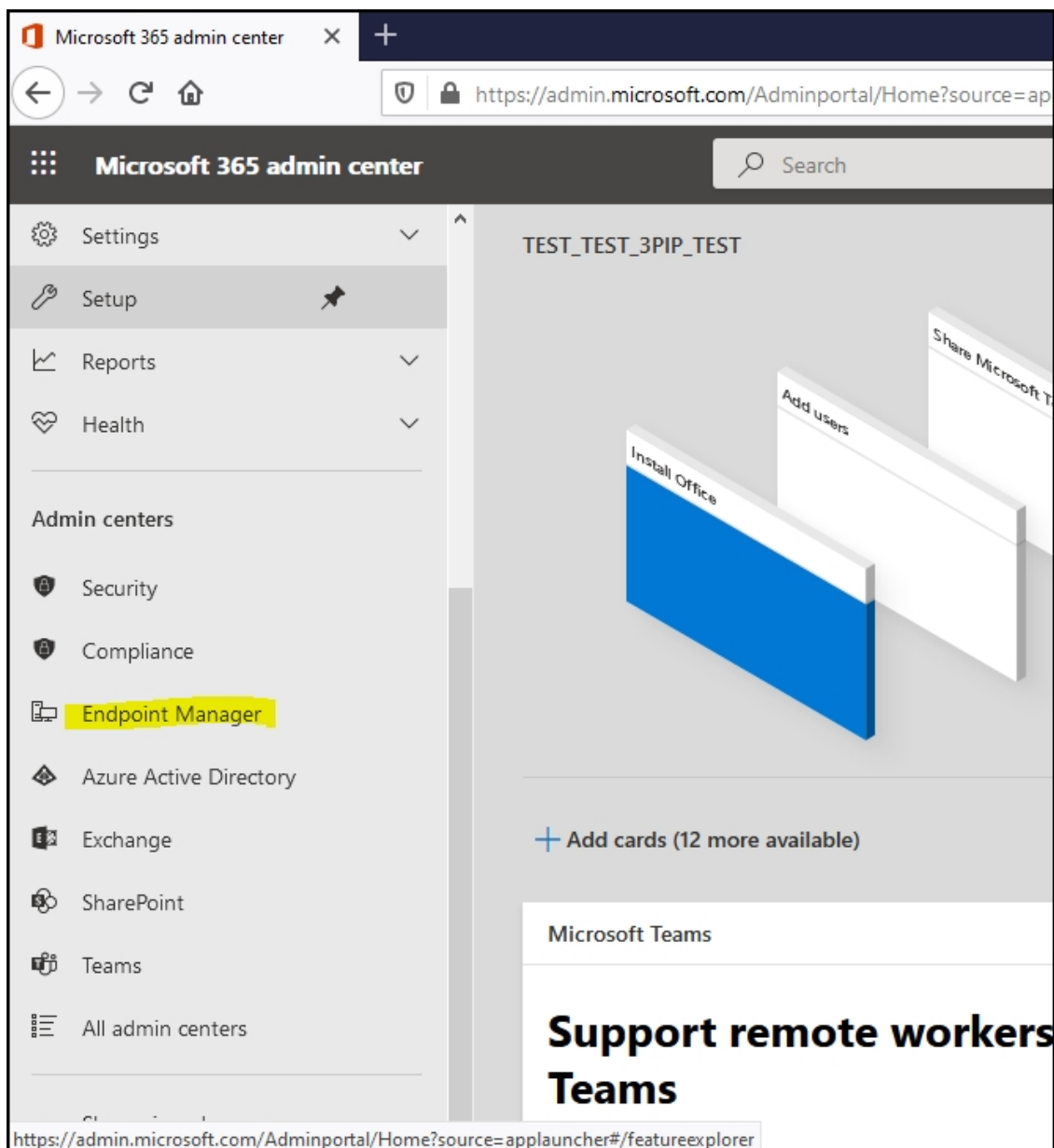
For instructions on how to update Microsoft Teams devices remotely, see <https://docs.microsoft.com/en-us/microsoftteams/devices/remote-update>.

8 Removing Devices from Intune Management

You can remove from Intune devices that are no longer needed, that are being repurposed, or that have gone missing.

➤ **To remove devices from Intune:**

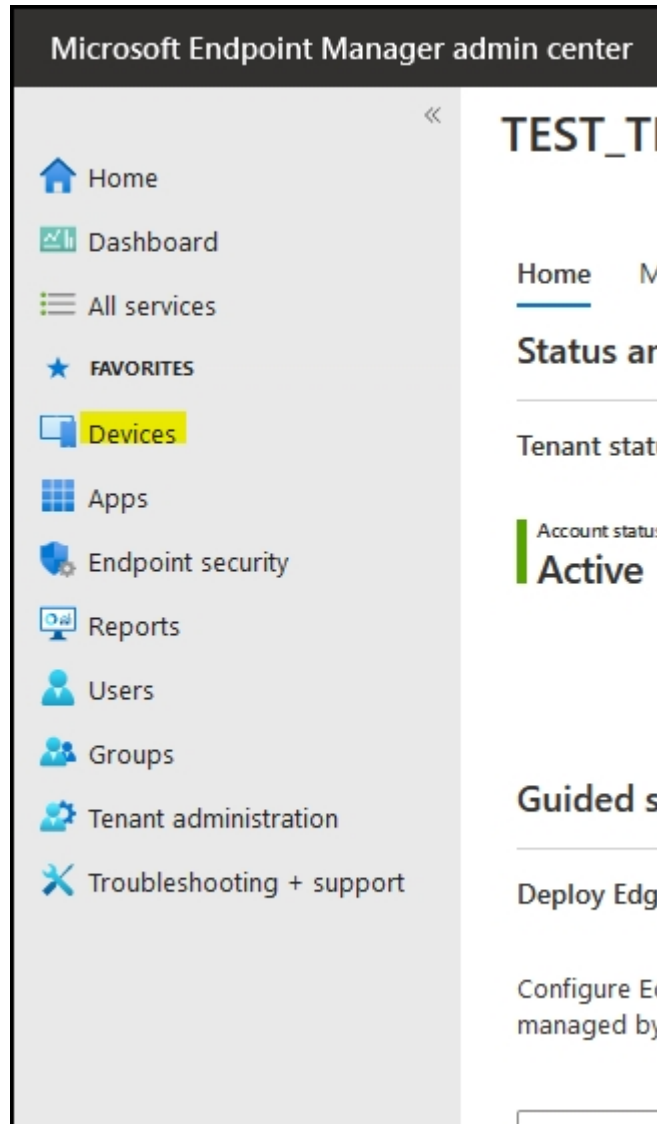
1. Go to Microsoft 365 Admin Centre [portal.office.com] and log in with an Administration account.
2. Navigate to **Endpoint Manager**.



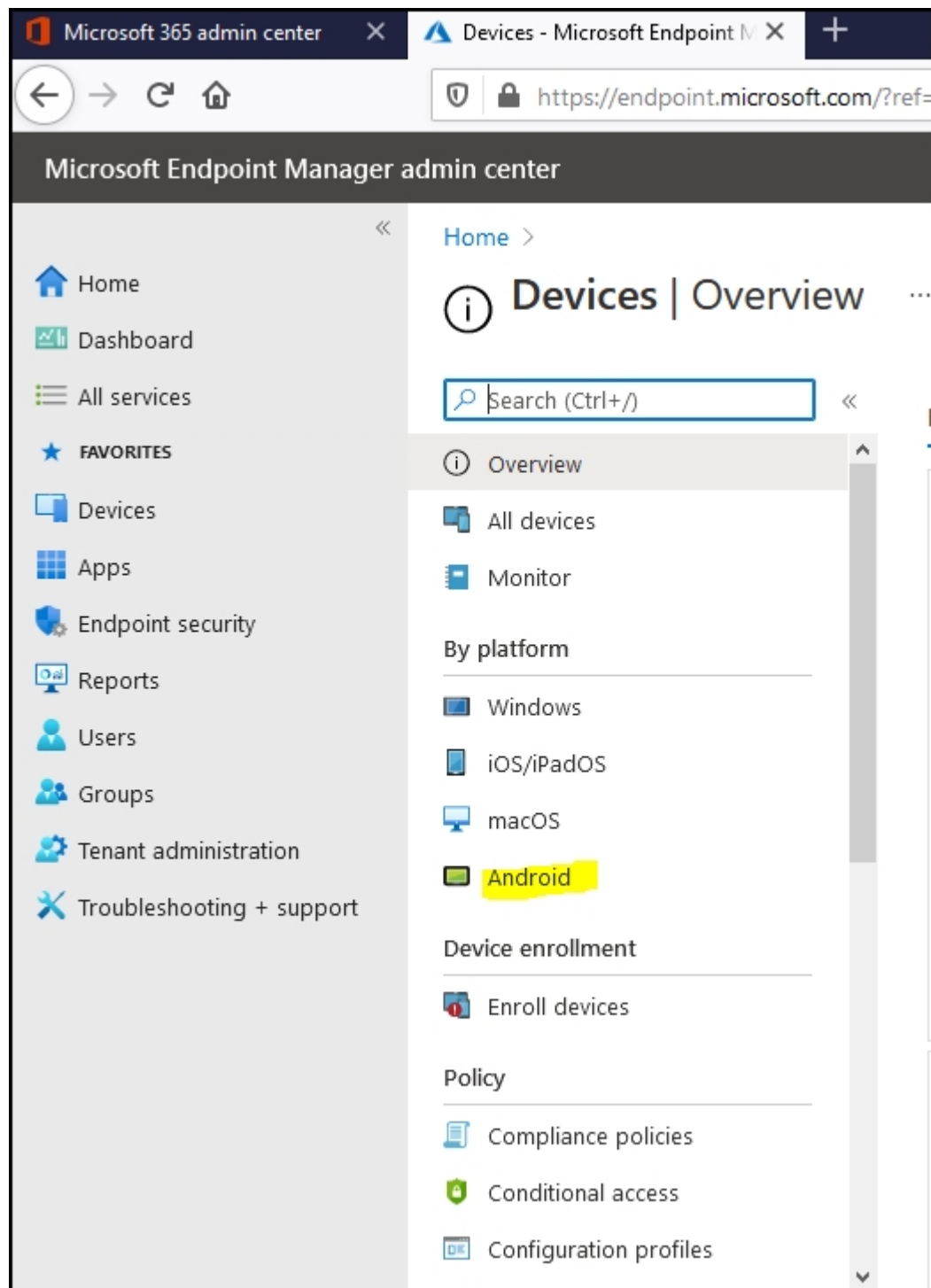


The Endpoint Manager service is licensed according to individual terms. Consequently, not all network administrators will be able to navigate to it. Check if the license you're using includes the service or not.

3. Click **Devices**.



4. Click **Android**.



5. Click **Android Devices > Bulk Device Actions**.

Microsoft Endpoint Manager admin center

Home > Devices > Android

Android | Android devices

Search (Ctrl+/) Refresh Filter Columns Export Bulk Device Actions

Overview

Android devices

Android enrollment

Android policies

Compliance policies

Configuration profiles

Filters applied: OS

Search by IMEI, serial number, email, user principal name, device name, management

Showing 1 to 25 of 427 records

Device name ↑↓	Managed by ↑↓	Ownership ↑↓	Compliance
deleteuser_Android_1...	Intune	Personal	Not Com
deleteuser_Android_1...	Intune	Personal	Not Com
deleteuser_Android_1...	Intune	Personal	Not Com
deleteuser_Android_1...	Intune	Personal	Not Com
deleteuser_Android_1...	Intune	Personal	Not Com
deleteuser_Android_1...	Intune	Personal	Not Com
deleteuser_Android_1...	Intune	Personal	Not Com
deleteuser_Android_1...	Intune	Personal	Not Com
deleteuser_Android_1...	Intune	Personal	Not Com

6. Select: **OS > Android (Device Administrator) Device Action > Delete** and then press **Next**.

Microsoft Endpoint Manager admin center

Home > Devices > Android >

Bulk device action

1 Basics 2 Devices 3 Review + create

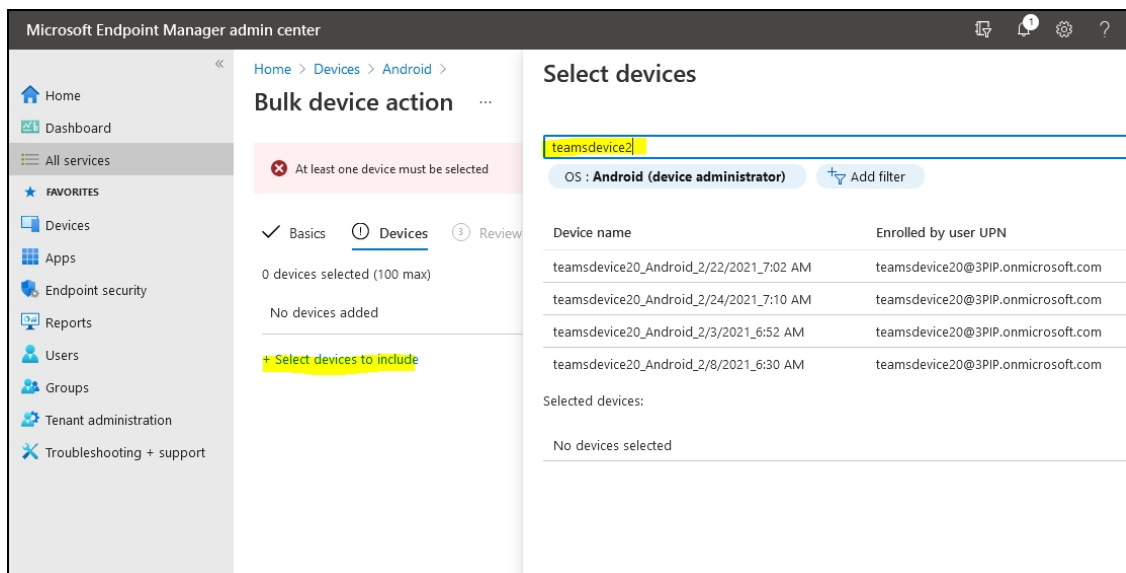
OS * Android (device administrator)

Device action * Delete

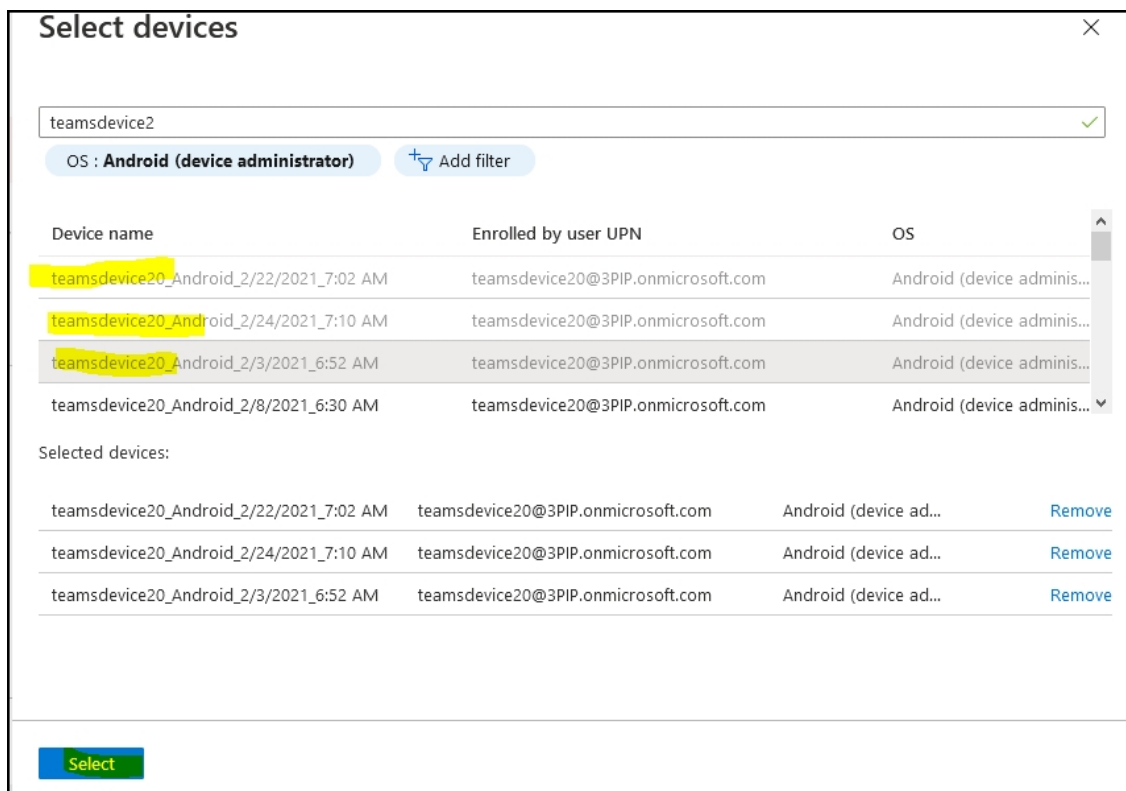
i If you delete this device, you will no longer be able to view or manage the device from the Intune portal. The device will no longer be allowed to access your company's corporate resources. Company data may be wiped from the device if the device tries to check-in after it is deleted.

Previous Next

7. Select **Devices to include** and search for the user for which enrolled devices are to be removed.



8. Select all the devices to be removed and click **Select icon**.



9. After the devices are selected, click **Next**.

Microsoft Endpoint Manager admin center

Home > Devices > Android >

Bulk device action ...

✓ Basics **2 Devices** 3 Review + create

9 devices selected (100 max)

Device name	Enrolled by user
teamsdevice20_Android_2/22/2021...	teamsdevice20@
teamsdevice20_Android_2/24/2021...	teamsdevice20@
teamsdevice20_Android_2/3/2021_...	teamsdevice20@
teamsdevice20_Android_2/8/2021_...	teamsdevice20@
teamsdevice20_Android_8/17/2020...	teamsdevice20@
teamsdevice20_Android_9/15/2020...	teamsdevice20@
teamsdevice20_Android_9/15/2020...	teamsdevice20@
teamsdevice20_Android_9/22/2020...	teamsdevice20@
teamsdevice21_Android_2/2/2021_...	teamsdevice21@

Previous **Next**

10. Click **Create**; a task to delete all the selected devices enrolled with a particular account is created.

Microsoft Endpoint Manager admin center

Home > Devices > Android >

Bulk device action

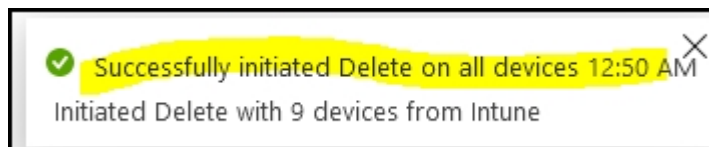
Devices

9 devices selected (100 max)

Device name	Enrolled by us
teamsdevice20_Android_2/22/2021_7:0...	teamsdevice20
teamsdevice20_Android_2/24/2021_7:1...	teamsdevice20
teamsdevice20_Android_2/3/2021_6:52 ...	teamsdevice20
teamsdevice20_Android_2/8/2021_6:30 ...	teamsdevice20
teamsdevice20_Android_8/17/2020_1:5...	teamsdevice20
teamsdevice20_Android_9/15/2020_9:0...	teamsdevice20
teamsdevice20_Android_9/15/2020_9:0...	teamsdevice20
teamsdevice20_Android_9/22/2020_5:4...	teamsdevice20
teamsdevice21_Android_2/2/2021_10:5...	teamsdevice21

Previous Create

11. Once the action is created, the admin receives notification.



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.

9 Troubleshooting

Users

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

Table 9-1: 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 74)
Touch screen display is poor	Touch 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 75).

Network Administrators

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

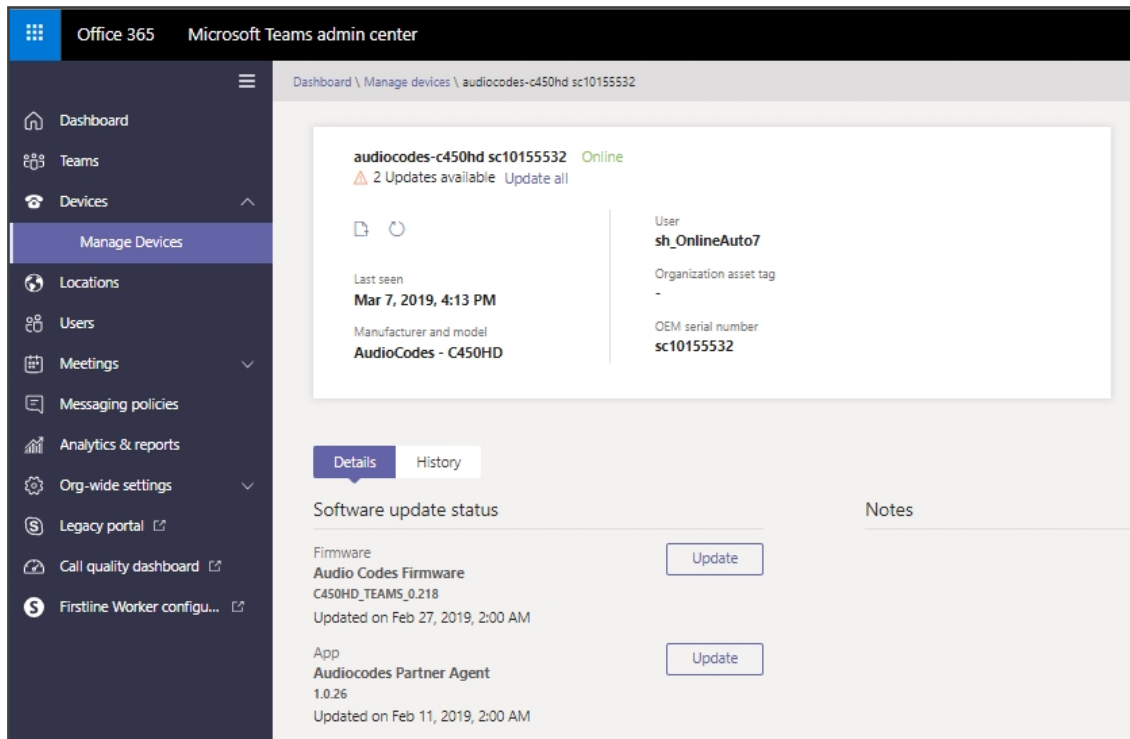
Collecting Logs

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

➤ **To collect logs:**

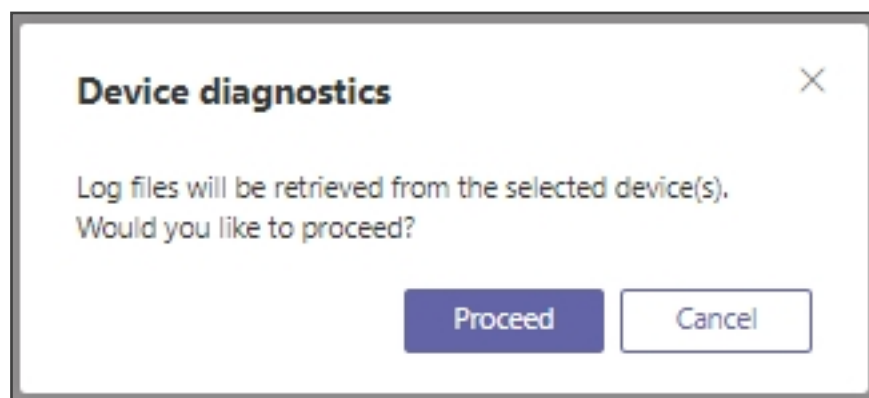
1. Reproduce the issue
2. Access Microsoft Admin Portal and under the **Devices** tab click the **Diagnostics** icon.

Figure 9-1: Microsoft Teams Admin Portal - Diagnostics

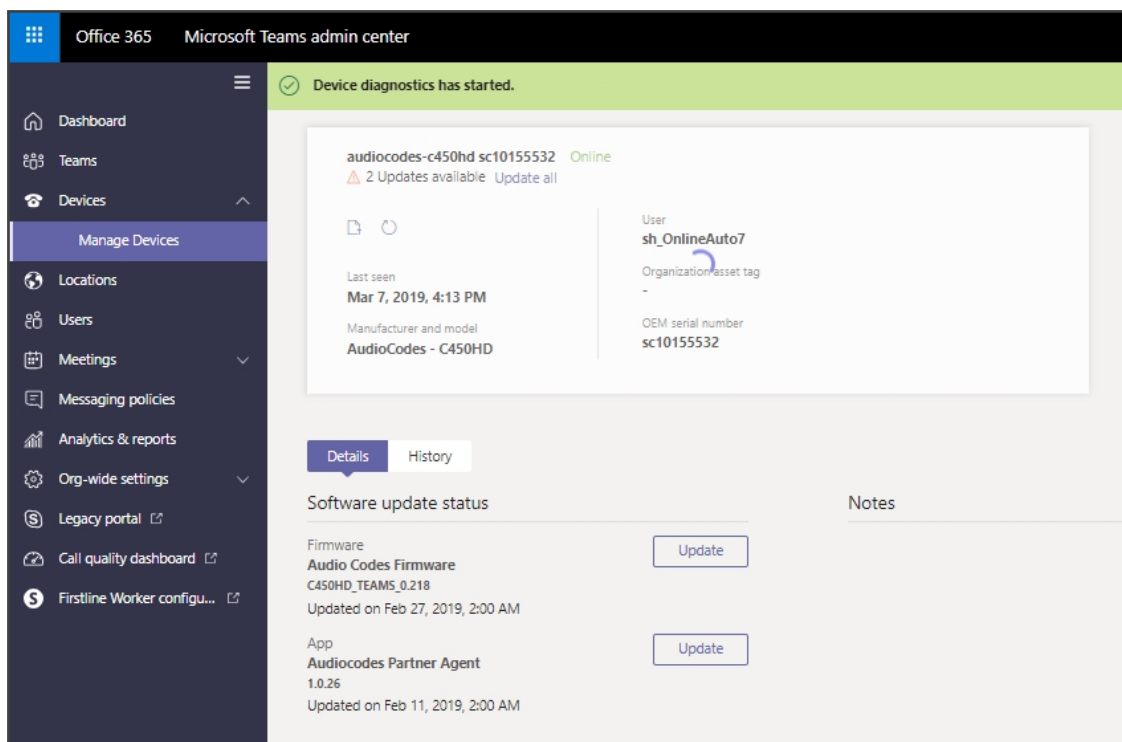


Applies to all AudioCodes phones for Microsoft Teams even though a specific model is shown in the figures here.

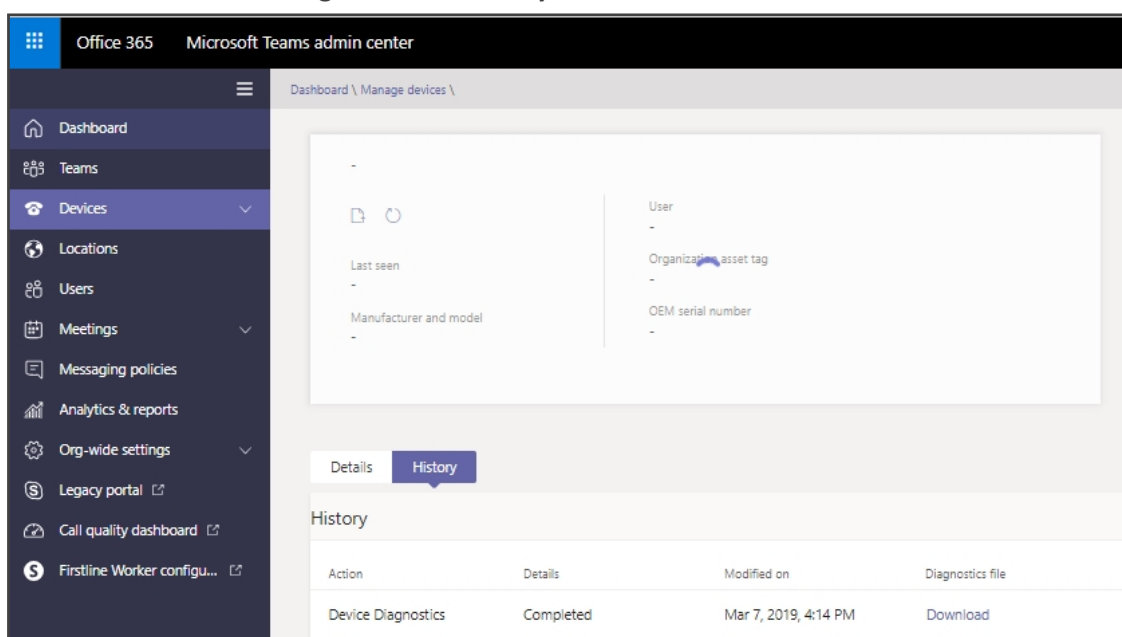
3. Click the **Diagnostics** icon .



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

Figure 9-2: Microsoft Teams Admin Portal – Logs Upload to Server

5. Click the **History** tab.

Figure 9-3: History - Download

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

Remote Logging

Remote Logging via Syslog provides the same log level as Device Diagnostics (performed via the Microsoft Admin Portal) with some additional information that may be relevant to device

issues (not Teams application issues).

Diagnostics via the Microsoft Admin Portal are saved to the device sdcard and collected after the event. Remote Logging via Syslog is different. The logs are collected in real time.

➤ **To enable from the phone Remote Logging via Syslog:**

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 ""
```

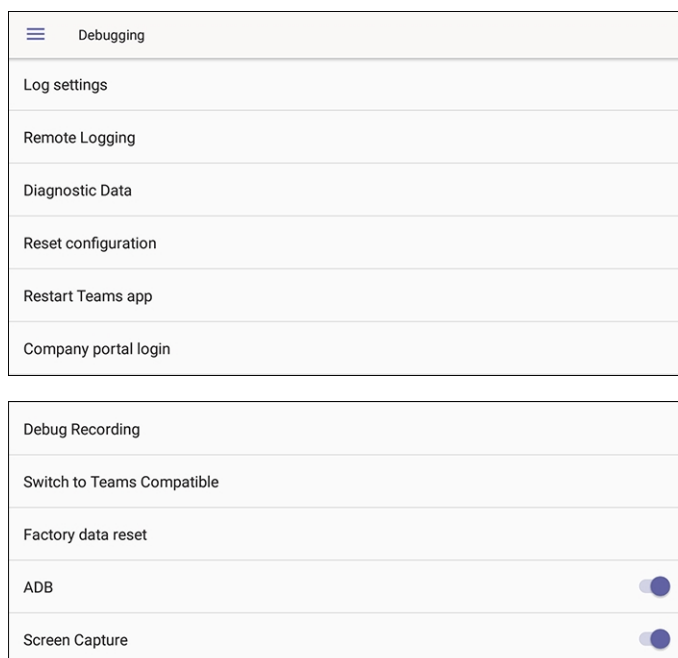
Diagnostic Data

Admin users who need to get logs from the device can dump the logs to the phone's Secure Digital (SD) Card and then later collect them using Secure Copy Protocol (SCP) based on Secure

Shell (SSH) protocol. Whenever an issue occurs, the Admin can dump the logs into the SD Card.

➤ **To use the tool:**

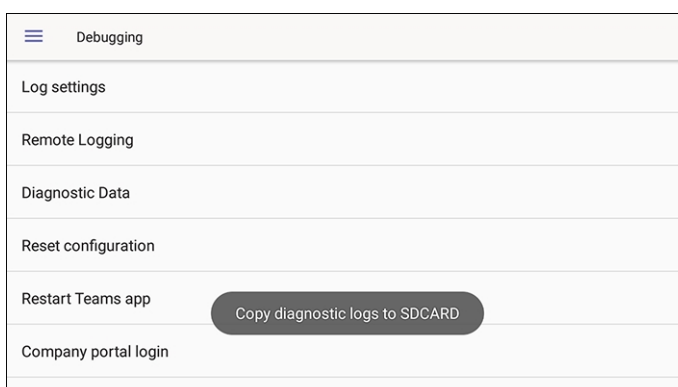
1. Log in to the phone as an Admin user
2. Open the Debugging screen (**Device Administration > Debugging**).



3. Touch the **Diagnostic Data** option.



4. Touch **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/ .
```

- Following are the relevant logs (version and ID may be different to those shown here):

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

SSH

After Administrator sign-in for which you need to know the administrator username and password **admin** and **1234** are the defaults), the phone is accessed by default via Secure Shell (SSH) cryptographic network protocol.

SSH access allows network administrators more debugging capabilities. For example:

- Pulling files from the phone sdcard (using the curl command)
- Capturing the phone screen (see [Capturing the Phone Screen](#) below for more information)
- Running the tcpdump tool (see [Running the tcpdump Tool](#) on the next page for more information)

Using SSH, network administrators can also:

- Activate DSP recording (see [Activating DSP Recording](#) on the next page for more information)
- Get the phone's IP address (see [Getting the Phone IP Address](#) on page 104 for more information)
- Get version information (see [Getting Information about Phones](#) on page 104 for more information)
- Install the Teams apk (or any other apk) (see [Installing the Teams APK \(or Any Other APK\) using SSH](#) on page 105 for more information)

Capturing the Phone Screen

This feature allows network administrators to effectively collaborate to debug issues.

➤ To capture the phone screen:

1. Access the phone via SSH
2. Run a TFTP client on your PC
3. Set the phone to the screen to capture
4. Run the commands:

- ✓ `screencap /sdcard/screen_cap.png`
- ✓ `curl -T /sdcard/screen_cap.png tftp://host_ip`

Running the tcpdump Tool

Running under the command line, this common packet analyzer allows network administrators to display TCP/IP and other packets transmitted or received over the IP telephony network.

➤ To run tcpdump:

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

```
cd /storage/emulated/0/  
mkdir recording  
cd recording/  
tcpdump -w rtp.pcap
```

2. After running TCPDump, reproduce the issue.
3. Press **Ctrl+C** to stop TCPDump:

```
curl -T /storage/emulated/0/recording/rtp.pcap tftp://host_ip/rtp.pcap
```

Activating DSP Recording

Network administrators can activate DSP recording using SSH protocol.

➤ To activate DSP recording using SSH protocol, type the following at the shell prompt:

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



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 SSH protocol.

- To deactivate DSP recording using SSH protocol, 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.

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:

```
su
```

```
ifconfig
```

Getting Information about Phones

Network administrators can get information about phones using SSH protocol.

- To get *firmware information* from a phone using SSH protocol, type the following at the shell prompt:

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

- To get *Bootloader information* using SSH protocol, type the following at the shell prompt:

```
getprop ro.bootloader
```

- To get *DSP information* using SSH protocol, type the following at the shell prompt:

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

- To get the *Microsoft Teams version* using SSH protocol, type the following at the shell prompt:

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

- To get the *Microsoft Company Portal version* using SSH protocol, type the following at the shell prompt:

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

- To get the *Microsoft Admin version* using SSH protocol, type the following at the shell prompt:

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

Installing the Teams APK (or Any Other APK) using SSH

Network administrators can install the Microsoft Teams APK (or any other APK) using SSH protocol. Here's an example of how to replace the Microsoft Teams application version.

- To replace the Microsoft Teams application version:

1. Upload the .apk file to the phone

```
curl http://<ip_address>/Microsoft-Teams-xxx.apk > /data/teams.apk
```

2. Install the .apk

```
pm install -r -d /data/teams.apk
```

3. Remove the .apk from /data

```
rm /data/teams.apk
```

Getting Company Portal Logs

Company Portal logs can be helpful to network administrators when there are issues with signing in to Teams from the phone.

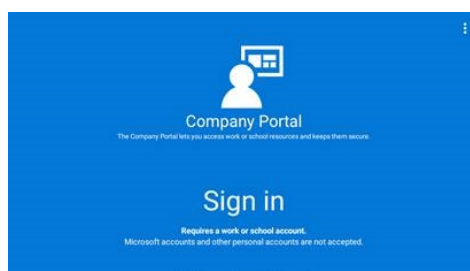
Logs can be gotten using one of two methods:

- via GUID/UUID (see [Getting Logs using UUID](#) on page 107)
- via the phone (see [Getting Logs via the Phone](#) on the next page)

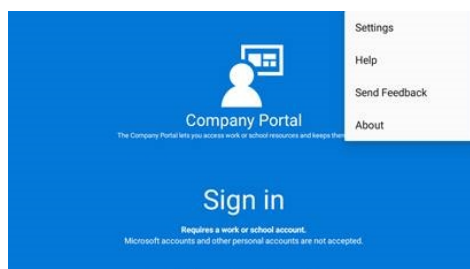
Getting Logs via the Phone

➤ To get Company Portal logs via the phone:

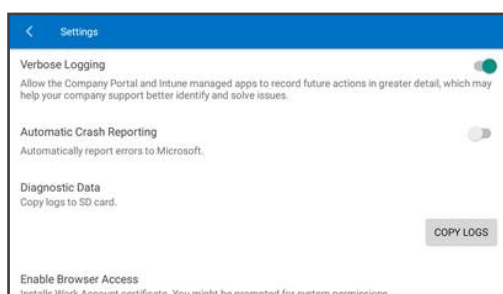
1. Reproduce the issue (logs are saved to the device so you first need to reproduce the issue and then get the logs).
2. Log in to the phone as Administrator and then go back.
3. Touch the **Debugging** option under Admin.
4. Touch **Company Portal login**.
5. Touch the icon located in the uppermost right corner of the screen, shown in the next figure:



6. Touch **Settings**.



7. Touch the **Copy Logs** key.



Company portal logs are copied to:

```
sdcard/Android/data/com.microsoft.windowsintune.companyportal/files/
```

8. To pull the logs, use the ssh:

```
scp -r admin@hosp  
ip:/sdcard/android/data/com.microsoft.windowsintune.companyportal/files/ .
```

Files are quite heavy so you may need to pull them one by one.

Getting Logs using UUID

Many different kinds of generators are available on the internet that enable you to generate a Universally Unique Identifier (UUID), a.k.a., GUID (Globally Unique Identifier), which can be used to get Company Portal logs.

➤ To get logs using a UUID generator:

1. Use an online generator such as <https://www.uuidgenerator.net/>

2. Copy the UUID number. In the example shown in the preceding figure, click **Copy** adjacent to the UUID.
3. Execute the command **adb shell** or **ssh shell**.
 - To execute the command **adb shell**, see [Getting Logs using UUID over ADB Shell](#) below
 - To execute the command **ssh**, see [Getting Logs using UUID over SSH](#) on the next page

Getting Logs using UUID over ADB Shell



To use this method of getting new logs, Android Debug Bridge (ADB), a command-line utility included with Google's Android SDK, must be installed on your PC.

➤ To execute the command **adb shell**:

1. After copying the UUID number as shown in [Getting Logs using UUID](#) above, execute the command **adb shell** as shown in the following example:

```
adb shell am broadcast -a
com.microsoft.windowsintune.companyportal.intent.action.IPPHONE_
UPLOAD_LOGS --es SessionID <Generated UUID> -n
com.microsoft.windowsintune.companyportal/.omadm.IPPhoneReceiver
```

2. Replace **<Generated UUID>** with the number that you copied, for example:

```
adb shell am broadcast -a
com.microsoft.windowsintune.companyportal.intent.action.IPPHONE_
UPLOAD_LOGS --es SessionID <0d23126e-0e2f-4b5b-92de-f07521f92e48>
-n com.microsoft.windowsintune.companyportal/.omadm.IPPhoneReceiver
```

3. After running the command, the logs are saved in 'Intune', Microsoft's cloud-based service for mobile device management (MDM) and mobile application management (MAM).
4. Send AudioCodes the UUID number.

Getting Logs using UUID over SSH

SSH (Secure Shell) cryptographic network protocol can also be used to secure getting Company Portal logs via UUID.

➤ To execute the command **ssh**:

1. After copying the UUID number as shown in [Getting Logs using UUID](#) on the previous page, execute the command **ssh** as shown in the following example:

```
am broadcast -a
com.microsoft.windowsintune.companyportal.intent.action.IPPHONE_
UPLOAD_LOGS --es SessionID <Generated GUID> -n
com.microsoft.windowsintune.companyportal/.omadm.IPPhoneReceiver
```

2. Replace **<Generated UUID>** with the number that you copied, for example:

```
am broadcast -a
com.microsoft.windowsintune.companyportal.intent.action.IPPHONE_
UPLOAD_LOGS --es SessionID <0d23126e-0e2f-4b5b-92de-f07521f92e48>
-n com.microsoft.windowsintune.companyportal/.omadm.IPPhoneReceiver
```

3. After running the command, the logs are saved in 'Intune', Microsoft's cloud-based service for mobile device management (MDM) and mobile application management (MAM).
4. Send AudioCodes the UUID number.

Getting Audio Debug Recording Logs

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

➤ To enable Audio Debug Recording logs:

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



3. Touch **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.
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/ .
```

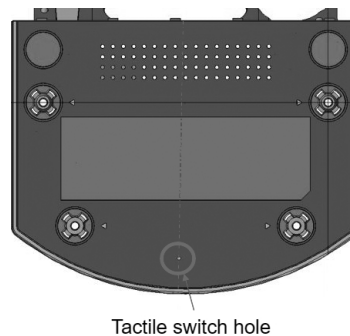
Manually Performing Recovery Operations



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. Note too that the 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 for Microsoft Teams 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.



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

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

Following are the recovery operation options using the reset key on the C470HD:

- Enter recovery mode - Long-press the reset key for 4 seconds or simultaneously press the 'back' key + the MENU key; the device's LED lights up red.
- Switch to the other slot - Long-press the reset key for 10 seconds or simultaneously press the '4' key + the '6' key; the device's LED lights up green.
- Enter the device's boot - Long-press the reset key for 15 seconds or simultaneously press the '1' key + the '3' key; the device's LED lights up yellow.
- Restore the phone to its default settings - Long-press the reset key for 25 seconds or simultaneously press the OK key + the MENU key; the device's LED lights up green + yellow.

You can also restore a device to its default settings while the phone is already powered up and functioning, by long-pressing the HOLD key for 15 seconds.

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.

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

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

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

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

©2021 AudioCodes Ltd. All rights reserved. AudioCodes, AC, HD VoIP, HD VoIP Sounds Better, IPmedia, Mediant, MediaPack, What's Inside Matters, OSN, SmartTAP, User Management Pack, VMAS, VoIPerfect, VoIPerfectHD, Your Gateway To VoIP, 3GX, VocaNom, AudioCodes One Voice, AudioCodes Meeting Insights, AudioCodes Room Experience and CloudBond are trademarks or registered trademarks of AudioCodes Limited. All other products or trademarks are property of their respective owners. Product specifications are subject to change without notice.

Document #: LTRT-13286

