User's and Administrator's Manual

AudioCodes 400HD IP Phone Series

C435HD IP Phones

Microsoft Teams Application

Version 2.3

Notice

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

This document is subject to change without notice.

Date Published: June-20-2024

WEEE EU Directive

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

Security Vulnerabilities

All security vulnerabilities should be reported to vulnerability@audiocodes.com.

Customer Support

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

Documentation Feedback

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

Stay in the Loop with AudioCodes

Related Documentation

Document Name
Android Device Utility User's Manual
IP Phones How To. A selection of video clips explaining how to perform a variety of frequently needed actions on AudioCodes IP phones quickly and easily.
C435HD IP Phone for Microsoft Teams Quick Guide
C435HD IP Phone for Microsoft Teams Release Notes
Device Manager Administrator's Manual
Device Manager Deployment Guide
https://docs.microsoft.com/en-us/MicrosoftTeams/phones-for-teams

Table of Contents

1 Overview

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 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
- Power-saving mode for MWI LED and LCD is automatically activated during non-working hours. The phone's uppermost-right LED is switched off and the LCD is dimmed. This conserves energy and minimizes light disturbance, providing a seamless and efficient user experience.

AudioCodes Teams phones can operate in a Survivable Branch Appliance (SBA) environment. Branch office survivability is aimed at providing limited calling functionality when a phone no longer has connectivity with the Teams cloud. Basic functionalities are:

- Making PSTN calls
- Receiving PSTN calls
- Hold & Resume of PSTN calls

If a user attempts to make a Teams call and the internet connection is down, they'll be notified that they can try calling a phone number instead. A 'No internet connection' indication is displayed suggesting that calling a phone number is available.

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

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

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

Specifications

The following table summarizes the phone's software specifications.

Table 1-1: Software Specifications

Feature	Details
Media Processing	■ Voice Coders: G.711, G.729, G.722, SILK, Opus ■ Acoustic Echo Cancelation: G.168-2004 compliant, 64-msec tail length ■ Adaptive Jitter Buffer ■ Voice Activity Detection ■ Comfort Noise Generation ■ Packet Lost Concealment ■ RTP/RTCP Packetization (RFC 3550, RFC 3551), SRTP (RFC 3711)
Microsoft Teams phones feature set	■ Authentication (Sign in with user credentials; Sign in using PC/Smartphone; Modern Authentication; Phone lock/unlock) ■ Calling (Incoming/Outgoing P2P calls; In-call controls via UI (Mute, hold/resume, transfer, end call); PSTN calls; Visual Voicemail; 911 support ■ Calendar and Presence (roadmap feature) (Calendar Access ; Presence Integration; Exchange Calendar Integration; Contact Picture Integration; Corporate Directory Access)
Configuration and Management	■ Teams admin center (TAC) ■ OVOC / Device Manager
Debugging Tools	■ AudioCodes' Android Device Utility (see Android Device Utility on page 97) ■ Log upload to Microsoft server (certification for 3rd party Skype for Business clients) ■ Remote logging via Syslog ■ SSH Access ■ Capturing the phone screen ■ TCPdump ■ Audio Debug recording logs ■ Media logs (*.blog) ■ Remote Packet Capture network sniffer application
Localization	■ Multi-lingual support; the language pack list is not yet final and is

Feature	Details
Support	subject to modification.
Hardware	■ Graphic 4.3" color screen, 480x272 resolution, with multi-lingual support ■ Wired connectivity: ✓ Two RJ-45 [Gigabit Ethernet (GbE)] (10/100/1000BaseT Ethernet) ports: LAN and PC port ✓ RJ-9 port (jack) for headset ✓ USB port for USB headset. Note that **C435HD-R** (**TEAMS-C435HD-R**) is a PoE Class 2 device (also when connecting a standard USB headset). If used with a loud USB speakerphone, an external power supply must be used. For more information, contact AudioCodes. ✓ RJ-11 interface ■ Power: ✓ DC jack adapter 12V ✓ Power supply AC 100 ~ 240V ✓ PoE Class 2: 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

Table 1-2: Teams Features Supported by the C435HD Phone

Teams Feature	C435HD
Call Transfer	√
Consultative Transfer	√
Escalate P2P call to Teams Meeting / Conference (Add-hoc Conference)	√
Call Queue	√
Contacts / People	√
Speed Dials dedicated keys	Not supported
Visual VM (when C435HD is used as a CAP, it's supported only after enabling 'Advanced calling')	√
Calendar	Not supported
Click to join meeting	Not supported
Hot Desking	√
Common Area Phone (CAP)	√
CAP: Advanced calling	√
CAP: Voice Mail (only applicable when 'CAP: Advanced calling' is enabled)	√
Music on Hold (MoH)	Not supported (to be supported in future Teams app releases)
Call Forward via phone UI	√
Teams self presence publish	√
Teams co-workers presence display	√
Call Park	Not supported
Favorites list for speed dial	√
Delegation	Supported but configured from Teams client

Teams Feature	C435HD
Meet Now	Not supported
Better Together (over Bluetooth)	Not supported
AudioCodes Device Duo	Roadmap
Survivable Branch Appliance (SBA)	√
Talkback	Not supported

Allowing URLs, Ports (Security)

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

From the device point of view, the following table summaries the ports the phone uses.

Table 1-3: URLs / Ports to Allow when Deploying Teams Phones (Security)

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

Security Guidelines for Android-based Native Teams Devices

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

When analyzing device security, two levels must be addressed:

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

AudioCodes recommends the following:

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

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

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

Android-Level Security Hardening

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

- See Google Play Services on the next page
- See Running Android in Kiosk Mode on the next page
- See Screen Lock on the next page
- See AudioCodes Private Key on the next page
- See Android Debug Bridge (ADB) on page 8
- See App Signing on page 8
- See Web Browser on page 8
- See Remote Configuration Management on page 8
- See AudioCodes Device Manager Validation on page 8
- See Sandboxing on page 9
- See Device File System on page 9

- See Keystore on page 9
- See Device Certificate on page 9
- See Data Protection on page 9
- See Debugging Interface on page 9
- See SSH Access: Reduced File System
- See Android Security Updates on page 10

Google Play Services

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

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

Running Android in Kiosk Mode

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

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

Screen Lock

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

AudioCodes Private Key

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

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

Android Debug Bridge (ADB)

⚠ The device does not allow access to ADB.

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

App Signing

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

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

Web Browser

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

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

Remote Configuration Management

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

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

AudioCodes Device Manager Validation

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

- The device is shipped with known trusted certificate installed. See AudioCodes Root CA Certificate on page 10.
- For the initial connection, the AudioCodes Device Manager accesses devices using a known trusted certificate.

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

Sandboxing

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

Device File System

The AudioCodes device's file system is encrypted on 435HDdevices. Customers may enforce a policy of device encryption via Microsoft's cloud-based Intune service.

Keystore

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

Device Certificate

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

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

⚠

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

Data Protection

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

Debugging Interface

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

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

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

SSH Access: Reduced File System Privileges

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

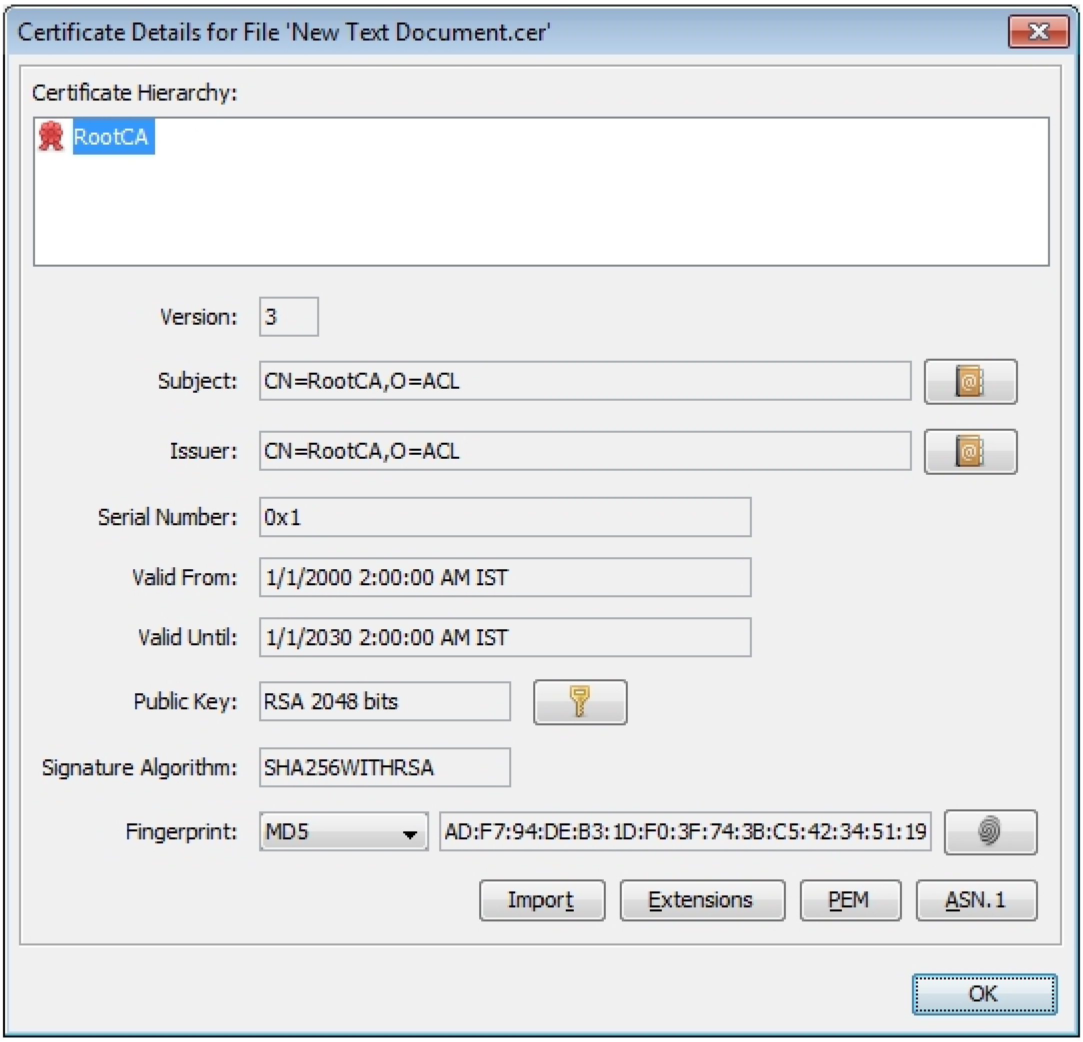
Android Security Updates

AudioCodes regularly adopts and integrates Android security updates.

For reference, see here.

AudioCodes Root CA Certificate

The following figure shows the AudioCodes Root CA Certificate.



Certificate Details for File 'New Text Document.cer'

Certificate Hierarchy:

RootCA

Version: 3

Subject: CN=RootCA,O=ACL

Issuer: CN=RootCA,O=ACL

Serial Number: 0x1

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

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

Public Key: RSA 2048 bits

Signature Algorithm: SHA256WITHRSA

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

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

MIIDMTCCAhmgAwIBAgIBATANBgkqhkiG9w0BAQsFADAfMQwwCgYDVQQKEwNBQ0wx

DzANBgNVBAMTBlJvb3RDQTAeFw0wMDAxMDEwMDAwMDBaFw0zMDAxMDEwMDAwMDBa

MB8xDDAKBgNVBAoTA0FDTDEPMA0GA1UEAxMGUm9vdENBMIIBIjANBgkqhkiG9w0B

AQEFAAOCAQ8AMIIBCgKCAQEA6GK495KUCXAm/UE17G4/cjnZN4LNaxYEYzbfZL0a

EhgSKYt/LQ+iUcDhojsneusNgrcGkpwKklKsGsvGWmSRNULV01CW+TX2VJN73+hh
V0uzhyOIYAUhbDaoqNM6Kp5b7sJ1ew4Ig9kfd/ma9CzI5koESLIw/inLj/r+rD96

```
mUcPEIWrKspv7Qy4I14fsK/yMArixRopTL1munVVPpSFM9Jh8IY3JHyr5CQJXKK
s
EhGAJsnHaRqsR2Su3X/WtsIgEF+cvP34pxhIhFL29nMfnaFATSS3rgGaFISvI1ZS

esLMqkWjp9cqGYrvt7K61sYnvMMb+o/KbWqVokXb+Fr7bwIDAQABo3gwdjAMB
gNV

HRMEBTADAQH/MB0GA1UdDgQWBBQDXySn9hz15lDraZ+iXddZGReB+zBHB
gNVHSME

QDA+gBQDXySn9hz15lDraZ+iXddZGReB+6EjpCEwHzEMMAoGA1UEChMDQU
NMMQ8w

DQYDVQQDEwZSb290Q0GCAQEwDQYJKoZIhvcNAQELBQADggEBAI0rUywo
mmWWJnH3

JOfKiS3+VnX5hJITZymvWanMXUz/6FonHccPXEBYTrUYwhiWx3dwELAFXDFK
kxMp

0KKWZ4F39cAOLRjqhzya+xUeeJ9HQZCXYAJ6XgvTfN2BtyZk9Ma8WG+H1hNv
vTZY

QLbWsjQdu4eFniEufeYDke1jQ6800LwMIFIc59hMQCeJTenRx4HdJbJV86k1gBU
E

A7fJT1ePrRnXNDRz6QtADWoX3OmN7Meqen/roTwvLpEP22nYwvB28dq3JetIQ
Kwu
XC4gwI/o8K2wo3pySLU9Y/vanxXCr0/en5I3RDz1YpYWmQwHA8jJIu8rxdhr+VNQ
Zv6R/Ys=
-----END CERTIFICATE----
```

2 Setting up the Phone

The instructions following show how to set up the phone.

Unpacking

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

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

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

Device Description

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

Front View

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

Figure 2-1: Front View

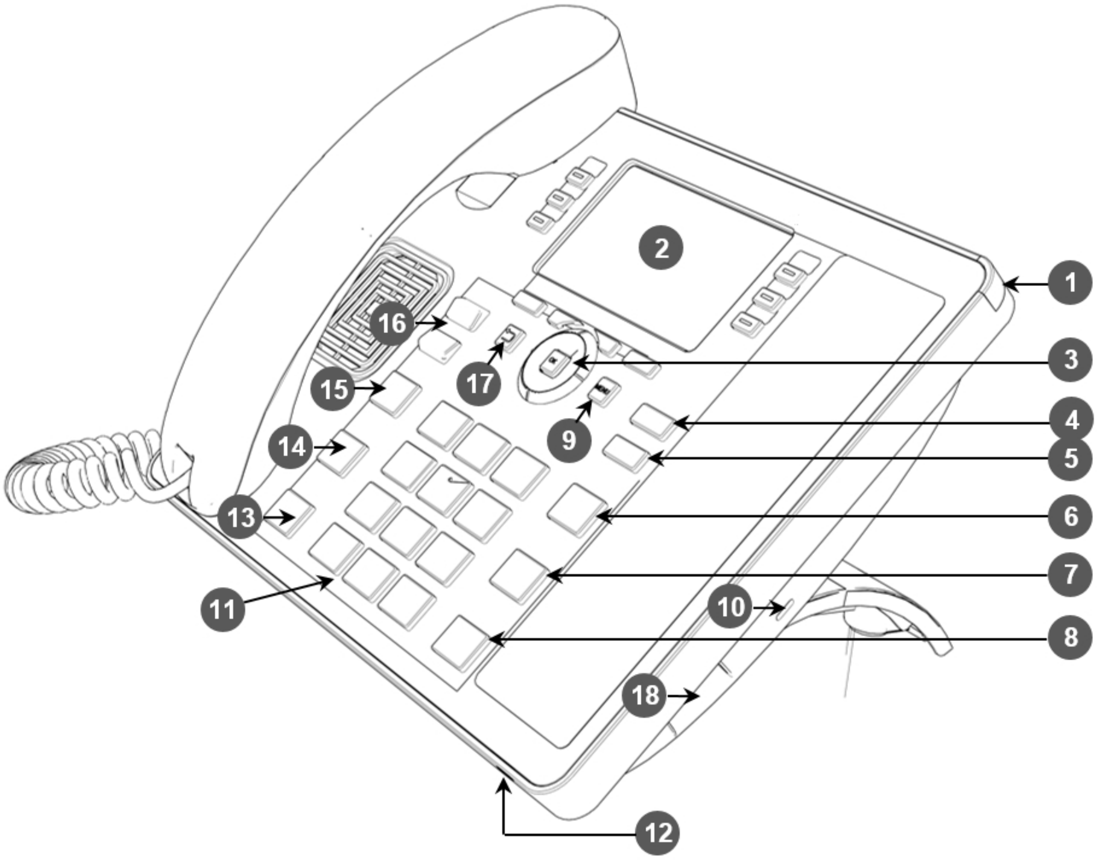


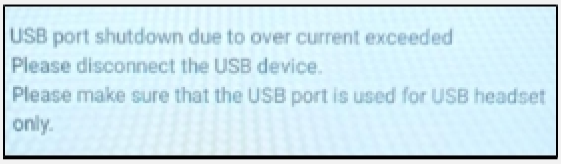
Table 2-1: Font View Description

Item #	Label Name	Description
1	Ring LED	Indicates phone status: ■ Green: Idle state ■ 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	T	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	For a USB headset. See also the note below.

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



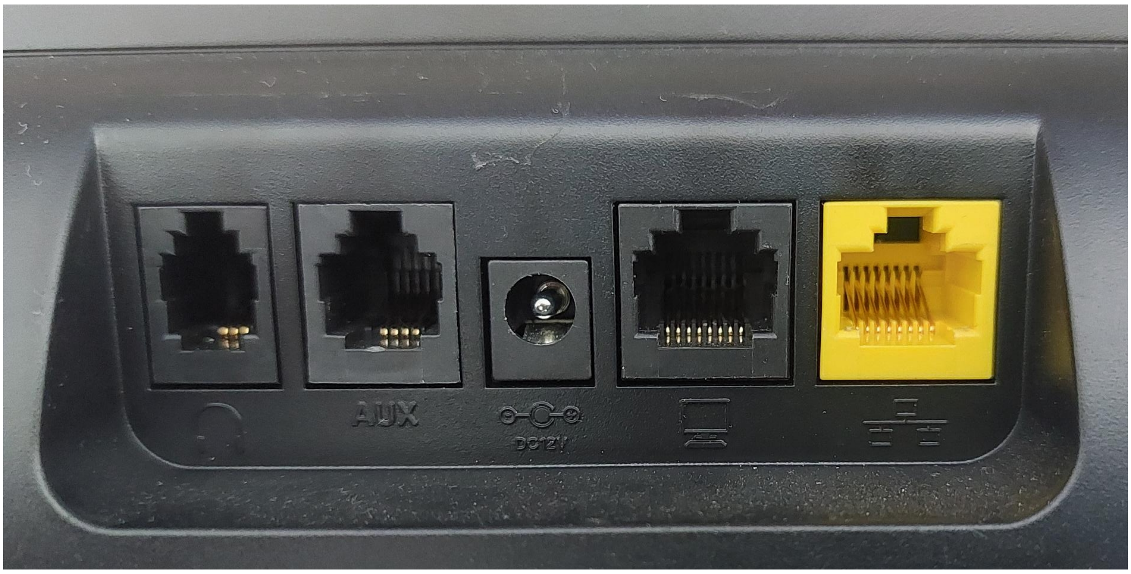
USB port shutdown due to over current exceeded
Please disconnect the USB device.
Please make sure that the USB port is used for USB headset only.

Navigate to menus and select menu items by:

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

Rear View

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



Ports (from right to left)	Description
🖧	RJ-45 port to connect to the Ethernet LAN cable for the LAN connection (uplink - 10/100/1000 Mbps). If you're using Power over Ethernet (PoE), power to the phone is supplied from the Ethernet cable (draws power from either a spare line or a signal line).
🖥	RJ-45 port to connect the phone to a PC (10/100/1000 Mbps downlink).
⊖-●-⊕ DC12V	12V DC power jack that connects to the AC power adapter.
AUX	[RJ-11 port] Used as a serial console port to access the phone's terminal.
🎧	Headset jack, i.e., RJ-9 port that connects to an external headset.
(Not seen in the image | Located at the bottom of the device)	RJ-9 port used to connect the phone’s handset.

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.

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

Mounting the Phone

The phone can be mounted on a:

- Desk (see Desktop Mounting)

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

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

Before Using AudioCodes Devices

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

➢ To clean a device's screen:

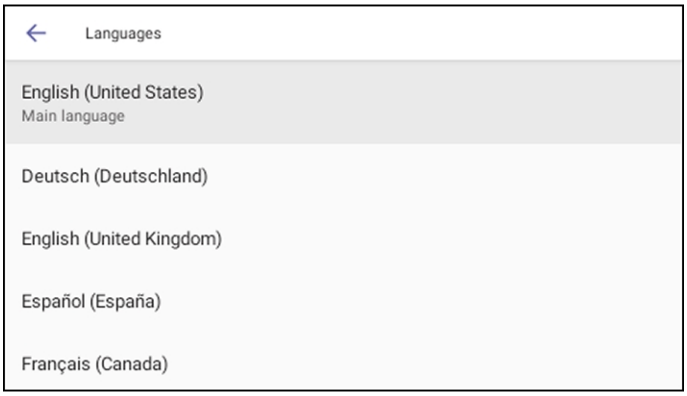
1. Disconnect all cables.
2. Spray onto a clean, dry, microfiber duster a medicinal isopropyl alcohol and water solution of 70:30. Don't oversaturate the duster. If it's wet, squeeze it out.
3. Lightly wipe the screen of the device.
4. Wait for the screen to dry before reconnecting cables.

3 Starting up

Here's how to start up the phone.

➢ To start up:

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



← Languages

English (United States)
Main language

Deutsch (Deutschland)

English (United Kingdom)

Español (España)

Français (Canada)

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

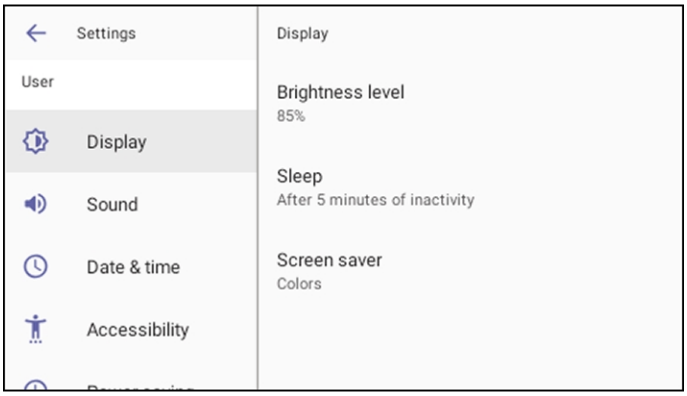
⚠ It will be necessary to repeat this only if the phone is restored to default settings.

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.



← Settings

User

Display

Sound

Date & time

Accessibility

Powersaving

Display

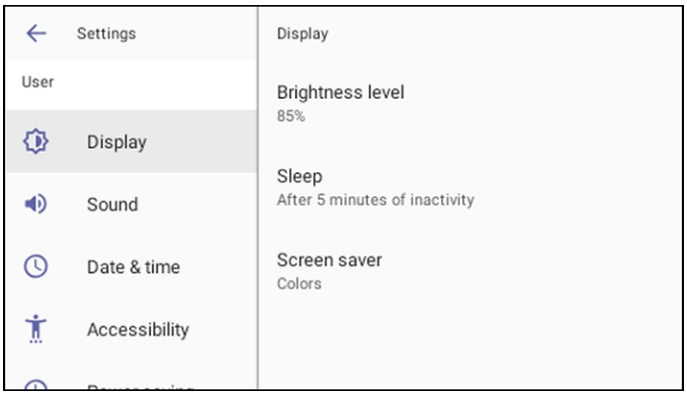
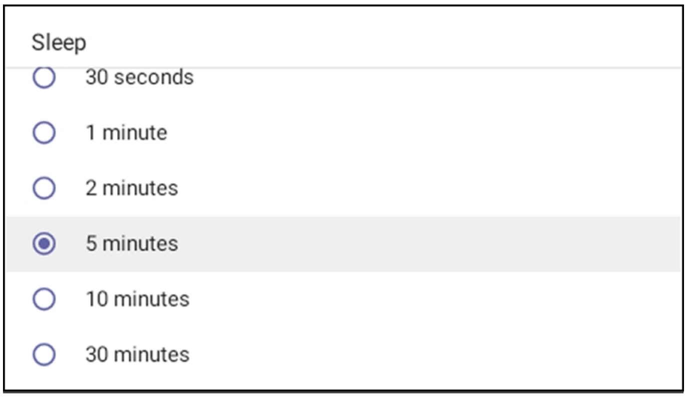
Brightness level
85%

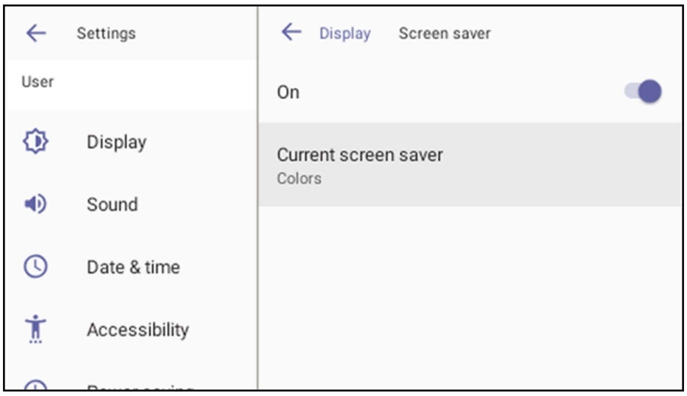
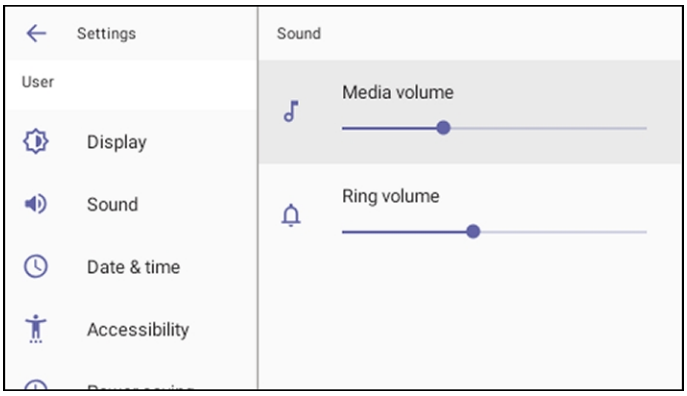
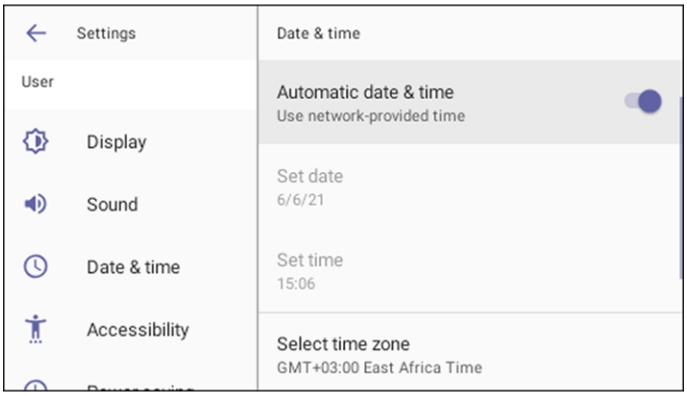
Sleep
After 5 minutes of inactivity

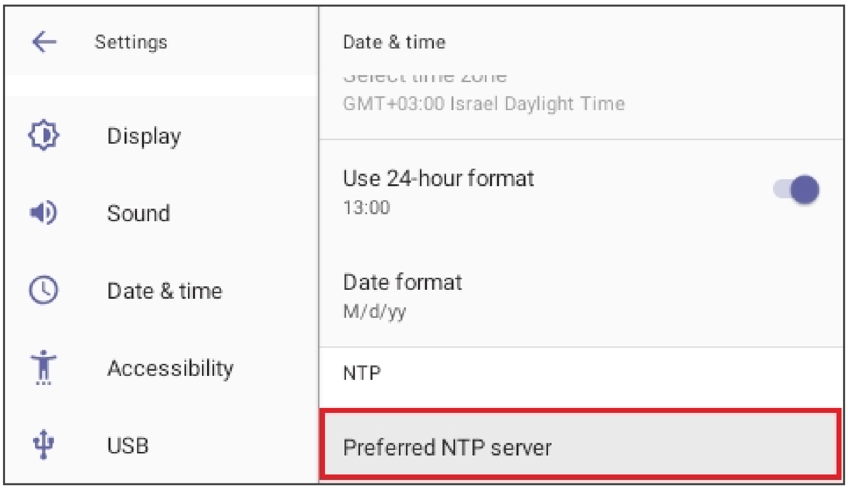
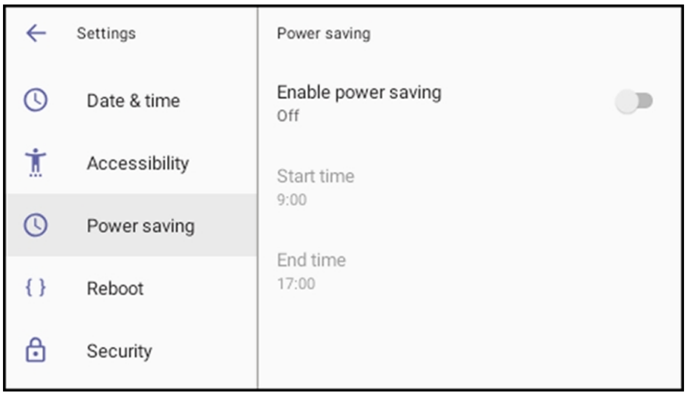
Screen saver
Colors

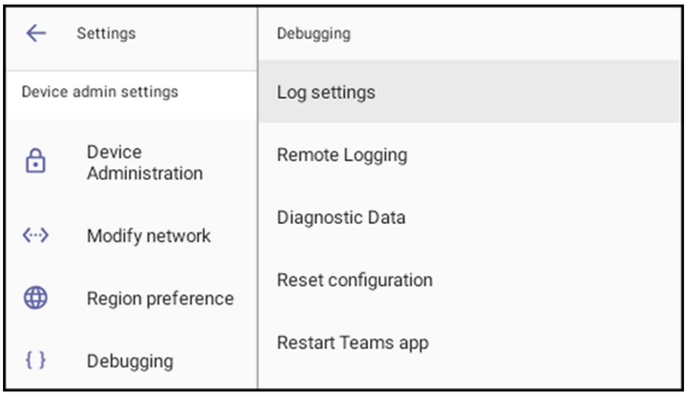
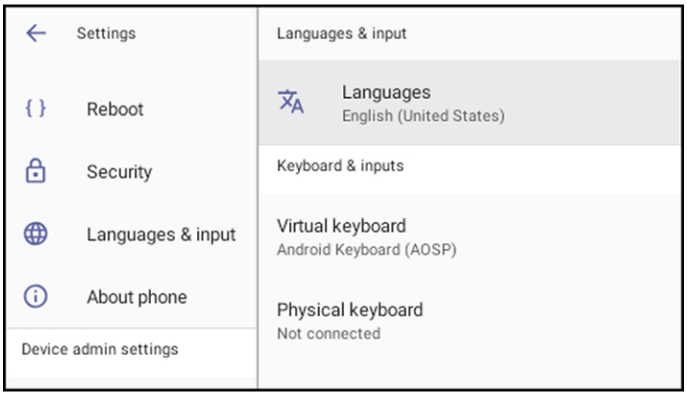
2. View the settings under 'User'. Select a setting to open it. Use the table following as reference. [To view settings related to the network administrator, scroll down and open 'Device Administration'].

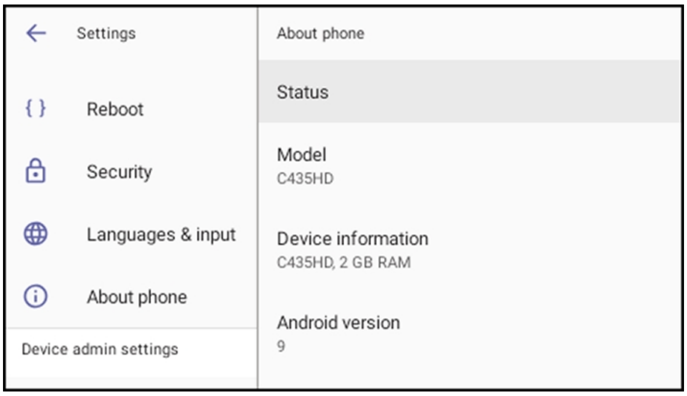
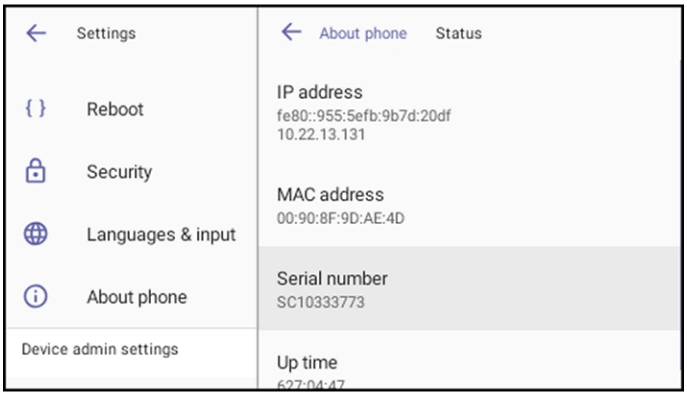
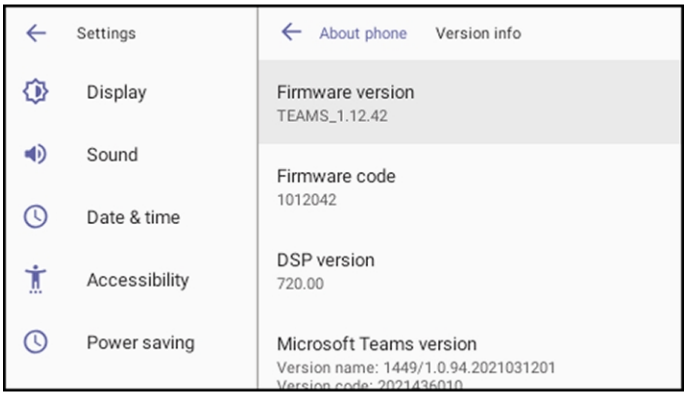
Table 3-1: Device Settings

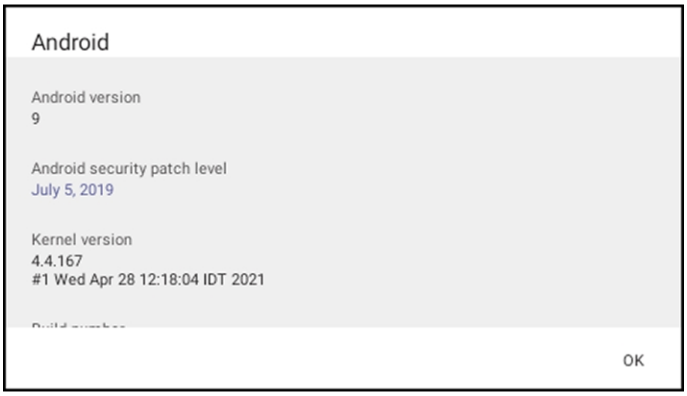
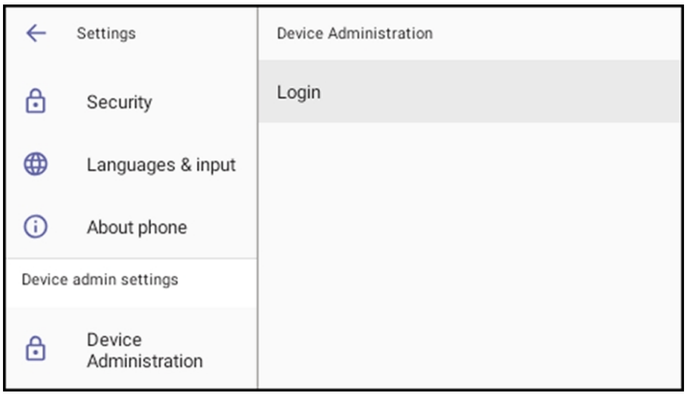
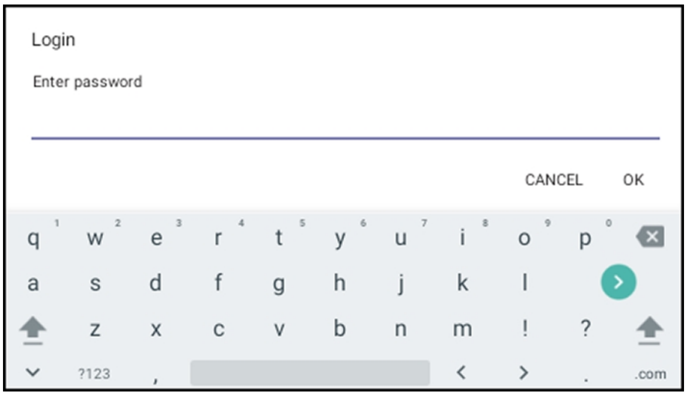
Setting	Description
User	
Display	Opens the ‘Display’ screen [Brightness level].  Settings User Display Sound Date & time Accessibility Display Brightness level 85% Sleep After 5 minutes of inactivity Screen saver Colors The phone's screen supports different brightness levels. Choose the level that suits your requirements. ■ Sleep  Sleep ○ 30 seconds ○ 1 minute ○ 2 minutes ● 5 minutes ○ 10 minutes ○ 30 minutes ■ Screen saver

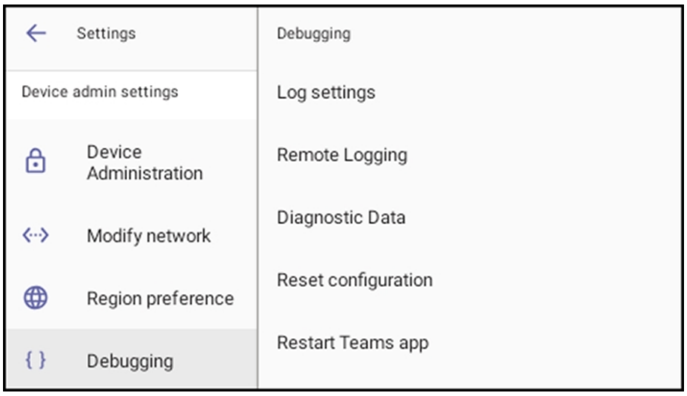
Setting	Description
	 Settings User Display Sound Date & time Accessibility Display Screen saver On Current screen saver Colors
Sound	Allows you to customize phone volume for a friendlier user experience. **Ring volume at n%**  Settings User Display Sound Date & time Accessibility Sound Media volume Ring volume
Date & time	Date and time are automatically retrieved from the deployed Network Time Protocol (NTP) server.  Settings User Display Sound Date & time Accessibility Date & time Automatic date & time Use network-provided time Set date 6/6/21 Set time 15:06 Select time zone GMT+03:00 East Africa Time Use 24-hour format [Allows you to select the Time format] Also supported is a simplified version of NTP called Simple Network Time Protocol (SNTP). Both can be used to synchronize device clocks. SNTP is typically used if full implementation of NTP is not required.

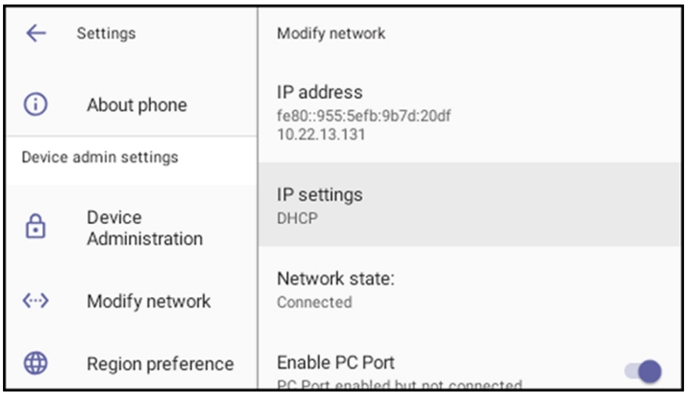
Setting	Description
NTP Preferred NTP server	Admins can use this parameter to *manually* define the NTP server, to comply with enterprise security requirements if those requirements preclude using DHCP Option 42. Manual configuration takes precedence over DHCP Option 42 and the time servers. Two ways to manually define the NTP server are available: ■ Admins can define it in the phone's GUI.  Settings Display Sound Date & time Accessibility USB Date & time Select time zone GMT+03:00 Israel Daylight Time Use 24-hour format 13:00 Date format M/d/yy NTP Preferred NTP server ■ Admins can alternatively use the newly added parameter 'date_time/ntp/server_address' in the phone's .cfg configuration file. See also under Signing In on page 37.
Power Saving	Allows users to contribute to power saving in the enterprise.  Settings Date & time Accessibility Power saving Reboot Security Power saving Enable power saving Off Start time 9:00 End time 17:00 Enable power saving Start time [The device consumes minimal energy before the user arrives at the office] End time [The device consumes minimal energy after the user leaves the office]
Debugging	Enables users to reboot the device.

Setting	Description
	 Settings Device admin settings Device Administration Modify network Region preference Debugging Debugging Log settings Remote Logging Diagnostic Data Reset configuration Restart Teams app 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 49
Languages & input	Allows users to customize inputting to suit personal requirements.  Settings Reboot Security Languages & input About phone Device admin settings Languages & input Keyboard & inputs Languages English (United States) Virtual keyboard Android Keyboard (AOSP) Physical keyboard Not connected
About	Provides users with device information.

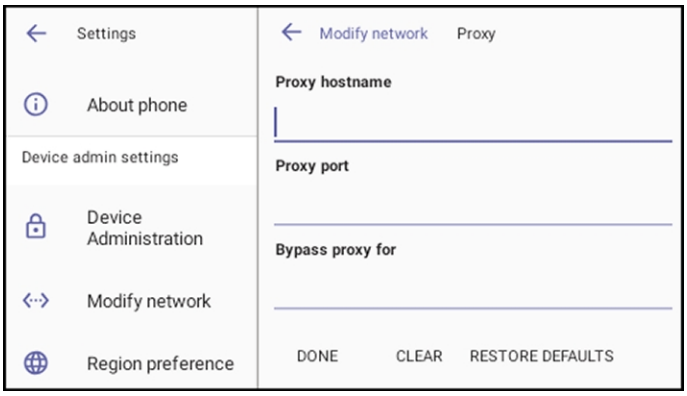
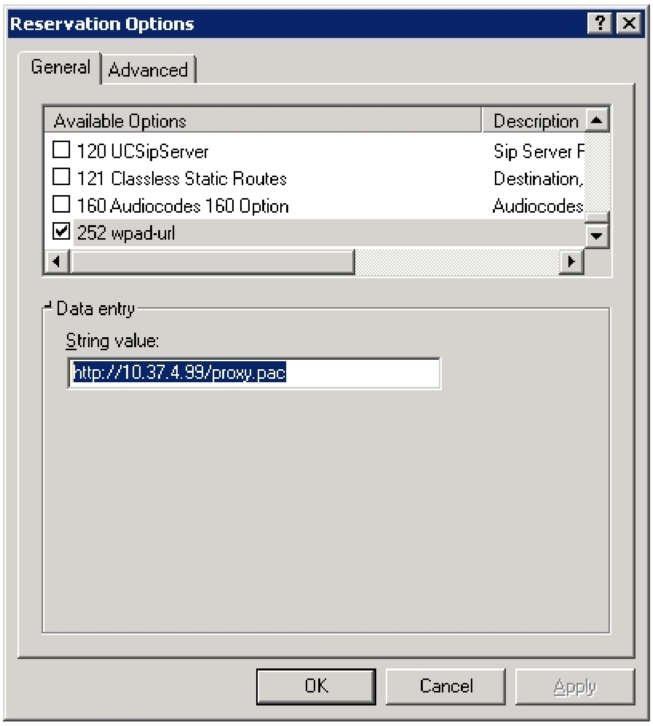
Setting	Description
	 Settings { } Reboot Security Languages & input About phone Device admin settings About phone Status Model C435HD Device information C435HD, 2 GB RAM Android version 9 To determine the device's IP address, select the 'Status' option.  Settings { } Reboot Security Languages & input About phone Device admin settings About phone Status IP address fe80::955:5efb:9b7d:20df 10.22.13.131 MAC address 00:90:8F:9D:AE:4D Serial number SC10333773 Up time 627:04:47 To get information about the version, select 'Version info'.  Settings Display Sound Date & time Accessibility Power saving About phone Version info Firmware version TEAMS_1.12.42 Firmware code 1012042 DSP version 720.00 Microsoft Teams version Version name: 1449/1.0.94.2021031201 Version code: 2021436010 To get information about the Android version, select 'Android version'.

Setting	Description
	 Android Android version 9 Android security patch level July 5, 2019 Kernel version 4.4.167 #1 Wed Apr 28 12:18:04 IDT 2021
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.  Settings Security Languages & input About phone Device admin settings Device Administration Device Administration Login Select **Login** and then in the Login screen that opens, select the 'Enter password' field and use the virtual keyboard to enter the password (**1234** or **1111**). Note that the virtual keyboard pops up for all ‘Settings’ fields to allow inputting characters and / or numbers. Two virtual keyboard types can be displayed: Numeric or QWERTY.  Login Enter password CANCEL OK q w e r t y u i o p a s d f g h j k l z x c v b n m ! ? ?123 , < > . .com

Setting	Description
	⚠ ● The phone support a strong password check in order to log in as Administrator. The feature strengthens security. Note that the default password: ✓ must be changed before accessing the device via SSH ✓ can be changed per device from the phone screen (the user first enters the default password and is then prompted to modify it to a more complete password) or via bulk configuration of multiple devices using Microsoft's TAC or AudioCodes' Device Manager. ● Criteria required for a strong password are provided. The password must: ✓ be greater than or equal to 8 characters in length. ✓ contain one or more uppercase characters. ✓ contain one or more lowercase characters. ✓ contain one or more numeric values. ✓ contain one or more special characters. The virtual keyboard is also displayed when the network administrator needs to enter an IP address to debug, or when they need to enter their PIN lock for the security tab. After logging in, scroll down in the Settings screen to the section 'Device Administration'.  Settings Device admin settings Device Administration Modify network Region preference Debugging Debugging Log settings Remote Logging Diagnostic Data Reset configuration Restart Teams app
Modify network	Enables the Admin user to determine network information and to modify network settings.

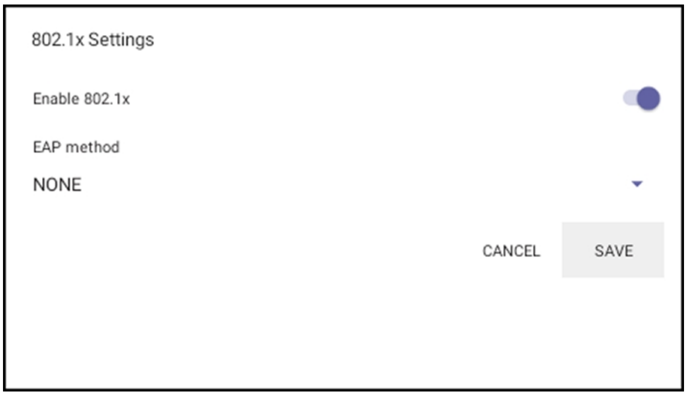
Setting	Description
	 Settings About phone Device admin settings Device Administration Modify network Region preference Modify network IP address fe80::955:5efb:9b7d:20df 10.22.13.131 IP settings DHCP Network state: Connected Enable PC Port PC Port enabled but not connected IP Address [Read Only] IP Settings [DHCP or Static IP] Network state [Read Only] Enable PC port Enable PC port mirror Proxy 802.1x Settings VLAN Settings. Allows you to configure the VLAN mode **Manual**, **CDP only** or **LLDP only**. Note that **LLDP** switch information is retrieved (for location purposes) when parameter network/lan/lldp/enabled=1 (even when VLAN is retrieved from **CDP** or VLAN is disabled or VLAN is **Manual**). In versions prior to 1.19, if network VLAN mode 'network/lan/vlan/mode' was set to **LLDP**, the phone retrieved the VLAN and LLDP switch information (for location purposes) from LLDP.
Proxy	The phone can be configured with an HTTP Proxy server by an Admin user in two ways: ■ **Manually**. The Admin user can use this method to configure HTTP proxy server parameters through the Teams application: a. Log in as Administrator and select **Modify network**. b. Select the **Proxy** option and then configure the proxy host name and port:

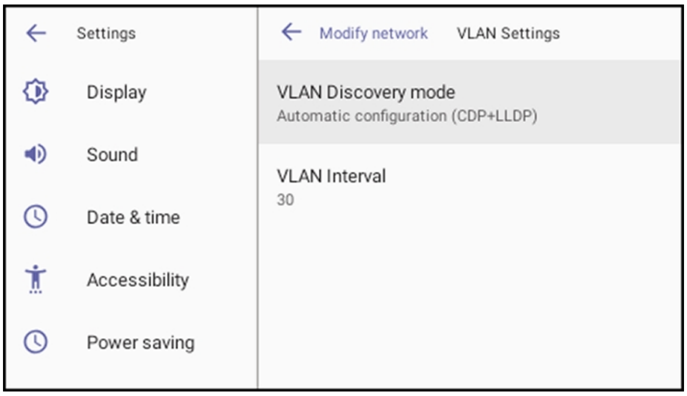
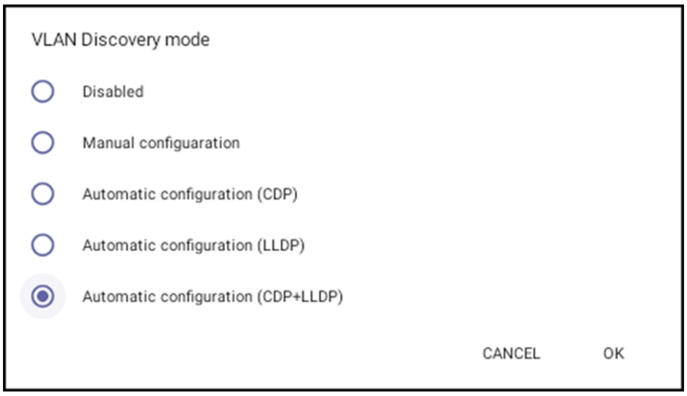
Setting	Description

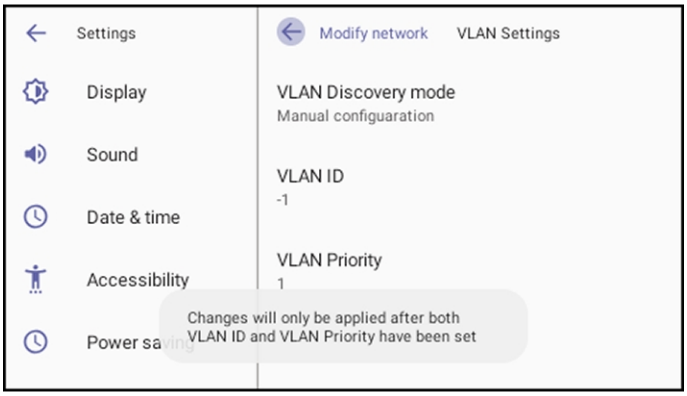
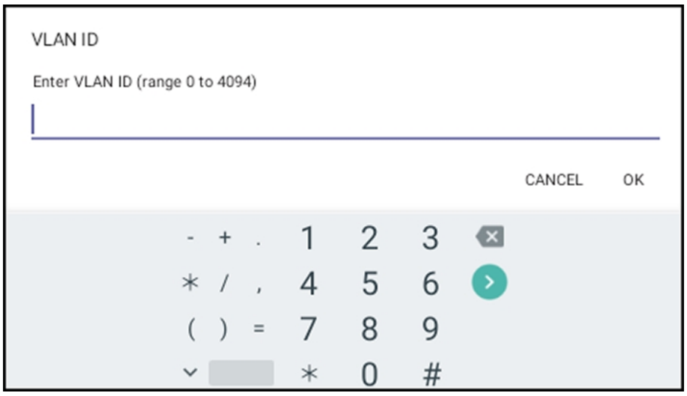
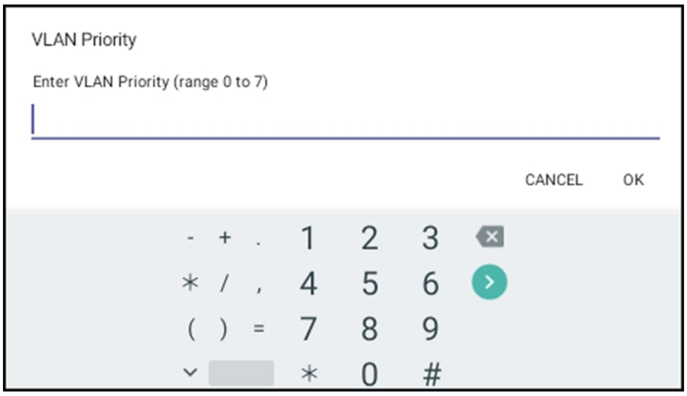
	
	 Settings
	About phone
	Device admin settings
	Device Administration
	Modify network
	Region preference
	Modify network
	Proxy
	Proxy hostname
	Proxy port
	Bypass proxy for
	DONE
	CLEAR
	RESTORE DEFAULTS
	■ **Over DHCP with Option 252**. It's recommended that the Admin user uses this method when provisioning multiple phones. Option 252 provides a DHCP client with a URL to use to configure its proxy settings:
	
	 Reservation Options
	General
	Advanced
	Available Options
	Description
	Data entry
	OK
	Cancel
	Apply
	□ 120 UCSipServer — Sip Server F
	□ 121 Classless Static Routes — Destination,
	□ 160 Audiocodes 160 Option — Audiocodes
	☑ 252 wpad-url
	String value: http://10.37.4.99/proxy.pac
	The proxy setting is provided in a Proxy Auto-Configuration (PAC) file that contains a set of rules coded in JavaScript which allows a web browser to determine whether to send web traffic directly to the Internet or to be sent via a proxy server. PAC files control how the phone handles HTTP, HTTPS and FTP traffic.
	Example of a basic PAC file:
	`function FindProxyForURL(url, host)`
	`{`
	`return "PROXY 10.13.2.40:3128";`

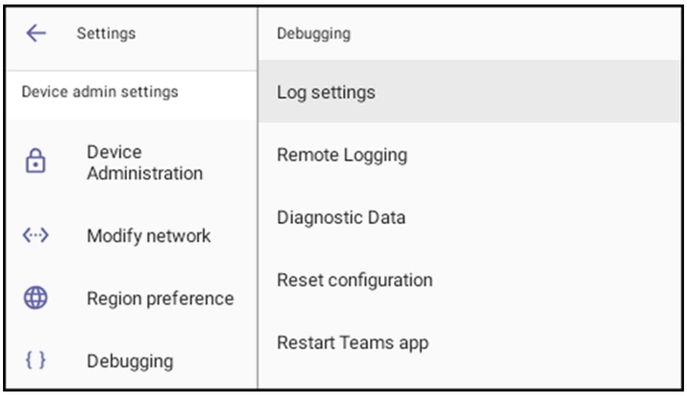
Setting	Description

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

802.1x Settings	802.1X Authentication is the IEEE Standard for Port-based Network Access Control (PNAC). See https://1.ieee802.org/security/802-1x/ for more information. **To configure an 802.1X Authentication method:** 1. From the 'Modify Network' screen (as an Admin), access the 802.1x Settings screen.  802.1x Settings Enable 802.1x EAP method NONE 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) ✓ device certificate (not required for every method) 4. Select the **Save** softkey The 802.1x settings are not only available via the phone screen, they're also supported in the device Configuration File, enabling network administrator's to perform pre-staging configuration for

Setting	Description
	802.1x. The 802.1x settings available in the Configuration File are: ■ Enable/Disable ■ EAP method ■ Identity ■ Password
VLAN Settings	Select the menu option **VLAN Settings**.  Settings Display Sound Date & time Accessibility Power saving Modify network VLAN Settings VLAN Discovery mode Automatic configuration (CDP+LLDP) VLAN Interval 30 Select **VLAN Discovery mode**.  VLAN Discovery mode ○ Disabled ○ Manual configuaration ○ Automatic configuration (CDP) ○ Automatic configuration (LLDP) ● Automatic configuration (CDP+LLDP) ■ 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:

Setting	Description
	 Settings Display Sound Date & time Accessibility Power saving Modify network VLAN Settings VLAN Discovery mode Manual configuaration VLAN ID -1 VLAN Priority 1 Changes will only be applied after both VLAN ID and VLAN Priority have been set Select **VLAN ID**.  VLAN ID Enter VLAN ID (range 0 to 4094) CANCEL OK - + . 1 2 3 * / , 4 5 6 ( ) = 7 8 9 * 0 # Select **VLAN Priority**.  VLAN Priority Enter VLAN Priority (range 0 to 7) CANCEL OK - + . 1 2 3 * / , 4 5 6 ( ) = 7 8 9 * 0 #
Debugging	Allows the Admin user to perform debugging for troubleshooting purposes. Available after logging in as Admin.

Setting	Description
	 Settings Device admin settings Device Administration Modify network Region preference Debugging Debugging Log settings Remote Logging Diagnostic Data Reset configuration Restart Teams app Log settings Remote Logging (see under Remote Logging (Syslog) on page 102 for more information) Diagnostic Data (see under Getting Diagnostics on page 103 for more information) Reset configuration (see here for more information) User data reset Restart Teams app Company portal login Debug Recording (for Media/DSP debugging) (see under Remote Logging (Syslog) on page 102 for more information) Erase all date (factory reset) (the equivalent of restore to defaults; including logout and device reboot) Screen Capture. By default, this setting is enabled. If it's disabled, the phone won't allow its screens to be captured.

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

AudioCodes Android devices can configure VLAN via a DHCP Option when CDP/LLDP isn’t allowed in the organization. The following DHCP Options offer a VLAN ID: Option 43, 132, 128, 129, 144, 157, 191. If the device gets more than one of these DHCP Options, it will apply only one according to the aforementioned order of priority.

Admins must configure ‘VLAN Discovery Mode’ to CDP/LLDP/CDP+LLDP to get VLAN via a DHCP Option. If ‘VLAN Discovery Mode’ is disabled, the devices will not get VLAN via a DHCP Option.

When CDP/LLDP is allowed in the organization, devices will get VLAN via LLDP/CDP Discovery; they will not get it from a DHCP Option. LLDP/CDP Discovery takes precedence over a DHCP Option.

Valid range of VLAN ID values: 0~4094.

DHCP Option syntax is as follows:

DHCP Option 43 (vendor-encapsulated-options). DHCP Server, for MSCPEClient Vendor Class, 010 VLANID (VLAN identifier) has two types:

- VLANID=544(string), packet: 0a0400353434, VLANID=544
- VLANID=0x10(Hex), packet: 0x0a 0x02 0x00 0x10, VLANID=16

DHCP Option 128/129/144/157/191

Syntax: VLAN-A=<value>;(value=hex, octal or decimal)

Examples:

- VLAN-A=12

  VLAN ID is decimal 12

- VLAN-A=0xc

  VLAN ID is Hex 0xc (i.e., decimal 12)

- VLAN-A=014

  VLAN ID is octal 014 (i.e., decimal 12)

DHCP Option 132

Syntax: <value>; only supports a decimal value

Example: 5

VLAN ID is 5

Restoring the Phone to Default Settings

Users can restore the device to factory default settings at any time.

Click here to view a video clip showing how to reset the AudioCodes Teams phone to its factory default settings. The principle is similar across all AudioCodes Teams phones.

The feature can be used if the admin user has forgotten their password, for example.

> ⚠ Restoring the phone to factory default settings brings up the phone with its original bundled Teams application.

Two kinds of restore are available:

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

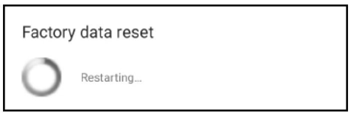
Performing a Hard Restore

You can either:

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

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

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



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

2. Select **OK**; the sign-in screen is displayed (see Signing In on page 37 for more information).

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

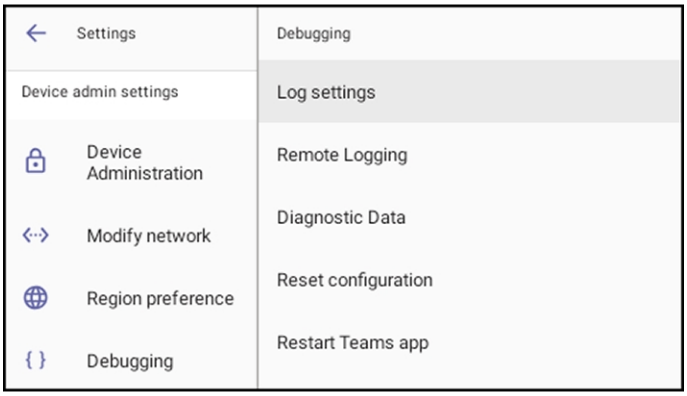
1. Press the OK + MENU keys simultaneously and keeping them pressed, unplug the power cable.
2. Plug the power cable back into the phone continuing to press the OK + MENU keys for +-5 seconds.
3. Release the OK + MENU keys; the phone' settings are restored to their defaults.

Performing a Soft Restore

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

➢ **To perform a soft restore:**

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



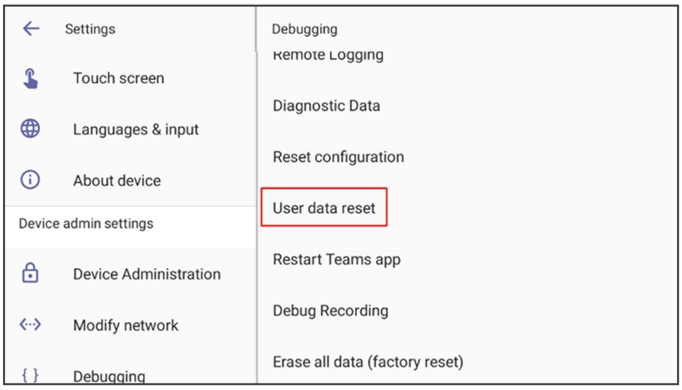
2. Select the **Reset configuration** option; the device performs a restore to default factory settings.

Performing User Data Reset

AudioCodes Teams devices provide a **User data reset** option that is similar to factory reset except that it preserves predefined data after firmware upgrade. The option enables the data to be retained to handle devices more efficiently in scenarios where the factory reset option is inappropriate.

➢ **To access the functionality:**

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



⚠ After ‘User data reset’, network settings are preserved.

Recovery Mode

If a phone goes into recovery mode, you can boot it using its hard keys as shown in Performing a Hard Restore on page 33.

Locking and Unlocking the Phone

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

- Unlock (see Unlock on the next page)
- Automatic lock (Automatic Lock below)

Automatic Lock

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

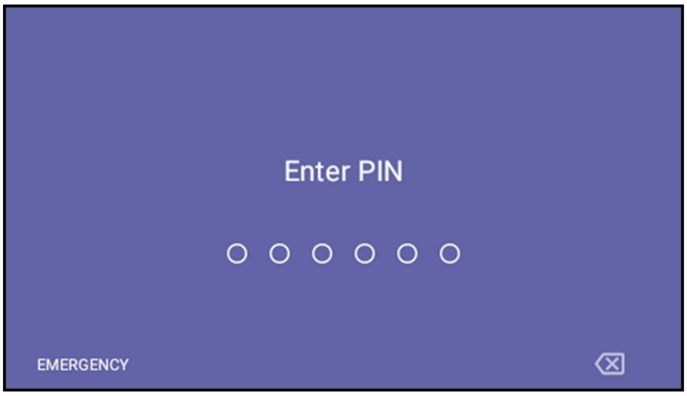
➢ **To lock the phone:**

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

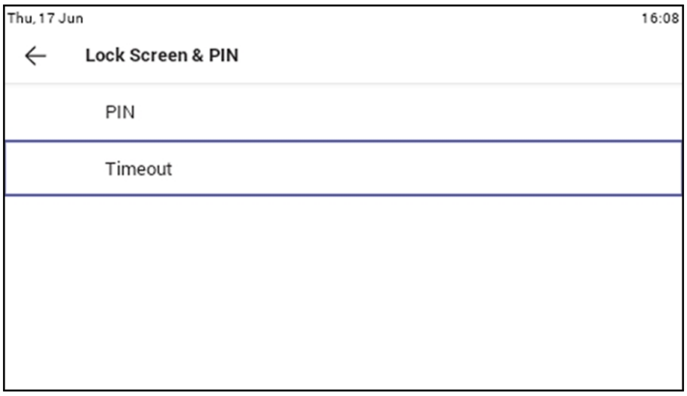
Unlock

➢ To unlock the phone:

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



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



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

4 Teams Application

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

Signing In

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

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

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

‘Modern Authentication’ is also supported.

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

- **DHCP Option 42 (NTP)**. If DHCP Option 42 (NTP) is opted for, the network administrator must specify the server providing NTP for the network.
- **time.android.com**. NTP server option for Android phones.
- **time.windows.com**. The phones’ default NTP server is sometimes not configured in DHCP Option 42. If not, the phones will attempt the Google NTP server. If DHCP Option 42 is not configured and the Google NTP server is blocked (for example), the phones will use this server and if it’s unavailable, the server **time.nist.gov**, described next.
- **time.nist.gov**. The phones’ default NTP server is sometimes not configured in DHCP Option 42. If not, the phones will attempt the Google NTP server. If DHCP Option 42 is not configured and the Google NTP server is blocked (for example), the phones will use this server (**time.nist.gov**) if the server **time.windows.com** described previously is unavailable.
- Admins can **manually define the NTP server** to comply if necessary with enterprise security requirements, if those requirements preclude using DHCP Option 42.

  Manual configuration takes precedence over DHCP Option 42 and the time servers.
  Two ways to manually define the NTP server are available:

  - in the phone's user interface
  - in the phone’s .cfg configuration file, using parameter 'date_time/ntp/server_address'

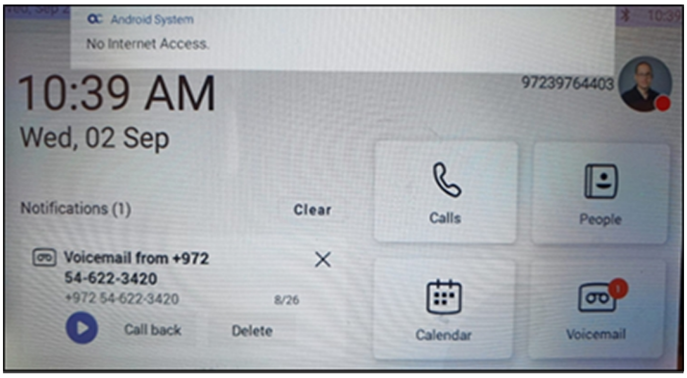
  See also under here for more information.

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

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

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

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



Android System
No Internet Access.

10:39 AM
Wed, 02 Sep

97239764403

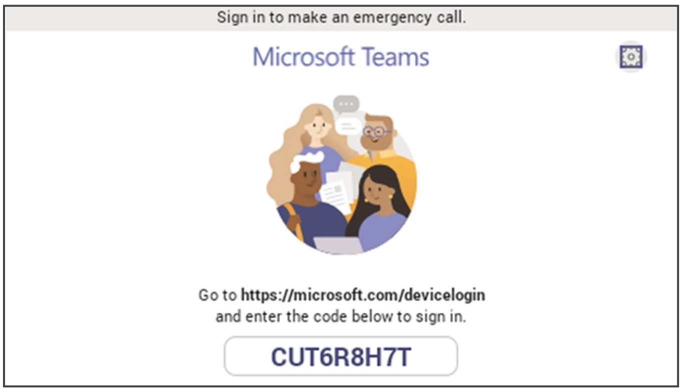
Notifications (1)

Voicemail from +972 54-622-3420
+972 54-622-3420 8/26

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

➢ To sign in:

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



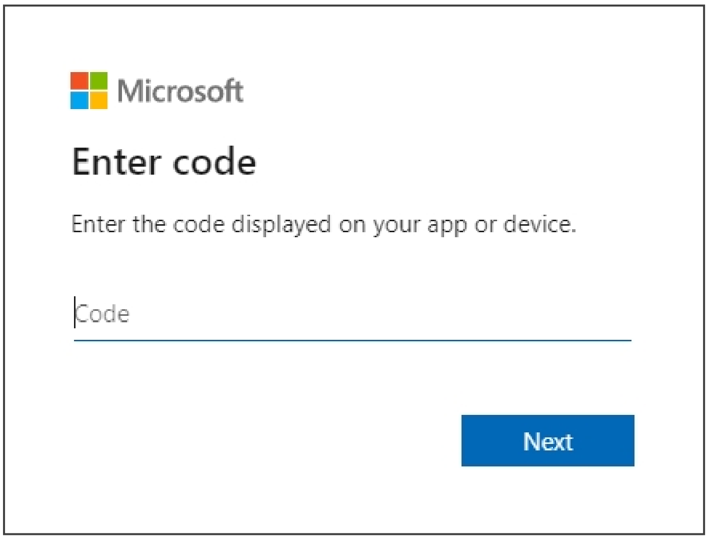
Sign in to make an emergency call.

Microsoft Teams

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

CUT6R8H7T

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



Microsoft

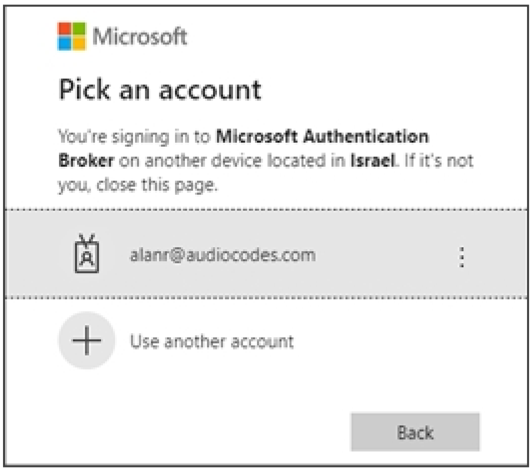
Enter code

Enter the code displayed on your app or device.

Code

Next

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



Microsoft

Pick an account

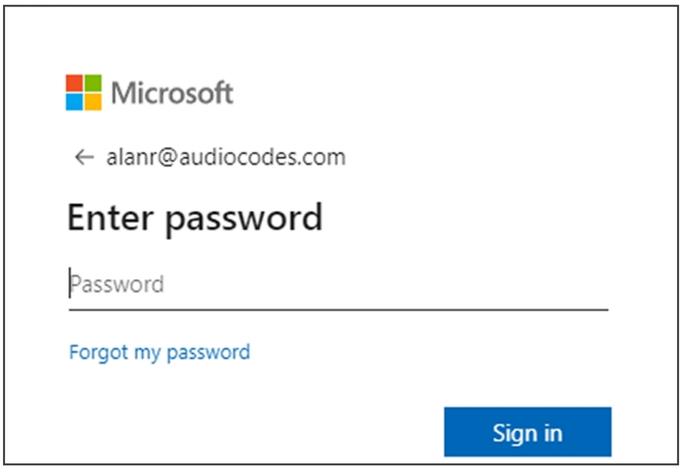
You're signing in to **Microsoft Authentication Broker** on another device located in **Israel**. If it's not you, close this page.

alanr@audiocodes.com

Use another account

Back

4. Click the account.



Microsoft

← alanr@audiocodes.com

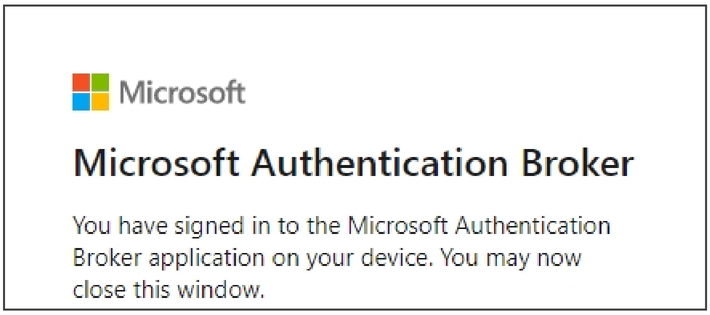
Enter password

Password

Forgot my password

Sign in

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

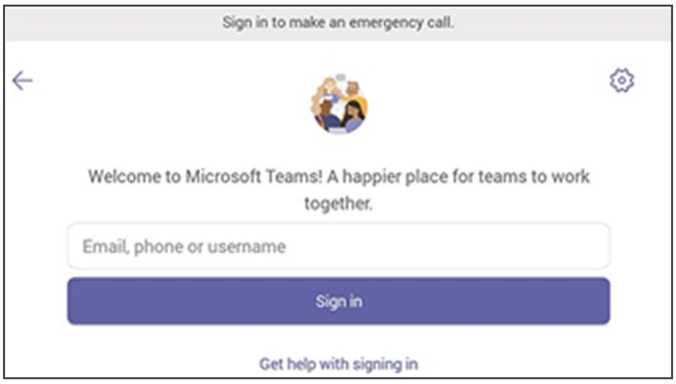


Microsoft

Microsoft Authentication Broker

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

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



Sign in to make an emergency call.

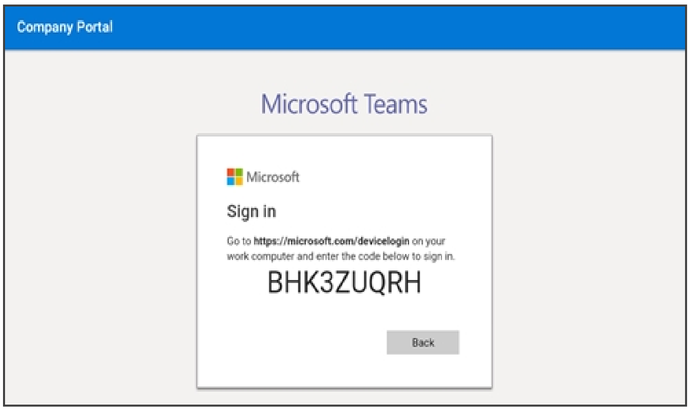
Welcome to Microsoft Teams! A happier place for teams to work together.

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

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

- must be changed before accessing the device via SSH
- can be changed per device in the phone screen (the user first enters the default password and is then prompted to modify it to a more complete password) or via bulk configuration of multiple devices using Microsoft's TAC or AudioCodes' Device Manager
- Criteria required for a strong password are provided: The password must:
  - ✓ be greater than or equal to 8 in length
  - ✓ contain one or more uppercase characters
  - ✓ contain one or more lowercase characters
  - ✓ contain one or more numeric values
  - ✓ contain one or more special characters

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



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

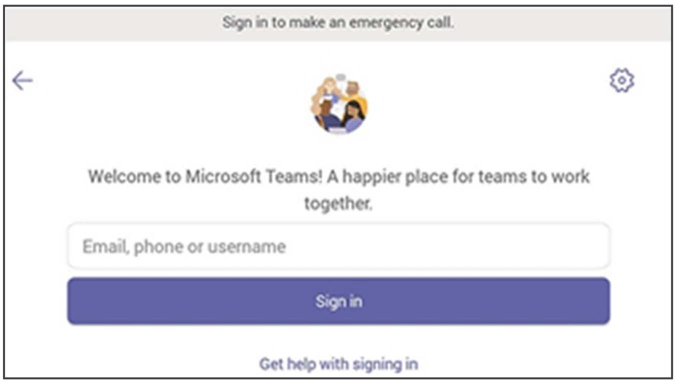
BHK3ZUQRH

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

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

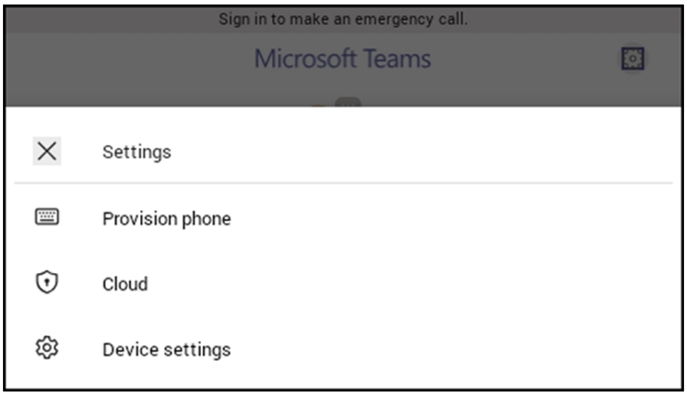
Multi-Cloud Sign-in

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



Sign in to make an emergency call.

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



Sign in to make an emergency call.

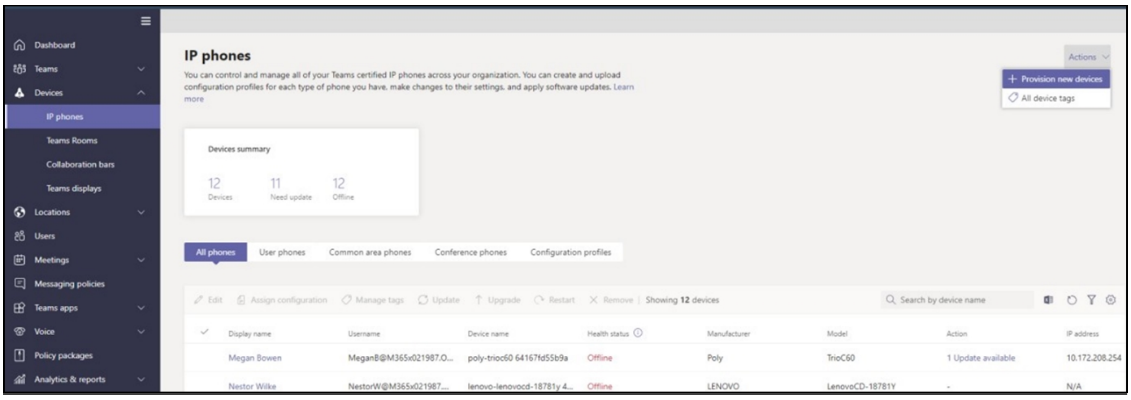
Remote Provisioning and Sign-in from Teams admin center

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

➢ Step 1: Add a device MAC address

Provision the device by imprinting a MAC address on it.

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



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

Showing **12** devices

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

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

Manually add a device MAC address

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

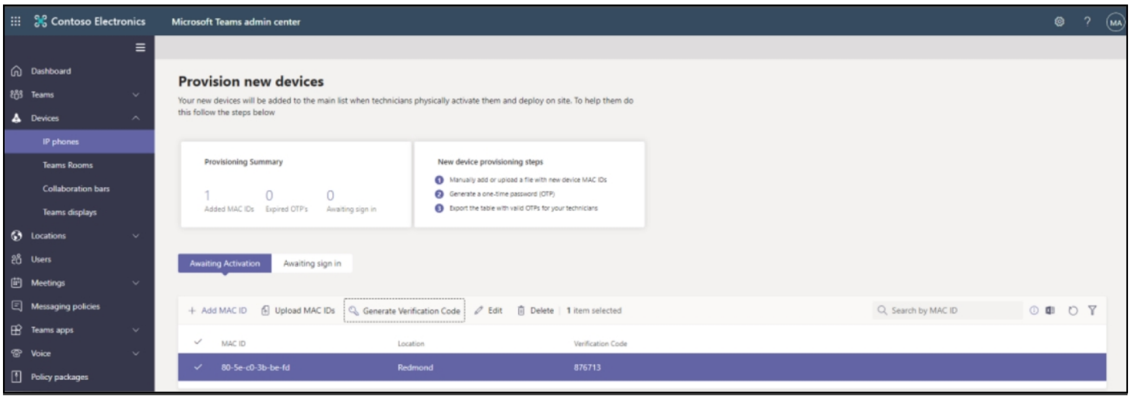
Upload a file to add a device MAC address

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

➢ Step 2: Generate a verification code

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

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



Provision new devices

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

Provisioning Summary

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

New device provisioning steps

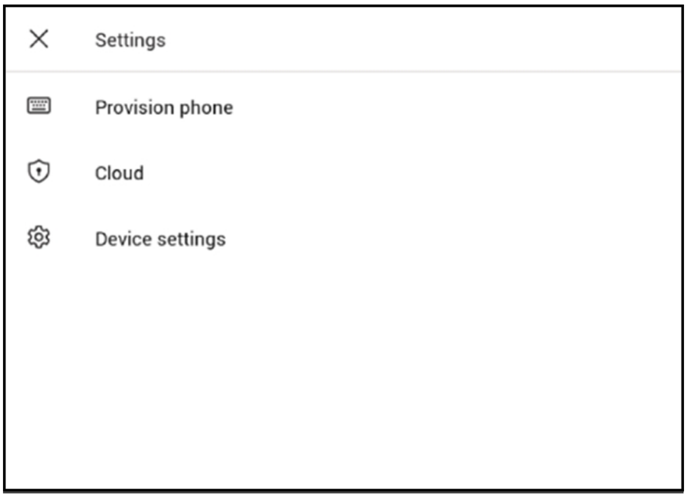
1. Manually add or upload a file with new device MAC IDs
2. Generate a one-time password (OTP)
3. Export the table with valid OTPs for your technicians

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

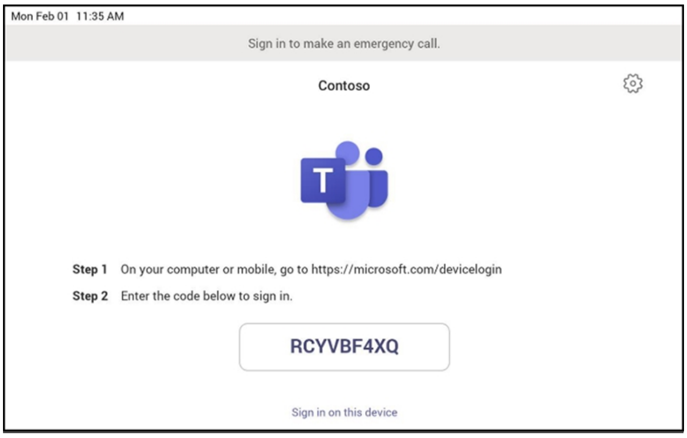
You'll need to provide the list of MAC IDs and verification codes to the field technicians. You can export the detail directly in a file and share the file with the technician who is doing the actual installation work.

➢ Step 3: Provisioning on the device

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



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



Mon Feb 01 11:35 AM

Sign in to make an emergency call.

Contoso

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

Step 2 Enter the code below to sign in.

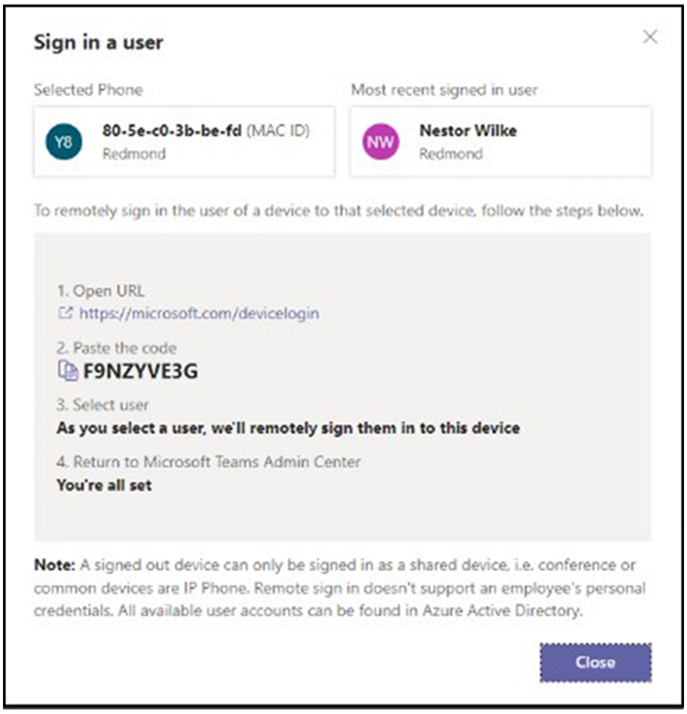
RCYVBF4XQ

Sign in on this device

➢ Step 4: Sign in remotely

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

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



Sign in a user

Selected Phone

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

Most recent signed in user

NW **Nestor Wilke**
Redmond

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

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

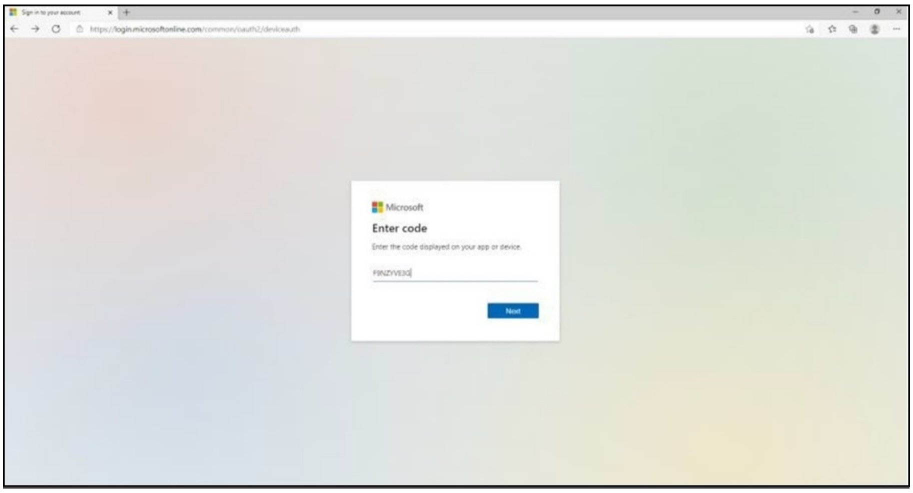
2. Paste the code
F9NZYVE3G

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

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

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

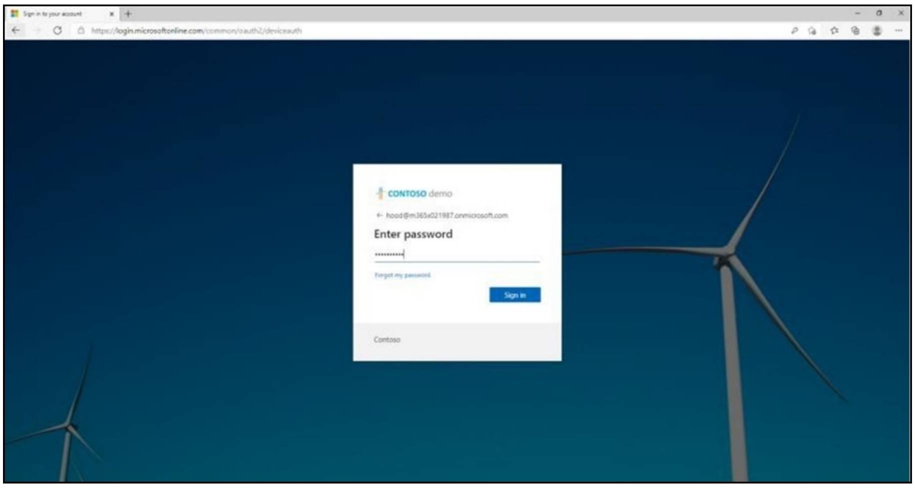
The tenant admin is expected to complete authentication on the device from any browser or smartphone.



Enter code

Enter the code displayed on your app or device.

F9NZYVE3G

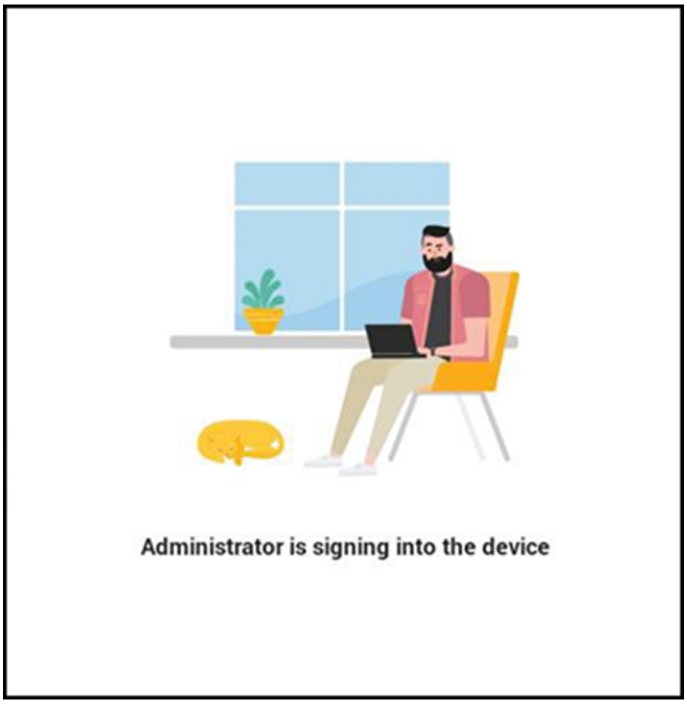


← hood@m365x021987.onmicrosoft.com

Enter password

••••••••••

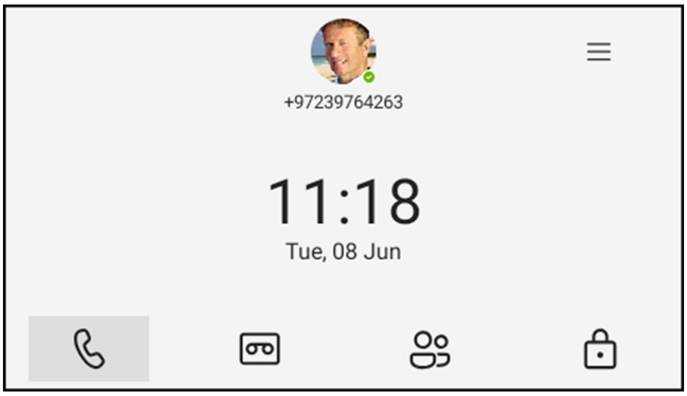
When the tenant admin is signing in from Teams Admin Center, the user interface on the device is blocked to prevent other actions on the phone.



Administrator is signing into the device

Getting Acquainted with the Phone Screen

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

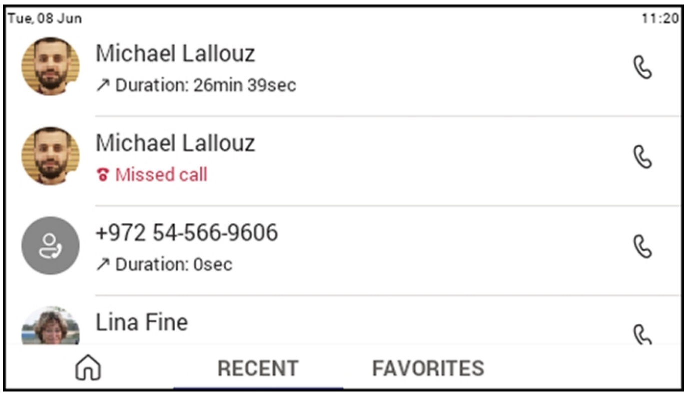


+97239764263

11:18

Tue, 08 Jun

The following figure shows the phone's Calls screen.



Tue, 08 Jun 11:20

Michael Lallouz
↗ Duration: 26min 39sec

Michael Lallouz
Missed call

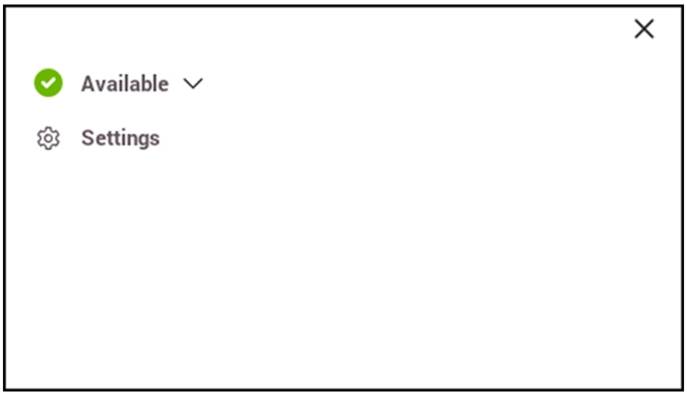
+972 54-566-9606
↗ Duration: 0sec

Lina Fine

The following table describes the phone's home screen.

Item	Description
Calls	Select the tab to open the Calls screen. The screen shown in the figure preceding this table opens.
People	Select the tab to open the People, shown under Using the People Screen on page 52 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 52 opens.

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



Use this table as reference.

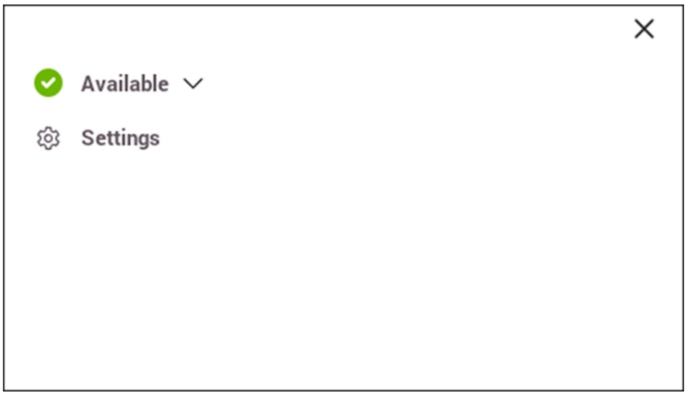
Item	Description
Presence status	See Changing Presence Status for more information.
Settings	See Configuring Teams Application Settings on page 49 for more information.

Setting Status

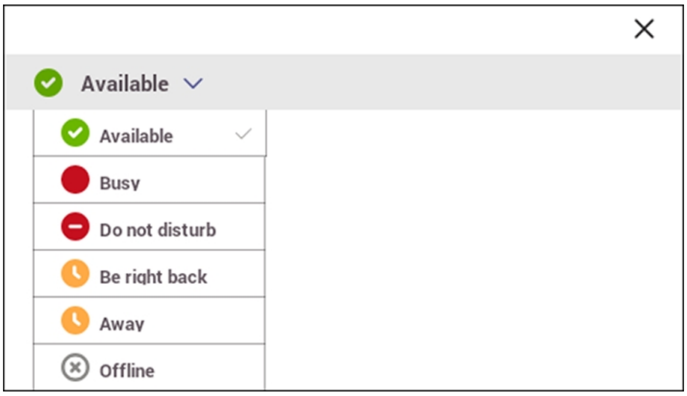
You can set a presence status such as 'Available' for others in the network to see.

➢ **To set presence status:**

1. In the home screen, select ☰.



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



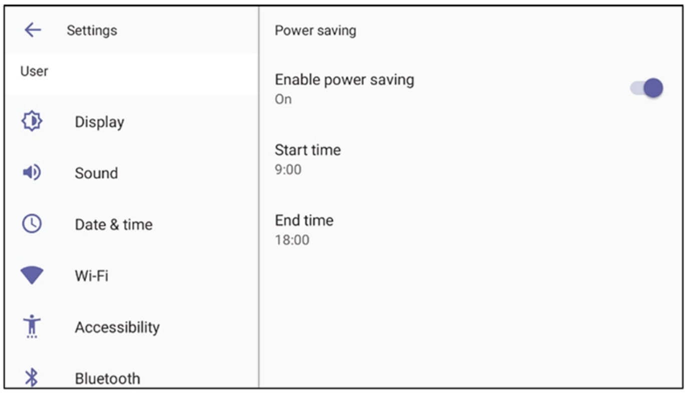
3. From the drop-down, select the status to set and then press the **OK** button.

Enabling Power Saving

This feature automatically activates power-saving mode during non-working hours. By default, during off hours, the phone's uppermost-right Message Waiting Indicator (MWI) / Presence LED is switched off and the LCD is dimmed. This conserves energy and minimizes light disturbance, providing a seamless and efficient user experience.

➢ **To enable this feature:**

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



Settings

User

Display

Sound

Date & time

Wi-Fi

Accessibility

Bluetooth

Power saving

Enable power saving
On

Start time
9:00

End time
18:00

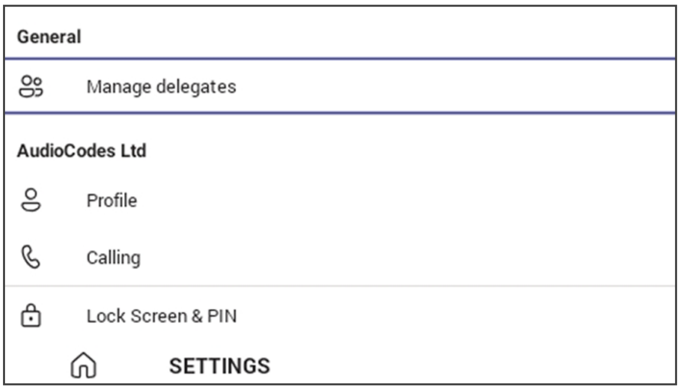
- By default, the feature is enabled.
- The feature is based on off work hours and sleep timeout.

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

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

Configuring Teams Application Settings

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



General

Manage delegates

AudioCodes Ltd

Profile

Calling

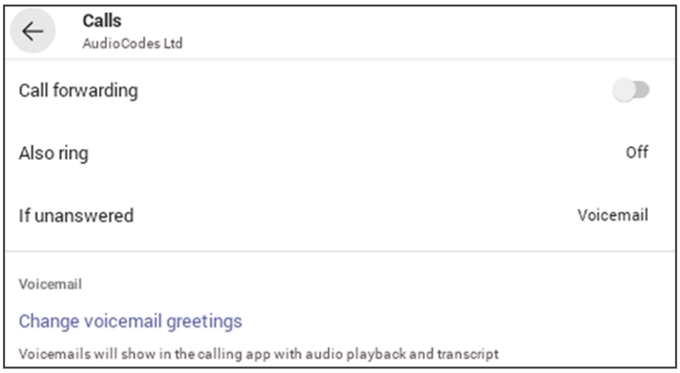
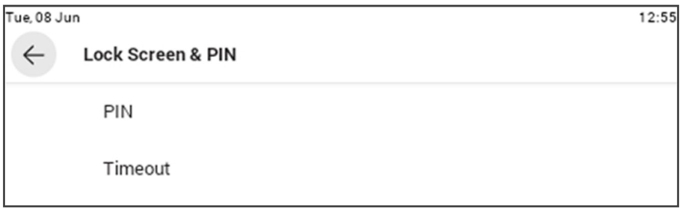
Lock Screen & PIN

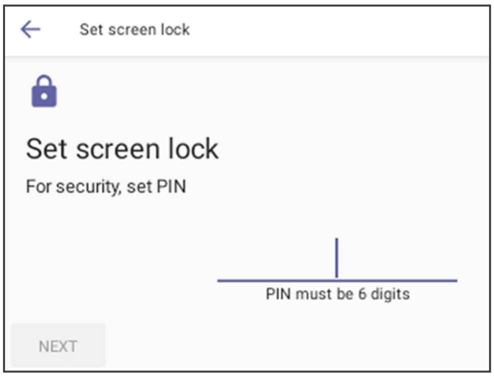
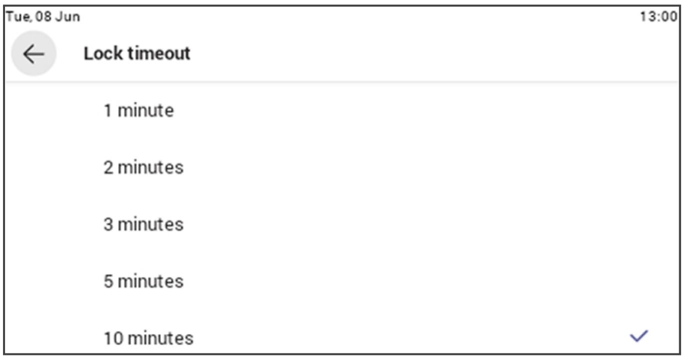
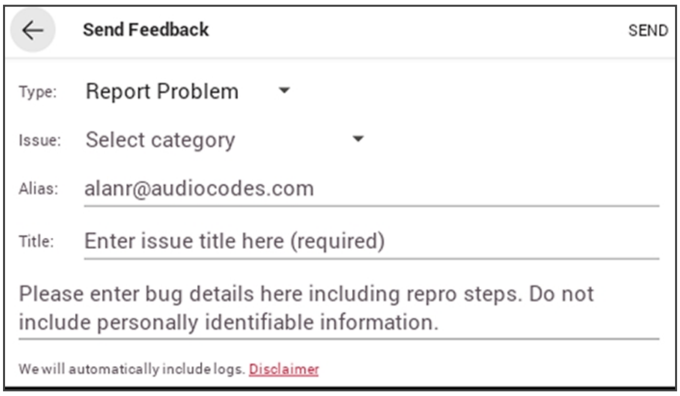
SETTINGS

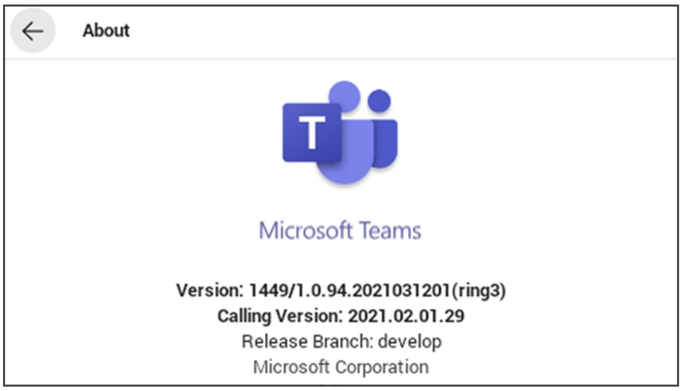
Use this table as reference:

Table 4-1: Idle Screen Description

Item	Description
Profile	Opens the user's email address and photo / avatar picture.
Calling	Opens the Calls screen.

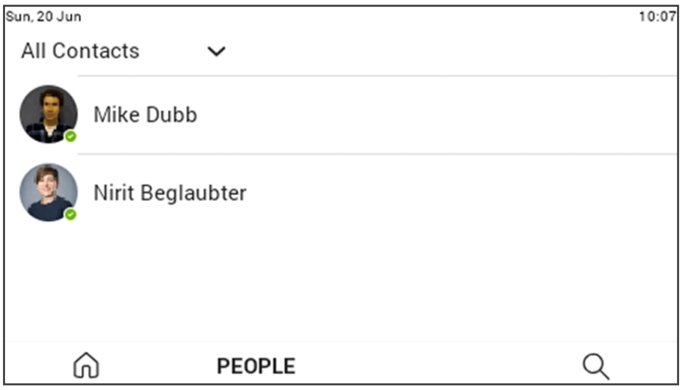
Item	Description
	 Calls AudioCodes Ltd Call forwarding Also ring Off If unanswered Voicemail Voicemail Change voicemail greetings Voicemails will show in the calling app with audio playback and transcript **Incoming Calls** - **Call forwarding**. Enables automatically redirecting an incoming call to 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.  Tue, 08 Jun 12:55 Lock Screen & PIN PIN Timeout Configure a lock option before attempting to lock the phone.

Item	Description
	 Set screen lock Set screen lock For security, set PIN PIN must be 6 digits NEXT  Tue, 08 Jun 13:00 Lock timeout 1 minute 2 minutes 3 minutes 5 minutes 10 minutes ✓ If a lock option isn't configured, the lock action won't work. To unlock a locked phone, see Unlock on page 36.
Report an issue	Microsoft Teams application's 'Report an issue' option opens the Send Feedback screen.  Send Feedback SEND Type: Report Problem Issue: Select category Alias: alanr@audiocodes.com Title: Enter issue title here (required) Please enter bug details here including repro steps. Do not include personally identifiable information. We will automatically include logs. Disclaimer 'Report an issue' can alternatively be triggered by simultaneously pressing the Vol up + Vol down keys. This can help the user to report an issue even if the application is stuck and does not allow the user to report the issue via the Application > Settings tab.
About	Opens the About screen.

Item	Description
	 About Microsoft Teams Version: 1449/1.0.94.2021031201(ring3) Calling Version: 2021.02.01.29 Release Branch: develop Microsoft Corporation
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 54 for detailed information.
Device Settings	Opens the [Device] Settings screen. See Configuring Device Settings on page 19 for detailed information.

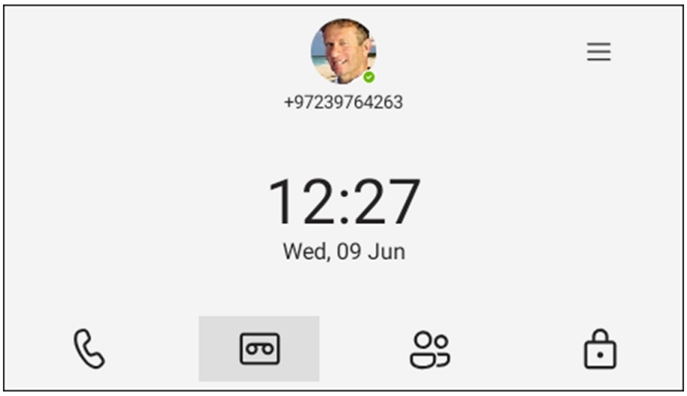
Using the People Screen

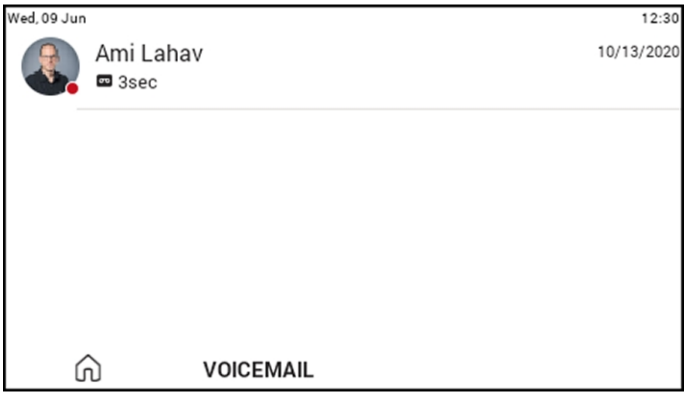
The People screen allows users to easily connect and collaborate with teammates, colleagues, friends and family. Through the screen, users can see all their contacts and create and manage contact groups to organize their contacts. The screen provides a simple user experience and aligns with the contacts 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.

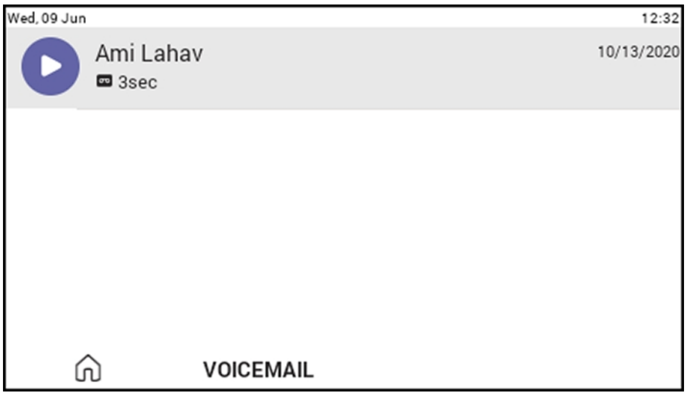


Accessing Voicemail

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.

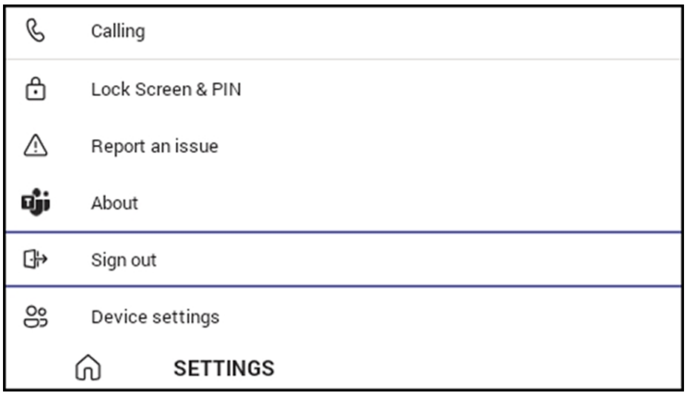
The feature enables the user to move away from their PC while seamlessly staying connected. The phone recognizes the user is in a call on another device and prompts them to transfer or add, letting them start their call from elsewhere and transfer to their desk phone.

Signing Out

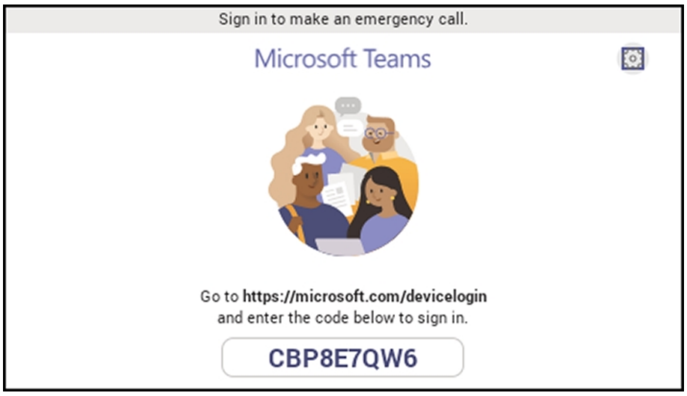
You can optionally sign out of the phone application and sign in as another user.

➢ 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.



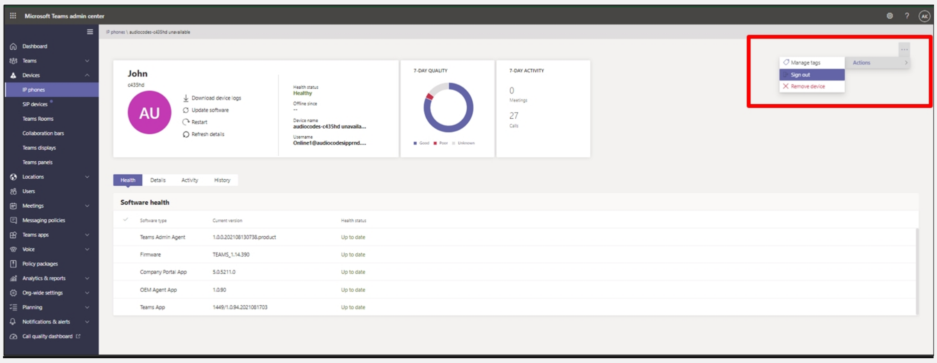
Sign in to make an emergency call.

Microsoft Teams

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

CBP8E7QW6

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



John
c435hd

Health status
Healthy

Offline since
--

Device name
audiocodes-c435hd unavaila...

Username
Online1@audiocodesipprnd....

0
Meetings

27
Calls

Software health

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

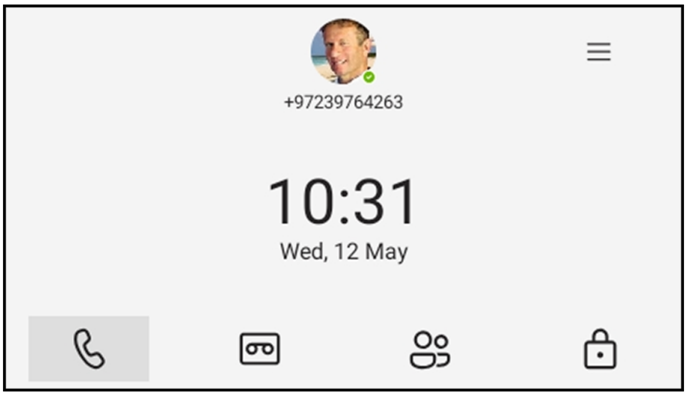
5 Performing Teams Call Operations

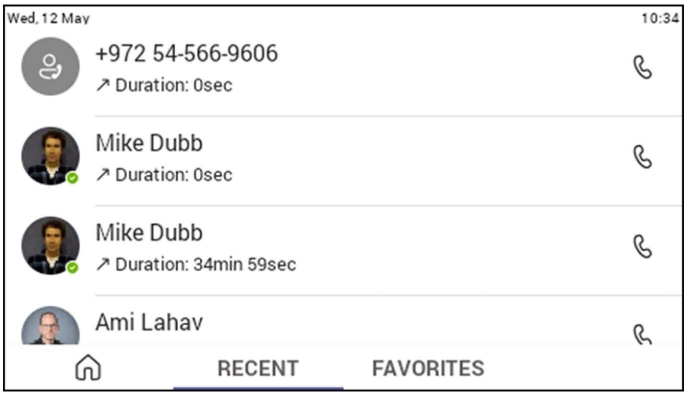
The following documentation shows how to perform basic operations with the phone.

Making a Call

Calls can be made in multiple ways, 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.





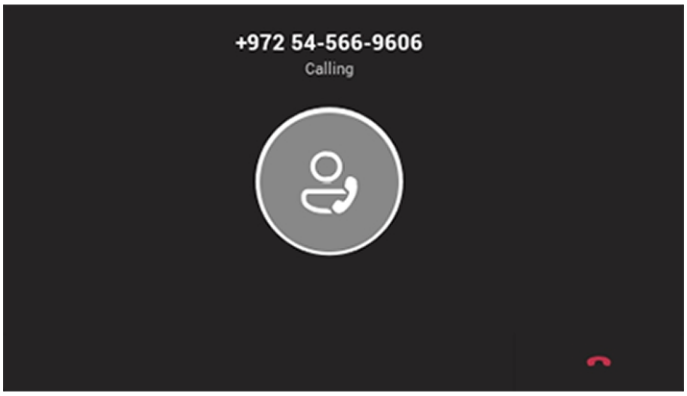
+972 54-566-9606
↗ Duration: 0sec

Mike Dubb
↗ Duration: 0sec

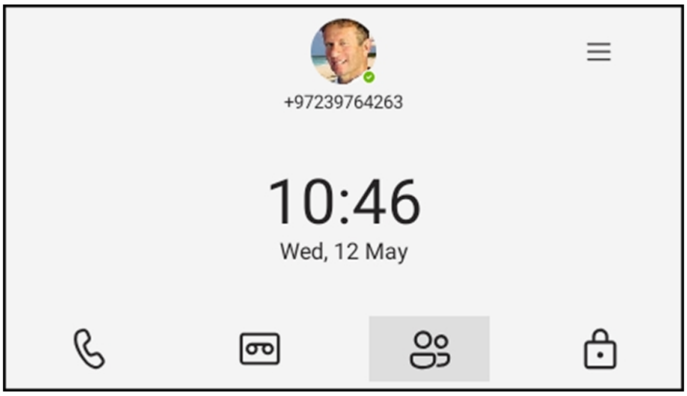
Mike Dubb
↗ Duration: 34min 59sec

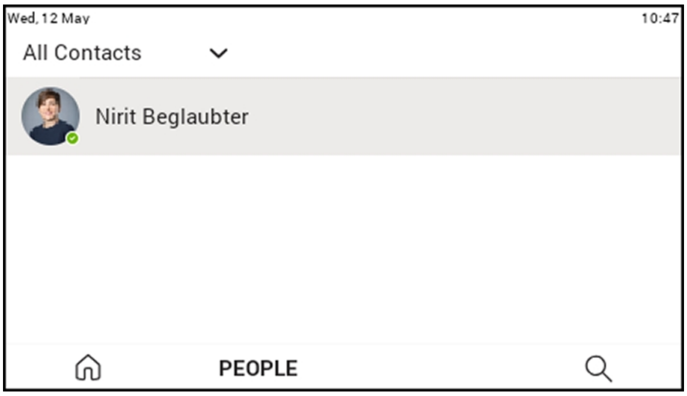
Ami Lahav

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

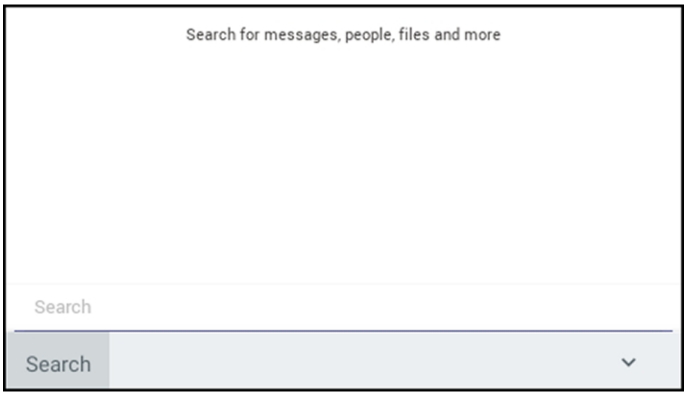


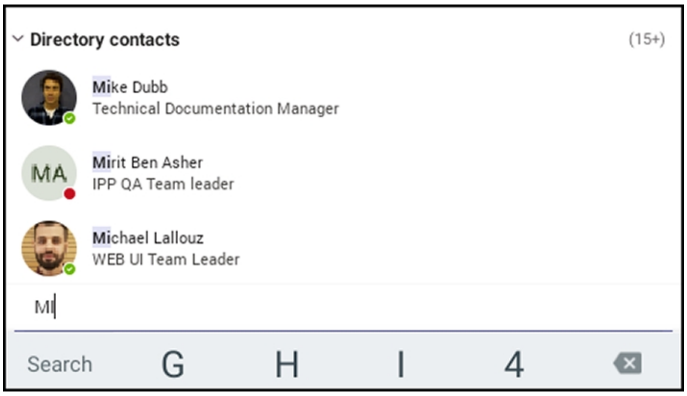
You can alternatively make a call using a speed dial from the People screen or from the 'Search people' feature in the People screen.





Nirit Beglaubter





Mike Dubb
Technical Documentation Manager

Mirit Ben Asher
IPP QA Team leader

Michael Lallouz
WEB UI Team Leader

Dialing a Missed Call

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

➢ **To dial a missed call:**

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

Select to Dial

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

Transferring a Call

See here for a video clip demonstrating how to use the call transfer feature while checking with the intended recipient that they want to take the call. The principle is similar across AudioCodes Teams phones.

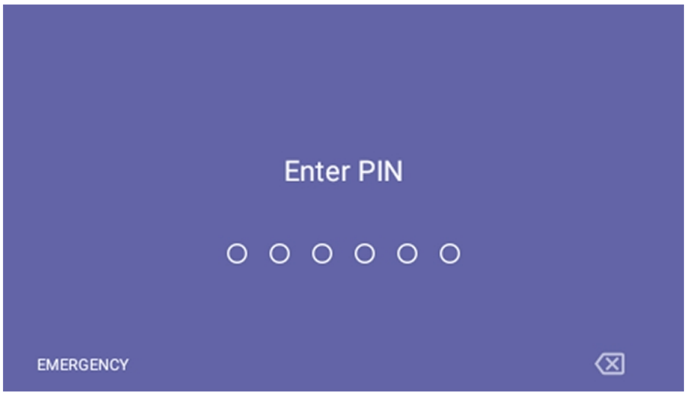
See here for a video clip demonstrating how to immediately transfer a call without verifying with the intended recipient that they want to take the call. The principle is similar across AudioCodes Teams phones.

➢ **To transfer a call received for another person:**

1. When the incoming call arrives, choose whether to transfer it immediately or not; you can transfer it directly right away, or you can decide to consult the intended recipient of the call to verify that they want to receive it.
2. To consult the intended recipient, select **Consult first** and search for the contact you want to transfer the call to. While you consult with the intended recipient about whether they want to take the incoming call, the caller will hear hold music and will not be a party to your discussion.
3. If the recipient decides to take the call, click the phone icon on the top-right of the screen and then confirm the transfer; the call is then transferred smoothly to the intended recipient.

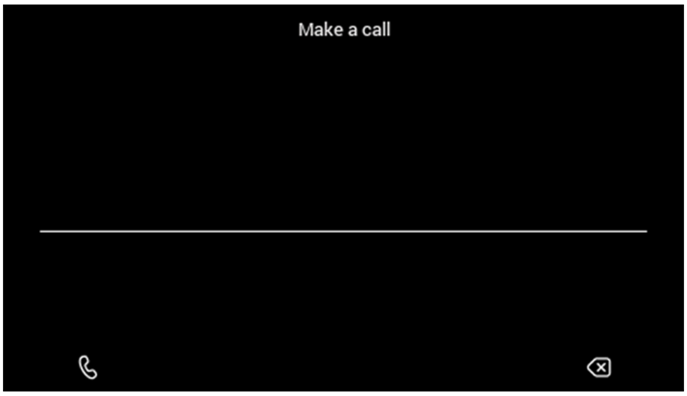
Making an Emergency Call

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



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

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



Answering Calls

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

➢ **To answer:**

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

Ending an Established Call

You can end an established call in a few ways.

➢ **To end an established call:**

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

Managing Calls

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

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

➢ To manage calls:

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

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

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

Paging to a Group of Phones (Multicast)

AudioCodes Android-based phones support multicast paging (including barge-in). The feature allows a call to be paged to a group of phones to notify a team about (for example) the time and place at which a meeting will commence. The paging call is multicast via a designated group IP address, in real time, on all phones in the group.

Barge-in enables paging to interrupt (barge in on) phone conversations that are in progress. The feature is configured in the phone’s cfg configuration file. Default: Disabled. When enabled, a paging call overrides an ongoing regular call/meeting due to emergency. When disabled, those who are in regular calls when a paging call comes in are prompted in the phone screen to accept or reject the paging call. If it's accepted, the regular call is put on hold and the paging is heard.

Related paging parameters in the cfg configuration file are:

/voip/services/group_paging/enabled

/voip/services/group_paging/codec

/voip/services/group_paging/group/*/activated

/voip/services/group_paging/group/*/multicast_addr

/voip/services/group_paging/group/*/port

/voip/services/group_paging/allow_barge_in/enabled

- The values of these parameters can be changed on the fly.
- Paging behavior is immediately affected.

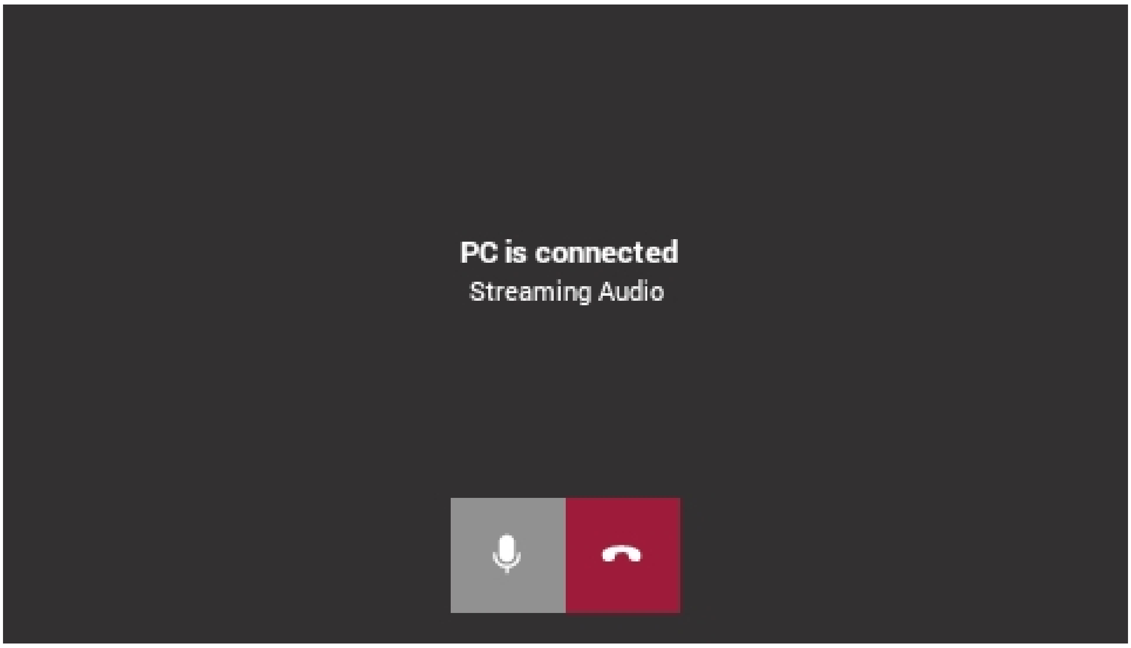
Use the following table as reference.

Parameter	Description
voip/services/group_paging/allow_barge_in/enabled=0	Allows | disallows the barge-in feature. - 0 = disabled - 1 = enabled
voip/services/group_paging/codec=PCMU	Defines the codec. Three available options: - PCMU (default) - PCMA - G722
voip/services/group_paging/enabled=0	Enables | disables the group paging feature. - 0 = disabled - 1 = enabled
voip/services/group_paging/group/0-4/activated=0	Activates| deactivates a group. - 0 = deactivated - 1 = activated Five groups labeled 0-4 are available.
voip/services/group_paging/group/0-4/multicast_addr=224.0.1.0	Defines the paging group's multicast IP address. Must be in the range: 224.0.0.0 - 239.255.255.255 Default: 224.0.1.0. **Important**: For phones to be in a group, all must be configured with the identical multicast address and port. The following three IP addresses (for example) denote three different paging groups: - 224.0.1.1:8888 - 224.0.1.1:2222 - 233.2.2.2:8888
voip/services/group_paging/group/0-4/port=8888	Defines the port through which paging is received. Must be in range: 1-65535 Default: 8888 **Important**: For phones to be in a group, all must be configured with the identical multicast address and

Parameter	Description
	port. Port 9998 and 9999 should not be used as they are used by the application.

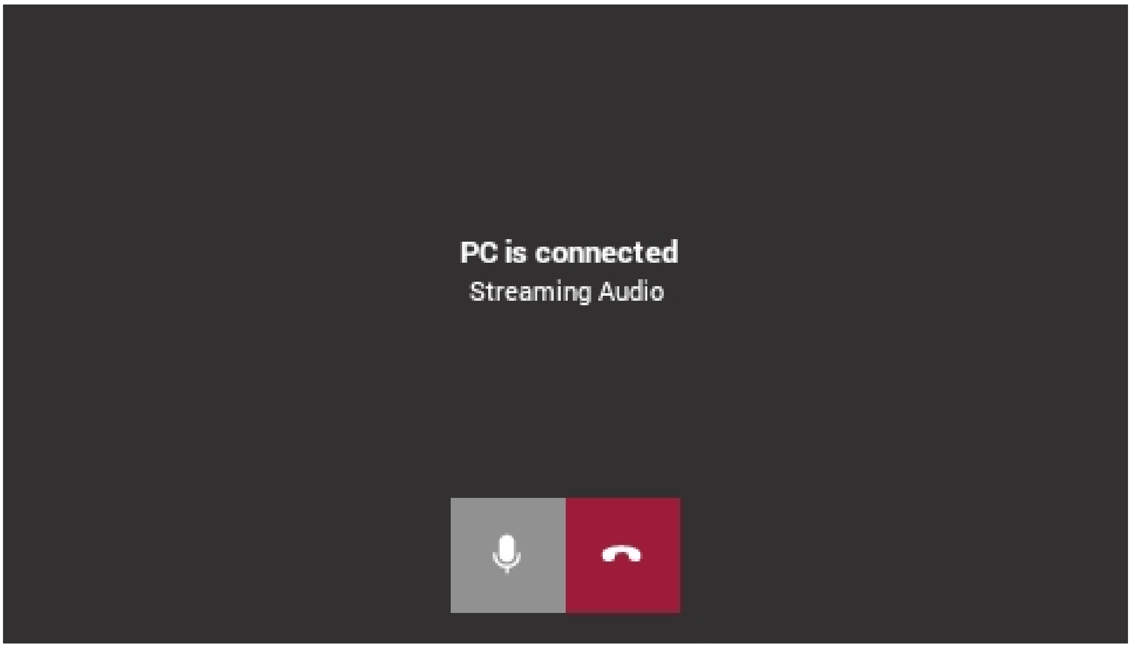
- AudioCodes Android-based phones currently support incoming paging calls (listening).
- Outgoing paging calls (broadcasting) will be supported in the future.

- When an incoming call is received on a phone that is in idle, the phone *immediately automatically* answers it, irrespective of whether barge-in is enabled or not:

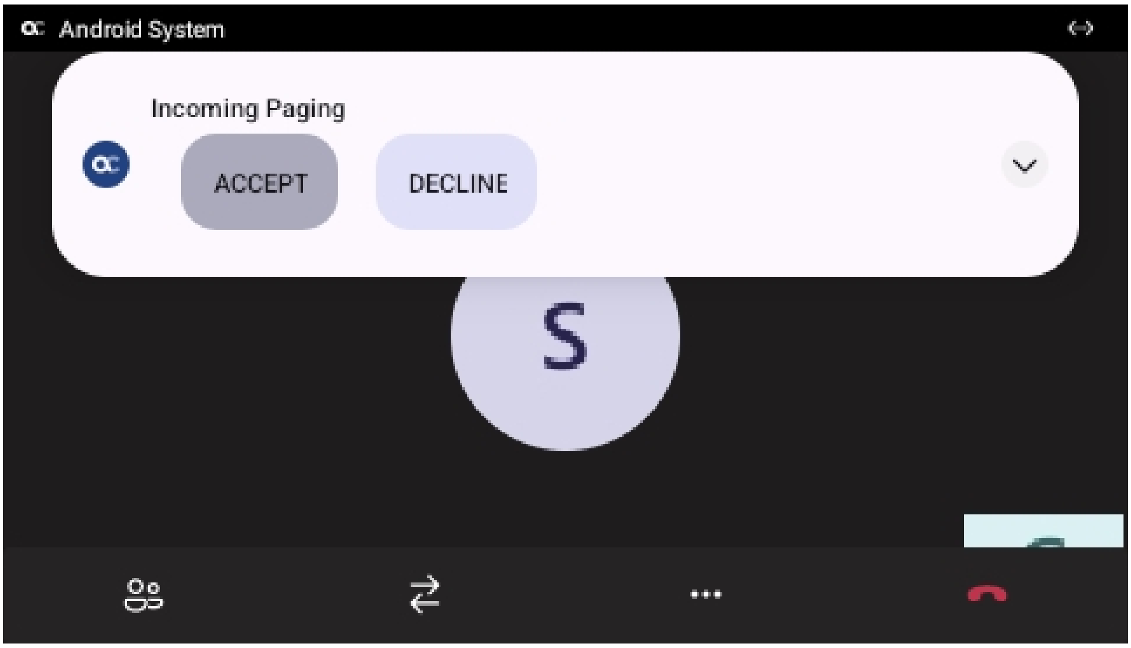


PC is connected
Streaming Audio

- When the phone is in a Teams call/meeting (active or on-hold):
  - If barge-in is enabled, i.e., if the new cfg configuration file parameter voip/services/group_paging/allow_barge_in/enabled=1, then the phone will *automatically immediately* display the **Audio announcement in progress** screen with an option to END the announcement.



- If barge-in is *disabled*, i.e., if the new cfg configuration file parameter voip/services/group_paging/allow_barge_in/enabled=0, then the phone will display the **Incoming audio announcement** screen with an option to ACCEPT or DECLINE it:



Transferring a Call to Frequent Contacts

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

Transferring a Call to Work Voicemail

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

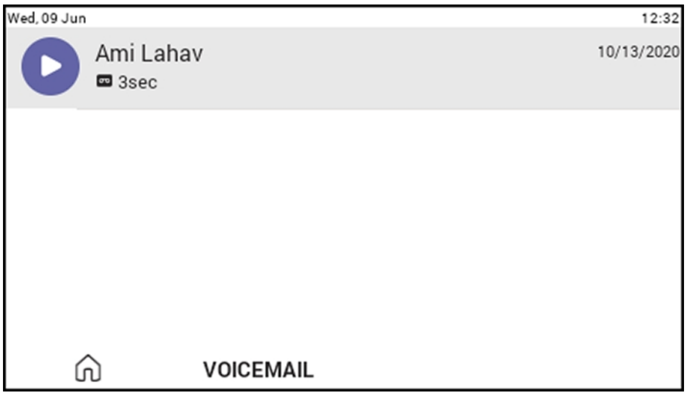
Viewing and Playing Voicemail Messages

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

See here for a video clip demonstrating how to view and play voicemail messages.

➢ To view a list of your voicemail messages:

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



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

   For more information, see here.

Rejecting an Incoming Call, Sending it Directly to Voicemail

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

➢ To send an incoming call directly to voicemail:

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

Adjusting Volume

The phone allows

- Adjusting Ring Volume on the next page
- Adjusting Tones Volume 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.

Playing Incoming Call Ringing through USB Headset

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

Click here to view a video clip demonstrating how to connect a USB headset to the phone. The principle is similar across AudioCodes Teams phones.

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

- Configure the following parameter:

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

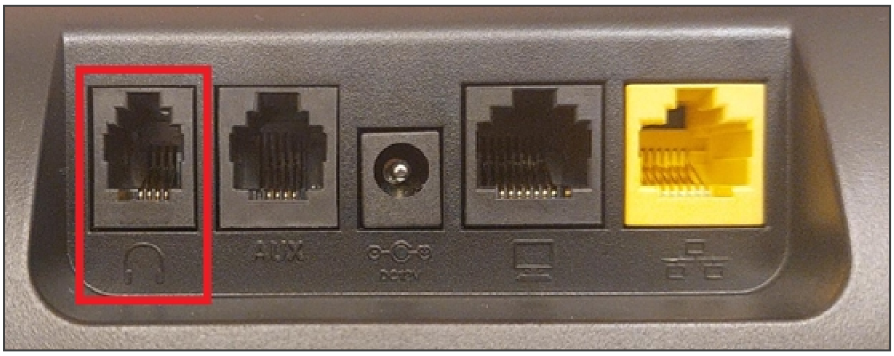
  - **BOTH**: Incoming calls play through both the USB headset and the phone’s speaker.
  - **BUILTIN_SPEAKER**: Incoming calls play through the phone’s speaker.
  - **TYPE_USB**: Incoming calls play through the USB headset.

Playing Incoming Call Ringing through RJ9 Headset

> ⚠ Only the C435HD phone is currently supported.

Support has been added for ringing via an RJ9 headset on the C435HD phone.

The figure below shows the RJ9 headset port:



Admins will use parameter audio/stream/ringer/0/audio_device to specify which device will ring when a call comes in.

Two new configuration values have been added:

```
TYPE_HEADSET (regular headset)
TYPE_RJ9_HEADSET
```

The parameter can be configured via the Device Manager as well as via SSH command. The parameter is also available in the template which can be applied to multiple phones via the Device Manager.

6 Performing Administrator-Related Operations

Network administrators can:

Update phone firmware manually (see Updating Phone Firmware Manually on page 74

Manually perform recovery operations (see Manually Performing Recovery Operations on page 81

Remove devices from Intune management (see Removing Devices from Intune admin center on page 83

Update Microsoft Teams devices remotely (see Updating Microsoft Teams Devices Remotely on page 86

Manage phones with the Device Manager (see Managing Phones with the Device Manager on page 88

Setting up Automatic Provisioning

Phones can be directed to a provisioning server using DHCP Option 160 or AudioCodes' HTTPS Redirect Server, to automatically load configuration (cfg) and firmware (img) files.

After the phone is powered up and network connectivity established, it automatically requests provisioning information; if it doesn't get via DHCP Option 160 provisioning method, it sends an HTTPS Request to the Redirect Server which responds with an HTTPS Redirect Response containing the URL of the provisioning server where the firmware and configuration files are located. When the phone successfully connects to the provisioning server's URL, an Automatic Update mechanism begins.

➢ **To set up DHCP Option 160, use this syntax:**

- <protocol>://<server IP address or host name>/<firmware file name>;<configuration file name>
- <protocol>://<server IP address or host name>
- <protocol>://<server IP address or host name>/<firmware file name>
- <protocol>://<server IP address or host name>/;<configuration file name>

Where <protocol> can be "ftp", "tftp", "http" or "https"

➢ **To set up AudioCodes' HTTPS Redirect Server, use this syntax:**

- <protocol>://<server IP address or host name>
- <protocol>://<server IP address or host name>/<firmware file name>
- <protocol>://<server IP address or host name>/<firmware file name>;<configuration file name>
- <protocol>://<server IP address or host name>/;<configuration file name>

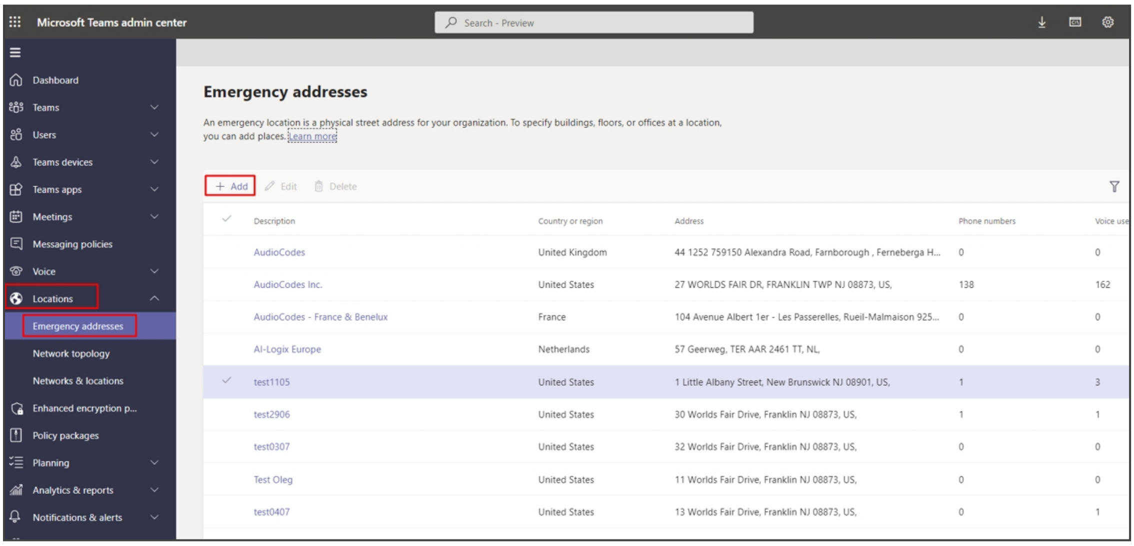
The Redirect Server's default URL is:
provisioning/redirect_server_url=https://redirect.audiocodes.com
It can be reconfigured if required.

Setting up an E911 Emergency Location using TAC

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

➢ To set up an E911 emergency location:

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

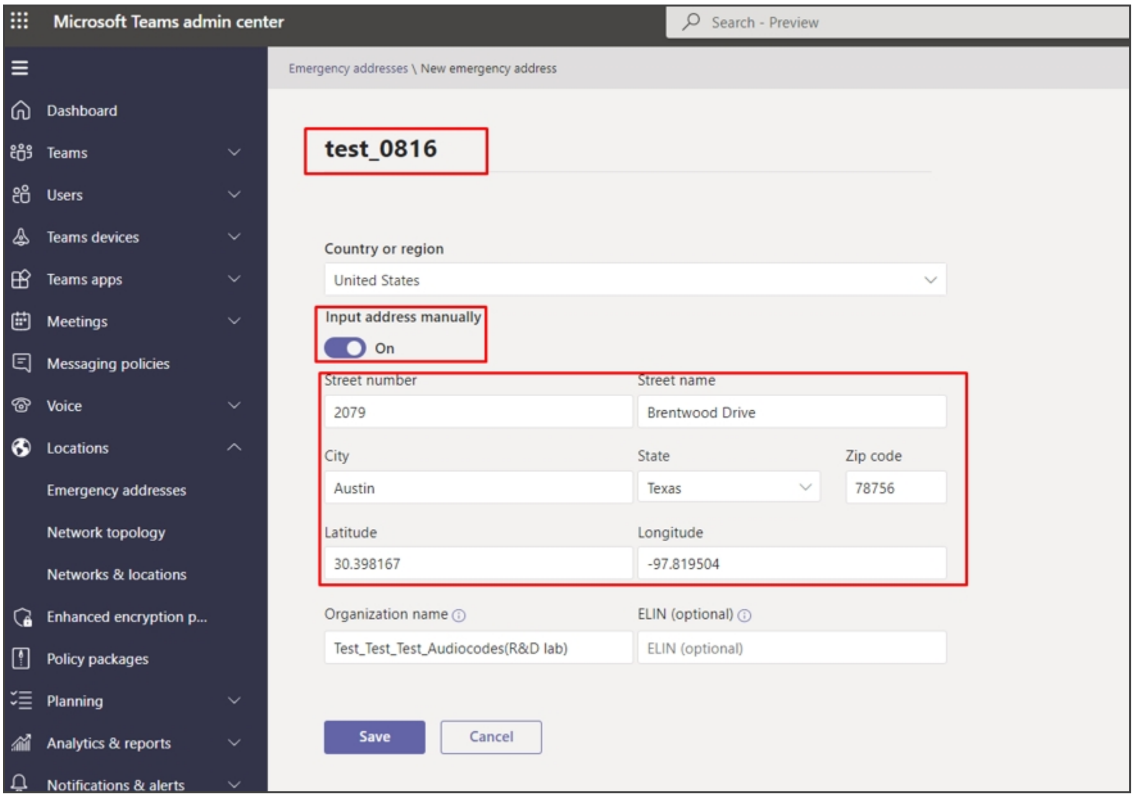


Emergency addresses

An emergency location is a physical street address for your organization. To specify buildings, floors, or offices at a location, you can add places. Learn more

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

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



Emergency addresses \ New emergency address

test_0816

Country or region: United States

Input address manually: On

Street number: 2079

Street name: Brentwood Drive

City: Austin

State: Texas

Zip code: 78756

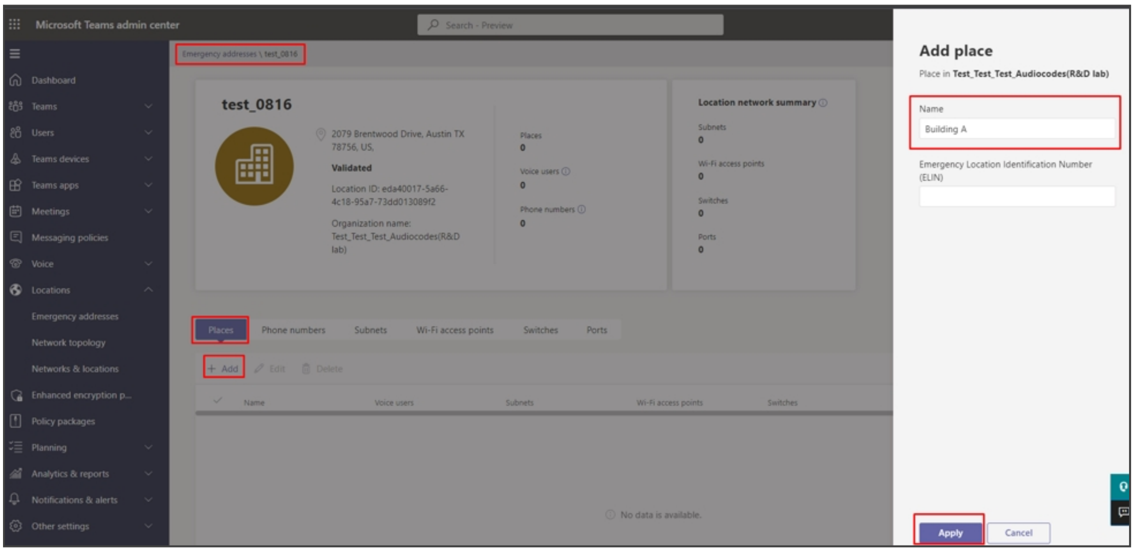
Latitude: 30.398167

Longitude: -97.819504

Organization name: Test_Test_Test_Audiocodes(R&D lab)

ELIN (optional): ELIN (optional)

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



Emergency addresses \ test_0816

test_0816

2079 Brentwood Drive, Austin TX 78756, US,

Validated

Location ID: eda40017-5a66-4c18-95a7-73dd013089f2

Organization name: Test_Test_Test_Audiocodes(R&D lab)

Places 0

Voice users 0

Phone numbers 0

Location network summary

Subnets 0

Wi-Fi access points 0

Switches 0

Ports 0

Add place

Place in **Test_Test_Test_Audiocodes(R&D lab)**

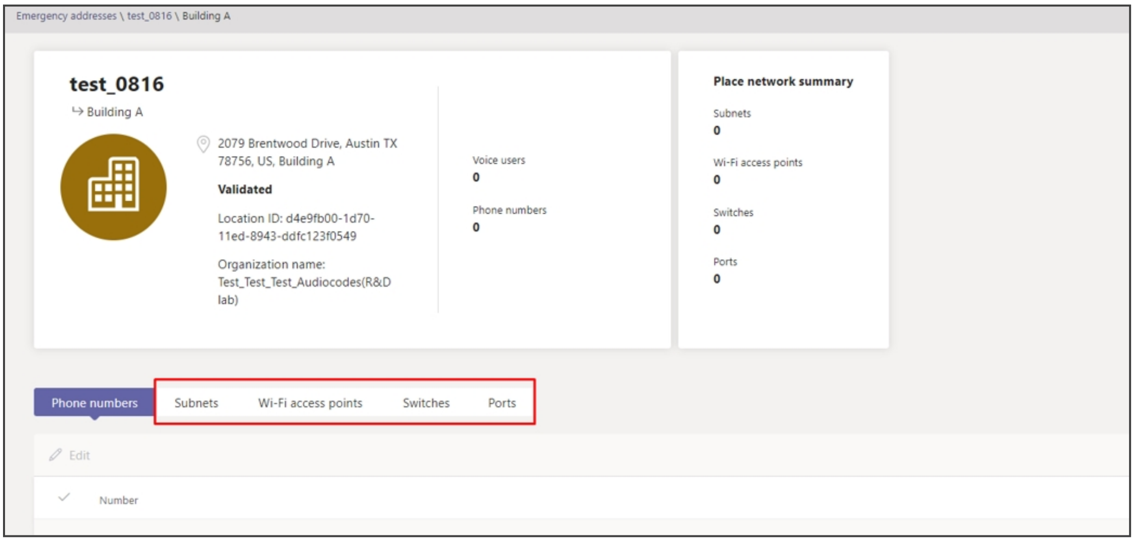
Name: Building A

Emergency Location Identification Number (ELIN)

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

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

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



test_0816
↳ Building A

2079 Brentwood Drive, Austin TX 78756, US, Building A

Validated

Location ID: d4e9fb00-1d70-11ed-8943-ddfc123f0549

Organization name: Test_Test_Test_Audiocodes(R&D lab)

Voice users
0

Phone numbers
0

Place network summary

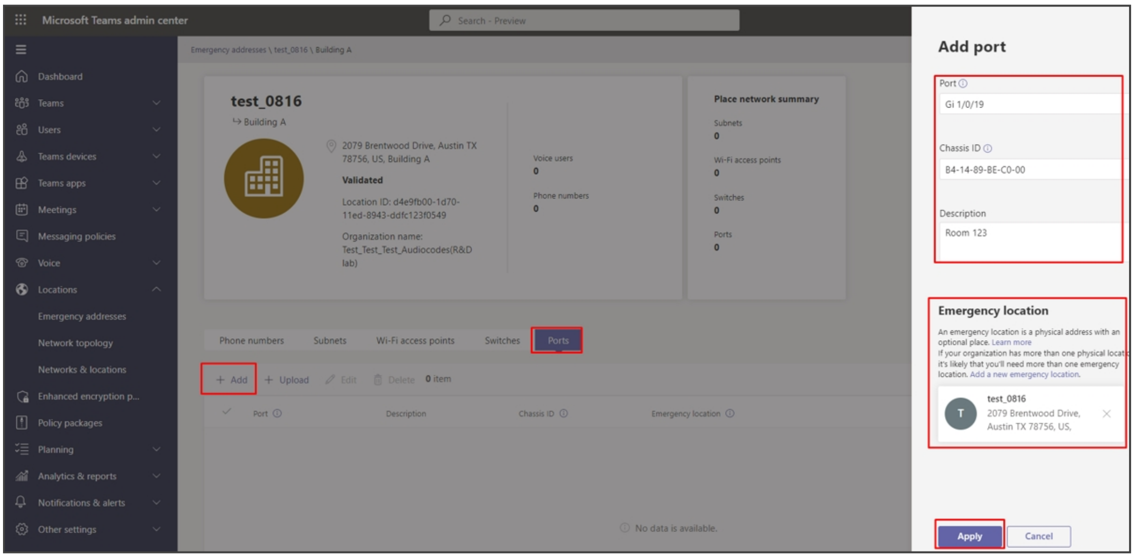
Subnets
0

Wi-Fi access points
0

Switches
0

Ports
0

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



test_0816
↳ Building A

2079 Brentwood Drive, Austin TX 78756, US, Building A

Validated

Location ID: d4e9fb00-1d70-11ed-8943-ddfc123f0549

Organization name: Test_Test_Test_Audiocodes(R&D lab)

Voice users
0

Phone numbers
0

Place network summary

Subnets
0

Wi-Fi access points
0

Switches
0

Ports
0

Add port

Port: Gi 1/0/19

Chassis ID: B4-14-89-BE-C0-00

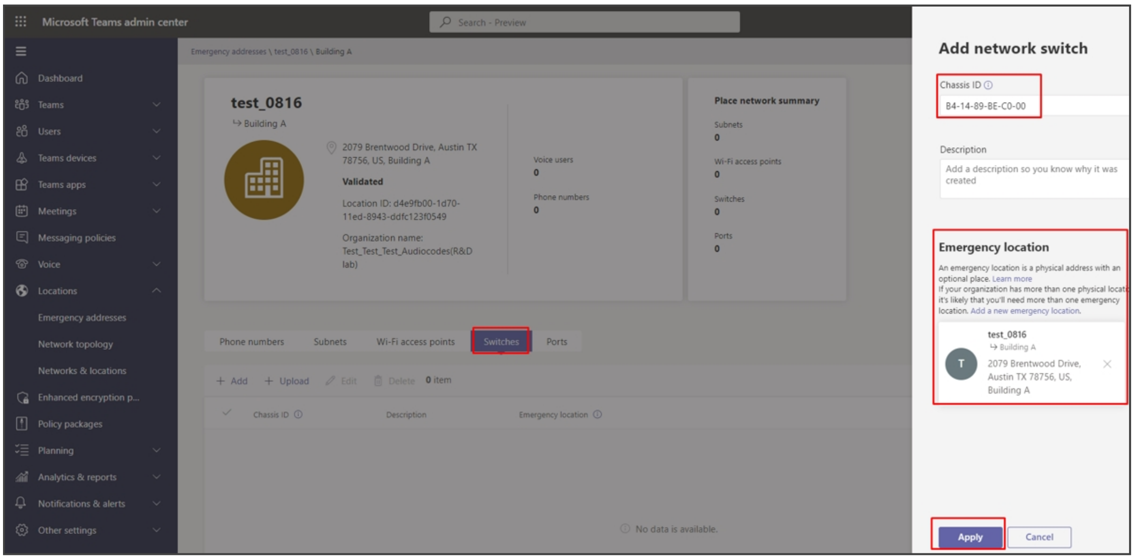
Description: Room 123

Emergency location

An emergency location is a physical address with an optional place. Learn more
If your organization has more than one physical locat it's likely that you'll need more than one emergency location. Add a new emergency location.

test_0816
2079 Brentwood Drive, Austin TX 78756, US,

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



test_0816
↳ Building A

2079 Brentwood Drive, Austin TX 78756, US, Building A

Validated

Location ID: d4e9fb00-1d70-11ed-8943-ddfc123f0549

Organization name: Test_Test_Test_Audiocodes(R&D lab)

Voice users 0

Phone numbers 0

Place network summary

Subnets 0

Wi-Fi access points 0

Switches 0

Ports 0

Add network switch

Chassis ID: B4-14-89-BE-C0-00

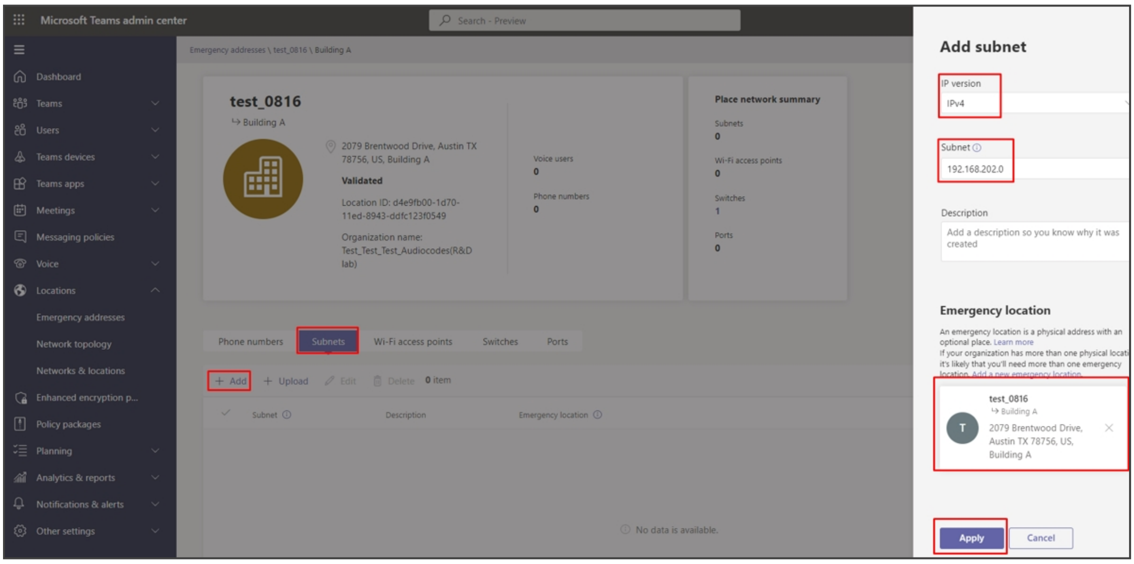
Description: Add a description so you know why it was created

Emergency location

An emergency location is a physical address with an optional place. Learn more
If your organization has more than one physical locat... it's likely that you'll need more than one emergency location. Add a new emergency location.

test_0816
↳ Building A
2079 Brentwood Drive, Austin TX 78756, US, Building A

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



test_0816
↳ Building A

2079 Brentwood Drive, Austin TX 78756, US, Building A

Validated

Location ID: d4e9fb00-1d70-11ed-8943-ddfc123f0549

Organization name: Test_Test_Test_Audiocodes(R&D lab)

Voice users 0

Phone numbers 0

Place network summary

Subnets 0

Wi-Fi access points 0

Switches 1

Ports 0

Add subnet

IP version: IPv4

Subnet: 192.168.202.0

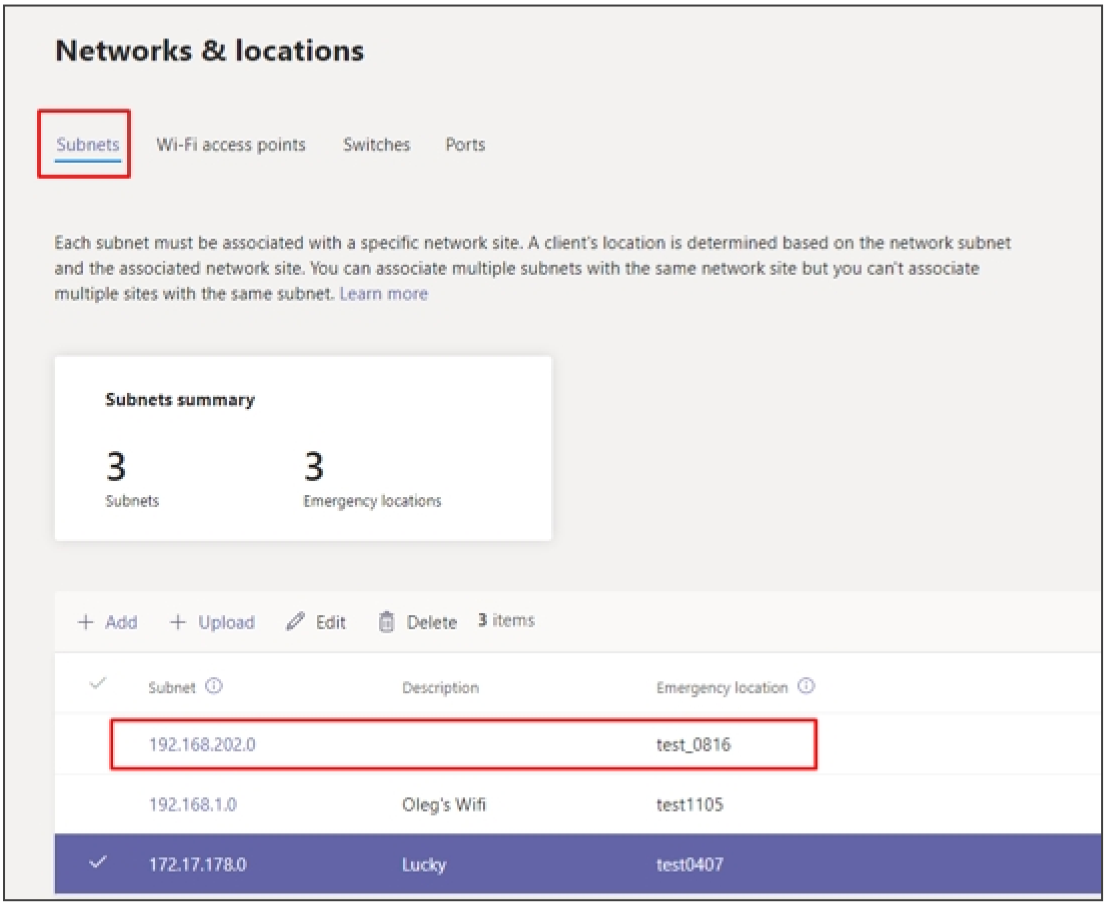
Description: Add a description so you know why it was created

Emergency location

An emergency location is a physical address with an optional place. Learn more
If your organization has more than one physical locati... it's likely that you'll need more than one emergency location. Add a new emergency location.

test_0816
↳ Building A
2079 Brentwood Drive, Austin TX 78756, US, Building A

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



Networks & locations

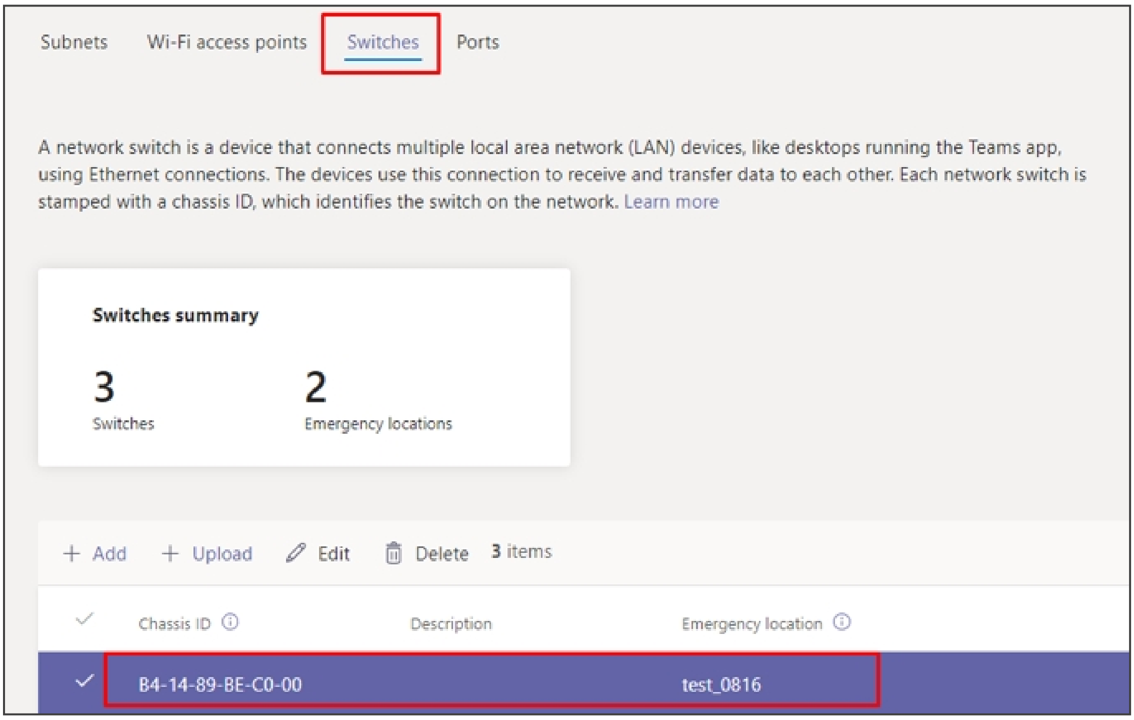
Each subnet must be associated with a specific network site. A client's location is determined based on the network subnet and the associated network site. You can associate multiple subnets with the same network site but you can't associate multiple sites with the same subnet. Learn more

Subnets summary

3 Subnets

3 Emergency locations

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



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

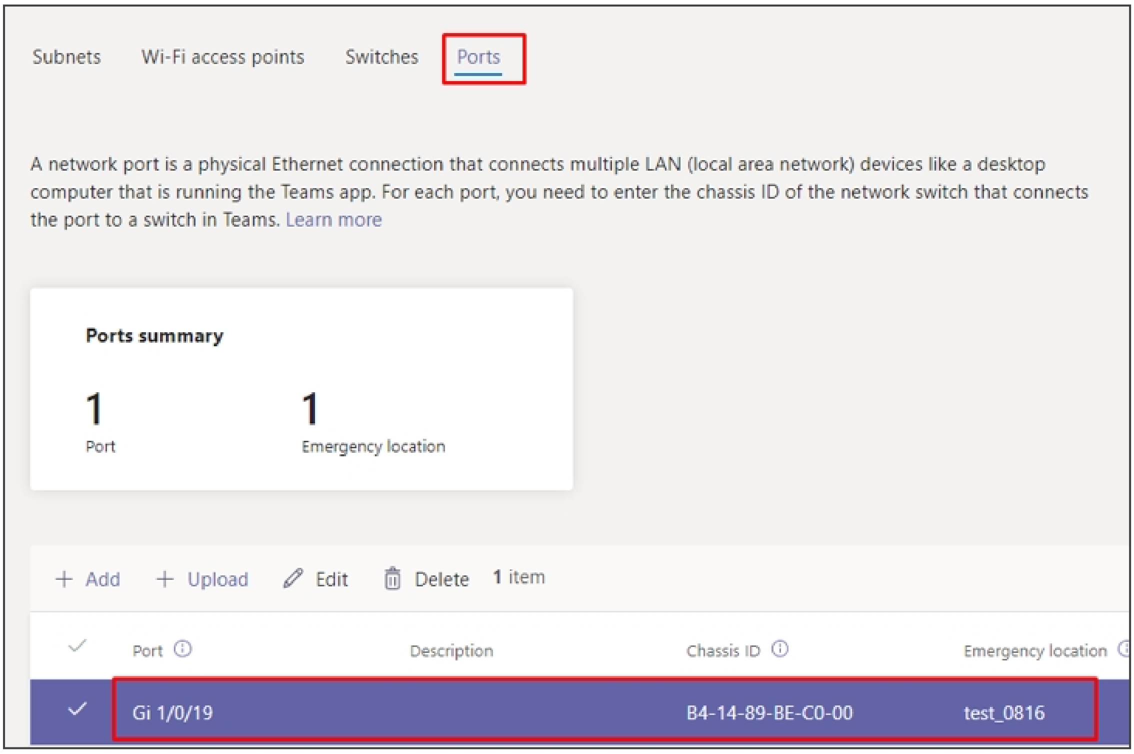
Switches summary

3 Switches

2 Emergency locations

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

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



Subnets Wi-Fi access points Switches Ports

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

Ports summary

1 Port

1 Emergency location

+ Add + Upload Edit Delete 1 item

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

After a location has been defined, make sure that:

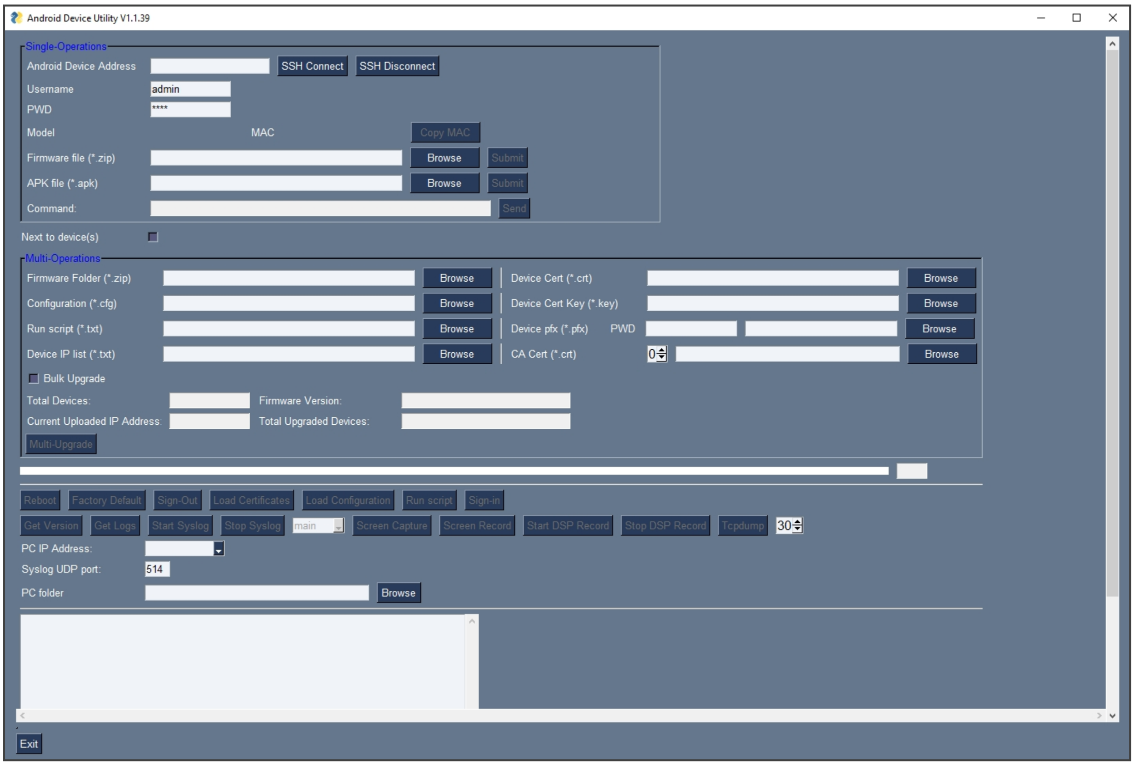
- AudioCodes' phone runs the latest firmware released.
- AudioCodes' phone runs the Teams app issued June 2022 and later (U3-A and higher).
- E911 information is displayed on the phone screen 30-120 minutes after the location is set (time estimated under laboratory conditions).
- To trigger information to be shown before that time period, dial a 933-test call and check if the location has been accepted, displayed and vocalized by the announcer.

Updating Phone Firmware Manually

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

➢ To manually update a phone's firmware:

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



Android Device Utility V1.1.39

Single-Operations

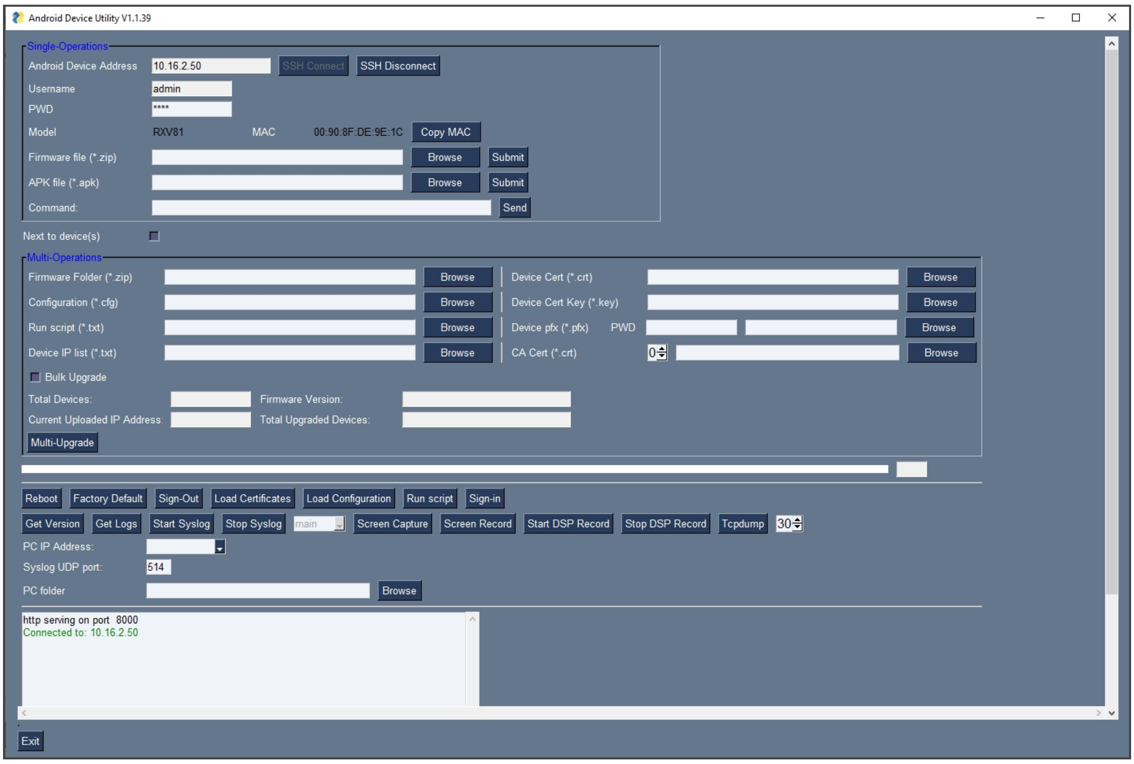
Username: admin

PWD: ****

Syslog UDP port: 514

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

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



Android Device Utility V1.1.39

Single-Operations

Android Device Address: 10.16.2.50

Username: admin

PWD: ****

Model: RXV81

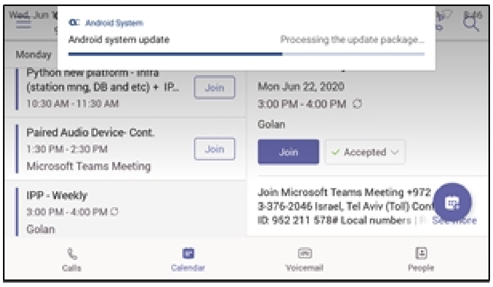
MAC: 00:90:8F:DE:9E:1C

Syslog UDP port: 514

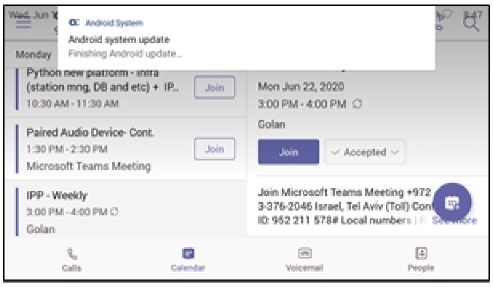
```
http serving on port  8000
Connected to: 10.16.2.50
```

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

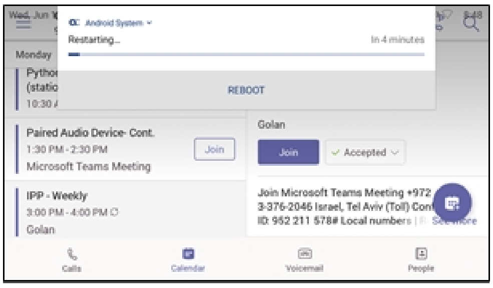
5. Click the **Submit** button; a firmware upgrade process starts; the phone is automatically rebooted; a notification pops up when the process finishes. The phone notifies you that it's being updated and rebooted.



Android System
Android system update
Processing the update package...



Android System
Android system update
Finishing Android update...



Android System
Restarting... In 4 minutes
REBOOT

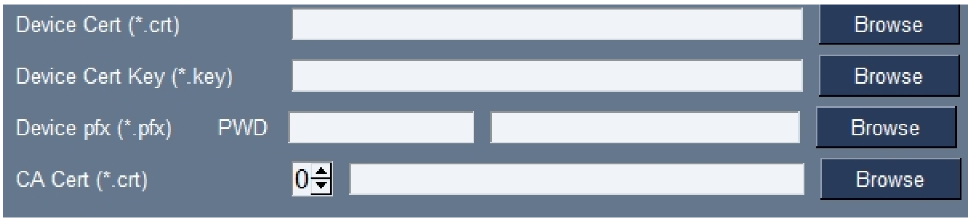
The above is also displayed when the phone is upgraded remotely from Microsoft Admin Portal or from AudioCodes' Device Manager.

Loading Certificates to Phones

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

Certificates can be downloaded using:

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



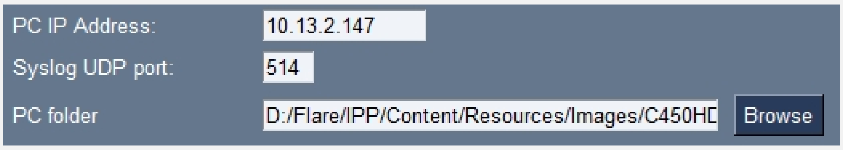
Device Cert (*.crt) Browse

Device Cert Key (*.key) Browse

Device pfx (*.pfx) PWD Browse

CA Cert (*.crt) 0 Browse

- The extension of the device certificate file must be **.crt**
- The extension of the private key must be **.key**
- Device certificates can be provisioned in **.pfx** file format (combining **.crt** and **.key**). The following parameter values can be configured in the devices' Configuration File:
  - ✓ /security/device_certificate_url = <url>/certificate.pfx
  - ✓ /security/device_private_key_url = NULL
  - ✓ security/device_certificate/password=<pfx password>
- The extension of the CA certificate file must be .crt. It's possible to load up to 5 CA certificates to the phone using the placement selector (0-4) (Default: 0).
- The IP address of the PC on which the certificate files are stored must be entered as shown here:



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

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

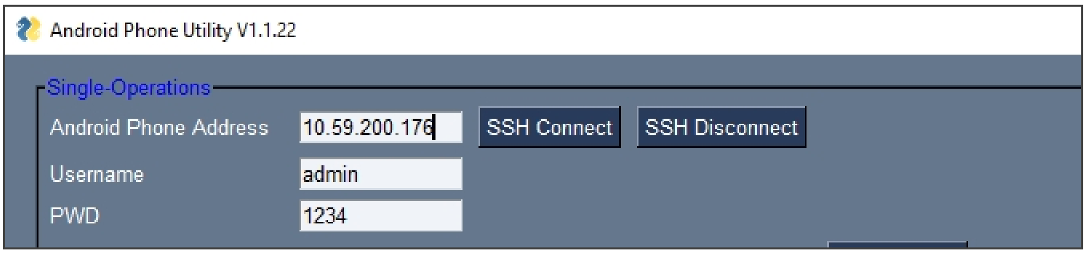
- The CA certificate (ca_cert) can also be loaded to devices using AudioCodes' Device Manager, in the 'Template' screen.
- Certificate loading is performed using HTTP. Prior to version 1.19, it was performed using SCP. The HTTP port is 8000. Make sure the port is not blocked by the organization's firewall.

AudioCodes Android Device Utility

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

➢ To load certificates to a single device:

1. In the Android Device Utility (see Android Device Utility on page 97 for detailed information about the application), enter the phone's IP address and click **SSH Connect** shown in the next figure.

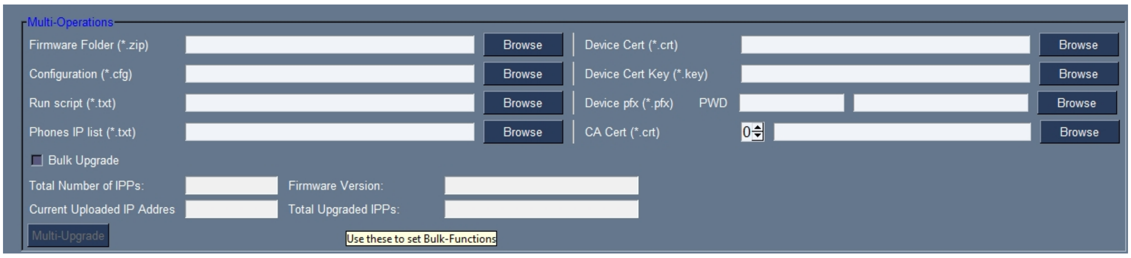


Android Phone Utility V1.1.22

Single-Operations

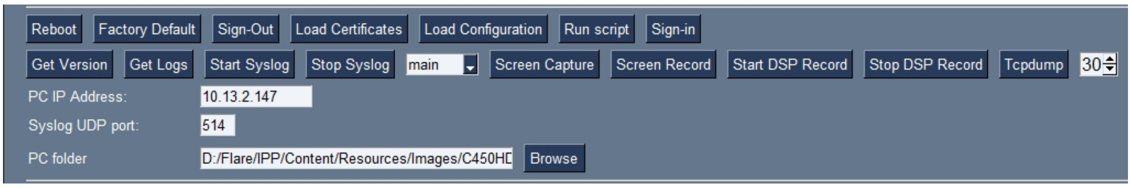
Android Phone Address	10.59.200.176
Username	admin
PWD	1234

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



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

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



PC IP Address: 10.13.2.147

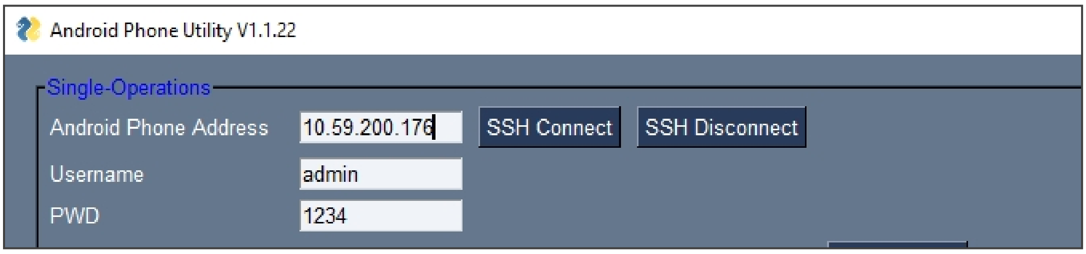
Syslog UDP port: 514

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

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

➢ To load certificates to multiple devices:

1. In the Android Device Utility (see Android Device Utility on page 97 for more information), enter the phone's IP address and click **SSH Connect**.



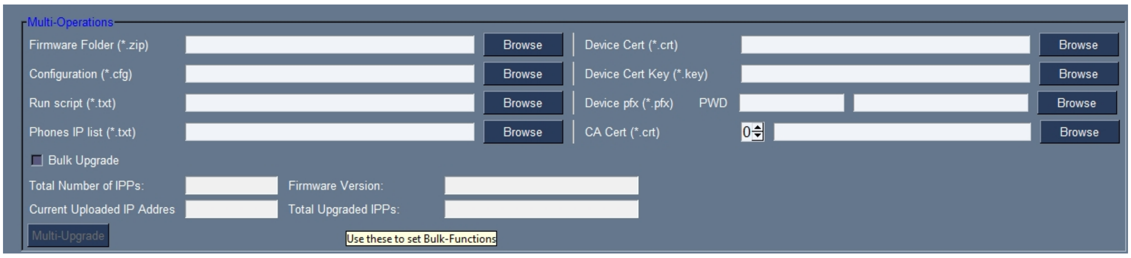
Android Phone Address 10.59.200.176

Username admin

PWD 1234

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

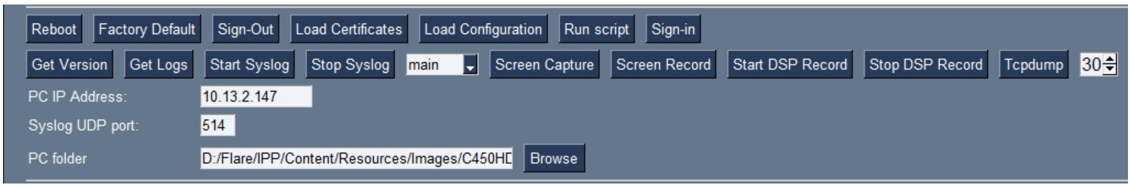
2. Click the**Browse** button next to the field 'Device Cert' under Multi Operations and then navigate to and select the certificate file to download.



3. Adjacent to the field 'Phones IP list' under 'Multi Operations', click the **Browse** button and then navigate to and select the txt file listing the IP addresses of the phones to which to

download the certificates. The IP addresses are listed one under the other. Each occupies its own line. No notation between them is required.

4. Click the now activated **Load Certificates** button shown in the next figure, to add the certificates to the phones.



main
30
PC IP Address: 10.13.2.147
Syslog UDP port: 514
PC folder D:/Flare/IPP/Content/Resources/Images/C450HD

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

Certificate Enrollment using SCEP

[Available from version 1.19] The device supports certificate enrollment using Simple Certificate Enrollment Protocol (SCEP) using Microsoft’s Network Device Enrollment Service (NDES) server, thereby allowing device certificates and CA certificate provisioning to be scaled to multiple devices.

After devices are provisioned with a SCEP-related configuration, they receive a CA certificate from the NDES, issue a Certificate Signing Request (CSR) to the NDES and receive a device certificate signed by the CA certificate (the one that the device received from NDES).

Configure the following three parameters:

- security/SCEPEnroll/ca_fingerprint
- security/SCEPEnroll/password_challenge
- security/SCEPServerURL

The next table shows the descriptions of the SCEP parameters.

Parameter	Description
security/SCEPEnroll/ca_fingerprint	Define the thumbprint (hash value) for the CA certificate. Default value: NULL. Network admins must set its value to (for example): 3EBE50003ABF1DF5E6B5A3230B02B856
security/SCEPEnroll/password_challenge	Define the enrollment challenge password. Default value: NULL. Network admins must set its value to (for example): 7A7F9FC4BB7625F0935E67EA6D6322ED
security/SCEPServerURL	Define the SCEP server URL. Default: NULL. If you use Microsoft NDES server, use:

Parameter	Description
	https://<NDES server IP address/Hostname>/certsrv/mscep/mscep.dll/pkiclient.exe
security/SCEPEnroll/renewal/advancethreshold	Define the renewal advance threshold of the device certificate. Configure between 50 and 100 (in units of percentage) Default: 80 This indicates that a renewal of the certificate (device.crt) will be initiated when 80 percent of its validity is reached.
security/SCEPEnroll/rollover/advancethreshold	Specify the threshold of the CA Root certificate's validity at which to initiate a renewal. Configure between 50 and 100 (in units of percentage). Default: 90 This indicates a renewal of the certificate (CAROOT.crt.) will be initiated when 90 percent of its validity is reached.
security/CSR/CommonName	Define a value according to the following 'wild-card' format: {mac} – the device's MAC address {IP} - the device's IP address {model} - the device model
security/CSR/Country	Define the name of the country used to generate the certificate signing request (CSR). Note: The ISO (International Organization for Standardization) code of the country / region in which the organization is located.
security/CSR/Email	Optionally, define the email address used to generate the CSR.
security/CSR/Organization	Optionally, define the legal name of the organization used to generate the CSR.
security/CSR/State	Optionally, define the name of the state / province used to generate the CSR.

Manually Performing Recovery Operations

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

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

Click here to view a video clip demonstrating how to recover the phone and reboot it to its original out-of-the-box state. The principle is similar across AudioCodes Teams phones.

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

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

When?	Action	Press key combination	LED flashes 3x after release
		Hold key for ~15 seconds	white once after release

Enrolling a Device with Intune Policies

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

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

Creating a Dynamic Group

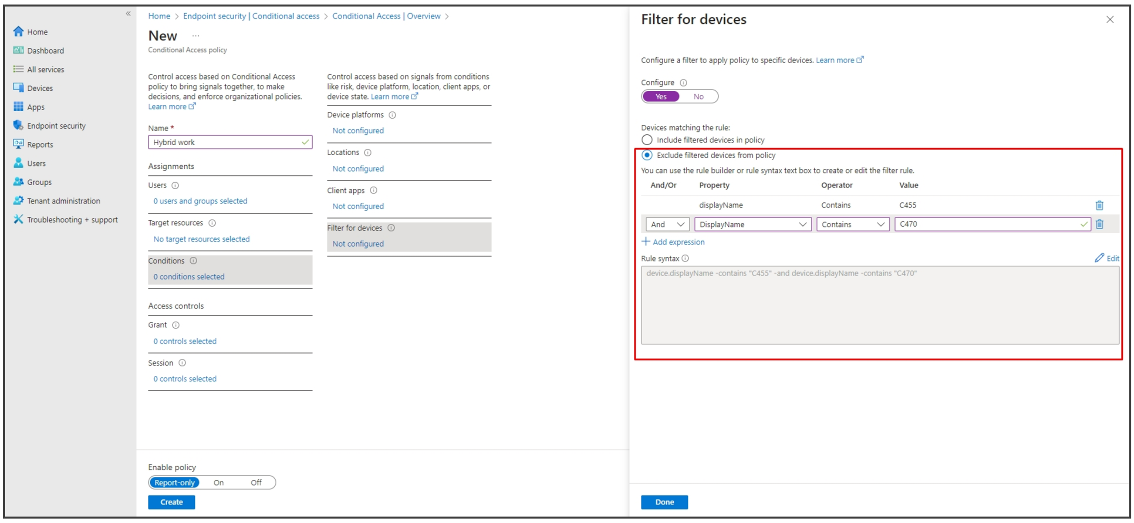
See here how to create dynamic groups in Intune for enrolling AudioCodes Android-based Teams devices.

Creating an Exclusion Group

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

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

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


Home
Dashboard
All services
Devices
Apps
Endpoint security
Reports
Users
Groups
Tenant administration
Troubleshooting + support
Home > Endpoint security | Conditional access > Conditional Access | Overview >

New

Conditional Access policy

Control access based on Conditional Access policy to bring signals together, to make decisions, and enforce organizational policies. Learn more

Name * Hybrid work

Assignments

Users: 0 users and groups selected

Target resources: No target resources selected

Conditions: 0 conditions selected

Access controls

Grant: 0 controls selected

Session: 0 controls selected

Control access based on signals from conditions like risk, device platform, location, client apps, or device state. Learn more

Device platforms: Not configured

Locations: Not configured

Client apps: Not configured

Filter for devices: Not configured

Enable policy: [✓ Report-only] On Off

Create

Filter for devices

Configure a filter to apply policy to specific devices. Learn more

Configure: [✓ Yes] No

Devices matching the rule:

○ Include filtered devices in policy

● Exclude filtered devices from policy

You can use the rule builder or rule syntax text box to create or edit the filter rule.

And/Or	Property	Operator	Value
	displayName	Contains	C455
And	DisplayName	Contains	C470

+ Add expression

Rule syntax

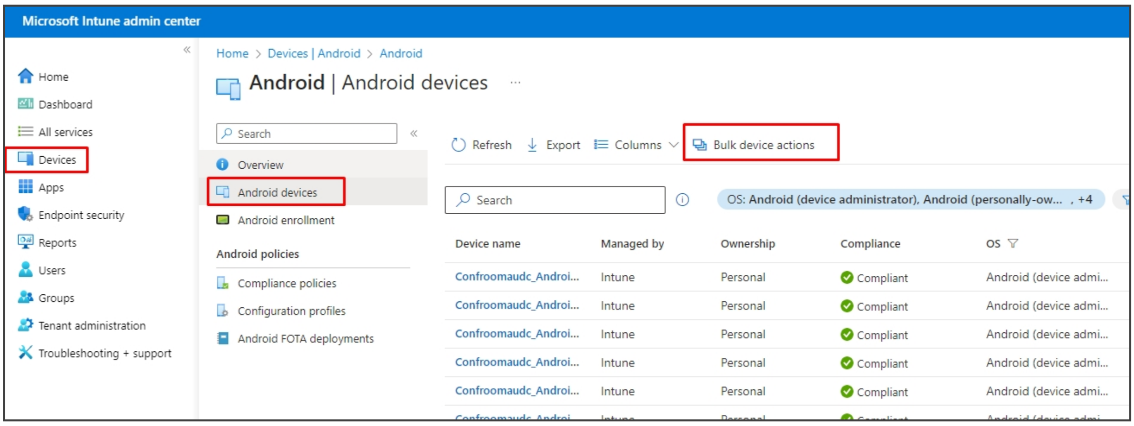
```
device.displayName -contains "C455" -and device.displayName -contains "C470"
```

Removing Devices from Intune admin center

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

➢ To remove devices from Intune admin center:

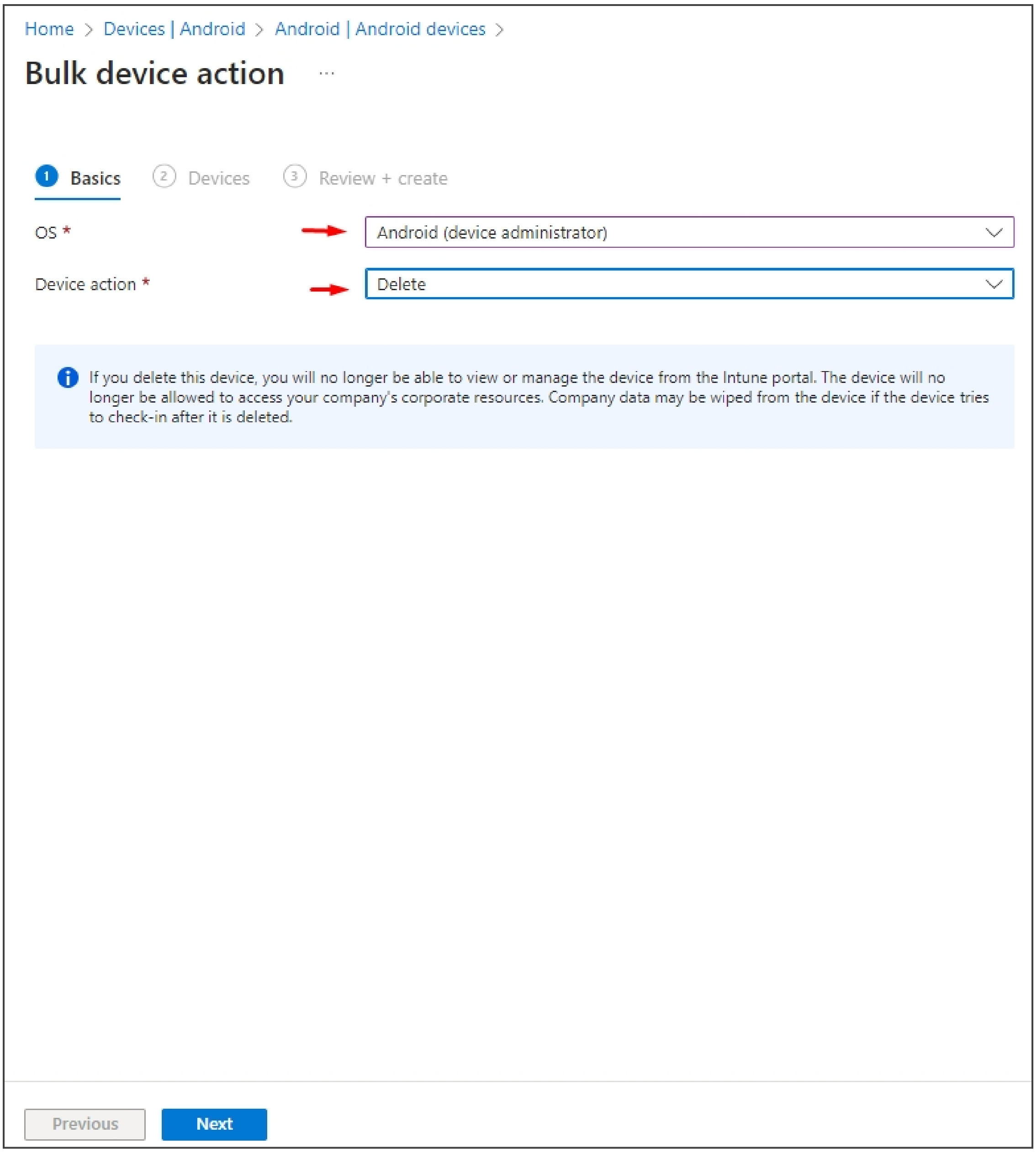
1. Go to Microsoft 365 admin center [portal.office.com] and log in with an Administration account.
2. Navigate to **Devices** > **Android devices**.



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

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

3. Click **Bulk device actions**.

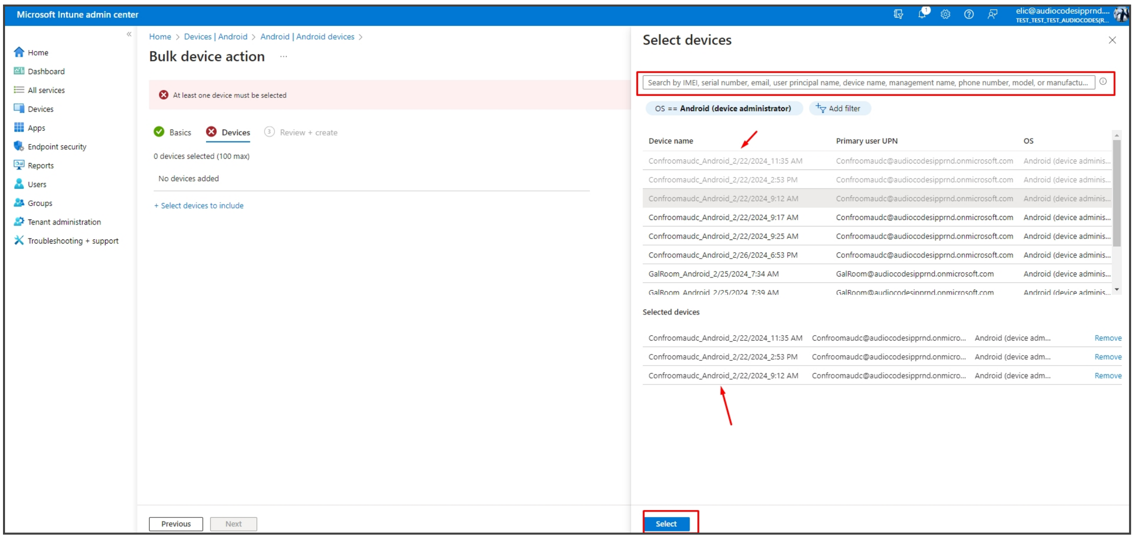


OS * Android (device administrator)

Device action * Delete

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

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


Microsoft Intune admin center
elic@audiocodesipprnd....
TEST_TEST_TEST_AUDIOCODES(R...
Home
Dashboard
All services
Devices
Apps
Endpoint security
Reports
Users
Groups
Tenant administration
Troubleshooting + support
Home > Devices | Android > Android | Android devices >
Basics
Devices
Review + create
Previous
Next
Add filter
Select

Bulk device action

At least one device must be selected

0 devices selected (100 max)

No devices added

+ Select devices to include

Select devices

Search by IMEI, serial number, email, user principal name, device name, management name, phone number, model, or manufactu...

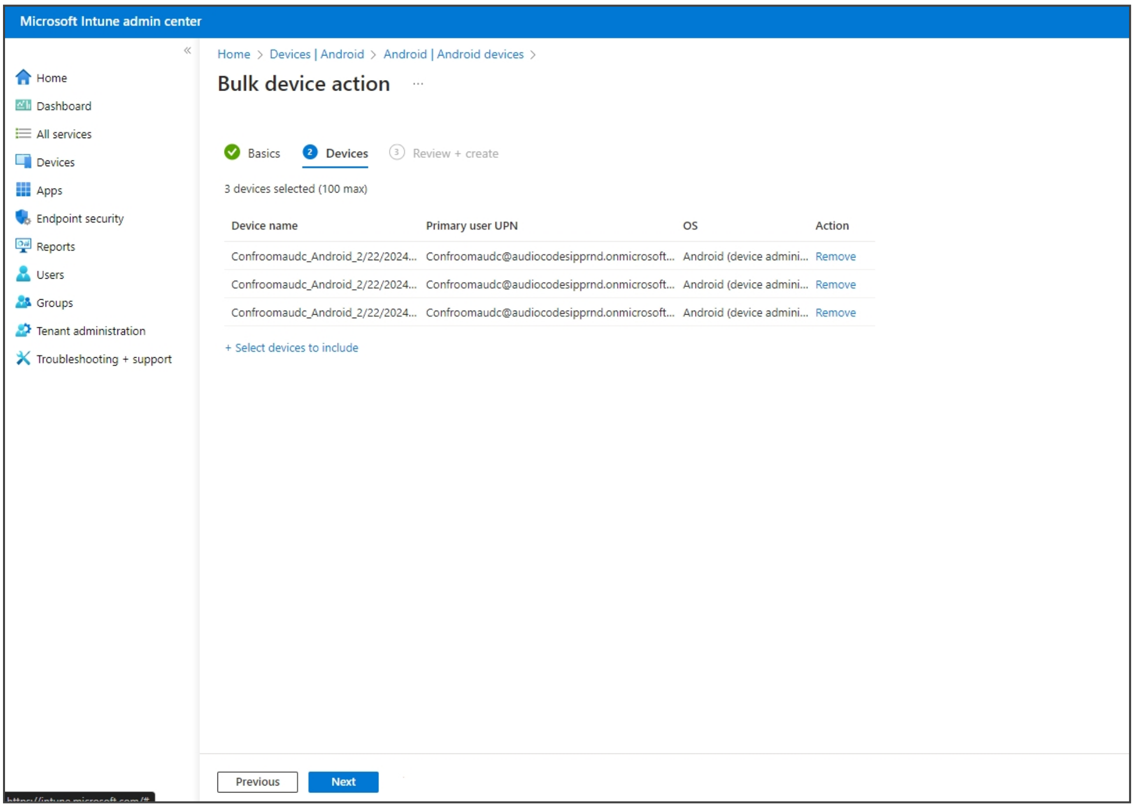
OS == **Android (device administrator)**

Device name	Primary user UPN	OS
Confroomaudc_Android_2/22/2024_11:35 AM	Confroomaudc@audiocodesipprnd.onmicrosoft.com	Android (device adminis...
Confroomaudc_Android_2/22/2024_2:53 PM	Confroomaudc@audiocodesipprnd.onmicrosoft.com	Android (device adminis...
Confroomaudc_Android_2/22/2024_9:12 AM	Confroomaudc@audiocodesipprnd.onmicrosoft.com	Android (device adminis...
Confroomaudc_Android_2/22/2024_9:17 AM	Confroomaudc@audiocodesipprnd.onmicrosoft.com	Android (device adminis...
Confroomaudc_Android_2/22/2024_9:25 AM	Confroomaudc@audiocodesipprnd.onmicrosoft.com	Android (device adminis...
Confroomaudc_Android_2/26/2024_6:53 PM	Confroomaudc@audiocodesipprnd.onmicrosoft.com	Android (device adminis...
GalRoom_Android_2/25/2024_7:34 AM	GalRoom@audiocodesipprnd.onmicrosoft.com	Android (device adminis...
GalRoom_Android_2/25/2024_7:39 AM	GalRoom@audiocodesipprnd.onmicrosoft.com	Android (device adminis...

Selected devices

Confroomaudc_Android_2/22/2024_11:35 AM	Confroomaudc@audiocodesipprnd.onmicro...	Android (device adm...	Remove
Confroomaudc_Android_2/22/2024_2:53 PM	Confroomaudc@audiocodesipprnd.onmicro...	Android (device adm...	Remove
Confroomaudc_Android_2/22/2024_9:12 AM	Confroomaudc@audiocodesipprnd.onmicro...	Android (device adm...	Remove

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



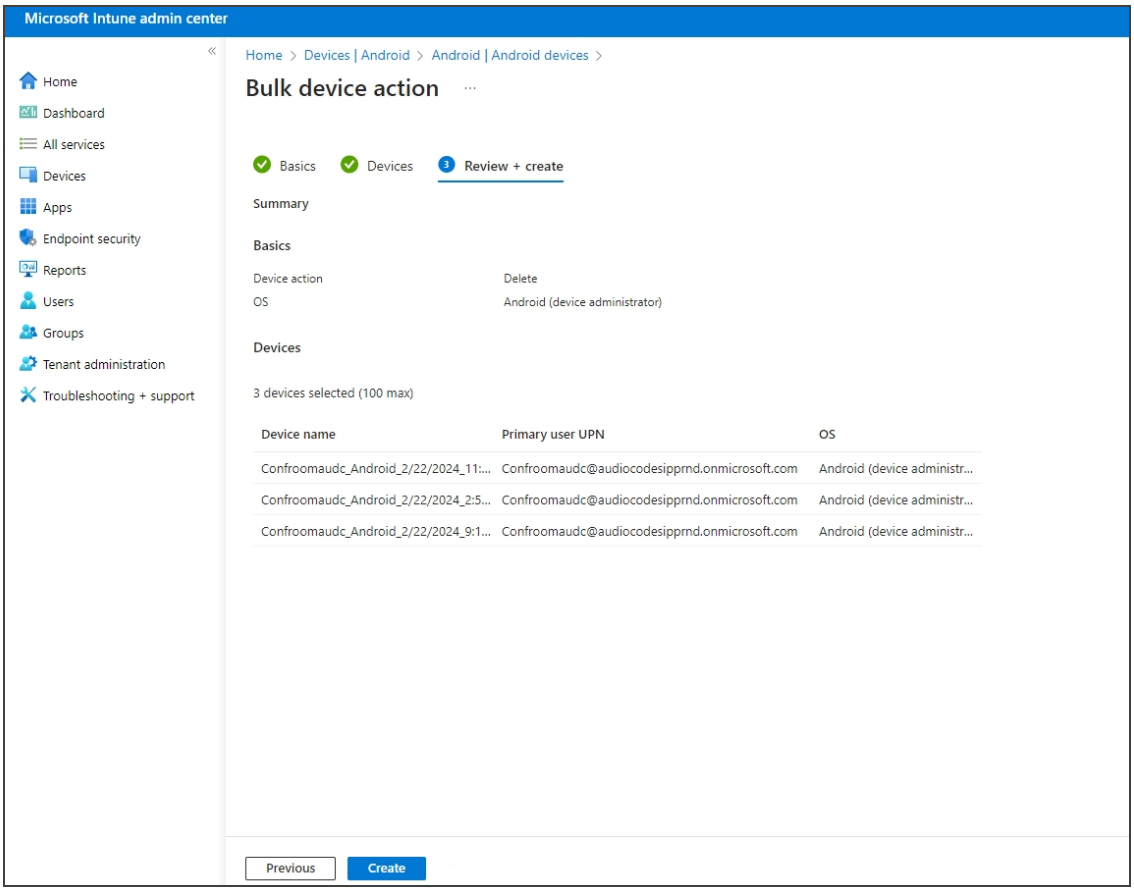
Bulk device action

3 devices selected (100 max)

Device name	Primary user UPN	OS	Action
Confroomaudc_Android_2/22/2024...	Confroomaudc@audiocodesipprnd.onmicrosoft...	Android (device admini...	Remove
Confroomaudc_Android_2/22/2024...	Confroomaudc@audiocodesipprnd.onmicrosoft...	Android (device admini...	Remove
Confroomaudc_Android_2/22/2024...	Confroomaudc@audiocodesipprnd.onmicrosoft...	Android (device admini...	Remove

+ Select devices to include

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



Summary

Basics

Device action	Delete
OS	Android (device administrator)

Devices

3 devices selected (100 max)

Device name	Primary user UPN	OS
Confroomaudc_Android_2/22/2024_11:...	Confroomaudc@audiocodesipprnd.onmicrosoft.com	Android (device administr...
Confroomaudc_Android_2/22/2024_2:5...	Confroomaudc@audiocodesipprnd.onmicrosoft.com	Android (device administr...
Confroomaudc_Android_2/22/2024_9:1...	Confroomaudc@audiocodesipprnd.onmicrosoft.com	Android (device administr...

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

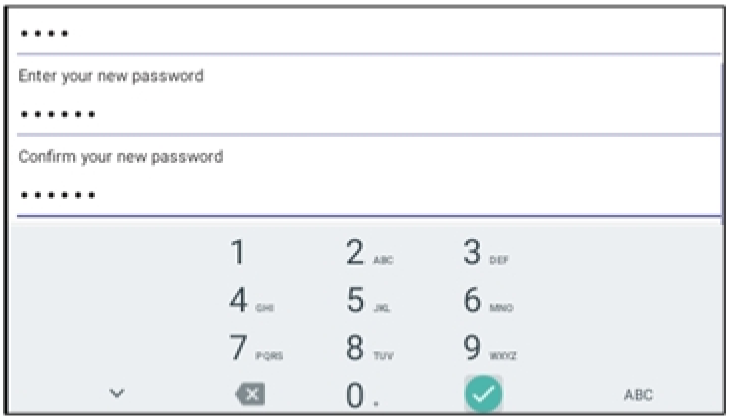
⚠ It may take some time to completely sync the devices with the account so after deleting the devices wait for 30 minutes before signing in.

Updating Microsoft Teams Devices Remotely

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

Defining Password Complexity

Admin-defined password complexity is designed mainly for non-touch screen phones but it can also be applied to touch-screen phones. The feature provides admin with the capability to finely adjust password complexity, ensuring that customers using low-cost phones (LCPs) can easily input passwords using the phone's hard keys.



••••

Enter your new password

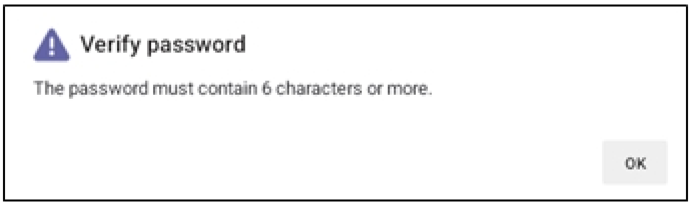
••••••

Confirm your new password

••••••

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

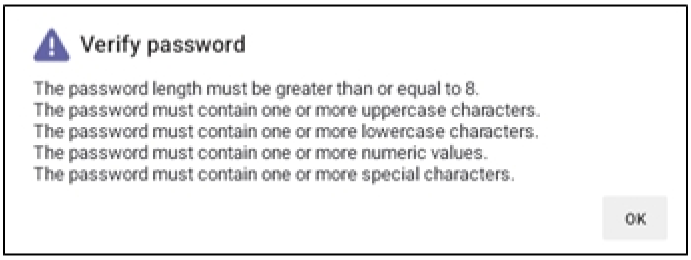
- When updating LCPs to the current version, the parameter is by default set to COMPLEXITY_MEDIUM. Password complexity rule: At least six characters and/or digits must be used.



Verify password

The password must contain 6 characters or more.

- When updating non-LCP touch-screen phones to the current version, the parameter default is COMPLEXITY_HIGH. Password complexity rules are as follows:



Verify password

The password length must be greater than or equal to 8.
The password must contain one or more uppercase characters.
The password must contain one or more lowercase characters.
The password must contain one or more numeric values.
The password must contain one or more special characters.

- If a phone was configured with a *complex* password in earlier versions, it *preserves* that password.
- Admin can optionally change it to a *non-complex* password.

Applying Firmware to a Phone from a USB Disk

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

➢ **To apply the firmware from the USB disk:**

1. Enter recovery mode by simultaneously pressing the ‘back’ key + the MENU key; the device’s LED lights up red.

2. Insert the USB disk with the target firmware.

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

Disabling a Device’s USB Port

⚠ Applies to all AudioCodes’ Teams phones.

This functionality complies with the physical security requirements of some customers, specifically, customers who are in the government space.

Customer admins can disable a phone’s USB port with the following parameter available in the phone’s .cfg configuration file:

```
admin/usb_enabled=1
admin/usb_enabled=0
```

The parameter can be configured via the AudioCodes One Voice Operations Center (OVOC) Device Manager module used to manage AudioCodes’ Teams phones, as well as via SSH command.

The parameter is also available in the template which can be applied to multiple phones via the Device Manager.

⚠

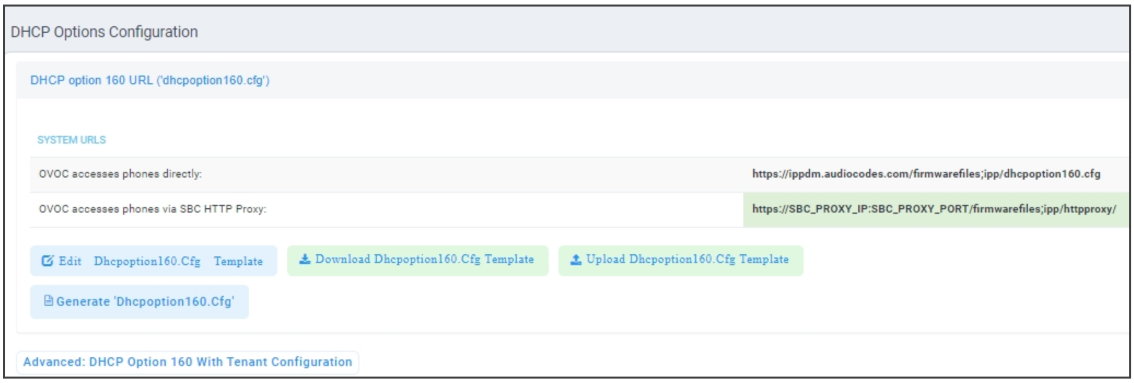
- After setting the parameter to 0, the phone cannot under any circumstances detect a plugged-in USB device.
- Additionally, all USB-related settings are removed from the phone’s user interface.

Managing Phones with the Device Manager

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

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

Table 6-1: DHCP Option 160 URL



DHCP Options Configuration

DHCP option 160 URL ('dhcpoption160.cfg')

SYSTEM URLS

OVOC accesses phones directly: https://ippdm.audiocodes.com/firmwarefiles;ipp/dhcpoption160.cfg

OVOC accesses phones via SBC HTTP Proxy: https://SBC_PROXY_IP:SBC_PROXY_PORT/firmwarefiles;ipp/httpproxy/

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

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

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

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

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

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

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

Configuring a Periodic Provisioning Cycle

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

➢ To configure how often periodic provisioning cycles will occur:

- Use the following table as reference.

Table 6-2: Periodic Provisioning Cycle

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

Configuring TimeZone and Daylight Savings

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

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

➢ To configure TimeZone and Daylight Savings:

- Use the following table as reference.

Table 6-3: TimeZone And Daylight Savings

Parameter	Description
date_time/-time_dst	[Boolean parameter]. Configuring **ENABLED** adds one hour to the configured time. Valid values are:

Parameter	Description
	- 1 - 0

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

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

date_time/time_dst=**1**

-OR-

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

date_time/time_dst=**0**

Managing Devices with HTTPS

Android-based Teams devices support an HTTPS connection.

➢ To establish an HTTPS connection:

- The server certificate must be signed by a well-known Certificate Authority

  -OR-

- A root/intermediate CA certificate must be loaded to the device's trust store via Configuration File parameter '/security/ca_certificate/[0-4]/uri'

➢ To maintain backward compatibility with devices previously running UC versions:

- Configure parameter '/security/SSLCertificateErrorsMode' to **Ignore**

Supported Parameters

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

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

- display/backlight = 80 (0-100)
- display/high_contrast = 0 (default) /1
- date_time/timezone = +02:00
- date_time/time_dst = 0 (default) /1
- date_time/time_format = 12 (default) / 24
- network/dhcp_enabled = 0/1
- network/ip_address =
- network/subnet_mask =
- network/default_gateway =
- network/primary_dns =
- network/pecondary_dns =
- network/pc_port = 0/1
- office_hours/start = 08:00
- office_hours/end = 17:00
- logging/enabled = 0/1
- logging/levels = VERBOSE, DEBUG, INFO, WARN, ERROR, ASSERT, SILENT
- admin/default_password = 1234
- admin/ssh_enabled=0/1 (default)
- security/SSLCertificateErrorsMode = IGNORE, NOTIFICATION, DISALLOW (default)
- security/ca_certificate/[0-4]/uri
- provisioning/period/daily/time
- provisioning/period/hourly/hours_interval
- provisioning/period/type = HOURLY, DAILY (default), WEEKLY, POWERUP, EVERY5MIN, EVERY15MIN
- provisioning/period/weekly/day
- provisioning/period/weekly/time
- provisioning/random_provisioning_time

Configuring QoS on PC Port

QoS settings for the PC port are supported (VLAN for PC port). Admin can configure PC port QoS via the device’s cfg configuration file which can be loaded to the device via (for example) AudioCodes' Device Manager. The following three cfg configuration file parameters are available configuring the feature:

Parameter	Description
network/lan/vlan/pc_port_tagging/enable=0	Defines the PC port VLAN as enabled / disabled. ■ 0 = PC port VLAN disabled ■ 1 = PC port VLAN enabled Default: 0
network/lan/vlan/pc_port_id=0	Defines the PC port VLAN ID. Range: 0-4096 Default: 0
network/lan/vlan/pc_port_priority=0	Defines PC port VLAN priority. Range: 0-7 Default: 0

The feature provides PC port QoS for AudioCodes' Android-based phones which feature settings for VLAN *and* VLAN Priority (802.1p) for the PC port.

Configuring Admin Login Timeout

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

settings/admin_logout_timeout,values=3

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

⚠

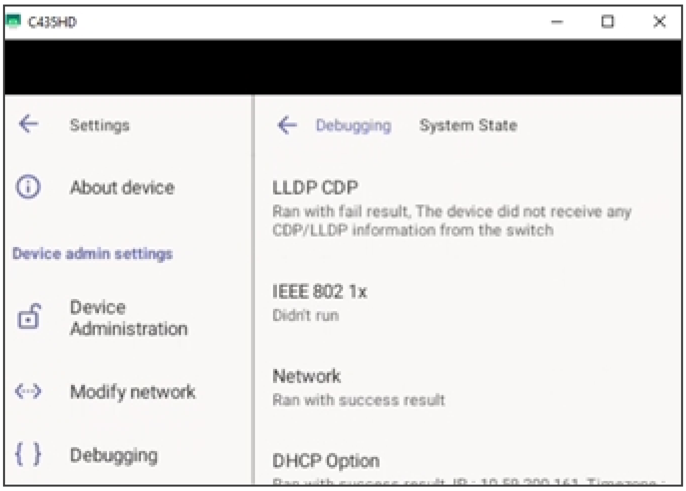
- The cfg file can be loaded to the device using Device Manager.
- Timing begins when exiting the 'Device Settings' menu.
- When the timeout expires, the device logs out automatically.
- The functionality works for both registered and unregistered devices.

Monitoring Phone Process Statuses

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

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

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

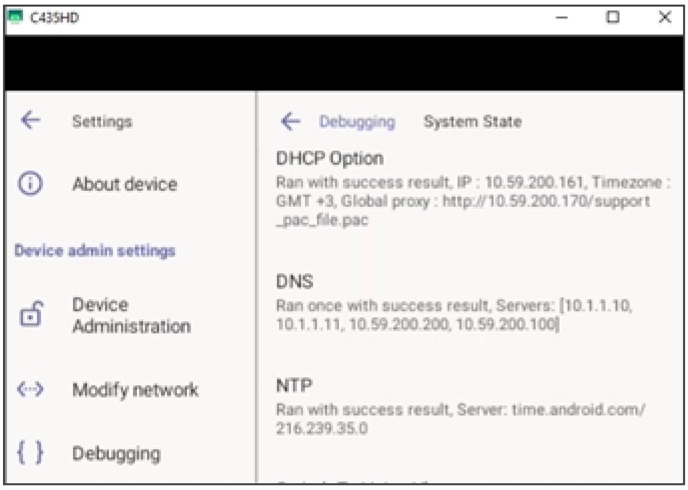


LLDP CDP
Ran with fail result, The device did not receive any CDP/LLDP information from the switch

IEEE 802 1x
Didn't run

Network
Ran with success result

DHCP Option
Ran with success result, IP : 10.59.200.161, Timezone :



DHCP Option
Ran with success result, IP : 10.59.200.161, Timezone : GMT +3, Global proxy : http://10.59.200.170/support_pac_file.pac

DNS
Ran once with success result, Servers: [10.1.1.10, 10.1.1.11, 10.59.200.200, 10.59.200.100]

NTP
Ran with success result, Server: time.android.com/216.239.35.0

7 Troubleshooting

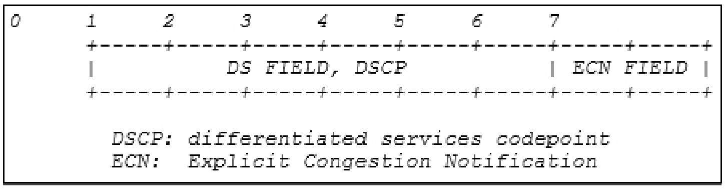
The information presented here shows how to troubleshoot AudioCodes devices.

DSCP

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

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

Figure 7-1: DS Field, DSCP



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

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

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

See also Microsoft's website for more information.

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

Figure 7-2: Recommended Values

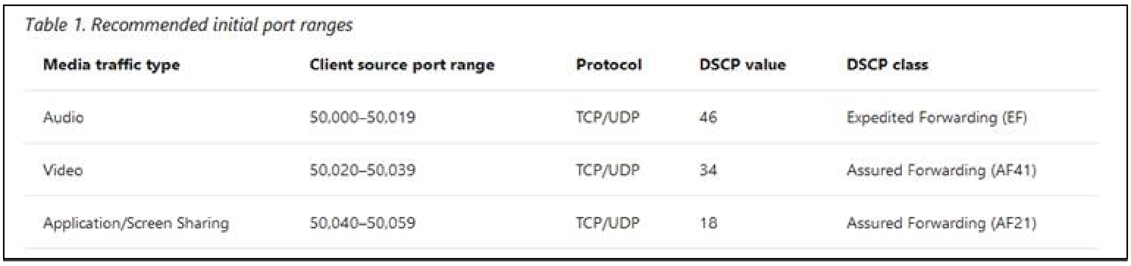
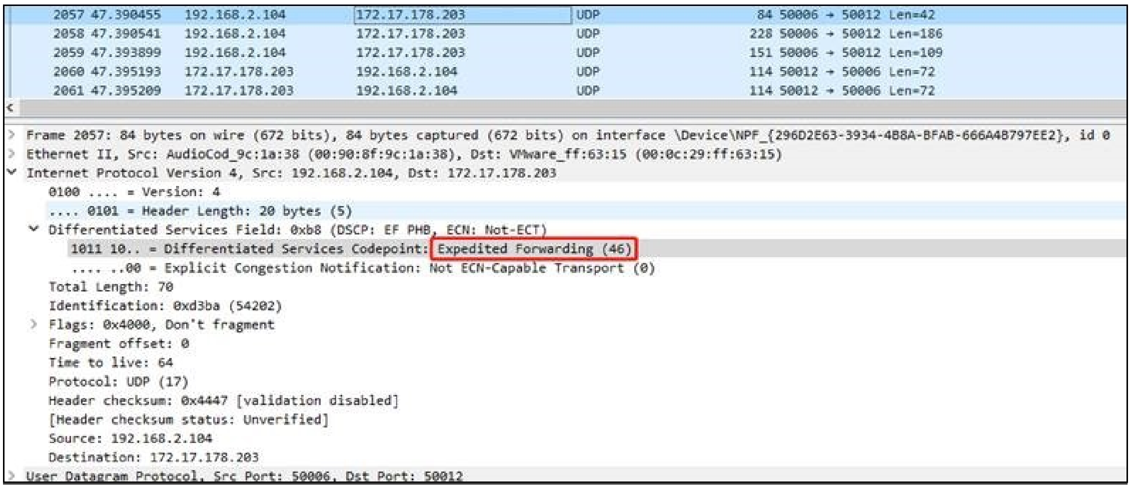


Table 1. Recommended initial port ranges

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

Figure 7-3: Audio



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

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

Users

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

Table 7-1: Troubleshooting

Symptom	Problem	Corrective Procedure
Phone is off (no screen displays and LEDs)	Phone is not receiving power	■ Make sure the AC/DC power adapter is attached firmly to the DC input on the rear of the phone. ■ Make sure the AC/DC power adapter is plugged into the electrical outlet. ■ Make sure the electrical outlet is functional. ■ If using Power over Ethernet (PoE), contact your network administrator to check that the switch is powering the phone.
Phone is not ringing	Ring volume is set too low	■ Increase the volume (see Adjusting Ring Volume on page 65)
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 66).

Exporting Logs to USB when Phone is in Recovery Mode

This feature empowers users to seamlessly save logs while their phone is in recovery mode. In Android recovery mode, the system automatically mounts a partition, enabling users to connect a USB stick. By simply clicking the 'Export logs to USB disk' option, all logs are efficiently copied to the USB stick, providing a convenient and reliable method for log management during recovery procedures.

Network Administrators

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

Android Device Utility

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

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

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

➢ To sign in to the utility:

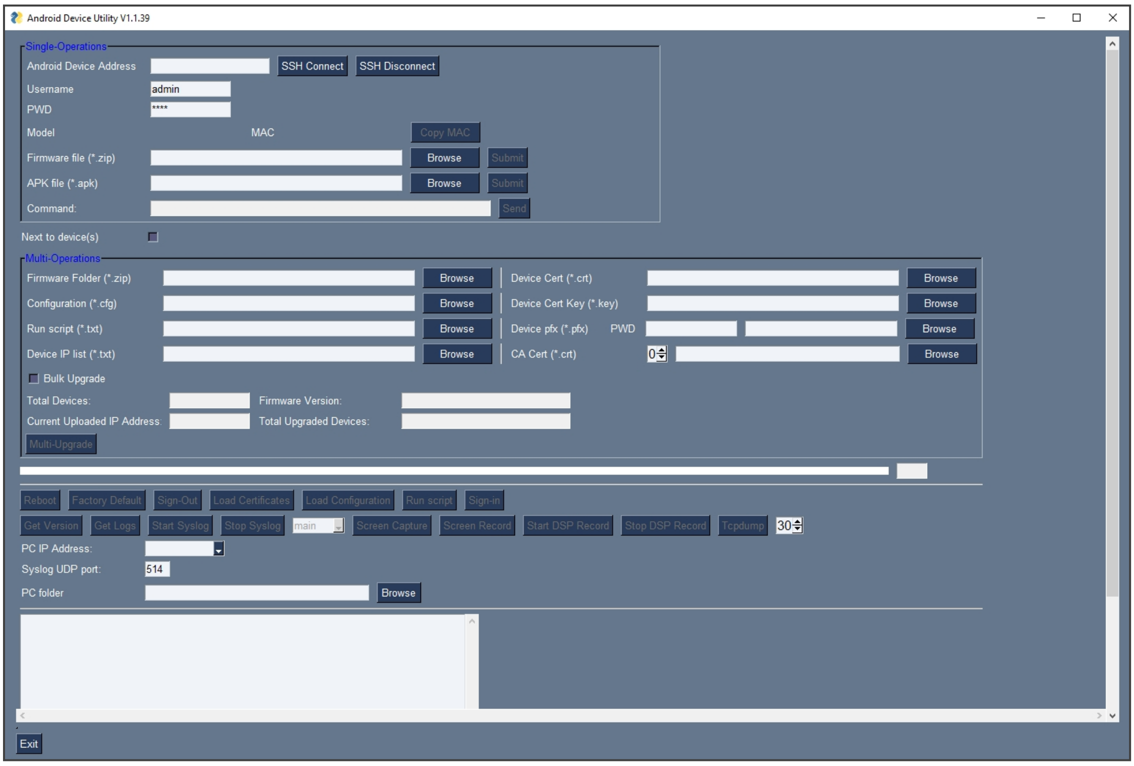
- Enter your username and password; **admin** and **1234** are the defaults.

The application gives network administrators the following debugging capabilities:

- Capturing the Phone Screen on page 99
- Running Tcpdump on page 100
- Getting Information about Phones on page 101
- Remote Logging (Syslog) on page 102
- Getting Diagnostics on page 103
- Getting Logs on page 105
- Activating DSP Recording on page 106
- Deactivating DSP Recording on page 107
- Getting Information about Phones on page 101

➢ To open the utility:

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



Username admin

PWD ****

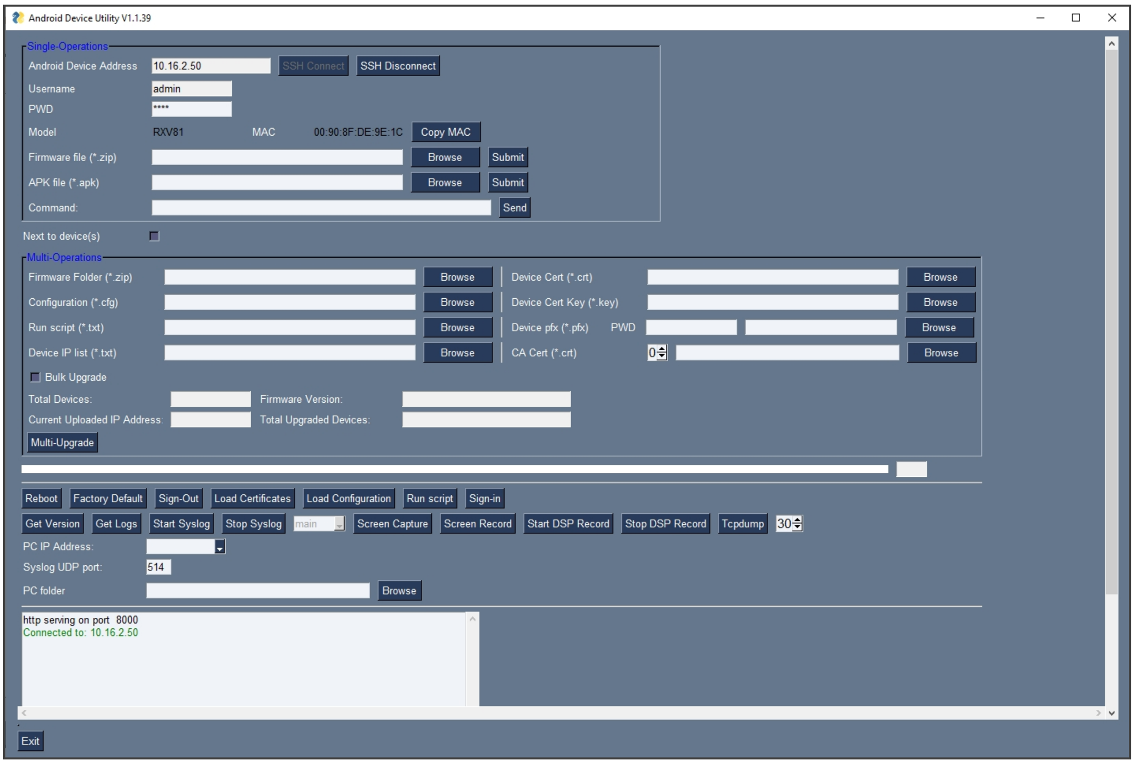
CA Cert (*.crt) 0

Tcpdump 30

Syslog UDP port: 514

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

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



Android Device Address 10.16.2.50

Username admin

PWD ****

Model RXV81 MAC 00:90:8F:DE:9E:1C

CA Cert (*.crt) 0

Tcpdump 30

Syslog UDP port: 514

```
http serving on port  8000
Connected to:  10.16.2.50
```

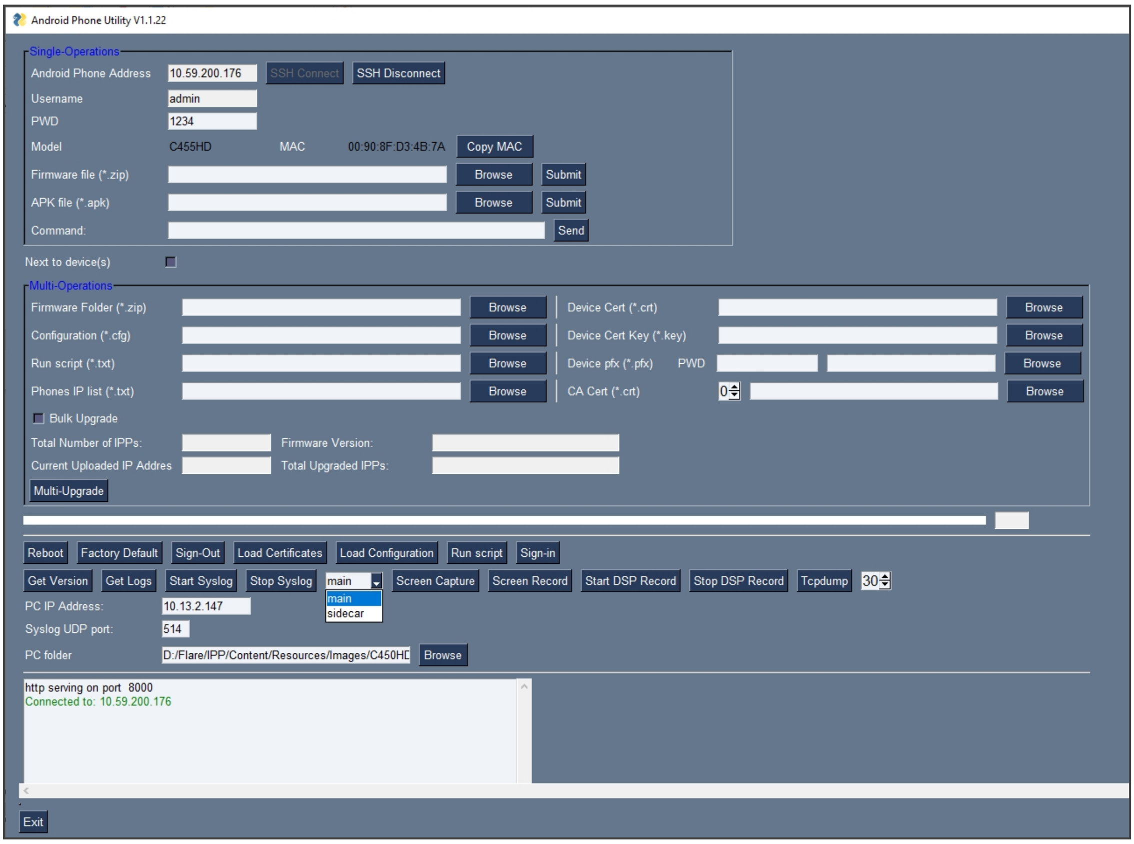
4. Next to the field 'PC folder', click the **Browse** button and navigate to and select the folder to which to send data to use for debugging.

Capturing the Phone Screen

AudioCodes' Android Device Utility allows network administrators to effectively collaborate and debug issues using the screen-capturing feature. The feature enables capturing the phone's main screen.

➢ To capture the phone screen:

1. Open the Android Device Utility: From the PC's **Start** menu, select the app icon or click the application's exe file in the folder in which you saved it.
2. In the 'Android Phone Address' field, enter the IP address of the device (get it by pressing the MENU hard key > **About phone** > **Status** > **IP Address**).
3. Click **SSH Connect**; a connection with the device is established.
4. Next to the field 'PC folder', click the **Browse** button and navigate to and select the folder to which to send the screen captures.
5. Make sure that the drop-down menu next to the **Screen Capture** button shows **main**.
6. Click the **Screen Capture** button; the phone's screen is captured and the screenshot is saved and sent to the folder.



Android Phone Address: 10.59.200.176
Username: admin
PWD: 1234
Model: C455HD MAC: 00:90:8F:D3:4B:7A
CA Cert (*.crt): 0
main
Tcpdump: 30
PC IP Address: 10.13.2.147
Syslog UDP port: 514
PC folder: D:/Flare/IPP/Content/Resources/Images/C450HD

```
http serving on port  8000
Connected to: 10.59.200.176
```

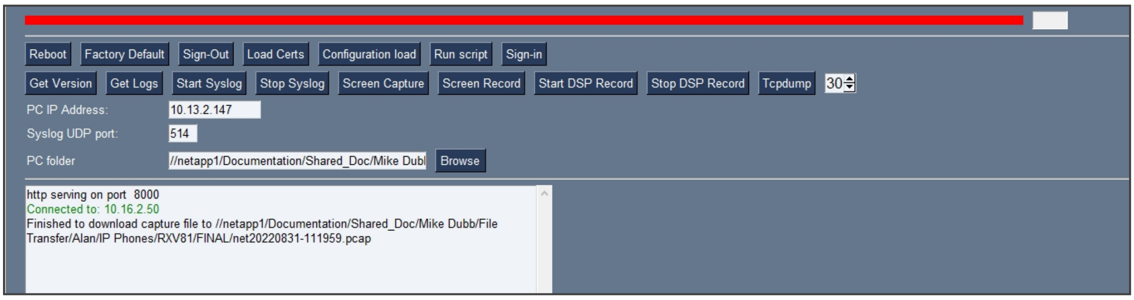
7. On your PC, navigate to the folder and retrieve the screenshot. Default file name: **screencap.png**. Rename it to a name related to the screen you captured. If you don't rename it, it will be overwritten the next time you take a screenshot.

Running Tcpdump

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

➢ To run Tcpdump:

1. In the Android Device Utility (see Android Device Utility on page 97 for more information about the application), enter the phone's IP address, click **SSH Connect** and browse to a folder on the PC to which to send the information.
2. Next to the **Tcpdump** button, set the time period or leave it at the default. Default: **30** seconds.
3. Click the **Tcpdump** button and then after the progress indicator reaches the end you'll view in the results pane a 'Finished' indication.



Tcpdump: 30

PC IP Address: 10.13.2.147

Syslog UDP port: 514

PC folder: //netapp1/Documentation/Shared_Doc/Mike Dubl

```
http serving on port  8000
Connected to: 10.16.2.50
Finished to download capture file to //netapp1/Documentation/Shared_Doc/Mike Dubb/File
Transfer/Alan/IP Phones/RXV81/FINAL/net20220831-111959.pcap
```

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

Alternatively, run Tcpdump *without* the utility.

➢ To run tcpdump without the utility:

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

```
setprop ac.ac_tcpdump.timeout <seconds>
```

2. After defining the capturing time as shown in the preceding command, start the capture:

```
setprop ac.ac_tcpdump 1
```

3. Tcpdump capture file will appear in this location:

```
/sdcard/recording/net.pcap
```

4. After running Tcpdump, reproduce the issue.
5. Execute the following command from your PC command prompt (cmd):

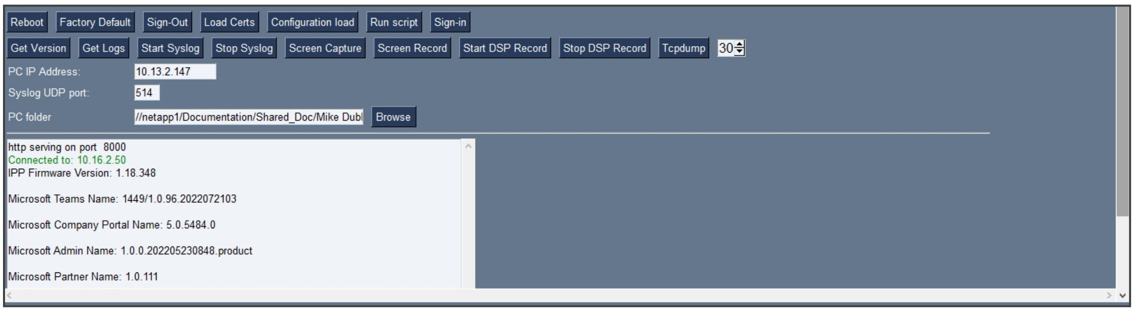
```
scp -r admin@%deviceIp%:/sdcard/recording/ %FolderOnPc%
```

Getting Information about Phones

Network administrators can get information about phones using AudioCodes' SSH protocol based Android Device Utility.

➢ To get information about the phone:

1. Open the Android Device Utility (see Android Device Utility on page 97 for more information about the application), enter the phone's IP address, click the adjacent **SSH Connect** button and browse to a folder on the PC to which to send the information.
2. Click the **Get Version** button.



30

PC IP Address: 10.13.2.147

Syslog UDP port: 514

PC folder //netapp1/Documentation/Shared_Doc/Mike Dubl

```
http serving on port  8000
Connected to: 10.16.2.50
IPP Firmware Version: 1.18.348

Microsoft Teams Name: 1449/1.0.96.2022072103

Microsoft Company Portal Name: 5.0.5484.0

Microsoft Admin Name: 1.0.0.202205230848.product

Microsoft Partner Name: 1.0.111
```

3. View the information in the pane.
4. Alternatively:
   - To get *firmware information*, in the 'Command' field enter the following and then click **Send**:

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

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

```
getprop ro.bootloader
```

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

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

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

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

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

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

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

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

Remote Logging (Syslog)

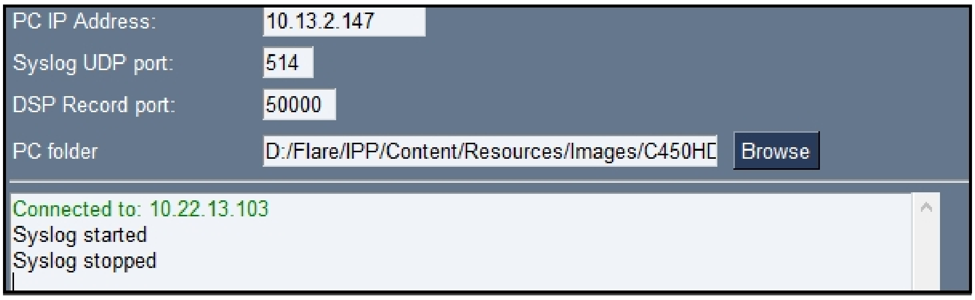
Remote Logging via Syslog provides the same log level as Device Diagnostics (performed via the Microsoft Teams Admin Center) with some additional information that may be relevant to device issues (not Teams application issues). Device Diagnostics via the Microsoft Admin Center are saved to the device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

Remote Logging via Syslog can be enabled from the

- Android Device Utility on page 97
- on the next page

➢ To enable Remote Logging via Syslog from the utility:

1. In the Android Device Utility (see Android Device Utility on page 97 for more information), enter the phone's IP address, click **SSH Connect** and browse to a folder on the PC to which to send the information.
2. In the 'PC IP Address' field, enter the IP address of the PC on which the utility is installed and then click the **Start Syslog** button.



PC IP Address: 10.13.2.147

Syslog UDP port: 514

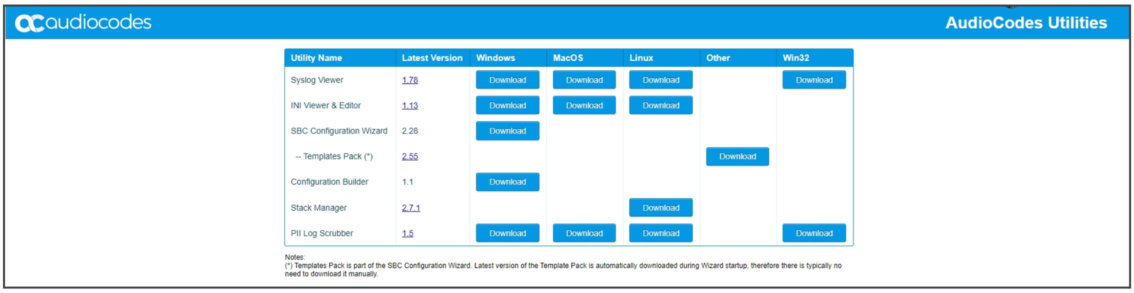
DSP Record port: 50000

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

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

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

4. To view Syslog, you can optionally download the Syslog Viewer available in AudioCodes' website.

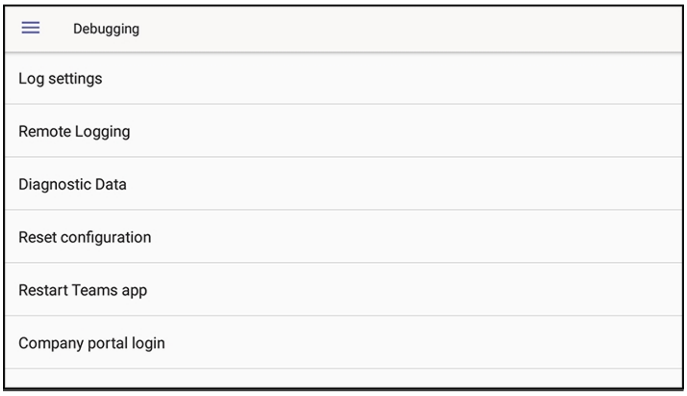


Utility Name	Latest Version	Windows	MacOS	Linux	Other	Win32
Syslog Viewer	1.78	Download	Download	Download		Download
INI Viewer & Editor	1.13	Download	Download	Download		
SBC Configuration Wizard	2.28	Download				
-- Templates Pack (*)	2.55				Download	
Configuration Builder	1.1	Download				
Stack Manager	2.7.1			Download		
PII Log Scrubber	1.5	Download	Download	Download		Download

Notes:
(*) Templates Pack is part of the SBC Configuration Wizard. Latest version of the Template Pack is automatically downloaded during Wizard startup, therefore there is typically no need to download it manually.

➢ To enable Remote Logging via Syslog from the phone:

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



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

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

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

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

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

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

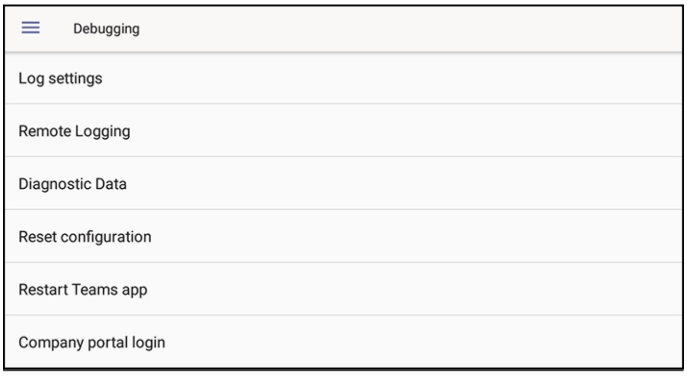
Getting Diagnostics

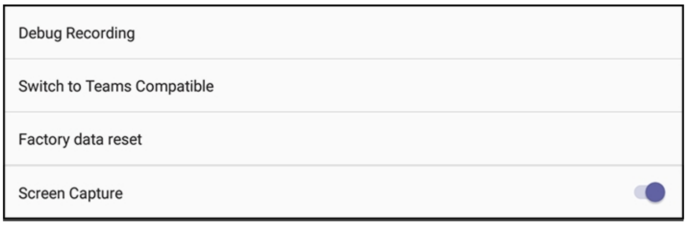
Network administrators can get diagnostics information to facilitate debugging.

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

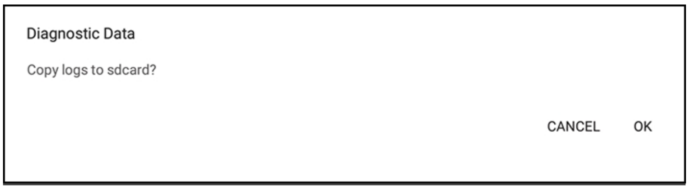
➢ To get diagnostics info:

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





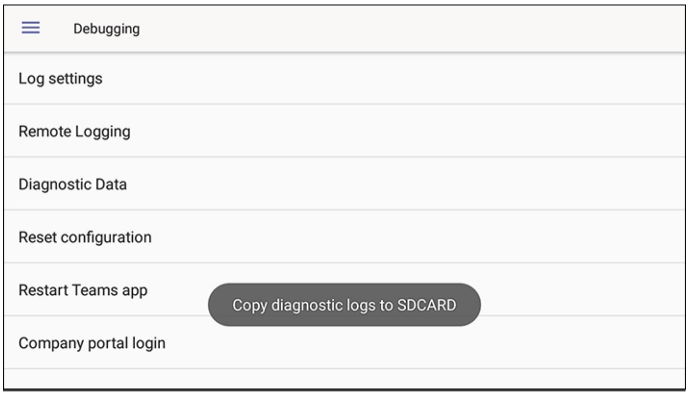
3. Select the **Diagnostic Data** option.



Diagnostic Data

Copy logs to sdcard?

4. Select **OK** to confirm.



Copy diagnostic logs to SDCARD

5. Wait until the screen shown in the preceding figure disappears; the phone creates all necessary logs and copies them to the its SD Card / Logs folder.

6. Get the logs using SCP notation as follows:

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

⚠ The following diagnostics files are then received from the phone:

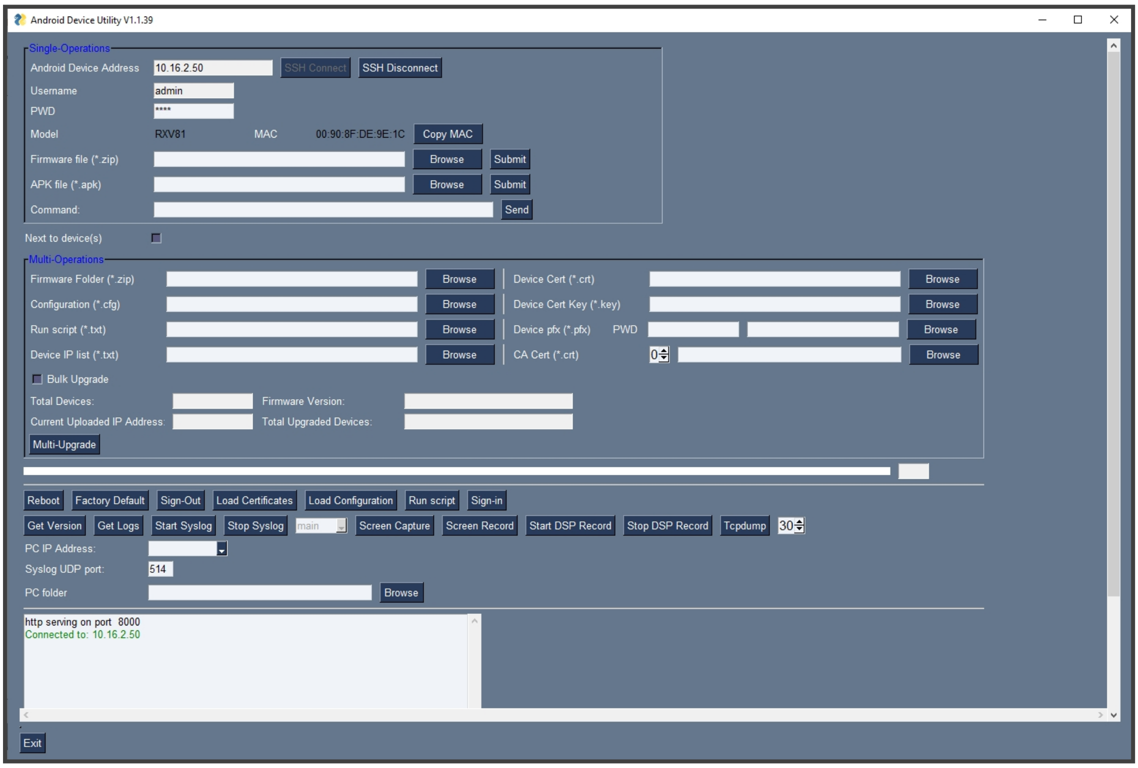
- dmesg.log
- dumpstate-c470hd-1.18.117_58793-41-undated-dumpstate_log-3458.txt
- dumpstate-c470hd-1.18.117_58793-41-undated.txt
- dumpstate-stats.txt
- logcat.log

Getting Logs

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

➢ To get logs:

1. In the AudioCodes Android Device Utility (seeAndroid Device Utility on page 97 for more information about the application), enter the phone's IP address, click **SSH Connect** and browse to a folder on the PC to which to send the information.



Android Device Utility V1.1.39

Android Device Address: 10.16.2.50

Username: admin

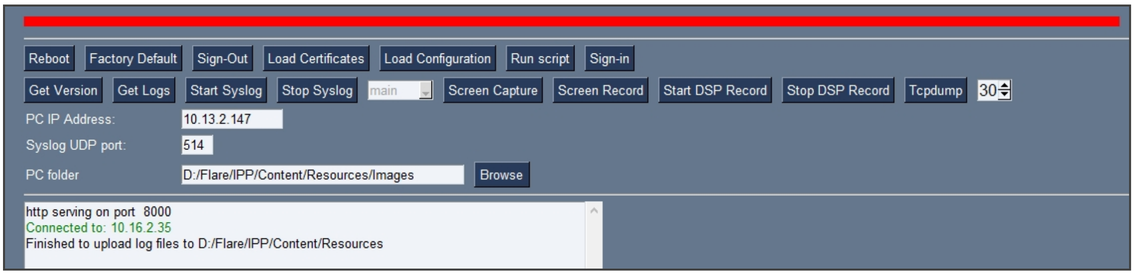
PWD: ****

Model: RXV81 MAC: 00:90:8F:DE:9E:1C

Syslog UDP port: 514

```
http serving on port  8000
Connected to: 10.16.2.50
```

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



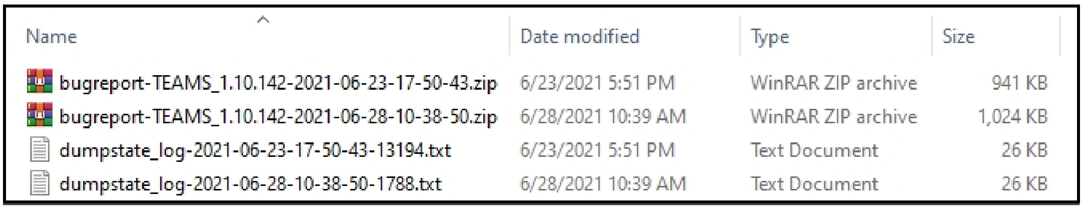
PC IP Address: 10.13.2.147

Syslog UDP port: 514

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

```
http serving on port  8000
Connected to: 10.16.2.35
Finished to upload log files to D:/Flare/IPP/Content/Resources
```

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



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

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

Activating DSP Recording

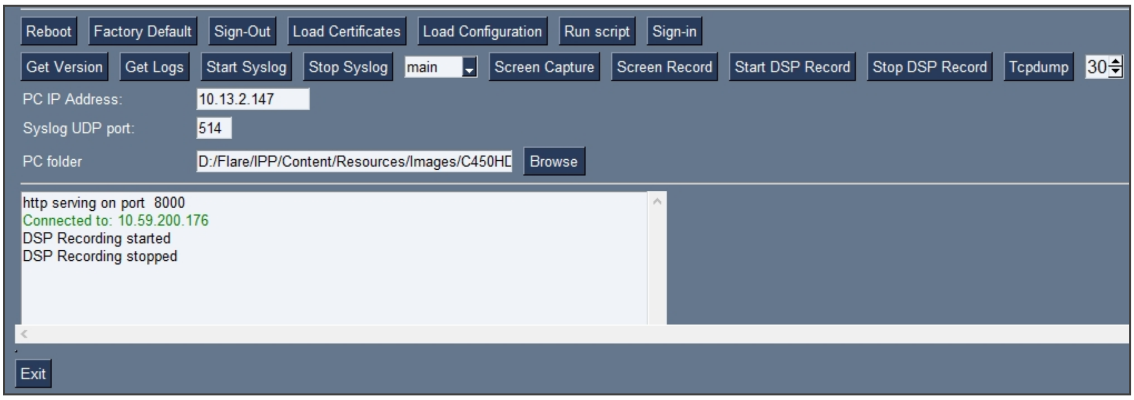
Network administrators can activate DSP recording using AudioCodes' SSH protocol based Android Device Utility.

➢ To activate DSP Recording:

1. In the AudioCodes Android Device Utility (see Android Device Utility on page 97 for more information about the application), enter the phone's IP address, click **SSH Connect** and then click the **Browse** button next to the field 'PC folder' to configure a folder on the PC to which to send the information.

2. In the 'PC IP Address' field, enter the IP address of the PC on which the utility is installed and then click the **Start DSP Record** button.

3. After a period of recording, click **Stop DSP Record**.



PC IP Address: 10.13.2.147

Syslog UDP port: 514

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

```
http serving on port  8000
Connected to: 10.59.200.176
DSP Recording started
DSP Recording stopped
```

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

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

➢ **To activate DSP recording using SSH protocol *without* the utility, type the following at the shell prompt:**

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

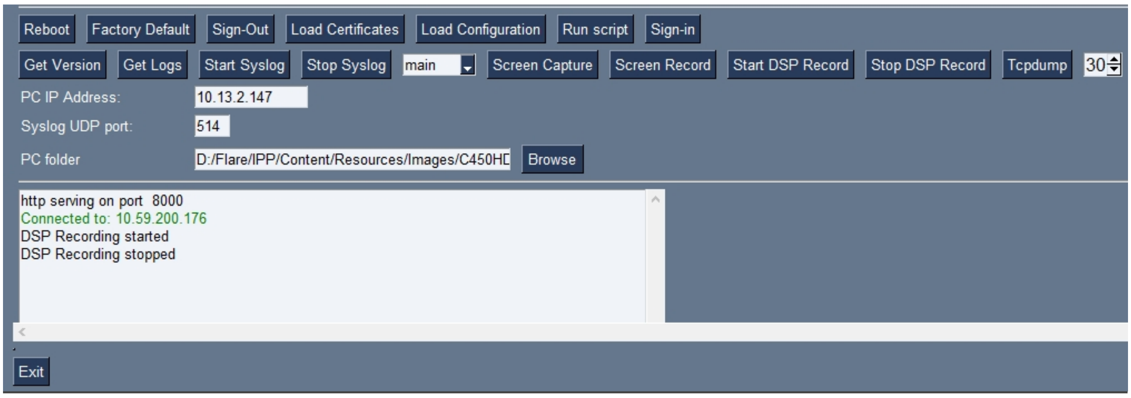
DSP recording can be activated on the fly without requiring the network administrator to reset the phone.

Deactivating DSP Recording

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

➢ **To deactivate DSP Recording:**

1. In the utility (see Android Device Utility on page 97 for more information about the application), click **Stop DSP Record** after a period of recording (see Activating DSP Recording on the previous page for information on how to start DSP recording).



main
30

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

```
http serving on port  8000
Connected to: 10.59.200.176
DSP Recording started
DSP Recording stopped
```

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

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

➢ **To deactivate DSP recording using SSH protocol *without* the utility, type the following at the shell prompt:**

```
setprop ac.dr_voice_enable false
```

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

SSH

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

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

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

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

SSH access allows administrators debugging capabilities such as:

- Getting the Phone IP Address below
- Pulling files from the phone sdcard (using the curl command)
- Activating DSP Recording on page 106
- Deactivating DSP Recording on the previous page
- Installing the APK using SSH on the next page

Getting the Phone IP Address

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

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

```
ifconfig
```

Installing the APK using SSH

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

Updating Phones using SSH Commands

➢ **To upgrade firmware:**

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

   For example, use the following:

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

2. Update the firmware using the following:

   ```
   setprop ctl.start local_update
   ```

3. Track progress using the following:

   ```
   logcat | grep  update_engine_client_android
   ```

➢ **To upgrade the Android Package Kit (APK):**

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

   For example use the following:

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

2. Update the APK using the following:

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

3. Delete the old APK using the following:

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

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

➢ **To collect logs:**

1. Collect logs using the following:

```
command/bugreport 1
```

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

   For example, use the following:

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

➢ **To install the Client Certificate:**

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

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

Microsoft Teams Admin Center

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

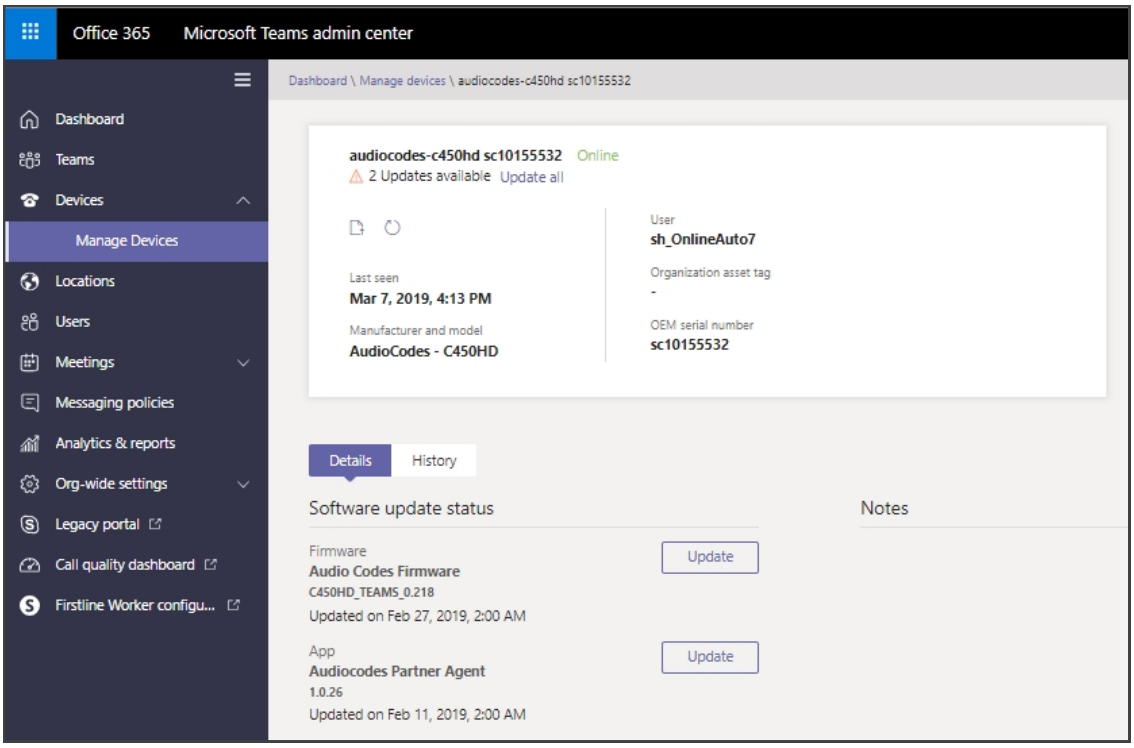
Collecting Logs

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

➢ **To collect logs:**

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

Figure 7-4: Microsoft Teams Admin Center - Diagnostics



Dashboard \ Manage devices \ audiocodes-c450hd sc10155532

audiocodes-c450hd sc10155532 Online

⚠ 2 Updates available Update all

Last seen
Mar 7, 2019, 4:13 PM

Manufacturer and model
AudioCodes - C450HD

User
sh_OnlineAuto7

Organization asset tag
-

OEM serial number
sc10155532

Software update status

Notes

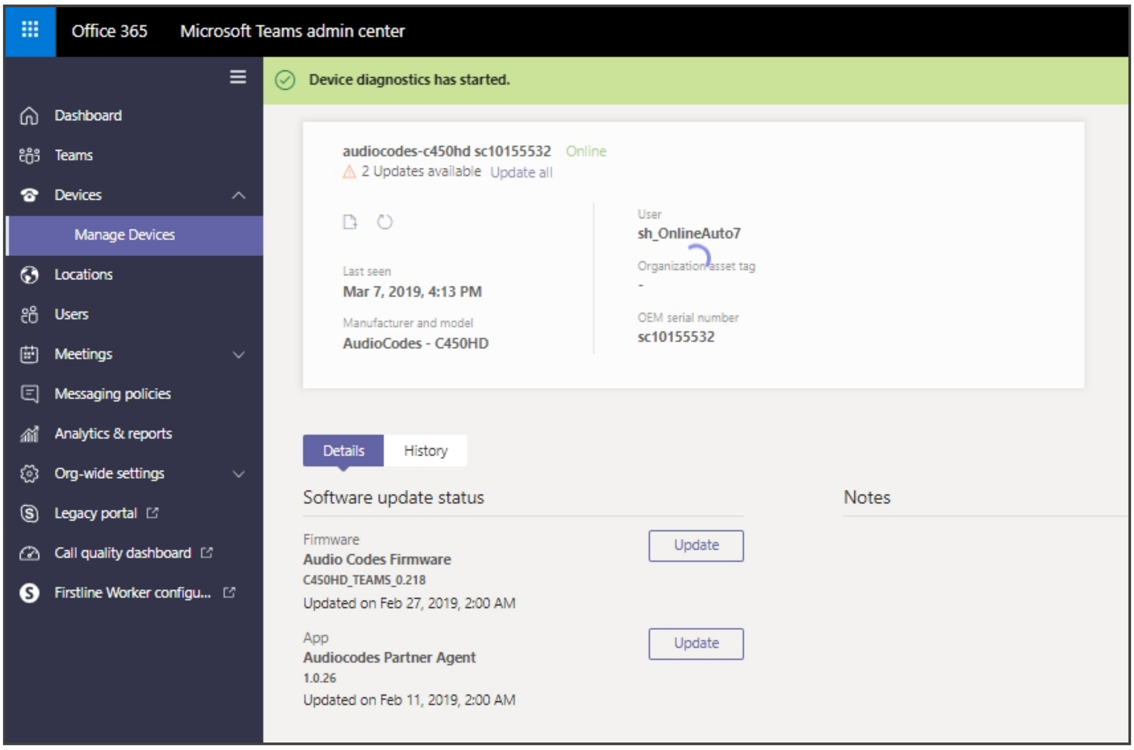
Firmware
Audio Codes Firmware
C450HD_TEAMS_0.218
Updated on Feb 27, 2019, 2:00 AM

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

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

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

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



Device diagnostics has started.

audiocodes-c450hd sc10155532 Online

⚠ 2 Updates available Update all

Last seen
Mar 7, 2019, 4:13 PM

Manufacturer and model
AudioCodes - C450HD

User
sh_OnlineAuto7

Organization asset tag
-

OEM serial number
sc10155532

Software update status

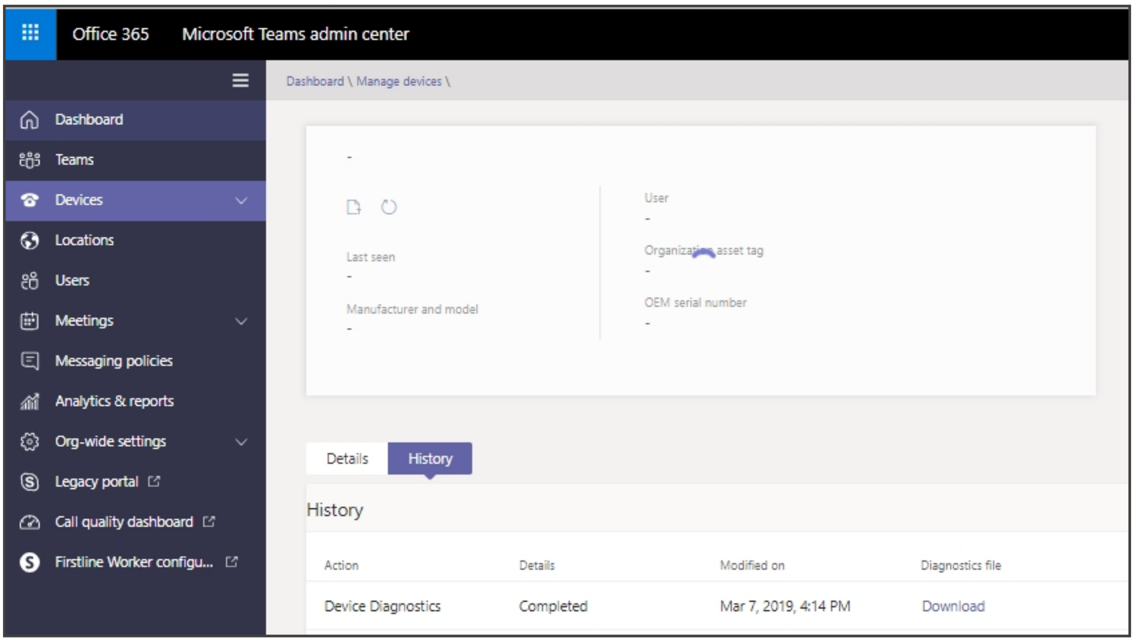
Notes

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

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

4. Click the **History** tab.

Figure 7-6: History - Download



-

Last seen
-

Manufacturer and model
-

User
-

Organization asset tag
-

OEM serial number
-

History

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

Click **Download** to download the logs.

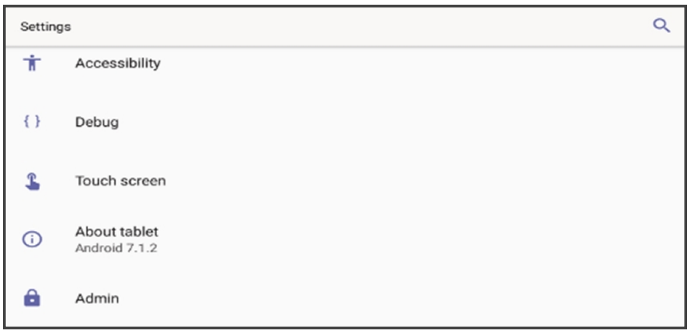
- AudioCodes Device Manager's 'Collect Logs' action also includes all information collected by Microsoft Teams admin center (TAC). The .zip file includes the following files:
  - ✓ Android BugReport
  - ✓ AdminAgentLogs.zip - includes logcat collected by the OVOC/Device Manager.
  - ✓ blog files (media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

Getting Audio Debug Recording Logs

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

➢ To enable Audio Debug Recording logs:

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



Settings

Accessibility

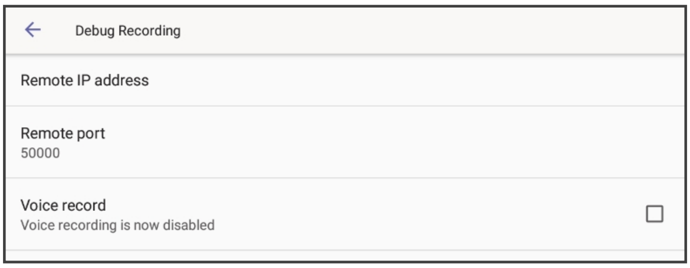
Debug

Touch screen

About tablet
Android 7.1.2

Admin

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



Debug Recording

Remote IP address

Remote port
50000

Voice record ☐
Voice recording is now disabled

4. Configure the remote IP address and port.

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

Collecting Media Logs (*.blog) from the Phone

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

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

1. Access the phone via SSH.

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

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

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

This page is intentionally left blank.

International Headquarters

6 Ofra Haza Street

Naimi Park

Or Yehuda, 6032303, Israel

Tel: +972-3-976-4000

Fax: +972-3-976-4040

AudioCodes Inc.

80 Kingsbridge Rd

Piscataway, NJ 08854, USA

Tel: +1-732-469-0880

Fax: +1-732-469-2298

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

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

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

Document #: LTRT-13436