User's and Administrator's Manual

AudioCodes 400HD IP Phone Series

C470HD IP Phone

Microsoft Teams Application

Version 1.17

audiocodes

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: August-10-2022

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
Device Manager Administrator's Manual

Document Name
Device Manager Deployment Guide
https://docs.microsoft.com/en-us/MicrosoftTeams/phones-for-teams

Table of Contents

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)

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

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

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

Specifications

The following table summarizes the phone's software specifications.

Table 1-1: Software Specifications

Feature	Details
Media Processing	■ Voice Coders: G.711, G.729, G.722, SILK, Opus ■ Acoustic Echo Cancelation: G.168-2004 compliant, 64-msec tail length

Feature	Details
	■ Adaptive Jitter Buffer ■ Voice Activity Detection ■ Comfort Noise Generation ■ Packet Lost Concealment ■ RTP/RTCP Packetization (RFC 3550, RFC 3551), SRTP (RFC 3711)
Microsoft Teams phones feature set	■ Authentication (Sign in with user credentials; Sign in using PC/Smartphone; Modern Authentication; Phone lock/unlock) ■ Calling (Incoming/Outgoing P2P calls; In-call controls via UI (Mute, hold/resume, transfer, end call); PSTN calls; Visual Voicemail; 911 support ■ Calendar and Presence (roadmap feature) (Calendar Access and Meeting Details; Presence Integration; Exchange Calendar Integration; Contact Picture Integration; Corporate Directory Access) ■ Meetings (roadmap feature) (One-click Join for Meetings; Join Skype for Business meetings; Meeting Call controls [Mute/unmute, hold/resume, hang up, add/remove participant]; Meeting Details. See also here for related Microsoft documentation.
Configuration and Management	■ Teams admin center (TAC) ■ OVOC / Device Manager
Debugging Tools	■ AudioCodes' Teams IP Phone Utility (see Teams IP Phone Utility on page 99) ■ Log upload to Microsoft server (certification for 3rd party Skype for Business clients) ■ Remote logging via Syslog ■ SSH Access ■ Capturing the phone screen ■ TCPdump ■ Audio Debug recording logs ■ Echo Canceler (EC) debug recording ■ Media logs (*.blog) ■ Remote Packet Capture network sniffer application

Feature	Details
Localization Support	■ Multi-lingual support; the language pack list is not yet final and is subject to modification.
Hardware	■ Graphical portrait 5.5" color touch screen, 1280 x 720 resolution, with multi-lingual support ■ Wired connectivity: ✓ Two RJ-45 [Gigabit Ethernet (GbE)] (10/100/1000BaseT Ethernet) ports: LAN and PC port ✓ USB port for USB headset. Note that **C435HD-R** (**TEAMS-C435HD-R**) is a PoE Class 2 device (also when connecting a standard USB headset). If used with a loud USB speakerphone, an external power supply must be used. For more information, contact AudioCodes. ✓ RJ-11 interface ✓ Survivable Branch Appliance (SBA) ■ Wireless connectivity: ✓ Dual band 2.4GHz/5GHz, 802.11b/g/n Wi-Fi support ✓ Wi-Fi supported protocols: WEP, WPA-PSK/WPA2-PSK and WPA/WPA2 Enterprise (802.1X) PEAP only ■ Bluetooth support; integrated; optional ■ Power: ✓ DC jack adapter 12V ✓ Power supply AC 100 ~ 240V ✓ PoE Class 2: IEEE802.3af (optional) ■ Keys: ✓ Hold ✓ Mute ✓ Transfer ✓ Volume ✓ Headset (including LED) ✓ Speaker (including LED) ✓ Back ✓ Home

Allowing URLs, Ports (Security)

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

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

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

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

Security Guidelines for Android-based Native Teams Devices

AudioCodes' Android-based Native Teams devices are purpose-built and customized for Microsoft Teams calling and meeting. Customers might perceive Android-based products as vulnerable to security issues but security is *less* of an issue on devices purpose-built and customized for Microsoft Teams calling and meeting. Security is in fact *enhanced* on these devices *as part of their default use*.

When analyzing device security, two levels must be addressed:

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

AudioCodes recommends the following:

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

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

- Overview of security and compliance - Microsoft Teams | Microsoft Docs
- Identity models and authentication for Microsoft Teams - Microsoft Teams | Microsoft Docs
- Sign in to Microsoft Teams - Microsoft Teams | Microsoft Docs

Android-Level Security Hardening

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

- See Google Play Services on the next page
- See Running Android in Kiosk Mode on the next page
- See Screen Lock on the next page
- See AudioCodes Private Key on the next page
- See Android Debug Bridge (ADB) on the next page
- See App Signing on page 7
- See Web Browser on page 7
- See Remote Configuration Management on page 7
- See AudioCodes Device Manager Validation on page 7
- See Sandboxing on page 7
- See Device File System on page 8
- See Keystore on page 8
- See Device Certificate on page 8
- See Data Protection on page 8
- See Debugging Interface on page 8
- See SSH Access: Reduced File System
- See Android Security Updates on page 9

Google Play Services

Goggle Play services were removed from the AudioCodes Native Teams device software. Access to any Google store or Play service is not allowed.

- Updating the AudioCodes Native Teams 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 AudioCodes Native Teams device will only run those specific approved apps and this cannot be changed in run time (only with a new software code provided by AudioCodes).

Screen Lock

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

AudioCodes Private Key

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

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

Android Debug Bridge (ADB)

⚠ The device does not allow access to ADB.

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

App Signing

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

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

Web Browser

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

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

Remote Configuration Management

AudioCodes 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 AudioCodes Native Teams devices 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 on page 9.
- 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.

Sandboxing

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

Device File System

The AudioCodes Native Teams device's file system is encrypted on C470HDdevices. Customers may enforce a policy of device encryption via Microsoft's cloud-based Intune service.

Keystore

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

Device Certificate

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

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

Data Protection

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

Debugging Interface

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

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

SSH Access: Reduced File System Privileges

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

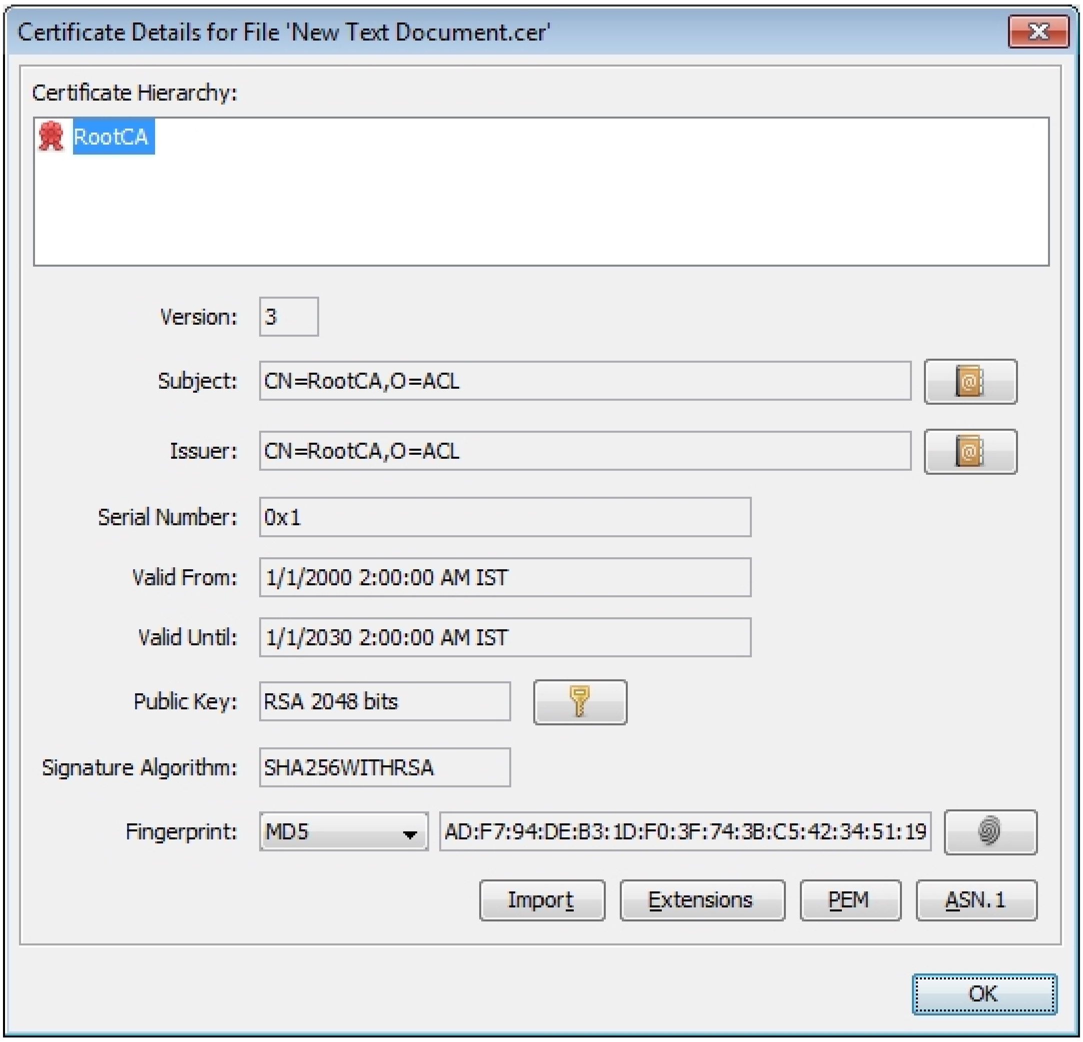
Android Security Updates

AudioCodes regularly adopts and integrates Android security updates.

For reference, see here.

AudioCodes Root CA Certificate

The following figure shows the AudioCodes Root CA Certificate.



Version: 3

Subject: CN=RootCA,O=ACL

Issuer: CN=RootCA,O=ACL

Serial Number: 0x1

Valid From: 1/1/2000 2:00:00 AM IST

Valid Until: 1/1/2030 2:00:00 AM IST

Public Key: RSA 2048 bits

Signature Algorithm: SHA256WITHRSA

Fingerprint: MD5 AD:F7:94:DE:B3:1D:F0:3F:74:3B:C5:42:34:51:19

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

MIIDMTCCAhmgAwIBAgIBATANBgkqhkiG9w0BAQsFADAfMQwwCgYDVQQKE
wNBQ0wx

```
DzANBgNVBAMTBlJvb3RDQTAeFw0wMDAxMDEwMDAwMDBaFw0zMDAxMD
EwMDAwMDBa

MB8xDDAKBgNVBAoTA0FDTDEPMA0GA1UEAxMGUm9vdENBMIIBIjANBgkqh
kiG9w0B

AQEFAAOCAQ8AMIIBCgKCAQEA6GK495KUCXAm/UE17G4/cjnZN4LNaxYEYz
bfZL0a

EhgSKYt/LQ+iUcDhojsneusNgrcGkpwKkIKsGsvGWmSRNULV01CW+TX2VJN7
3+hh
V0uzhyOIYAUhbDaoqNM6Kp5b7sJ1ew4Ig9kfd/ma9CzI5koESLIw/inLj/r+rD96

mUcPEIWrKspv7Qy4I14fsK/yMArixRopTL1munVVPpSFM9Jh8IY3JHyr5CQJXKK
s
EhGAJsnHaRqsR2Su3X/WtsIgEF+cvP34pxhIhFL29nMfnaFATSS3rgGaFISvI1ZS

esLMqkWjp9cqGYrvt7K61sYnvMMb+o/KbWqVokXb+Fr7bwIDAQABo3gwdjAMB
gNV

HRMEBTADAQH/MB0GA1UdDgQWBBQDXySn9hz15lDraZ+iXddZGReB+zBHB
gNVHSME

QDA+gBQDXySn9hz15lDraZ+iXddZGReB+6EjpCEwHzEMMAoGA1UEChMDQU
NMMQ8w

DQYDVQQDEwZSb290Q0GCAQEwDQYJKoZIhvcNAQELBQADggEBAI0rUywo
mmWWJnH3

JOfKiS3+VnX5hJITZymvWanMXUz/6FonHccPXEBYTrUYwhiWx3dwELAFXDFK
kxMp

0KKWZ4F39cAOLRjqhzya+xUeeJ9HQZCXYAJ6XgvTfN2BtyZk9Ma8WG+H1hNv
vTZY

QLbWsjQdu4eFniEufeYDke1jQ6800LwMIFIc59hMQCeJTenRx4HdJbJV86k1gBU
E

A7fJT1ePrRnXNDRz6QtADWoX3OmN7Meqen/roTwvLpEP22nYwvB28dq3JetIQ
Kwu
XC4gwI/o8K2wo3pySLU9Y/vanxXCr0/en5I3RDz1YpYWmQwHA8jJIu8rxdhr+VNQ
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

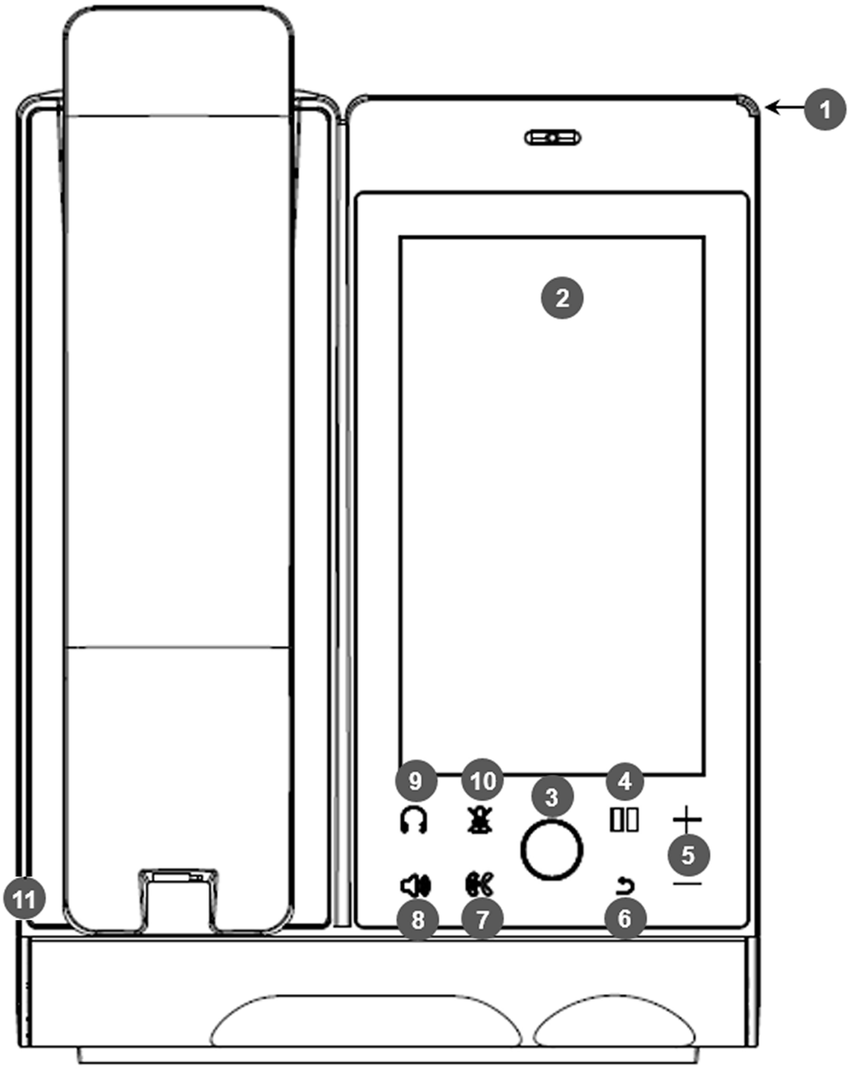
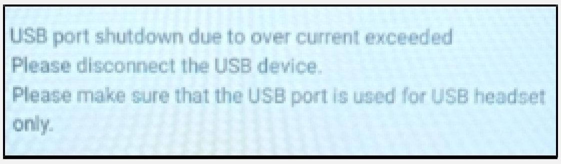


Table 2-1: Font View Description

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

Item #	Label/Name	Description
		- Flashing red: Incoming call (ringing) - Red: Answered call
2	TFT touch screen	Thin Film Transistor touch screen, a type of LCD (Liquid Crystal Display) interactive screen which displays calling information and lets you configure phone features by touching the glass.
3	Home	- Touch the key to return to the phone's home (idle) screen from any screen. - Long-press the key to open the device Settings screen. - Visual indications: ✓ If the key is illuminated red (constantly, without flashing), it indicates ‘No network’; touching the key then gives the user direct access to the Network menu. ✓ Flashing red indicates a system alert, for example, when a user tries to charge via the device’s USB port (see the note after this table). ✓ Flashing yellow indicates that the phone is in the process of a software upgrade.
4	Hold	Touch to place an active call on hold.
5	Volume	Increases or decreases the volume of the handset, headset, speaker, ring tone or call progress tones. See Adjusting Volume on page 72 for detailed information.
6	'Back' key	Touch to return to the previous screen.
7	Call transfer	Touch to transfer a call to a third party.
8	Speaker	Touch to activate the speaker, allowing a hands-free conversation.
9	Headset	Touch to activate a call using an external headset.
10	Mute	Touch to mute an established call.
11	USB port	For a USB headset. See also the note below.

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



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

Rear View

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

Figure 2-2: Rear View

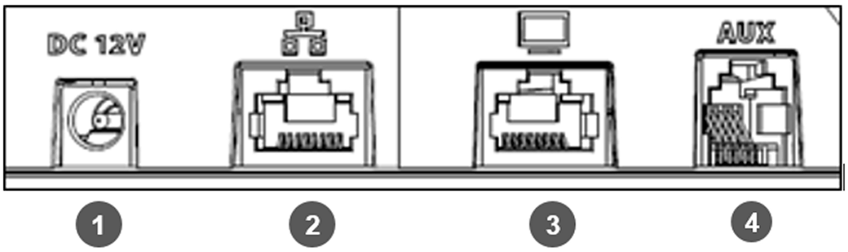


Table 2-2: Rear View Description

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

Cabling

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

Mounting the Phone

The phone can be mounted on a:

- Desk
- Wall

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

See also here for a clip showing *the principle* of how to mount an AudioCodes IP phone. The principle is the same across all AudioCodes IP phones.

Before Using AudioCodes Devices

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

➢ **To clean a device's screen:**

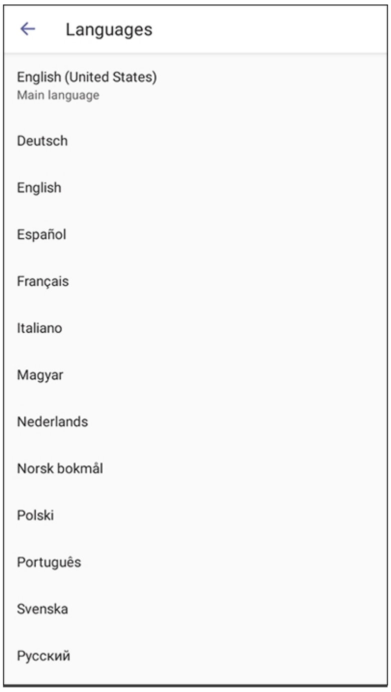
1. Disconnect all cables.
2. Spray onto a clean, dry, microfiber duster a medicinal isopropyl alcohol and water solution of 70:30. Don't oversaturate the duster. If it's wet, squeeze it out.
3. Lightly wipe the screen of the device.
4. Wait for the screen to dry before reconnecting cables.

3 Starting up

Here's how to start up the phone.

➢ **To start up:**

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



← Languages

English (United States)
Main language

Deutsch

English

Español

Français

Italiano

Magyar

Nederlands

Norsk bokmål

Polski

Português

Svenska

Русский

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

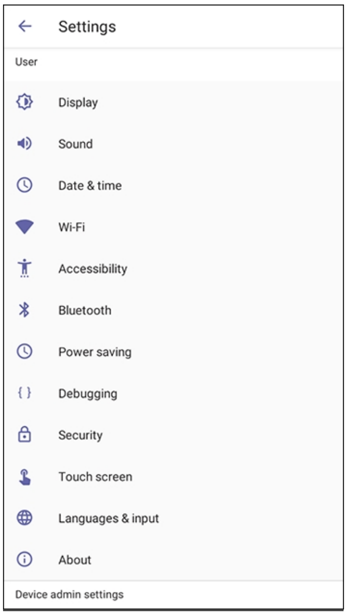
It will be necessary to repeat this only if the phone is restored to default settings.

Configuring Device Settings

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

➢ **To access device settings:**

1. In the home screen, select the user (avatar) picture and then select the **Settings** option and then **Device settings**.



Settings

User

Display

Sound

Date & time

Wi-Fi

Accessibility

Bluetooth

Power saving

Debugging

Security

Touch screen

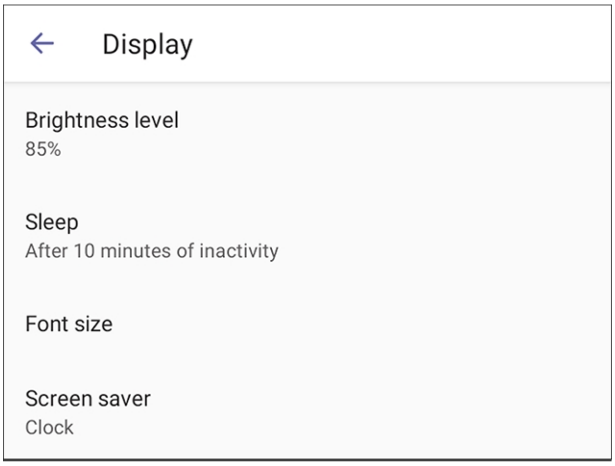
Languages & input

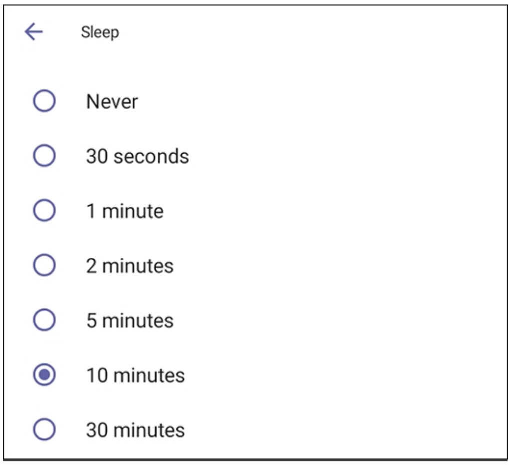
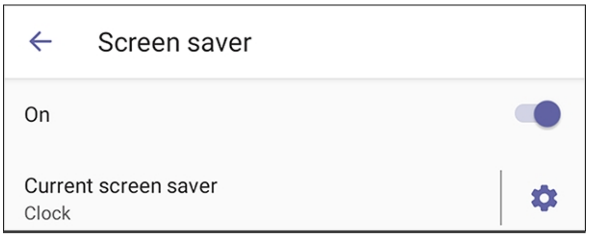
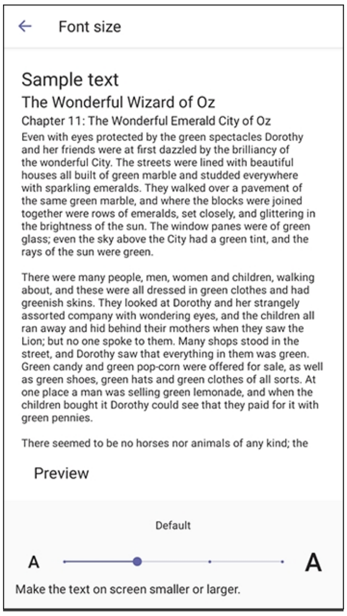
About

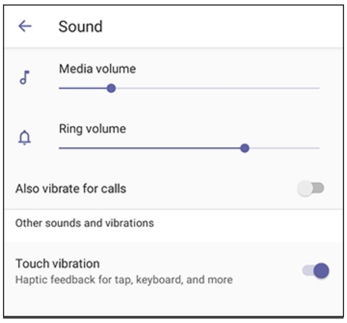
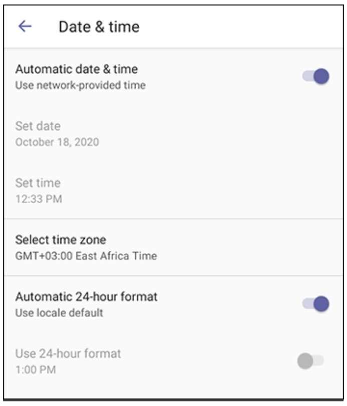
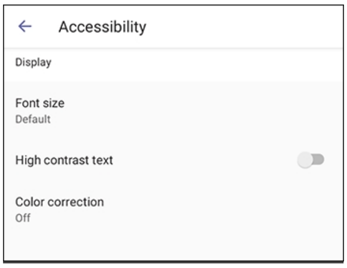
Device admin settings

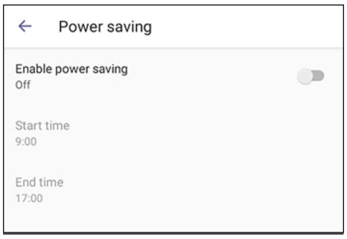
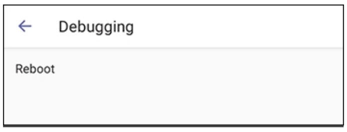
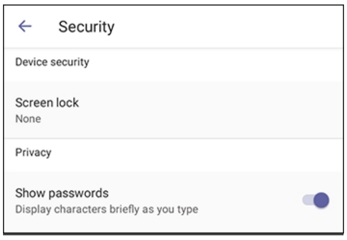
2. View the settings under 'User'. Select a setting to open it. Use the table following as reference. [To view settings related to the network administrator, scroll down and open 'Device admin settings'].

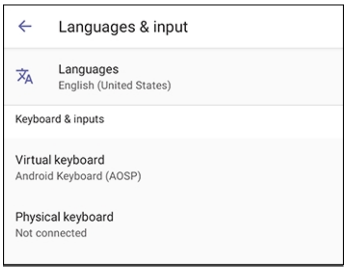
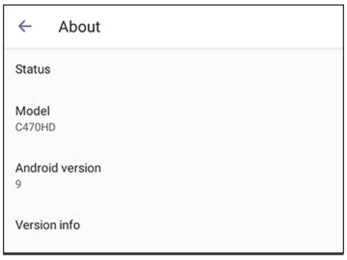
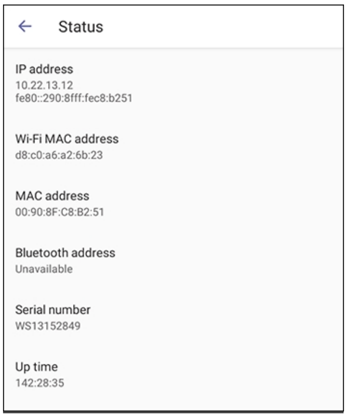
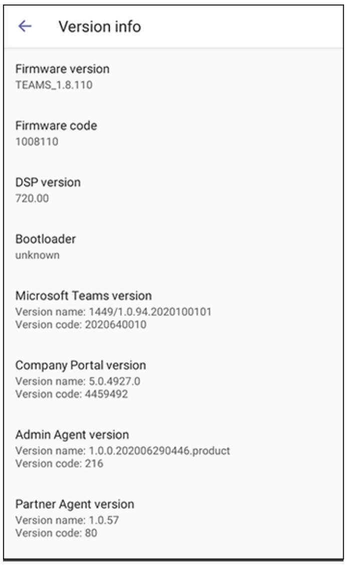
Table 3-1: Device Settings

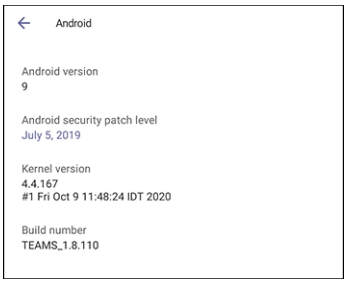
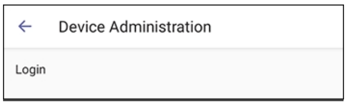
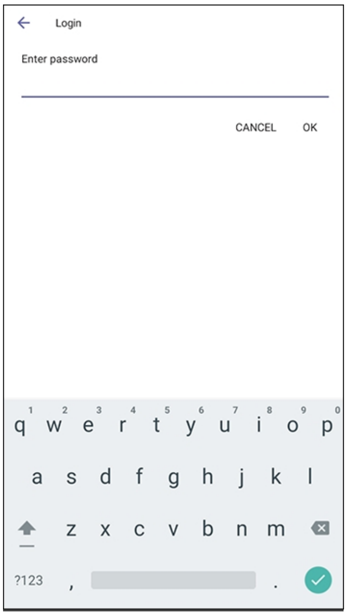
Setting	Description
User	
Display	Opens the 'Display' screen [Brightness level].  Display Brightness level 85% Sleep After 10 minutes of inactivity Font size Screen saver Clock The phone's screen supports different brightness levels. Choose the level that suits your requirements. ■ Sleep

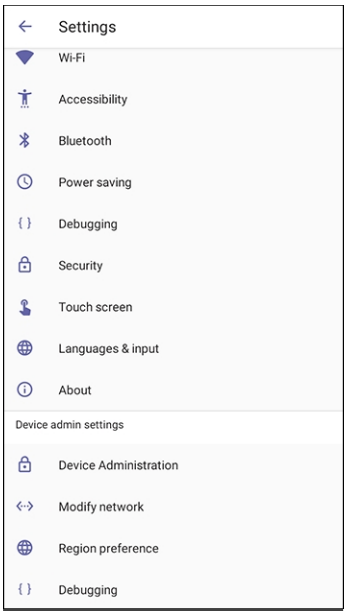
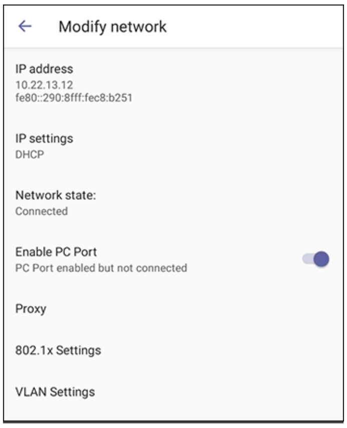
Setting	Description
	 Sleep ○ Never ○ 30 seconds ○ 1 minute ○ 2 minutes ○ 5 minutes ● 10 minutes ○ 30 minutes ■ Screen saver  Screen saver On Current screen saver Clock ■ Font size  Font size Sample text The Wonderful Wizard of Oz Chapter 11: The Wonderful Emerald City of Oz Even with eyes protected 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. 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. There seemed to be no horses nor animals of any kind; the Preview Default A A Make the text on screen smaller or larger.
Sound	Allows you to customize phone volume for a friendlier user experience. **Ring volume at n%**

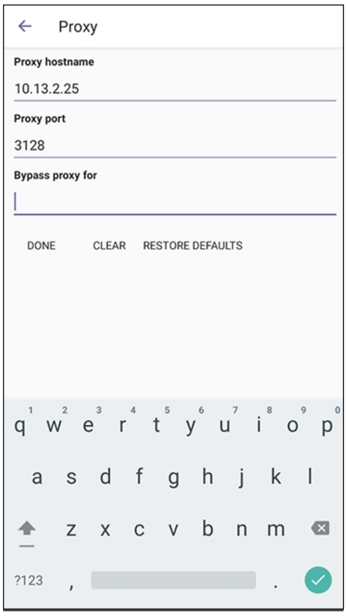
Setting	Description
	 Sound Media volume Ring volume Also vibrate for calls Other sounds and vibrations Touch vibration Haptic feedback for tap, keyboard, and more
Date & time	Date and time are automatically retrieved from the deployed Network Time Protocol (NTP) server.  Date & time Automatic date & time Use network-provided time Set date October 18, 2020 Set time 12:33 PM Select time zone GMT+03:00 East Africa Time Automatic 24-hour format Use locale default Use 24-hour format 1:00 PM Use 24-hour format [Allows you to select the Time format] Also supported is a simplified version of NTP called Simple Network Time Protocol (SNTP). Both can be used to synchronize device clocks. SNTP is typically used if full implementation of NTP is not required.
Wi-Fi	The phone can connect to an Access Point via Wi-Fi. See the phone's *Quick Guide* for detailed information on setting up Wi-Fi. See also Configuring Wi-Fi in this document for information about configuring the feature.
Accessibility	Allows making the screen reader-friendlier. See also Enabling Google Talkback on page 47.  Accessibility Display Font size Default High contrast text Color correction Off
Bluetooth	Hands free profile where the phone is able to connect to Bluetooth headset or speaker.

Setting	Description
	See the phone's *Quick Guide* for detailed information on setting up Bluetooth.
Power Saving	Allows users to contribute to power saving in the enterprise.  Power saving Enable power saving Off Start time 9:00 End time 17:00 Enable power saving Start time [The device consumes minimal energy before the user arrives at the office] End time [The device consumes minimal energy after the user leaves the office]
Debugging	Enables users to reboot the device.  Debugging Reboot Log in as Administrator for more debugging settings to be available.
Security	Helps secure the enterprise telephony network against breaches.  Security Device security Screen lock None Privacy Show passwords Display characters briefly as you type Screen lock [The phone automatically locks after a configured period to secure it against unwanted use. If left unattended for 10 minutes (default), it automatically locks and is inaccessible to anyone who doesn't know its lock code.] Make passwords available
Touch screen	Allows users to disable the phone’s touch screen.
Languages & input	Allows users to customize inputting to suit personal requirements.

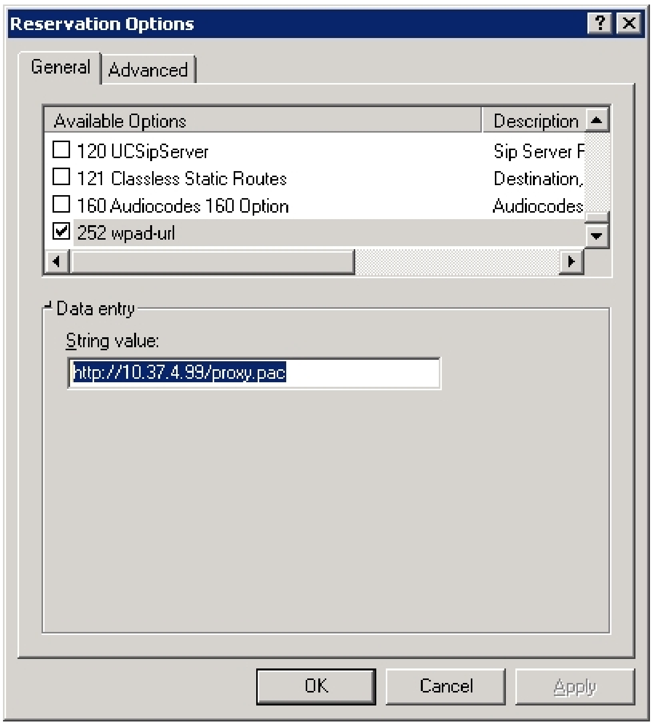
Setting	Description
	 Languages & input Languages English (United States) Keyboard & inputs Virtual keyboard Android Keyboard (AOSP) Physical keyboard Not connected
About [Android 7.1.2]	Enables users to determine device information.  About Status Model C470HD Android version 9 Version info To determine the device’s IP address, select the ‘Status’ option.  Status IP address 10.22.13.12 fe80::290:8fff:fec8:b251 Wi-Fi MAC address d8:c0:a6:a2:6b:23 MAC address 00:90:8F:C8:B2:51 Bluetooth address Unavailable Serial number WS13152849 Up time 142:28:35 To get information about the version, select ‘Version info’.  Version info Firmware version TEAMS_1.8.110 Firmware code 1008110 DSP version 720.00 Bootloader unknown Microsoft Teams version Version name: 1449/1.0.94.2020100101 Version code: 2020640010 Company Portal version Version name: 5.0.4927.0 Version code: 4459492 Admin Agent version Version name: 1.0.0.202006290446.product Version code: 216 Partner Agent version Version name: 1.0.57 Version code: 80

Setting	Description
	To get information about the Android version, select ‘Android version’.  Android Android version 9 Android security patch level July 5, 2019 Kernel version 4.4.167 #1 Fri Oct 9 11:48:24 IDT 2020 Build number TEAMS_1.8.110
Device admin settings	
Device administration	Allows the user to log in as Administrator, necessary for some of the debugging options. It is password protected. Default password: 1234 (or 1111 in early versions). After logging in as an Administrator, the user can log out | change password.  Device Administration Login Select **Login** and then in the Login screen that opens, select the 'Enter password' field and use the virtual keyboard to enter the password (**1234** or **1111**). Note that the virtual keyboard pops up for all ‘Settings’ fields to allow inputting characters and / or numbers. Two virtual keyboard types can be displayed: Numeric or QWERTY.  Login Enter password CANCEL OK 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 , . The virtual keyboard is also displayed when the network administrator needs to enter an IP address to debug, or when they need to enter their PIN lock for the security tab.

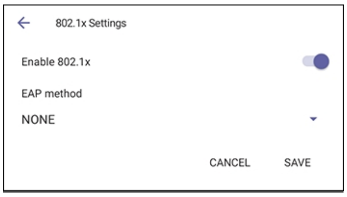
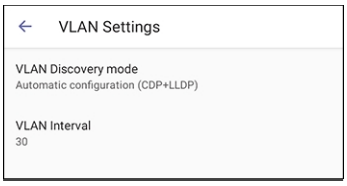
Setting	Description
	After logging in, scroll down in the Settings screen to the section 'Device admin settings'.  Settings Wi-Fi Accessibility Bluetooth Power saving Debugging Security Touch screen Languages & input About Device admin settings Device Administration Modify network Region preference Debugging
Modify network	Enables the Admin user to determine network information and to modify network settings.  Modify network IP address 10.22.13.12 fe80::290:8fff:fec8:b251 IP settings DHCP Network state: Connected Enable PC Port PC Port enabled but not connected Proxy 802.1x Settings VLAN Settings IP Address [Read Only] IP Settings [DHCP or Static IP] Network state [Read Only] Enable PC port Enable PC port mirror Proxy 802.1x Settings VLAN Settings. Allows you to configure the VLAN mode **Manual**, **CDP only** or **LLDP only**.

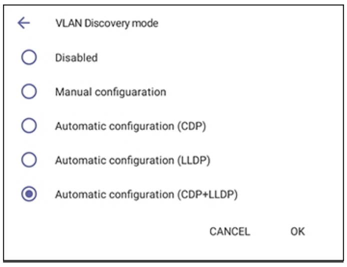
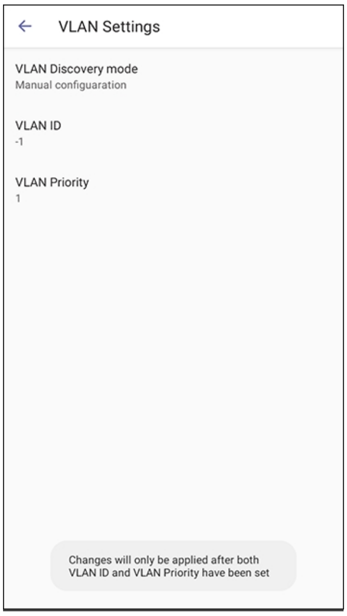
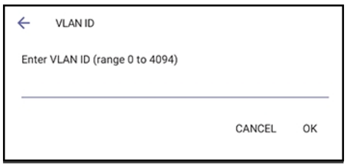
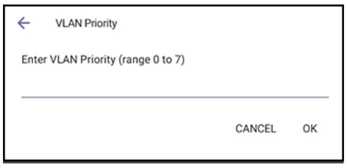
Setting	Description
Proxy	The phone can be configured with an HTTP Proxy server by an Admin user in two ways: ■ **Manually**. The Admin user can use this method to configure HTTP proxy server parameters through the Teams application: a. Log in as Administrator and select **Modify network**. b. Select the **Proxy** option and then configure the proxy host name and port:  Proxy Proxy hostname 10.13.2.25 Proxy port 3128 Bypass proxy for DONE CLEAR RESTORE DEFAULTS 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 , . ■ **Over DHCP with Option 252**. It's recommended that the Admin user uses this method when provisioning multiple phones. Option 252 provides a DHCP client with a URL to use to configure its proxy settings:

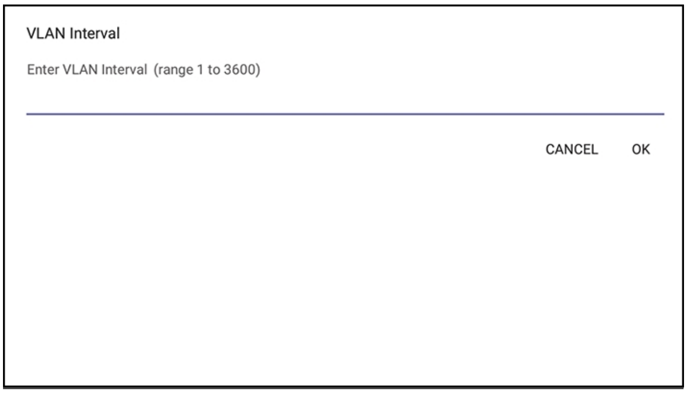
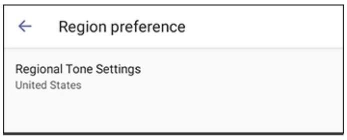
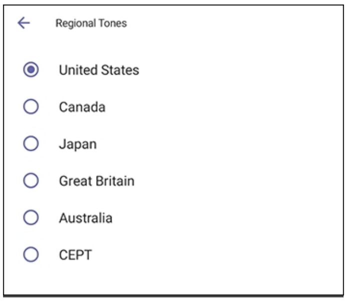
Setting	Description

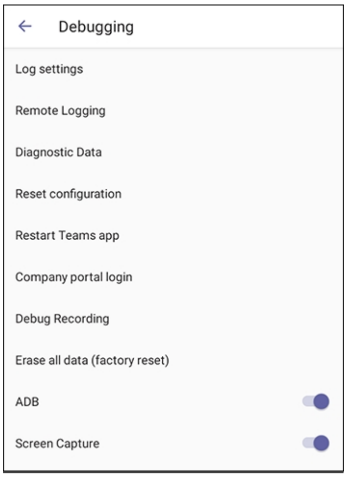
	 Reservation Options
	General
	Advanced
	OK
	Cancel
	Apply
	Available Options | Description
	☐ 120 UCSipServer | Sip Server F
	☐ 121 Classless Static Routes | Destination,
	☐ 160 Audiocodes 160 Option | Audiocodes
	☑ 252 wpad-url
	Data entry
	String value: http://10.37.4.99/proxy.pac
	The proxy setting is provided in a Proxy Auto-Configuration (PAC) file that contains a set of rules coded in JavaScript which allows a web browser to determine whether to send web traffic directly to the Internet or to be sent via a proxy server. PAC files control how the phone handles HTTP, HTTPS and FTP traffic.
	Example of a basic PAC file:
	`function FindProxyForURL(url, host)`
	`{`
	`return "PROXY 10.13.2.40:3128";`
	`}`
	If the enterprise features a proxy server that requires user authentication, the network administrator can use the PAC file and DHCP Option 252 to configure it. Alternatively, the administrator can configure it using the following parameters:
	`http_client/fwd_proxy/ip=0.0.0.0`
	`http_client/fwd_proxy/password=`
	`http_client/fwd_proxy/port=8080`
	`http_client/fwd_proxy/username=`

802.1x Settings	802.1X Authentication is the IEEE Standard for Port-based Network Access Control (PNAC). See https://1.ieee802.org/security/802-1x/ for more information. **To configure an 802.1X Authentication method:**

Setting	Description
	1. From the 'Modify Network' screen (as an Admin), access the 802.1x Settings screen.  802.1x Settings Enable 802.1x EAP method NONE CANCEL SAVE **2.** From the 'EAP method' drop-down, select the method: MD5 or TLS (for example). **3.** Enter this information: ✓ Identity: User ID ✓ Password ✓ root certificate (not required for every method) ✓ client certificate (not required for every method) **4.** Select the **Save** softkey The 802.1x settings are not only available via the phone screen, they're also supported in the device Configuration File, enabling network administrator's to perform pre-staging configuration for 802.1x. The 802.1x settings available in the Configuration File are: ■ Enable/Disable ■ EAP method ■ Identity ■ Password
VLAN Settings	Select the menu option **VLAN Settings**.  VLAN Settings VLAN Discovery mode Automatic configuration (CDP+LLDP) VLAN Interval 30 Select **VLAN Discovery mode**.

Setting	Description
	 VLAN Discovery mode ○ Disabled ○ Manual configuaration ○ Automatic configuration (CDP) ○ Automatic configuration (LLDP) ● Automatic configuration (CDP+LLDP) CANCEL OK ■ Cisco Discovery Protocol (**CDP**) is a Cisco proprietary Data Link Layer protocol ■ Link Layer Discovery Protocol (**LLDP**) is a standard, layer two discovery protocol Select the mode you require and then select **OK**. If you select **Manual configuration**, this screen opens:  VLAN Settings VLAN Discovery mode Manual configuaration VLAN ID -1 VLAN Priority 1 Changes will only be applied after both VLAN ID and VLAN Priority have been set Select **VLAN ID**.  VLAN ID Enter VLAN ID (range 0 to 4094) CANCEL OK Select **VLAN Priority**.  VLAN Priority Enter VLAN Priority (range 0 to 7) CANCEL OK

Setting	Description
	Select **VLAN Interval**.  VLAN Interval Enter VLAN Interval (range 1 to 3600) 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.
Region preference	Select the menu option **Region preference**.  Region preference Regional Tone Settings United States 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. Select **Regional Tone Settings** and select the country in which the phone is located.  Regional Tones ● United States ○ Canada ○ Japan ○ Great Britain ○ Australia ○ CEPT
Debugging	Allows the Admin user to perform debugging for troubleshooting purposes. Available after logging in as Admin.

Setting	Description
	 Debugging Log settings Remote Logging Diagnostic Data Reset configuration Restart Teams app Company portal login Debug Recording Erase all data (factory reset) ADB Screen Capture Log settings Remote Logging (see under Remote Logging (Syslog) on page 106 for more information) Diagnostic Data (see under Getting Diagnostics on page 107 for more information) Reset configuration Restart Teams app Company portal login Debug Recording (for Media/DSP debugging) (see under Remote Logging (Syslog) on page 106 for more information) Factory data reset (the equivalent of restore to defaults; including logout and device reboot) ADB (Android Debug Bridge command-line tool used to debug the Teams app); the setting is disabled by default. The device does not allow access to ADB. Screen Capture. By default, this setting is enabled. If it's disabled, the phone won't allow its screens to be captured.

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:

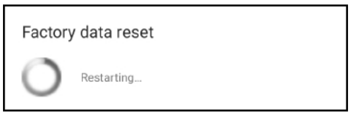
- Performing a Hard Restore below
- Performing a Soft Restore on the next page

Performing a Hard Restore

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

➢ 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.



Factory data reset

Restarting...

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

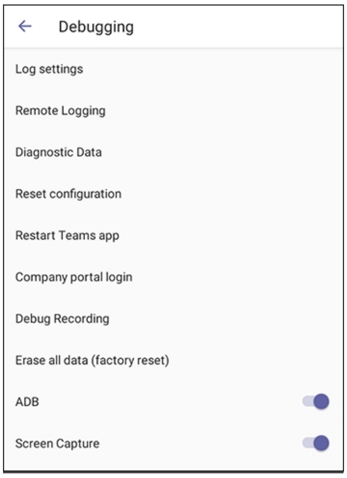
2. Select **OK**; the sign-in screen is displayed (see Signing In on page 35 for more information).

Performing a Soft Restore

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

➢ To perform a soft restore:

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



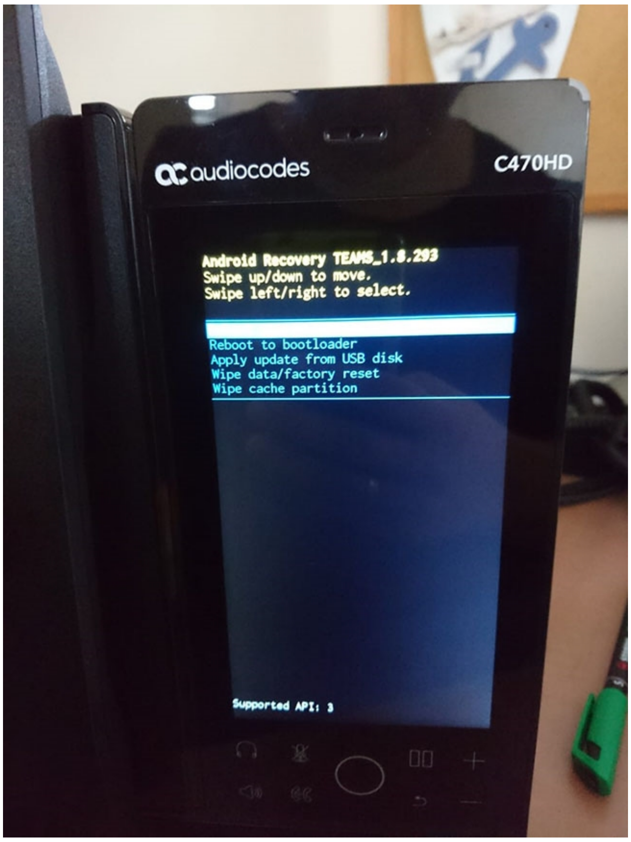
2. Select the **Erase all data (factory reset)** option; the device performs a restore to default factory settings.

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**.



```
Android Recovery TEAMS_1.8.293
Swipe up/down to move.
Swipe left/right to select.

Reboot to bootloader
Apply update from USB disk
Wipe data/factory reset
Wipe cache partition

Supported API: 3
```

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

Locking and Unlocking the Phone

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

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

Automatic Lock

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

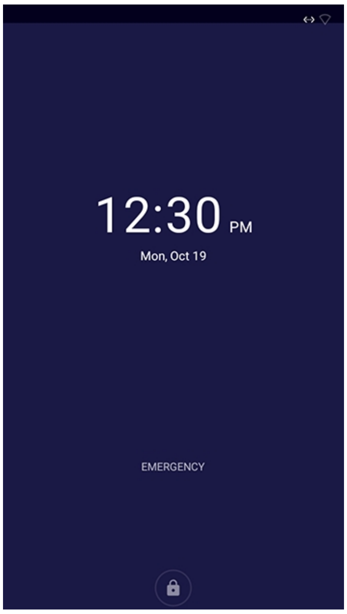
➢ **To lock the phone:**

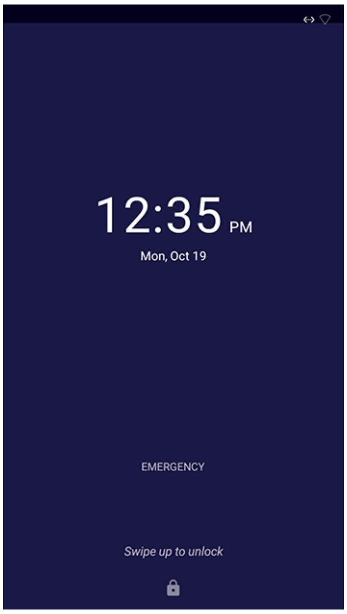
- Press the back key ⮌ on the phone for at least three seconds for the device to automatically lock.

Unlock

➢ **To unlock the phone:**

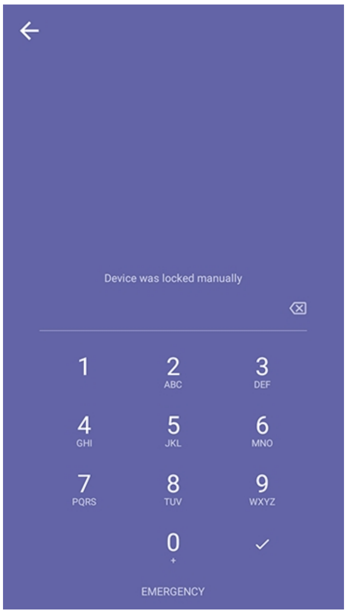
1. When the screen shown in the figure below is displayed, touch the lock icon and swipe up





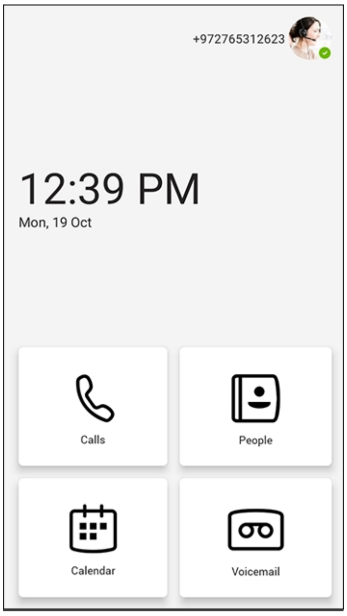
Swipe up to unlock

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



Device was locked manually

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


+972765312623
12:39 PM
Mon, 19 Oct
Calls
People
Calendar
Voicemail

4 Teams Application

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

Signing In

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

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

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

'Modern Authentication' is also supported.

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

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

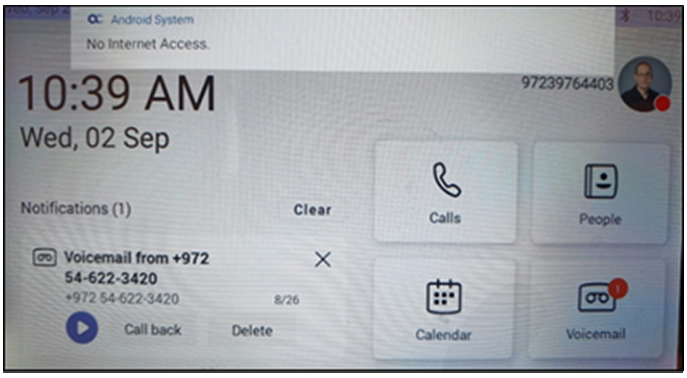
In most regions, Daylight Saving Time changes the regional time twice a year. DST Validation allows maintaining accurate time. Two options for phones to get the correct time are:

- [Recommended] If the DHCP server offers Timezone Options (100/101), the phone will set the obtained time zone and display the correct time on the screen; the time will be calculated based on an embedded Time Zone database, factoring in DST.
- If the DHCP server offers Time Offset Option only (2), the phone will assign the obtained time offset to the first matched region in the list but there is a good chance it won't reflect

the actual geographical location, therefore the displayed time might be incorrect in some cases. For example, if the given time offset is GMT-5 and the phone is located in Mexico, the phone will get the time (and the DST setting) from central time and not from Mexico because in GMT-5 there is also Central Daylight Time.

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

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



Android System

No Internet Access.

10:39 AM

Wed, 02 Sep

97239764403

Notifications (1)

Voicemail from +972 54-622-3420

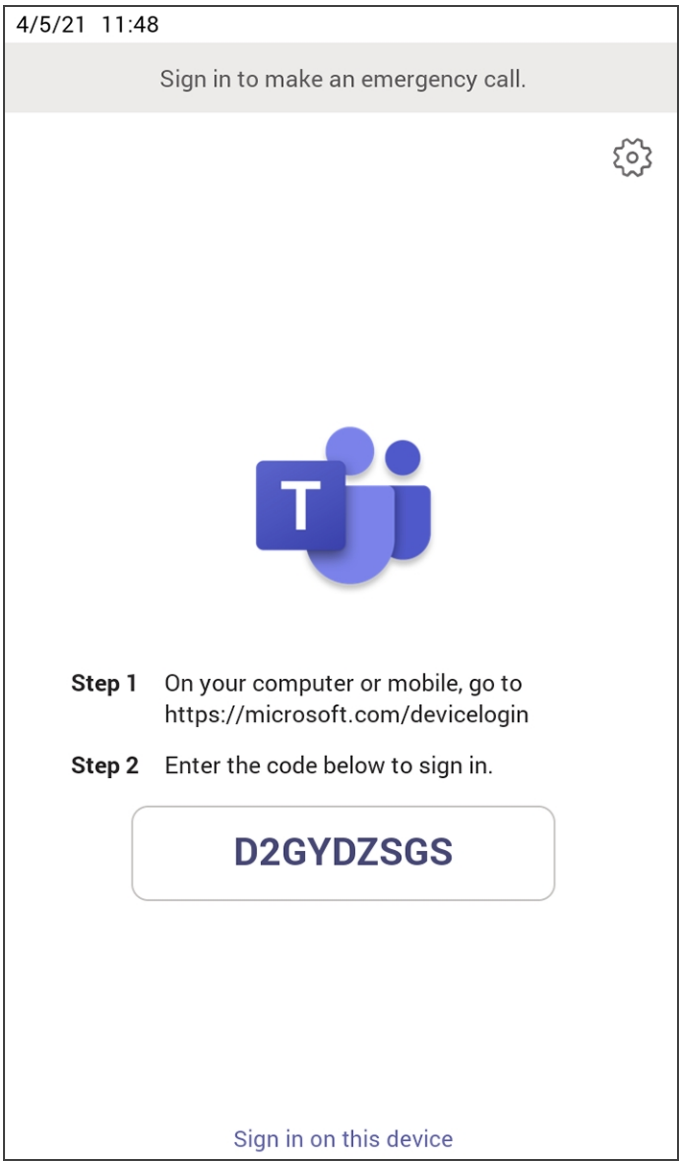
+972 54-622-3420

8/26

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

➢ To sign in:

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



4/5/21 11:48

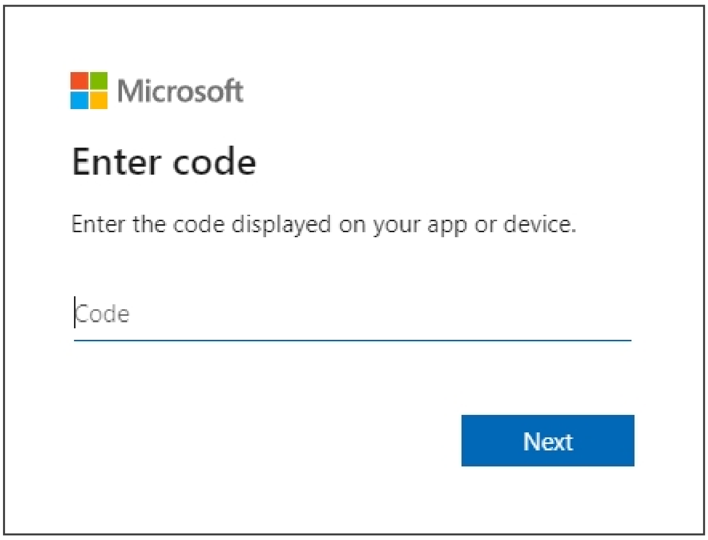
Sign in to make an emergency call.

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

Step 2 Enter the code below to sign in.

D2GYDZSGS

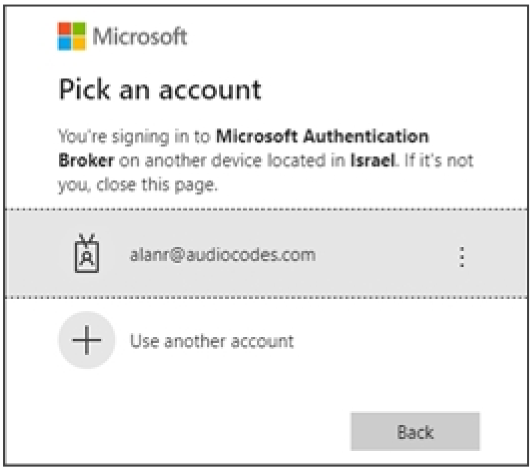
2. Open your browser and point it to **https://microsoft.com/devicelogin** as instructed in the preceding screen.



Enter code

Enter the code displayed on your app or device.

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



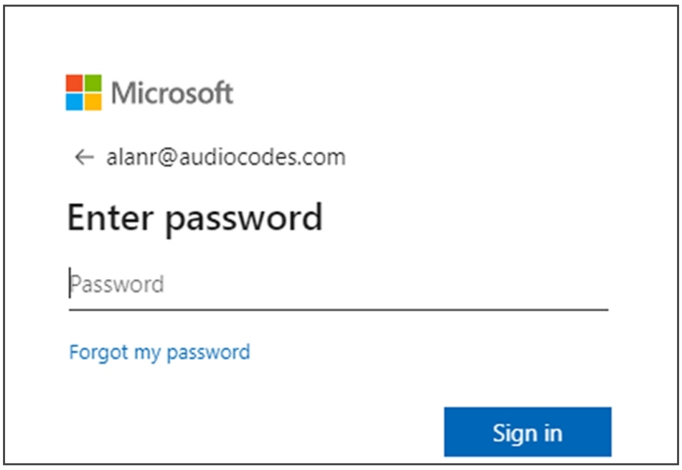
Microsoft

Pick an account

You're signing in to **Microsoft Authentication Broker** on another device located in **Israel**. If it's not you, close this page.

alanr@audiocodes.com

4. Click the account.

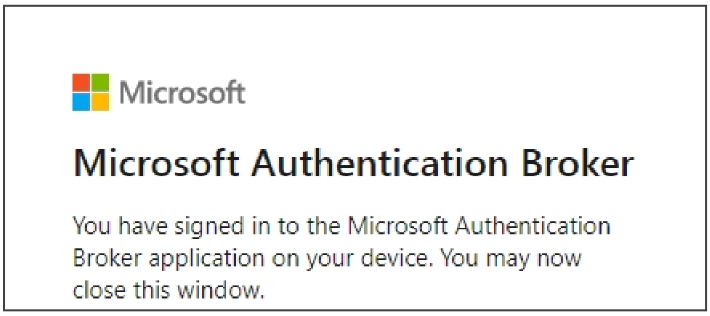


Microsoft

alanr@audiocodes.com

Enter password

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



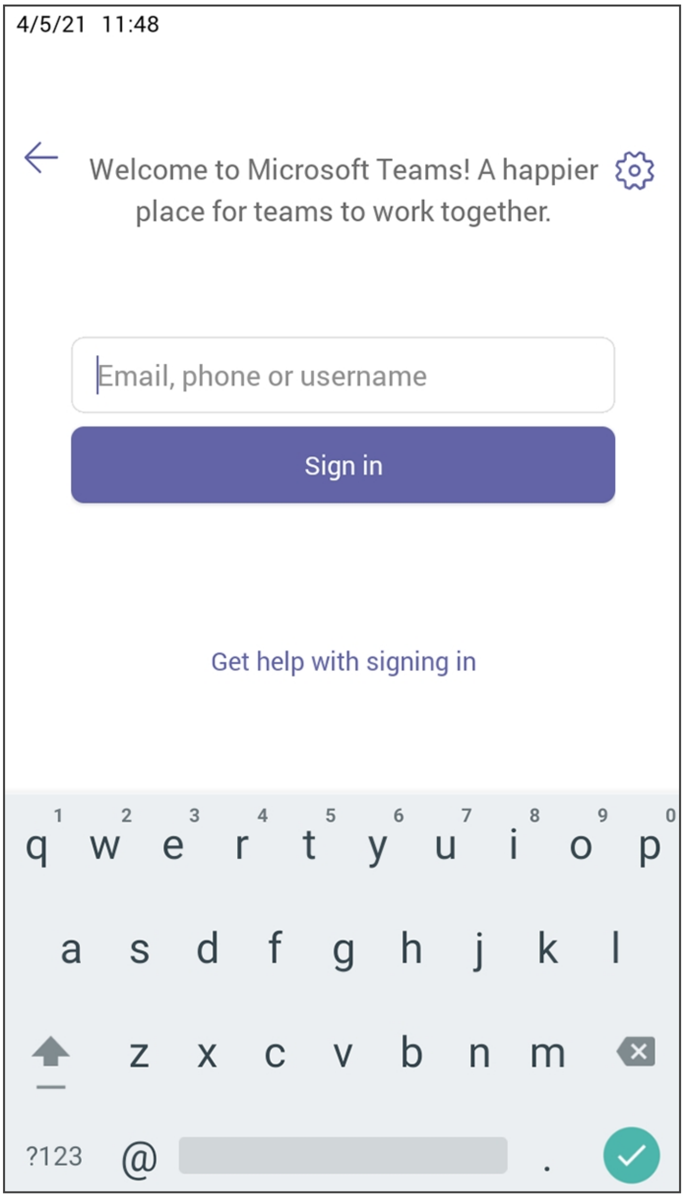
Microsoft

Microsoft Authentication Broker

You have signed in to the Microsoft Authentication Broker application on your device. You may now close this window.

6. Close the window shown in the preceding figure.

7. Observe that the phone returns to the initial code screen. In that screen, select **Sign in on this device**.



4/5/21 11:48

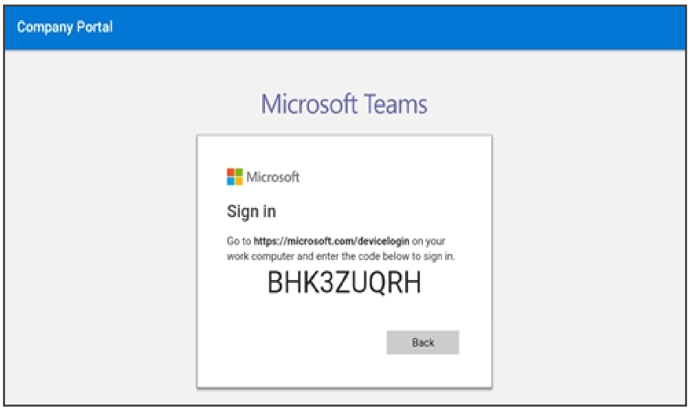
Welcome to Microsoft Teams! A happier place for teams to work together.

Email, phone or username

8. Select the 'Email, phone or username' field; a virtual keyboard pops up. Enter one of them and then choose **Sign in**. The 'home' screen opens.

   - If you opt to **Sign in from another device**, complete authentication from your PC or smart phone. This is recommended if you're using Multi Factor Authentication (MFA).

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



Company Portal

Microsoft Teams

Microsoft

Sign in

Go to **https://microsoft.com/devicelogin** on your work computer and enter the code below to sign in.

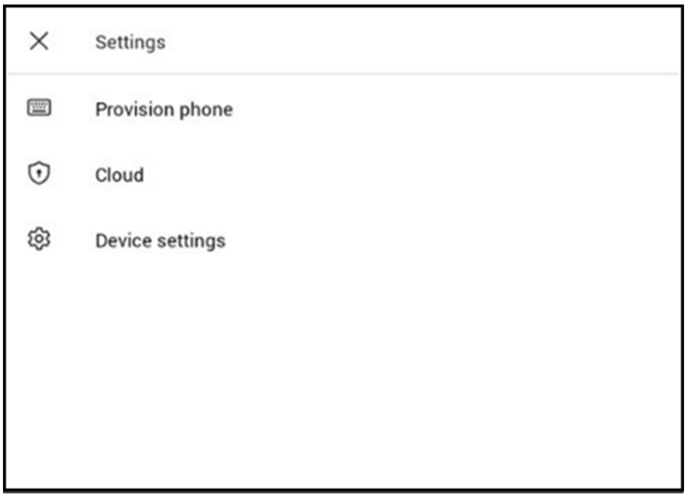
BHK3ZUQRH

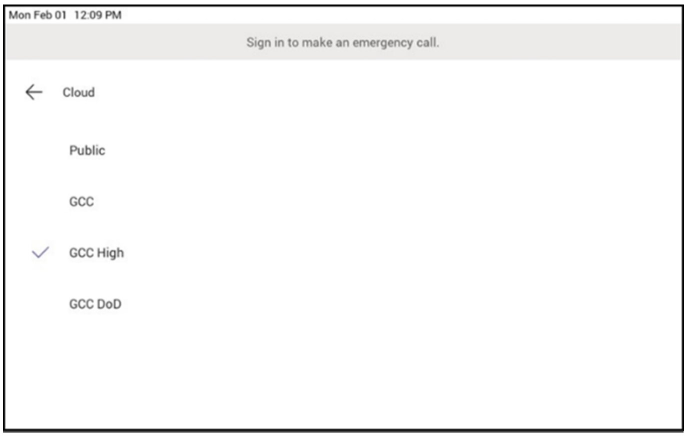
- In the browser on your PC or smart phone, enter the URL indicated in the preceding screen and then in the phone's Web interface that opens, perform sign-in (as noted previously, this option is recommended if using MFA).

> ⚠ 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.





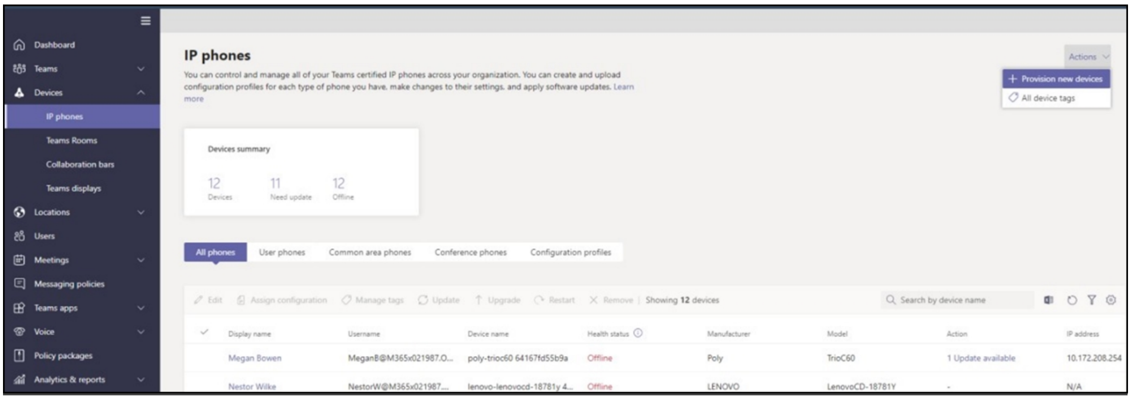
Remote Provisioning and Sign-in from Teams Admin Center

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.



IP phones

You can control and manage all of your Teams certified IP phones across your organization. You can create and upload configuration profiles for each type of phone you have, make changes to their settings, and apply software updates. Learn more

12	11	12
Devices	Need update	Offline

Showing 12 devices

Display name	Username	Device name	Health status	Manufacturer	Model	Action	IP address
Megan Bowen	MeganB@M365x021987.O...	poly-trioc60 64167fd55b9a	Offline	Poly	TrioC60	1 Update available	10.172.208.254
Nestor Wilke	NestorW@M365x021987....	lenovo-lenovocd-18781y 4...	Offline	LENOVO	LenovoCD-18781Y	-	N/A

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.

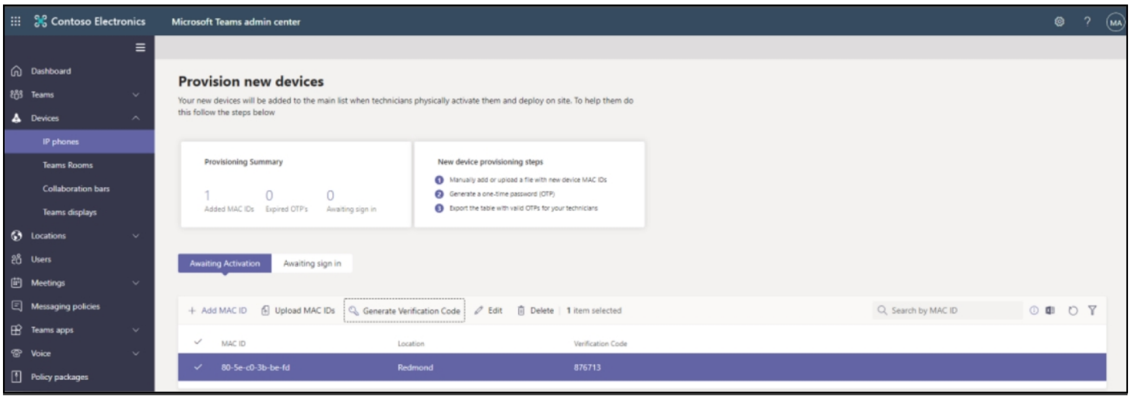
Upload a file to add a device MAC address

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.



Provision new devices

Your new devices will be added to the main list when technicians physically activate them and deploy on site. To help them do this follow the steps below

Provisioning Summary

1	0	0
Added MAC IDs	Expired OTP's	Awaiting sign in

New device provisioning steps

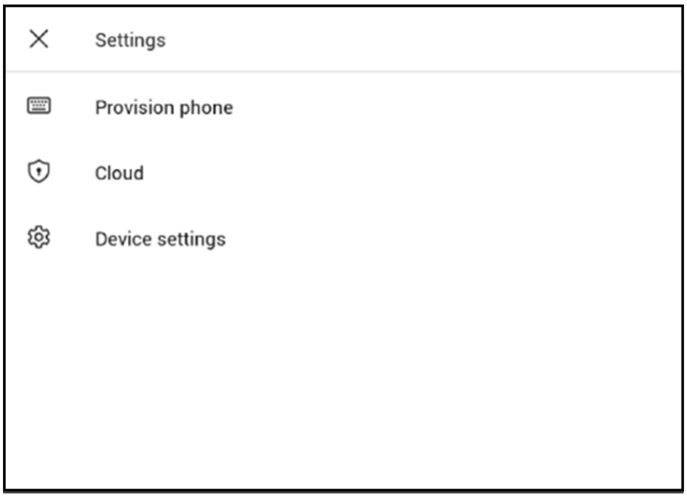
1. Manually add or upload a file with new device MAC IDs
2. Generate a one-time password (OTP)
3. Export the table with valid OTPs for your technicians

MAC ID	Location	Verification Code
80-5e-c0-3b-be-fd	Redmond	876713

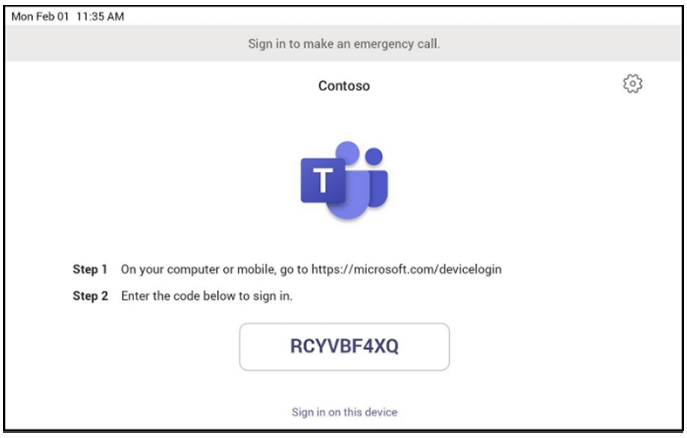
You'll need to provide the list of MAC IDs and verification codes to the field technicians. You can export the detail directly in a file and share the file with the technician who is doing the actual installation work.

➢ 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.



Mon Feb 01 11:35 AM

Sign in to make an emergency call.

Contoso

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

Step 2 Enter the code below to sign in.

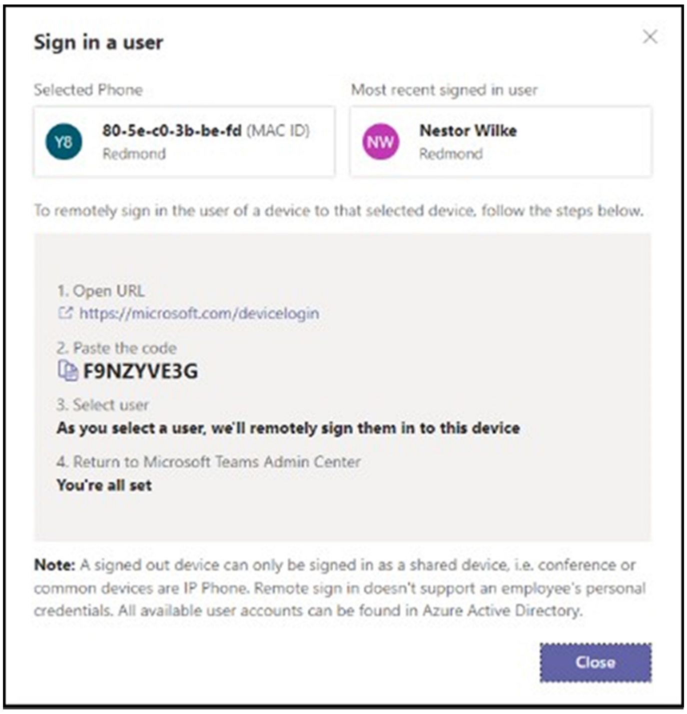
RCYVBF4XQ

Sign in on this device

➢ 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**.



Sign in a user

Selected Phone

Y8 **80-5e-c0-3b-be-fd** (MAC ID)
Redmond

Most recent signed in user

NW **Nestor Wilke**
Redmond

To remotely sign in the user of a device to that selected device, follow the steps below.

1. Open URL
https://microsoft.com/devicelogin

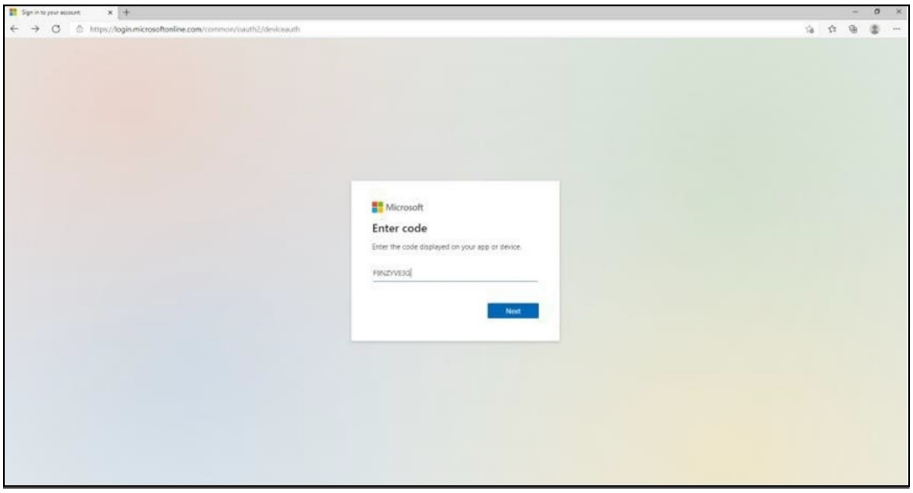
2. Paste the code
F9NZYVE3G

3. Select user
As you select a user, we'll remotely sign them in to this device

4. Return to Microsoft Teams Admin Center
You're all set

Note: A signed out device can only be signed in as a shared device, i.e. conference or common devices are IP Phone. Remote sign in doesn't support an employee's personal credentials. All available user accounts can be found in Azure Active Directory.

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



Sign in to your account

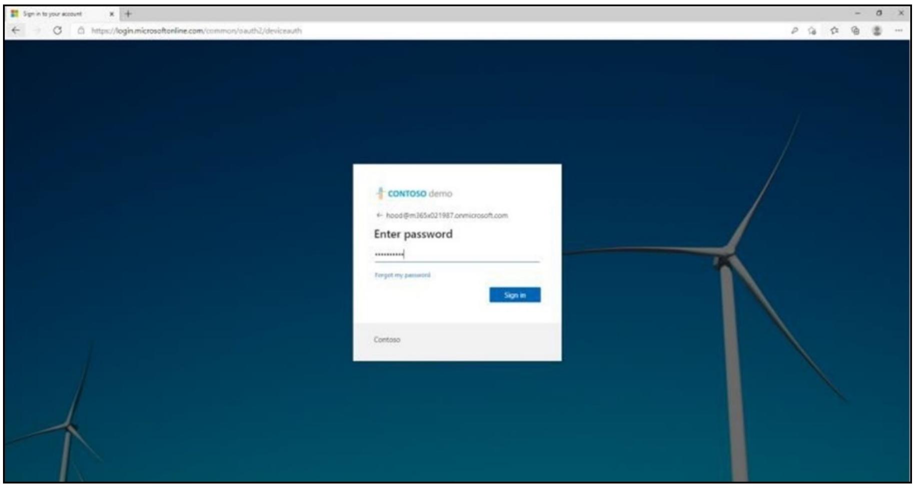
https://login.microsoftonline.com/common/oauth2/deviceauth

Microsoft

Enter code

Enter the code displayed on your app or device.

F9NZYVE3G



Sign in to your account

https://login.microsoftonline.com/common/oauth2/deviceauth

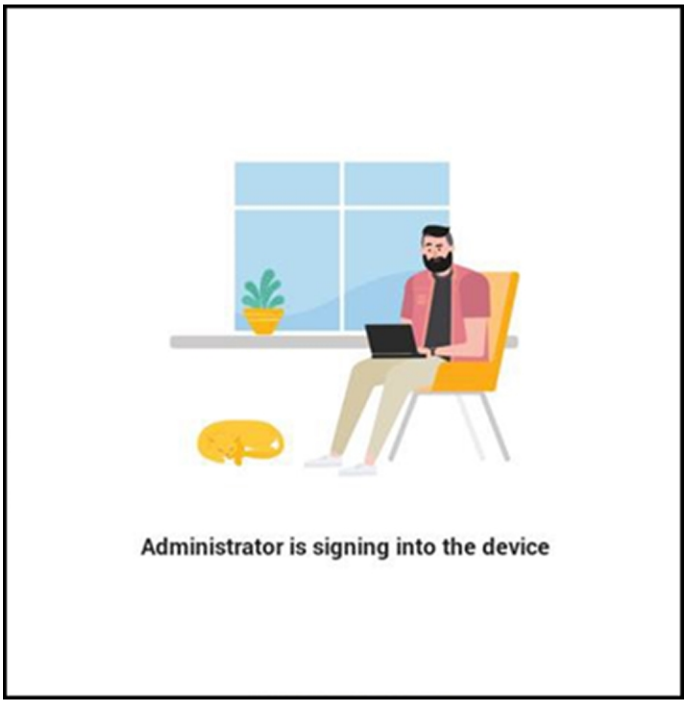
CONTOSO demo

← hood@m365x021987.onmicrosoft.com

Enter password

••••••••••

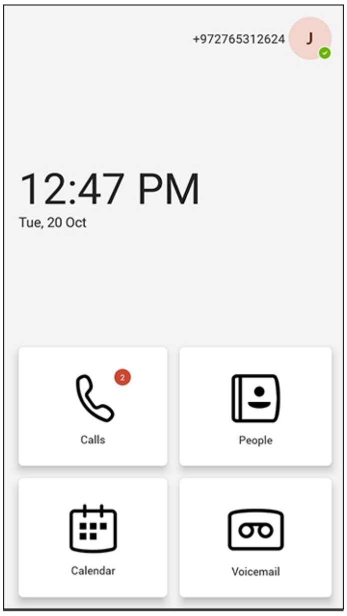
When the tenant admin is signing in from Teams Admin Center, the user interface on the device is blocked to prevent other actions on the phone.



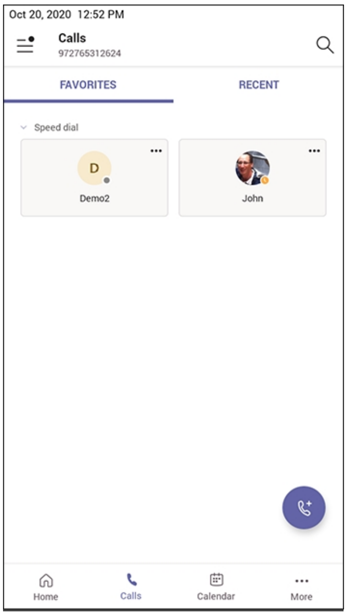
Administrator is signing into the device

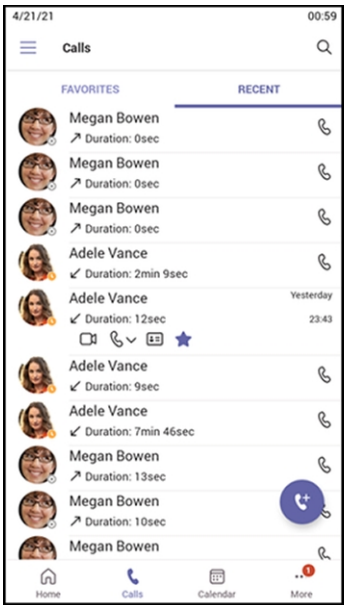
Getting Acquainted with the Phone Screen

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



The following figure shows the phone's Calls screen.





Megan Bowen ↗ Duration: 0sec

Megan Bowen ↗ Duration: 0sec

Megan Bowen ↗ Duration: 0sec

Adele Vance ↙ Duration: 2min 9sec

Adele Vance ↙ Duration: 12sec Yesterday 23:43

Adele Vance ↙ Duration: 9sec

Adele Vance ↙ Duration: 7min 46sec

Megan Bowen ↗ Duration: 13sec

Megan Bowen ↗ Duration: 10sec

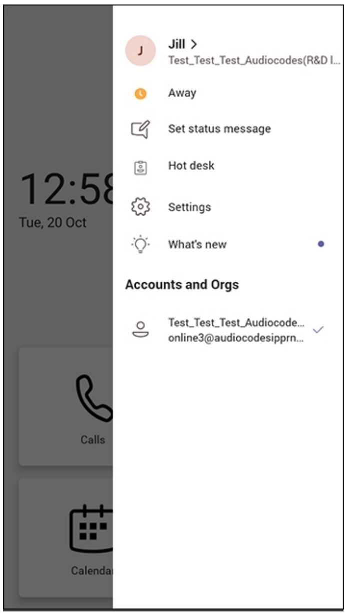
Megan Bowen

The following table describes the phone's home screen.

Table 4-1: Calls Screen

Item	Description
☰	The phone menu. Select it to open the menu shown in the figure following this table.
Calls	Select the tab to open the Calls screen. The screen shown in the figure preceding this table opens.
People	Select the tab to open the People, shown under Using the People Screen on page 57 opens. Allows you to easily connect and collaborate with teammates, colleagues, friends and family. Through this screen, you can see all your contacts and create and manage contact groups to organize your contacts. The screen provides a simple user experience and aligns with the contacts on the Teams desktop client. If a contact has multiple numbers, the phone screen allows the user to select from a drop-down menu the intended contact method.
Calendar	Select to open the Calendar screen, shown under Setting up a Meeting on page 56 opens.
Voicemail	Select the tab to open the Voicemail screen, shown under Accessing Voicemail on page 58 opens.

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



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.
Set status message	See Setting Status on page 50 for more information.
Connect a device	See Connecting a Device for more information.
Hot desk	See Hot Desking on page 51 for more information.
Settings	See Configuring Teams Application Settings on page 54 for more information.
Sign Out	See Signing Out on page 60 for more information.

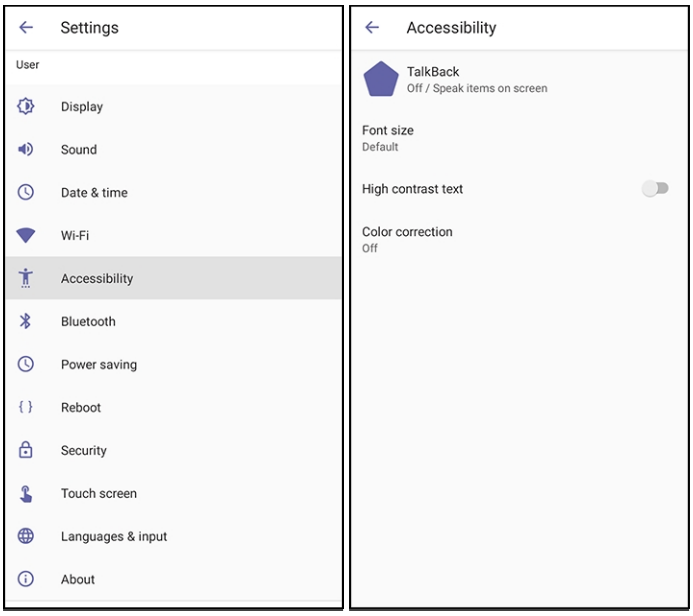
Enabling Google Talkback

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

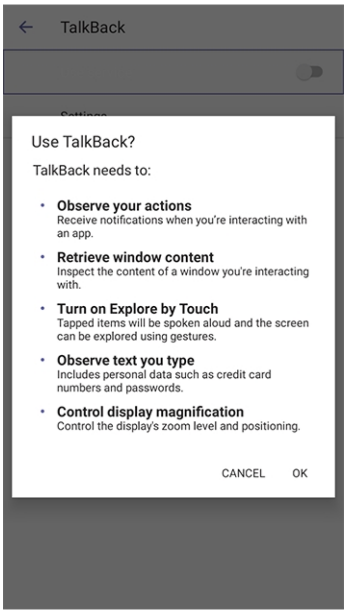
The feature improves the experience of these users.

➢ To enable the feature:

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



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



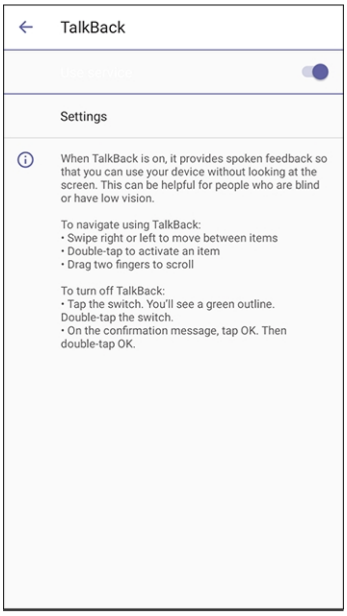
TalkBack

Use TalkBack?

TalkBack needs to:

- **Observe your actions**
  Receive notifications when you're interacting with an app.
- **Retrieve window content**
  Inspect the content of a window you're interacting with.
- **Turn on Explore by Touch**
  Tapped items will be spoken aloud and the screen can be explored using gestures.
- **Observe text you type**
  Includes personal data such as credit card numbers and passwords.
- **Control display magnification**
  Control the display's zoom level and positioning.

CANCEL OK



TalkBack

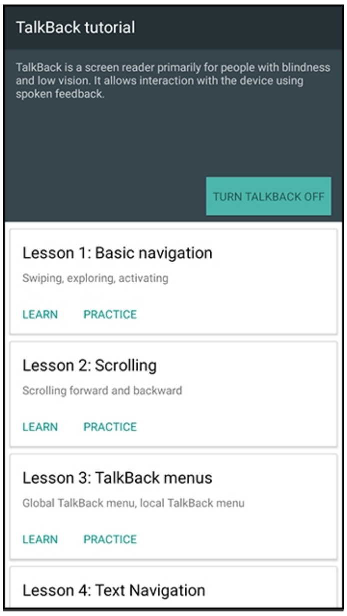
Settings

When TalkBack is on, it provides spoken feedback so that you can use your device without looking at the screen. This can be helpful for people who are blind or have low vision.

To navigate using TalkBack:
• Swipe right or left to move between items
• Double-tap to activate an item
• Drag two fingers to scroll

To turn off TalkBack:
• Tap the switch. You'll see a green outline. Double-tap the switch.
• On the confirmation message, tap OK. Then double-tap OK.

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.



TalkBack tutorial

TalkBack is a screen reader primarily for people with blindness and low vision. It allows interaction with the device using spoken feedback.

TURN TALKBACK OFF

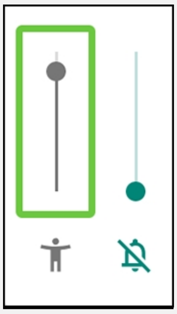
Lesson 1: Basic navigation
Swiping, exploring, activating
LEARN PRACTICE

Lesson 2: Scrolling
Scrolling forward and backward
LEARN PRACTICE

Lesson 3: TalkBack menus
Global TalkBack menu, local TalkBack menu
LEARN PRACTICE

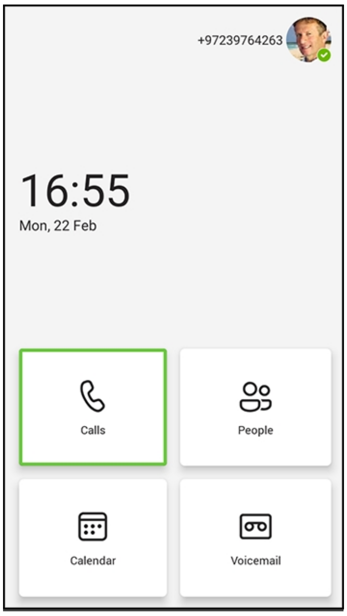
Lesson 4: Text Navigation

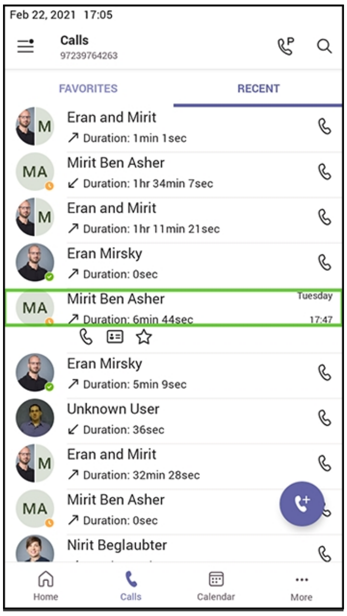
- After TalkBack is switched on, operations are performed by *touching to select* and then *double-touching to activate*.
- To turn up the volume, touch the **+** key on the phone and in the volume pop-up shown in the figure below, touch the slider to select it; audio announces what level you're at.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





Feb 22, 2021 17:05

Calls
97239764263

FAVORITES RECENT

Eran and Mirit
↗ Duration: 1min 1sec

Mirit Ben Asher
↙ Duration: 1hr 34min 7sec

Eran and Mirit
↗ Duration: 1hr 11min 21sec

Eran Mirsky
↗ Duration: 0sec

Mirit Ben Asher Tuesday
↗ Duration: 6min 44sec 17:47

Eran Mirsky
↗ Duration: 5min 9sec

Unknown User
↙ Duration: 36sec

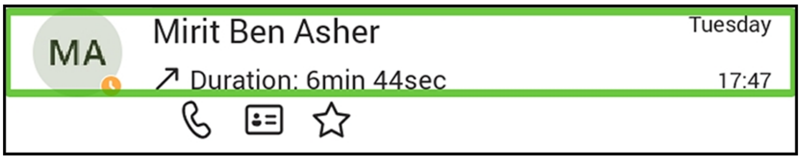
Eran and Mirit
↗ Duration: 32min 28sec

Mirit Ben Asher
↗ Duration: 0sec

Nirit Beglaubter

➢ To interact with the Calls screen:

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



Mirit Ben Asher

↗ Duration: 6min 44sec

Tuesday

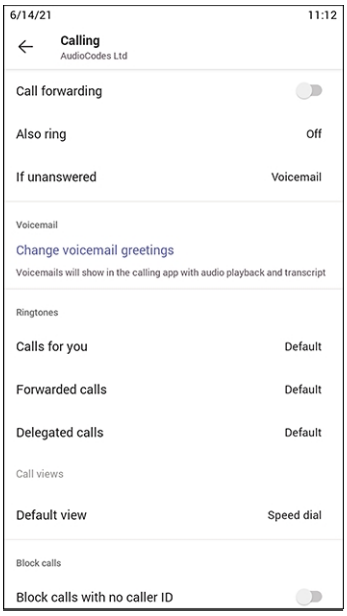
17:47

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

5. Select the star icon; audio informs you that you can add to Favorites; double-touch to activate it.

Opting in or out of Call Queues

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



6/14/21 11:12

Calling
AudioCodes Ltd

Call forwarding

Also ring Off

If unanswered Voicemail

Voicemail

Change voicemail greetings

Voicemails will show in the calling app with audio playback and transcript

Ringtones

Calls for you Default

Forwarded calls Default

Delegated calls Default

Call views

Default view Speed dial

Block calls

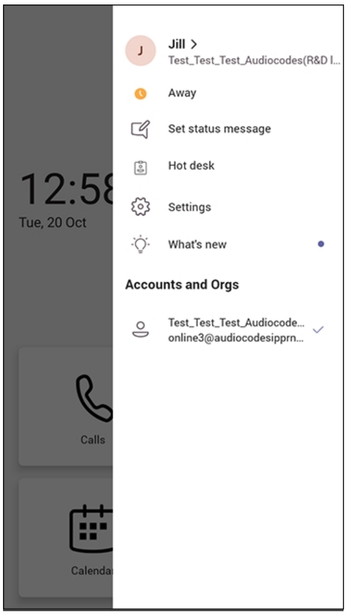
Block calls with no caller ID

Setting Status

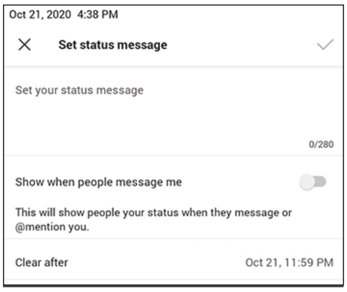
You can set a status message to add more substance to your presence status. For example, a status message such as 'Working from home' adds more substance to the presence status of 'Available'.

➢ To set presence status:

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



2. Select **Set status message**.



Oct 21, 2020 4:38 PM

Set status message

Set your status message

0/280

Show when people message me

This will show people your status when they message or @mention you.

Clear after Oct 21, 11:59 PM

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

Hot Desking

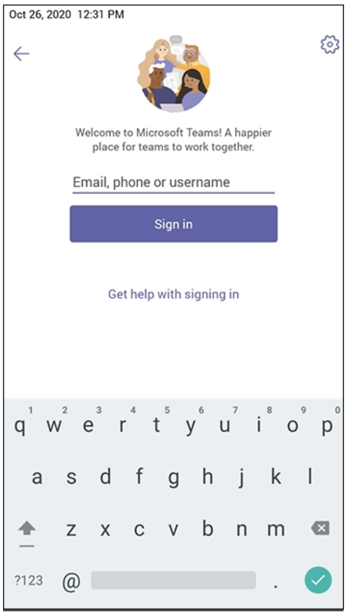
The hot desk feature allows a user to sign in to a phone that is already signed in to by another user without signing out the original user to whom the phone was assigned for primary use.

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

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

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

Figure 4-3: Hot desk



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

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

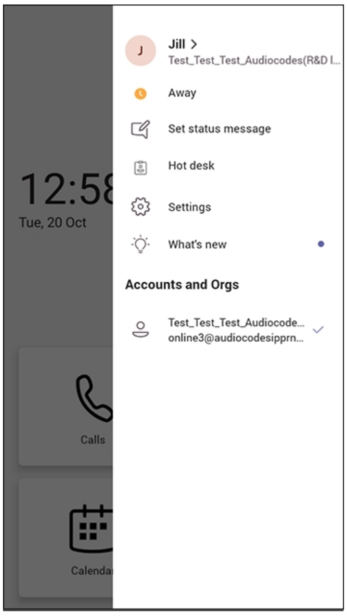
Changing Presence Status

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

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

➢ To change presence status:

1. In the home screen, select the user (avatar) picture or in the Calls and Calendar screen, select ☰.



J Jill >
Test_Test_Test_Audiocodes(R&D I...

Away

Set status message

Hot desk

Settings

What's new

Accounts and Orgs

Test_Test_Test_Audiocode...
online3@audiocodesipprn...

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

Table 4-3: Presence Statuses

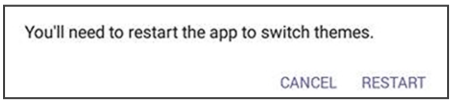
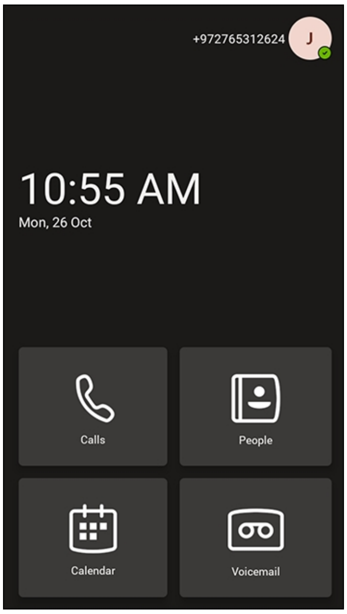
Icon	Presence Status	Description
✅	Available	You're online and available for other contacts to call.
🔴	Busy	You’re busy and don’t want to be interrupted.
⛔	Do not disturb	You don’t want to be disturbed. Stops the phone from ringing when others call you. If DnD is activated, callers hear a tone indicating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

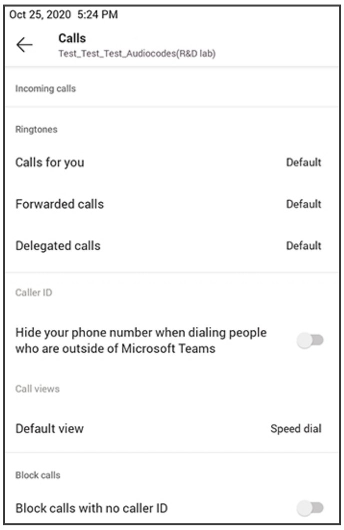
Configuring Teams Application Settings

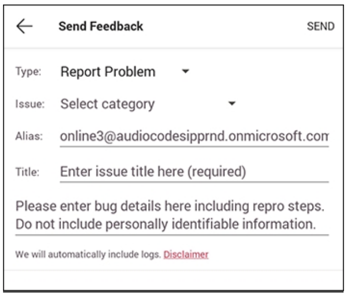
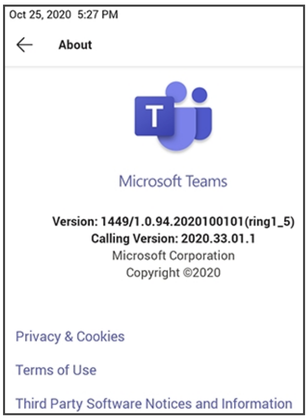
The following describes the Teams application's settings. In the home screen, select the user picture / avatar. Alternatively, in the Calls screen (or People screen, Calendar screen or Voicemail screen), select the phone menu ☰ and then the **Settings** option.

Use this table as reference:

Table 4-4: Idle Screen Description

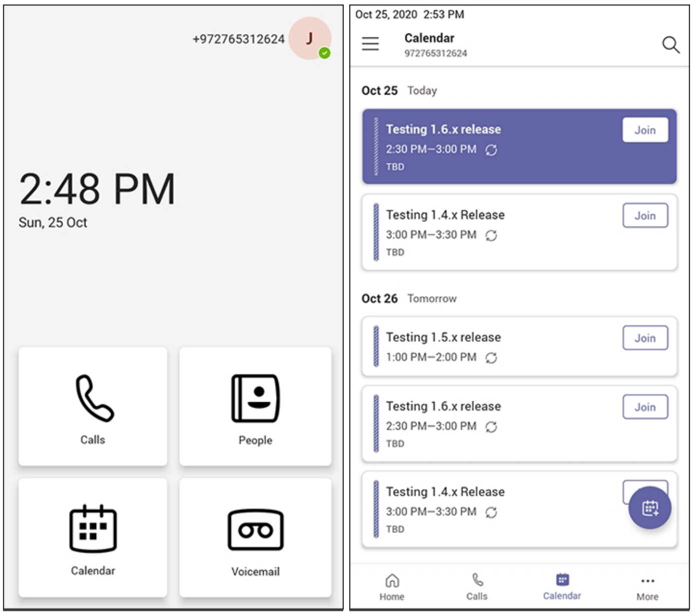
Item	Description
Dark Theme	Dark Theme can be enabled to suit user preference. To enable Dark Theme: **1.** Drag the 'Dark Theme' setting slider to the 'on' position; the following prompt is displayed:  You'll need to restart the app to switch themes. CANCEL RESTART **2.** Choose **Restart** and then verify after the Teams application restarts that all screens (Teams application and Device Settings) are dark themed:  +972765312624 J 10:55 AM Mon, 26 Oct Calls People Calendar Voicemail
Profile	Opens the user's email address and photo / avatar picture.
Calling	Opens the Calls screen.

Item	Description
	 Oct 25, 2020 5:24 PM Calls Test_Test_Test_Audiocodes(R&D lab) Incoming calls Ringtones Calls for you: Default Forwarded calls: Default Delegated calls: Default Caller ID Hide your phone number when dialing people who are outside of Microsoft Teams Call views Default view: Speed dial Block calls Block calls with no caller ID **Incoming Calls** ■ **Call forwarding**. Enables automatically redirecting an incoming call to another destination. ■ **Forward to**. Only displayed if the previous setting is enabled. Defines the destination to which to forward incoming calls. ■ **Also ring**. Only displayed if 'Call forwarding' is disabled. Select either **Off**, **Contact or number**, or **Call group**. ■ **If unanswered**. Only displayed if 'Call forwarding' is disabled. Defines the destination to which to forward unanswered incoming calls. Select either **Off**, **Voicemail**, **Contact or number**, or Call group. **Caller ID** ■ Hide your phone number when dialing people who are outside of Microsoft Teams **Block Calls** **Block calls with no caller ID**. Enables blocking calls that do not have a Caller ID.
Home screen	Default: On (enabled). Slide left to switch off (disable) and block the home screen from view; the Calendar screen takes its place.
Notifications	Default: On (enabled). Allows notifications to be displayed. Slide left to switch off (disable); notifications will not be displayed.
Report an issue	Opens the Send Feedback screen.

Item	Description
	 Send Feedback SEND Type: Report Problem Issue: Select category Alias: online3@audiocodesipprnd.onmicrosoft.com Title: Enter issue title here (required) Please enter bug details here including repro steps. Do not include personally identifiable information. We will automatically include logs. Disclaimer
About	Opens the About screen.  Oct 25, 2020 5:27 PM About Microsoft Teams Version: 1449/1.0.94.2020100101(ring1_5) Calling Version: 2020.33.01.1 Microsoft Corporation Copyright ©2020 Privacy & Cookies Terms of Use Third Party Software Notices and Information
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 60 for detailed information.
Device Settings	Opens the [Device] Settings screen. See Configuring Device Settings on page 17 for detailed information.

Setting up a Meeting

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

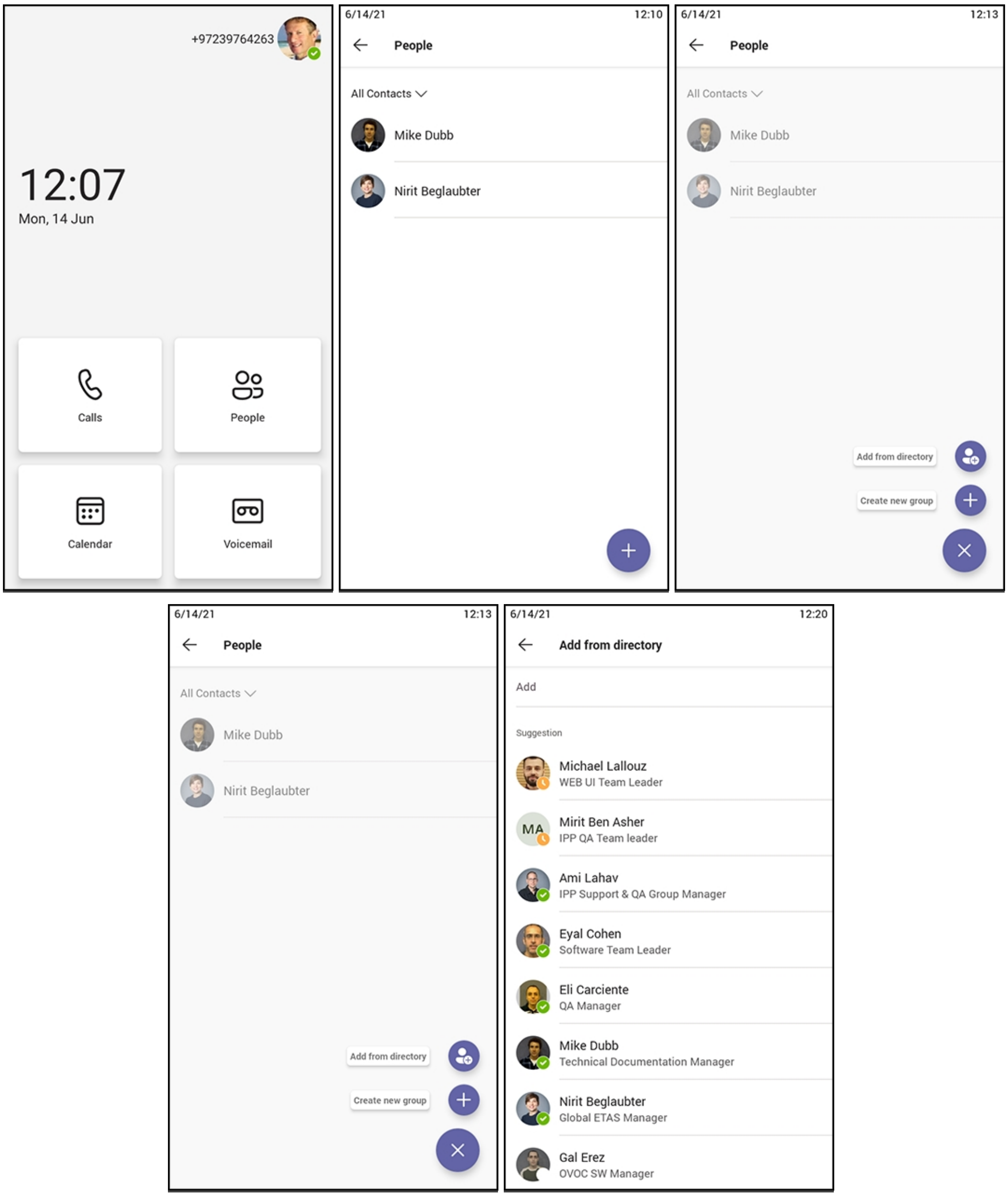


You can join calendered meetings and / or you can select to add a new event to the calendar.

Using the People Screen

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

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



+97239764263

12:07

Mon, 14 Jun

Calls

People

Calendar

Voicemail

6/14/21 12:10

People

All Contacts

Mike Dubb

Nirit Beglaubter

6/14/21 12:13

People

All Contacts

Mike Dubb

Nirit Beglaubter

Add from directory

Create new group

6/14/21 12:13

People

All Contacts

Mike Dubb

Nirit Beglaubter

Add from directory

Create new group

6/14/21 12:20

Add from directory

Add

Suggestion

Michael Lallouz
WEB UI Team Leader

Mirit Ben Asher
IPP QA Team leader

Ami Lahav
IPP Support & QA Group Manager

Eyal Cohen
Software Team Leader

Eli Carciente
QA Manager

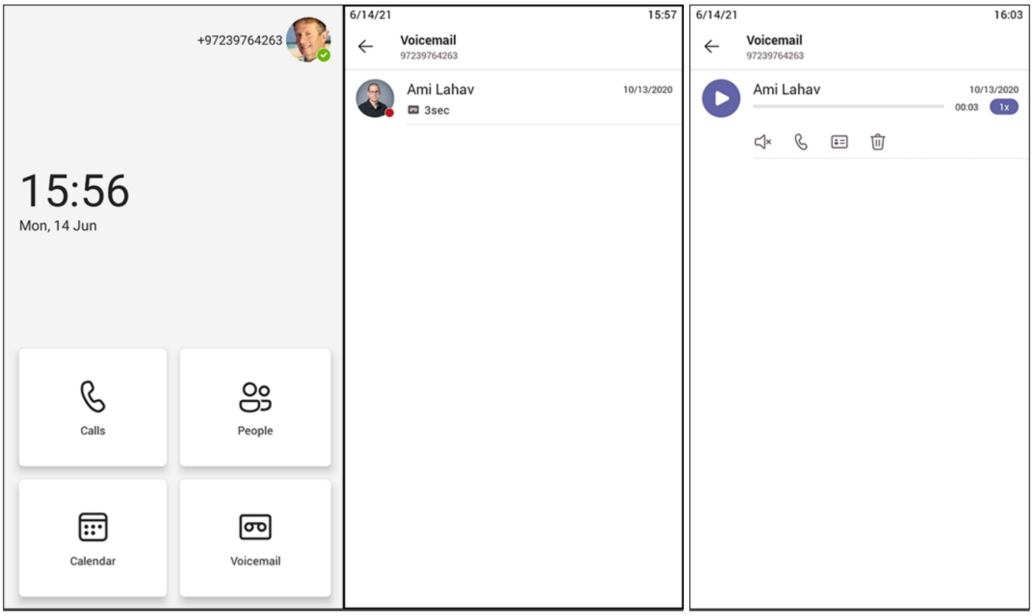
Mike Dubb
Technical Documentation Manager

Nirit Beglaubter
Global ETAS Manager

Gal Erez
OVOC SW Manager

Accessing Voicemail

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



Using Audio Devices

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

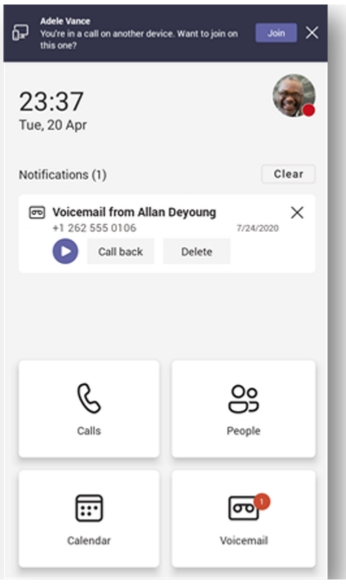
- **Handset**: To make a call or answer a call, lift the handset off the cradle.
- **Speaker** (hands-free mode)
  - To activate it, press the speaker key during a call or when making a call.
  - To deactivate it, press the speaker key again.
- **Headset** (hands-free mode). When talking on the phone,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

You can easily change audio device during a call.

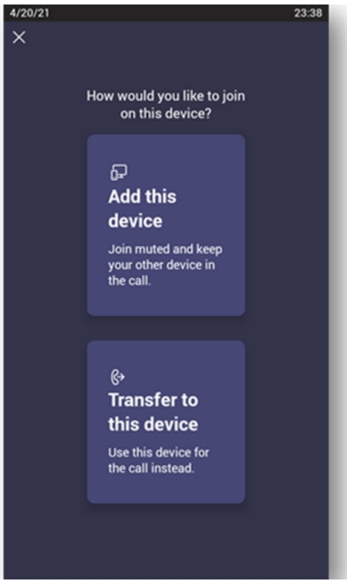
- **To change from speaker/headset to handset**: Activate speaker/headset and pick up the handset; the speaker/headset is automatically disabled.
- **To change from handset to speaker/headset**: Off-hook the handset and press the speaker/headset key to activate the speaker/headset. Return the handset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

Transferring Calls and Meetings across Devices

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



Adele Vance
You're in a call on another device. Want to join on this one?



How would you like to join on this device?

Add this device

Join muted and keep your other device in the call.

Transfer to this device

Use this device for the call instead.

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

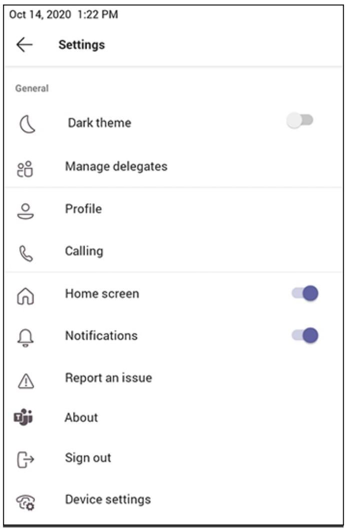
Signing Out

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

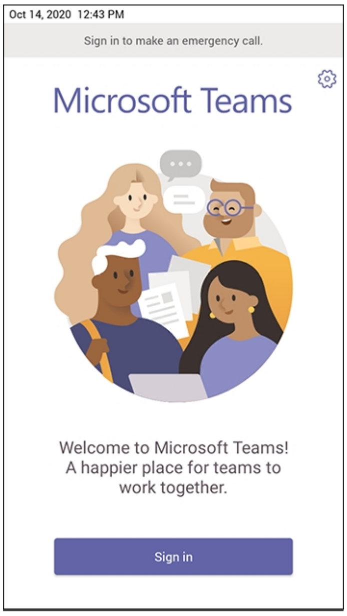
➢ To sign out:

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

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



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



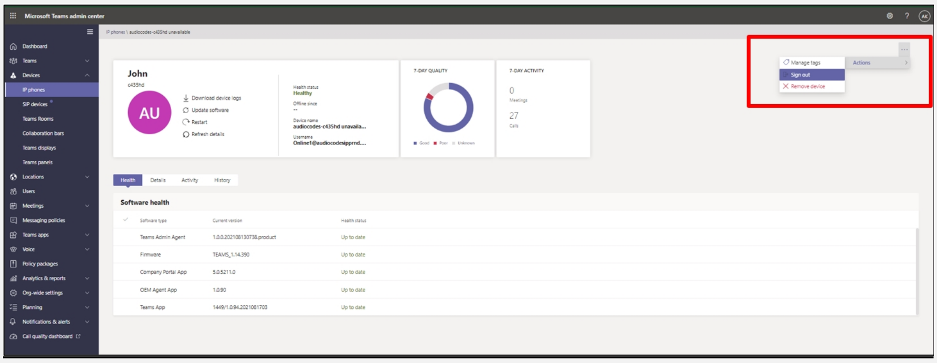
Oct 14, 2020 12:43 PM

Sign in to make an emergency call.

Microsoft Teams

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

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



IP phones \ audiocodes-c435hd unavailable

John
c435hd

AU

Health status
Healthy

Offline since
--

Device name
audiocodes-c435hd unavaila...

Username
Online1@audiocodesipprnd....

7-DAY ACTIVITY

0
Meetings

27
Calls

Software health

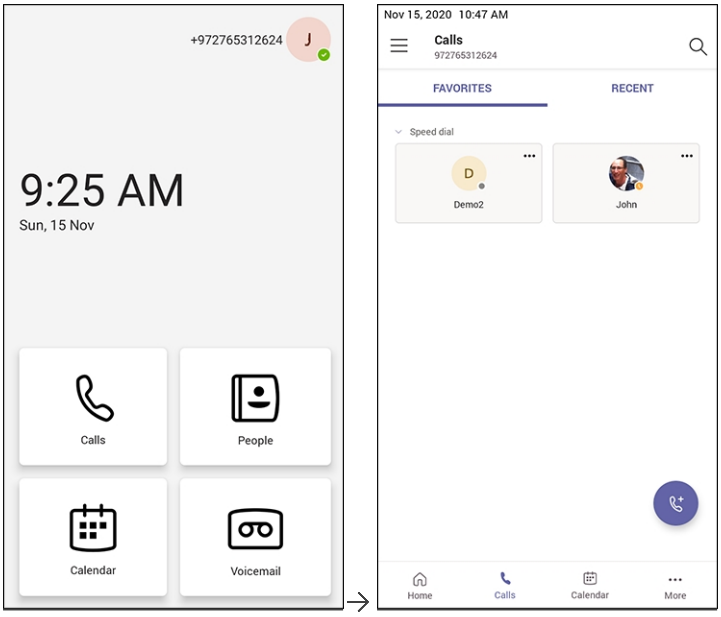
Software type	Current version	Health status
Teams Admin Agent	1.0.0.202108130738.product	Up to date
Firmware	TEAMS_1.14.390	Up to date
Company Portal App	5.0.5211.0	Up to date
OEM Agent App	1.0.90	Up to date
Teams App	1449/1.0.94.2021081703	Up to date

5 Performing Teams Call Operations

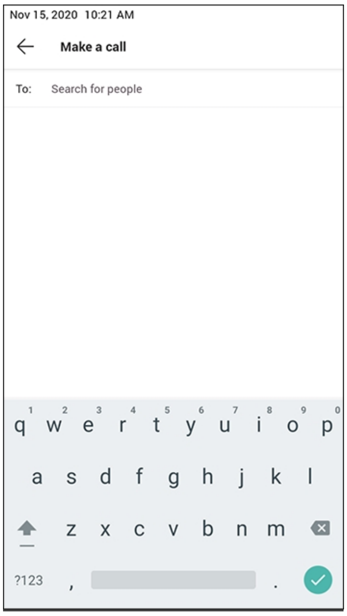
The following documentation shows how to perform basic operations with the phone.

Making a Call

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



In the Calls screen that opens, touch ☎.



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

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

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

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

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

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

- Touch 🔊 on the phone.

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

- Touch ☎

➢ **To dial a URL:**

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

Dialing a Missed Call

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

➢ **To dial a missed call:**

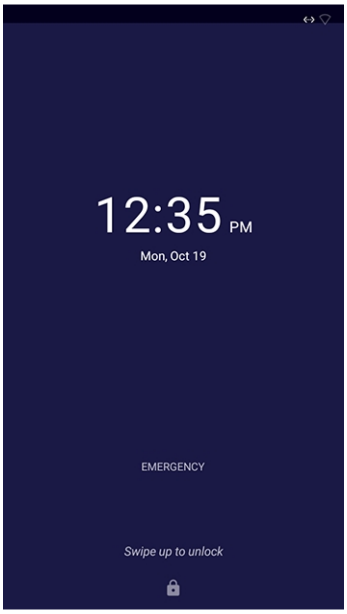
- Select **Calls** and then in the Calls screen under the **Recent** tab, scroll to the missed call to dial if there is more than one listed.
- Select ✆ adjacent to the missed call.

Select to Dial

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

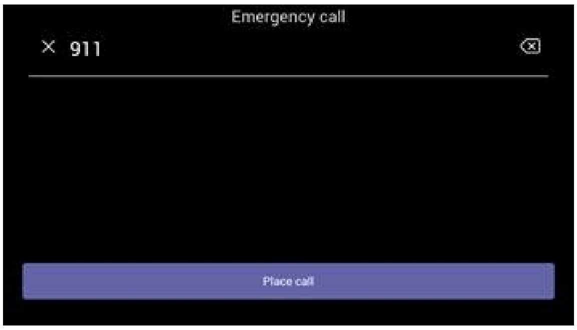
Making an Emergency Call

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



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

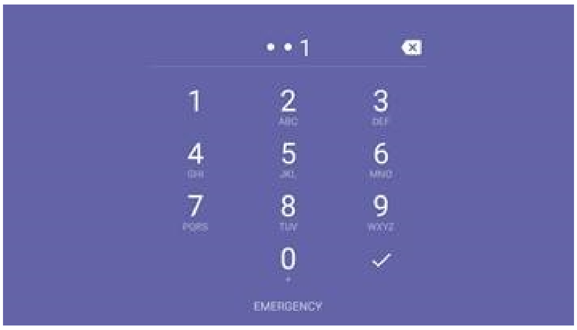
- Select the **EMERGENCY** softkey shown in the preceding figure of the locked idle screen and then enter the emergency number.



-OR-

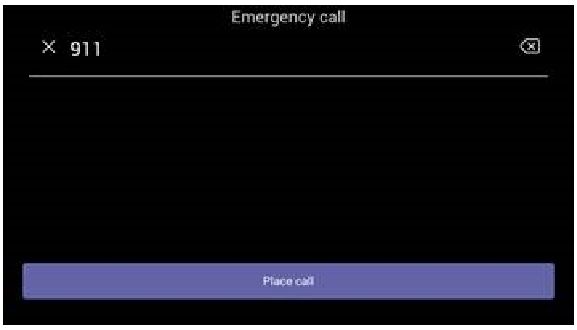
- Dial from the locked idle screen without needing to use the **EMERGENCY** key:

a. Dial **911**.



b. Activate the speaker button on the phone.

c. View the ‘Emergency call’ screen displaying the dialed emergency number.



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

Answering Calls

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

➢ **To answer:**

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

Ending an Established Call

You can end an established call in a few ways.

➢ **To end an established call:**

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

Managing Calls

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

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

➢ **To manage calls:**

1. Select **Calls** and in the Calls screen, select **Recent**.

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

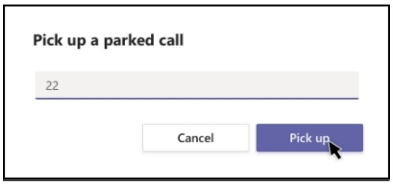
2. Select a call in the list and then select ☎ to call someone back.

Parking a Call

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

➢ To park a call:

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



Pick up a parked call

22

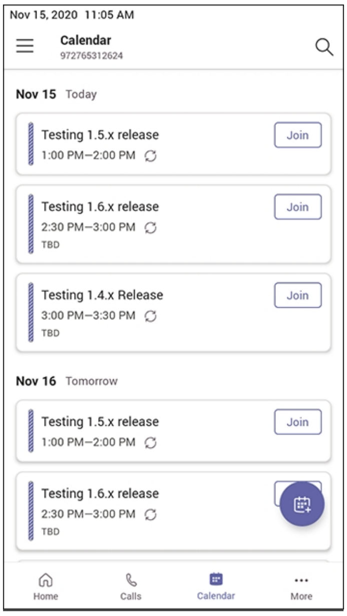
3. The user on the other device enters the code communicated to them and then selects the **Pick up** button to pick up the call.

Managing Teams Meetings

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

➢ To manage conference meetings:

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



Nov 15, 2020 11:05 AM

Calendar
972765312624

Nov 15 Today

Testing 1.5.x release
1:00 PM–2:00 PM
Join

Testing 1.6.x release
2:30 PM–3:00 PM
TBD
Join

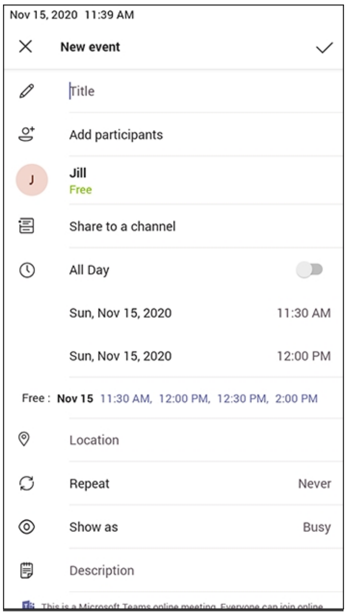
Testing 1.4.x Release
3:00 PM–3:30 PM
TBD
Join

Nov 16 Tomorrow

Testing 1.5.x release
1:00 PM–2:00 PM
Join

Testing 1.6.x release
2:30 PM–3:00 PM
TBD

2. Touch the 📅 icon.



Nov 15, 2020 11:39 AM

New event

Title

Add participants

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

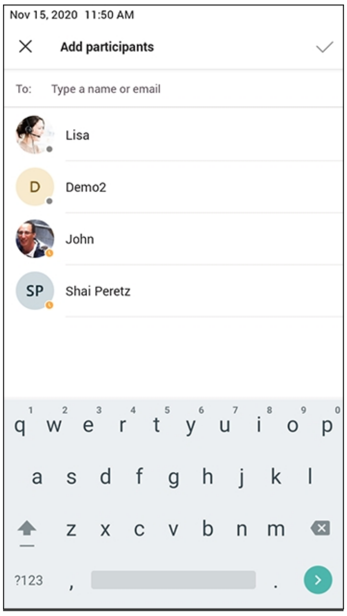
Show as Busy

Description

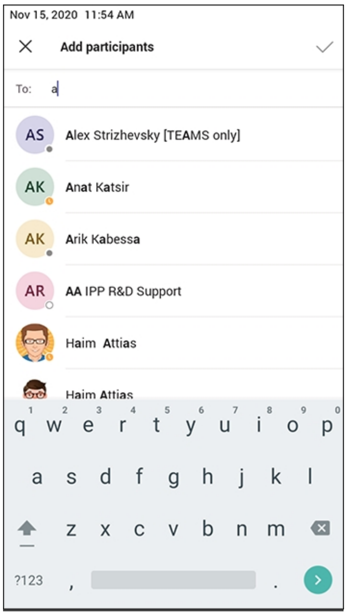
This is a Microsoft Teams online meeting. Everyone can join online

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.



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



6. Touch an entry in the list and then touch ›; the participant is added to the meeting.

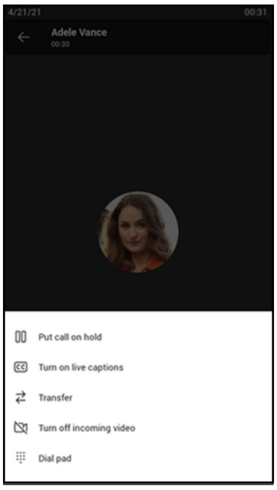
7. Define 'Share to a channel', date, date and time, 'Location', 'Show as' and provide a 'Description' of the meeting to facilitate effective management later.

8. Touch the ✓ icon; the meeting is calendarized.

Using Live Captions

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

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



For more information, see here.

Raising a Hand During a Meeting

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

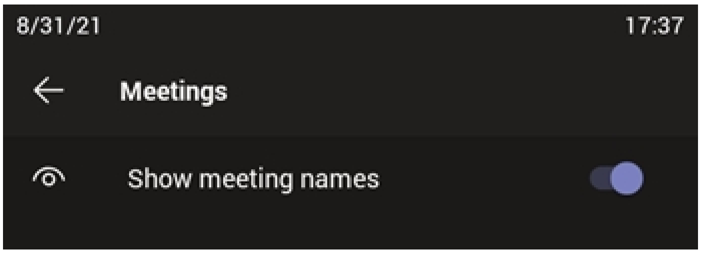
For more information, see here.

Hiding Names and Meeting Titles for Individual Devices

Names and meeting titles can be hidden for individual devices.

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

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


8/31/21 17:37

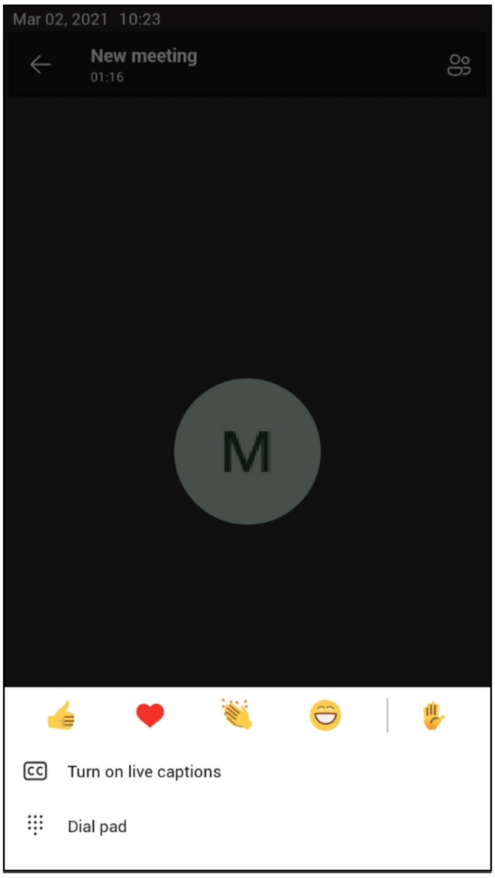
Meetings

Show meeting names

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

Reacting During a Meeting

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



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

Transferring a Call to Frequent Contacts

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

Transferring a Call to Work Voicemail

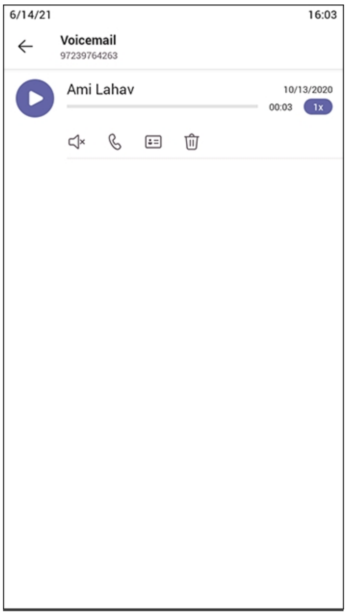
Users can directly transfer a call into someone's work voicemail without needing to ring the far-end user. This allows them to discreetly leave voicemails for users without interrupting them.

Viewing and Playing Voicemail Messages

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

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

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



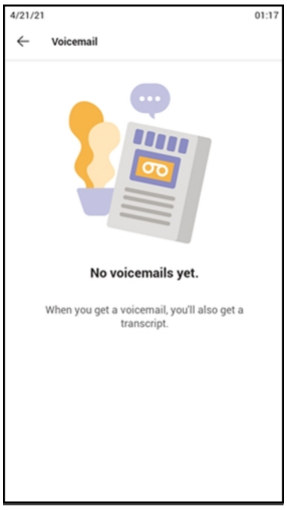
6/14/21 16:03

Voicemail
97239764263

Ami Lahav 10/13/2020
00:03 1x

2. Scroll down to select from the list of messages (if there are voicemail messages in your box) which message to **Play**, **Call** or **Delete**.

3. You'll view the following screen if you don't yet have any voicemail messages:



4/21/21 01:17

Voicemail

No voicemails yet.

When you get a voicemail, you'll also get a transcript.

For more information, see here.

Rejecting an Incoming Call, Sending it Directly to Voicemail

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

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

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

Adjusting Volume

The phone allows

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

For more information about sound and volume, see here.

Adjusting Ring Volume

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

➢ **To adjust ring volume:**

1. When the phone is in idle state, 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, activate the speaker key on the phone.
2. Touch **+** or **-**; the volume bar is displayed on the screen. After adjusting the volume, the volume bar disappears from the screen.

Adjusting Headset Volume

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

➢ **To adjust the headset volume:**

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

Playing Incoming Call Ringing through USB Headset

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

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

■ Configure the following parameter:

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

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

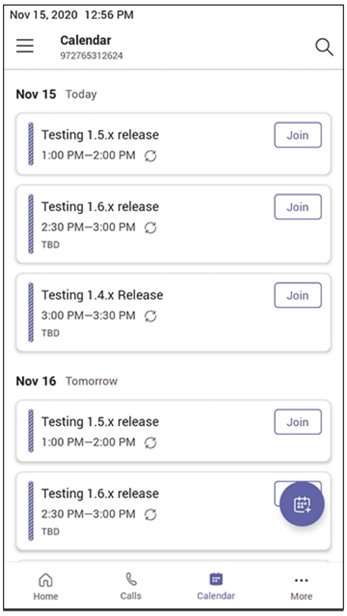
Using the Phone as a USB Speaker

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

⚠ For more information, see the *Device Duo Application Note for Personal Use*.

Viewing and Joining Meetings

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



Nov 15, 2020 12:56 PM

Calendar
972765312624

Nov 15 Today

Testing 1.5.x release
1:00 PM–2:00 PM
Join

Testing 1.6.x release
2:30 PM–3:00 PM
TBD
Join

Testing 1.4.x Release
3:00 PM–3:30 PM
TBD
Join

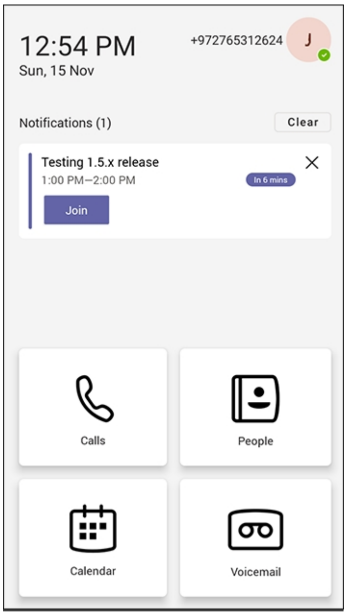
Nov 16 Tomorrow

Testing 1.5.x release
1:00 PM–2:00 PM
Join

Testing 1.6.x release
2:30 PM–3:00 PM
TBD

➢ To view the details of a meeting:

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



12:54 PM
Sun, 15 Nov
+972765312624

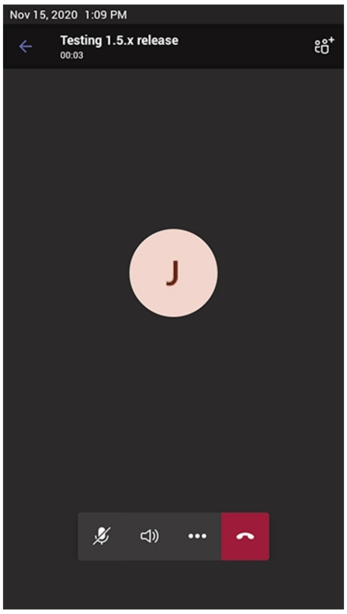
Notifications (1) Clear

Testing 1.5.x release
1:00 PM–2:00 PM
In 6 mins
Join

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

➢ To join a meeting:

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



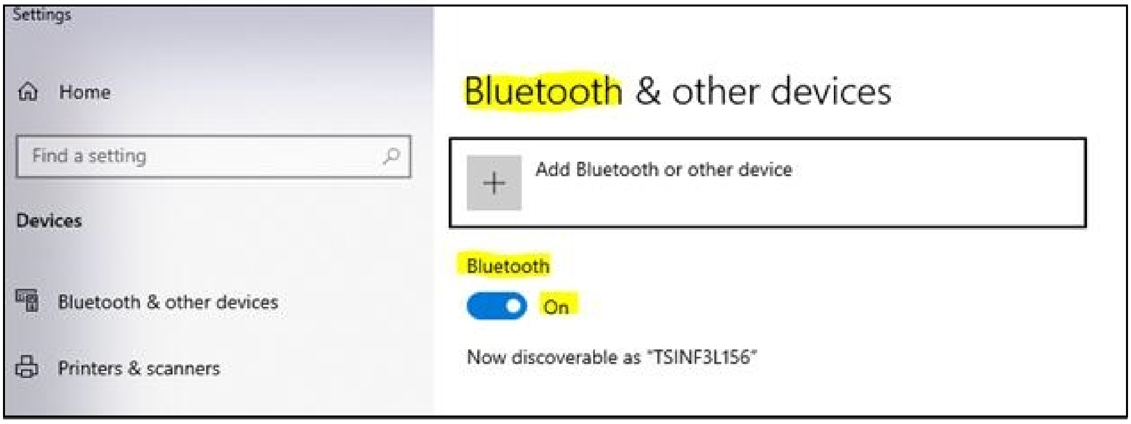
Better Together over Bluetooth

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

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

➢ To set up Bluetooth on the PC side:

1. Enable Bluetooth on your PC.


Settings

Home

Find a setting

Devices

Bluetooth & other devices

Printers & scanners

Bluetooth & other devices

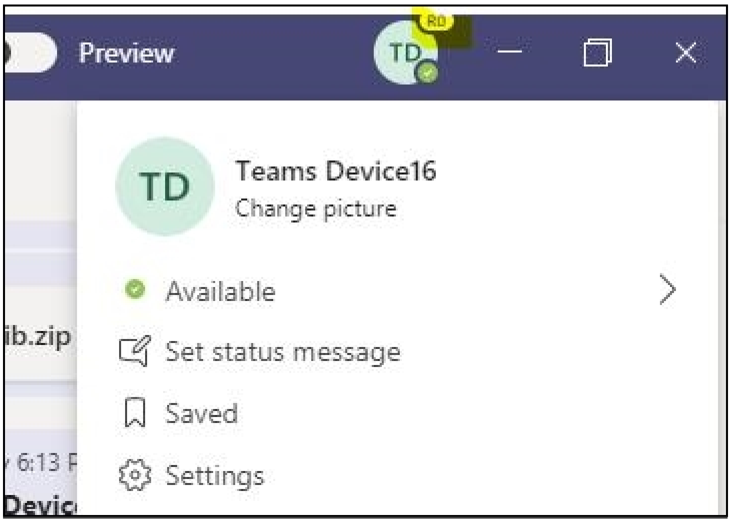
Add Bluetooth or other device

Bluetooth

On

Now discoverable as "TSINF3L156"

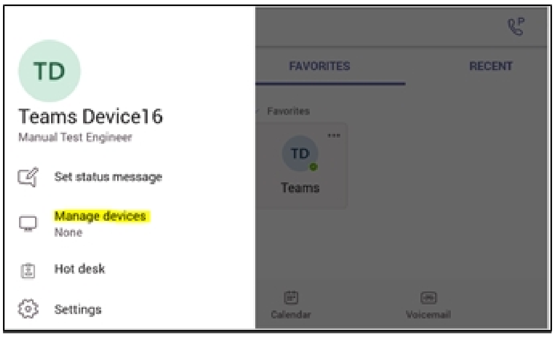
2. Install Teams PC Client on the PC.
3. Sign in to the Teams PC Client with your account (it's necessary to sign in with the same accounts to both the Teams PC Client and to the device).



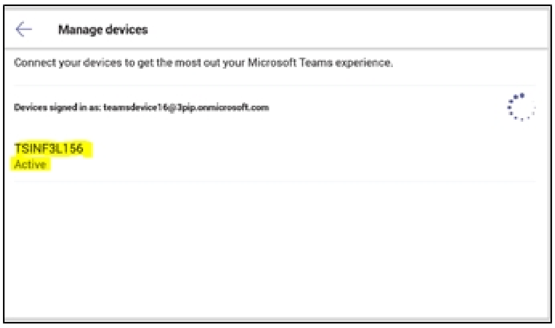
➢ To set up Bluetooth on the device side:

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.

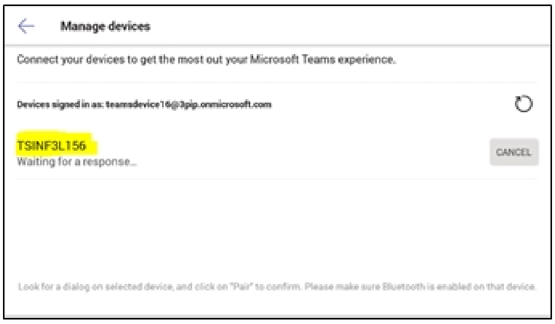

Manage devices

Connect your devices to get the most out your Microsoft Teams experience.

Devices signed in as: teamsdevice16@3pip.onmicrosoft.com

TSINF3L156
Active

4. Pair the device with your PC.



Manage devices

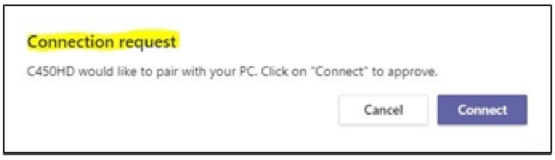
Connect your devices to get the most out your Microsoft Teams experience.

Devices signed in as: teamsdevice16@3pip.onmicrosoft.com

TSINF3L156
Waiting for a response...

Look for a dialog on selected device, and click on "Pair" to confirm. Please make sure Bluetooth is enabled on that device.

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

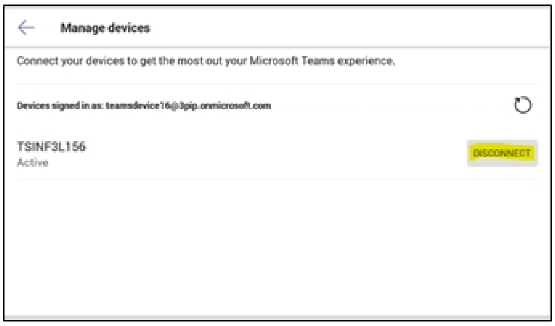


Connection request

C450HD would like to pair with your PC. Click on "Connect" to approve.

6. Accept the notification from PC.

7. Check the device and make sure pairing was successful:



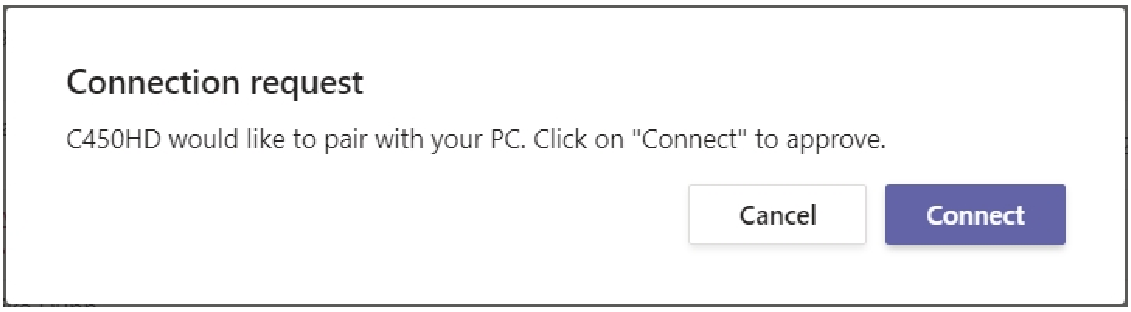
Manage devices

Connect your devices to get the most out your Microsoft Teams experience.

Devices signed in as: teamsdevice16@3pip.onmicrosoft.com

TSINF3L156
Active

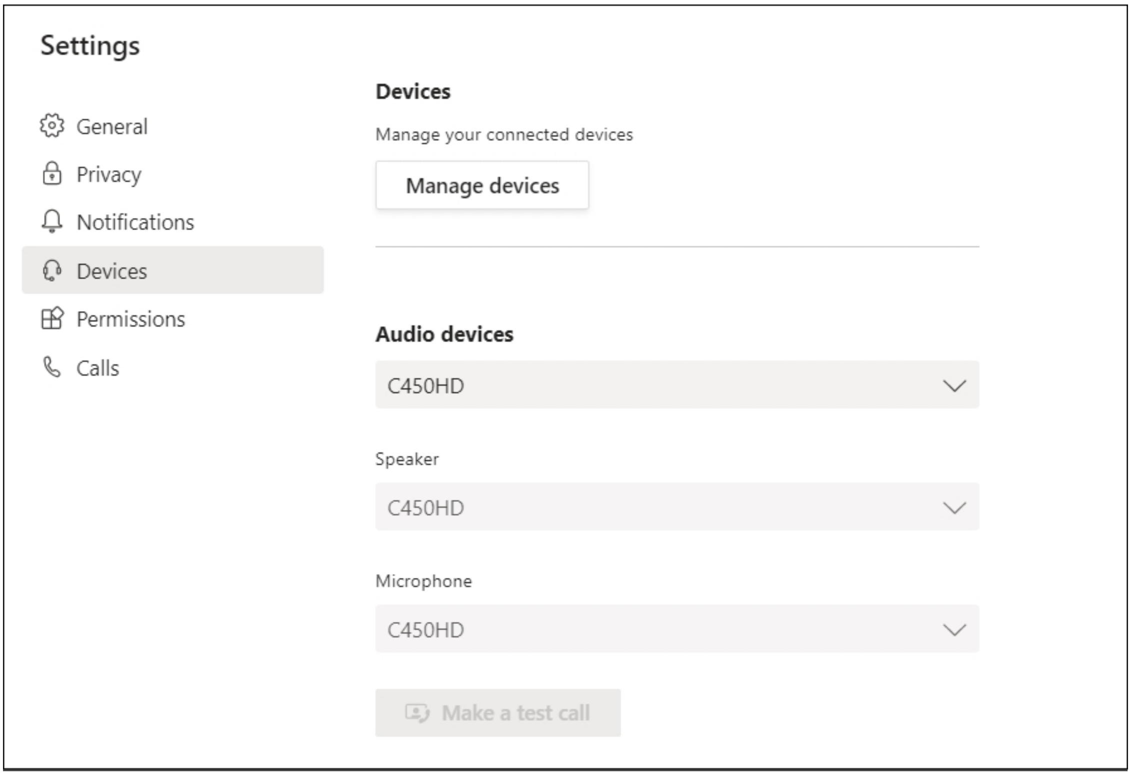
8. When pairing the phone with the PC Client, the PC Client presents the following request for approval:



Connection request

C450HD would like to pair with your PC. Click on "Connect" to approve.

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



Audio devices: C450HD

Speaker: C450HD

Microphone: C450HD

6 Performing Administrator-Related Operations

Network administrators can:

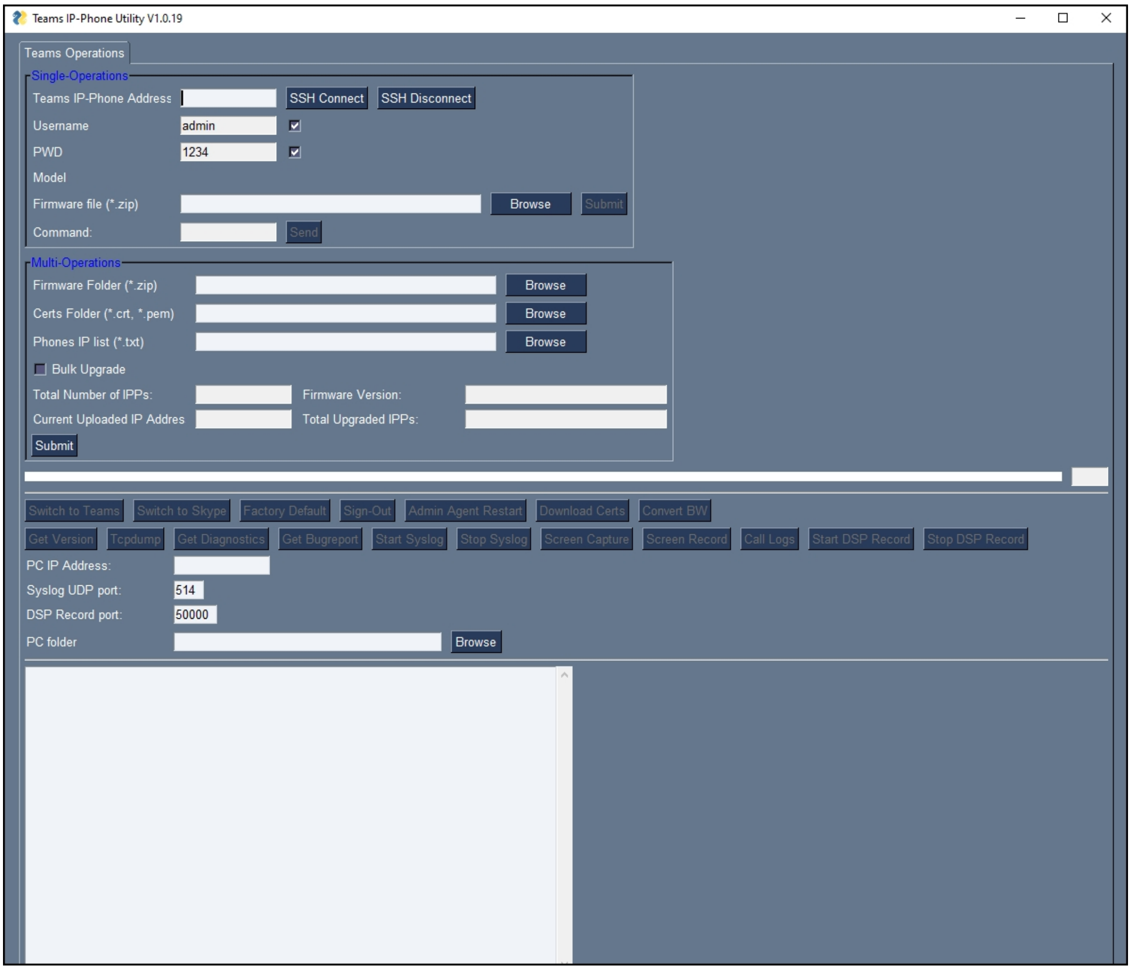
- Updating Phone Firmware Manually below
- Manually Performing Recovery Operations on page 83
- Removing Devices from Intune Management on page 84
- Updating Microsoft Teams Devices Remotely on page 92
- Managing Phones with the Device Manager on page 92

Updating Phone Firmware Manually

AudioCodes' Teams IP Phone Utility allows network administrators to manually update a phone's firmware.

➢ To manually update a phone's firmware:

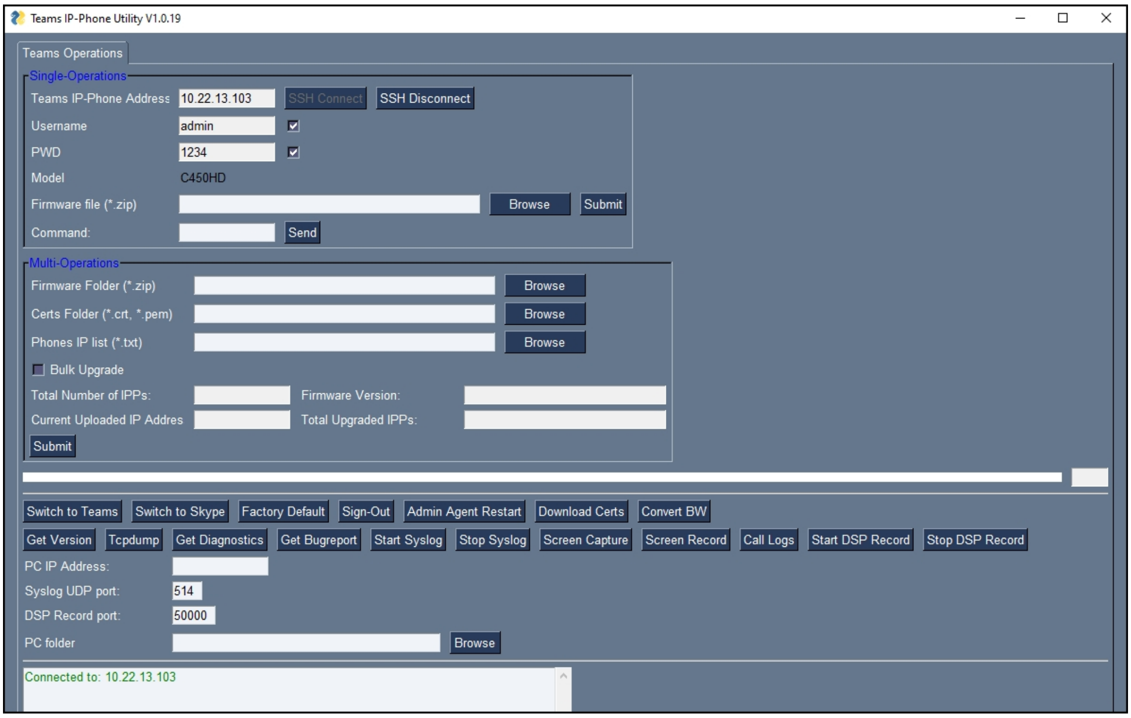
1. From the PC's **Start** menu, select the app icon or click the application's exe file in the folder in which you saved it.



Username: admin ☑
PWD: 1234 ☑
Syslog UDP port: 514
DSP Record port: 50000

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

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



Teams IP-Phone Utility V1.0.19

Teams IP-Phone Address: 10.22.13.103

Username: admin ☑

PWD: 1234 ☑

Model: C450HD

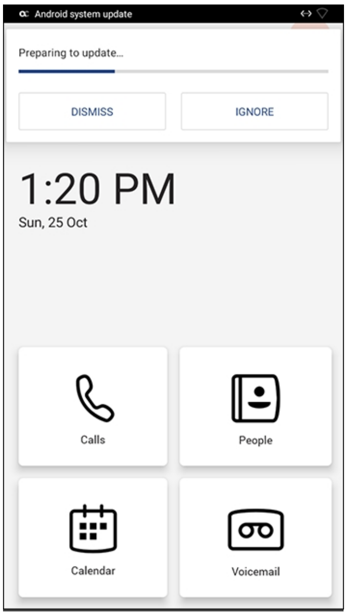
Syslog UDP port: 514

DSP Record port: 50000

Connected to: 10.22.13.103

4. Under the Operations section of the screen next to the field 'Firmware file', click the **Browse** button and navigate to and select the candidate image file.

5. Click the **Submit** button; a firmware upgrade process starts; the phone is automatically rebooted; a notification pops up when the process finishes. The phone notifies you that it's being updated and rebooted.



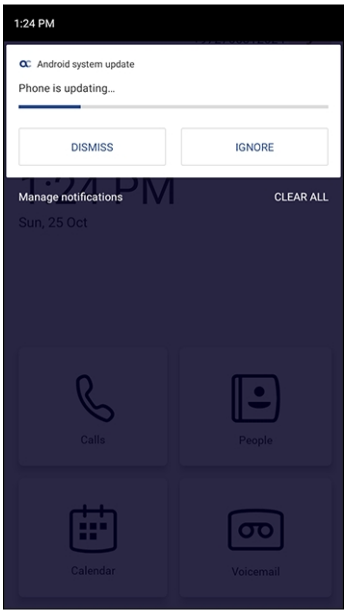
Android system update

Preparing to update...

1:20 PM

Sun, 25 Oct

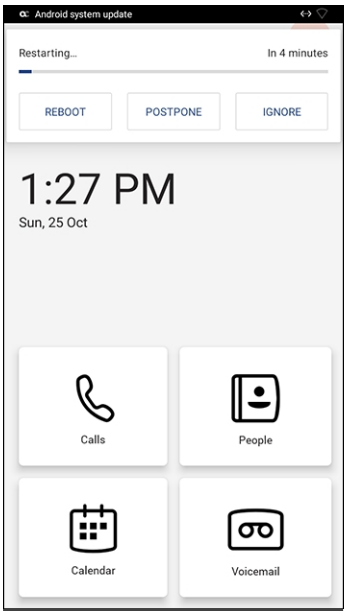
6. Swipe down twice in rapid succession to present the **Manage notifications** option.



7. Touch **Manage notifications**; the screen that is then displayed allows viewing notifications such as:

- Upgrade state (Preparing, updating, etc.)
- Internet access issues

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



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

Downloading 802.1x Certificates

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

802.1x certificates can be downloaded using AudioCodes'

- Device Manager (see the *Device Manager Administrator's Manual*)
- Teams IP Phone Utility on page 99

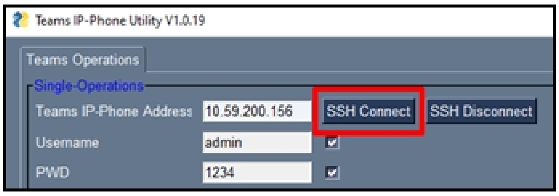
> ⚠
> - The client certificate files must be named **dot1x_cert.crt** and **dot1x_pkey.key**
> - The CA certificate file must be named **factory_ca.pem**

AudioCodes Teams IP Phone Utility

802.1x certificates can be downloaded using AudioCodes' Teams IP Phone Utility.

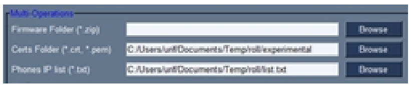
➢ **To download certificates to a single Teams device:**

1. In the Teams IP Phone Utility (see Teams IP Phone Utility on page 99 for detailed information about the application), enter the phone's IP address and click **SSH Connect**.



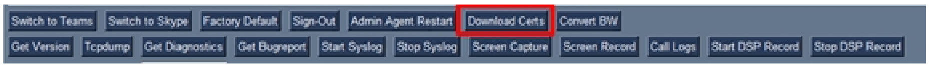
Teams IP-Phone Address 10.59.200.156
Username admin ☑
PWD 1234 ☑

2. Click theBrowse button next to the field 'Certs Folder' and navigate to and select the certificate file to download.



Firmware Folder (*.zip)
Certs Folder (*.crt, *.pem) C:/Users/unf/Documents/Temp/roll/experimental
Phones IP list (*.txt) C:/Users/unf/Documents/Temp/roll/list.txt

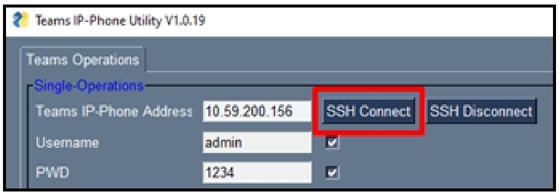
3. Click **Download Certs** to add the certificate.



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

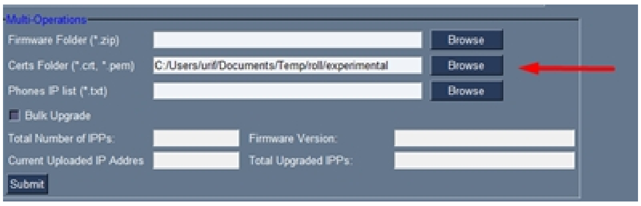
➢ **To download certificates to multiple Teams devices:**

1. In the Teams IP Phone Utility (see Teams IP Phone Utility on page 99 for more information), enter the phone's IP address and click **SSH Connect**.



Teams IP-Phone Address 10.59.200.156
Username admin ☑
PWD 1234 ☑

2. Click theBrowse button next to the field 'Certs Folder' under Multi Operations and then navigate to and select the certificate files to download.



Multi-Operations

Firmware Folder (*.zip)

Certs Folder (*.crt, *.pem) C:/Users/uril/Documents/Temp/roll/experimental

Phones IP list (*.txt)

□ Bulk Upgrade

Total Number of IPPs:

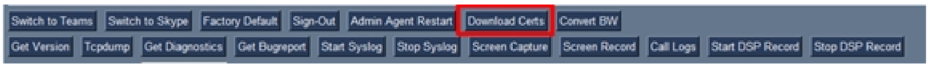
Firmware Version:

Current Uploaded IP Addres

Total Upgraded IPPs:

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

4. Click the now activated **Download Certs** button to add the certificates to the phones.



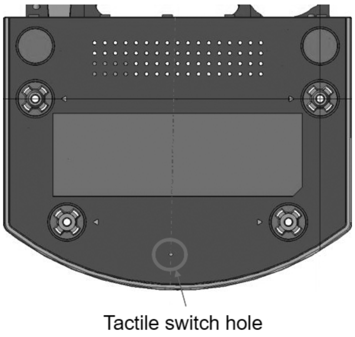
5. After a short period, view in the results pane 'Certs Successfully Installed'.

Manually Performing Recovery Operations

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

All AudioCodes devices 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 (for phones *without* hard digits, e.g., C470HD) -OR- by using a two-key combination (for phones *with* hard digits, e.g., C455HD).

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.

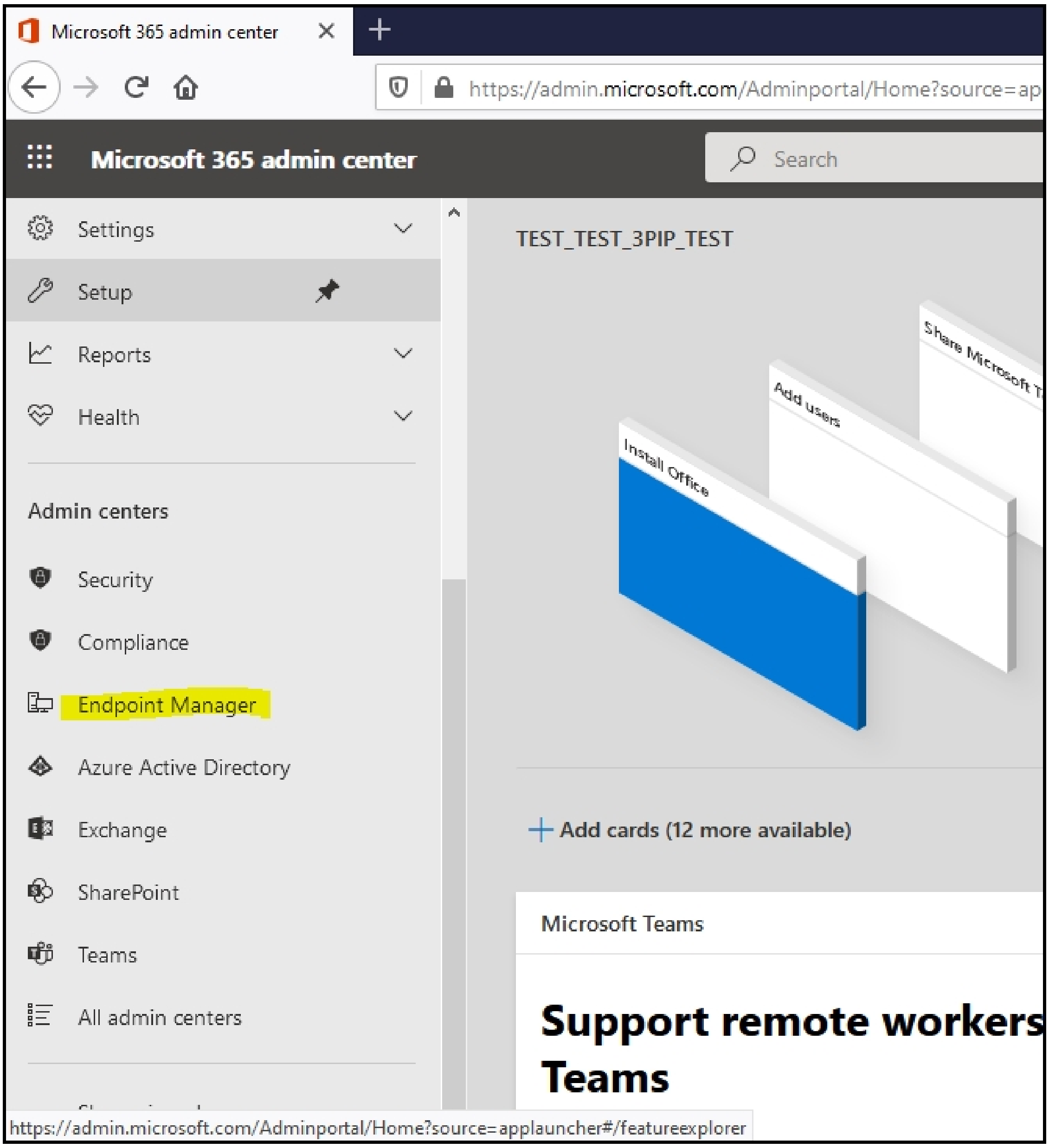
When?	Action	Press for how long?	Press key combination	LED flashes 3x after release
Start pressing immediately after power up (on U-Boot / Universal Boot Loader)	Recovery mode (you can restore defaults from there)	~ 4 seconds	Back key + **MENU** key (3 seconds)	Red
	Switch slots A / B	~ 10 seconds	**4** key + **6** key (3 seconds)	Green
	Loader	~ 15 seconds	**1** key + **3** key (3 seconds)	Blue / Yellow
	Switch Skype for Business to Android (and vice versa)	~ 20 seconds	Back key + **OK** key (3 seconds)	Red + Green
	Restore defaults	~25 seconds	**OK** key + **MENU** key (3 seconds)	Green + blue / Green + yellow
When successfully booted (on Android)	Reboot	Takes ~ 4 seconds	From the 'Admin' menu	-
	Restore defaults	Takes ~15 seconds	Long-press **Hold** key	Flashes yellow once after release

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.

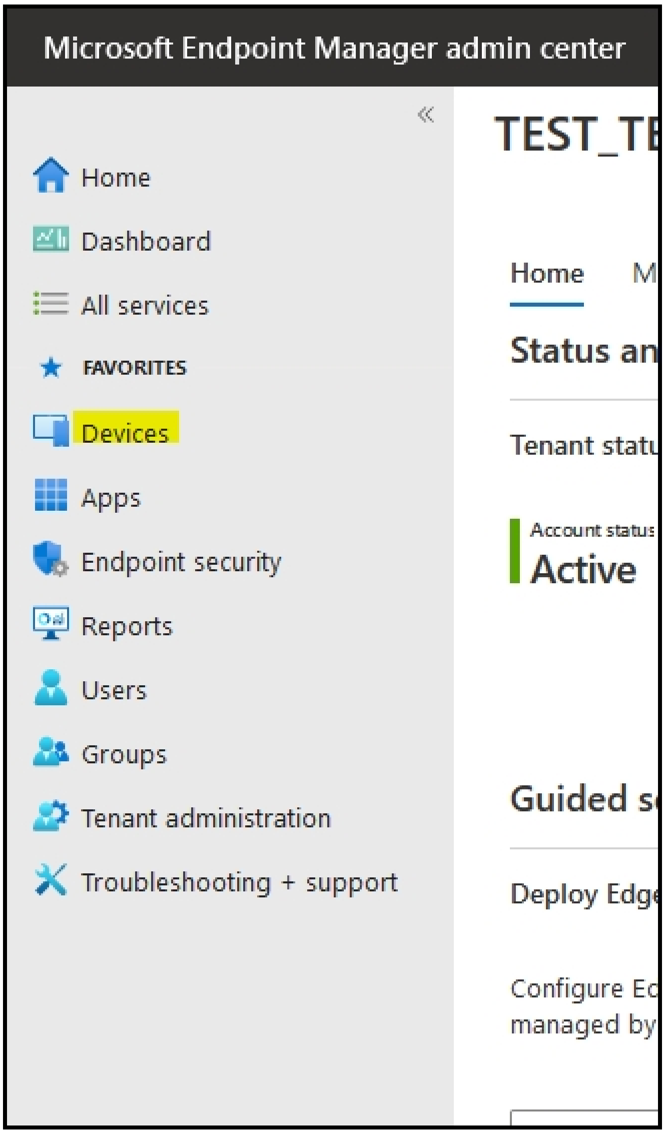
➢ To remove devices from Intune:

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

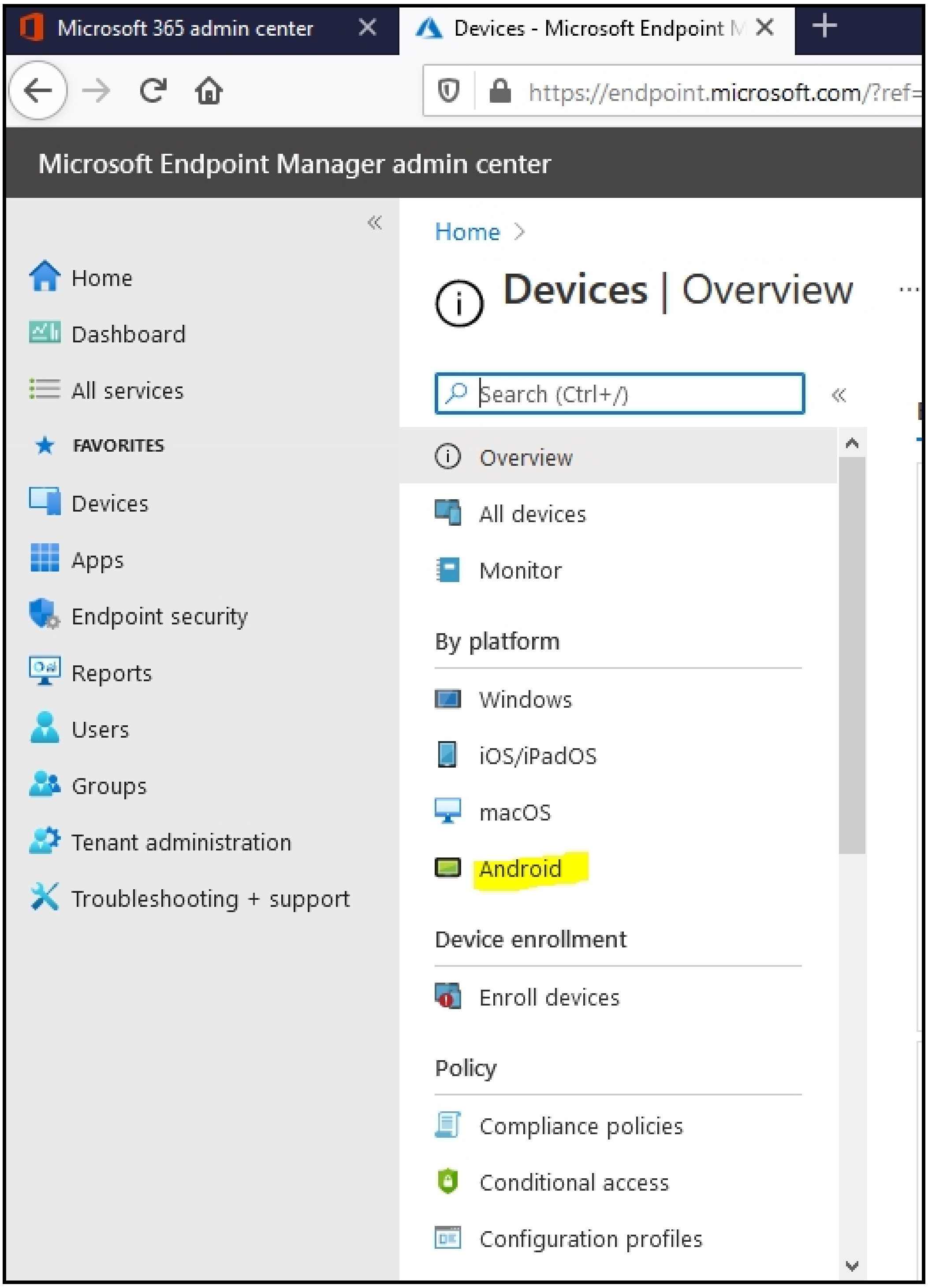


⚠ The Endpoint Manager service is licensed according to individual terms. Consequently, not all network administrators will be able to navigate to it. Check if the license you're using includes the service or not.

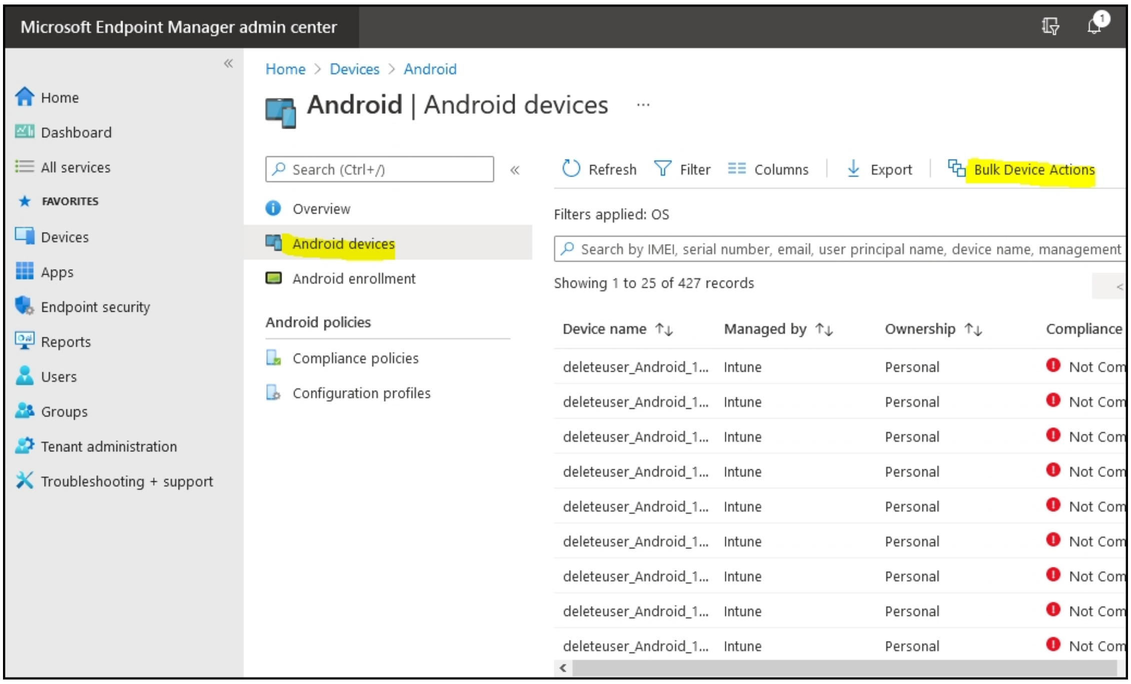
3. Click **Devices**.



4. Click **Android**.



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

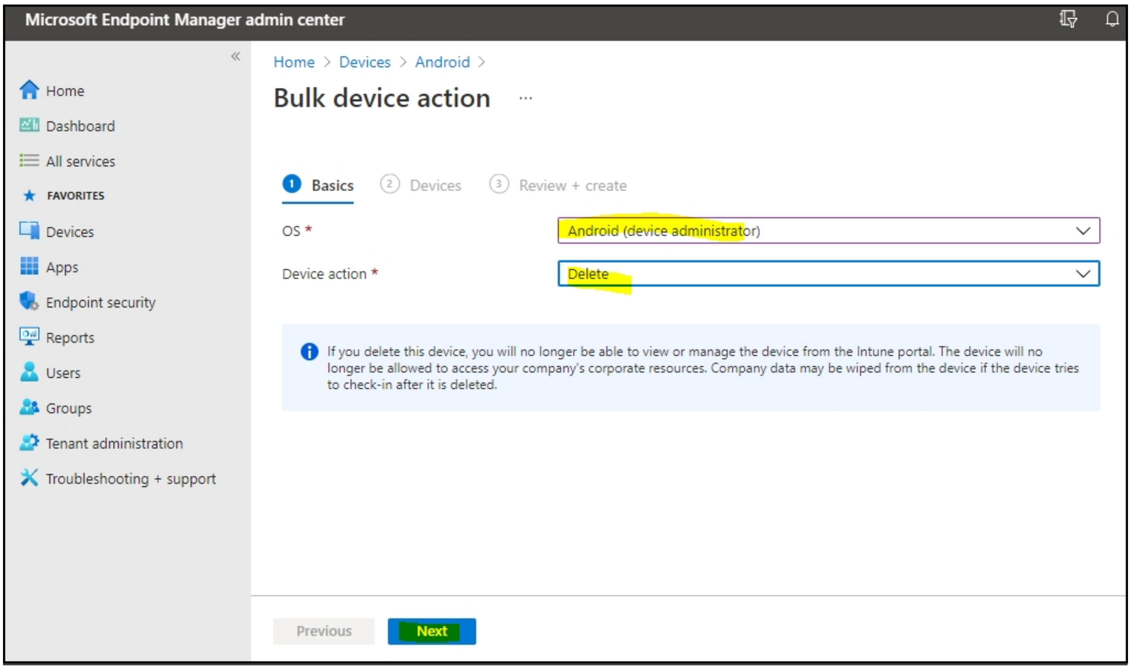


Filters applied: OS

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 **Next**.

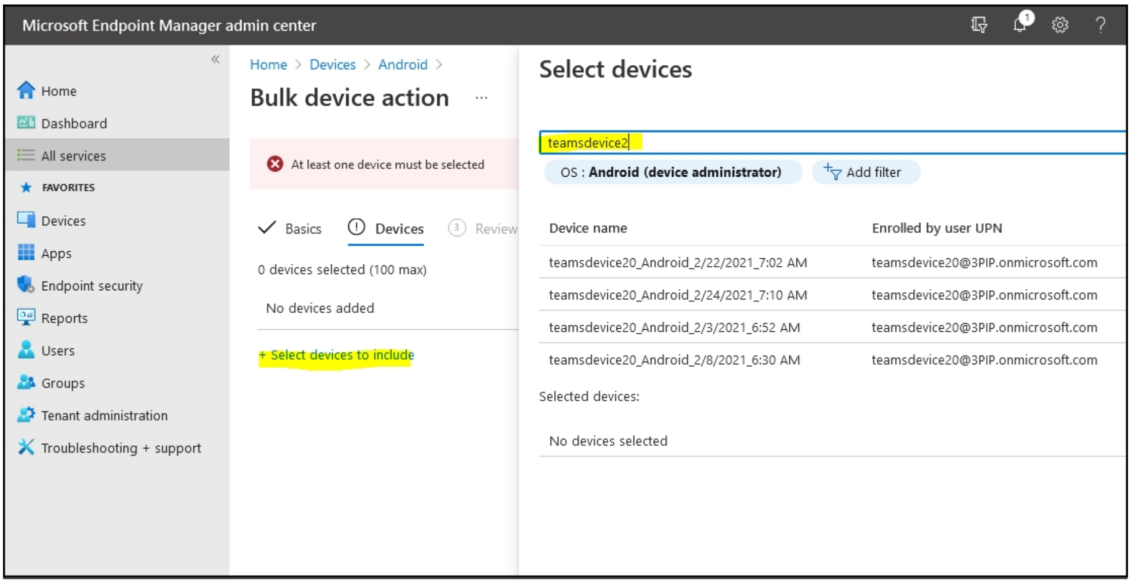


OS * Android (device administrator)

Device action * Delete

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.

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



Microsoft Endpoint Manager admin center

Home > Devices > Android >

Bulk device action

At least one device must be selected

0 devices selected (100 max)

No devices added

+ Select devices to include

Select devices

teamsdevice2

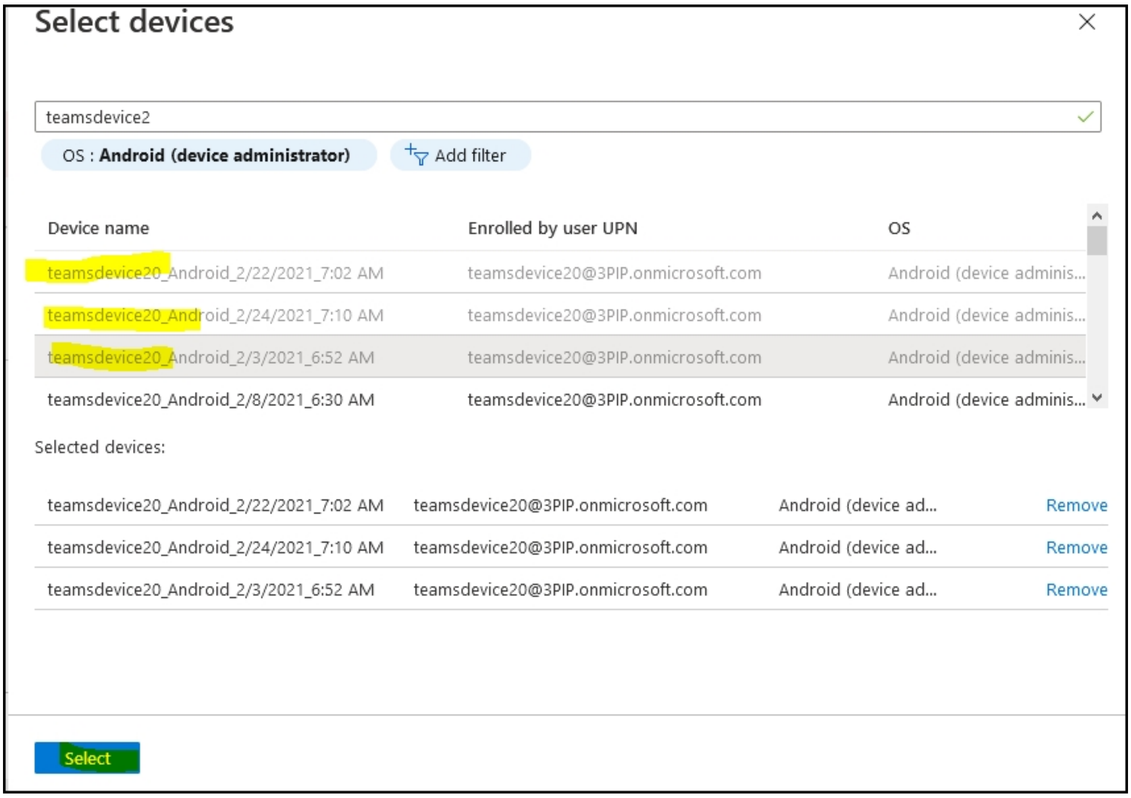
OS : **Android (device administrator)** Add filter

Device name	Enrolled by user UPN
teamsdevice20_Android_2/22/2021_7:02 AM	teamsdevice20@3PIP.onmicrosoft.com
teamsdevice20_Android_2/24/2021_7:10 AM	teamsdevice20@3PIP.onmicrosoft.com
teamsdevice20_Android_2/3/2021_6:52 AM	teamsdevice20@3PIP.onmicrosoft.com
teamsdevice20_Android_2/8/2021_6:30 AM	teamsdevice20@3PIP.onmicrosoft.com

Selected devices:

No devices selected

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



Select devices

teamsdevice2

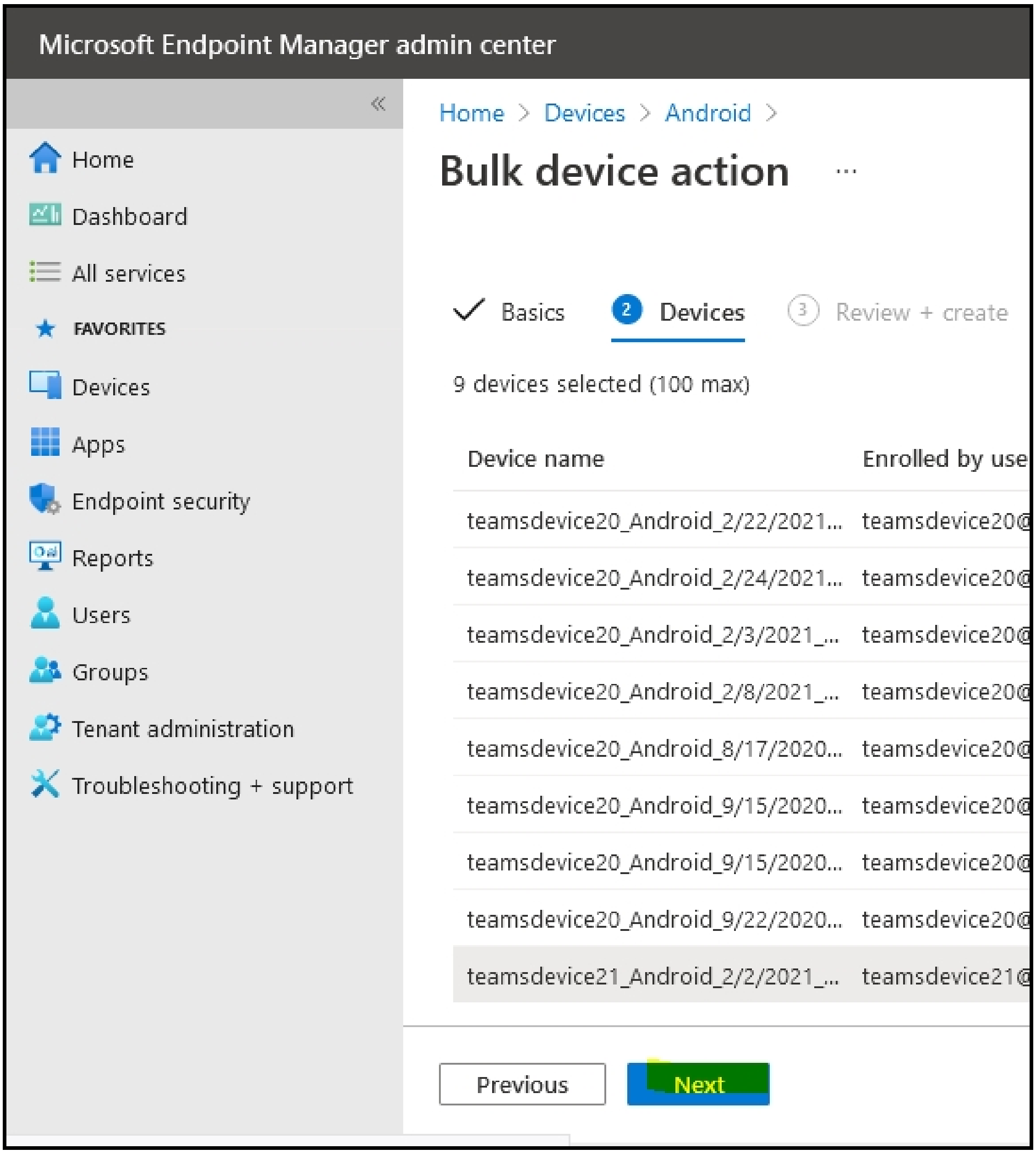
OS : **Android (device administrator)** Add filter

Device name	Enrolled by user UPN	OS
teamsdevice20_Android_2/22/2021_7:02 AM	teamsdevice20@3PIP.onmicrosoft.com	Android (device adminis...
teamsdevice20_Android_2/24/2021_7:10 AM	teamsdevice20@3PIP.onmicrosoft.com	Android (device adminis...
teamsdevice20_Android_2/3/2021_6:52 AM	teamsdevice20@3PIP.onmicrosoft.com	Android (device adminis...
teamsdevice20_Android_2/8/2021_6:30 AM	teamsdevice20@3PIP.onmicrosoft.com	Android (device adminis...

Selected devices:

teamsdevice20_Android_2/22/2021_7:02 AM	teamsdevice20@3PIP.onmicrosoft.com	Android (device ad...	Remove
teamsdevice20_Android_2/24/2021_7:10 AM	teamsdevice20@3PIP.onmicrosoft.com	Android (device ad...	Remove
teamsdevice20_Android_2/3/2021_6:52 AM	teamsdevice20@3PIP.onmicrosoft.com	Android (device ad...	Remove

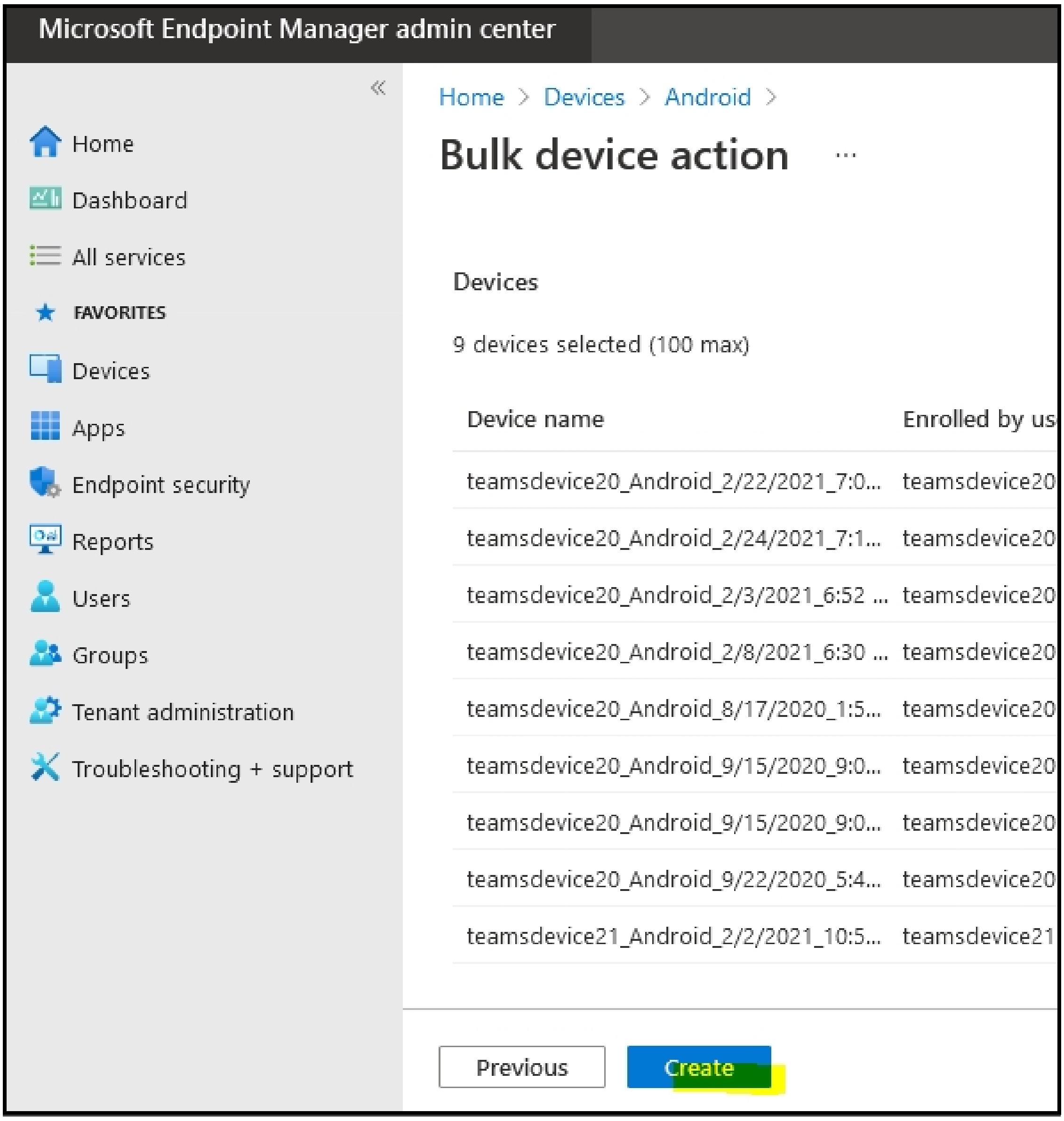
9. After the devices are selected, click **Next**.



9 devices selected (100 max)

Device name	Enrolled by use
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@

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



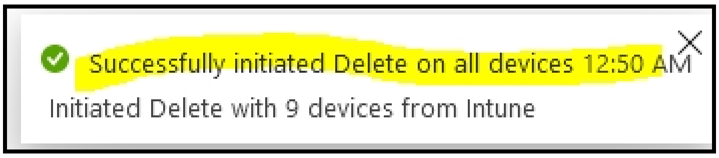
Bulk device action ...

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

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



Successfully initiated Delete on all devices 12:50 AM

Initiated Delete with 9 devices from Intune

⚠ 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.

Configuring Audio-Related Parameters for Noisy Environments

Network administrators can configure audio-related parameters to support the phone in special environments (such as noisy environments). To use the capability, contact AudioCodes Support.

Updating Microsoft Teams Devices Remotely

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

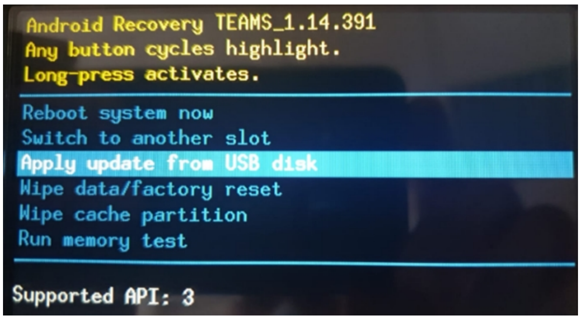
Applying Firmware to a Phone from a USB Disk

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

➢ To apply the firmware from the USB disk:

1. Enter recovery mode by long-pressing the reset key for 4 seconds; the device's LED lights up red.
2. Insert the USB disk with the target firmware.

Figure 6-1: Apply update from a USB disk



```
Android Recovery TEAMS_1.14.391
Any button cycles highlight.
Long-press activates.
```

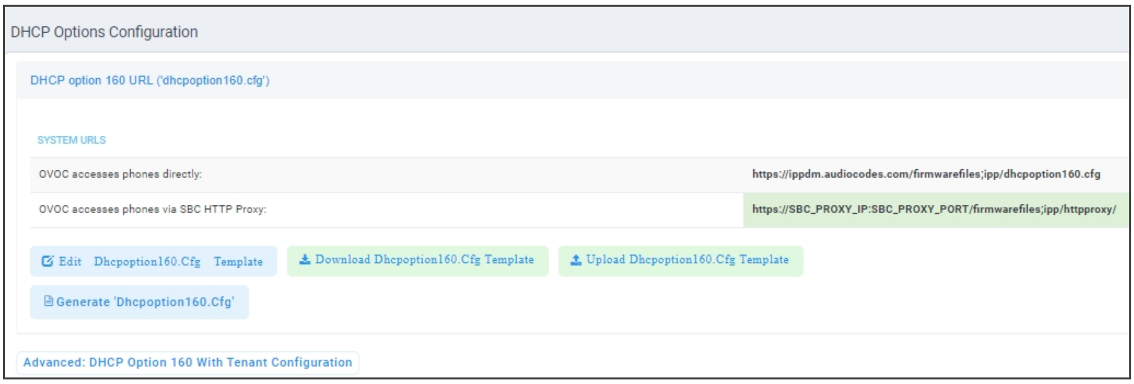
3. Select the 'Apply update from USB disk' option and then choose the correct firmware image from the disk.

Managing Phones with the Device Manager

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

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

Table 6-1: DHCP Option 160 URL



DHCP Options Configuration

DHCP option 160 URL ('dhcpoption160.cfg')

SYSTEM URLS

OVOC accesses phones directly:	https://ippdm.audiocodes.com/firmwarefiles;ipp/dhcpoption160.cfg
OVOC accesses phones via SBC HTTP Proxy:	https://SBC_PROXY_IP:SBC_PROXY_PORT/firmwarefiles;ipp/httpproxy/

Edit Dhcpoption160.Cfg Template
Download Dhcpoption160.Cfg Template
Upload Dhcpoption160.Cfg Template
Generate 'Dhcpoption160.Cfg'
Advanced: DHCP Option 160 With Tenant Configuration

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

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

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

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

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

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

Configuring a Periodic Provisioning Cycle

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

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

- Use the following table as reference.

Table 6-2: Periodic Provisioning Cycle

Parameter	Description
provisioning/period/type	Defines the frequency of the periodic provisioning cycle. Valid values are: ■ HOURLY ■ DAILY (default) ■ WEEKLY ■ POWERUP ■ EVERY5MIN ■ EVERY15MIN Each value type is accompanied by additional parameters (see Supported Parameters on the next page) that further defines the selected frequency.

Configuring TimeZone and Daylight Savings

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

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

➢ **To configure TimeZone and Daylight Savings:**

- Use the following table as reference.

Table 6-3: TimeZone And Daylight Savings

Parameter	Description
date_time/-timezone	Defines the Timezone. Valid values are: ■ +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:

Parameter	Description
	- 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

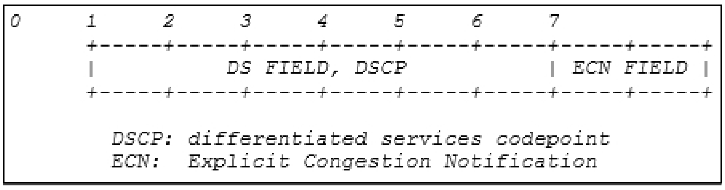
7 Troubleshooting

DSCP

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

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

Figure 7-1: DS Field, DSCP



```
0      1      2      3      4      5      6      7
       +-----+-----+-----+-----+-----+-----+-----+-----+
       |          DS FIELD, DSCP           | ECN FIELD |
       +-----+-----+-----+-----+-----+-----+-----+-----+

         DSCP: differentiated services codepoint
         ECN:  Explicit Congestion Notification
```

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

See also Microsoft's website for more information.

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

Figure 7-2: Recommended Values

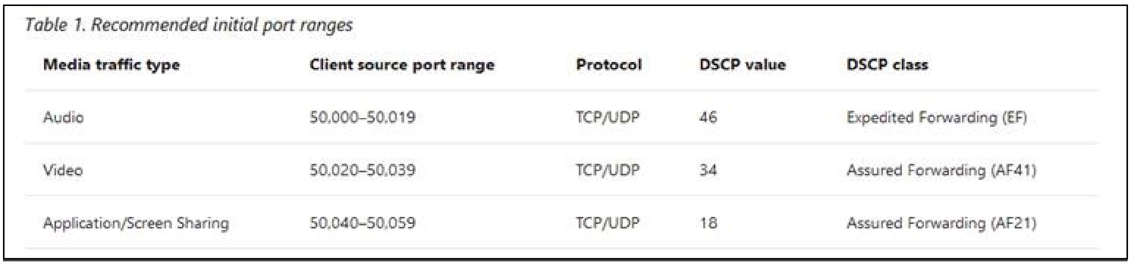
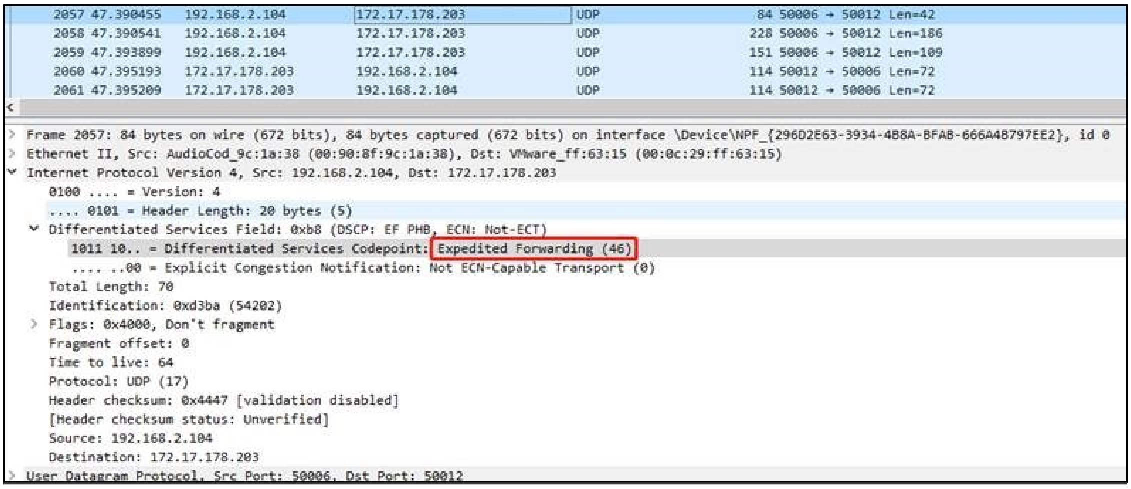


Table 1. Recommended initial port ranges

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

Figure 7-3: Audio



```
  2057 47.390455   192.168.2.104    172.17.178.203   UDP            84 50006 → 50012 Len=42
  2058 47.390541   192.168.2.104    172.17.178.203   UDP           228 50006 → 50012 Len=186
  2059 47.393899   192.168.2.104    172.17.178.203   UDP           151 50006 → 50012 Len=109
  2060 47.395193   172.17.178.203   192.168.2.104    UDP           114 50012 → 50006 Len=72
  2061 47.395209   172.17.178.203   192.168.2.104    UDP           114 50012 → 50006 Len=72

> Frame 2057: 84 bytes on wire (672 bits), 84 bytes captured (672 bits) on interface \Device\NPF_{296D2E63-3934-4B8A-BFAB-666A48797EE2}, id 0
> Ethernet II, Src: AudioCod_9c:1a:38 (00:90:8f:9c:1a:38), Dst: VMware_ff:63:15 (00:0c:29:ff:63:15)
v Internet Protocol Version 4, Src: 192.168.2.104, Dst: 172.17.178.203
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  v Differentiated Services Field: 0xb8 (DSCP: EF PHB, ECN: Not-ECT)
      1011 10.. = Differentiated Services Codepoint: Expedited Forwarding (46)
      .... ..00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)
    Total Length: 70
    Identification: 0xd3ba (54202)
  > Flags: 0x4000, Don't fragment
    Fragment offset: 0
    Time to live: 64
    Protocol: UDP (17)
    Header checksum: 0x4447 [validation disabled]
    [Header checksum status: Unverified]
    Source: 192.168.2.104
    Destination: 172.17.178.203
> User Datagram Protocol, Src Port: 50006, Dst Port: 50012
```

Users

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

Table 7-1: Troubleshooting

Symptom	Problem	Corrective Procedure
Phone is off (no screen displays and LEDs)	Phone is not receiving power	■ Make sure the AC/DC power adapter is attached firmly to the DC input on the rear of the phone. ■ Make sure the AC/DC power adapter is plugged into the electrical outlet. ■ Make sure the electrical outlet is functional. ■ If using Power over Ethernet (PoE), contact your network administrator to check that the switch is powering the phone.
Phone is not ringing	Ring volume is set too low	■ Increase the volume (see Adjusting Ring Volume on page 72)
Screen display is poor	Screen settings	■ Adjust the phone's screen brightness
Headset has no audio	Headset not connected properly	■ Make sure your headset is securely plugged into the headset port located on the side of the phone. ■ Make sure the headset volume level is adjusted adequately (see Adjusting Headset Volume on page 73).

Network Administrators

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

Teams IP Phone Utility

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

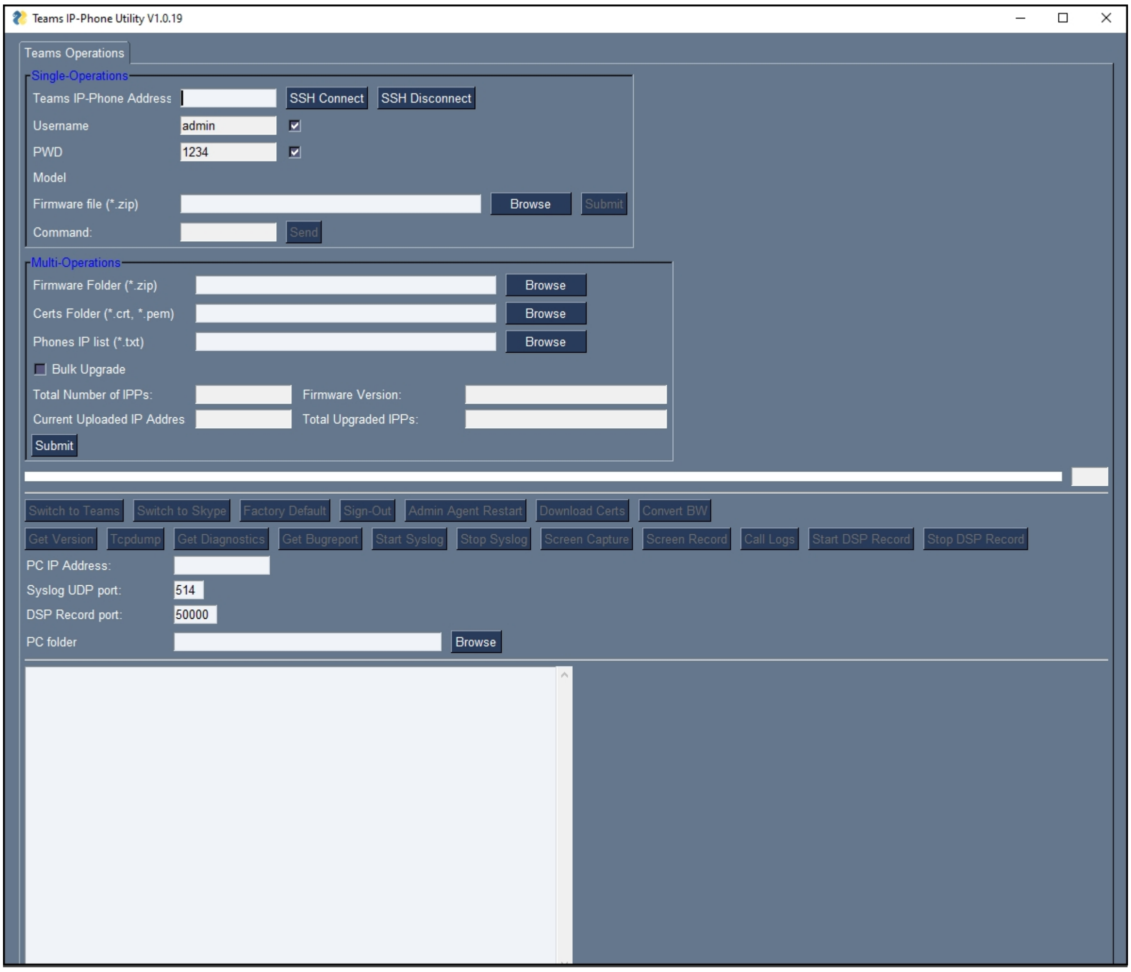
> ⚠ SSH is by default disabled and can be enabled with Administrator permissions in the phone screen (Device Administration > Debugging > SSH).

AudioCodes provides network administrators with the SSH-based Teams IP Phone Utility. To sign in, network administrators need to know their username and password; **admin** and **1234** are the default username and password. The application gives network administrators the following debugging capabilities:

- Capturing the Phone Screen on page 101
- Running Tcpdump on page 103
- Getting Information about Phones on page 104
- Remote Logging (Syslog) on page 106
- Getting Diagnostics on page 107
- Getting a Bug Report on page 110
- Activating DSP Recording on page 111
- Deactivating DSP Recording on page 112
- Getting Information about Phones on page 104

➢ **To open the Teams IP Phone Utility:**

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



Username admin ☑

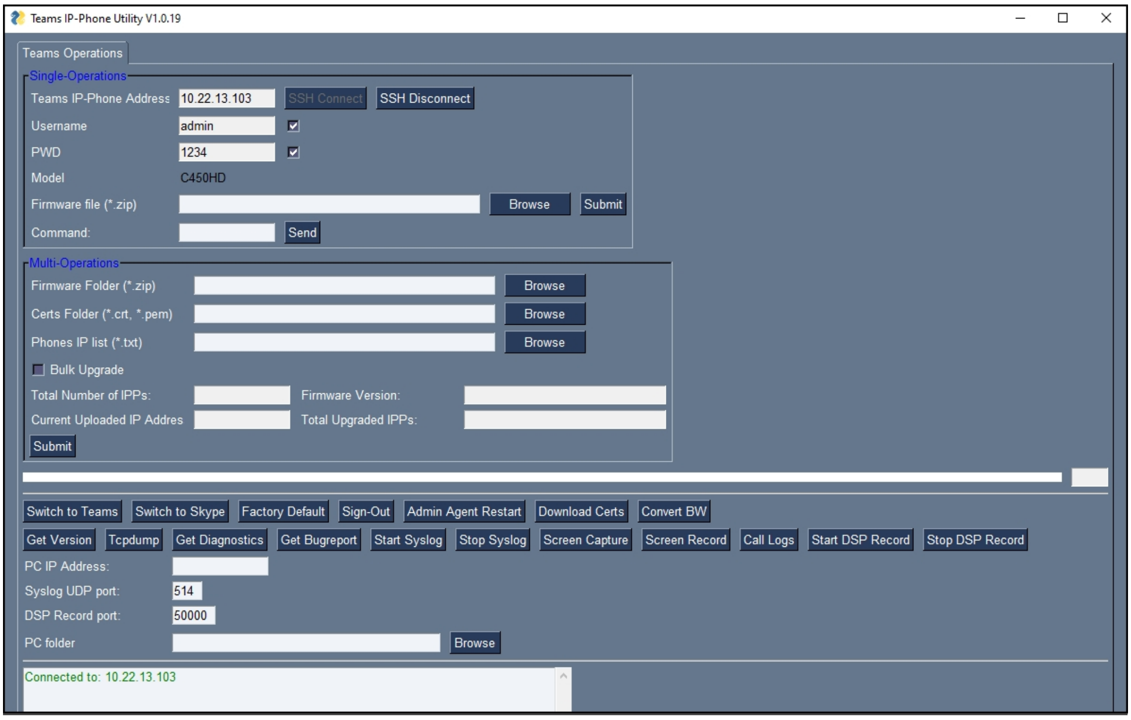
PWD 1234 ☑

Syslog UDP port: 514

DSP Record port: 50000

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

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



Teams IP-Phone Utility V1.0.19

Teams IP-Phone Address: 10.22.13.103

Username: admin ☑

PWD: 1234 ☑

Model: C450HD

Syslog UDP port: 514

DSP Record port: 50000

Connected to: 10.22.13.103

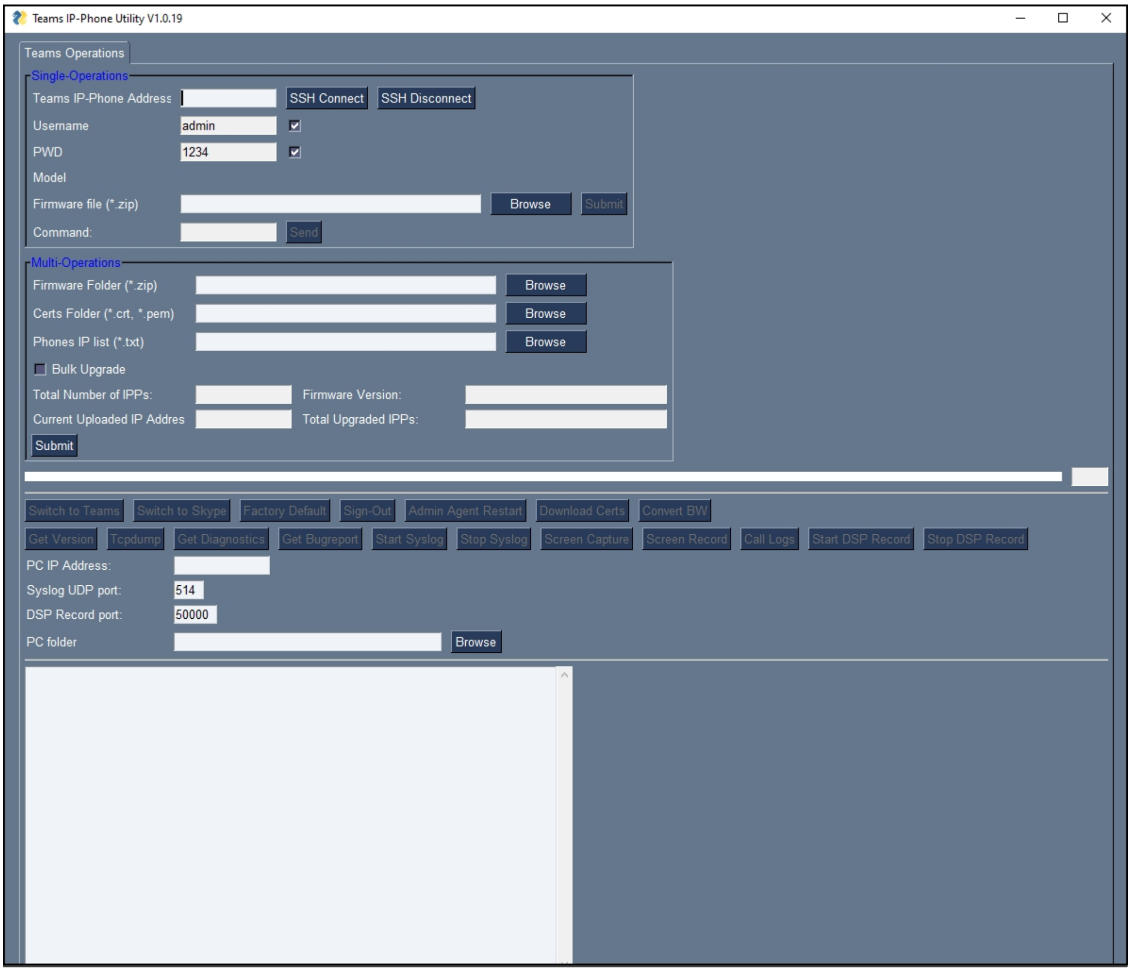
4. Next to the field 'PC folder', click the **Browse** button and navigate to and select the folder to which to send data to use for debugging.

Capturing the Phone Screen

AudioCodes' screen-capturing application Teams IPP GUI Tool allows network administrators to effectively collaborate and debug issues.

➢ To capture the phone screen:

1. From your PC's Start menu, open the AudioCodes Teams IPP GUI Tool application.



Teams IP-Phone Address

Username admin ☑

PWD 1234 ☑

Firmware file (*.zip)

Command:

Firmware Folder (*.zip)

Certs Folder (*.crt, *.pem)

Phones IP list (*.txt)

□ Bulk Upgrade

Total Number of IPPs: Firmware Version:

Current Uploaded IP Addres Total Upgraded IPPs:

PC IP Address:

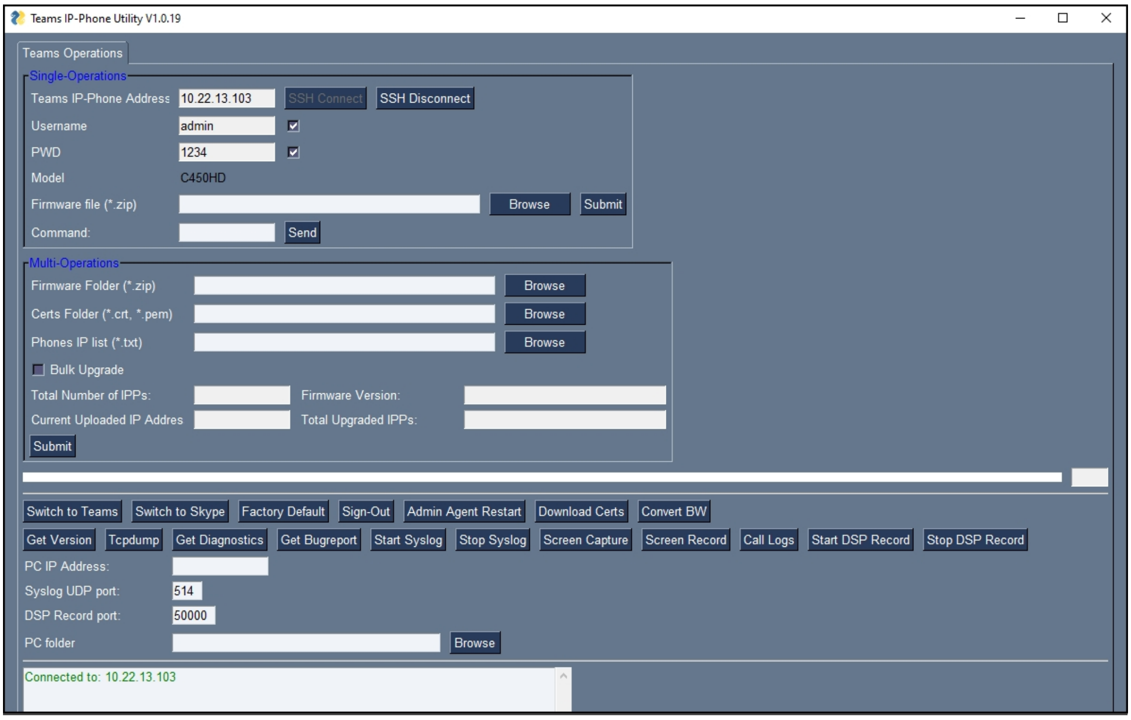
Syslog UDP port: 514

DSP Record port: 50000

PC folder

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

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



Teams IP-Phone Address 10.22.13.103

Username admin ☑

PWD 1234 ☑

Model C450HD

Firmware file (*.zip)

Command:

Firmware Folder (*.zip)

Certs Folder (*.crt, *.pem)

Phones IP list (*.txt)

□ Bulk Upgrade

Total Number of IPPs: Firmware Version:

Current Uploaded IP Addres Total Upgraded IPPs:

PC IP Address:

Syslog UDP port: 514

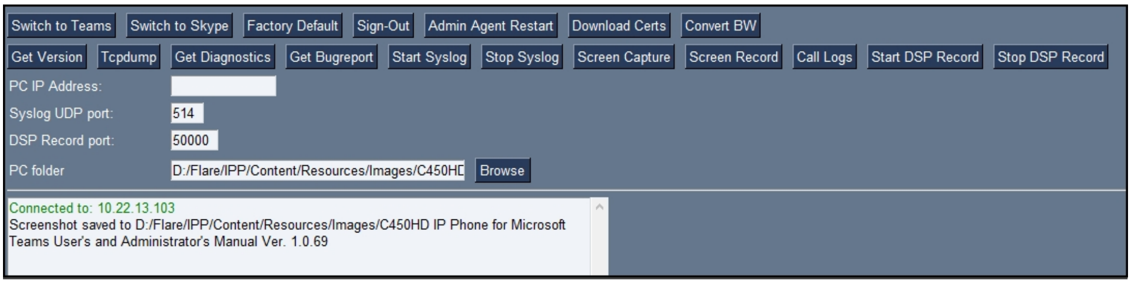
DSP Record port: 50000

PC folder

```
Connected to: 10.22.13.103
```

4. Next to the field 'PC folder', click the **Browse** button and navigate to and select the folder to which to send the screen captures.

5. Click the **Screen Capture** button; the phone's screen is captured and the screenshot is saved and sent to the folder.



PC IP Address:

Syslog UDP port: 514

DSP Record port: 50000

PC folder D:/Flare/IPP/Content/Resources/Images/C450HD

```
Connected to: 10.22.13.103
Screenshot saved to D:/Flare/IPP/Content/Resources/Images/C450HD IP Phone for Microsoft
Teams User's and Administrator's Manual Ver. 1.0.69
```

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

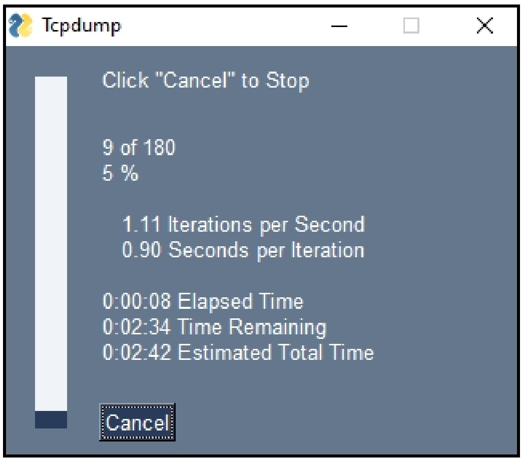
Running Tcpdump

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

➢ To run Tcpdump:

1. In the Teams IP Phone Utility (see Teams IP Phone Utility on page 99 for more information), enter the phone's IP address, click **SSH Connect** and browse to a folder on the PC to which to send the information.

2. Click the **Run Tcpdump** button.



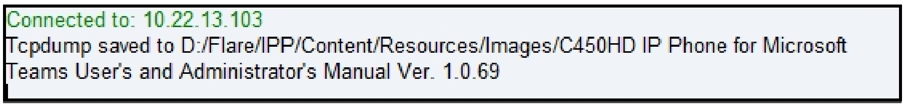
```
Click "Cancel" to Stop

9 of 180
5 %

   1.11 Iterations per Second
   0.90 Seconds per Iteration

0:00:08 Elapsed Time
0:02:34 Time Remaining
0:02:42 Estimated Total Time
```

3. After a short period, view in the results pane a 'Finished' indication.



```
Connected to: 10.22.13.103
Tcpdump saved to D:/Flare/IPP/Content/Resources/Images/C450HD IP Phone for Microsoft
Teams User's and Administrator's Manual Ver. 1.0.69
```

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

Alternatively, run Tcpdump *without* the Teams IP Phone Utility.

➢ To run tcpdump without the Teams IP Phone Utility:

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.
4. Execute the following command from your PC command prompt (cmd):

```
scp -r admin@%deviceIp%:/storage/emulated/0/recording/ %FolderOnPc%
```

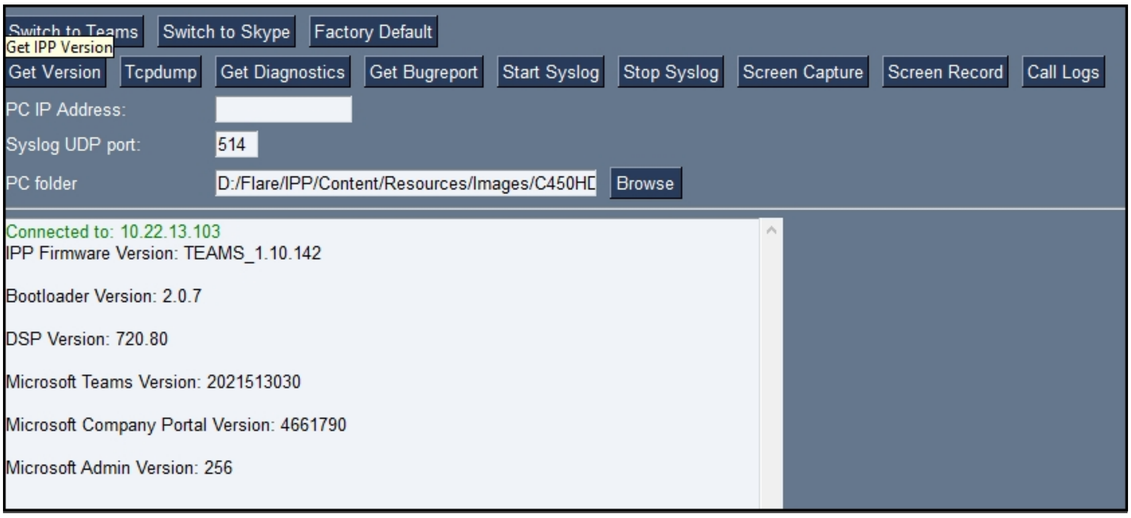
Getting Information about Phones

Network administrators can get information about phones using AudioCodes' SSH protocol based Teams IP Phone Utility.

➢ To get information from the phone:

1. Open the Teams IP Phone Utility (see Teams IP Phone Utility on page 99 for more information about the application) and click **Get Version** (after entering the phone's IP

address, clicking **SSH Connect** and browsing to a folder on the PC to which to send the information).



PC IP Address:
Syslog UDP port: 514
PC folder D:/Flare/IPP/Content/Resources/Images/C450HD

```
Connected to: 10.22.13.103
IPP Firmware Version: TEAMS_1.10.142

Bootloader Version: 2.0.7

DSP Version: 720.80

Microsoft Teams Version: 2021513030

Microsoft Company Portal Version: 4661790

Microsoft Admin Version: 256
```

2. Alternatively:

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

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

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

```
getprop ro.bootloader
```

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

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

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

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

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

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

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

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

Remote Logging (Syslog)

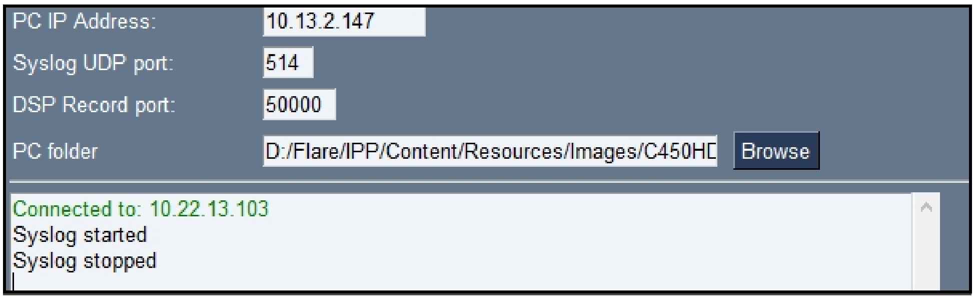
Remote Logging via Syslog provides the same log level as Device Diagnostics (performed via the Microsoft Admin Center) with some additional information that may be relevant to device issues (not Teams application issues). Device Diagnostics via the Microsoft Admin Center are saved to the device sdcard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

Remote Logging via Syslog can be enabled from the

- below
- below

➢ To enable Remote Logging via Syslog from the Teams IP Phone Utility:

1. In the Teams IP Phone Utility (see Teams IP Phone Utility on page 99 for more information), enter the phone's IP address, click **SSH Connect** and browse to a folder on the PC to which to send the information.
2. In the 'PC IP Address' field, enter the IP address of the PC on which the utility is installed and then click the **Start Syslog** button.



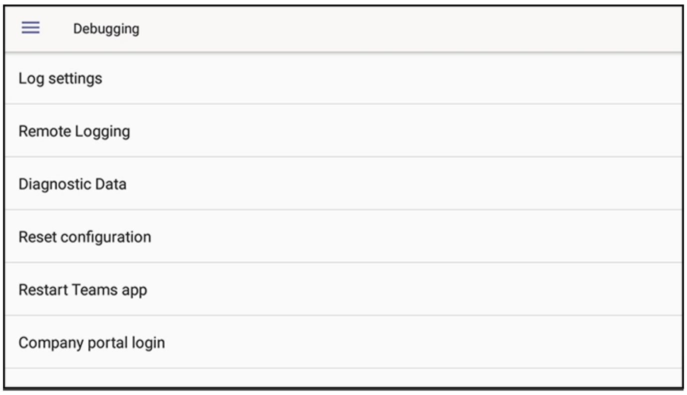
PC IP Address: 10.13.2.147
Syslog UDP port: 514
DSP Record port: 50000
PC folder D:/Flare/IPP/Content/Resources/Images/C450HD

```
Connected to: 10.22.13.103
Syslog started
Syslog stopped
```

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

➢ To enable Remote Logging via Syslog from the phone:

1. Log in to the phone as Administrator and go back.
2. In the ‘Device administration’ screen, select **Debugging**.
3. Select **Remote logging**.


Debugging

Log settings

Remote Logging

Diagnostic Data

Reset configuration

Restart Teams app

Company portal login

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

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

➢ **To enable Syslog using SSH protocol, type the following command at the shell prompt:**

```
setprop persist.ac.rl_address <syslog_server_ip>:<port>.
```

➢ **To disable Syslog using SSH, type the following command at the shell prompt:**

```
setprop persist.ac.rl_address ""
```

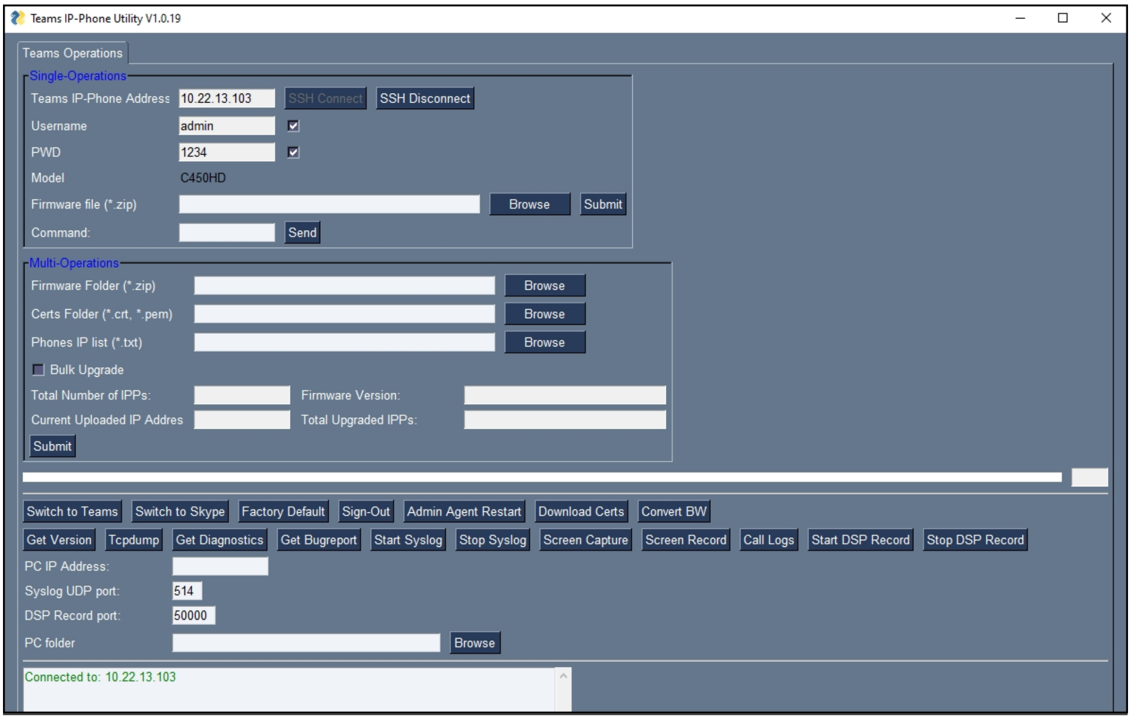
Getting Diagnostics

Getting Diagnostics is identical to Getting a Bug Report on page 110 with these exceptions:

- Diagnostics can be gotten on one phone; a Bug Report can be on many phones
- Diagnostics is in zip file format; a Bug Report is not
- Diagnostics are formatted differently to a Bug Report

➢ **To get diagnostics:**

1. In the Teams IP Phone Utility (see Teams IP Phone Utility on page 99 for more information), enter the phone's IP address, click **SSH Connect** and browse to a folder on the PC to which to send the information.



Teams IP-Phone Address 10.22.13.103

Username admin ☑

PWD 1234 ☑

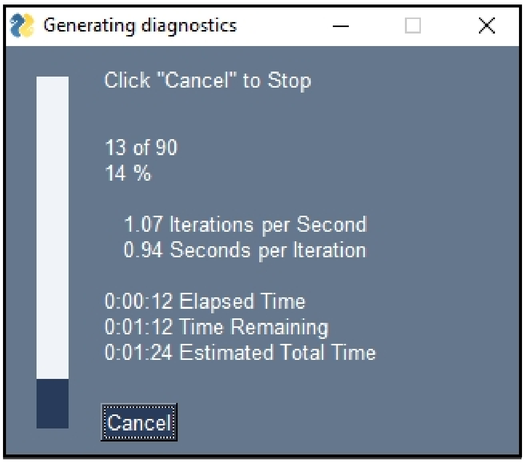
Model C450HD

Syslog UDP port: 514

DSP Record port: 50000

Connected to: 10.22.13.103

2. Click **Get Diagnostics**.



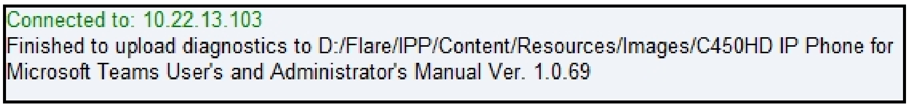
Click "Cancel" to Stop

13 of 90
14 %

1.07 Iterations per Second
0.94 Seconds per Iteration

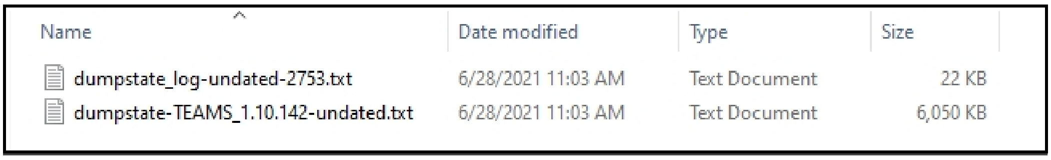
0:00:12 Elapsed Time
0:01:12 Time Remaining
0:01:24 Estimated Total Time

3. After a short period, view in the results pane a 'Finished' indication.



Connected to: 10.22.13.103
Finished to upload diagnostics to D:/Flare/IPP/Content/Resources/Images/C450HD IP Phone for Microsoft Teams User's and Administrator's Manual Ver. 1.0.69

4. Open the folder on the PC to which you commanded the application to send the information and locate and open the sub-folder 'logs'.



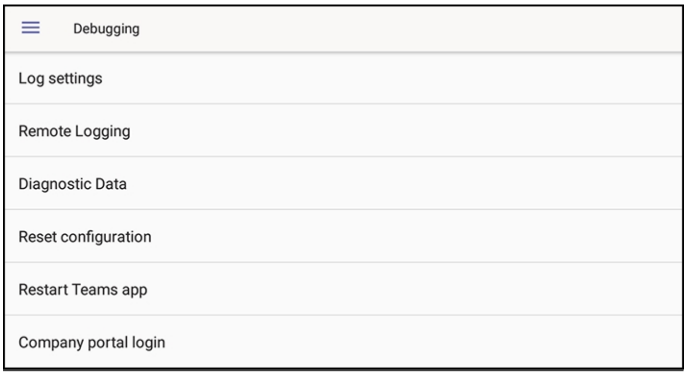
Name	Date modified	Type	Size
dumpstate_log-undated-2753.txt	6/28/2021 11:03 AM	Text Document	22 KB
dumpstate-TEAMS_1.10.142-undated.txt	6/28/2021 11:03 AM	Text Document	6,050 KB

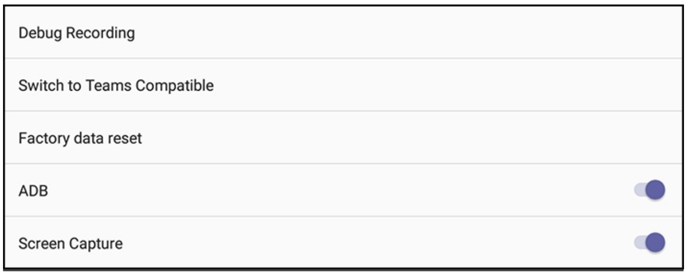
5. Open the txt files to view the diagnostics.

Network administrators who need to get diagnostics from the device can alternatively dump the logs to the phone's Secure Digital (SD) Card and then later collect them using Secure Copy Protocol (SCP) based on Secure Shell (SSH) protocol. Whenever an issue occurs, the administrator can dump the logs into the SD Card.

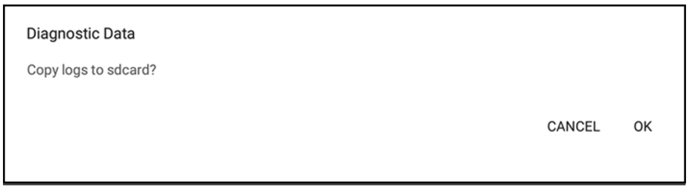
➢ To do this:

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





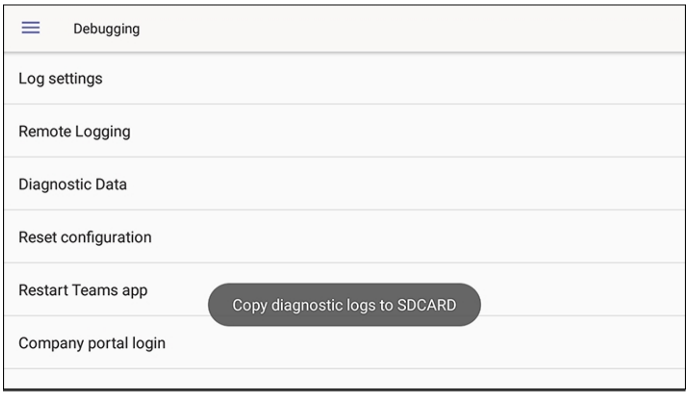
3. Select the **Diagnostic Data** option.



Diagnostic Data

Copy logs to sdcard?

4. Select **OK** to confirm.



Copy diagnostic logs to SDCARD

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

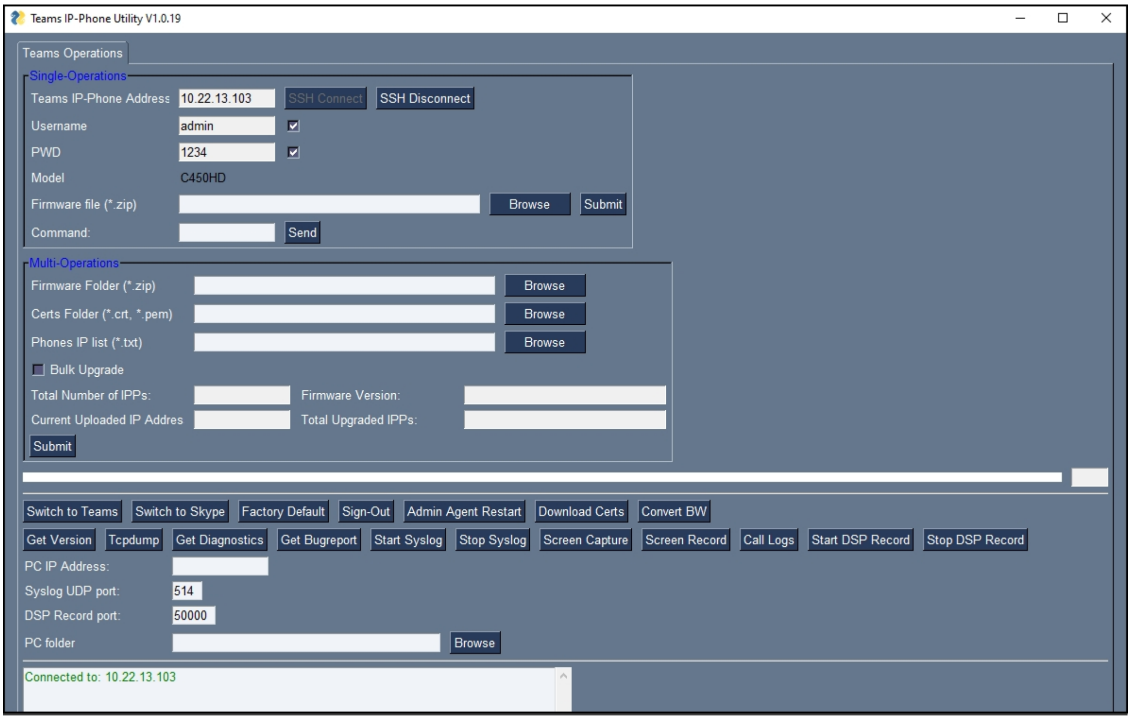
Getting a Bug Report

Getting a Bug Report is identical to Getting Diagnostics on page 107 with these exceptions:

- A Bug Report can be on many phones; Diagnostics is on one
- A Bug Report is in zip file format; Diagnostics are not
- A Bug Report is formatted differently to Diagnostics

➢ To get a Bug Report:

1. In the AudioCodes Teams IP Phone Utility (see Teams IP Phone Utility on page 99 for more information), enter the phone's IP address, click **SSH Connect** and browse to a folder on the PC to which to send the information.



Teams IP-Phone Address 10.22.13.103

Username admin ☑

PWD 1234 ☑

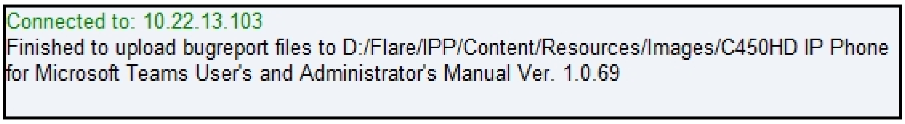
Model C450HD

Syslog UDP port: 514

DSP Record port: 50000

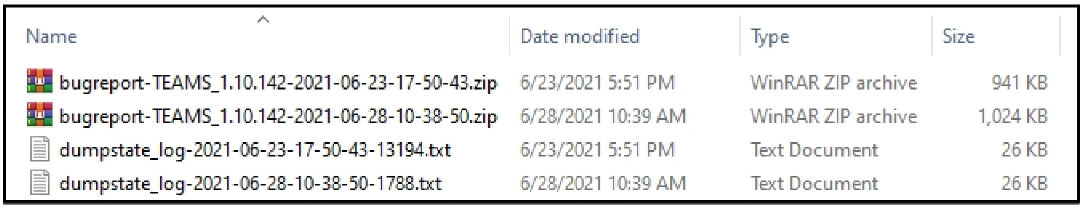
Connected to: 10.22.13.103

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



```
Connected to: 10.22.13.103
Finished to upload bugreport files to D:/Flare/IPP/Content/Resources/Images/C450HD IP Phone
for Microsoft Teams User's and Administrator's Manual Ver. 1.0.69
```

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



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

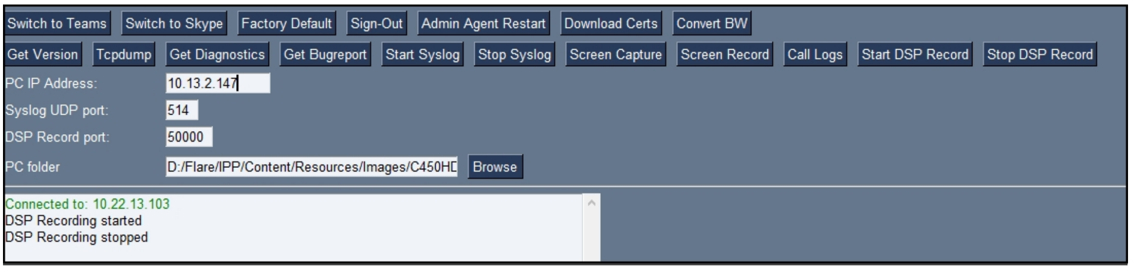
4. Unzip the zipped files and open the txt files to view the report.

Activating DSP Recording

Network administrators can activate DSP recording using AudioCodes' SSH protocol based Teams IP Phone Utility.

➢ To activate DSP Recording:

1. In the AudioCodes Teams IP Phone Utility (see Teams IP Phone Utility on page 99 for more information), enter the phone's IP address, click **SSH Connect** and browse to a folder on the PC to which to send the information.
2. In the 'PC IP Address' field, enter the IP address of the PC on which the utility is installed and then click the **Start DSP Record** button.
3. After a period of recording, click **Stop DSP Record**.



PC IP Address: 10.13.2.147
Syslog UDP port: 514
DSP Record port: 50000
PC folder: D:/Flare/IPP/Content/Resources/Images/C450HD

```
Connected to: 10.22.13.103
DSP Recording started
DSP Recording stopped
```

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

Network administrators can alternatively activate a DSP recording using SSH protocol *without* the Teams IP Phone Utility, as shown next.

➢ **To activate DSP recording using SSH protocol *without* the Teams IP Phone Utility, type the following at the shell prompt:**

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

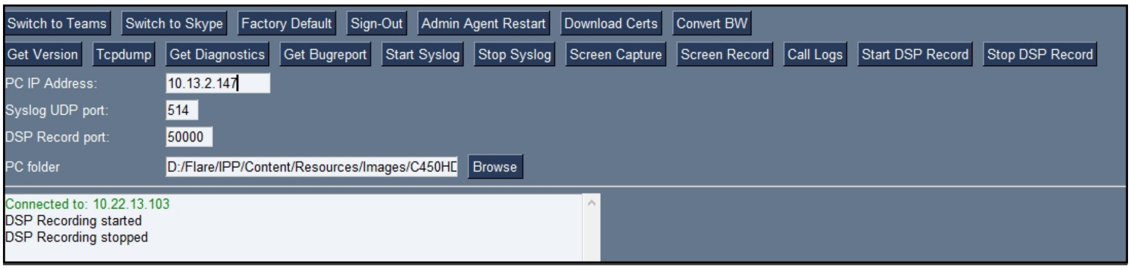
⚠ DSP recording can be activated on the fly without requiring the network administrator to reset the phone.

Deactivating DSP Recording

Network administrators can deactivate DSP recording using AudioCodes' SSH protocol based Teams IP Phone Utility.

➢ **To deactivate DSP Recording:**

1. In the AudioCodes Teams IP Phone Utility (see Teams IP Phone Utility on page 99 for more information), click **Stop DSP Record** after a period of recording (see Activating DSP Recording on the previous page for information on how to start DSP recording.



PC IP Address: 10.13.2.147
Syslog UDP port: 514
DSP Record port: 50000
PC folder D:/Flare/IPP/Content/Resources/Images/C450HD

```
Connected to: 10.22.13.103
DSP Recording started
DSP Recording stopped
```

2. View in the PC Folder you configured the DSP recording.

⚠ Network administrators can alternatively deactivate a DSP recording using SSH protocol *without* the Teams IP Phone Utility, as shown next.

➢ **To deactivate DSP recording using SSH protocol *without* the Teams IP Phone Utility, type the following at the shell prompt:**

```
setprop ac.dr_voice_enable false
```

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

SSH

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

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

To sign in, the administrator needs to know their username and password; **admin** and **1234** are the defaults. SSH access allows administrators debugging capabilities such as:

- Getting the Phone IP Address below
- Pulling files from the phone sdcard (using the curl command)
- Activating DSP Recording on page 111
- Deactivating DSP Recording on the previous page
- Installing the Teams APK (or Any Other APK) using SSH below

Getting the Phone IP Address

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

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

```
ifconfig
```

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

Network administrators can install the Microsoft Teams Android Application Package (or any other APK) using SSH protocol.

Updating Teams Phones using SSH Commands

➢ **To upgrade firmware:**

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

   For example, use the following:

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

2. Update the firmware using the following:

   ```
   setprop ctl.start local_update
   ```

3. Track progress using the following:

```
logcat | grep  update_engine_client_android
```

➢ To upgrade the Android Package Kit (APK):

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

   For example use the following:

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

2. Update the APK using the following:

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

3. Delete the old APK using the following:

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

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

➢ To collect logs:

1. Collect logs using the following:

```
command/bugreport 1
```

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

   For example, use the following:

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

➢ To install the Client Certificate:

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

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

Microsoft Admin Center

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

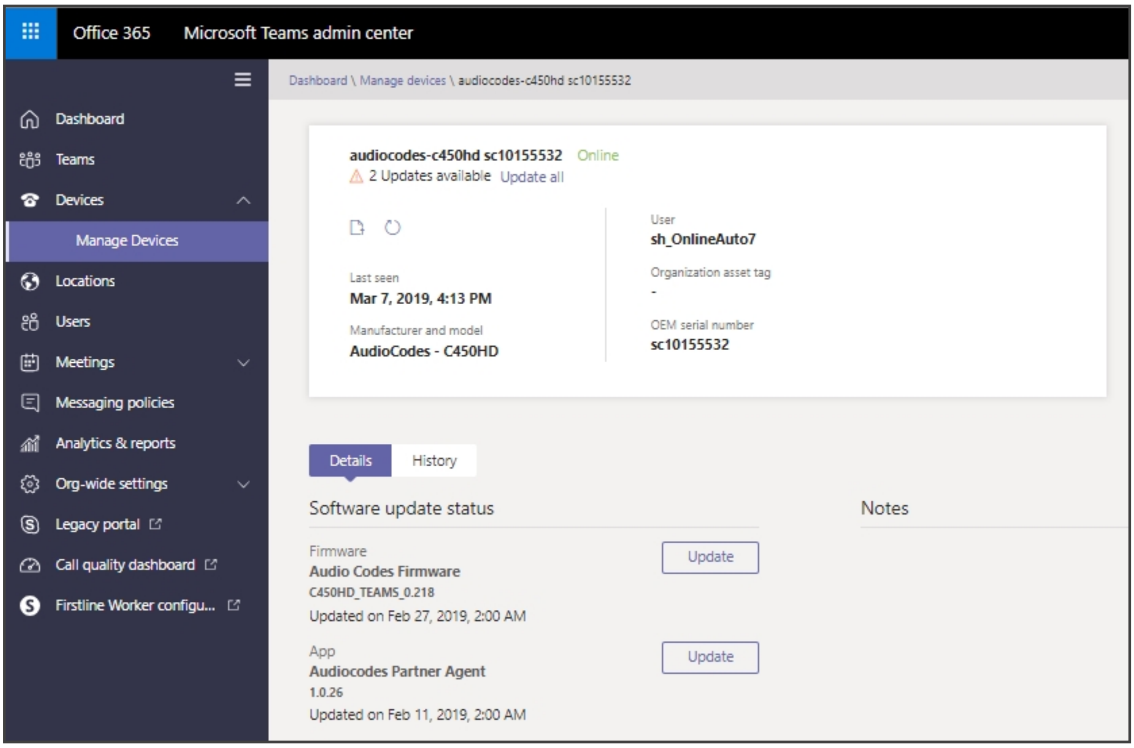
Collecting Logs

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

➢ **To collect logs:**

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

Figure 7-4: Microsoft Teams Admin Center - Diagnostics



Dashboard \ Manage devices \ audiocodes-c450hd sc10155532

audiocodes-c450hd sc10155532 Online

⚠ 2 Updates available Update all

Last seen
Mar 7, 2019, 4:13 PM

Manufacturer and model
AudioCodes - C450HD

User
sh_OnlineAuto7

Organization asset tag
-

OEM serial number
sc10155532

Software update status

Notes

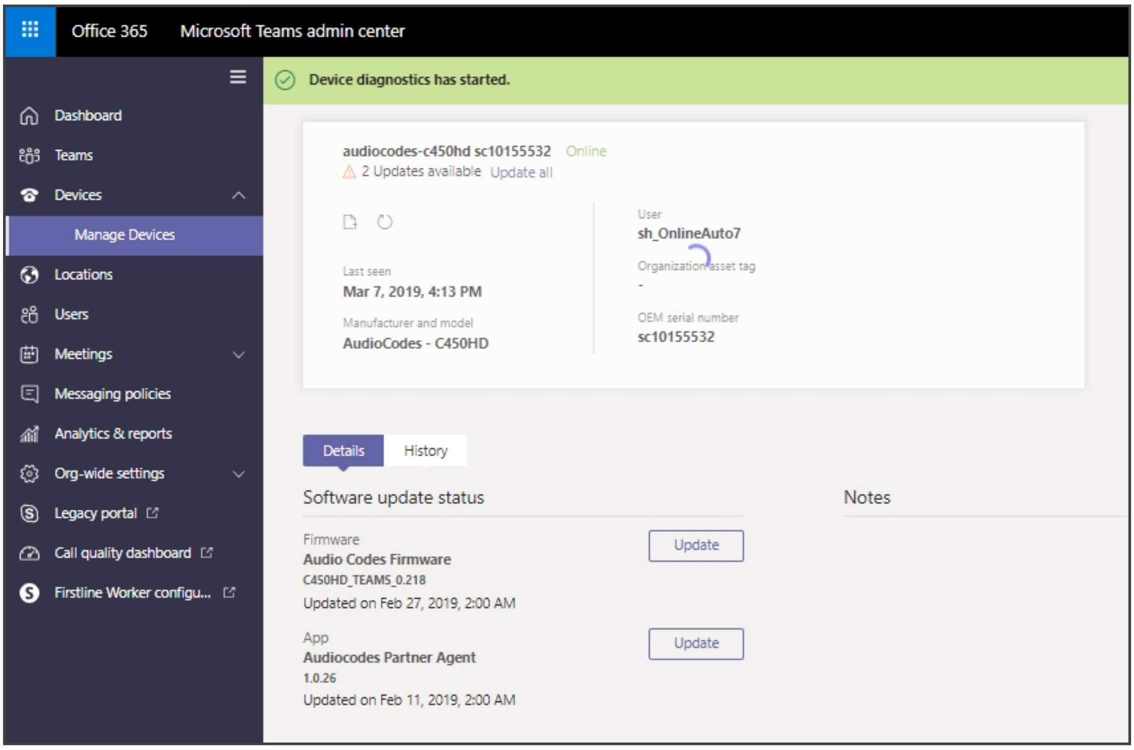
Firmware
Audio Codes Firmware
C450HD_TEAMS_0.218
Updated on Feb 27, 2019, 2:00 AM

App
Audiocodes Partner Agent
1.0.26
Updated on Feb 11, 2019, 2:00 AM

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

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

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



Device diagnostics has started.

audiocodes-c450hd sc10155532 Online
2 Updates available Update all

Last seen
Mar 7, 2019, 4:13 PM

Manufacturer and model
AudioCodes - C450HD

User
sh_OnlineAuto7

Organization asset tag
-

OEM serial number
sc10155532

Software update status

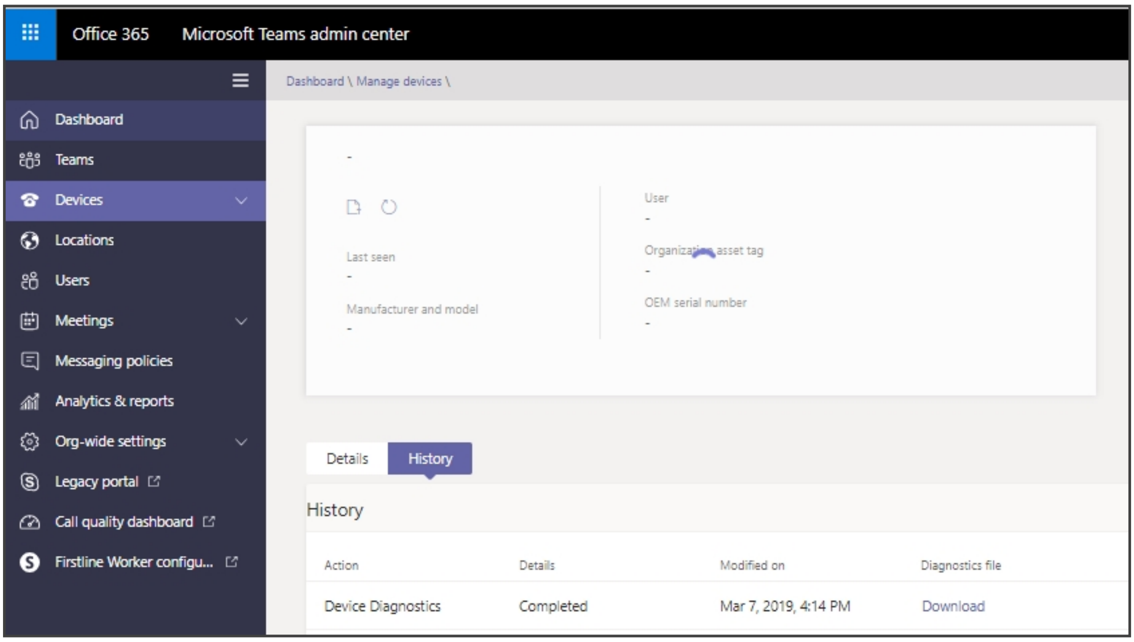
Notes

Firmware
Audio Codes Firmware
C450HD_TEAMS_0.218
Updated on Feb 27, 2019, 2:00 AM

App
Audiocodes Partner Agent
1.0.26
Updated on Feb 11, 2019, 2:00 AM

4. Click the **History** tab.

Figure 7-6: History - Download



Dashboard \ Manage devices \

-

Last seen
-

Manufacturer and model
-

User
-

Organization asset tag
-

OEM serial number
-

History

Action	Details	Modified on	Diagnostics file
Device Diagnostics	Completed	Mar 7, 2019, 4:14 PM	Download

Click **Download** to download the logs.

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

Getting 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 obtained using one of two methods:

- via GUID/UUID (see Getting Logs using UUID on page 119)
- via the phone (see Getting Logs via the Phone on the next page)

Getting Logs via the Phone

Although the documentation here shows you how to get logs via the phone, logs can alternatively be collected via Microsoft Teams admin center (TAC). Network administrators can download all logs from the TAC, including logcat, dumpsys, ANRs, Client Log, Call Policies File, Call Log Info File, Sky lib Log Files, Media Log Files, and CP. All information collected by Microsoft Teams admin center (TAC) is added to the bug report.

Collecting logs via the Device Manager provides the following zipped file:

bugreport-00908f9d6888-TEAMS_1.14.455-2021-12-15-11-14-06.zip

Collecting logs via Microsoft's TAC provides the following zipped file:

1639562988_TeamsLogs-1639557967162.zip

These zipped files include the following files:

- AdminAgentLogs.zip [includes logcat collected by the Device Manager]
- blog files (media logs): app_process32.msrtc-0-3054496316.blog and Skylib-0-3692023773.blog
- SessionID_For_Company_Portal_Logs.txt [this is the CP SSDI, not the logs; the logs are sent to the server]

The following are also supported:

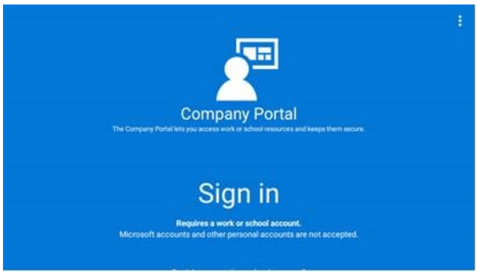
- Logs collected via Microsoft's TAC are included in the bugreport so collection of logs via the Device Manager is similar to the collection of logs via Microsoft's TAC.
- When collecting logs via Microsoft's TAC, the AdminAgentLogs.zip file includes the logcat with bugreport.

Other logs collected are:

- AudioCodes' configuration is packed into the bugreport
- DSP logs [the DSP must be enabled separately so it's unnecessary to add to the default log collection]

➢ 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. Select the **Debugging** option under Admin.
4. Select **Company Portal login**.
5. Select the icon located in the uppermost right corner of the screen, shown in the next figure:



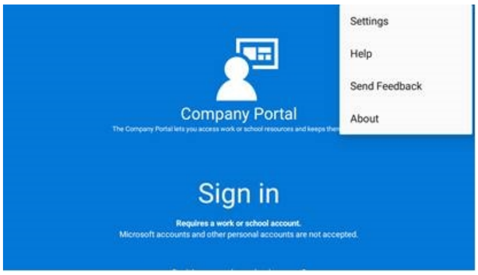
Company Portal

The Company Portal lets you access work or school resources and keeps them secure.

Sign in

Requires a work or school account.
Microsoft accounts and other personal accounts are not accepted.

6. Select **Settings**.



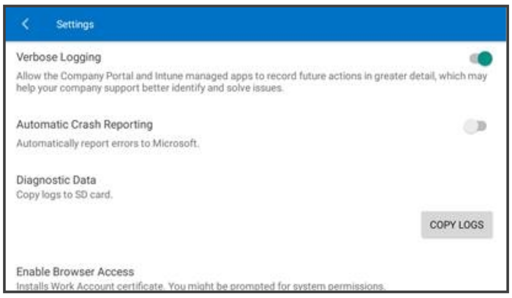
Company Portal

The Company Portal lets you access work or school resources and keeps them

Sign in

Requires a work or school account.
Microsoft accounts and other personal accounts are not accepted.

7. Select the **Copy Logs** key.



Settings

Verbose Logging ●
Allow the Company Portal and Intune managed apps to record future actions in greater detail, which may help your company support better identify and solve issues.

Automatic Crash Reporting ○
Automatically report errors to Microsoft.

Diagnostic Data
Copy logs to SD card.

Enable Browser Access
Installs Work Account certificate. You might be prompted for system permissions.

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.

➢ **To get logs via the Device Manager:**

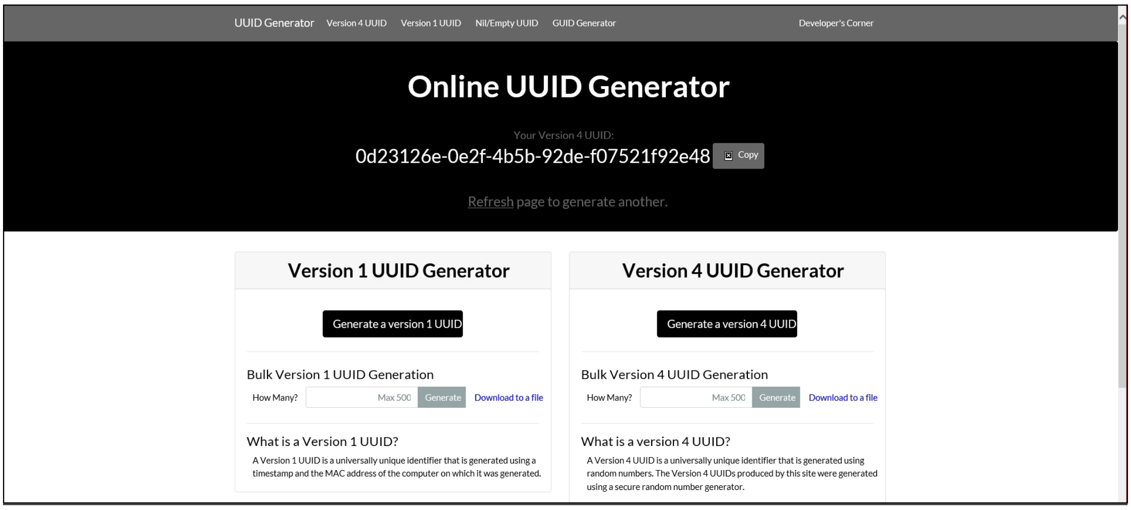
- See the *Device Manager Administrator's Guide* available here.

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/



Online UUID Generator

Your Version 4 UUID:

0d23126e-0e2f-4b5b-92de-f07521f92e48

Refresh page to generate another.

Version 1 UUID Generator

Bulk Version 1 UUID Generation

What is a Version 1 UUID?

A Version 1 UUID is a universally unique identifier that is generated using a timestamp and the MAC address of the computer on which it was generated.

Version 4 UUID Generator

Bulk Version 4 UUID Generation

What is a version 4 UUID?

A Version 4 UUID is a universally unique identifier that is generated using random numbers. The Version 4 UUIDs produced by this site were generated using a secure random number generator.

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 on the previous page, 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.

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

➢ **To execute the command ssh:**

1. After copying the UUID number as shown in Getting Logs using UUID on page 119, 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
```

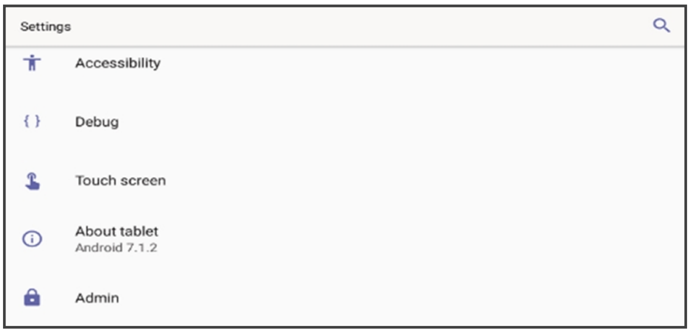
3. After running the command, the logs are saved in 'Intune', Microsoft's cloud-based service for mobile device management (MDM) and mobile application management (MAM).
4. Send AudioCodes the UUID number.

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:

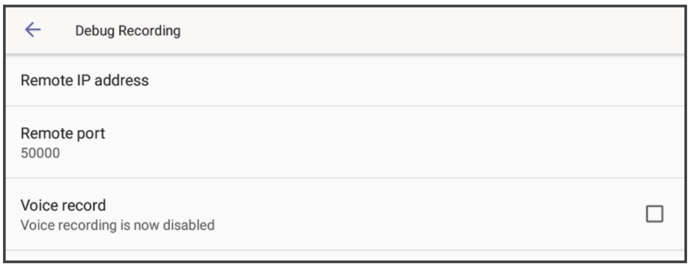
1. Log in as Administrator.
2. Open the Settings screen and scroll down to **Debug**.



Settings

- Accessibility
- Debug
- Touch screen
- About tablet
  Android 7.1.2
- Admin

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



Debug Recording

Remote IP address

Remote port
50000

Voice record
Voice recording is now disabled □

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

Collecting Media Logs (*.blog) from the Phone

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

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

1. Access the phone via SSH.

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

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

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

This page is intentionally left blank.

International Headquarters

1 Hayarden Street,

Airport City

Lod 7019900, Israel

Tel: +972-3-976-4000

Fax: +972-3-976-4040

AudioCodes Inc.

80 Kingsbridge Rd

Piscataway, NJ 08854, USA

Tel: +1-732-469-0880

Fax: +1-732-469-2298

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

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

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

Document #: LTRT-13312