

C436HD IP Phones

Microsoft Teams Application

Version 2.7



Notice

Information contained in this document is believed to be accurate and reliable at the time of publishing. However, due to ongoing product improvements and revisions, AudioCodes cannot guarantee accuracy of published 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: May-07-2025

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
C470HD-C455HD-C436HD-C435HD-C430HD IP Phones for Microsoft Teams Release Notes
Security Guidelines for AudioCodes' Android-based Devices
Android Device Utility User's Manual
IP Phones How To Video Tutorials

Document Revision Record

LTRT	Description
13426	Initial document release for Version 2.7; ISED warning added; SIP fallback (emergency calling) feature when Teams unavailable; line key assignment; mandatory change of lock PIN; minimum and maximum ring volume; logging Application Not Responding (ANR) error / core dumps; disabling speakerphone; return to previous version; added note to Call Transfer

Notes and Warnings

FCC Caution

Part 15.21

Any Changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

Part 15.19

This device complies with part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

Part 15.105

Note: This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following

measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

FCC RF Radiation Exposure Statement

1. This Transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.
2. This equipment complies with RF radiation exposure limits set forth for an uncontrolled environment.
3. This equipment should be installed and operated with minimum distance 20cm between the radiator & your body.

User manuals for license-exempt radio apparatus shall contain the following or equivalent notice in a conspicuous location in the user manual or alternatively on the device or both.

[EN] This device complies with Industry Canada license-exempt RSS standard(s). Operation is subject to the following two conditions:

- (1) this device may not cause interference, and
- (2) this device must accept any interference, including interference that may cause undesired operation of the device.

[FR] Le présent appareil est conforme aux CNR d'Industrie Canada applicables aux appareils radio exempts de licence. L'exploitation est autorisée aux deux conditions suivantes :

- (1) l'appareil ne doit pas produire de brouillage, et
- (2) l'utilisateur de l'appareil doit accepter tout brouillage radioélectrique subi, même si le brouillage est susceptible d'en compromettre le fonctionnement.

[EN] Radio apparatus containing digital circuitry which can function separately from the operation of a transmitter or an associated transmitter, shall comply with ICES-003. In such cases, the labelling requirements of the applicable RSS apply, rather than the labelling requirements in ICES-003. This Class B digital apparatus complies with Canadian ICES-003.

[FR] Cet appareil numérique de la classe B est conforme à la norme NMB-003 du Canada.

IC SAR Warning

[EN] This equipment should be installed and operated with minimum distance 20 cm between the radiator and your body.

[FR] Lors de l'installation et de l'exploitation de ce dispositif, la distance entre le radiateur et le corps est d'au moins 20 cm.

ISED Warning

[EN] Operation of 5150-5250 MHz is restricted to indoor use only.

This device complies with Innovation, Science, and Economic Development Canada licence-exempt RSS standard(s). Operation is subject to the following two conditions:

- (1) this device may not cause interference, and
- (2) this device must accept any interference, including interference that may cause undesired operation of the device.

Privacy of communications may not be ensured when using this phone.

[FR] Le fonctionnement de 5150-5250 MHz est limité à une utilisation en intérieur uniquement.

Le présent appareil est conforme aux CNR d'Innovation, Sciences et Développement économique Canada applicables aux appareils radio exempts de licence. L'exploitation est autorisée aux deux conditions suivantes :

- (1) l'appareil n' doit pas produire de brouillage, et
- (2) l'utilisateur de l'appareil doit accepter tout brouillage radioélectrique subi, même si le brouillage est susceptible d'en compromettre le fonctionnement.

La confidentialité des communications peut ne pas être garantie lors de l'utilisation de ce téléphone

Radiation Exposure Statement

[EN] The device is compliance with RF exposure guidelines, users can obtain Canadian information on RF exposure and compliance. The minimum distance from body to use the device is 20cm.

[FR] Le présent appareil est conforme Après examen de ce matériel aux conformité ou aux limites d'intensité de champ RF, les utilisateurs peuvent sur l'exposition aux radiofréquences et la conformité and compliance d'acquérir les informations correspondantes. La distance minimale du corps à utiliser le dispositif est de 20cm.

Table of Contents

1 Overview	1
Specifications	1
Migration to Android Open Source Project (AOSP)	3
Allowing URLs, Ports (Security)	4
Security Guidelines for Android-based Devices	4
2 Setting up the Phone	5
Unpacking	5
Device Description	6
Front View	6
Rear View	10
Cabling	11
Mounting the Phone	11
Before Using AudioCodes Devices	11
3 Starting up	12
Configuring Device Settings	12
Configuring VLAN via DHCP Option when CDP-LLDP isn't Allowed	16
Restoring the Phone to Default Settings	17
Performing a Hard Restore	18
Performing a Soft Restore	18
Performing User Data Reset	18
Recovery Mode	18
Locking and Unlocking the Phone	18
Automatic Lock	19
Unlock	19
4 Performing Teams Call Operations	20
Making a Call	20
Dialing a Missed Call	20
Select to Dial	20
Configuring Speed Dials	20
Transferring a Call	22
Making an Emergency Call	23
Answering Calls	23
Ending an Established Call	23
Managing Calls	23
Paging to a Group of Phones (Multicast)	24
Transferring a Call to Frequent Contacts	26
Transferring a Call to Work Voicemail	26
Viewing and Playing Voicemail Messages	26
Rejecting an Incoming Call, Sending it Directly to Voicemail	26
Adjusting Volume	27

Adjusting Ring Volume	27
Adjusting Tones Volume	27
Adjusting Handset Volume	27
Adjusting Speaker Volume	28
Adjusting Headset Volume	28
Playing Incoming Call Ringing through USB Headset	28
Assigning a Line Key for Speed Dial or Features	28
5 Performing Administrator-Related Operations	34
Setting up Automatic Provisioning	34
Enabling Users to Make Calls even if Teams is Unavailable	35
Applying a Partial Configuration Profile	37
Configuring an Option to Force Users to Change their Device Lock PIN	37
Configuring Minimum and Maximum Ringer Volumes via the Phone's Configuration File	39
Manually Performing Recovery Operations	40
Defining Password Complexity	41
Disabling a Device's USB Port	42
Disabling the Phone's Speaker Hard Key	42
Configuring Time Zone on Teams Devices	44
Configuring QoS on PC Port	44
Configuring Admin Login Timeout	45
Monitoring Phone Process Statuses	45
6 Troubleshooting	46
Network Administrators	46
SSH	46
Getting the Phone IP Address	46
Installing the APK using SSH	47
Updating Phones using SSH Commands	47
Microsoft Teams Admin Center	48
Collecting Logs	48
Getting Audio Debug Recording Logs	51
Collecting Media Logs (*.blog) from the Phone	52
Encountering an ANR Error - Core Dump	52
Retrieving Bug Report Automatically Produced if 'Boot Reason' is FATAL or PANIC	52
Return to Previous Version	53

1 Overview

The AudioCodes C436HD IP phone is a Microsoft Teams-native low cost phone (LCP) designed to support the next generation of enterprise collaboration technologies. Equipped with a 4.3" color LCD screen, the C436HD supports Microsoft Teams out-of-the-box to deliver feature-rich unified communications.

AudioCodes IP phones are offered as part of a comprehensive Managed IP Phone solution, defined as an IT-managed entity that delivers end-to-end lifecycle management of edge devices.

C436HD Features:

- Crystal-clear sound
- Native support for Microsoft Teams
- USB headset support
- Firmware upgrade via USB stick

IP Phone Series Highlights

- Superior voice quality
- Full duplex speaker phone
- Robust security mechanisms
- PoE or external power supply
- Centralized management using the AudioCodes One Voice Operations Center (OVOC) Device Manager

Specifications

The following table summarizes the phone's specifications.

Table 1-1: 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

Feature	Details
	■ 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) ■ 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 Support	■ Multi-lingual support; the language pack list is not yet final and is subject to modification.
Hardware	■ Graphic 4.3" color screen, 480x272 resolution ■ Integrated sidecar 12 BLF keys and non-touch monochrome 5.4" LCD 376 x 60 resolution ■ Wired connectivity: ✓ Two RJ-45 [Gigabit Ethernet (GbE)] (10/100/1000BaseT Ethernet) ports: LAN and PC port ✓ USB port for USB headset ✓ RJ-11 interface

Feature	Details
	■ SOC – RockChip PX30 ■ Power: ✓ 12V DC jack ✓ Power supply AC 100 ~ 240V ✓ PoE Class 2: IEEE802.3af (optional) ■ Keys: ✓ Illuminated VOICE MAIL message hotkey ✓ 6 function/programmable keys around the main LCD with red/green backlight ✓ 12 BLF keys next to the sidecar LCD with red/green backlight ✓ 4-way navigation button with OK key ✓ MENU ✓ HOLD ✓ Illuminated MUTE hotkey ✓ TRANSFER ✓ VOLUME control key ✓ Illuminated HEADSET hotkey ✓ Illuminated SPEAKER hotkey ✓ BACK ✓ CONTACTS ✓ AC (AudioCodes) (including white LED) ■ Storage / Memory ✓ 8GB / 16GB eMMC (Flash) ✓ 2GB DDR2 (Memory)

Migration to Android Open Source Project (AOSP)

Migration to Android Open Source Project (AOSP) is supported. Intune offers an AOSP mobile device management (MDM) solution referred to as AOSP Device Management. This MDM platform is used for Teams Android-based devices that enroll in Intune, replacing Android Device Administrator. AOSP Device Management leverages a new agent and Authenticator app, eliminating dependencies on the Company Portal app.

An *AOSP Migration Guide* for Android AOSP Management for Microsoft Teams Android devices can now be obtained on Microsoft Learn [here](#).

The guide provides customers with detailed instructions and best practices for a smooth migration. It also shows how to migrate Teams Android devices to AOSP Device Management.

All migration actions are performed in the Microsoft Intune Company Portal. Phone firmware has been upgraded with the Authenticator app.

Allowing URLs, Ports (Security)

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

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

Table 1-2: URLs / Ports to Allow when Deploying 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)

Security Guidelines for Android-based Devices

For security guidelines for AudioCodes native Teams Android-based devices, refer to the document [Security Guidelines for AudioCodes Native Teams Android-based Devices](#).

2 Setting up the Phone

The following instructions 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, refer to the phone's *Quick Guide* (scan the barcode on the box in which the phone was shipped or see [Related Documentation](#) on page iii).

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

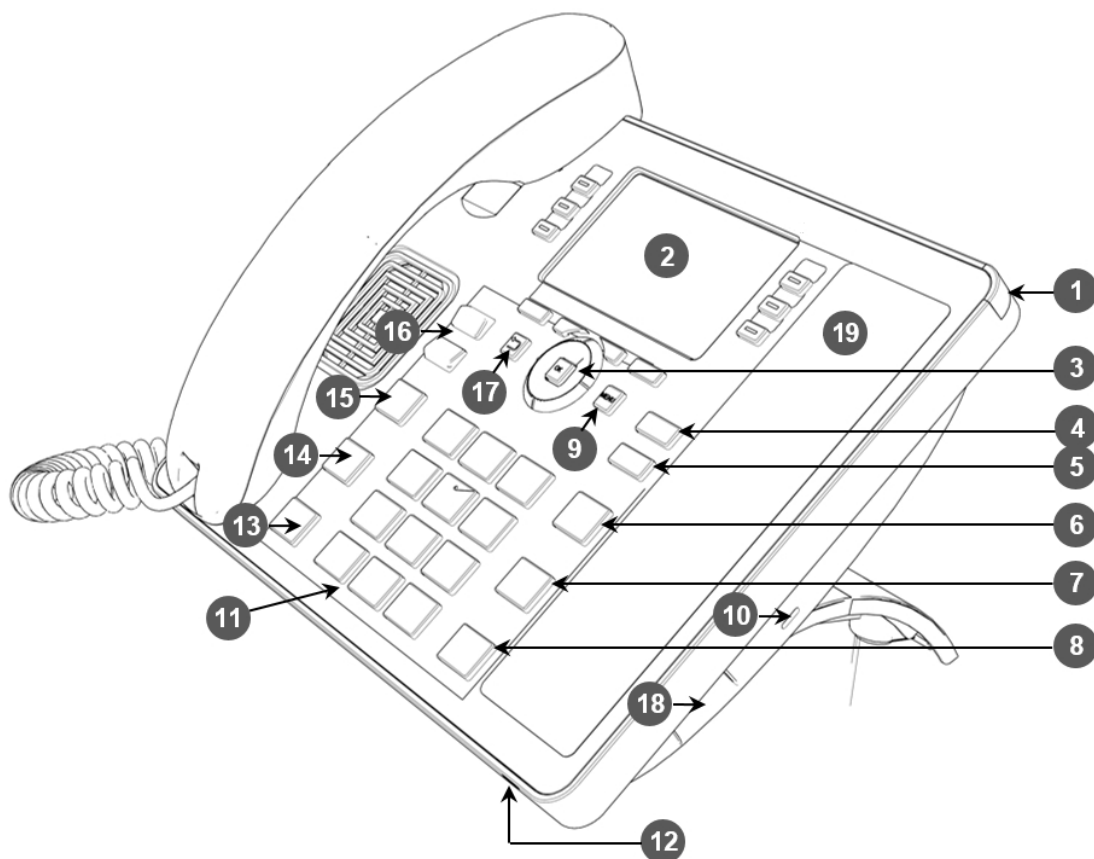


Table 2-1: Font View Description

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	Smart Button	Returns the phone to the 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	Alphanumeric 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.
19	Sidecar	Twelve speed dial buttons to quickly call contacts whose names are displayed adjacent to them. Configure these speed dial buttons as shown here .



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 ✓ key on the control button

Rear View

Cabling

For detailed information on how to cable the phone, refer to the phone's *Quick Guide* (scan the barcode on the box in which the phone was shipped or see [Related Documentation](#) on page iii).

Mounting the Phone

You can desktop or wall mount the phone. For detailed information on how to mount the phone, refer to the phone's *Quick Guide* (scan the barcode on the box in which the phone was shipped or see [Related Documentation](#) on page iii).

To view a video showing *the principle* of how to mount an AudioCodes IP phone, click [here](#). The principle is the same across all AudioCodes IP phone models.

Before Using AudioCodes Devices

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

➤ To clean a device's screen:

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

3 Starting up

Here's how to start up the phone.

➤ **To start up:**

1. Connect the phone to the network (or reset it); the language selection screen is displayed by default.
2. Select the language of your choice and then configure device settings to suit specific requirements.



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

Configuring Device Settings

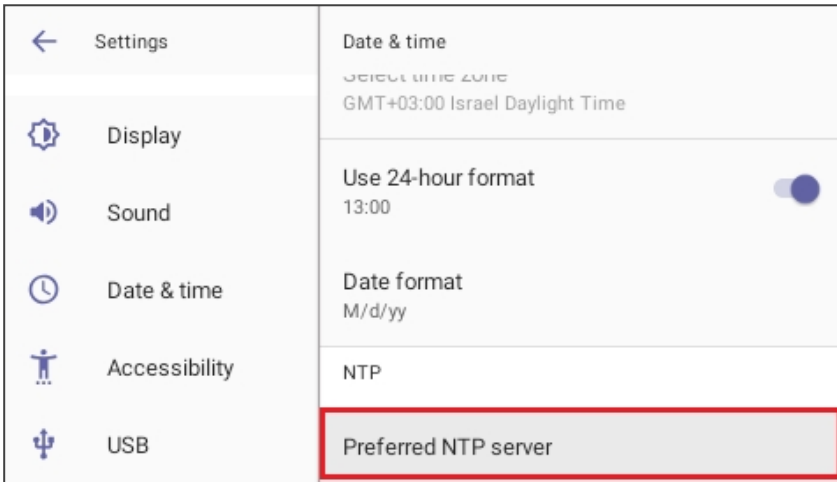
The section familiarizes you with the phone's settings. Phones are delivered to customers configured with their default settings. Customers can customize these settings to suit specific personal or enterprise requirements.

➤ **To access device settings:**

1. 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].

Table 3-1: Device Settings

Setting	Description
User	
Display	Opens the 'Display' screen [Brightness level]. The phone's screen supports different brightness levels. Choose the level that suits your requirements. ■ Sleep ■ Screen saver
Sound	Allows you to customize phone volume for a friendlier user experience. Ring volume at n%
Date & time	Date and time are automatically retrieved from the deployed Network Time Protocol (NTP) server. Use 24-hour format [Allows you to select the Time format] Also supported is a simplified version of NTP called Simple Network

Setting	Description
	Time Protocol (SNTP). Both can be used to synchronize device clocks. SNTP is typically used if full implementation of NTP is not required.
NTP Preferred NTP server	Admins can use this parameter to <i>manually</i> define the NTP server, to comply with enterprise security requirements if those requirements preclude using DHCP Option 42. Manual configuration takes precedence over DHCP Option 42 and the time servers. Two ways to manually define the NTP server are available: - Admins can define it in the phone's GUI.  - Admins can alternatively use the newly added parameter 'date_time/ntp/server_address' in the phone's .cfg configuration file. See also under here.
Power Saving	Allows users to contribute to power saving in the enterprise. Enable power saving Start time [The device consumes minimal energy before the user arrives at the office] End time [The device consumes minimal energy after the user leaves the office]
Debugging	Enables users to reboot the device. Log in as Administrator for more debugging settings to be available.
Languages & input	Allows users to customize inputting to suit personal requirements.
About	Provides users with device information. To determine the device's IP address, select the 'Status' option. To get information about the version, select 'Version info'.

Setting	Description
	To get information about the Android version, select 'Android version'.
Device administration	Allows the user to log in as Administrator, necessary for some of the debugging options. It is password protected. Default password: 1234. After logging in as an Administrator, the user can log out change password. Select Login and then in the Login screen that opens, select the 'Enter password' field and use the virtual keyboard to enter the password . 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.  • 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. • 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 .
Modify network	Enables the Admin user to determine network information and to modify network settings. IP Address [Read Only] IP Settings [DHCP or Static IP] Network state [Read Only] Enable PC port

Setting	Description
	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.
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. 2. From the 'EAP method' drop-down, select the method: MD5 or TLS (for example).  In version 2.3, the option for non-validating a CA certificate was removed. 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 802.1x. The 802.1x settings available in the Configuration File are: ■ Enable/Disable ■ EAP method ■ Identity

Setting	Description
	■ Password
VLAN Settings	Select the menu option VLAN Settings. Select VLAN Discovery mode. ■ 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:
Debugging	Allows the Admin user to perform debugging for troubleshooting purposes. Available after logging in as Admin. Log settings Remote Logging (see under Remote Logging for more information) Diagnostic Data (see under Diagnostic Data for more information) Reset configuration (see here for more information) User data reset Restart app Debug Recording (for Media/DSP debugging) (see under Remote Logging for more information) Erase all data (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 application.

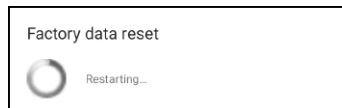
Two kinds of restore are available:

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

Performing a Hard Restore

➤ 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 for more information).

Performing a Soft Restore

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

➤ To perform a soft restore:

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

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.

- To lock the phone:

Unlock

4 Performing Teams Call Operations

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

Making a Call

Dialing a Missed Call

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

➤ To dial a missed call:

Select 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.

Configuring Speed Dials

You can configure a speed dial in one of two ways:

- Through Teams desktop client.
- Via call logs on the phone (see below).

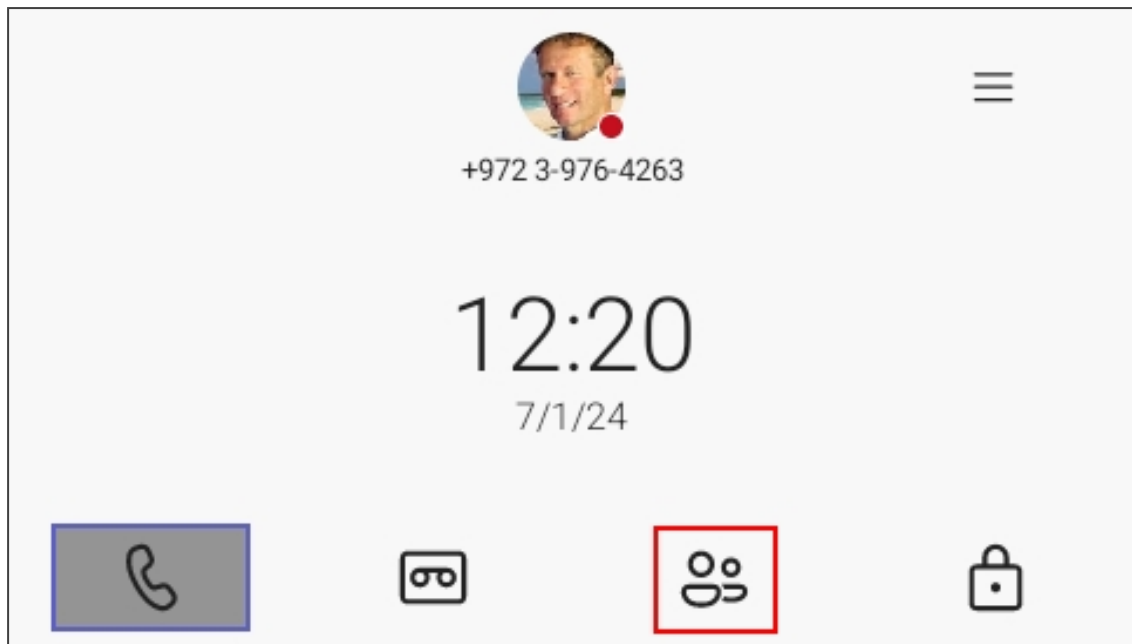
➤ To configure a speed dial:

➤ To configure a speed dial group to display on the sidecar:

Speed dials are private. They are for each users personal use and are preserved even if you sign out.

Each of the 12 buttons on the phone's sidecar can be configured as a speed dial. These enable the user to place a call to a contact at the press of the button.

1. Go to the phone's home screen (press the **Smart Button** on the phone's physical interface).



2. Navigate to **Speed dial**:



3. Select the contacts you want to add to your speed dial group.
4. The speed dial group displays in the side car:

Alex Strizheusky
Eli Carciente
Eli Shoual
Eliezer Davila
Elyasaf Bar Haim
Home
Maxim Geller
Meron F12
Moriya Sharabi
Nati Davidi
Nir Pardo
Oleg Friedman

Transferring a Call



During a call, you can also transfer the call using the device's physical **Transfer** button:

- Short press – opens a dialog to select a contact to transfer the call immediately.
- Long press – opens a dialog to select a contact for consultation before completing the transfer.

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)

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

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

Rejecting an Incoming Call, Sending it Directly to Voicemail

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

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

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

Adjusting Volume

The phone allows

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

For more information about sound and volume, see [here](#).

Adjusting Ring Volume

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

➤ **To adjust ring volume:**

1. When the phone is in idle state,
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. 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. 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. 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.

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

- Configure the following parameter:

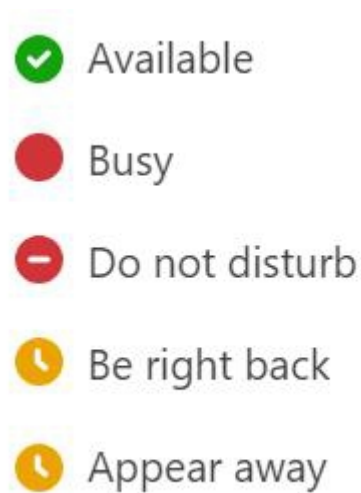
audio/stream/ringer/0/audio_device=**BOTH** (default), **BUILTIN_SPEAKER** or **TYPE_USB**

- **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.

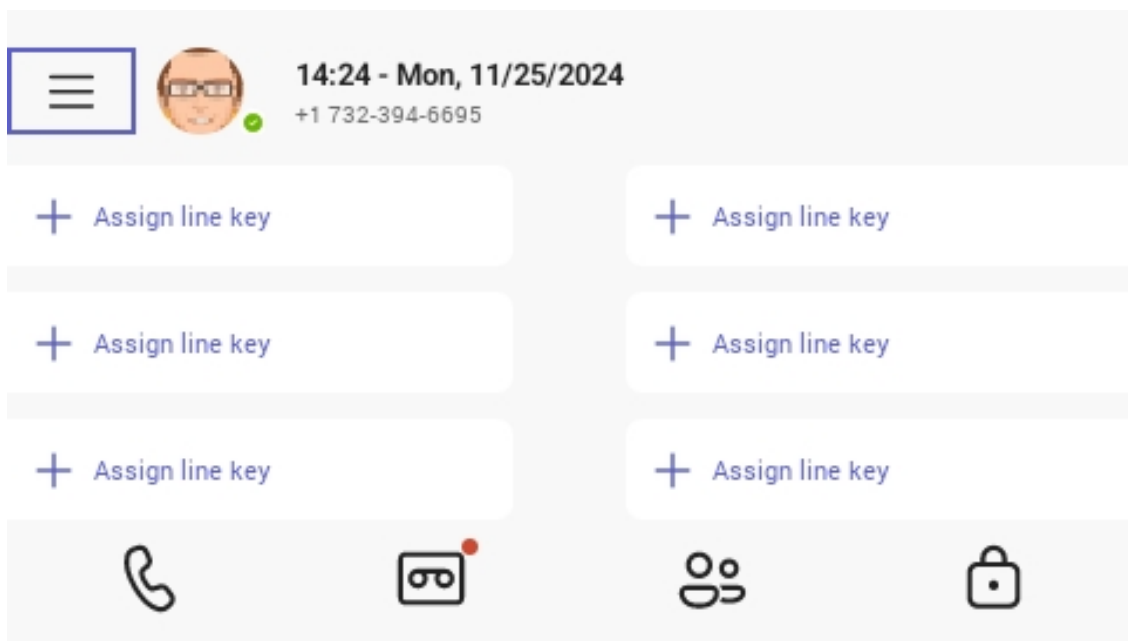
Assigning a Line Key for Speed Dial or Features

Line keys provide quick access to features like redial and voicemail. You can also assign predefined functions or people to line keys and label them for speed dial.

The presence/ status of a contact displays by their name (account avatar) in the LCD home screen:

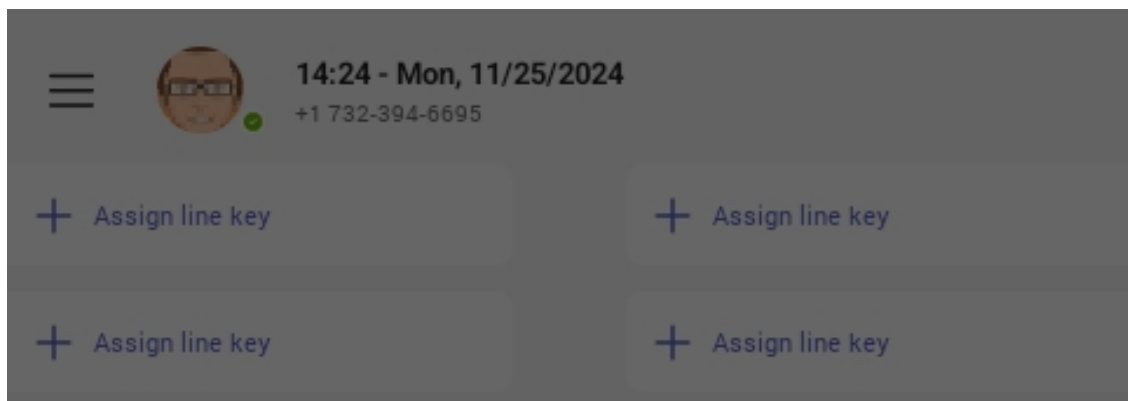


The LCD home screen displays an 'Assign line key' option:



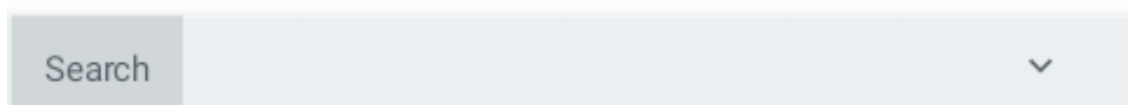
➤ **To assign a line key:**

1. Use the navigation control to navigate to the 'Assign line key' you want to associate with a named person.
2. Press the tick button on the navigation control to select; the assign key menu displays:

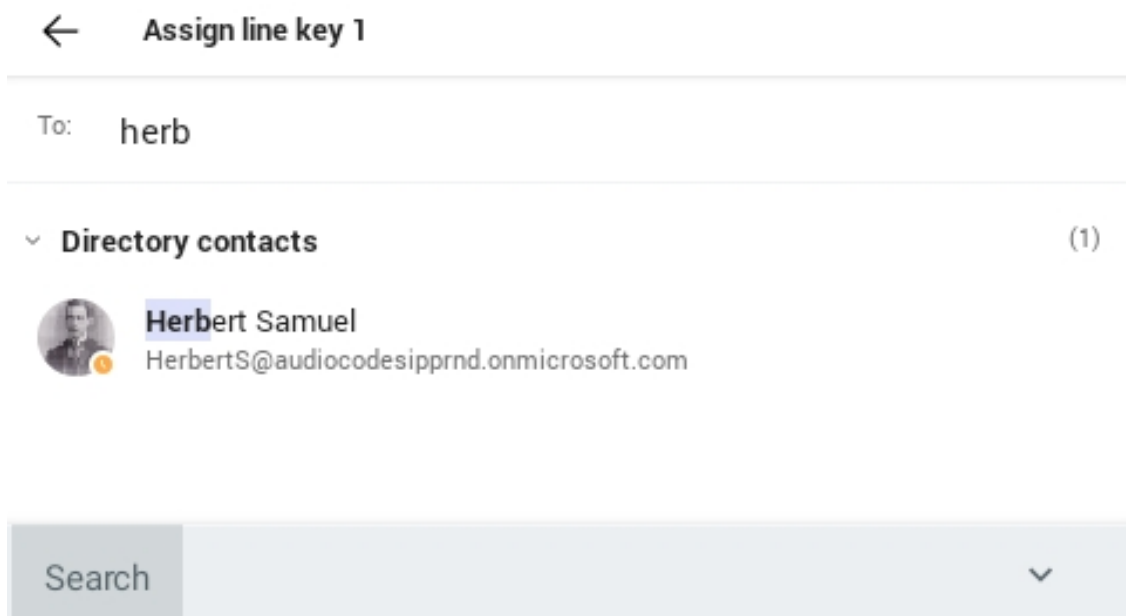


-  Assign line key
-  Manage line keys

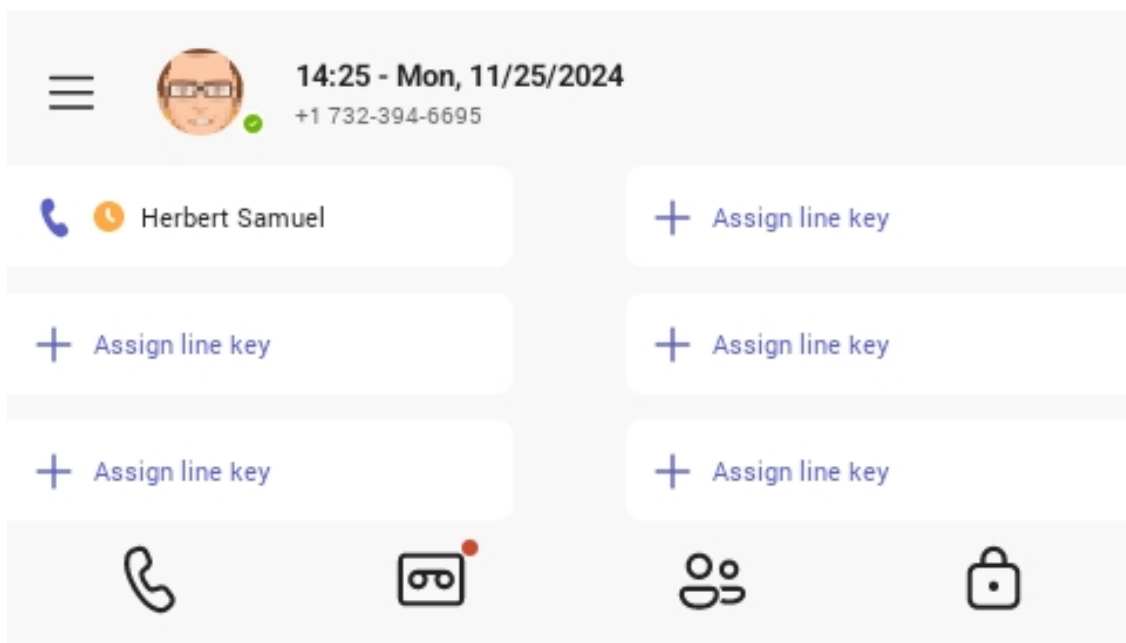
- Press the tick button again and use the dial pad to spell out the first couple of letters to 'Search for people':



- Use the navigation control to navigate to the contact you wish to select. Press the tick button. The searched name displays in full:

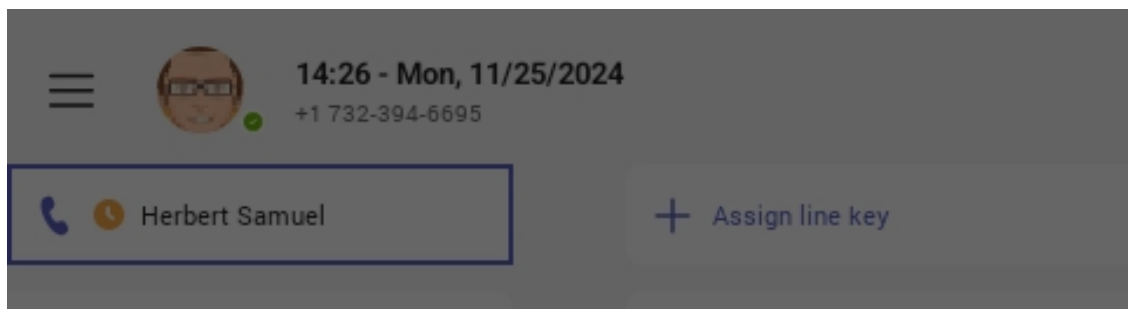


5. Press the navigation control tick button to confirm. The screen displays the assigned line:



➤ **To reassign or unassign a line:**

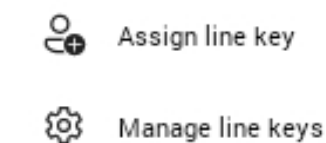
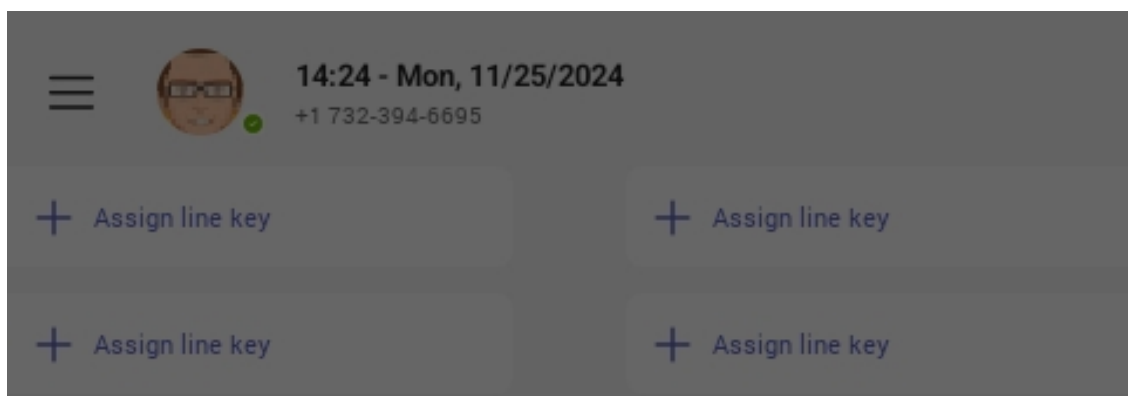
1. Press the softkey to display the menu:



2. Use the navigation control to select 'Reassign line key' or 'Unassign line key'. If you select 'Reassign line key', follow [these steps](#).

➤ **To reformat the LED assign screen:**

1. Follow [these steps](#) and then navigate to 'Manage line keys':



2. Press the tick button. The format options display:

Mon, 25 Nov	14:26
Left Column	>
Right Column	>

← Manage line keys

3. Use navigation control to select the field you want to format and then press the tick button.
4. You can now assign a line or delete a contact from a line.

Mon, 25 Nov	14:26
Line Key 1	Herbert Samuel 
Line Key 2	+
Line Key 3	+

← Manage line keys

5 Performing Administrator-Related Operations

Network administrators can:

Update phone firmware manually (see [Update Phone Firmware Manually](#))

Manually perform recovery operations (see [Manually Performing Recovery Operations](#) on page 40)

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

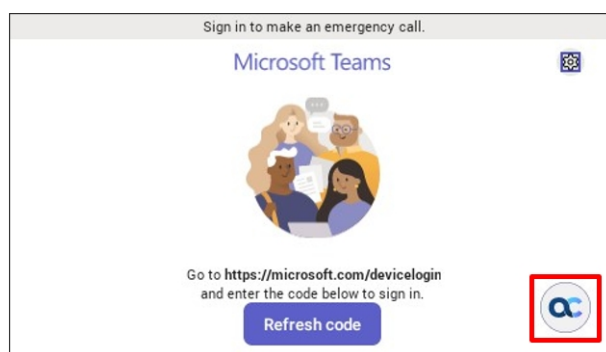
It can be reconfigured if required.

Enabling Users to Make Calls even if Teams is Unavailable

A fallback feature enables users to make calls even if Teams is unavailable. If Teams is unavailable, the device will still have connectivity to the internet via the SBC using a SIP-based application.

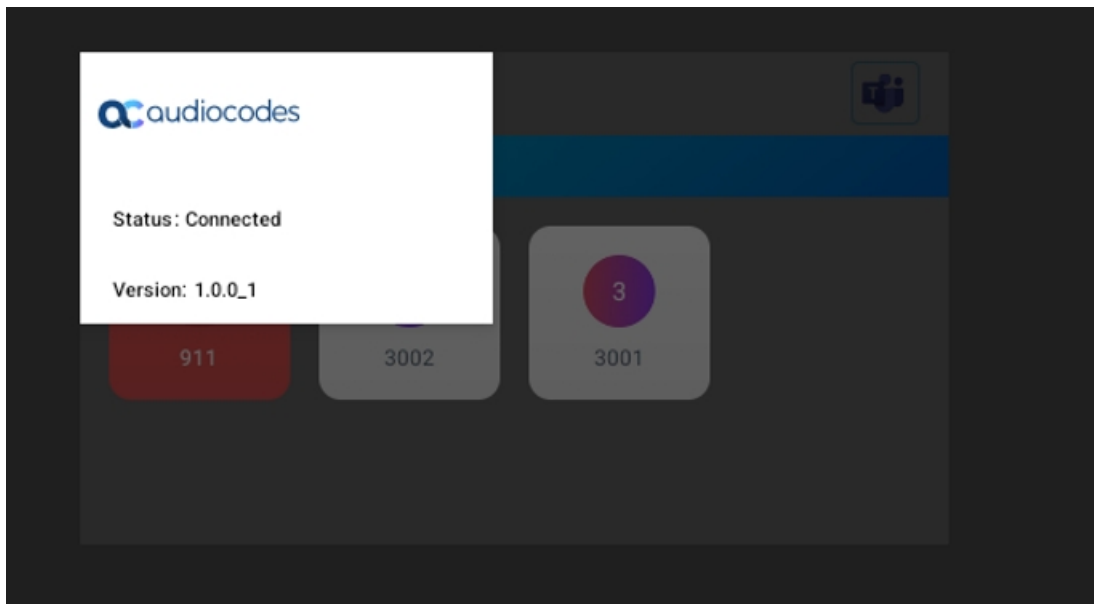
➤ **To enable it, admin must:**

1. Set parameter 'system/ace/shortcut_enabled' to **1** (default = **0**); an AC soft button is then displayed in the lower right corner of the phone screen (if Teams is unavailable) as shown here:



➤ **To register a SIP account (sign in), admin must:**

1. Set the following parameters:
 - personal_settings/sip/server =wss://<SBC URL>
 - personal_settings/sip/port ="SBC server port", e.g., 443
 - personal_settings/sip/domain =<domain name>
 - personal_settings/sip/username="account name"
 - personal_settings/sip/password="account password"
2. View 'Connected' if the account status is registered. View 'Not Connected' if the account status is not registered.



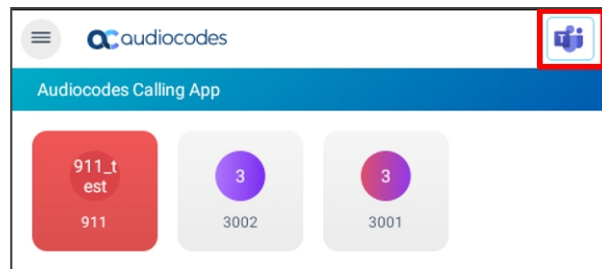
➤ **To enter the app, the user must:**

- Press the **AC** button to switch to the app. To switch back to Teams, press the Teams button as shown in the figure below the next.



➤ **To add (up to) 41 speed dial keys, admin must:**

1. Use the following parameters:
 - `personal_settings/functional_key/[0-40]/speed_dial_number= "the destination"`
 - `personal_settings/functional_key/[0-40]/type = DEFAULT` (button retains its Teams color) -or- `EMERGENCY` (button is colored red)
 - `personal_settings/functional_key/[0-40]/display_name= "destination display name"`



➤ **To make a call, the user must:**

1. View the phone's calling screen:
2. View the phone's incoming call screen:
3. [Optionally] During the call, the user can adjust the volume, mute, unmute, DTMF, switch audio source, etc.



- The app blocks incoming calls when Teams is in the foreground.
- When Teams is available and the app is in the foreground in idle state, the phone cannot get an incoming Teams call.
- After rebooting, the device always displays the Teams home screen.

Applying a Partial Configuration Profile

Configuration profiles enable admin to simultaneously assign several settings to multiple Android devices. Different types of settings are supported, e.g., general settings, device settings, network settings applied to the device through a partner agent, and meeting settings applied on the Teams app.

When admin assigns a configuration profile to a device, not all settings that are part of that profile are applied to the device. Settings on the device that were configured by the user are not overridden. Admin can change a particular setting without overriding the other setting values defined by the user.

Configuring an Option to Force Users to Change their Device Lock PIN

Historically, users have always been provided with an option to lock their device, but in addition, *admin* can configure an option to *force users to change their device lock PIN*.

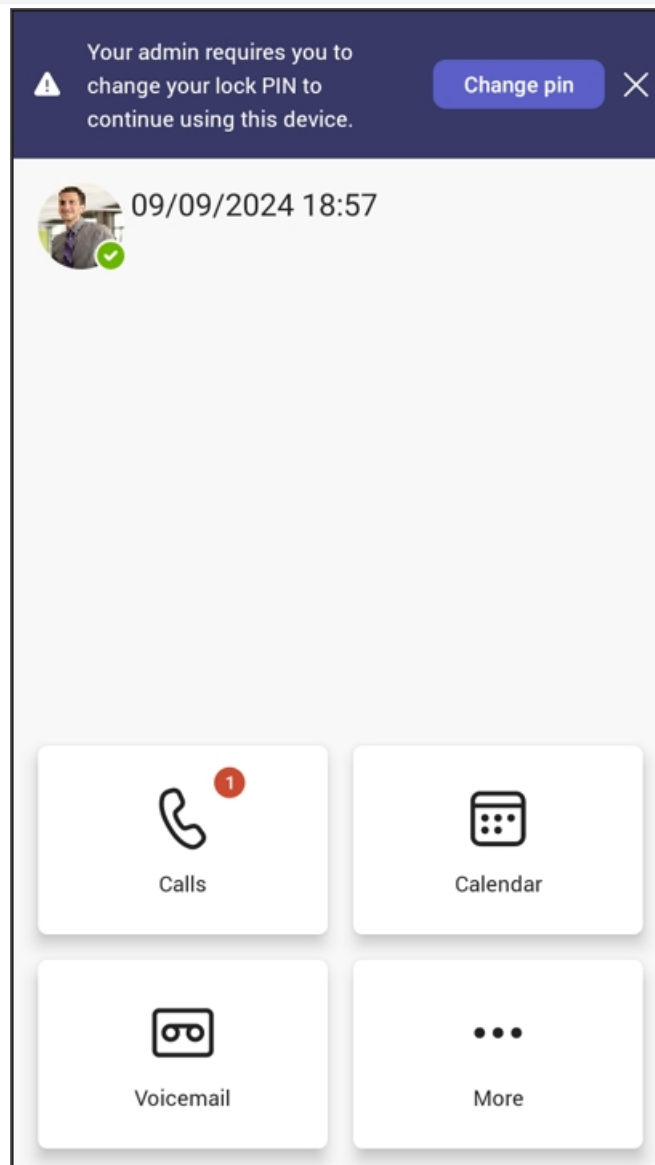
➤ **To force users to update their device lock PIN admin must:**

1. Configure the configuration file parameter 'forceChangePIN'.

```
System Config
Lock PIN: 123445
```

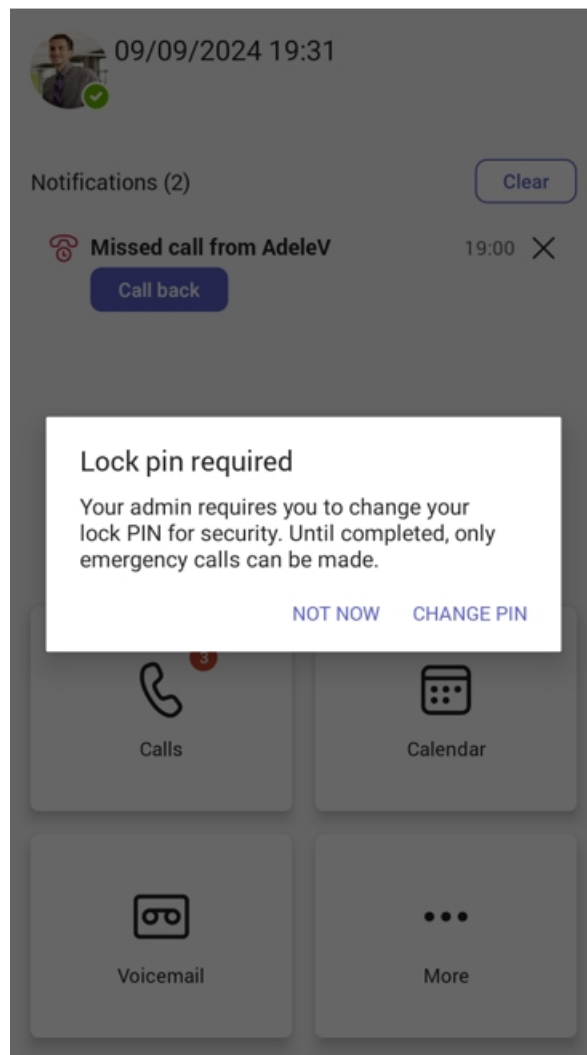
Device Lock Timeout: 600

Date Time Config: test



- The same principle applies across all phone models, only the screen dimensions change.
- The configuration option is received as part of the configuration profile settings assigned to the device.
- Once timeout configured by admin lapses, firmware locks the device.

2. When the Teams app detects a PIN lock configuration where a force PIN configuration is toggled, a popup is displayed allowing the user to navigate to device lock settings to change the PIN.



3. If the user clicks **CHANGE PIN**, they can navigate to Device Settings to reset the PIN.
4. If the reset PIN configuration times out and the user has not changed their PIN, the device is locked by the Teams app and the user is restricted to emergency calls along with the set PIN notification.

Configuring Minimum and Maximum Ringer Volumes via the Phone's Configuration File

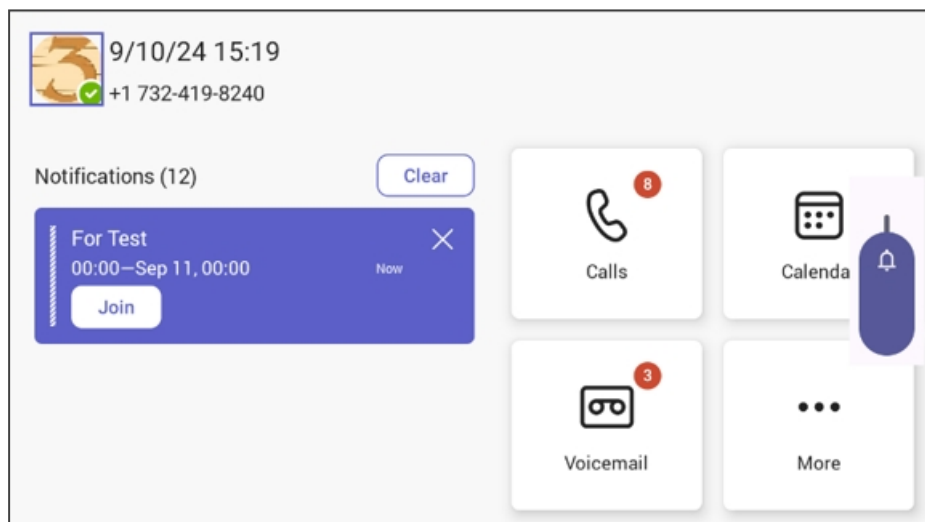
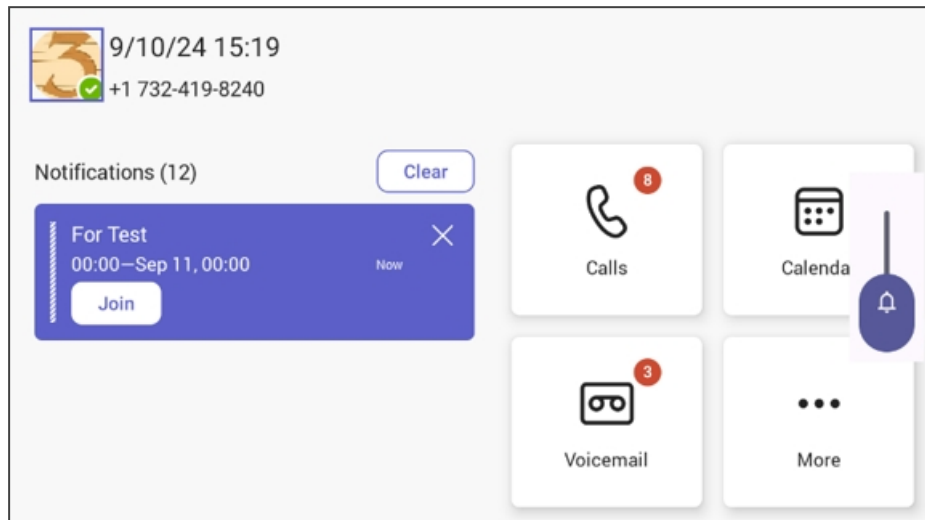
Android phones feature a capability enabling admin to configure minimum and maximum ringer volumes via the phone's configuration file. The feature complies with industrial customers' requirements for phone ringers to be louder and for admin to be able to stop users from reducing ringer volume to too low.

➤ To configure maximum and minimum volume:

1. Set the configuration file parameter 'audio/ringer/volume_max' to **10**.
2. Set the configuration file parameter 'audio/ringer/volume_min' to **0**.



- Ringer volume by default has a range of **0-10**, where **0** is mute.
- The capability allows admin to define a *new minimum | maximum range of 3-7* so that the user will be able to reach a minimum of **30%** and a maximum of **70%** of the original **0-100%** range as shown in the figures below. The same principle applies to all phone models. Only screen dimensions vary.



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.



While a device is powering up, you can perform recovery operations

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

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.

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.

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



- 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.

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.

Disabling the Phone's Speaker Hard Key

The speaker hard key on the phone can be configured to be disabled so that in an office environment, the user won't have the option to use the speaker. Speaker functionality will then be disabled during calls. Pressing the hard key will have no impact and its light will not illuminate. Only use of the handset and headset will be enabled.

The feature complies with requests from customers in whose offices discretion is important (e.g., government).

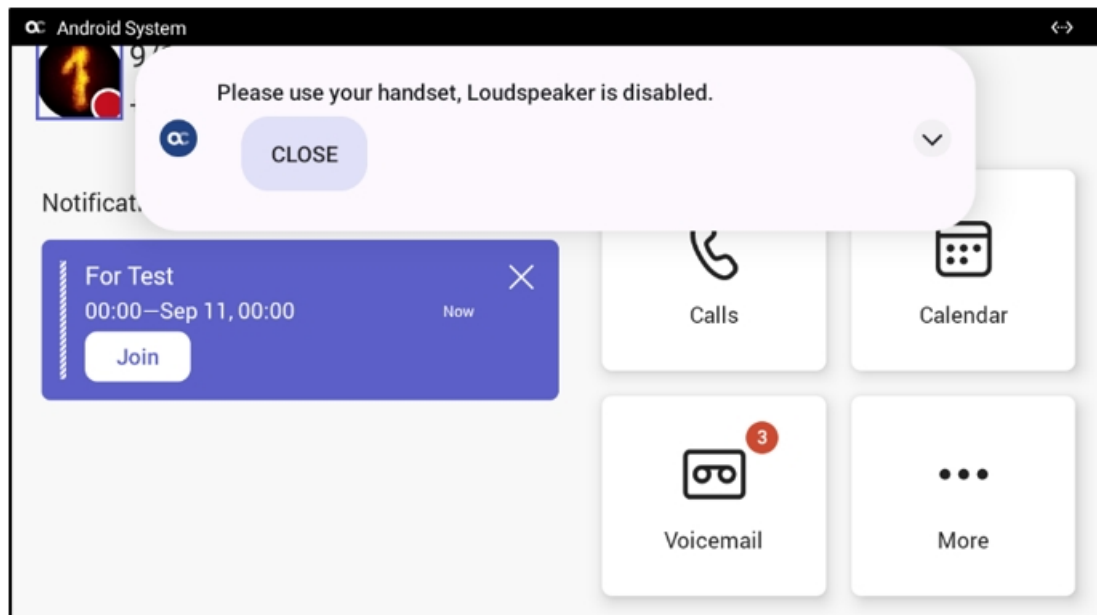
➤ To configure the speaker hard key on the phone to be disabled:

1. Configure the configuration file parameter 'audio/speakerphone/enable' to:
 - **0** = Disable (default)
 - **1** = Enable

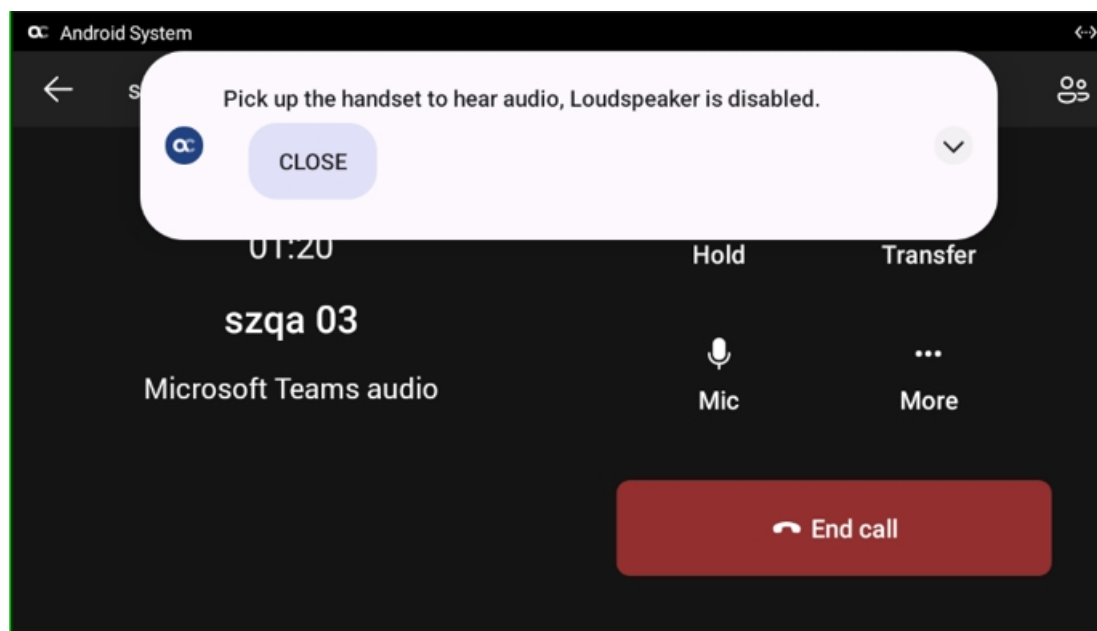


Ring to speaker still functions.

2. If after the feature is enabled the user presses the 'Speaker' button in the idle screen, the following popup message is displayed in the phone screen:



3. If after the feature is enabled the user presses the 'Accept' softkey or the speaker hard key, the following popup message is displayed in the phone screen:



4. The user can then answer by picking up the handset or by putting on the headset if a USB headset is connected. The popup indication then disappears.

Configuring Time Zone on Teams Devices



- AudioCodes recommends using Geolocation as the time zone configuration method.
- Geolocation is the default setting, if no other changes to the time zone settings are made, the device retrieves the time from it's geographical location.



Manual time zone setting is NOT recommended. Choosing a time zone manually may cause retrieval of the incorrect time zone, and cause functionality issues.

You can configure the time zone using one of the following methods, which are listed in order of preference for best performance:

■ Geolocation (Default):

- The default geolocation method uses a devices public IP address to obtain it's location. If the devices are behind NAT they are using STUN server to discover their public IP addresses.
- A common STUN server example is Google's publicly accessible server: `stun.l.google.com:19302` (default URL).

■ DHCP Option 100/101 (posix/tzdbx):

- Configuration is obtained from DHCP server.

■ Admin Provisioning:

Use one of the following:

- Teams Admin Center, created under configuration profile.
- Device Manager, created in configuration parameters setup.

The supported parameters for Device Manager configuration can be found in product specific Admin and User guides. For Teams Admin Center refer to Microsoft documentation > Configuration profile.

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
<code>network/lan/vlan/pc_port_tagging/enable=0</code>	Defines the PC port VLAN as enabled / disabled.

Parameter	Description
	■ 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**).

6 Troubleshooting

The information presented here shows how to troubleshoot AudioCodes devices.

Network Administrators

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

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.
- 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
- Deactivating DSP Recording

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/.apk**

For example use the following:

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

2. Update the APK using the following:

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

3. Delete the old APK using the following:



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:

```
param_tool scp 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

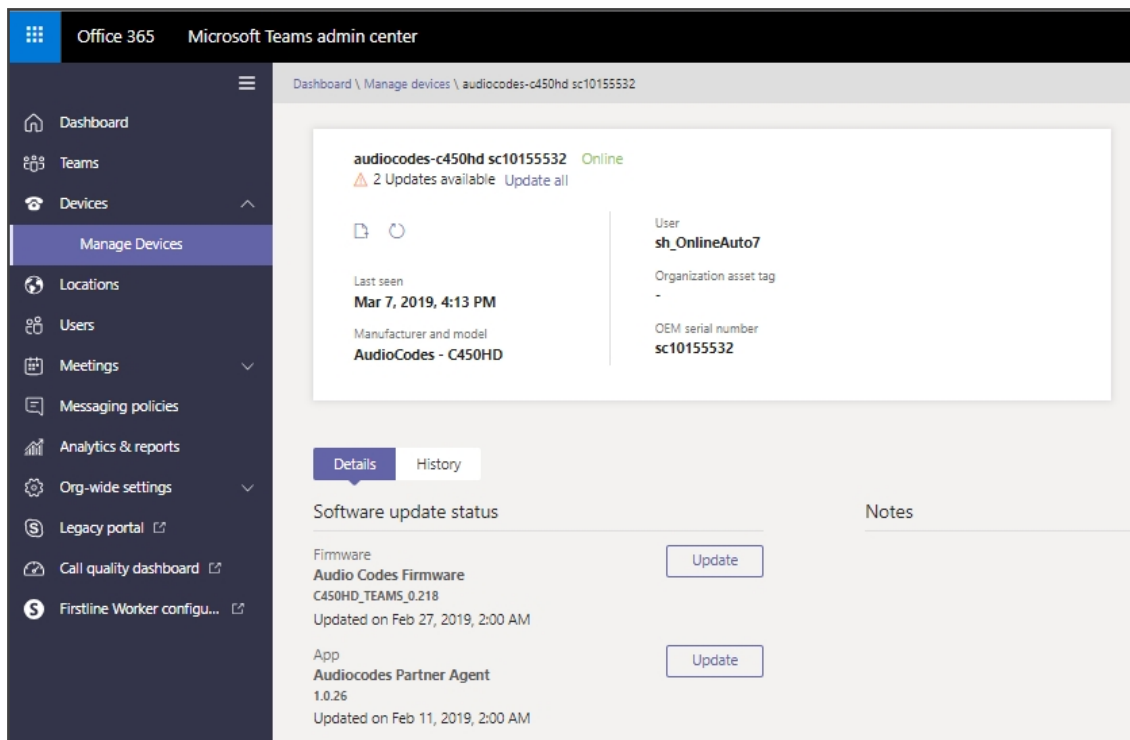
The Microsoft Teams Admin Center allows network administrators to troubleshoot issues encountered with the phone.

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.

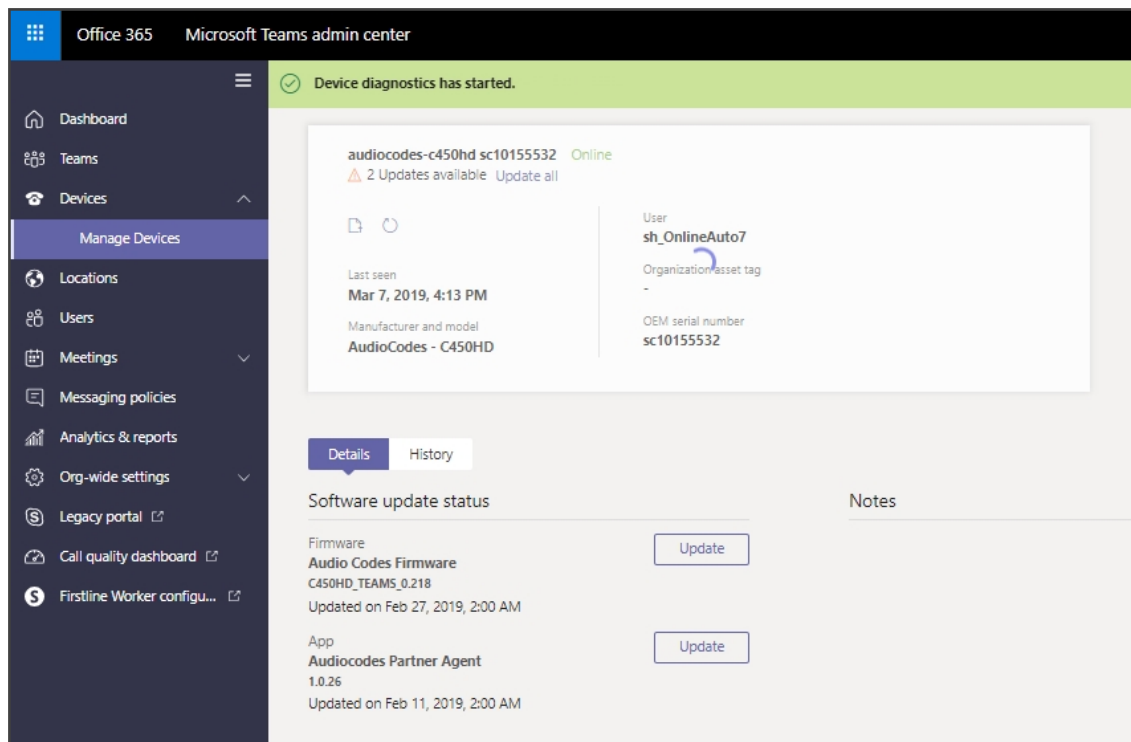
➤ **To collect logs:**

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

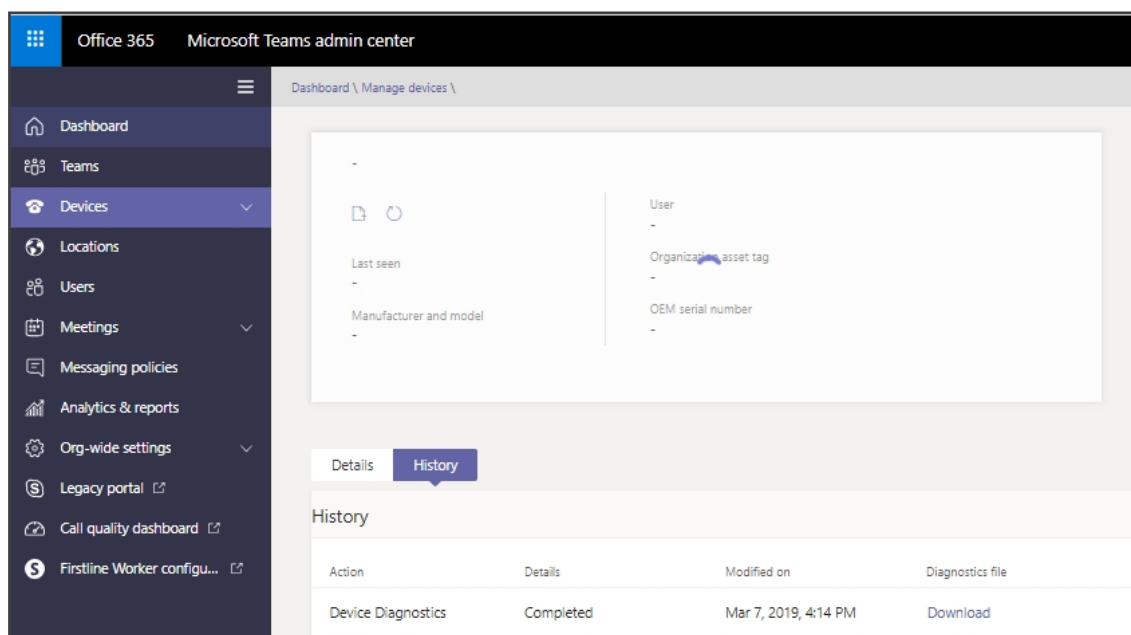
Figure 6-1: Microsoft Teams Admin Center - Diagnostics

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

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

Figure 6-2: Microsoft Teams Admin Center – Logs Upload to Server

4. Click the **History** tab.

Figure 6-3: History - Download

Click **Download** to download the logs.



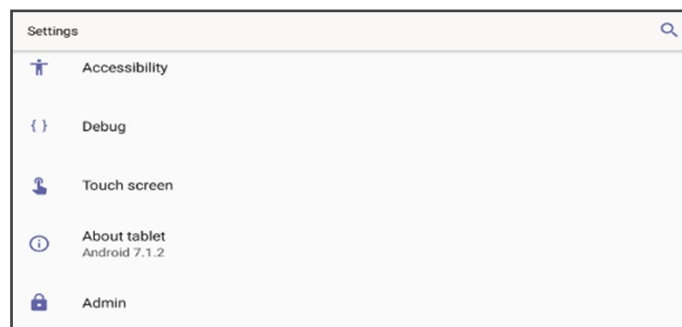
- AudioCodes Device Manager's 'Collect Logs' action also includes all information collected by Microsoft Teams admin center (TAC). The .zip file includes the following files:
 - ✓ Android BugReport
 - ✓ AdminAgentLogs.zip - includes logcat collected by the OVOC/Device Manager.
 - ✓ blog files (media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

Getting Audio Debug Recording Logs

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

➤ To enable Audio Debug Recording logs:

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



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



4. Configure the remote IP address and port.

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

Collecting Media Logs (*.blog) from the Phone

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

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

1. Access the phone via SSH.



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

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

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

Encountering an ANR Error - Core Dump

If an Application Not Responding (ANR) error / core dump occurs, logging capability helps admin ensure a high level of customer experience (CX). The logging feature automatically stores the logs (as a Bugreport file) when an application or service in Android crashes (including FATAL/PANIC) or gets stuck. When this happens, it takes the logs from the event and saves them under 'sdcard/logs'.

When a device does not encounter an ANR error / core dump, log files don't appear.



- The feature is available for all devices running Android 10 or Android 12 operating system.
- Only the last 10 logs are stored on the device. If this number is exceeded, the previous logs are deleted.

Retrieving Bug Report Automatically Produced if 'Boot Reason' is FATAL or PANIC

A bug report is automatically produced if the 'boot reason' after the device is booted up is FATAL or PANIC (or anything that falls in the FATAL category).

The trigger is included in the bug report.

The report is stored in the 'sdcard/logs' folder.

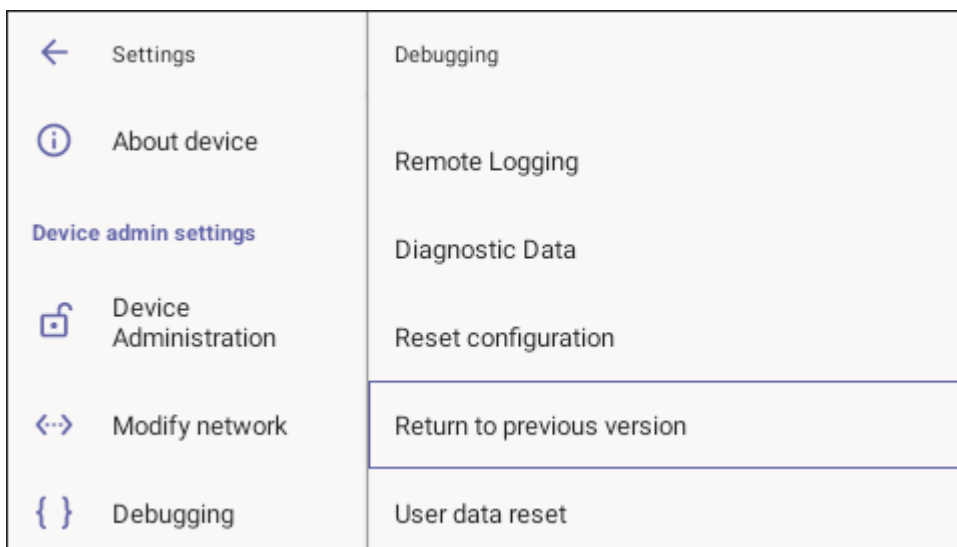
Return to Previous Version

When a customer receives a build for testing and completes the testing, they must switch back to the previous firmware version.

This version is the Global Availability (GA) build running on the device. The user needs to change the active firmware slot and perform a factory reset.

➤ To switch back to previous firmware

- Select **Return to previous version** in the **Debugging** menu:



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>

©2025 AudioCodes Ltd. All rights reserved. AudioCodes, AC, HD VoIP, HD VoIP Sounds Better, IPmedia, Mediant, MediaPack, What's Inside Matters, OSN, SmartTAP, User Management Pack, VMAS, VoIPerfect, VoIPerfectHD, Your Gateway To VoIP, 3GX, AudioCodes One Voice, AudioCodes Meeting Insights, and AudioCodes Room Experience are trademarks or registered trademarks of AudioCodes Limited. All other products or trademarks are property of their respective owners. Product specifications are subject to change without notice.

Document #: LTRT-13426

