User's and Administrator's Manual

AudioCodes 400HD IP Phone Series

C430HD IP Phones

Microsoft Teams Application

Version 2.3

audiocodes

Notice

Date Published: September-15-2024

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.
C430HD IP Phone for Microsoft Teams Quick Guide
C430HD 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 C430HD 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
- 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 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 ■ 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.

Feature	Details
Hardware	■ Graphic 4.3" color screen, 480x272 resolution ■ Wired connectivity: ✓ Two RJ-45 [Gigabit Ethernet (GbE)] (10/100/1000BaseT Ethernet) ports: LAN and PC port ✓ USB port for USB headset. Note that **C430HD-R** (**TEAMS-C430HD-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: ✓ 12V DC jack ✓ Power supply AC 100 ~ 240V ✓ PoE Class 2: IEEE802.3af (optional) ■ Keys: ✓ Illuminated VOICE MAIL message hotkey ✓ 4-way navigation button with OK key ✓ MENU ✓ HOLD ✓ Illuminated MUTE hotkey ✓ TRANSFER ✓ VOLUME control key ✓ Illuminated HEADSET hotkey ✓ Illuminated SPEAKER hotkey ✓ BACK ✓ CONTACTS ✓ Teams home key

Table 1-2: Teams Features Supported by theC430HD Phone

Teams Feature	C430HD
Call Transfer	√

Teams Feature	C430HD
Consultative Transfer	√
Escalate P2P call to Teams Meeting / Conference (Add-hoc Conference)	√
Call Queue	√
Contacts / People	√
Speed Dials dedicated keys	√
Visual VM (when C430HD 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)	√
Call Forward via phone UI	√
Teams self presence publish	√
Teams co-workers presence display	√
Call Park	√
Favorites list for speed dial	√
Delegation	Supported but configured from Teams client
Meet Now	Not supported
Better Together (over wireless)	Not supported
AudioCodes Device Duo	Roadmap

Teams Feature	C430HD
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.

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

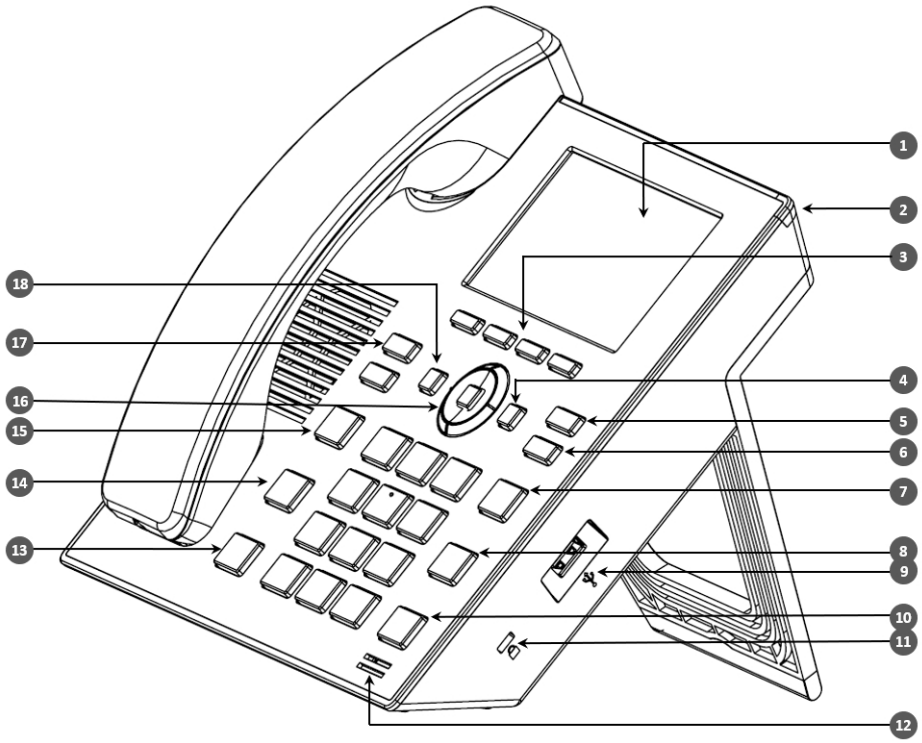


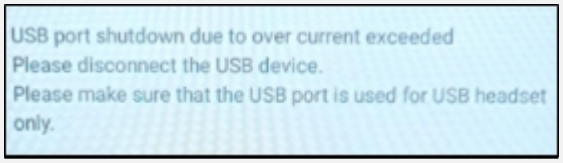
Table 2-1: Font View Description

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

Item #	Label Name	Description
3	Four softkeys	Enable the user to open (from left to right) the Calls menu, the Voicemail menu, the Contacts menu and the Lock menu.
4	Menu	Opens and provides access to the phone's menu.
5	Voicemail	Retrieves voicemail messages.
6	CONTACTS	Accesses the People screen.
7	AC	General purpose key.
8	TRANSFER	Transfers a call to another party.
9	USB port	For a USB headset. See also the note below.
10	HOLD	Places an active call on hold.
11	Kensington lock	Allows locking the device.
12	Microphone	Allows talking and 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	Navigation Control / OK	■ Press the button's upper rim to scroll up

Item #	Label Name	Description
		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.
17	▲ VOL ▼ VOL	Increases or decreases the volume of the handset, headset, speaker, ring tone and call progress tones.
18	'Back' key	Returns you back to the previous screen.

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.

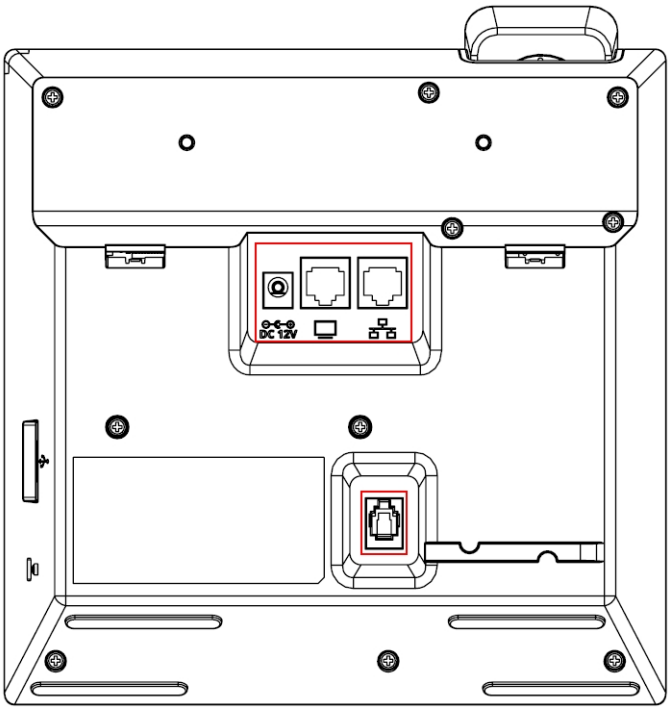


Navigate to menus and select menu items by:

- 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.
(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:**

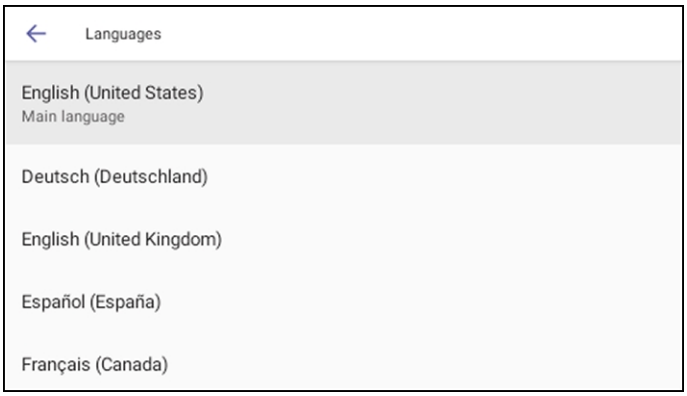
1. Disconnect all cables.
2. Spray onto a clean, dry, microfiber duster a medicinal isopropyl alcohol and water solution of 70:30. Don't oversaturate the duster. If it's wet, squeeze it out.
3. Lightly wipe the screen of the device.
4. Wait for the screen to dry before reconnecting cables.

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.



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

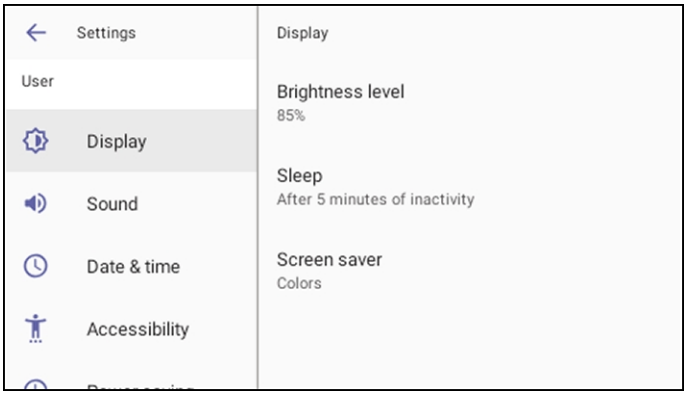
It will be necessary to repeat this only if the phone is restored to default settings.

Configuring Device Settings

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

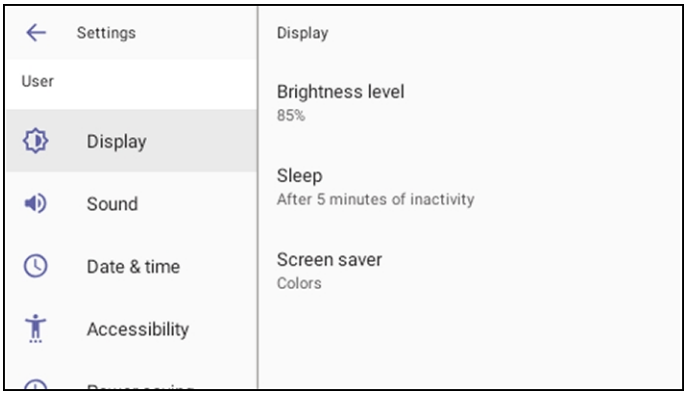
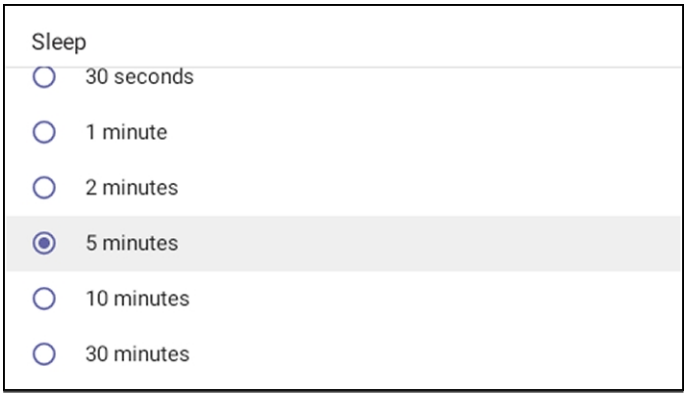
➢ **To access device settings:**

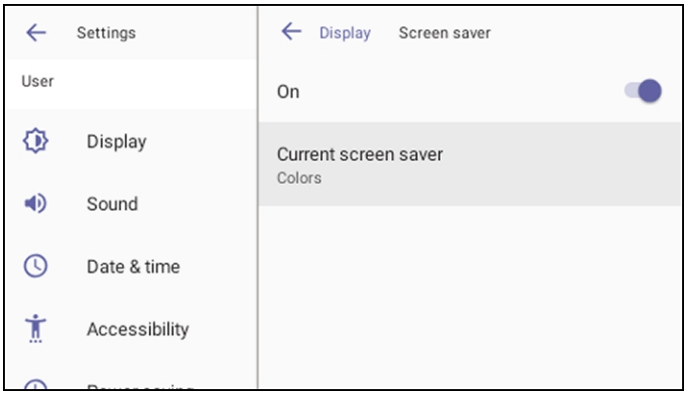
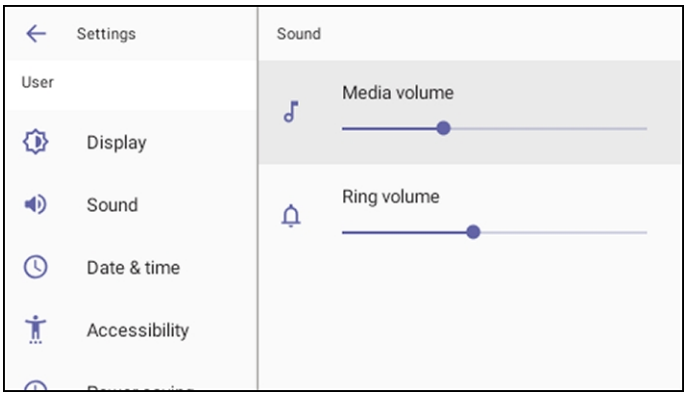
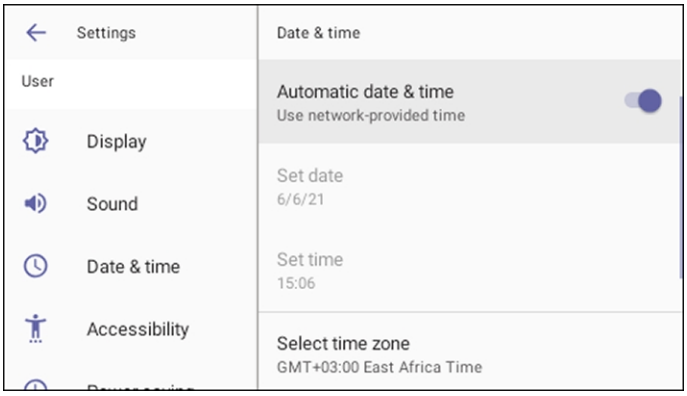
1. In the home screen, select , select **Settings** and then press the **Settings** softkey.

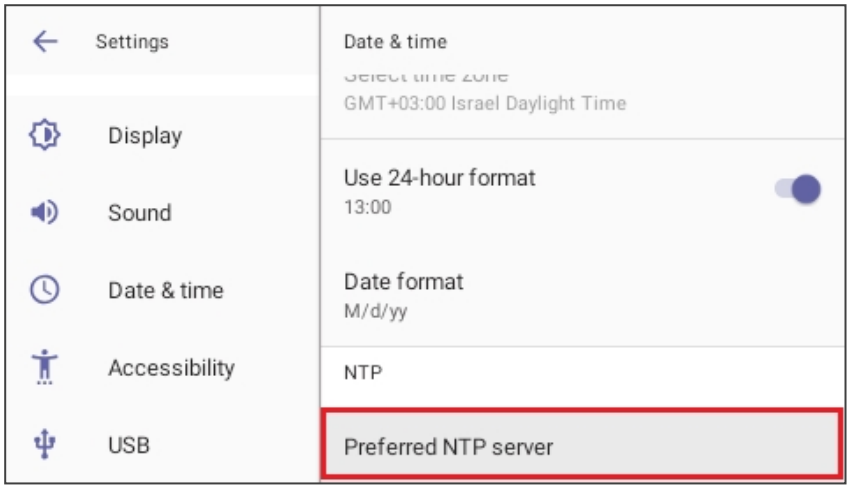
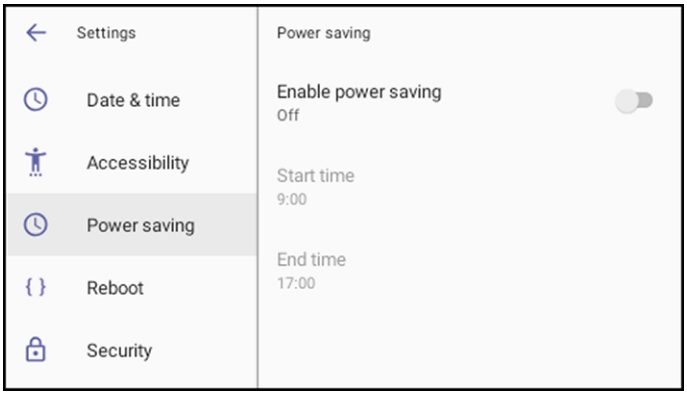


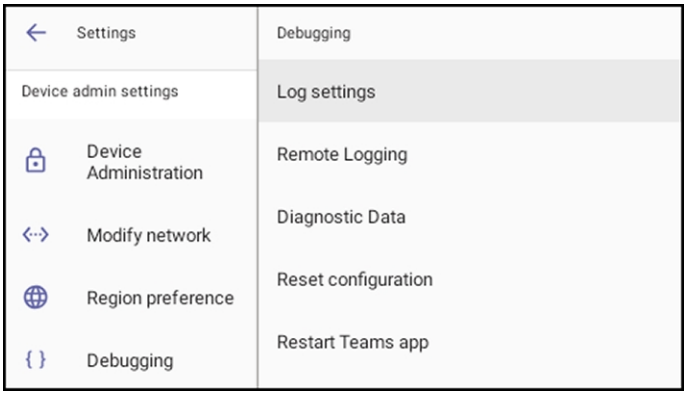
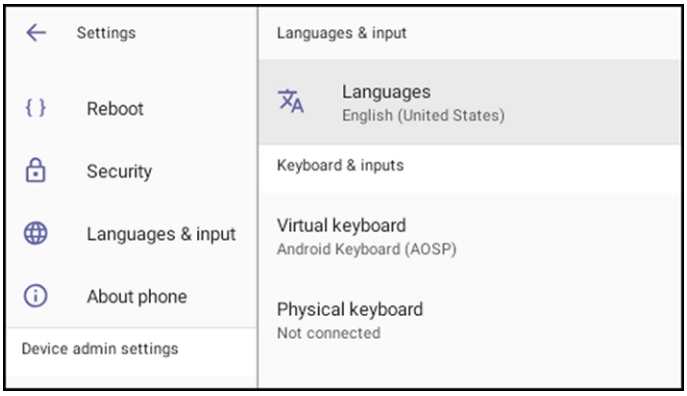
2. View the settings under 'User'. Select a setting to open it. Use the table following as reference. [To view settings related to the network administrator, scroll down and open 'Device Administration'].

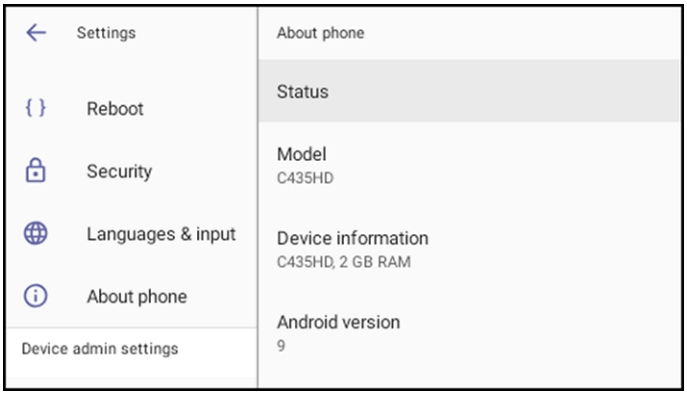
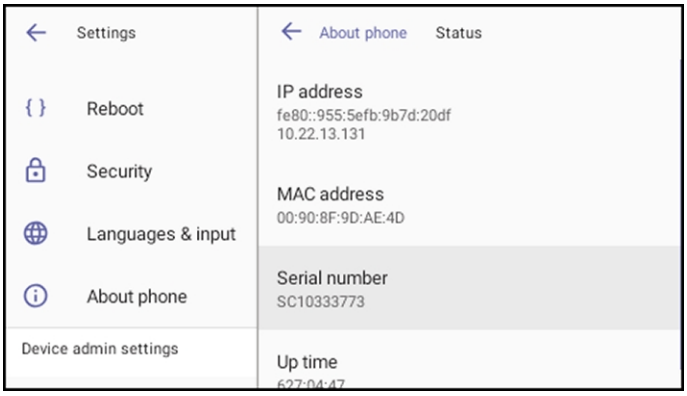
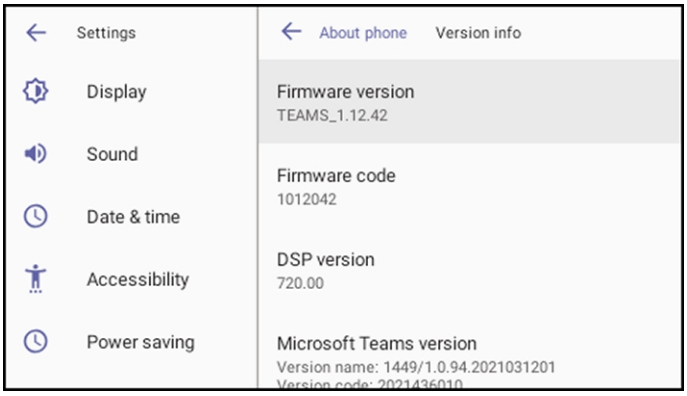
Table 3-1: Device Settings

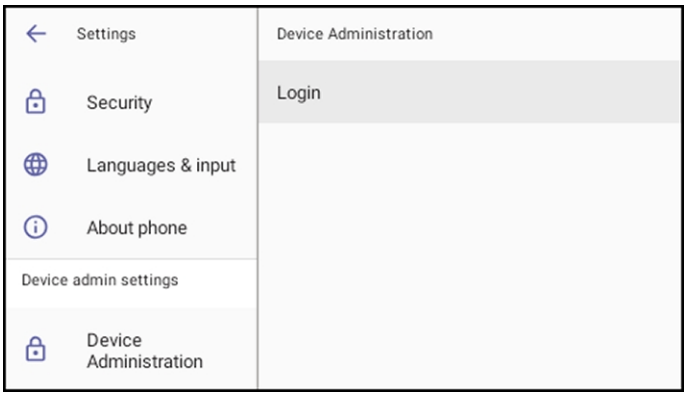
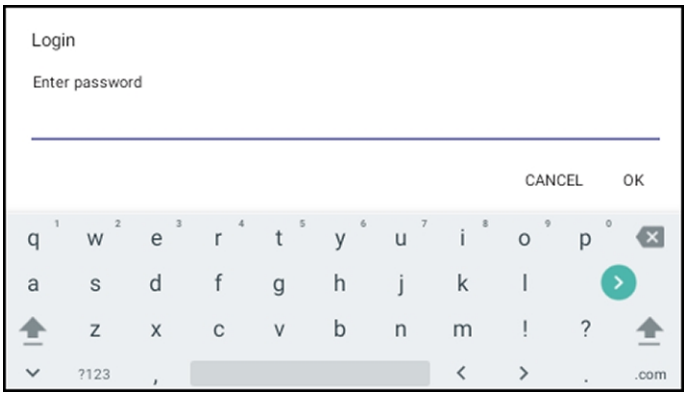
Setting	Description
User	
Display	Opens the 'Display' screen [Brightness level].  The phone's screen supports different brightness levels. Choose the level that suits your requirements. ■ Sleep  ■ Screen saver

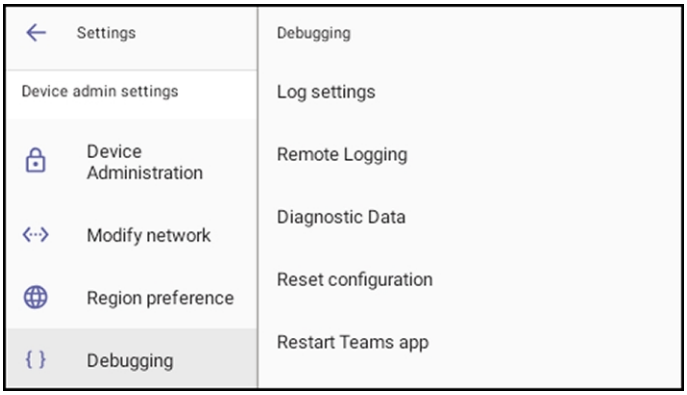
Setting	Description
	
Sound	Allows you to customize phone volume for a friendlier user experience. **Ring volume at n%** 
Date & time	Date and time are automatically retrieved from the deployed Network Time Protocol (NTP) server.  Use 24-hour format [Allows you to select the Time format] Also supported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

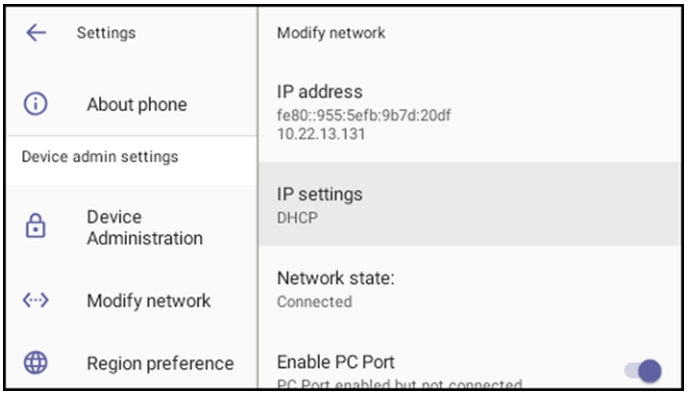
Setting	Description
NTP Preferred NTP server	Admins can use this parameter to *manually* define the NTP server, to comply with enterprise security requirements if those requirements preclude using DHCP Option 42. Manual configuration takes precedence over DHCP Option 42 and the time servers. Two ways to manually define the NTP server are available: ■ Admins can define it in the phone's GUI.  ■ 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.

Setting	Description
	 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.
Languages & input	Allows users to customize inputting to suit personal requirements. 
About	Provides users with device information.

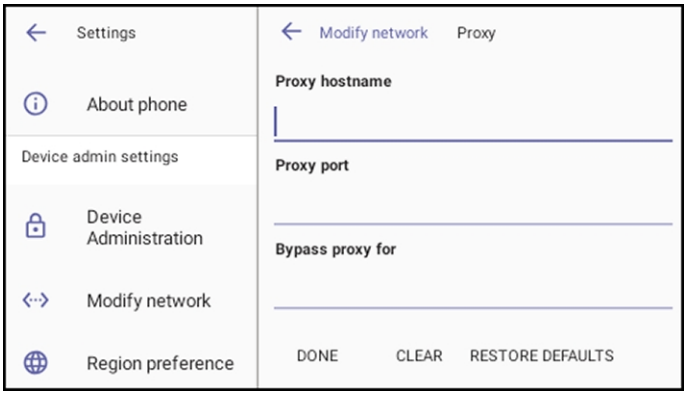
Setting	Description
	 To determine the device's IP address, select the 'Status' option.  To get information about the version, select 'Version info'.  To get information about the Android version, select 'Android version'.

Setting	Description
	
Device Administration	
Device administration	Allows the user to log in as Administrator, necessary for some of the debugging options. It is password protected. Default password: 1234 (or 1111 in early versions). After logging in as an Administrator, the user can log out | change password.  Select **Login** and then in the Login screen that opens, select the 'Enter password' field and use the virtual keyboard to enter the password (**1234** or **1111**). Note that the virtual keyboard pops up for all 'Settings' fields to allow inputting characters and / or numbers. Two virtual keyboard types can be displayed: Numeric or QWERTY. 

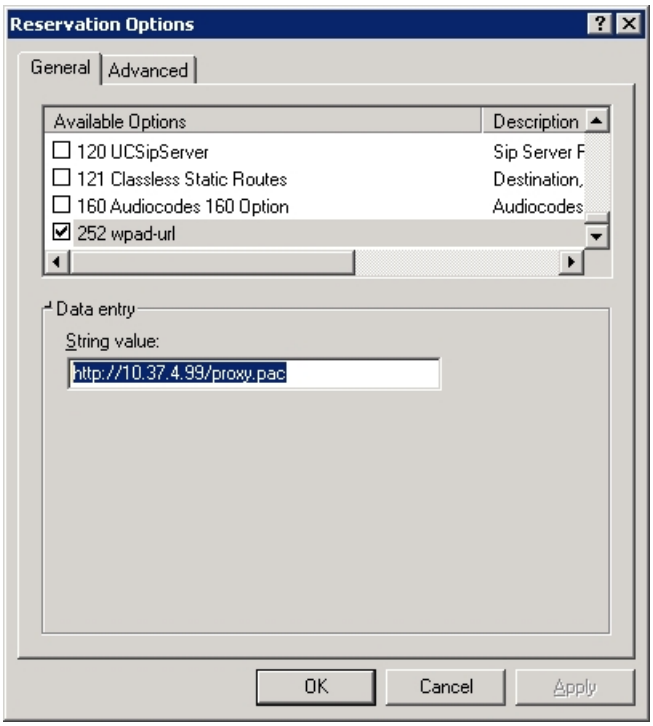
Setting	Description
	⚠ • The phone support a strong password check in order to log in as Administrator. The feature strengthens security. Note that the default password: ✓ must be changed before accessing the device via SSH ✓ can be changed per device from the phone screen (the user first enters the 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'. 
Modify network	Enables the Admin user to determine network information and to modify network settings.

Setting	Description
	 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



- **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:



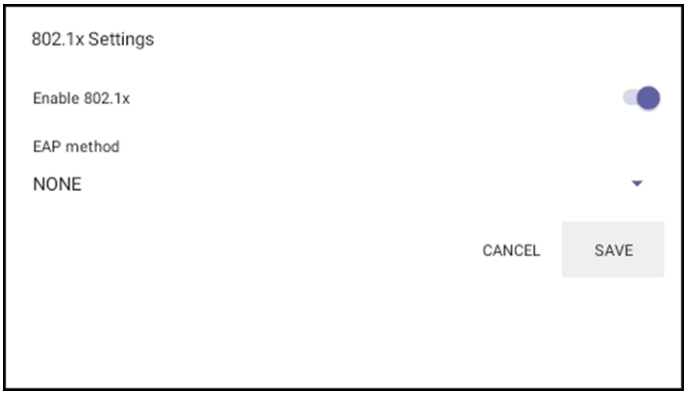
The proxy setting is provided in a Proxy Auto-Configuration (PAC) file that contains a set of rules coded in JavaScript which allows a web browser to determine whether to send web traffic directly to the Internet or to be sent via a proxy server. PAC files control how the phone handles HTTP, HTTPS and FTP traffic.

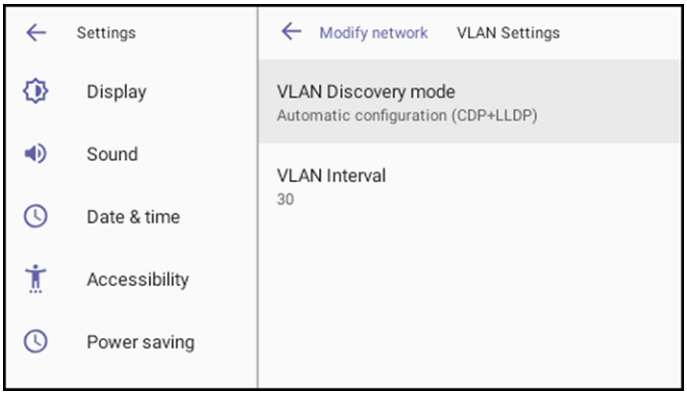
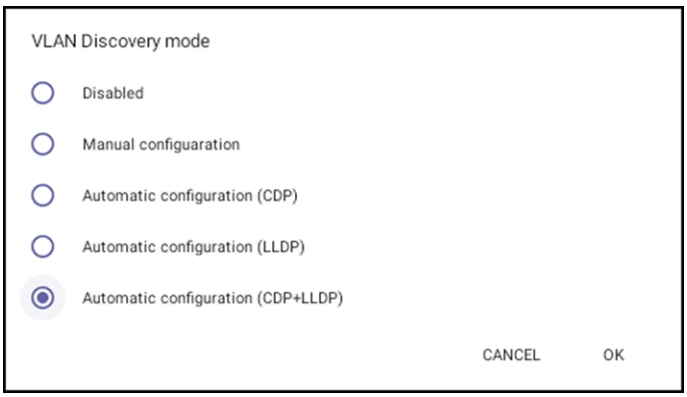
Example of a basic PAC file:

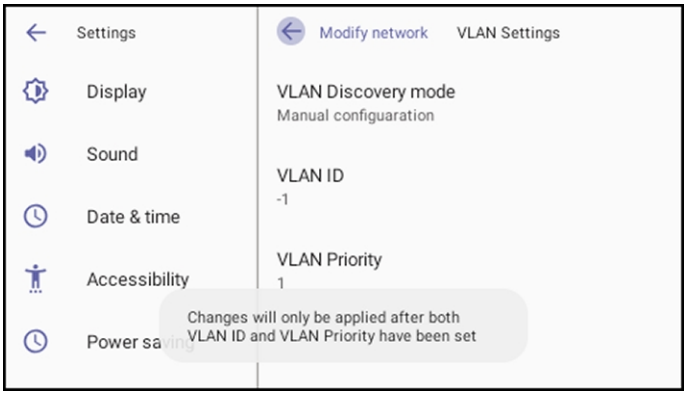
```
function FindProxyForURL(url, host)
{
return "PROXY 10.13.2.40:3128";
```

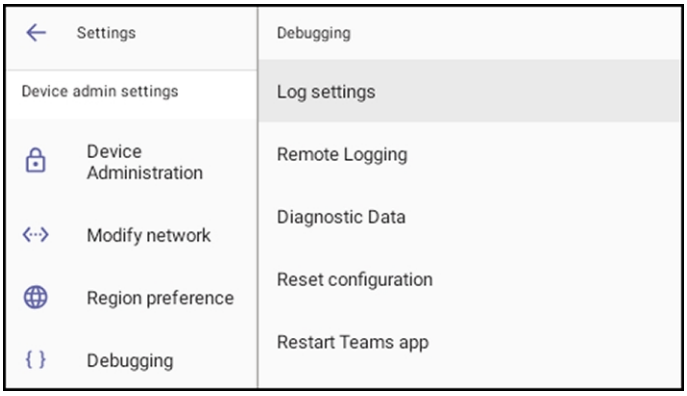
Setting	Description

	}
	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.  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**.  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:

Setting	Description
	 Select **VLAN ID**.  Select **VLAN Priority**. 
Debugging	Allows the Admin user to perform debugging for troubleshooting purposes. Available after logging in as Admin.

Setting	Description
	 Log settings Remote Logging (see under Remote Logging for more information) Diagnostic Data (see under Diagnostic Data 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 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

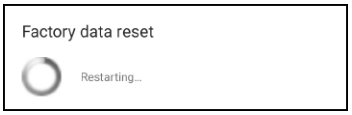
Performing a Hard Restore

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 for more information).

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

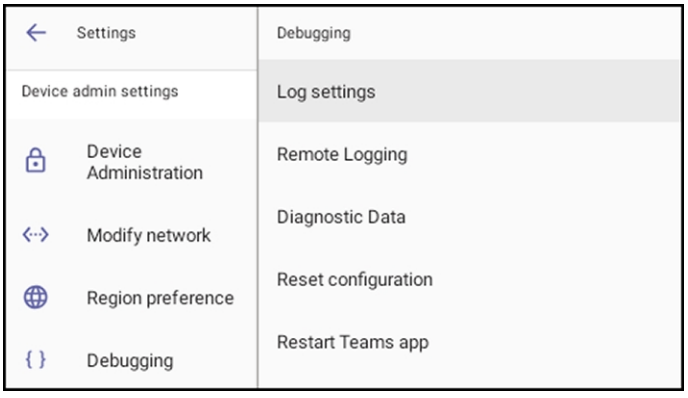
1. Press the OK + MENU keys simultaneously and keeping them pressed, unplug the power cable.
2. Plug the power cable back into the phone continuing to press the OK + MENU keys for +-5 seconds.
3. Release the OK + MENU keys; the phone' settings are restored to their defaults.

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 26.

Locking and Unlocking the Phone

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

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

Automatic Lock

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

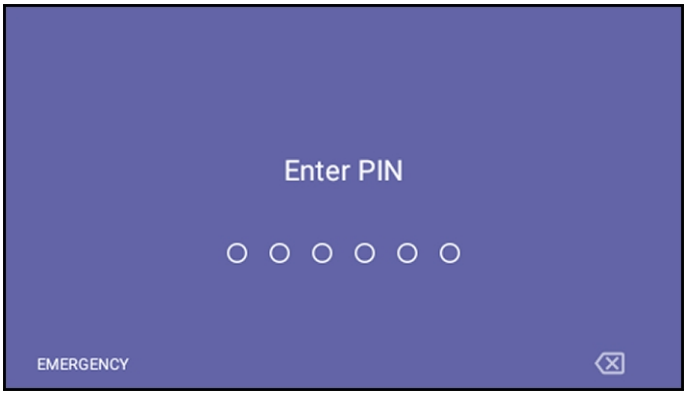
➢ **To lock the phone:**

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

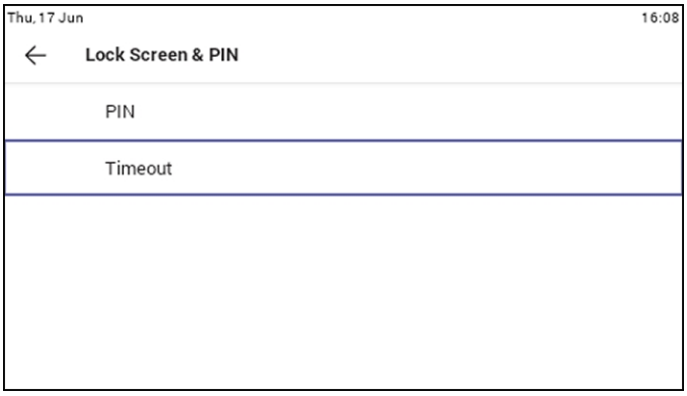
Unlock

➢ **To unlock the phone:**

1. When 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 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 below

Remove devices from Intune management (see Remove Devices from Intune Management)

Update Microsoft Teams devices remotely (see Update Microsoft Teams Devices Remotely)

Manage phones with the Device Manager (see Manage Phones with the Device Manager)

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.

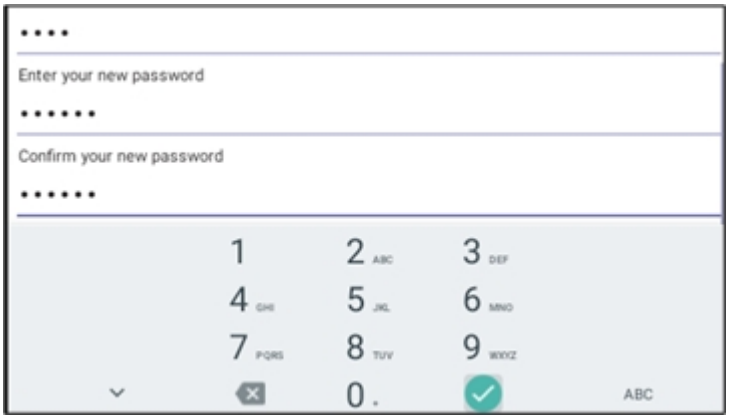
While a device is powering up, you can perform recovery operations by using a two-key combination.
When using a two-key combination, the device's main LED changes color after every *n* seconds; each color is aligned with a recovery operation option.

When?	Action	Press key combination	LED flashes 3x after release
Start pressing immediately after power up (on U-Boot / Universal Boot Loader)	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 +	Green +

When?	Action	Press key combination	LED flashes 3x after release
		MENU key (3 seconds)	blue / Green + yellow
When successfully booted (on Android)	Reboot	From the 'Admin' menu	-
	Restore defaults	Long-press **Hold** key for ~15 seconds	Flashes white once after release

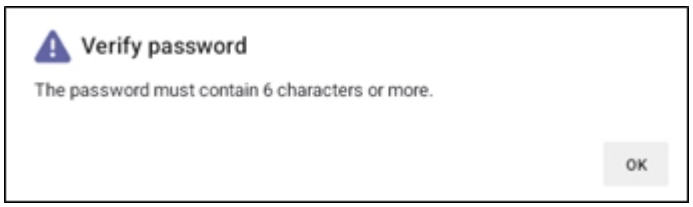
Defining Password Complexity

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.

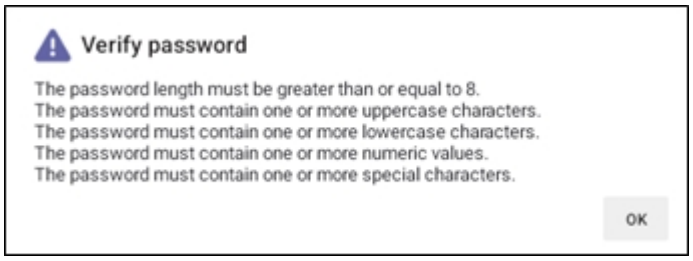


Admin can set password complexity using the cfg configuration file parameter 'system/admin_password/strength'.

- 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.

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) Audi-

oCodes' 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)

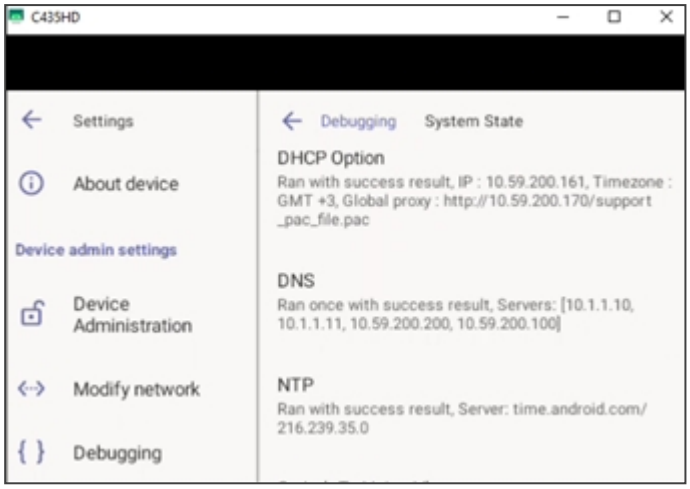
- The cfg file can be loaded to the device using Device Manager.
- Timing begins when exiting the 'Device Settings' menu.
- When the timeout expires, the device logs out automatically.
- The functionality works for both registered and unregistered devices.

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**).



5 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.

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.

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-13452