User's and Administrator's Manual

AudioCodes 400HD IP Phone Series

C435HD IP Phones

Microsoft Teams Application

Version 1.12

audiocodes

Notice

Date Published: July-13-2021

WEEE EU Directive

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

Customer Support

Customer technical support and services are provided by AudioCodes or by an authorized AudioCodes Service Partner. For more information on how to buy technical support for AudioCodes products and for contact information, please visit our website at https://www.audiocodes.com/services-support/maintenance-and-support.

Documentation Feedback

AudioCodes continually strives to produce high quality documentation. If you have any comments (suggestions or errors) regarding this document, please fill out the Documentation Feedback form on our website at https://online.audiocodes.com/documentation-feedback.

Stay in the Loop with AudioCodes

Related Documentation

Document Name
https://docs.microsoft.com/en-us/MicrosoftTeams/phones-for-teams
C435HD IP Phone for Microsoft Teams Quick Guide
C435HD IP Phone for Microsoft Teams Release Notes

Table of Contents

1 Overview

The AudioCodes C435HD IP phones are Microsoft Teams-native entry level/common area phones designed to support the next generation of enterprise collaboration technologies with a large color LCD screen and full UC integration for the Native Microsoft Teams Online market.

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

Feature highlights:

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

Specifications

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

Table 1-1: Software Specifications

Feature	Details
Media Processing	■ Voice Coders: G.711, G.729, G.722, SILK Opus ■ Acoustic Echo Cancelation: G.168-2004 compliant, 64-msec tail length ■ Adaptive Jitter Buffer ■ Voice Activity Detection ■ Comfort Noise Generation ■ Packet Lost Concealment ■ RTP/RTCP Packetization (RFC 3550, RFC 3551), SRTP (RFC 3711)
Microsoft Teams phones feature set	■ Authentication (Sign in with user credentials; Sign in using PC/Smartphone; Modern Authentication; Phone lock/unlock) ■ Calling (Incoming/Outgoing P2P calls; In-call controls via UI (Mute,

Feature	Details
	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.
Configuration and Management	■ Microsoft Teams & Skype for Business Admin Center (Provisioning and Logging) ■ AudioCodes Device Management and AudioCodes Redirect Server for monitoring, upgrading and configuring
Debugging Tools	■ AudioCodes' Teams IP Phone Utility (see Teams IP Phone Utility on page 75) ■ Log upload to Microsoft server (certification for 3rd party Skype for Business clients) ■ Remote logging via Syslog ■ SSH Access ■ Capturing the phone screen ■ TCPdump ■ Company Portal (Intune) logs ■ Audio Debug recording logs ■ Media logs (*.blog) ■ Port mirroring network monitoring (C450HD) ■ Remote Packet Capture network sniffer application
Localization Support	■ Multi-lingual support; the language pack list is not yet final and is subject to modification.
Hardware	■ Graphic 4.3" color screen, 480x272 resolution, with multi-lingual support ■ Wired connectivity: ✔ Two RJ-45 [Gigabit Ethernet (GbE)] (10/100/1000BaseT

Feature	Details
	Ethernet) ports: LAN and PC port ✔ RJ-9 port (jack) for headset ✔ 1 x USB port for headset support ✔ RJ-11 interface ■ Power: ✔ DC jack adapter 12V ✔ Power supply AC 100 ~ 240V ✔ PoE Class 3: IEEE802.3af (optional) ■ Keys: ✔ VOICE MAIL message hotkey (including LED) ✔ 4-way navigation button with OK key ✔ MENU ✔ HOLD ✔ MUTE (including LED) ✔ TRANSFER ✔ VOLUME control key ✔ HEADSET (including LED) ✔ SPEAKER (including LED) ✔ BACK ✔ CONTACTS ✔ Teams home key

Allowing URLs, Ports (Security)

This section guides 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	-

Server Role	Service Name	Port	Protocol	Notes
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 below
- 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 the next page
- See Web Browser on the next page
- 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 7
- See Keystore on page 7
- See Device Certificate on page 8
- See Data Protection on page 8
- See Debugging Interface on page 8
- See Android Security Updates on page 8

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)

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 the next page.
- 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 the C470HD, C435HD and C450HD-DBW devices. 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.

Data Protection

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

Debugging Interface

- The 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.

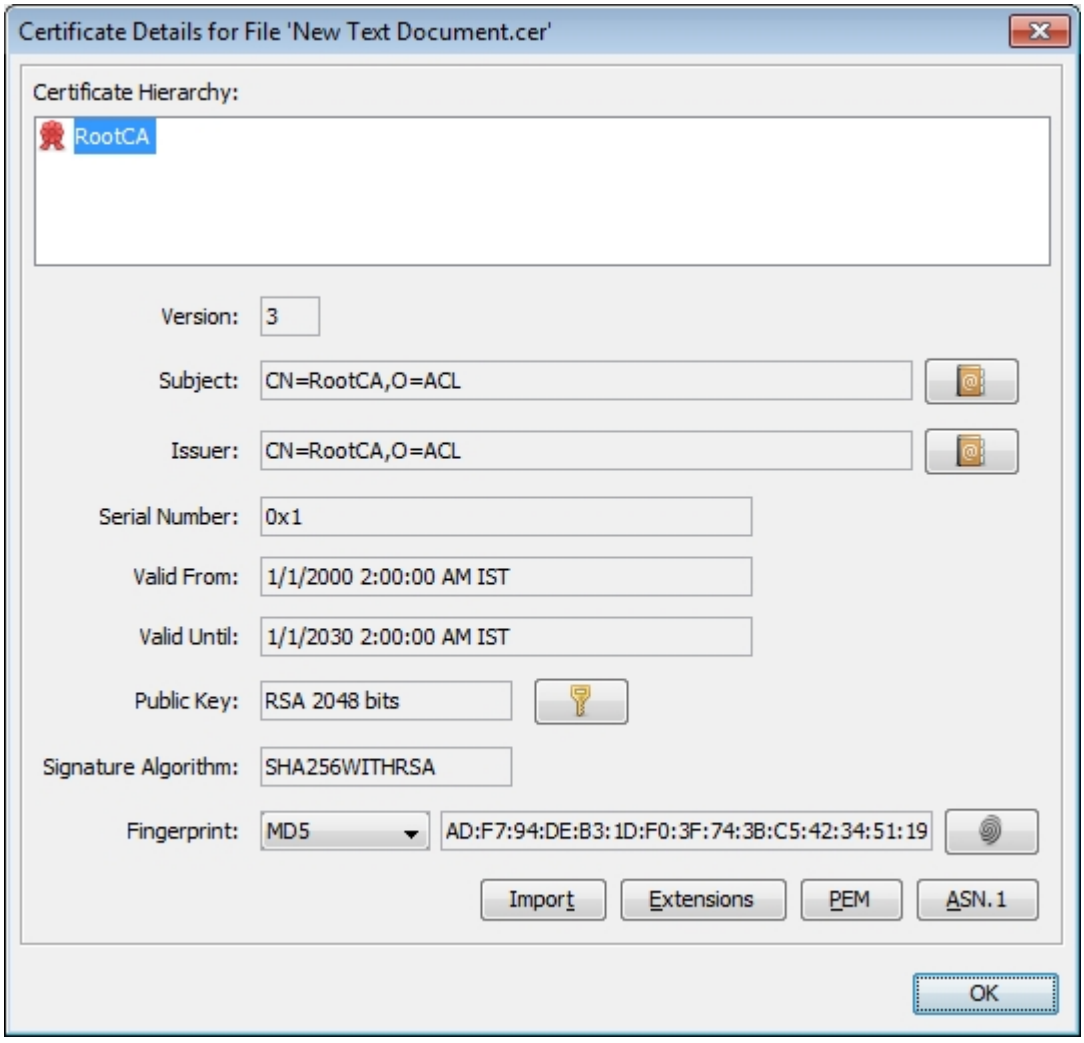
Android Security Updates

AudioCodes regularly adopts and integrates Android security updates.

For reference, see here.

AudioCodes Root CA Certificate

The following figure shows the AudioCodes Root CA Certificate.



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

MIIDMTCCAhmgAwIBAgIBATANBgkqhkiG9w0BAQsFADAfMQwwCgYDVQQK
EwNBQ0wx

DzANBgNVBAMTBlJvb3RDQTAeFw0wMDAxMDEwMDAwMDBaFw0zMDAxM
DEwMDAwMDBa

MB8xDDAKBgNVBAoTA0FDTDEPMA0GA1UEAxMGUm9vdENBMIIBIjANBgkq
hkiG9w0B

AQEFAAOCAQ8AMIIBCgKCAQEA6GK495KUCXAm/UE17G4/cjnZN4LNaxYE
YzbfZL0a

EhgSKYt/LQ+iUcDhojsneusNgrcGkpwKklKsGsvGWmSRNULV01CW+TX2VJN7
3+hh
V0uzhyOIYAUhbDaoqNM6Kp5b7sJ1ew4Ig9kfd/ma9Czl5koESLlw/inLj/r+rD96

mUcPEIWrKspv7Qy4I14fsK/yMArixRopTL1munVVPpSFM9Jh8IY3JHyr5CQJXK
Ks
EhGAJsnHaRqsR2Su3X/WtslgEF+cvP34pxhlhFL29nMfnaFATSS3rgGaFlSvl1ZS

esLMqkWjp9cqGYrvt7K61sYnvMMb+o/KbWqVokXb+Fr7bwIDAQABo3gwdjAMB
gNV

HRMEBTADAQH/MB0GA1UdDgQWBBQDXySn9hz15lDraZ+iXddZGReB+zBH
BgNVHSME

QDA+gBQDXySn9hz15lDraZ+iXddZGReB+6EjpCEwHzEMMAoGA1UEChMDQ
UNMMQ8w

DQYDVQQDEwZSb290Q0GCAQEwDQYJKoZIhvcNAQELBQADggEBAI0rUyw
ommWWJnH3

JOfKiS3+VnX5hJITZymvWanMXUz/6FonHccPXEBYTrUYwhiWx3dwELAFXDF
KkxMp

0KKWZ4F39cAOLRjqhzya+xUeeJ9HQZCXYAJ6XgvTfN2BtyZk9Ma8WG+H1hN
vvTZY

QLbWsjQdu4eFniEufeYDke1jQ6800LwMlFlc59hMQCeJTenRx4HdJbJV86k1gBU
E

A7fJT1ePrRnXNDRz6QtADWoX3OmN7Meqen/roTwvLpEP22nYwvB28dq3JetI
QKwu

XC4gwI/o8K2wo3pySLU9Y/vanxXCr0/en5l3RDz1YpYWmQwHA8jJIu8rxdhr+VN
Q
Zv6R/Ys=
-----END CERTIFICATE----

2 Setting up the Phone

Unpacking

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

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

For detailed information, see the phone's *Quick Guide* shipped with the device or available from AudioCodes.

Device Description

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

Front View

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

Figure 2-1: Front View

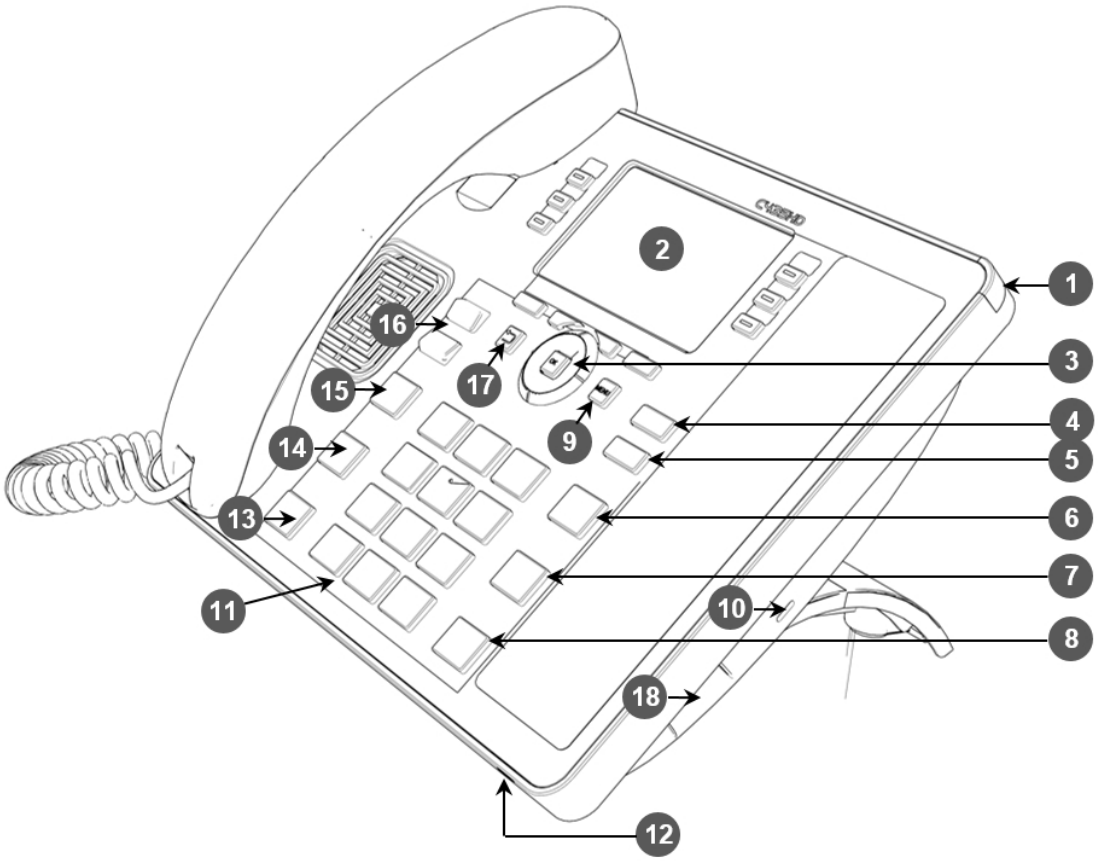


Table 2-1: Font View Description

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

Item #	Label Name	Description
		displays calling information.
3	Navigation Control / OK	■ Press the button's upper rim to scroll up menus / items. ■ Press the button's lower rim to scroll down. ■ Press the button's left or right rim to move the cursor left or right (when editing a contact number for example). ■ Press **OK** to select a menu/item/option.
4	Voicemail	Retrieves voicemail messages.
5	CONTACTS	Accesses the People screen.
6		Returns you to the Teams home screen.
7	TRANSFER	Transfers a call to another party.
8	HOLD	Places an active call on hold.
9	MENU	Accesses the Settings screen.
10	Kensington lock	Allows locking the device.
11	Alphanumerical Keypad	Keys for entering numbers, alphabetical letters and symbols (e.g., colons)
12	Microphone	Allows talking and

Item #	Label Name	Description
		listening. The network administrator can disable it if necessary.
13	Speaker	Activates the speaker, allowing a hands-free conversation.
14	Headset	Activates a call using an external headset.
15	Mute	Mutes a call.
16	▲ VOL ▼ VOL	Increases or decreases the volume of the handset, headset, speaker, ring tone and call progress tones.
17	'Back' key	Returns you back to the previous screen.
18	USB port	Allows using a USB headset if necessary.

Navigate to menus and select menu items by:

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

Rear View

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

Table 2-2: Rear View Description

Item #	Label	Description
1		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).
2		RJ-45 port to connect the phone to a PC (10/100/1000 Mbps downlink).
3		12V DC power jack that connects to the AC power adapter.
4	AUX	[RJ-11 port] Used as a serial console port to access the phone's terminal.
5		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:**

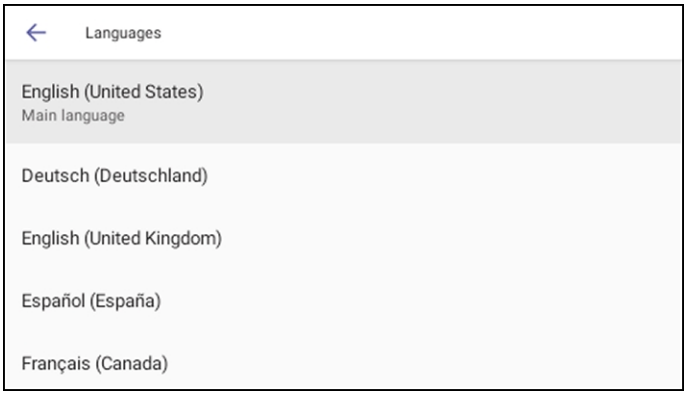
1. Disconnect all cables.
2. Spray onto a clean, dry, microfiber duster a medicinal isopropyl alcohol and water solution of 70:30. Don't oversaturate the duster. If it's wet, squeeze it out.
3. Lightly wipe the screen of the device.
4. Wait for the screen to dry before reconnecting cables.

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.



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

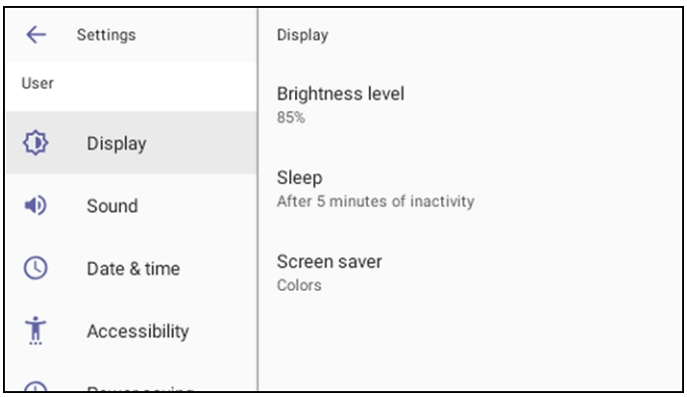
It will be necessary to repeat this only if the phone is restored to default settings.

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.

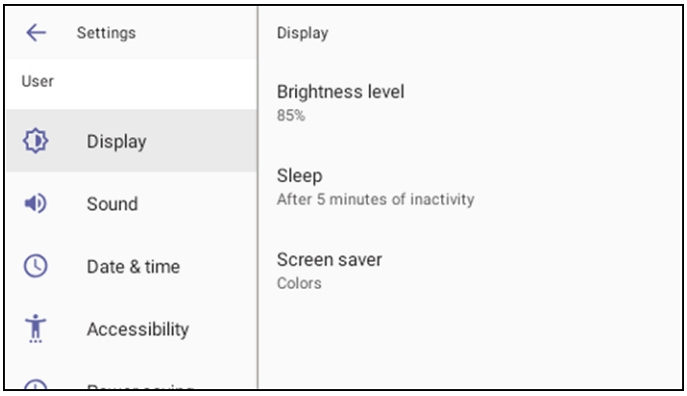
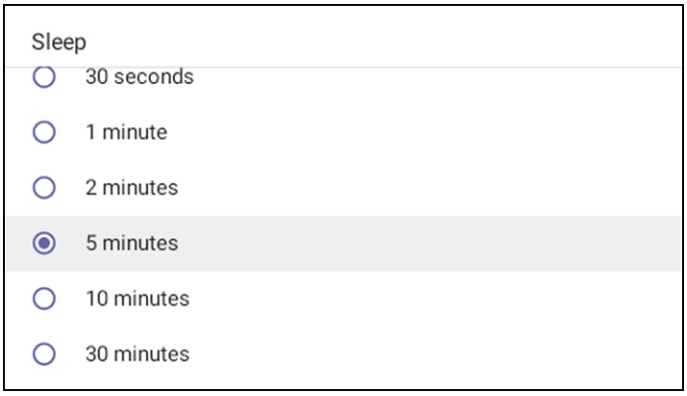
➢ **To access device settings:**

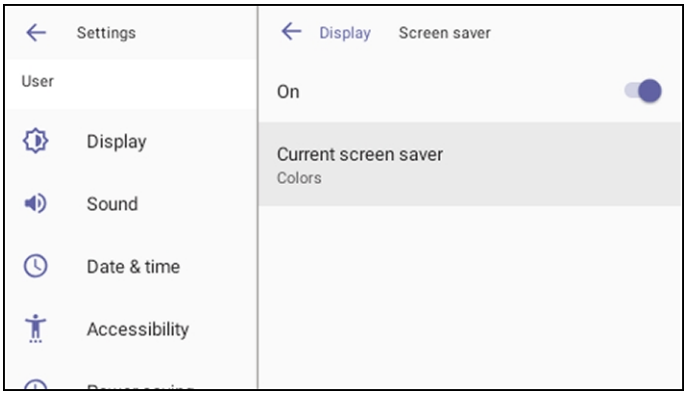
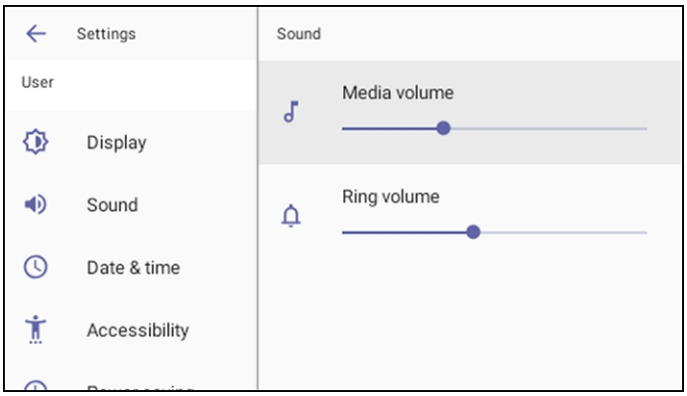
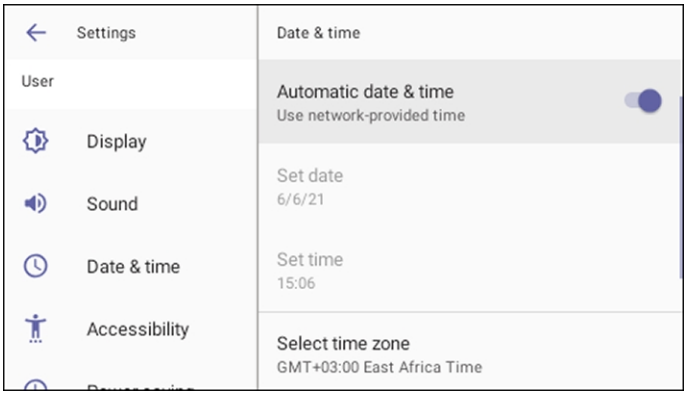
1. In the home screen, select ☰, select **Settings** and then press the **Settings** softkey.

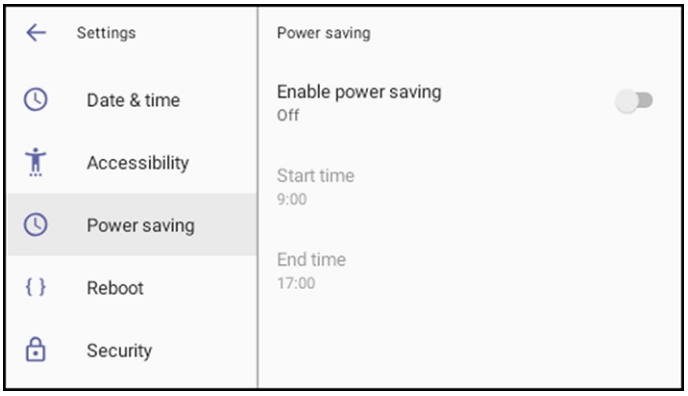
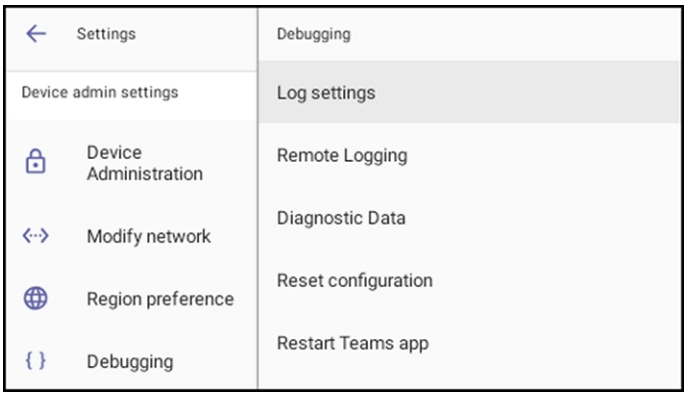


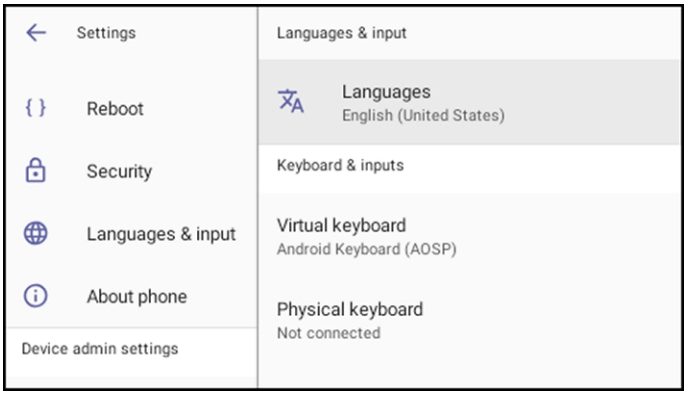
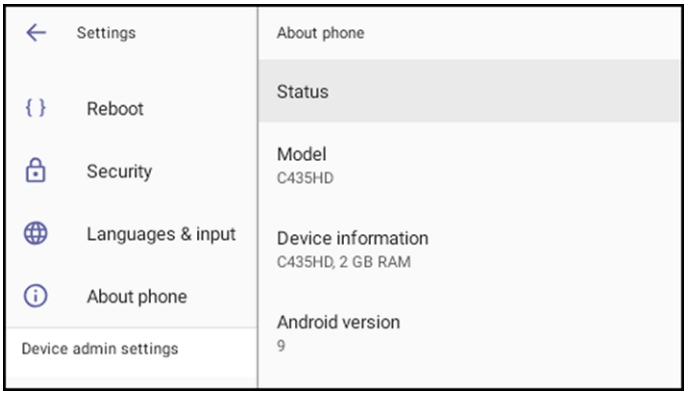
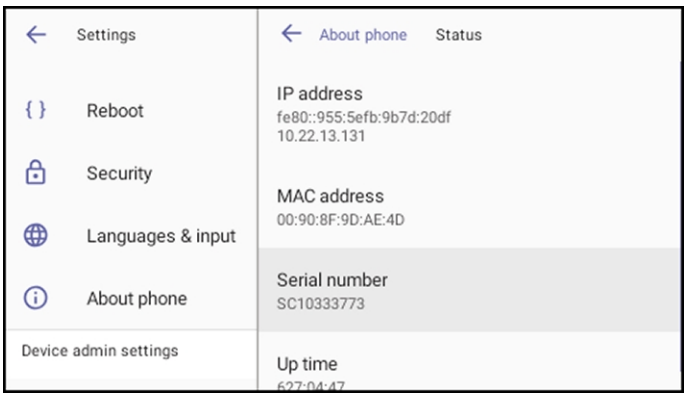
2. View the settings under 'User'. Select a setting to open it. Use the table following as reference. [To view settings related to the network administrator, scroll down and open 'Device Administration'].

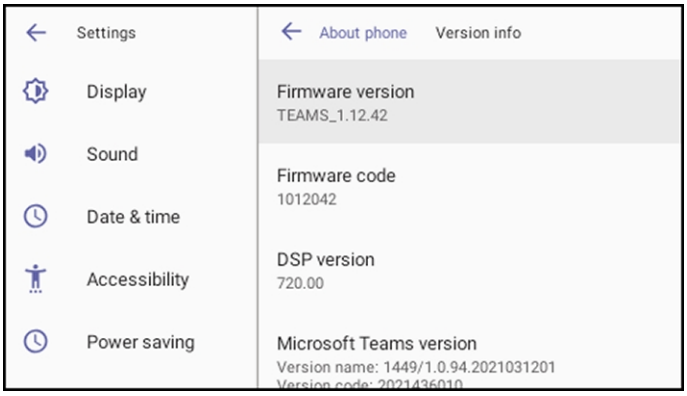
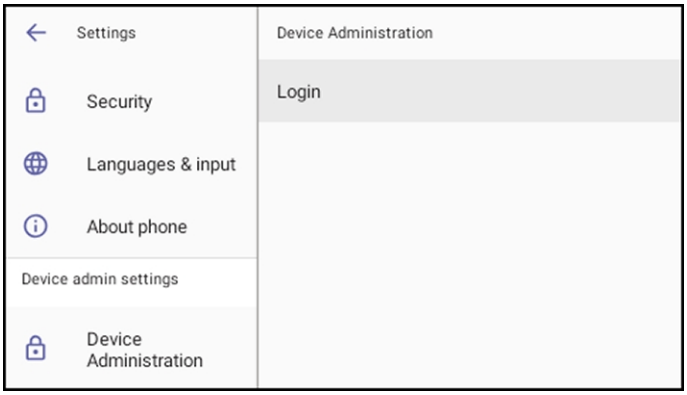
Table 3-1: Device Settings

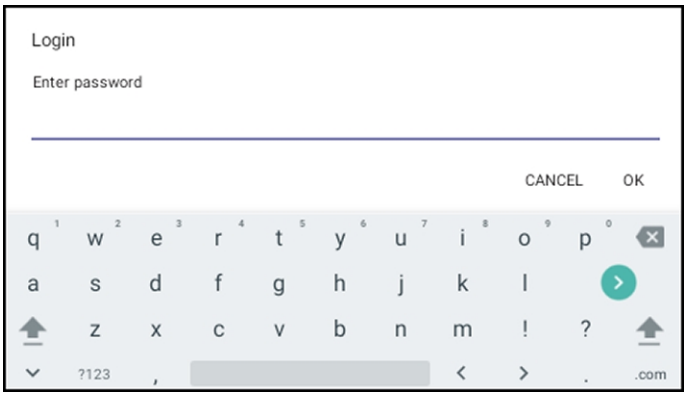
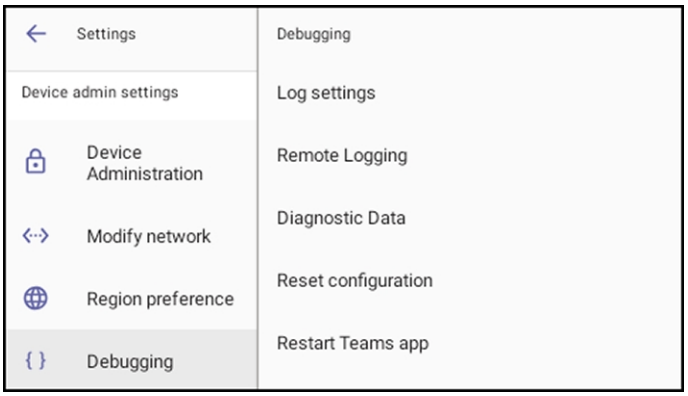
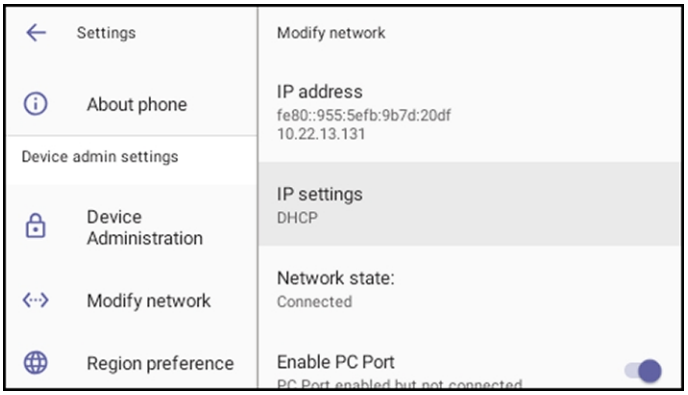
Setting	Description
User	
Display	Opens the 'Display' screen [Brightness level].  The phone's screen supports different brightness levels. Choose the level that suits your requirements. ■ Sleep  ■ Screen saver

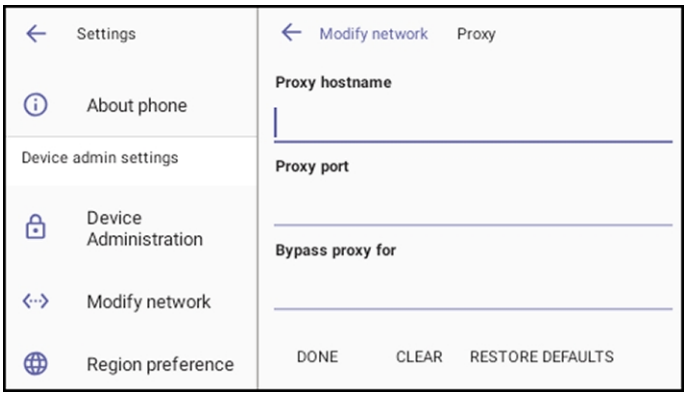
Setting	Description
	
Sound	Allows you to customize phone volume for a friendlier user experience. **Ring volume at n%** 
Date & time	Date and time are automatically retrieved from the deployed Network Time Protocol (NTP) server.  Use 24-hour format [Allows you to select the Time format]
Power Saving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

Setting	Description
	 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.  Log in as Administrator for more debugging settings to be available.
Security	Helps secure the enterprise telephony network against breaches. Screen lock [The phone automatically locks after a configured period to secure it against unwanted use. If left unattended for 10 minutes (default), it automatically locks and is inaccessible to anyone who doesn't know its lock code.] Make passwords available See 'Lock Screen & PIN' under Configuring Teams Application Settings on page 44
Languages & input	Allows users to customize inputting to suit personal requirements.

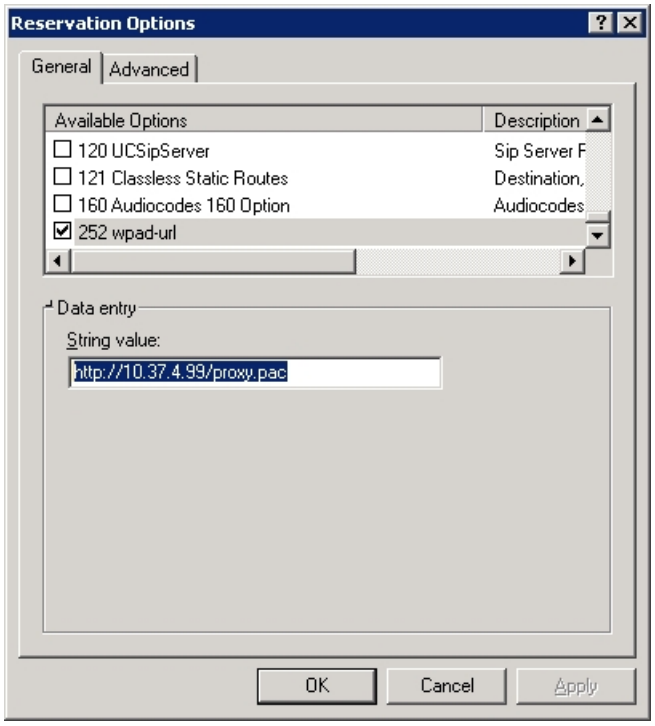
Setting	Description
	
About [Android 7.1.2]	Enables users to determine device information.  To determine the device's IP address, select the 'Status' option.  To get information about the version, select 'Version info'.

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

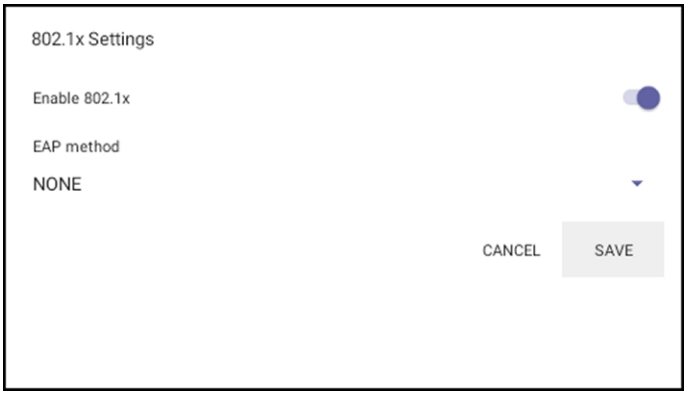
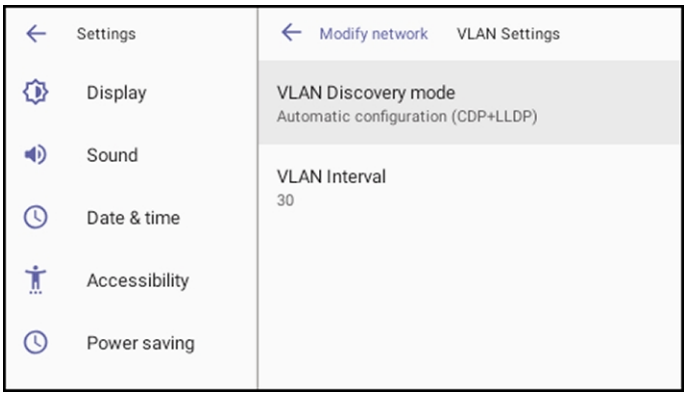
Setting	Description
	'Settings' fields to allow inputting characters and / or numbers. Two virtual keyboard types can be displayed: Numeric or QWERTY.  The virtual keyboard is also displayed when the network administrator needs to enter an IP address to debug, or when they need to enter their PIN lock for the security tab. After logging in, scroll down in the Settings screen to the section 'Device Administration'. 
Modify network	Enables the Admin user to determine network information and to modify network settings.  IP Address [Read Only]

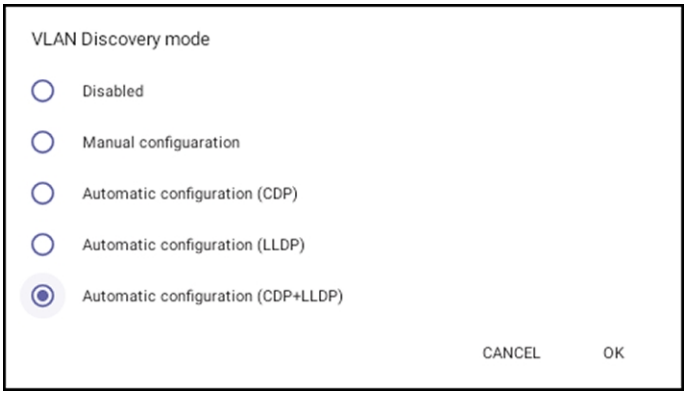
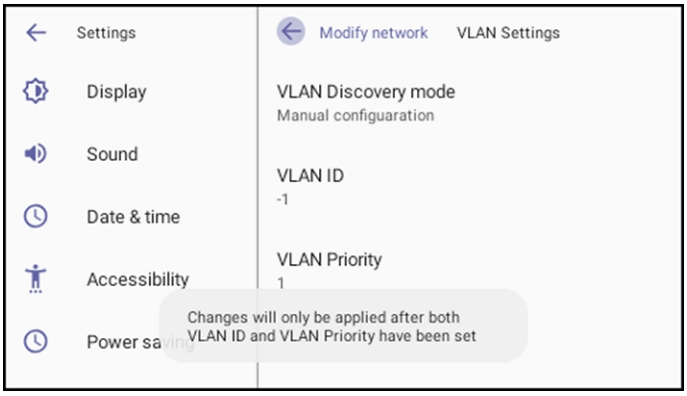
Setting	Description
	IP Settings [DHCP or Static IP] Network state [Read Only] Enable PC port Enable PC port mirror Proxy 802.1x Settings VLAN Settings. Allows you to configure the VLAN mode **Manual**, **CDP only** or **LLDP only**.
Proxy	The phone can be configured with an HTTP Proxy server by an Admin 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:  ■ **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:

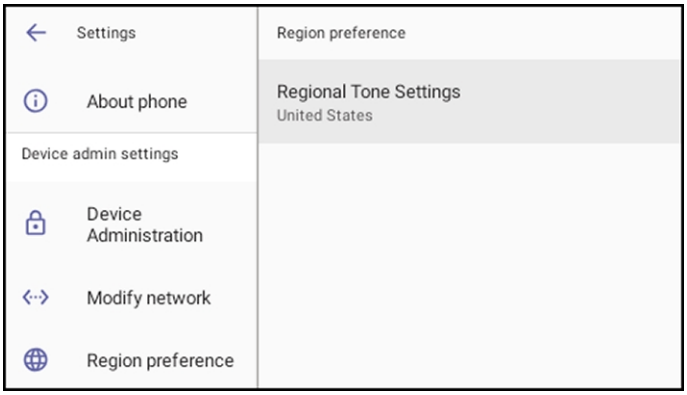
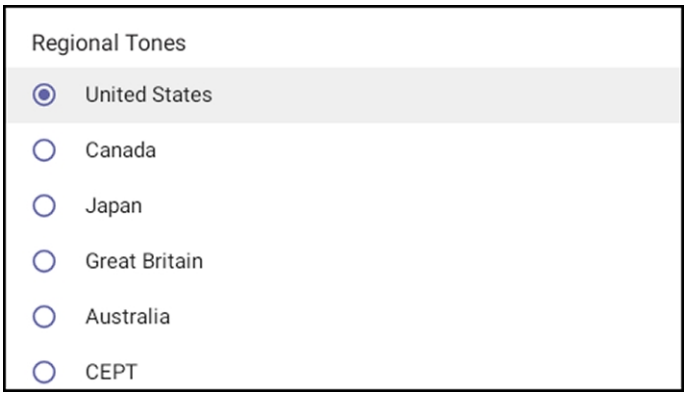
Setting	Description

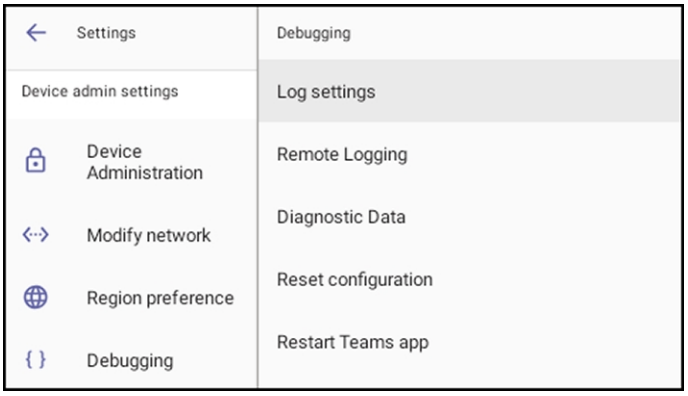
	
	The proxy setting is provided in a Proxy Auto-Configuration (PAC) file that contains a set of rules coded in JavaScript which allows a web browser to determine whether to send web traffic directly to the Internet or to be sent via a proxy server. PAC files control how the phone handles HTTP, HTTPS and FTP traffic.
	Example of a basic PAC file:
	function FindProxyForURL(url, host)
	{
	return "PROXY 10.13.2.40:3128";
	}

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:** 1. From the 'Modify Network' screen (as an Admin), access the 802.1x Settings screen.

Setting	Description
	 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
VLAN Settings	Select the menu option **VLAN Settings**.  Select **VLAN Discovery mode**.

Setting	Description
	 ■ 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:  Select **VLAN ID**.  Select **VLAN Priority**.

Setting	Description
	
Region preference	Select the menu option **Region preference**.  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. 
Debugging	Allows the Admin user to perform debugging for troubleshooting purposes. Available after logging in as Admin.

Setting	Description
	 Log settings Remote Logging (see under Remote Logging (Syslog) on page 82 for more information) Diagnostic Data (see under Getting Diagnostics on page 83 for more information) Reset configuration Restart Teams app Company portal login Debug Recording (for Media/DSP debugging) (see under Remote Logging (Syslog) on page 82 for more information) Switch to Teams Compatible 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; leave it unchanged at the default unless there's a real necessity to use it. 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

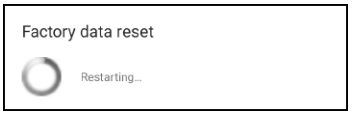
You can either:

- perform a hard restore while the phone is up and running (see below)

- restore the phone's settings to their defaults when the phone is not connected (see below)

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

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



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

2. Select **OK**; the sign-in screen is displayed (see Signing In on page 33 for more information).

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

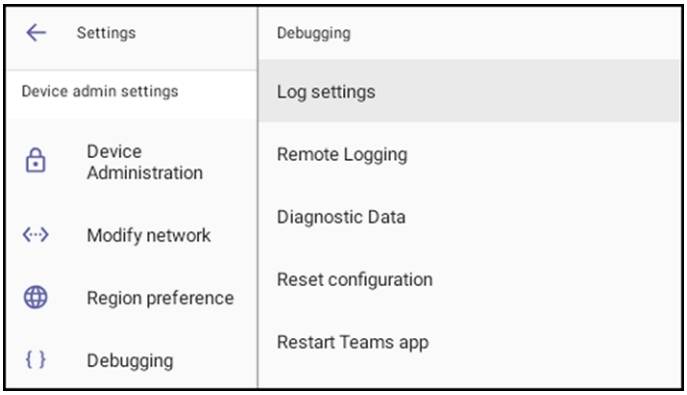
1. Press the OK + MENU keys simultaneously and keeping them pressed, unplug the power cable.
2. Plug the power cable back into the phone continuing to press the OK + MENU keys for +-5 seconds.
3. Release the OK + MENU keys; the phone' settings are restored to their defaults.

Performing a Soft Restore

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

➢ **To perform a soft restore:**

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



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

Recovery Mode

If a phone goes into recovery mode, you can boot it using its hard keys as shown in Performing a Hard Restore on page 29.

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. Make sure the phone is configured with any of the lock options before attempting to lock it. If a lock option isn't configured, the lock action won't work.

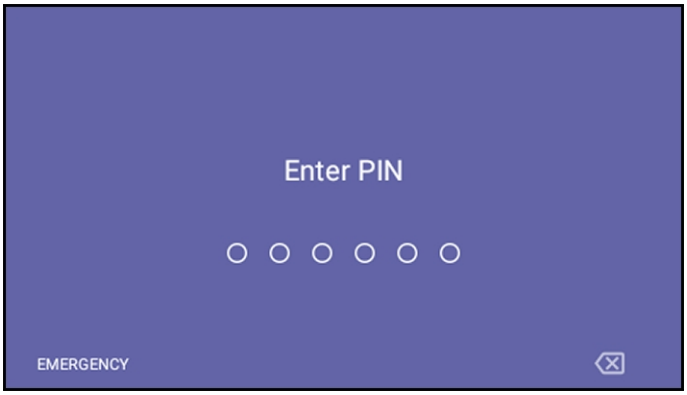
➢ **To lock the phone:**

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

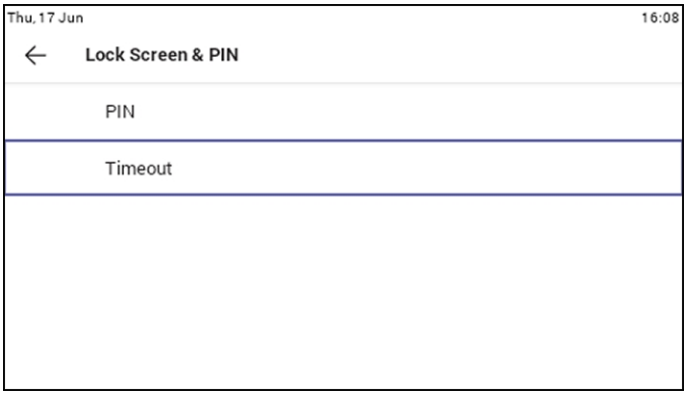
Unlock

➢ **To unlock the phone:**

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



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



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

4 Teams Application

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

Signing In

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

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

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

'Modern Authentication' is also supported.

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

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

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

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

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

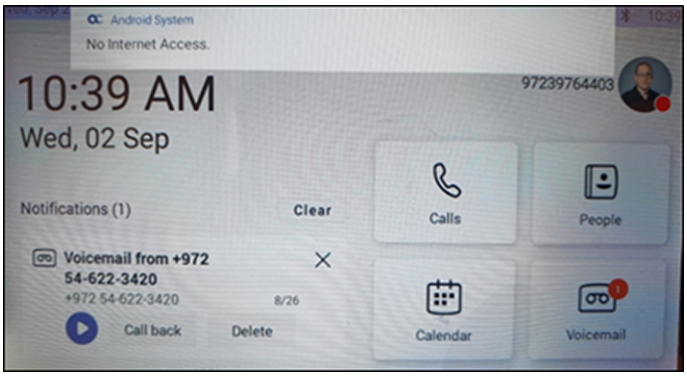
https://www.google.com/generate_204

http://connectivitycheck.gstatic.com/generate_204

http://www.google.com/gen_204

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

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

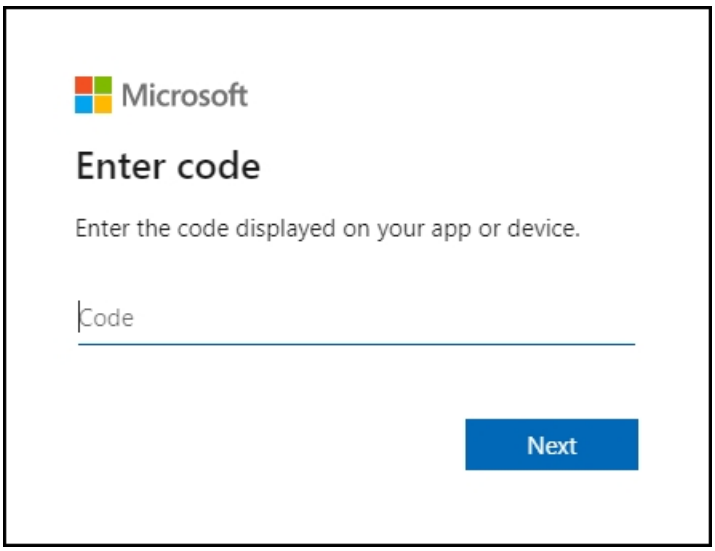


This can point to a problem that is preventing the phone from fully functioning in a Teams environment. The user can ignore the message if the Teams application is fully functioning, or can report a problem if the Teams application is not fully functioning.

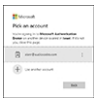
➢ **To sign in:**

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

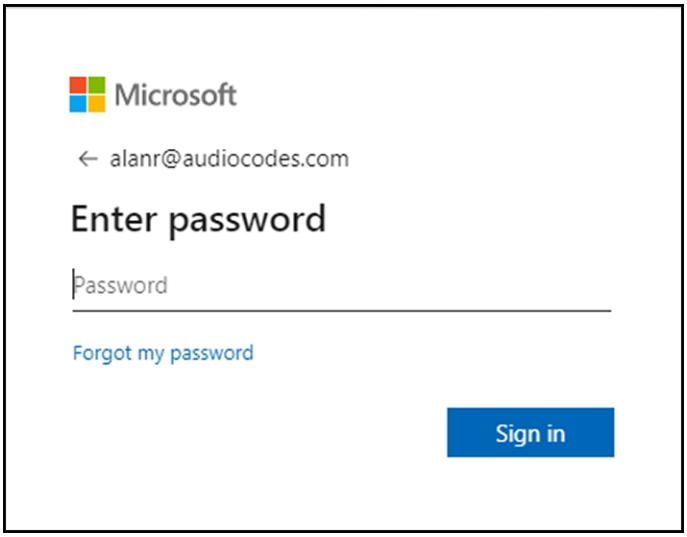
2. Open your browser and point it to **https://microsoft.com/devicelogin** as instructed in the preceding screen.



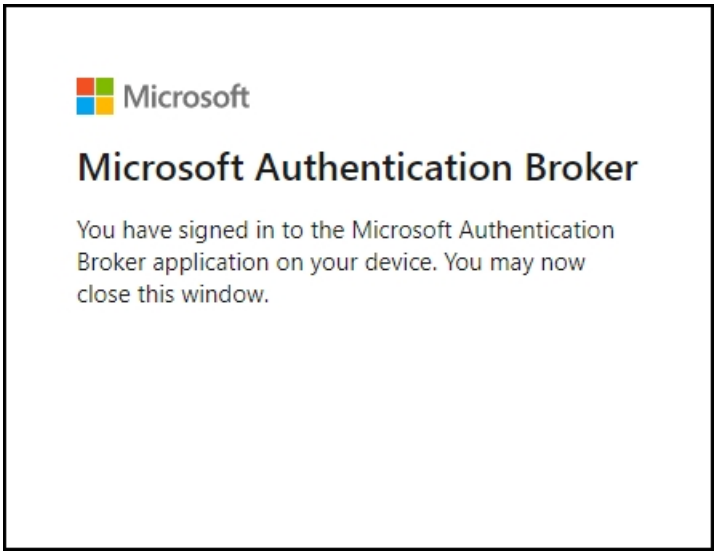
3. Enter the code and then click **Next**.



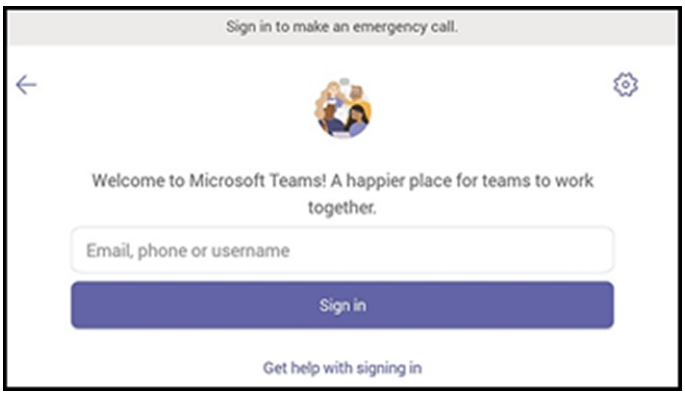
4. Click the account.



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



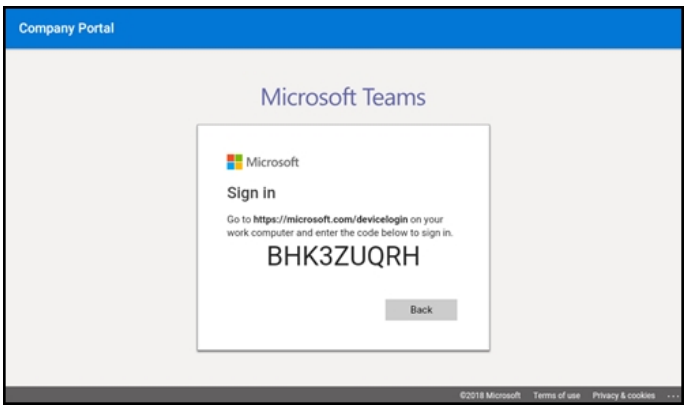
6. Close the window shown in the preceding figure.
7. Observe that the phone returns to the initial code screen. In that screen, select **Sign in on this device**.



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

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

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

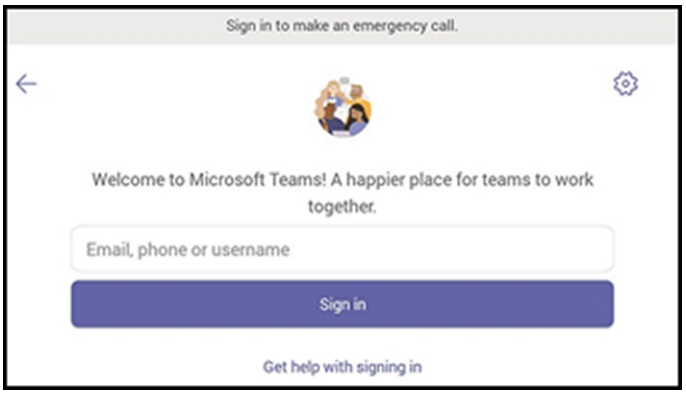


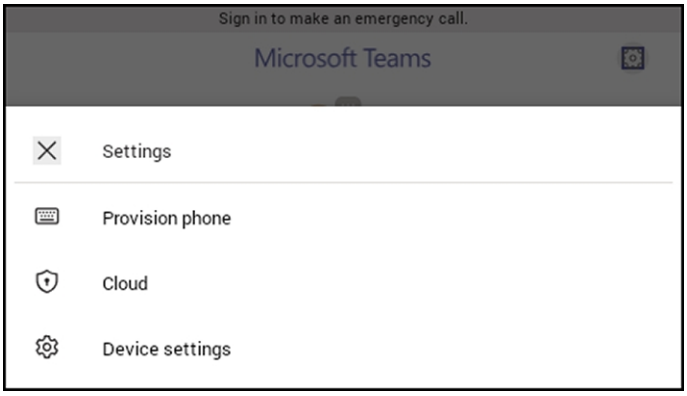
   - In the browser on your PC or smart phone, enter the URL indicated in the preceding screen and then in the phone's Web interface that opens, perform sign-in (as noted previously, this option is recommended if using MFA).

LLDP-MED (Link Layer Discovery Protocol – Media Endpoint Discovery) is a standard link layer protocol used by network devices to advertise their identity, capabilities, and neighbors on a local area network based on IEEE802 technology, principally wired Ethernet. Teams devices connected to the network via Ethernet will dynamically update location information for emergency calling services based on changes to network attributes including chassis ID and port ID.

Multi-Cloud Sign-in

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





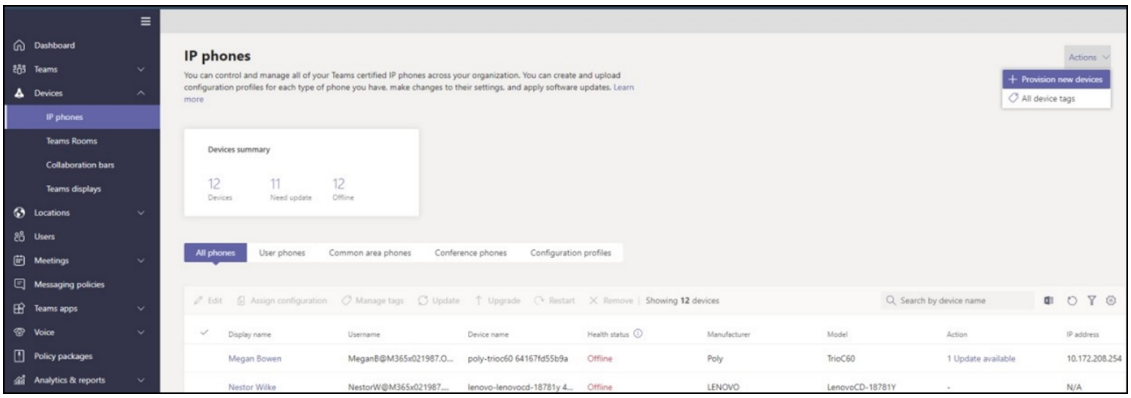
Remote Provisioning and Sign-in from Teams Admin Center

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

➢ Step 1: Add a device MAC address

Provision the device by imprinting a MAC address on it.

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



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

Manually add a device MAC address

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

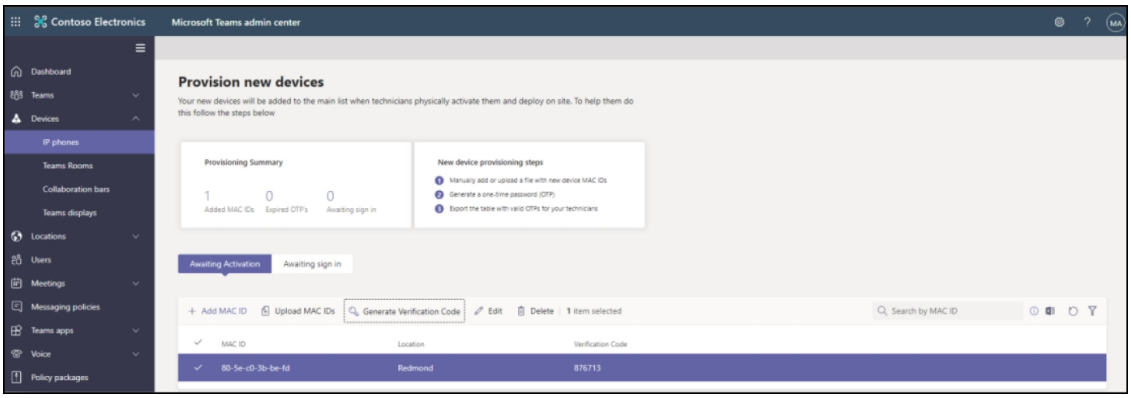
Upload a file to add a device MAC address

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

➢ Step 2: Generate a verification code

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

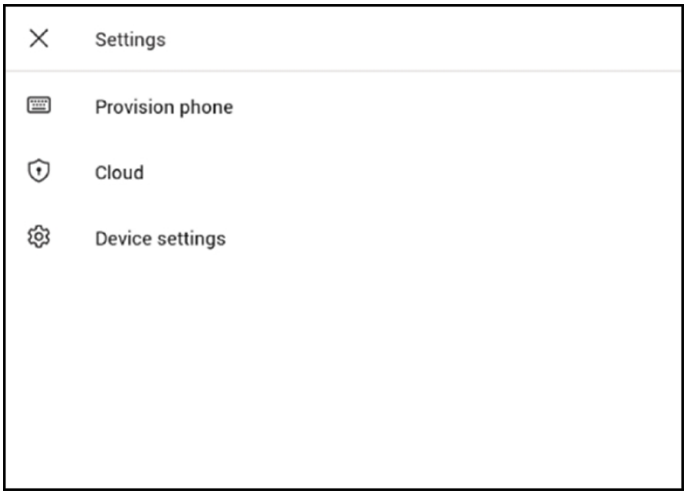
From the **Awaiting Activation** tab, select an existing MAC ID. A password is created for the MAC address and is shown in the **Verification Code** column.



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

➢ Step 3: Provisioning on the device

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

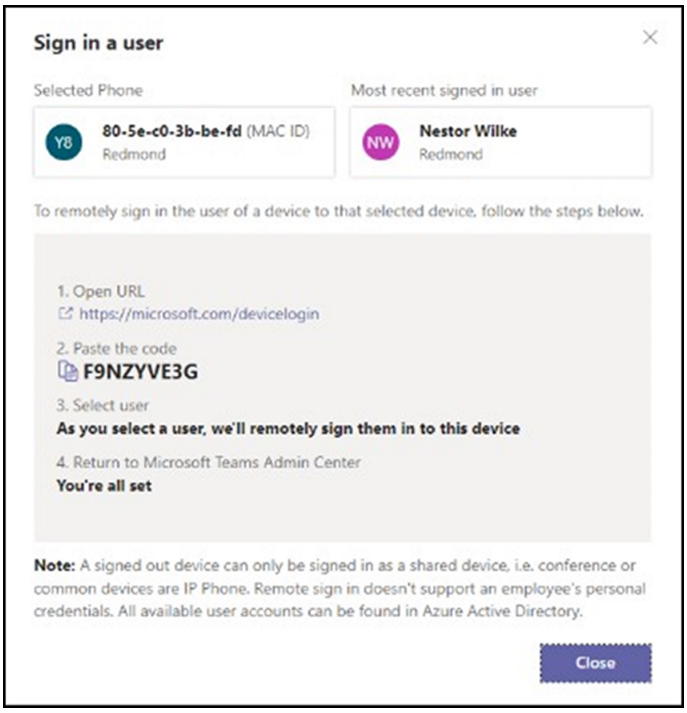


The technician is then expected to enter the device-specific Verification code that was provided in the Teams admin center on the phone's user interface. Once the device is provisioned successfully, the tenant name will be available on the sign in page.

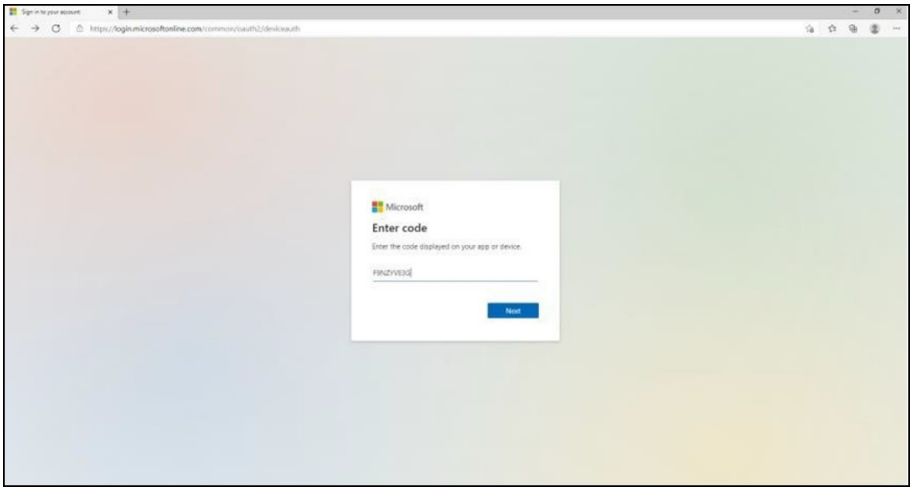
➢ Step 4: Sign in remotely

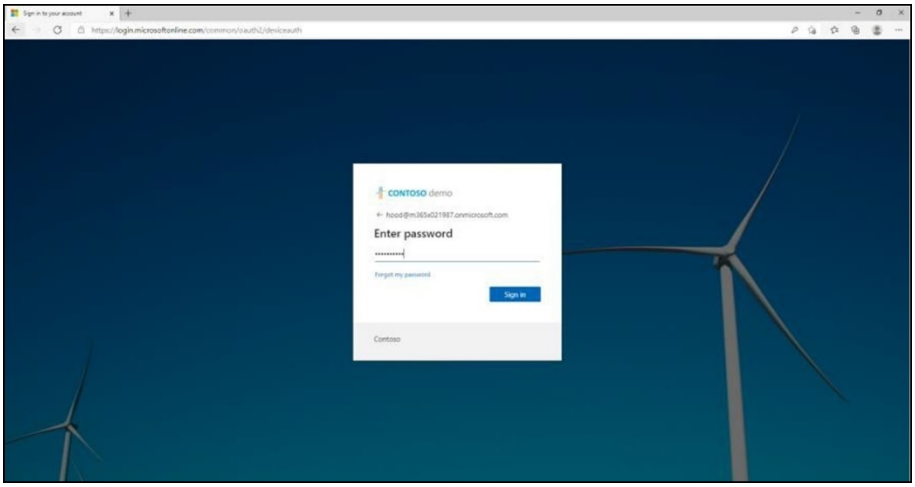
The provisioned device appears in the Awaiting sign in tab. Initiate the remote sign-in process by selecting the individual device.

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



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

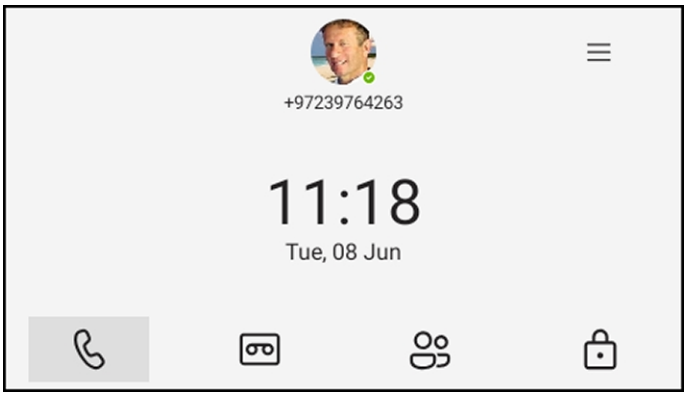




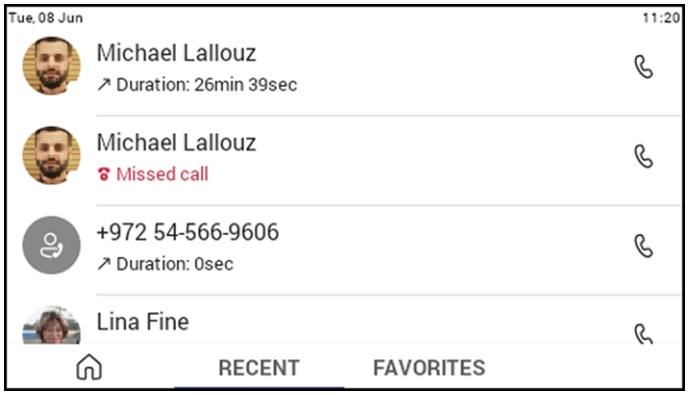
When the tenant admin is signing in from Teams Admin Center, the user interface on the device is blocked to prevent other actions on the phone.

Getting Acquainted with the Phone Screen

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



The following figure shows the phone's Calls screen.



The following table describes the phone's home screen.

Table 4-1: Calls Screen

Item	Description
Calls	Select the tab to open the Calls screen. The screen shown in the figure preceding this table opens.
People	Select the tab to open the People, shown under Using the People Screen on page 47 opens. Allows you to easily connect and collaborate with teammates, colleagues, friends and family. Through this screen, you can see all your contacts and create and manage contact groups to organize your contacts. The screen provides a simple user experience and aligns with the contacts on the Teams desktop client. If a contact has multiple numbers, the phone screen allows the user to select from a drop-down menu the intended contact method.
Calendar	Select to open the Calendar screen, shown under Setting up a Meeting opens.
Voicemail	Select the tab to open the Voicemail screen, shown under Accessing Voicemail on page 48 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 for more information.
Settings	See Configuring Teams Application Settings on the next page for more information.

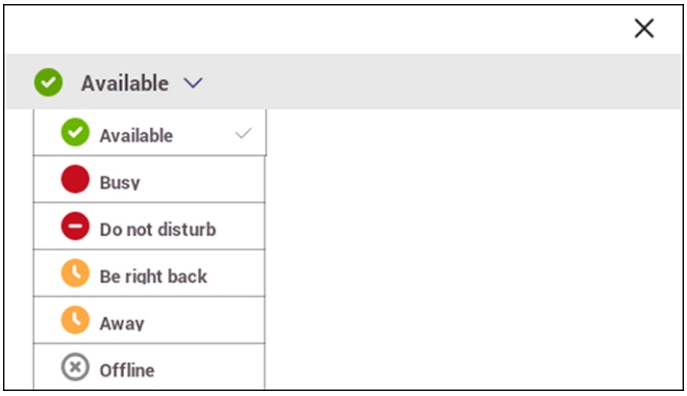
Setting Status

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

➢ **To set presence status:**

1. In the home screen, select ☰.

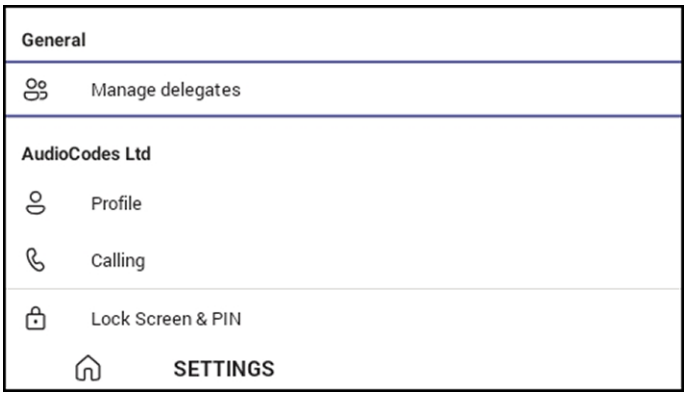
2. Select the status displayed; in the preceding figure, 'Available' is displayed.



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

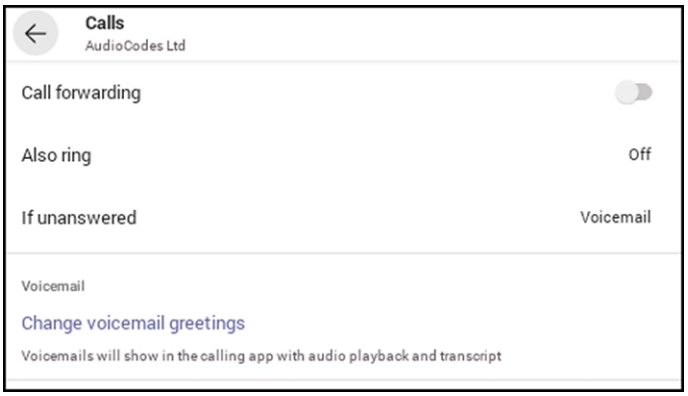
Configuring Teams Application Settings

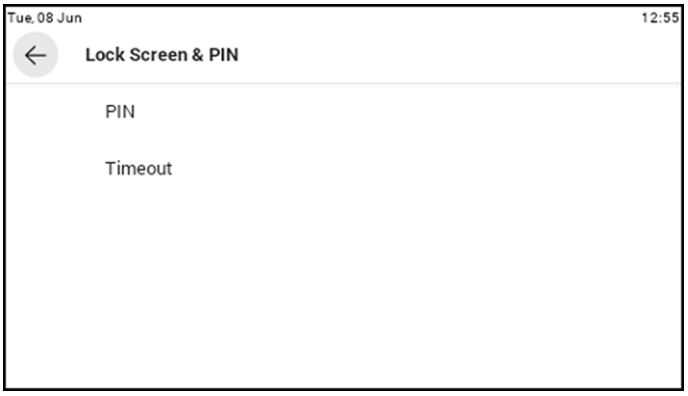
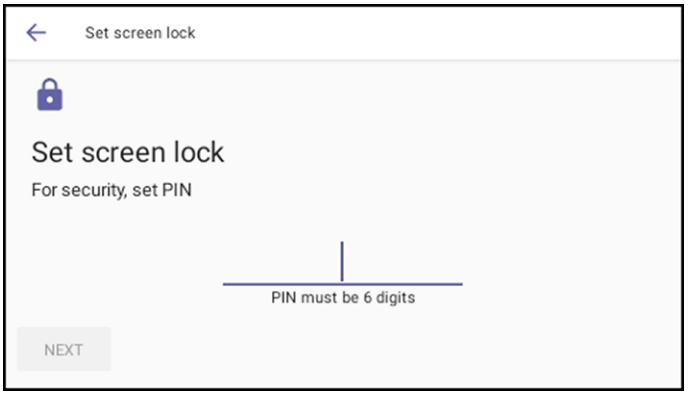
The following describes the Teams application's settings. In the home screen, select ☰.

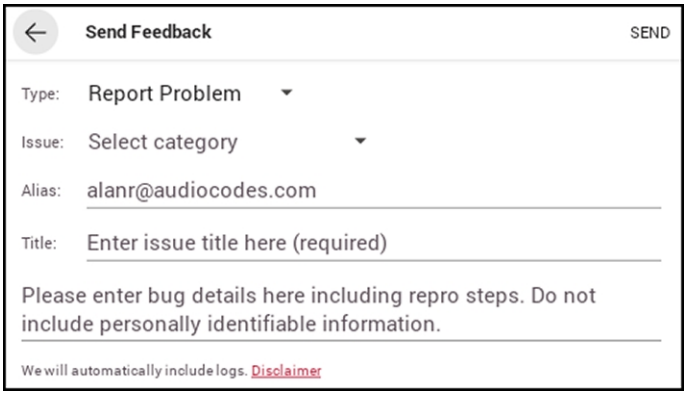


Use this table as reference:

Table 4-3: Idle Screen Description

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

Item	Description
	 Configure a lock option before attempting to lock the phone.   If a lock option isn't configured, the lock action won't work. To unlock a locked phone, see Unlock on page 31.
Report an issue	Opens the Send Feedback screen.

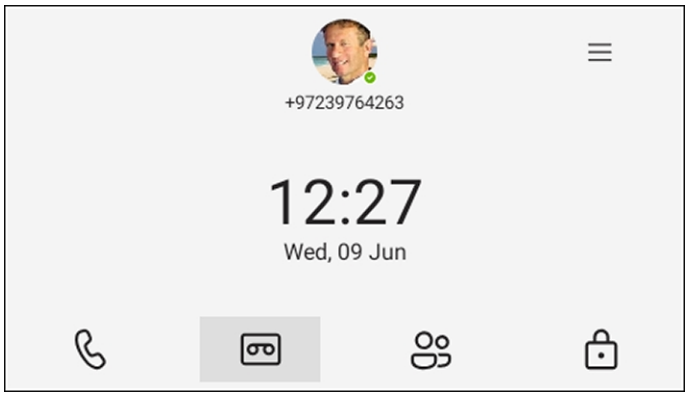
Item	Description
	
About	Opens the About screen. 
Sign out	Lets you sign out of the phone application as one user and optionally sign in again as another user. See Signing Out on page 49 for detailed information.
Device Settings	Opens the [Device] Settings screen. See Configuring Device Settings on page 17 for detailed information.

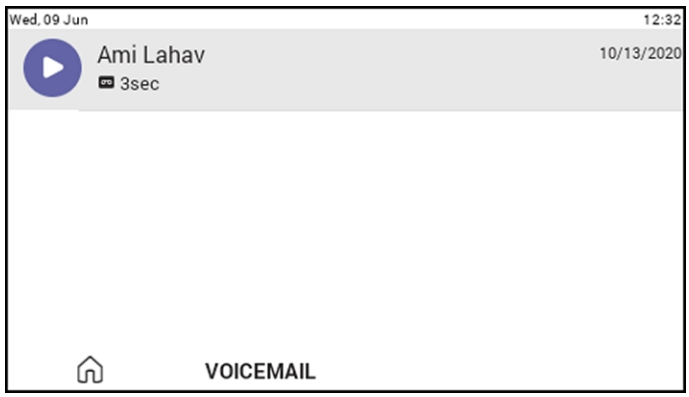
Using the People Screen

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

Accessing Voicemail

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





Using Audio Devices

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

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

You can easily change audio device during a call.

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

Transferring Calls and Meetings across Devices

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

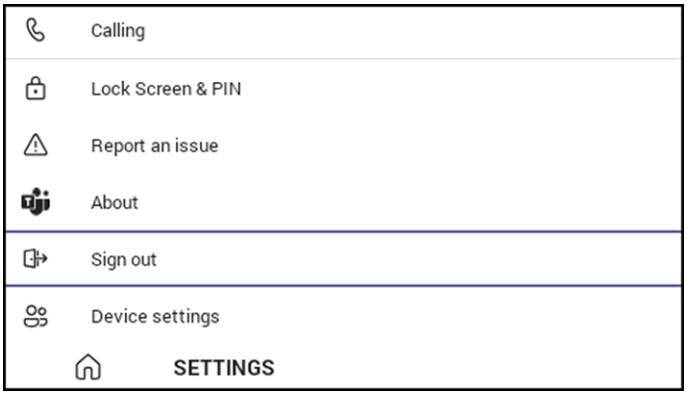
The feature enables the user to move away from their PC while seamlessly staying connected. The phone recognizes the user is in a call on another device and prompts them to transfer or add, letting them start their call from elsewhere and transfer to their desk phone.

Signing Out

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

➢ **To sign out:**

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



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

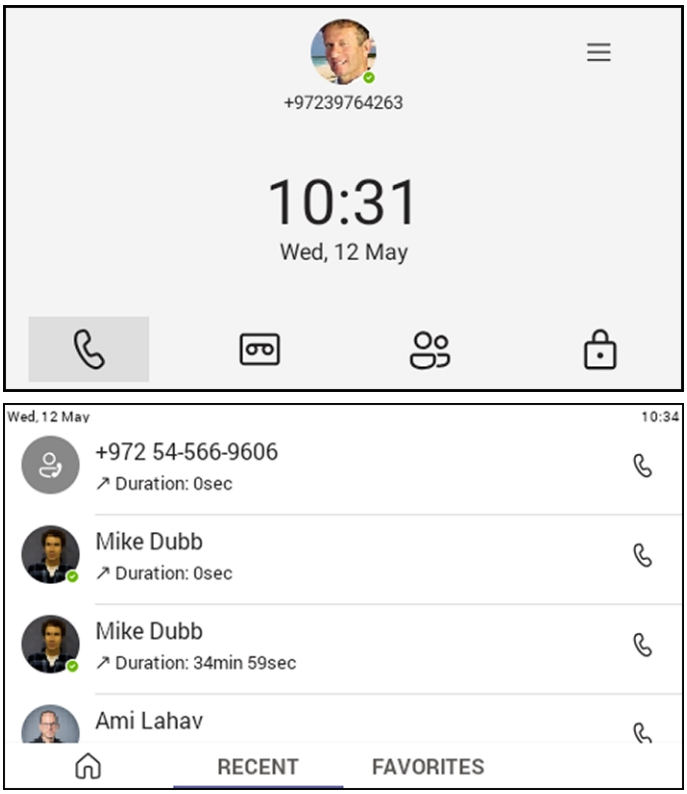
5 Performing Teams Call Operations

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

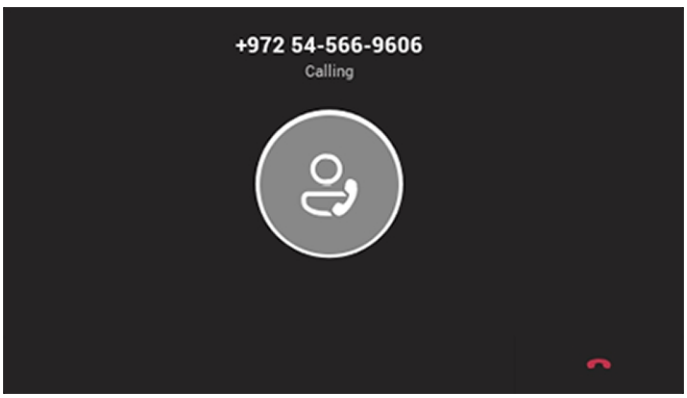
Making a Call

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

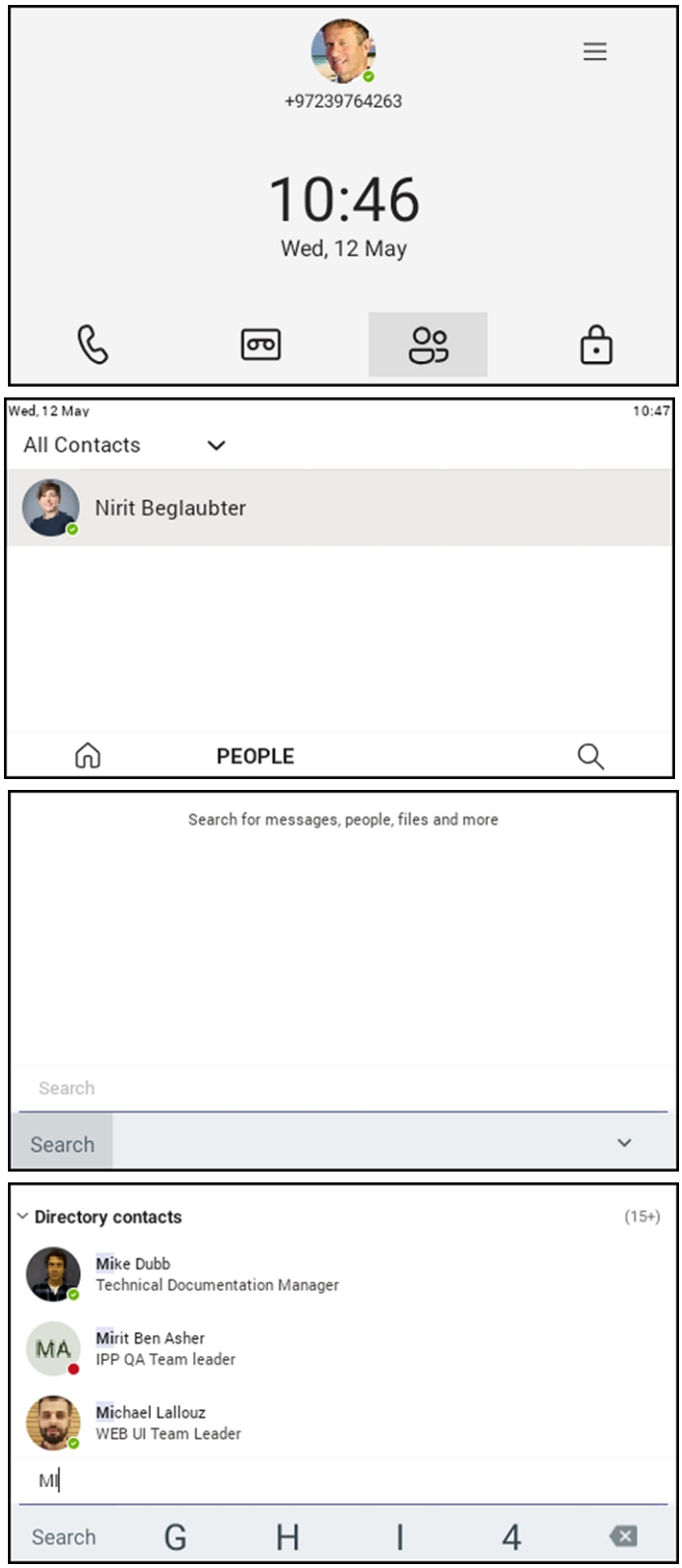
Alternatively, in the home screen you can press the softkey and in the RECENT screen that opens you can navigate to a recent call and then press the **OK** button.



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



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



Dialing a Missed Call

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

➢ **To dial a missed call:**

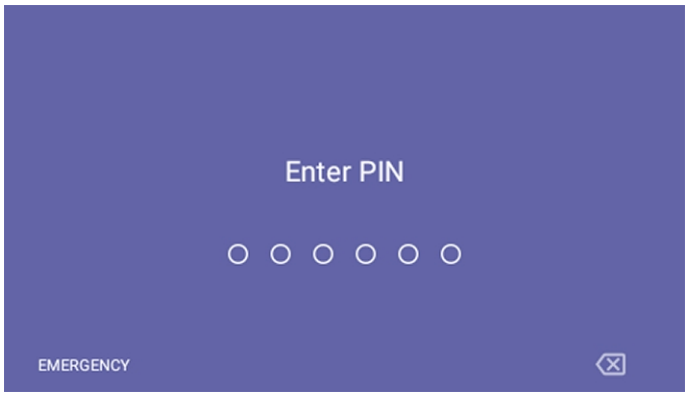
- In the home screen, select the icon and then in the 'Recent' screen that opens navigate to and select the missed call.

Select to Dial

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

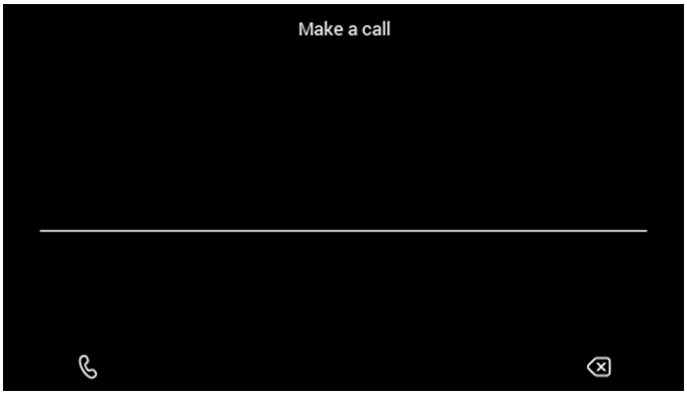
Making an Emergency Call

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



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

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



Answering Calls

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

➢ **To answer:**

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

Ending an Established Call

You can end an established call in a few ways.

➢ **To end an established call:**

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

Managing Calls

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

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

➢ **To manage calls:**

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

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

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

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

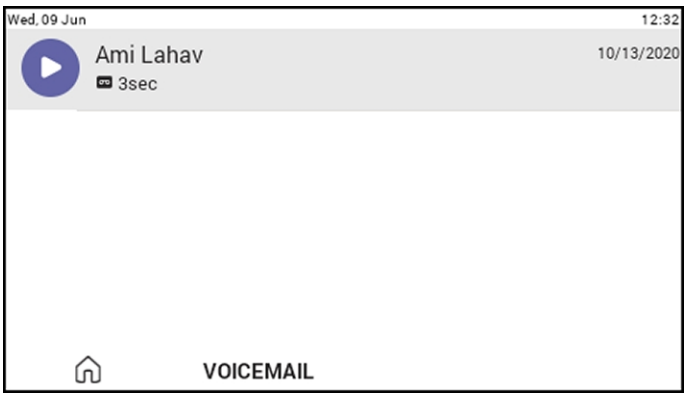
Users can directly transfer a call into someone's work voicemail without needing to ring the far-end user. This allows them to discreetly leave voicemails for users without interrupting them.

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



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

   For more information, see here.

Rejecting an Incoming Call, Sending it Directly to Voicemail

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

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

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

Adjusting Volume

The phone allows

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

- Adjusting Handset Volume below
- Adjusting Speaker Volume below
- Adjusting Headset Volume on the next page

For more information about sound and volume, see here.

Adjusting Ring Volume

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

➢ **To adjust ring volume:**

1. When the phone is in idle state, select the VOL ▲ or VOL ▼ key on the phone.
2. After adjusting, the volume bar disappears from the screen.

Adjusting Tones Volume

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

➢ **To adjust tones volume:**

1. Off-hook the phone (using handset, speaker or headset).
2. Select the VOL ▲ or VOL ▼ key to adjust the volume.
3. After adjusting, the volume bar disappears from the screen.

Adjusting Handset Volume

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

➢ **To adjust handset volume:**

1. During a call or when making a call, make sure the handset is off the cradle.
2. Select the VOL ▲ or VOL ▼ key; the volume bar is displayed on the screen. After adjusting, the volume bar disappears from the screen.

Adjusting Speaker Volume

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

➢ **To adjust the speaker volume:**

1. During a call, activate the speaker key on the phone.

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

Adjusting Headset Volume

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

➢ **To adjust the headset volume:**

1. During a call, activate the headset key on the phone.
2. the volume bar is displayed on the screen.

6 Performing Administrator-Related Operations

Network administrators can:

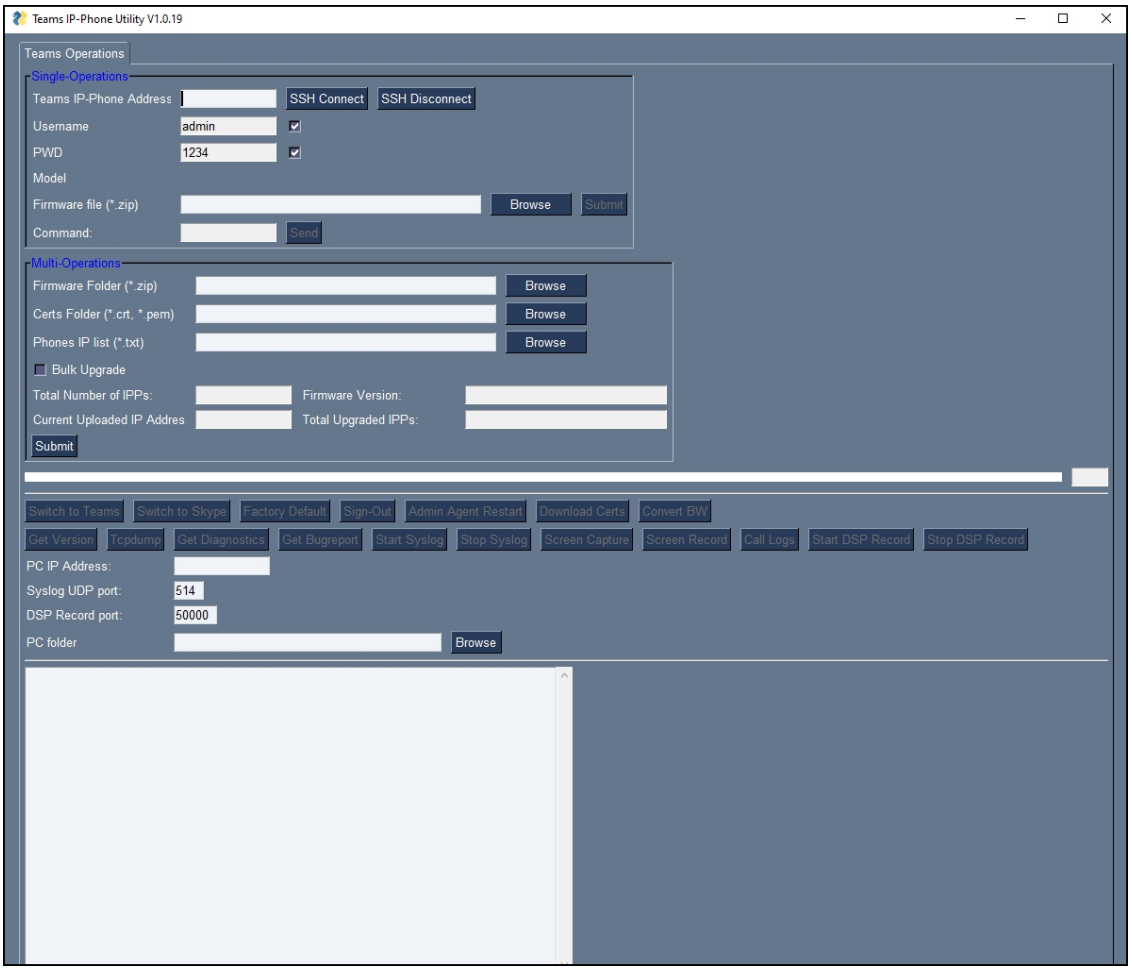
- Updating Phone Firmware Manually below
- Manually Performing Recovery Operations on page 61
- Removing Devices from Intune Management on page 62
- Updating Microsoft Teams Devices Remotely on page 69
- Managing Phones with the Device Manager on page 70

Updating Phone Firmware Manually

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

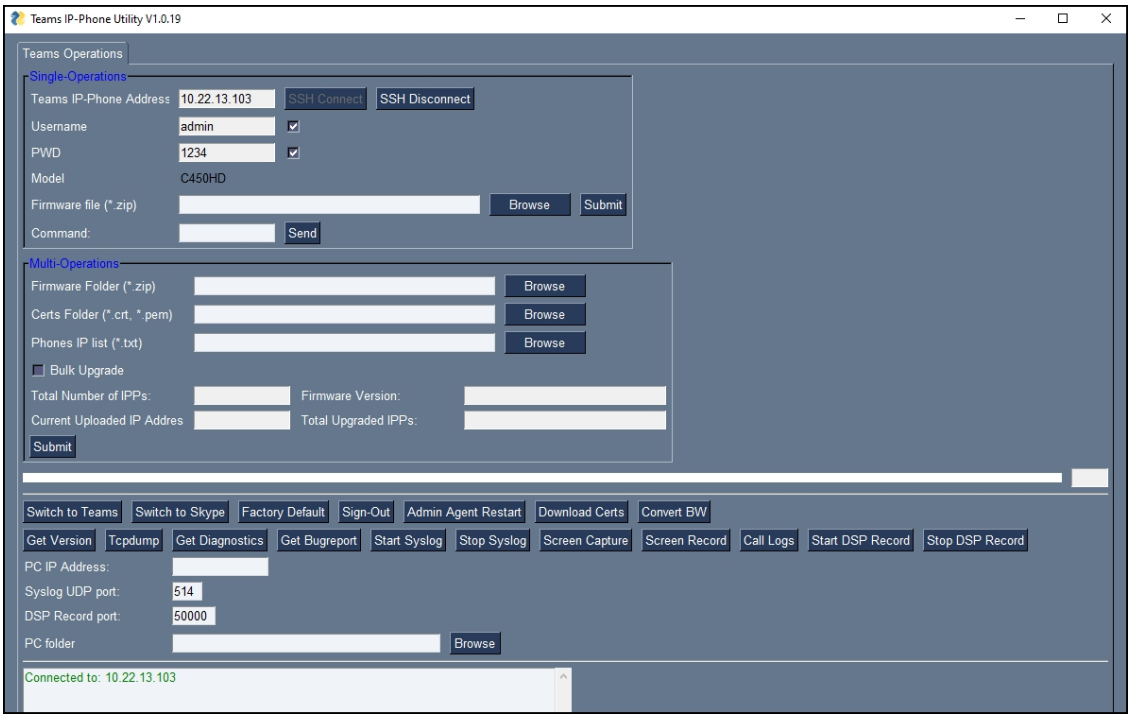
➢ To manually update a phone's firmware:

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.



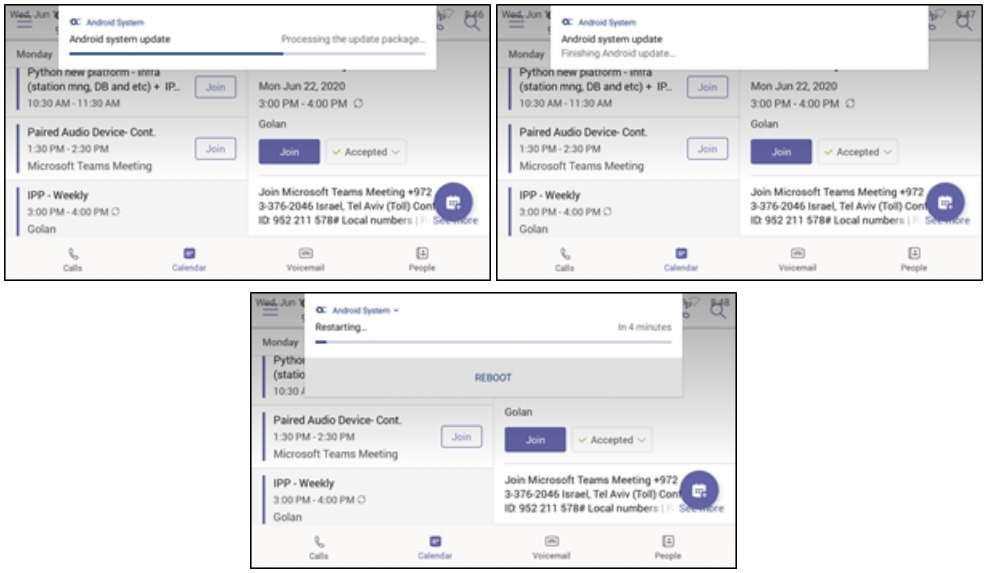
2. In the 'Teams IP-Phone Address' field, enter the IP address of the device (get it by pressing the MENU hard key > **About phone** > **Status** > **IP Address**).

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



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

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



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

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 75

- 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 75 for detailed information about the application), enter the phone's IP address and click **SSH Connect**.

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

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

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

3. Click the**Browse** 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. Note too that the Android phones also feature a 'hardware watchdog'. This feature resets the phone if Android is stacked and doesn't respond (though Android stacking is unlikely); there's no recovery process; the phone is only reset.

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

The C450HD / C448HD devices feature a two-key combination to activate each action. To activate an action, *simultaneously press the two keys for three seconds*.

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

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

Following are the recovery operation options using the two-key combination on the phone:

- Enter recovery mode - Long-press the reset key for 4 seconds or simultaneously press the 'back' key + the MENU key; the device's LED lights up red.

- Switch to the other slot - Long-press the reset key for 10 seconds or simultaneously press the '4' key + the '6' key; the device's LED lights up green.
- Enter the device's boot - Long-press the reset key for 15 seconds or simultaneously press the '1' key + the '3' key; the device's LED lights up blue.
- Switch from Teams Compatible to Teams Native and vice versa - simultaneously press the 'back' key + the OK key; the phone's LED lights up red + green.
- Restore the phone to its default settings - Long-press the reset key for 25 seconds or simultaneously press the OK key + the MENU key; the device's LED lights up green + blue.

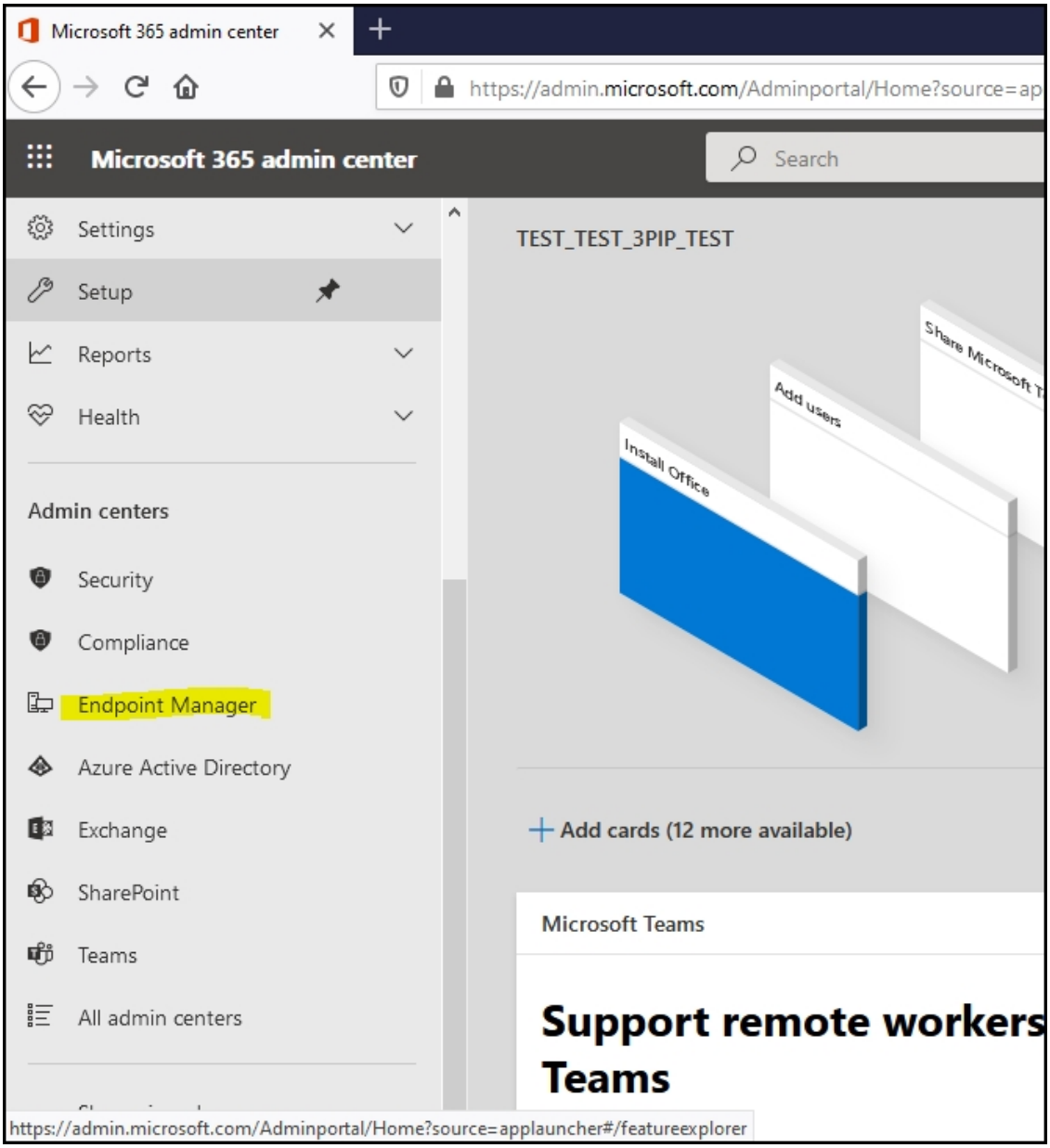
You can also restore a device to its default settings while the phone is already powered up and functioning, by long-pressing the HOLD key for 15 seconds.

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.

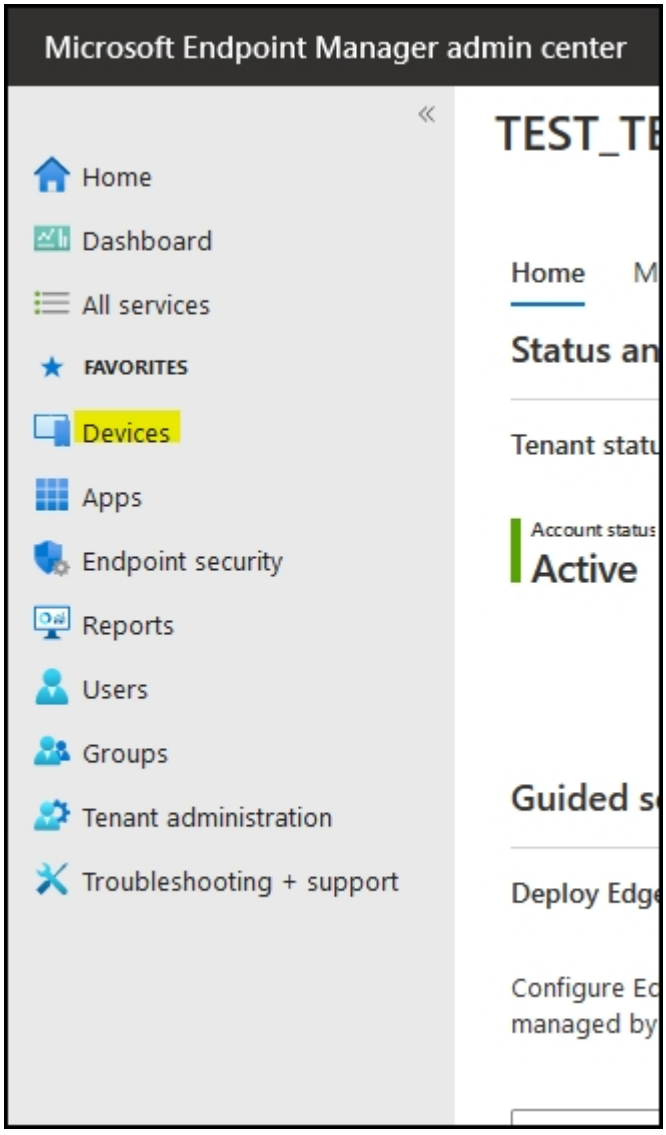
➢ **To remove devices from Intune:**

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

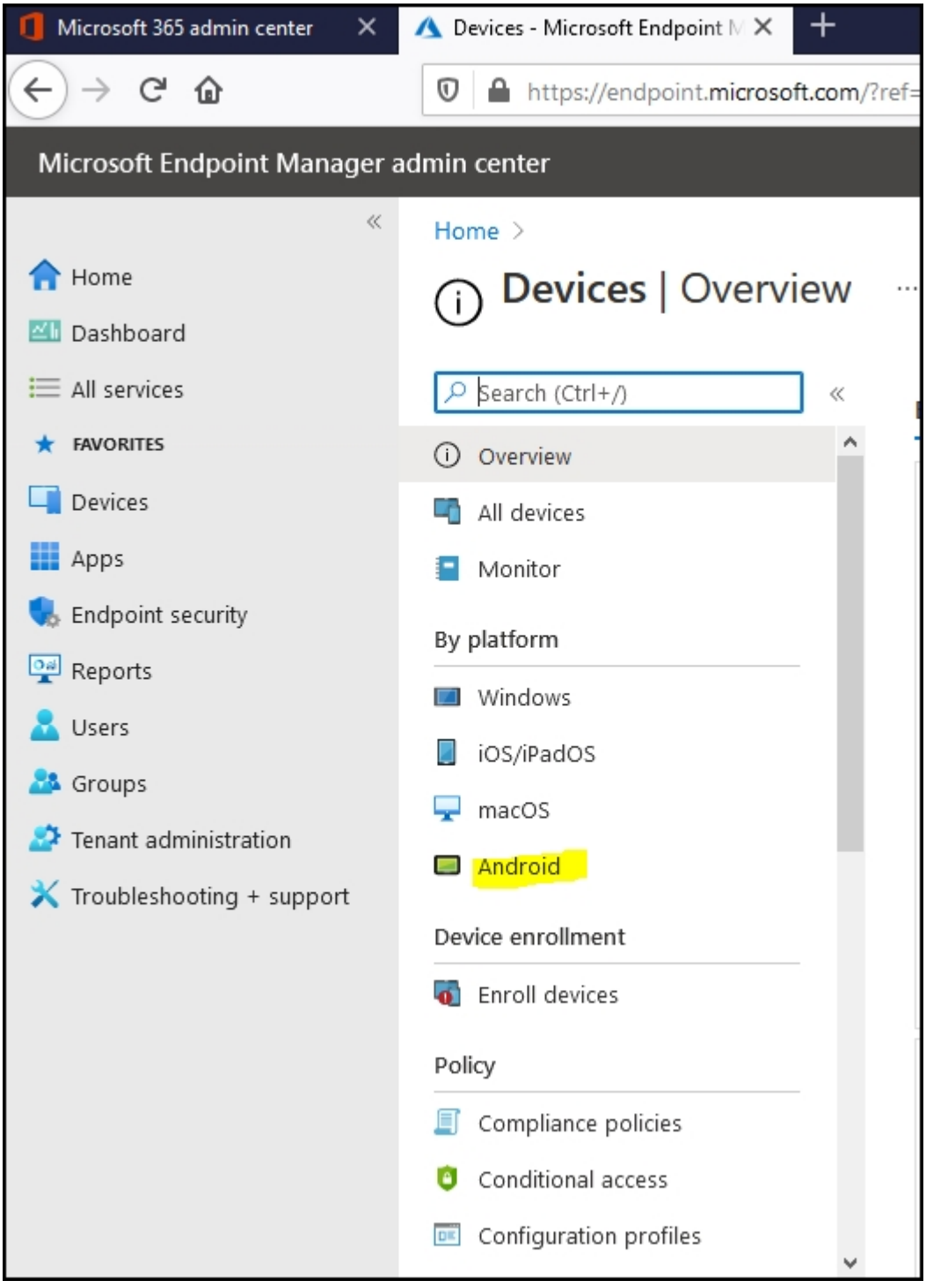


The Endpoint Manager service is licensed according to individual terms. Consequently, not all network administrators will be able to navigate to it. Check if the license you're using includes the service or not.

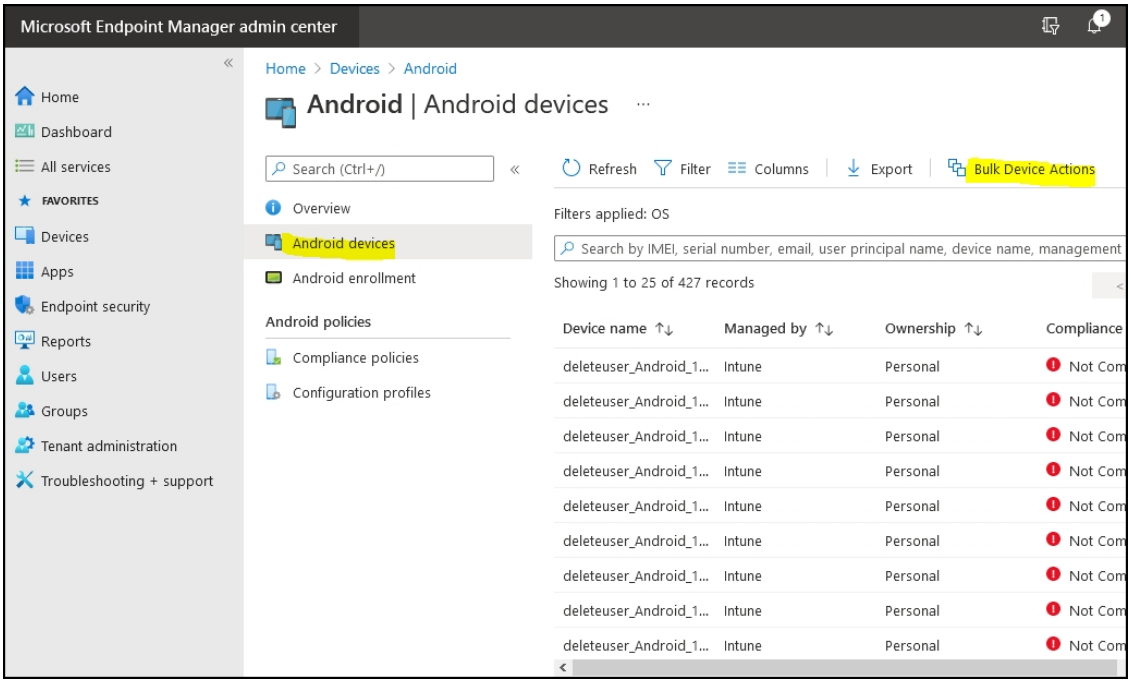
3. Click **Devices**.



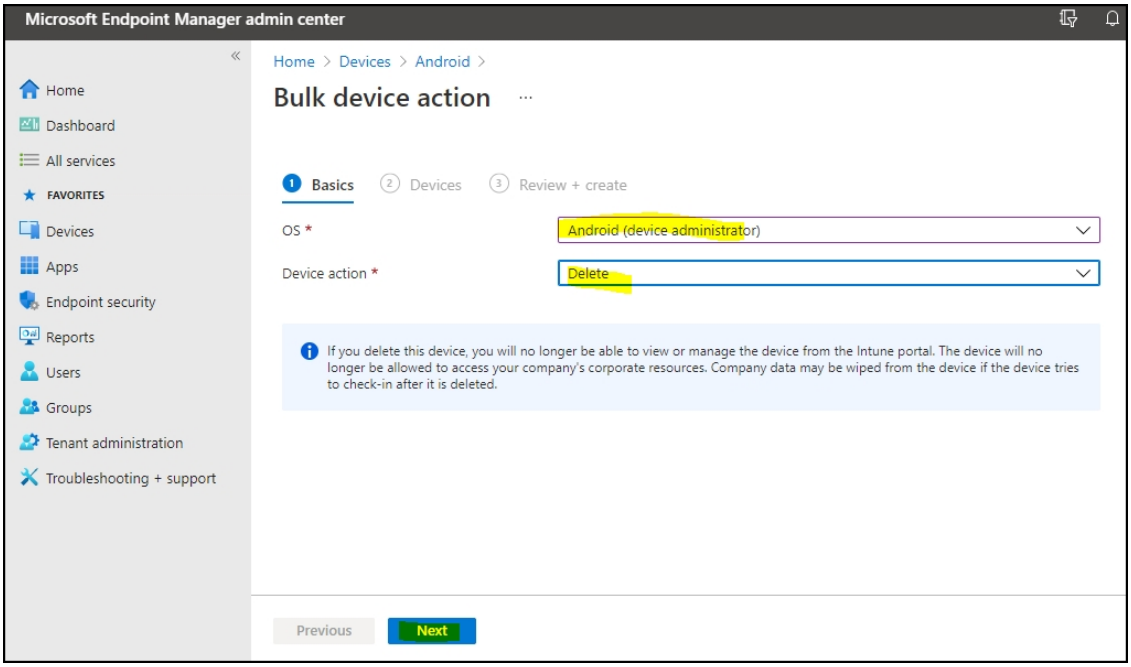
4. Click **Android**.



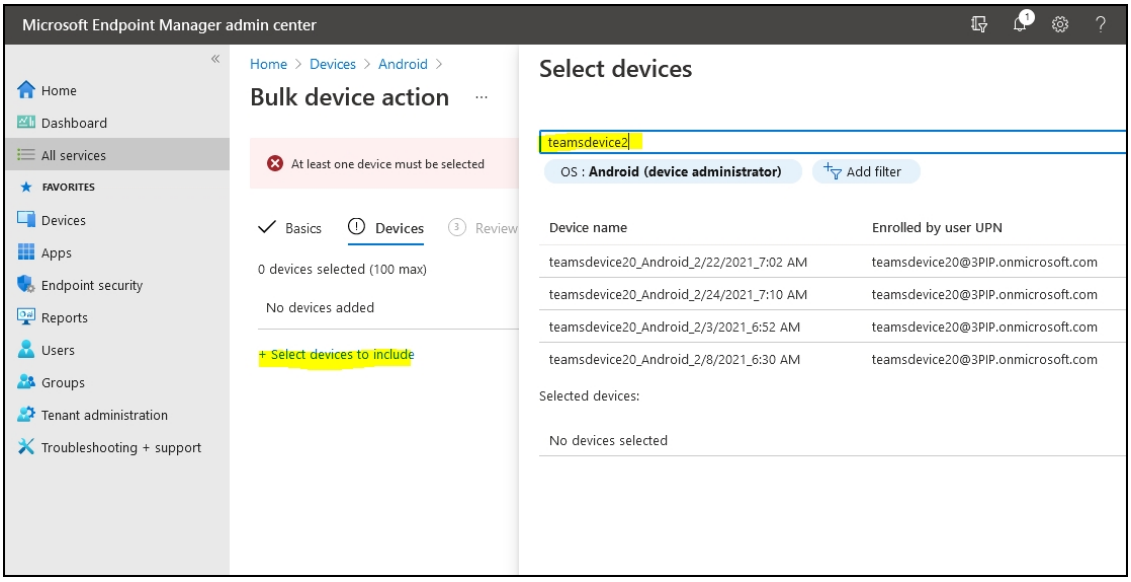
5. Click **Android Devices** > **Bulk Device Actions**.



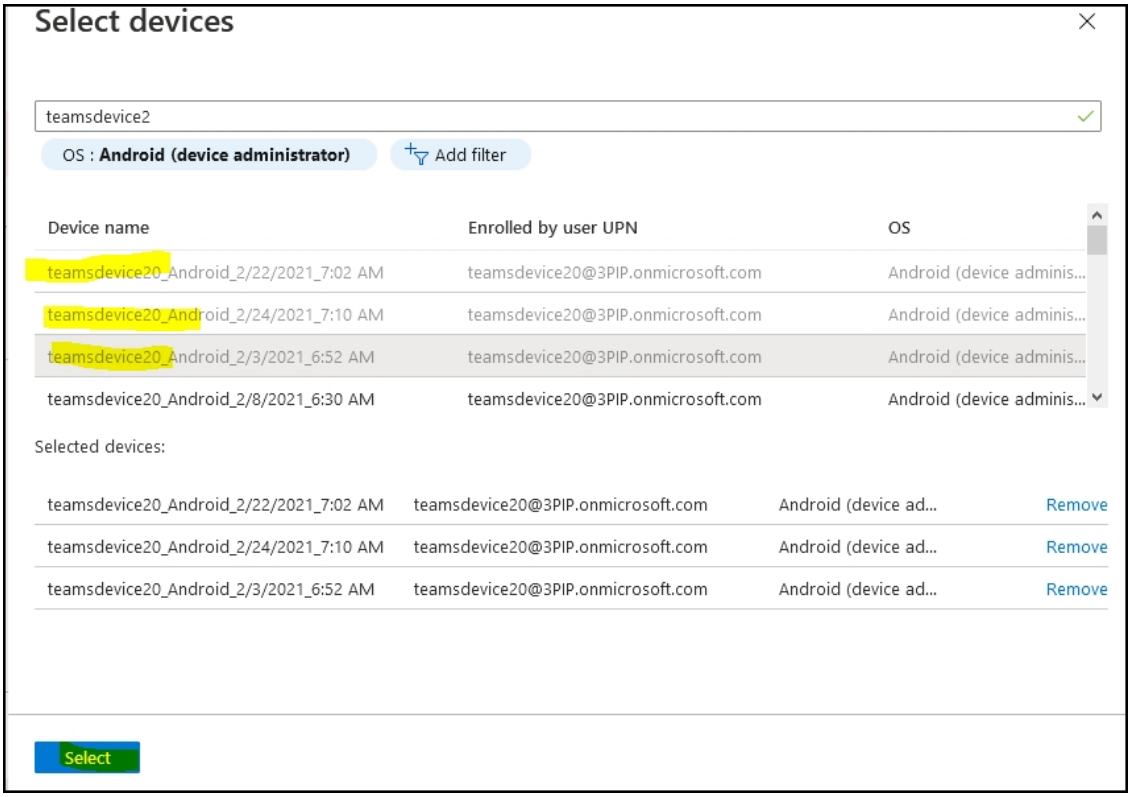
6. Select: **OS** > **Android** (Device Administrator) **Device Action** > **Delete** and then **Next**.



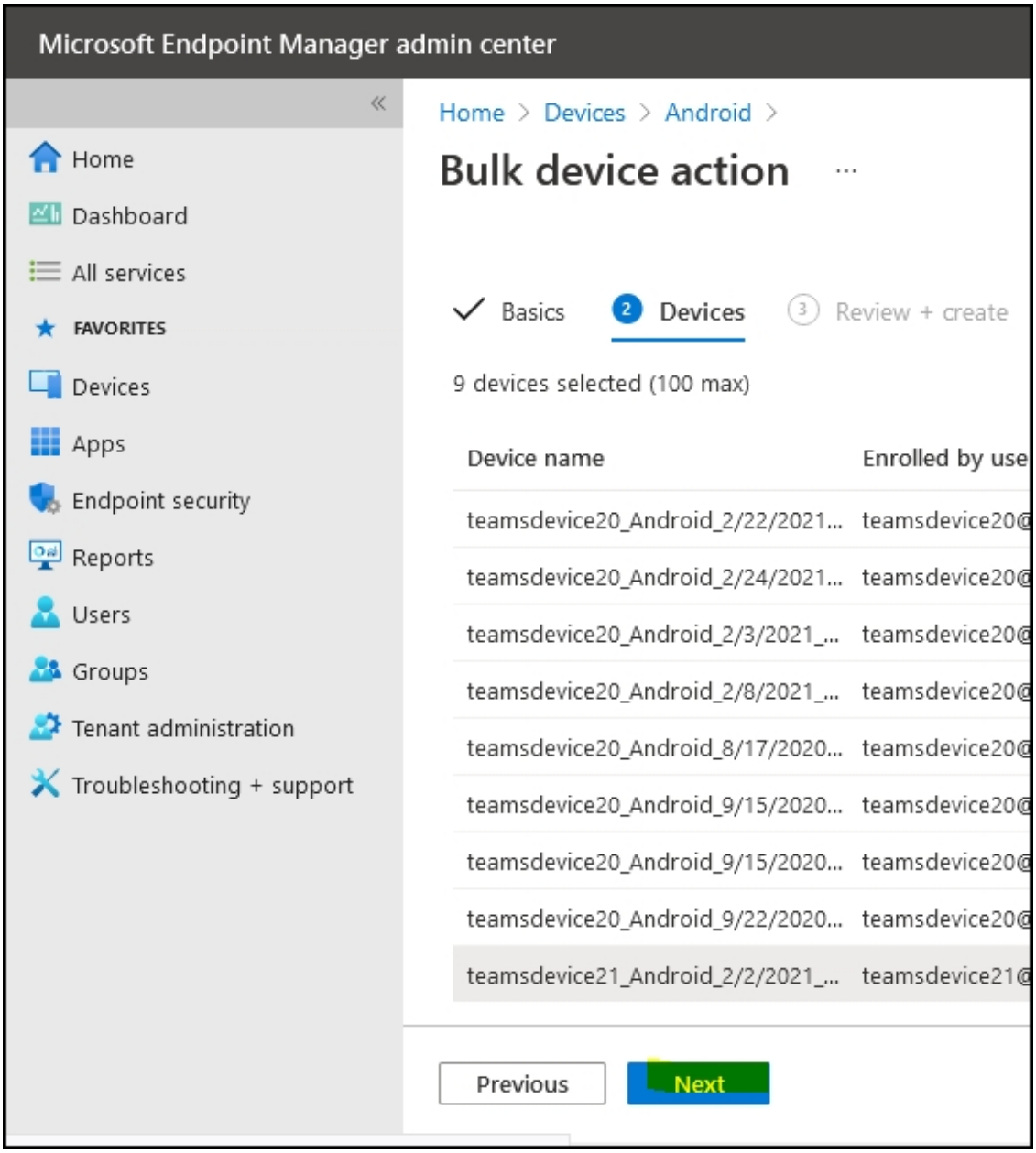
7. Select **Devices to include** and search for the user for which enrolled devices are to be removed.



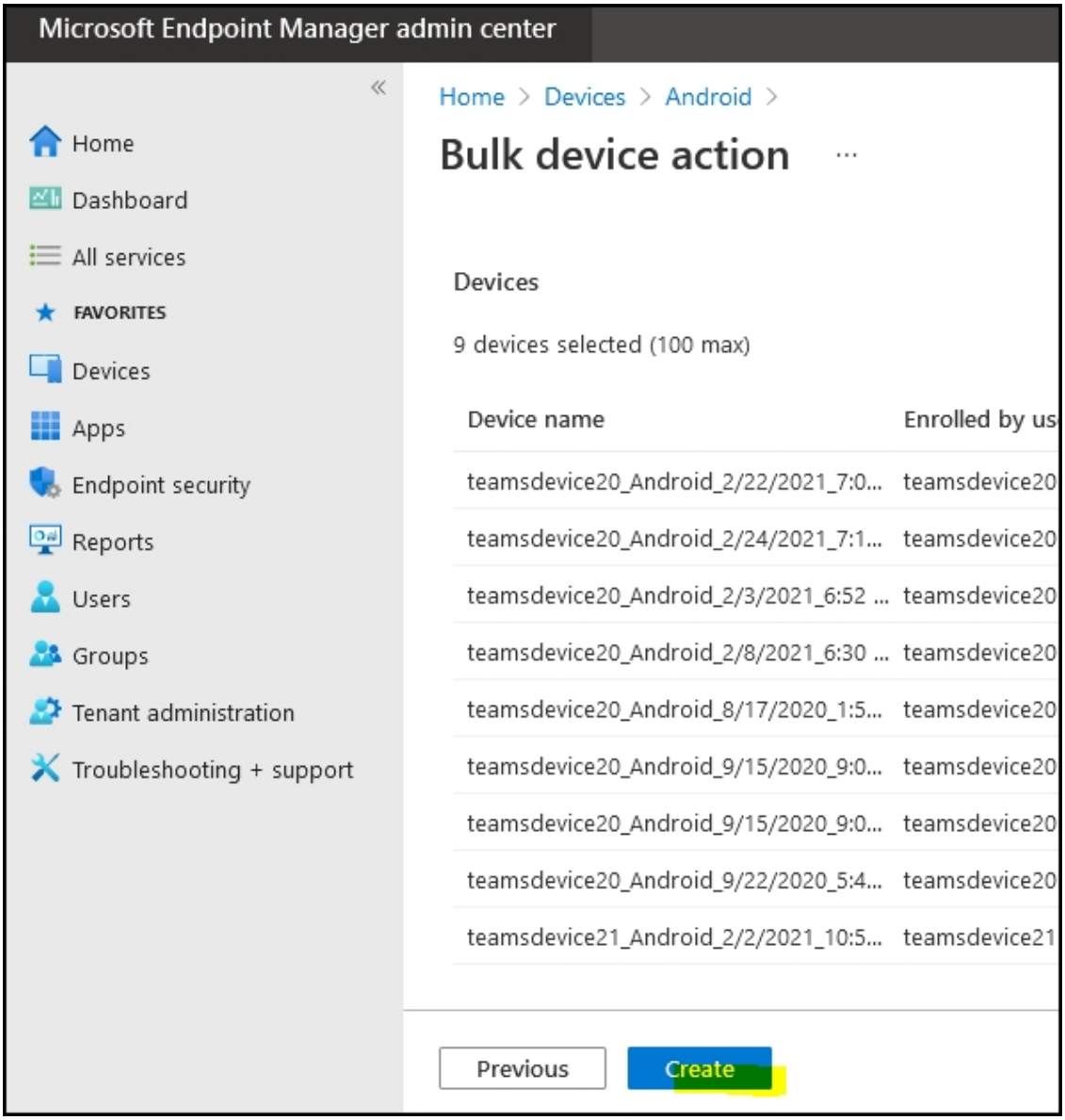
8. Select all the devices to be removed and click **Select icon**.



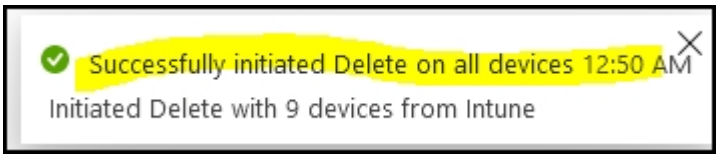
9. After the devices are selected, click **Next**.



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



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



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

Updating Microsoft Teams Devices Remotely

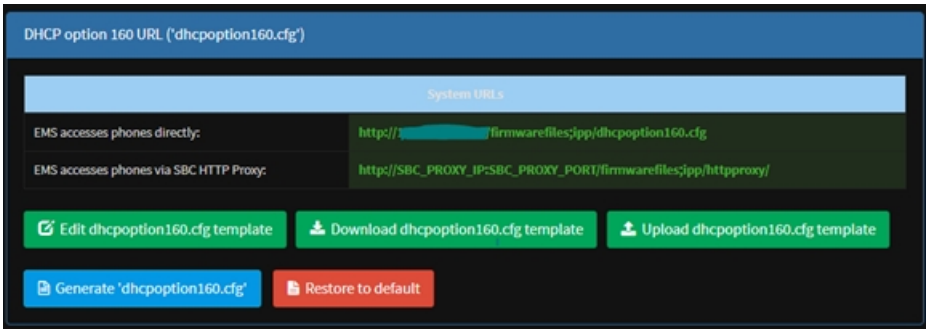
For instructions on how to update Microsoft Teams devices remotely, see here.

Managing Phones with the Device Manager

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

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

Table 6-1: DHCP Option 160 URL



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

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

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

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

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

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

Configuring a Periodic Provisioning Cycle

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

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

- Use the following table as reference.

Table 6-2: Periodic Provisioning Cycle

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

Configuring TimeZone and Daylight Savings

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

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

- Use the following table as reference.

Table 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: ■ 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

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 56)
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 57).

Network Administrators

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

Teams IP Phone Utility

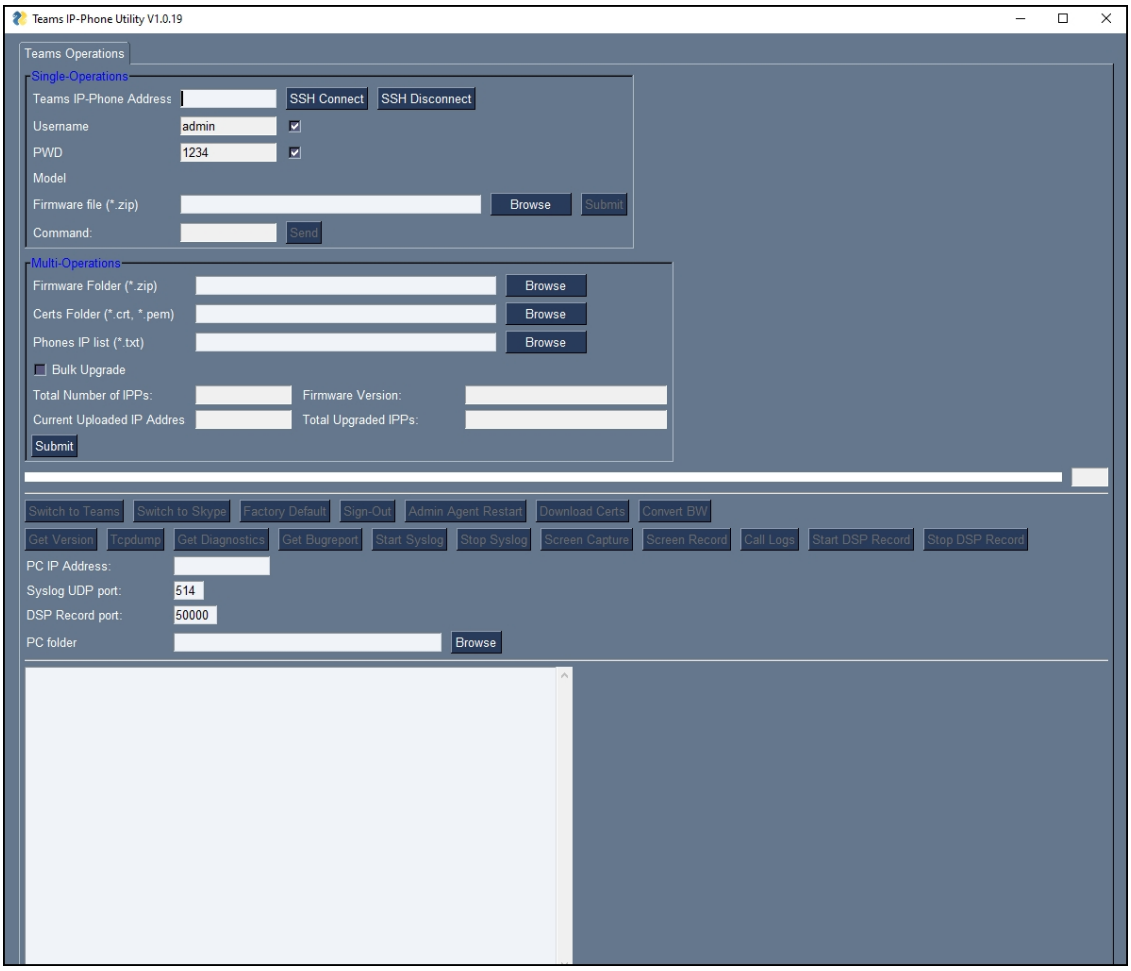
AudioCodes' Teams IP phone is by default accessed via Secure Shell (SSH) cryptographic network protocol after the network administrator signs in. Network administrators need to know their username and password in order to sign in; **admin** and **1234** are the default username and password.

AudioCodes provides network administrators with the SSH-based Teams IP Phone Utility. The application gives network administrators the following debugging capabilities:

- Capturing the Phone Screen on the next page
- Running Tcpdump on page 79
- Getting Information about Phones on page 80
- Remote Logging (Syslog) on page 82
- Getting Diagnostics on page 83
- Getting a Bug Report on page 86
- Activating DSP Recording on page 87
- Deactivating DSP Recording on page 88
- Getting Information about Phones on page 80

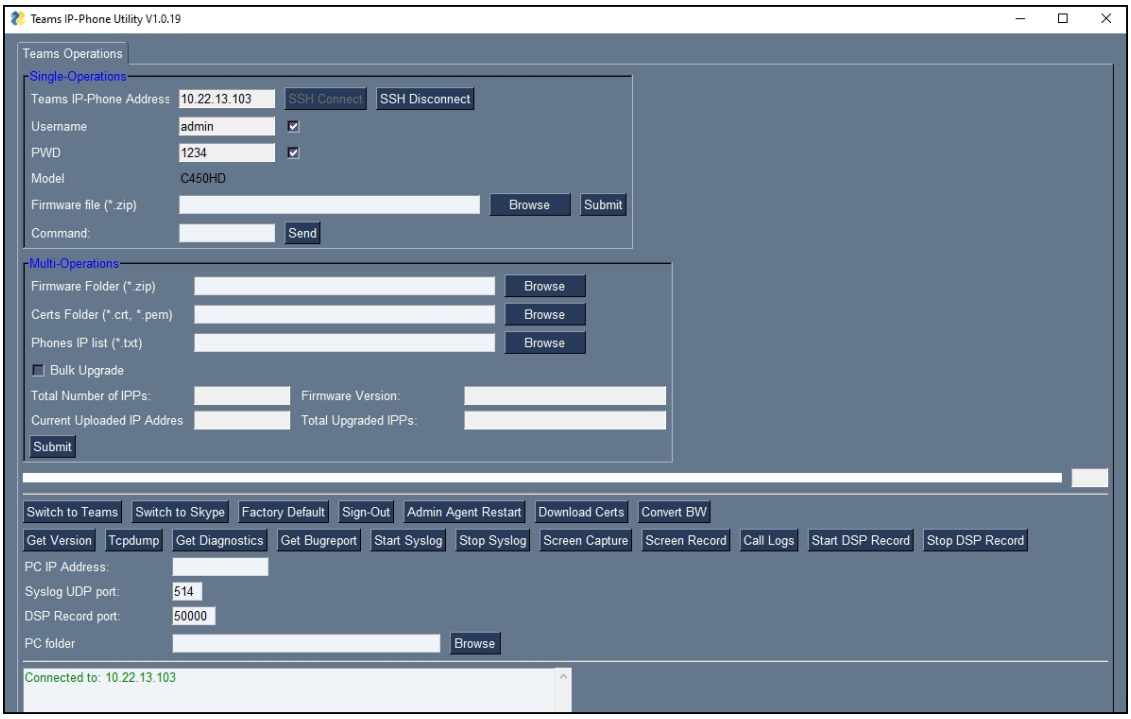
➢ To open the Teams IP Phone Utility:

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.



2. In the 'Teams IP-Phone Address' field, enter the IP address of the device (get it by pressing the MENU hard key > **About phone** > **Status** > **IP Address**).

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



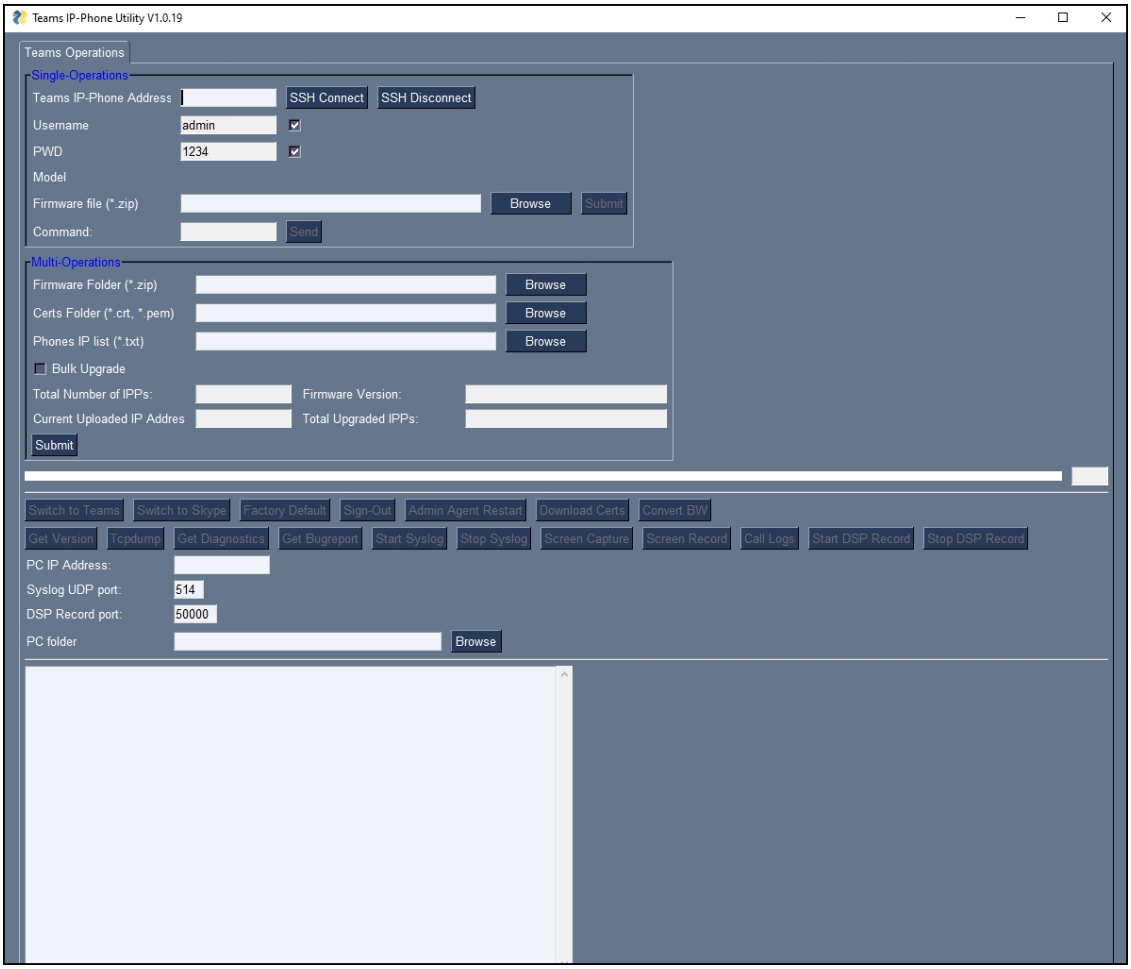
4. Next to the field 'PC folder', click the **Browse** button and navigate to and select the folder to which to send data to use for debugging.

Capturing the Phone Screen

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

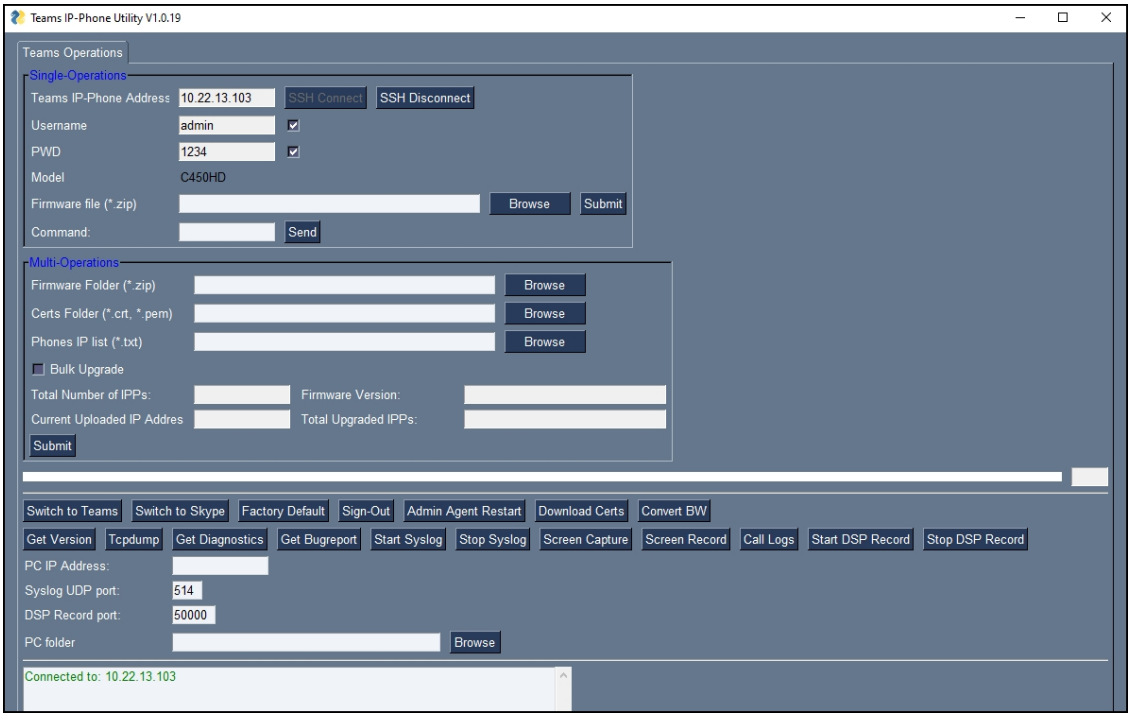
➢ To capture the phone screen:

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



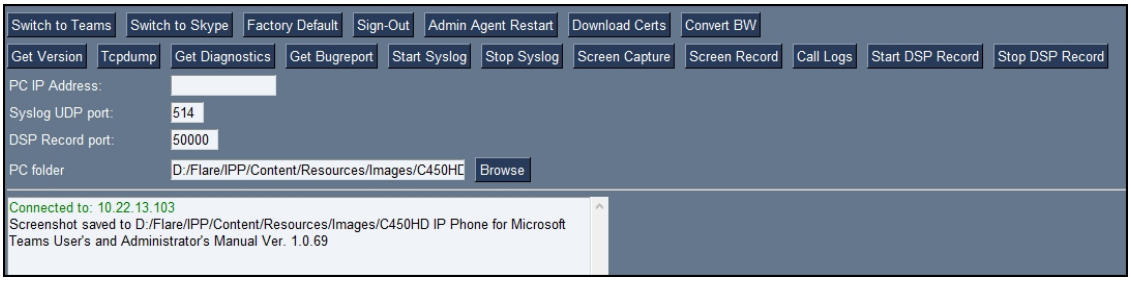
2. In the 'Teams IP-Phone Address' field, enter the IP address of the device (get it by pressing the MENU hard key > **About phone** > **Status** > **IP Address**).

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



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

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



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.

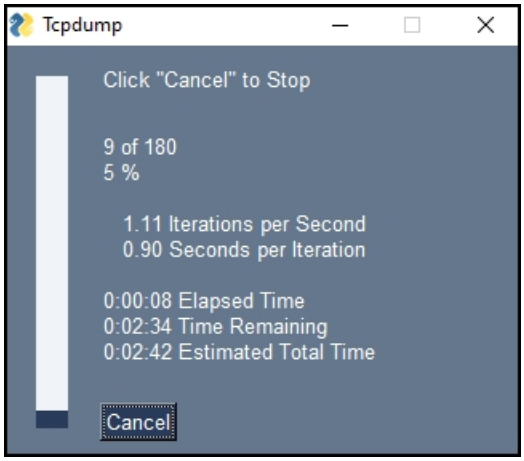
Running Tcpdump

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.

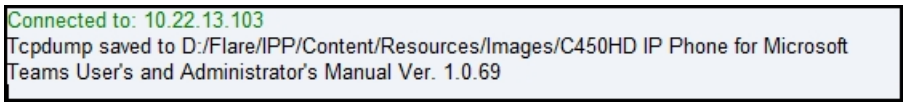
➢ To run Tcpdump:

1. In the Teams IP Phone Utility (see Teams IP Phone Utility on page 75 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.



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



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

Alternatively, run Tcpdump *without* the 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:

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

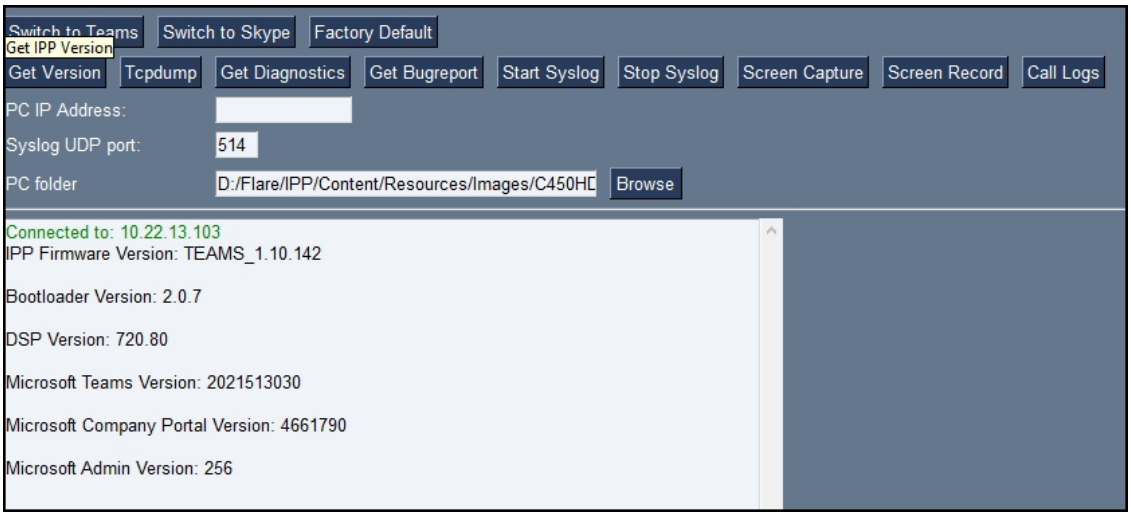
Getting Information about Phones

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 75 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).



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)

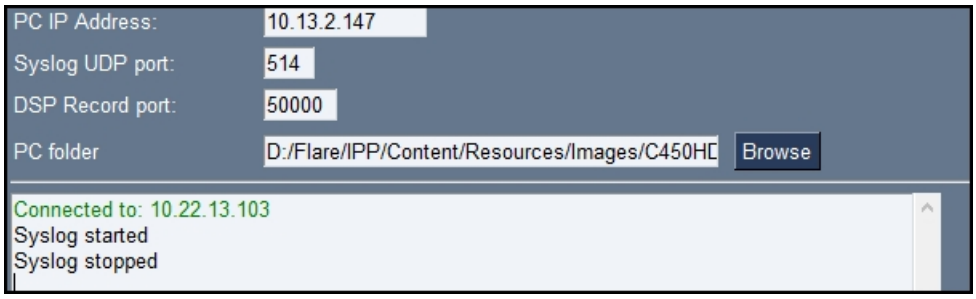
Remote Logging via Syslog provides the same log level as Device Diagnostics (performed via the Microsoft Admin Center) with some additional information that may be relevant to device issues (not Teams application issues). Device Diagnostics via the Microsoft Admin Center are saved to the device sdcard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

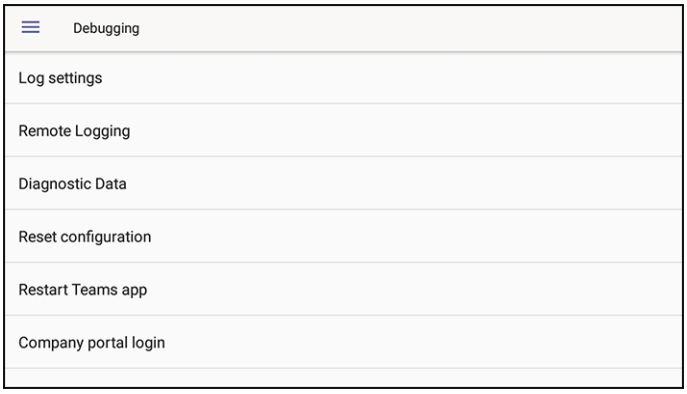
1. In the Teams IP Phone Utility (see Teams IP Phone Utility on page 75 for more information), enter the phone's IP address, click **SSH Connect** and browse to a folder on the PC to which to send the information.
2. In the 'PC IP Address' field, enter the IP address of the PC on which the utility is installed and then click the **Start Syslog** button.



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

➢ To enable Remote Logging via Syslog from the phone:

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



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

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

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

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

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

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

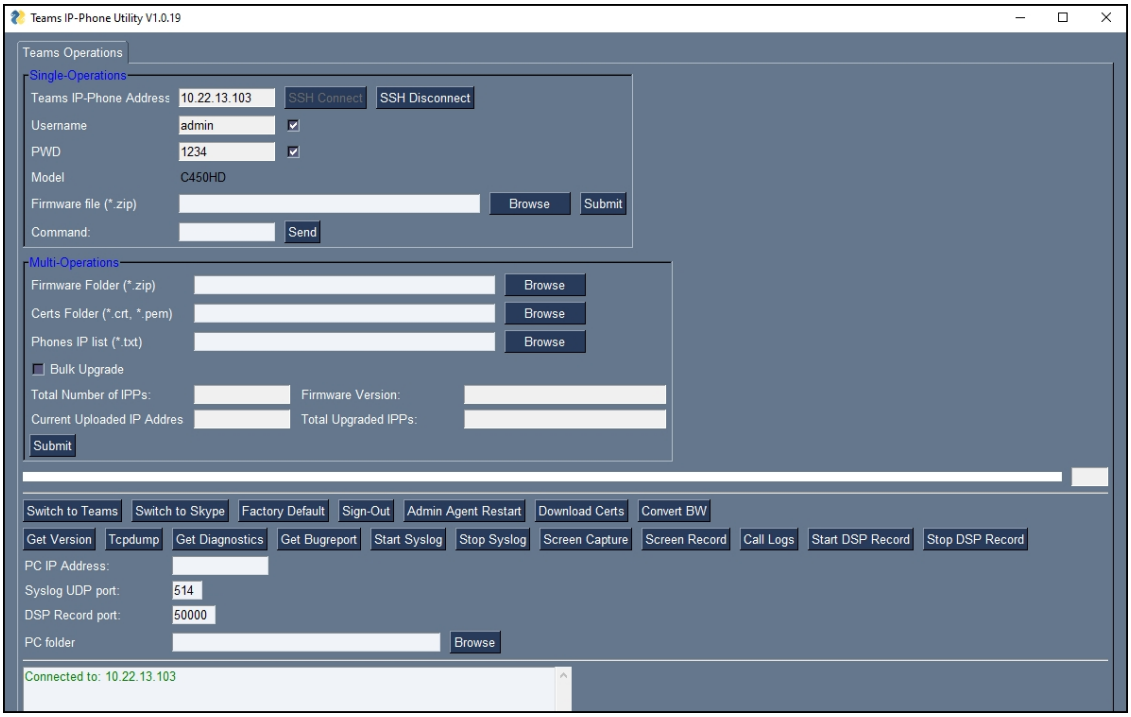
Getting Diagnostics

Getting Diagnostics is identical to Getting a Bug Report on page 86 with these exceptions:

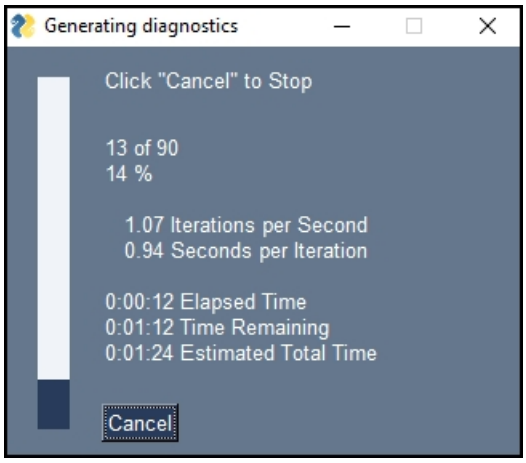
- Diagnostics can be gotten on one phone; a Bug Report can be on many phones
- Diagnostics is in zip file format; a Bug Report is not
- Diagnostics are formatted differently to a Bug Report

➢ **To get diagnostics:**

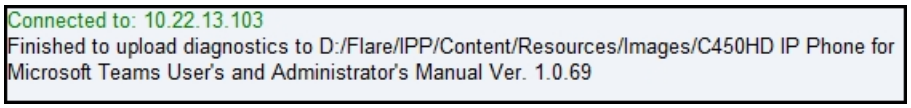
1. In the Teams IP Phone Utility (see Teams IP Phone Utility on page 75 for more information), enter the phone's IP address, click **SSH Connect** and browse to a folder on the PC to which to send the information.



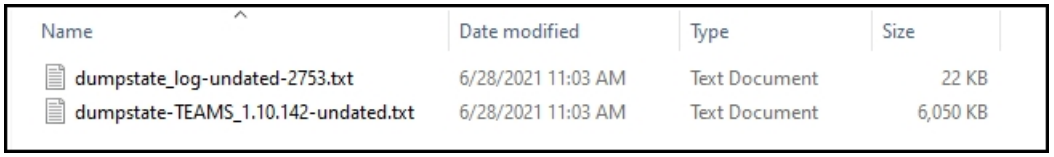
2. Click **Get Diagnostics**.



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



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

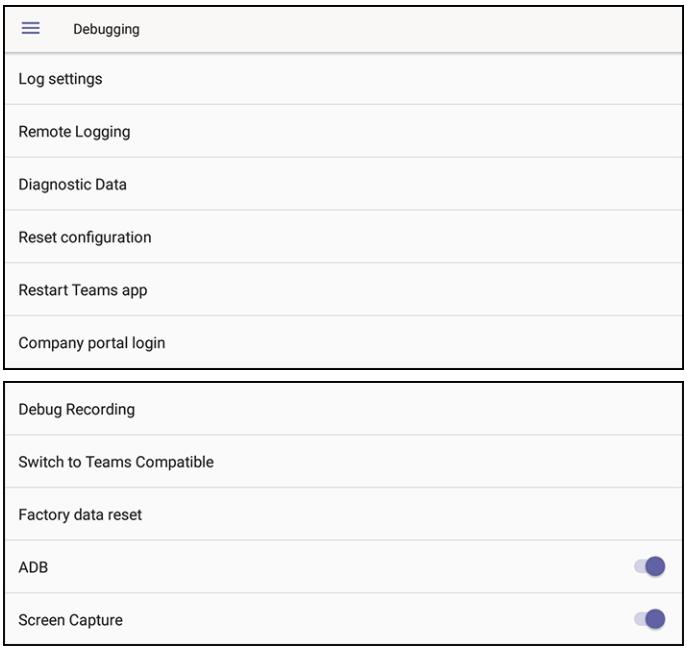


5. Open the txt files to view the diagnostics.

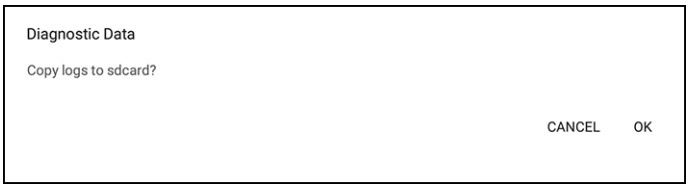
Network administrators who need to get diagnostics from the device can alternatively dump the logs to the phone's Secure Digital (SD) Card and then later collect them using Secure Copy Protocol (SCP) based on Secure Shell (SSH) protocol. Whenever an issue occurs, the administrator can dump the logs into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



4. Select **OK** to confirm.

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

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

- 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

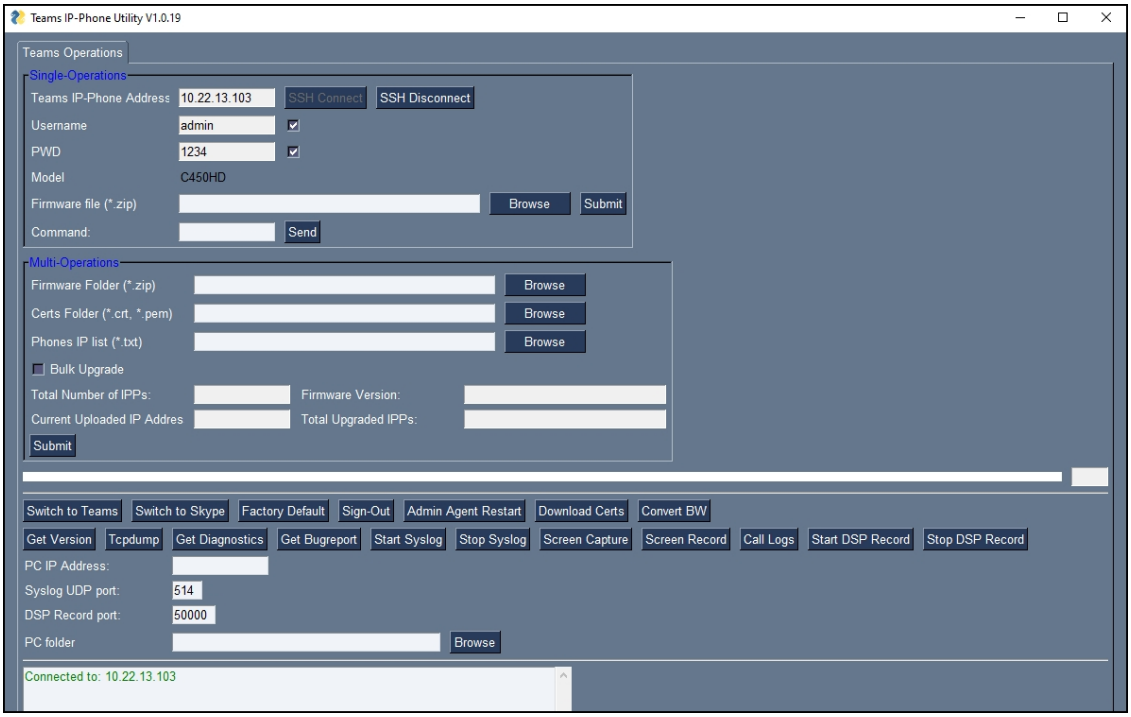
Getting a Bug Report

Getting a Bug Report is identical to Getting Diagnostics on page 83 with these exceptions:

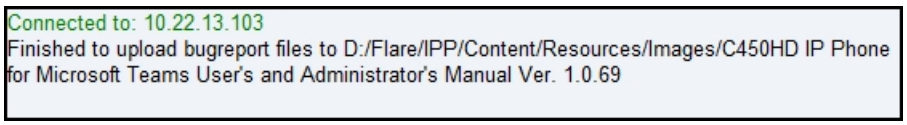
- A Bug Report can be on many phones; Diagnostics is on one
- A Bug Report is in zip file format; Diagnostics are not
- A Bug Report is formatted differently to Diagnostics

➢ To get a Bug Report:

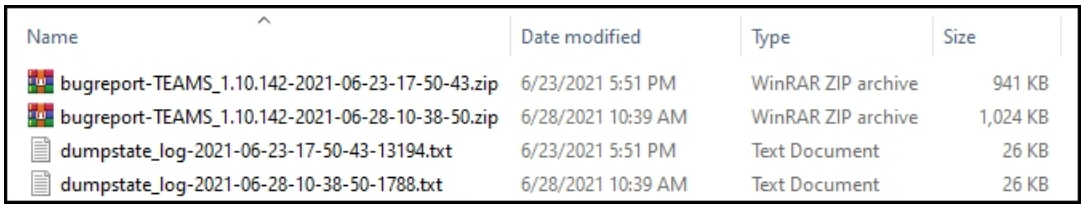
1. In the AudioCodes Teams IP Phone Utility (see Teams IP Phone Utility on page 75 for more information), enter the phone's IP address, click **SSH Connect** and browse to a folder on the PC to which to send the information.



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



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



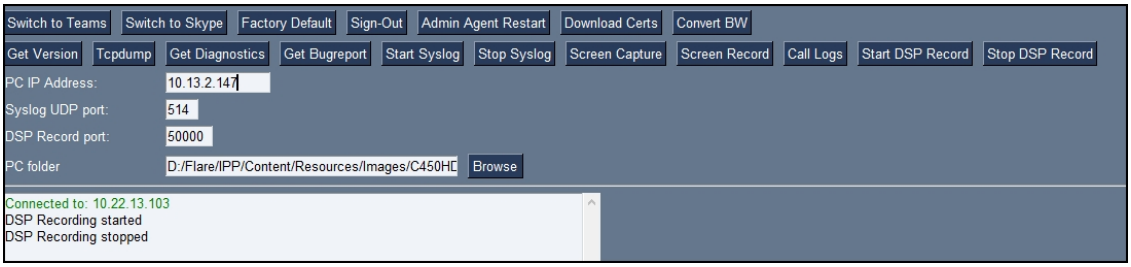
4. Unzip the zipped files and open the txt files to view the report.

Activating DSP Recording

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

➢ To activate DSP Recording:

1. In the AudioCodes Teams IP Phone Utility (see Teams IP Phone Utility on page 75 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**.



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

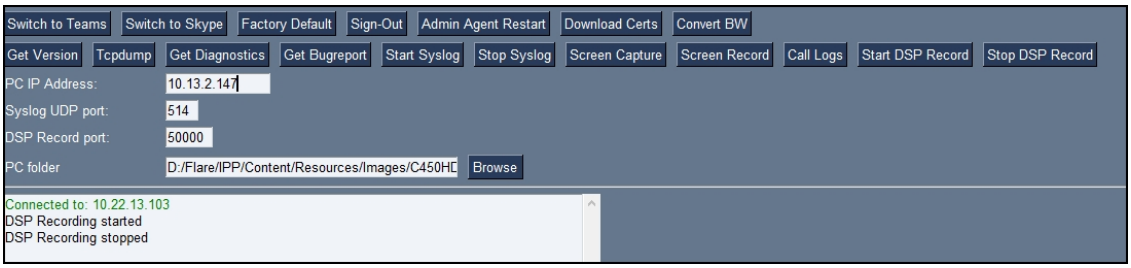
DSP recording can be activated on the fly without requiring the network administrator to reset the phone.

Deactivating DSP Recording

Network administrators can deactivate DSP recording using 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 75 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.



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 is by default accessed via Secure Shell (SSH) cryptographic network protocol after the network administrator signs in. Administrators need to know their username and password in order to sign in; **admin** and **1234** are the defaults.

SSH access allows network 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 87
- 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:**

```
su
```

```
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. Here's an example of how to replace the Microsoft Teams application version.

➢ **To replace the Microsoft Teams application version:**

1. Upload the .apk file to the phone

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

2. Install the .apk

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

3. Remove the .apk from /data

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

Microsoft Admin Center

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

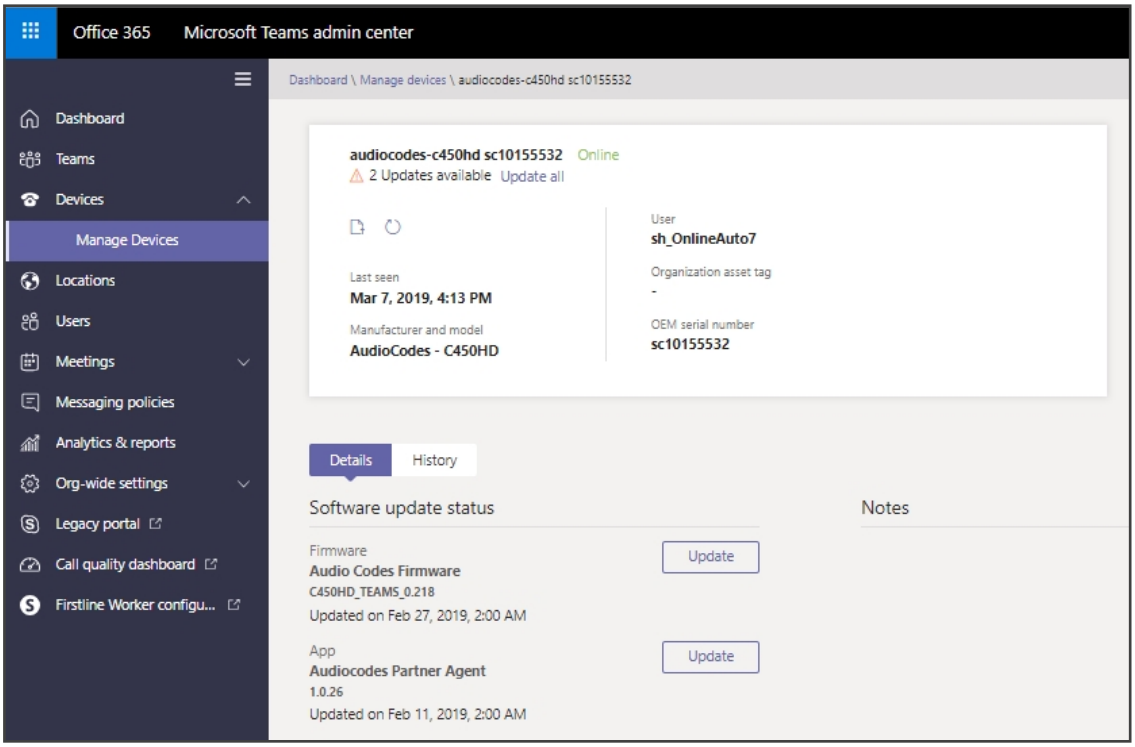
Collecting Logs

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

➢ To collect logs:

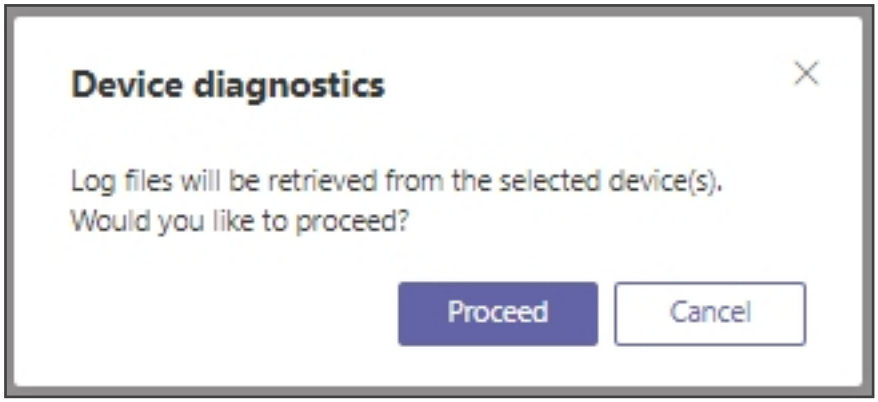
1. Reproduce the issue
2. Access Microsoft Admin Center and under the **Devices** tab click the **Diagnostics** icon.

Figure 7-1: Microsoft Teams Admin Center - Diagnostics



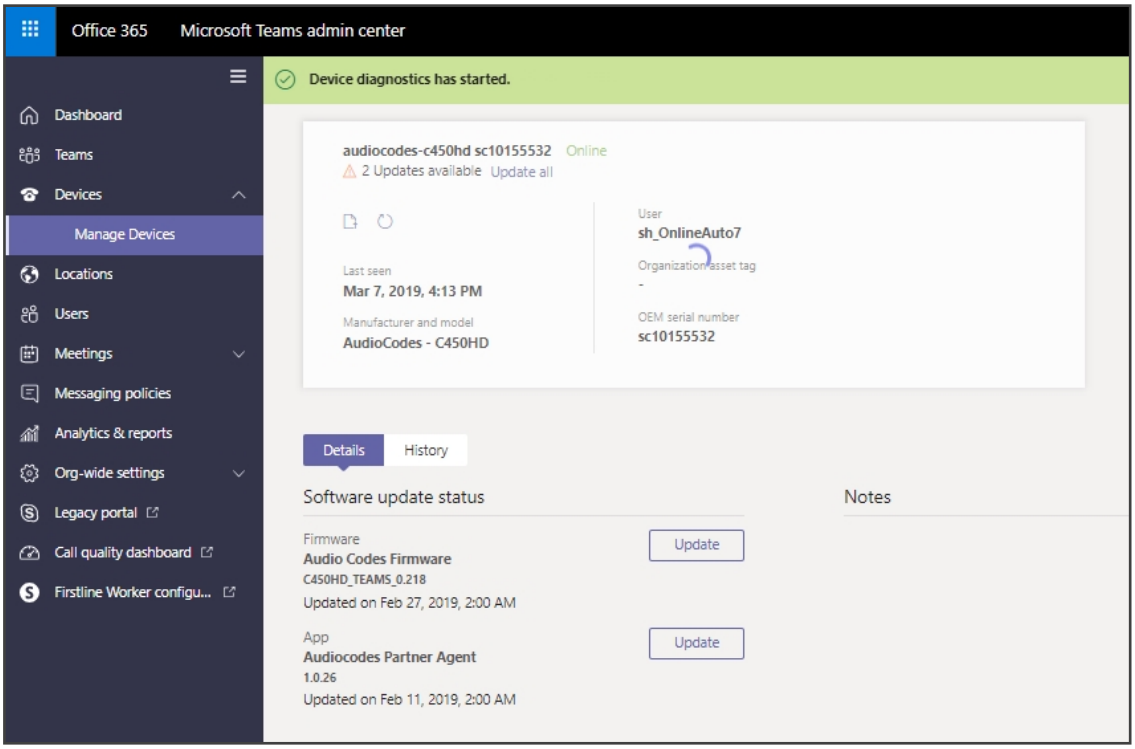
Applies to all AudioCodes phones for Microsoft Teams even though a specific model is shown in the figures here.

3. Click the **Diagnostics** icon .



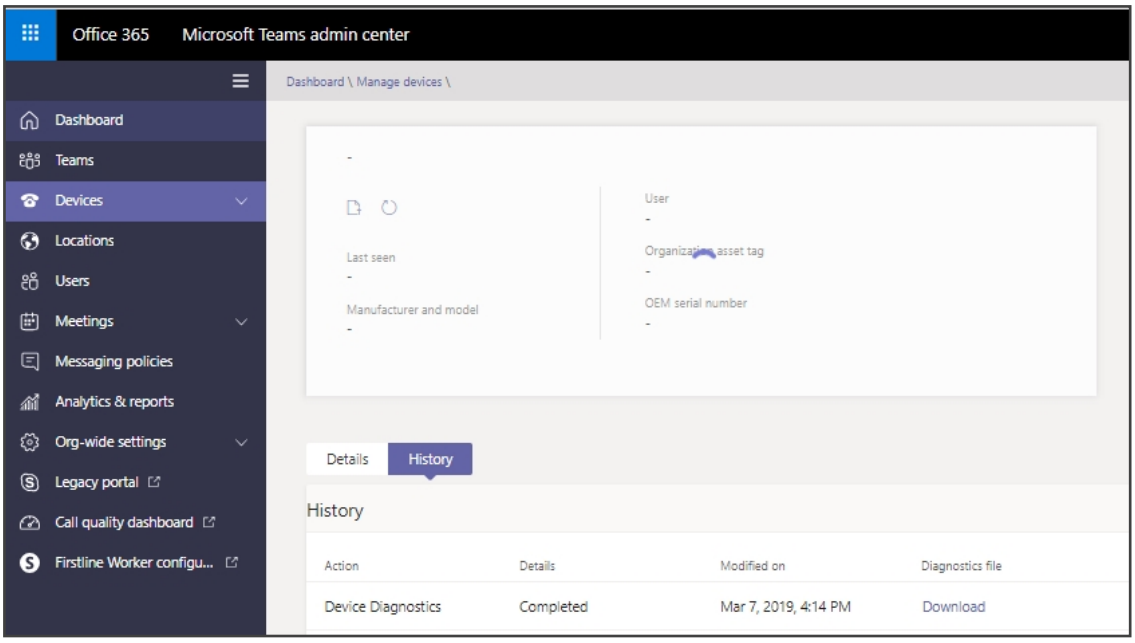
4. Click **Proceed**; the logs are uploaded to the server.

Figure 7-2: Microsoft Teams Admin Center – Logs Upload to Server



5. Click the **History** tab.

Figure 7-3: History - Download



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

Getting Company Portal Logs

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

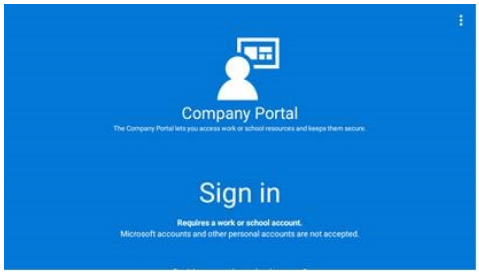
Logs can be gotten using one of two methods:

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

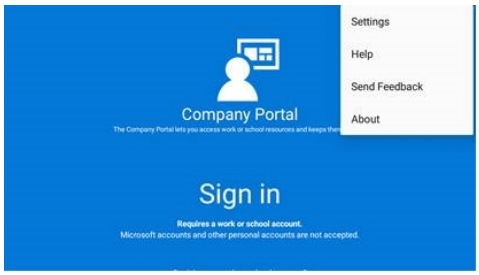
Getting Logs via the Phone

➢ **To get Company Portal logs via the phone:**

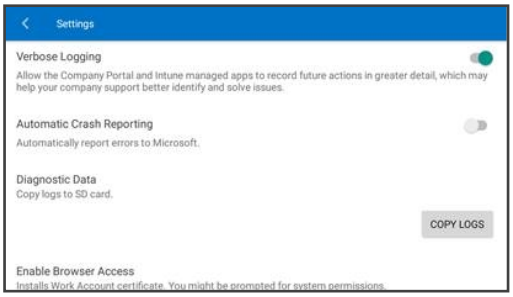
1. Reproduce the issue (logs are saved to the device so you first need to reproduce the issue and then get the logs).
2. Log in to the phone as Administrator and then go back.
3. Select the **Debugging** option under Admin.
4. Select **Company Portal login**.
5. Select the icon located in the uppermost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



6. Select **Settings**.



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



Company portal logs are copied to:

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

8. To pull the logs, use the ssh:

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

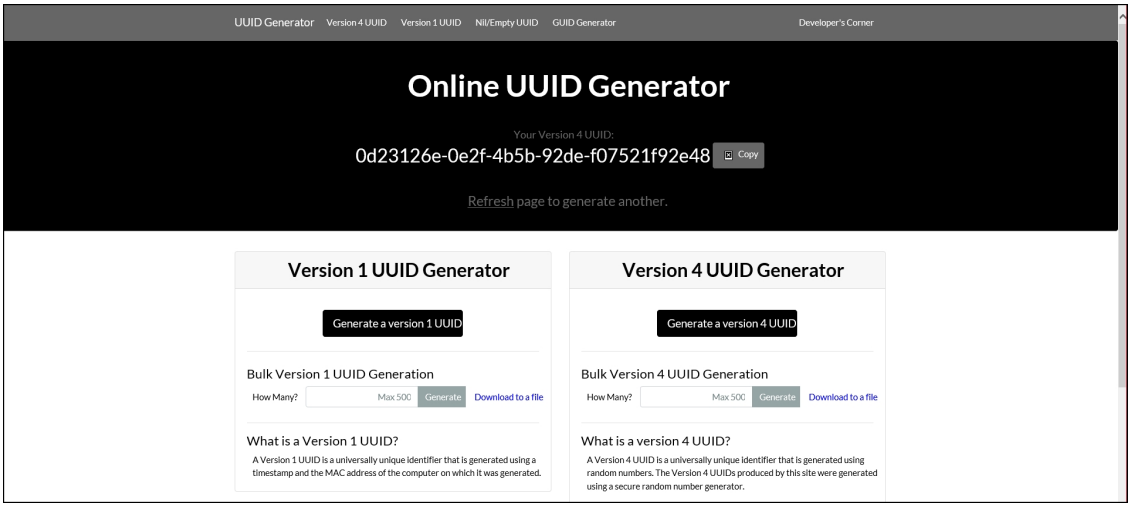
Files are quite heavy so you may need to pull them one by one.

Getting Logs using UUID

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

➢ **To get logs using a UUID generator:**

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



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

Getting Logs using UUID over ADB Shell

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

➢ To execute the command adb shell:

1. After copying the UUID number as shown in Getting Logs using UUID 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.

➢ **To execute the command ssh:**

1. After copying the UUID number as shown in Getting Logs using UUID on page 93, execute the command **ssh** as shown in the following example:

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

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

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

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

Getting Audio Debug Recording Logs

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

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

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

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

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

Collecting Media Logs (*.blog) from the Phone

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

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

1. Access the phone via SSH.
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.

200 Cottontail Lane

Suite A101E

Somerset NJ 08873

Tel: +1-732-469-0880

Fax: +1-732-469-2298

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

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

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

Document #: LTRT-13291