User's Manual

AudioCodes 400HD IP Phone Series

Android Device Utility

Version 1.1.37

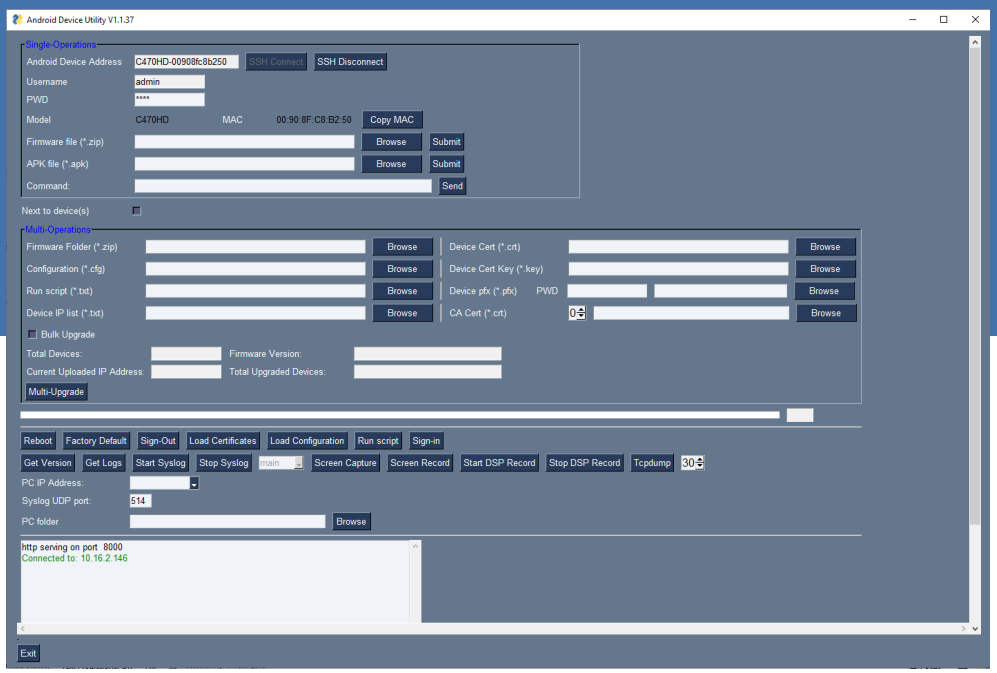


Table of Contents

This page is intentionally left blank.

Notice

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

This document is subject to change without notice.

Date Published: April-10-2023

WEEE EU Directive

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

Customer Support

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

Stay in the Loop with AudioCodes

Abbreviations and Terminology

Each abbreviation, unless widely used, is spelled out in full when first used.

Related Documentation

Document Name
C435HD IP Phone for Microsoft Teams User's and Administrator's Manual
C448HD & C450HD IP Phone for Microsoft Teams User's and Administrator's Manual
C455HD IP Phone for Microsoft Teams User's and Administrator's Manual
C470HD IP Phone for Microsoft Teams User's and Administrator's Manual
C470HD-C455HD-C450HD-C448HD-C435HD IP Phones for Microsoft Teams Release Notes
RXV81 Standalone Video Collaboration Bar Release Notes
RXV81 Standalone Video Collaboration Bar User's and Administrator's Manual
RXV81 Standalone Video Collaboration Bar Deployment Guide

Document Revision Record

LTRT	Description
21951	This is the first *User's Manual* released for Android Device Utility.

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 Web site at https://online.audiocodes.com/documentation-feedback.

1 Introduction

AudioCodes' Android Device Utility is a light, portable and highly versatile management application that enables customer IT admins to quickly connect to AudioCodes' Android based IP devices and Meeting Rooms and in a very friendly, simple and intuitive user interface, efficiently perform management operations on these devices.

Operations that IT admins can perform are:

- **Debugging operations** (see here for more information)
  - Capturing device & sidecar screens
  - Running TCP Dump
  - Getting device info (version)
  - Starting Syslog | Stopping Syslog (remote logging)
  - Getting Logs
  - Recording DSP | Stopping DSP recording
- **Inputting operations** (see here for more information)
  - Uploading firmware
  - Uploading an Android package (APK) file
  - Uploading a certificate
  - Uploading a certificate key
  - Uploading a device PFX
  - Uploading a CA certificate
- **Processing operations** (see here for more information)
  - Rebooting a device
  - Restoring to factory defaults
  - Signing out
  - Loading certificates
  - Loading configuration
  - Running script
  - Signing in

The utility is particularly effective for customer IT admins who encounter issues and require immediate diagnoses and fixes. Admins use the utility to remotely retrieve information from devices (debugging) and send it to AudioCodes FAEs who diagnose the data and send a fix.

Based on Secure Shell (SSH) cryptographic network protocol which gives IT admins secure access to devices over unsecured networks, the utility supports:

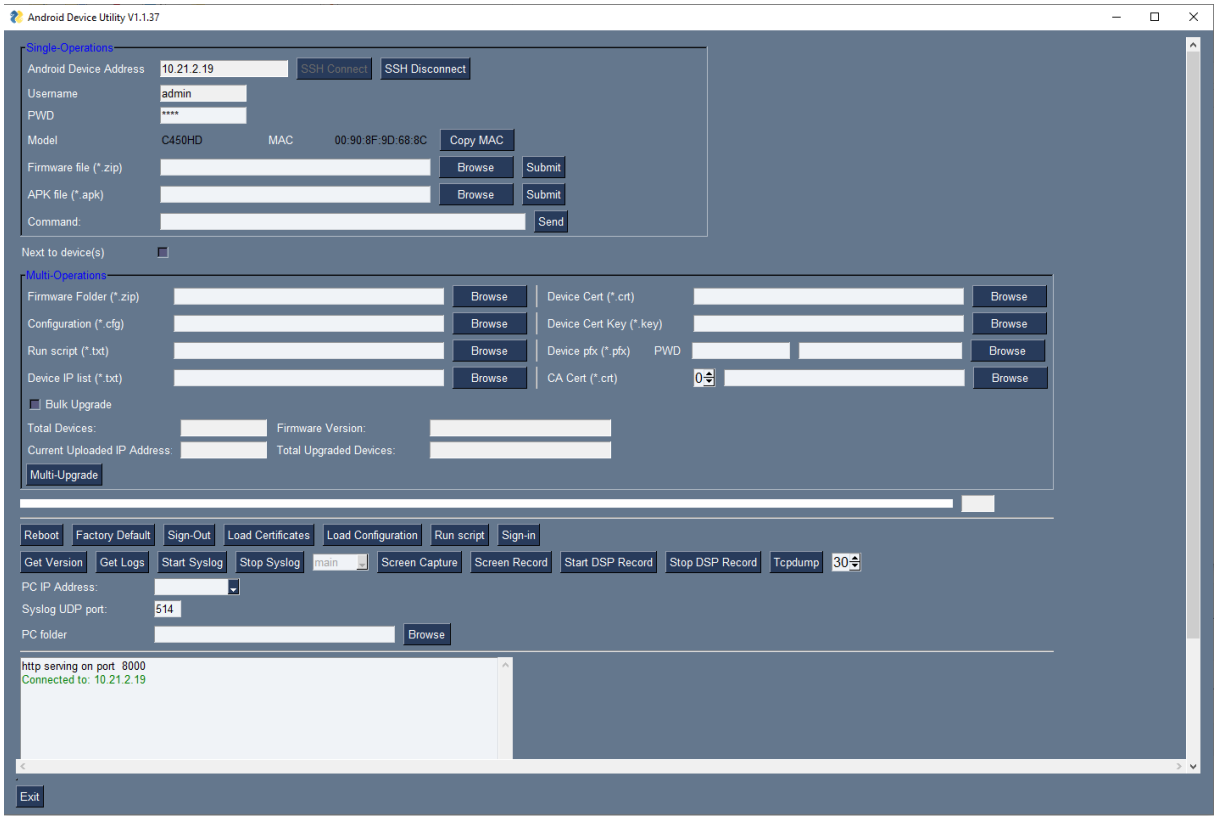
- Uploading files (CFG files, CRT files, etc.) for up to 3 devices simultaneously (in bulk).
- Performing operations such as running a script on an unlimited number of devices simultaneously.

The utility can reduce downtime significantly, helping customers maintain high productivity levels.

This page is intentionally left blank.

2 Installation

After receiving an executable (.exe) file from your AudioCodes representative (**Android Device Utility v1.1.30.exe**, for example), save it on your pc | laptop in path **C:\audc\prod** for example, and then double-click it.



Note: The utility's certificate loading mechanism is performed using HTTP. The HTTP port is 8000. IT admins must make sure the port is not blocked by the organization's firewall.

This page is intentionally left blank.

3 Connecting to Device(s)

Note: Only AudioCodes Android-based devices are supported.

Before performing management operations, you need to connect the utility to the device(s).

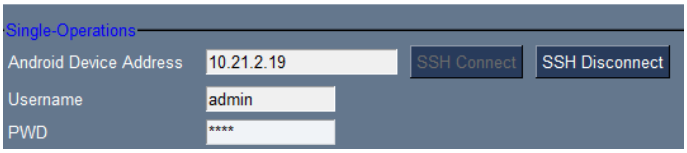
➢ To connect to the device(s):

1. In the 'Android Device Address' field, enter the IP address of the device. For multiple devices, enter each IP address on a separate line.

Note:

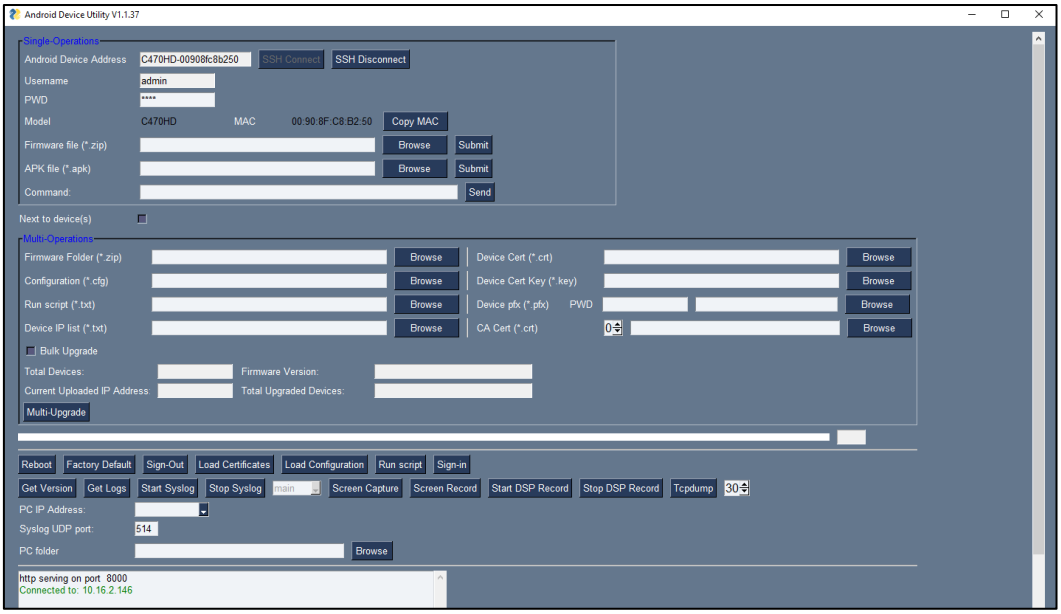
- You can get the IP address of the C435HD, C448HD, C450HD and C455HD phone models by pressing the MENU hard key > About phone > Status > IP Address.
- You can get the IP address of the C470HD phone model by touching the user's picture | avatar in the home screen > Settings > Device Settings > About phone > Status > IP Address).

2. Enter the 'Username' (Default: **admin**) and 'Password' (Default: **1234**).



3. Click the **SSH Connect** button adjacent to the 'Android Device Address' field.
4. View in the lowermost pane an indication that you've been successfully connected.

Note: If you don't know the device's IP address, you can nonetheless connect to it using host name, e.g., <model>-<mac> or C470HD-00908fc8b250 as shown in the figure below.



This page is intentionally left blank.

4 Debugging Devices

The app gives admins these debugging capabilities:

- Capturing the Device & Sidecar Screen (see here for details)
- Running the Tcpdump Tool (see here for details)
- Getting Information about Devices (see here for details)
- Remote Logging (Syslog) (see here for details)
- Getting Logs (see here for details)
- Activating DSP Recording (see here for details)
- Deactivating DSP Recording (see here for details)

4.1 Capturing Device & Sidecar Screens

The utility allows admins to effectively collaborate and debug issues using the screen-capturing feature.

Note: The feature enables capturing the device's main screen as well as the device's Expansion Module (sidecar) in the case of the C450HD phone model with sidecar and the C455HD phone model with sidecar.

➢ **To capture the device's screen:**

1. In the 'Android Device Address' field, enter the IP address of the device.
2. Click **SSH Connect**; a connection with the device is established.
3. Next to the field 'PC folder', click the **Browse** button and navigate to and select the folder to which to send the screen captures.
4. Make sure that the drop-down menu next to the **Screen Capture** button shows **main**.
5. Click the **Screen Capture** button; the device's screen is captured and the screenshot is saved and sent to the folder.
6. On your PC, navigate to the folder and retrieve the screenshot. The screenshot is saved with a timestamp in the filename so each file gets a unique name, avoiding the need for renaming to prevent it from being overwritten next capture. Example filename: **screencap20230330-160132.png**

➢ **To capture the Expansion Module (sidecar) screen:**

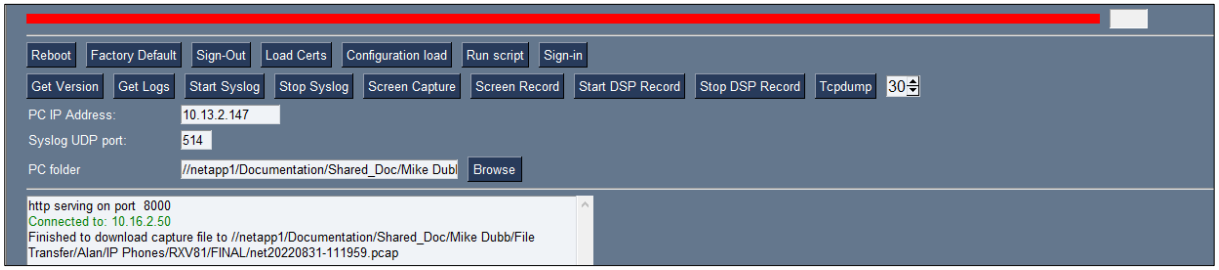
1. Make sure the drop-down menu next to the **Screen Capture** button shows **sidecar**. By default, the field indicates **main**, i.e., the device's main screen.
2. Click the **Screen Capture** button; the device's sidecar screen is captured and the screenshot is saved and sent to the folder you defined previously.
3. On your PC, navigate to the folder and retrieve the screenshot. The screenshot is saved with a timestamp in the filename so each file gets a unique name, avoiding the need for renaming to prevent it from being overwritten next capture. Example filename: **screencap20230330-160132.png**

4.2 Running Tcpdump

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

➢ **To run Tcpdump:**

1. In the utility, enter the device's IP address, click **SSH Connect** and browse to a folder on the PC to which to send the information.
2. Next to the **Tcpdump** button, set time period or leave at default. Default: 30 seconds.
3. Click the **Tcpdump** button and then after the progress indicator reaches the end, you'll view in the results pane a 'Finished' indication.



4. Open the folder on the PC to which you commanded the application to send the information and locate and open the file 'net.pcap'.
5. Alternatively, run Tcpdump without the utility.

➢ **To run tcpdump without the utility:**

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

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

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

```
setprop ac.ac_tcpdump 1
```

3. Tcpdump capture file will appear in this location:

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

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

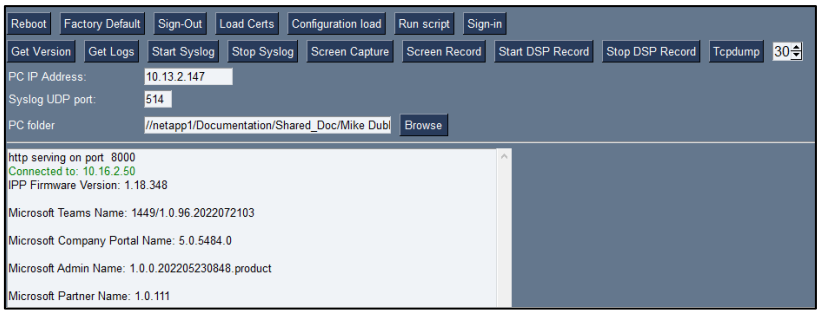
```
scp -r admin@%deviceIp%:/sdcard/recording/ %FolderOnPc%
```

4.3 Getting Info about a Device

Admins can use the utility to get info about a device.

➢ **To get info about a device:**

1. Enter the device's IP address, click the adjacent **SSH Connect** button and browse to a folder on the PC to which to send the information.
2. Click the **Get Version** button.



3. View the information in the utility's lowermost pane.

Alternatively

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

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

- To get **Bootloader** info, in the 'Command' field enter the following SSH command and then click **Send**:

```
getprop ro.bootloader
```

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

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

The following applies to the C435HD, C448HD, C450HD, C455HD and C470HD phones:

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

```
getprop ro.teams.versiongetprop ro.zoom.version
```

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

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

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

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

4.4 Performing Remote Logging via Syslog

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

Device Diagnostics via the Microsoft Admin Center are saved to the device sdcard and collected after the event. When performing Remote Logging via Syslog, the logs are collected in real time.

Remote Logging via Syslog can be enabled from the utility.

➢ To enable Remote Logging via Syslog from the utility:

1. Enter the device's IP address, click **SSH Connect** and browse to a folder on the PC to which to send the information.
2. In the 'PC IP Address' field, enter the IP address of the PC on which the utility is installed and then click the **Start Syslog** button.

3. Open the folder on the PC to which you commanded the application to send the information and locate the Syslog file.
4. To view Syslog, you can optionally download the Syslog Viewer available in AudioCodes' website.

Admins can also enable | disable Syslog using Secure Shell (SSH) protocol.

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

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

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

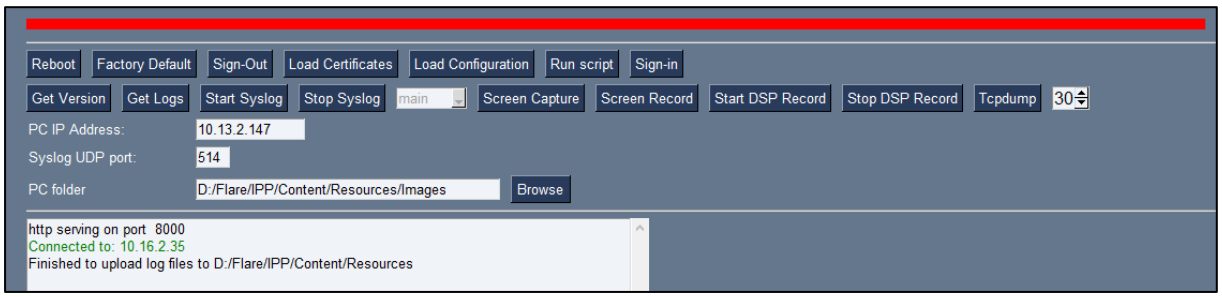
```
setprop persist.ac.rl_address ""
```

4.5 Getting Logs Using the Utility Interface

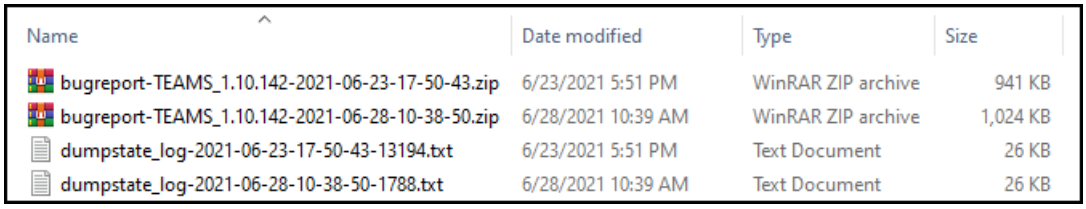
Admins can get bug report logs, including a logcat file and a configuration file, to expedite debugging.

➢ **To get logs:**

1. Enter the phone's IP address, browse to a folder on the PC to which to send the information and click **SSH Connect**.
2. Click **Get Logs**; after a short period, view a 'Finished' indication in the results pane.



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



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

4.6 Getting Logs Using SSH Command

IT admins can optionally collect logs using SSH commands.

➢ **To collect logs:**

1. In the 'Command' field, enter the following command and then click **Send**:

```
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.
4. For example, use the following:

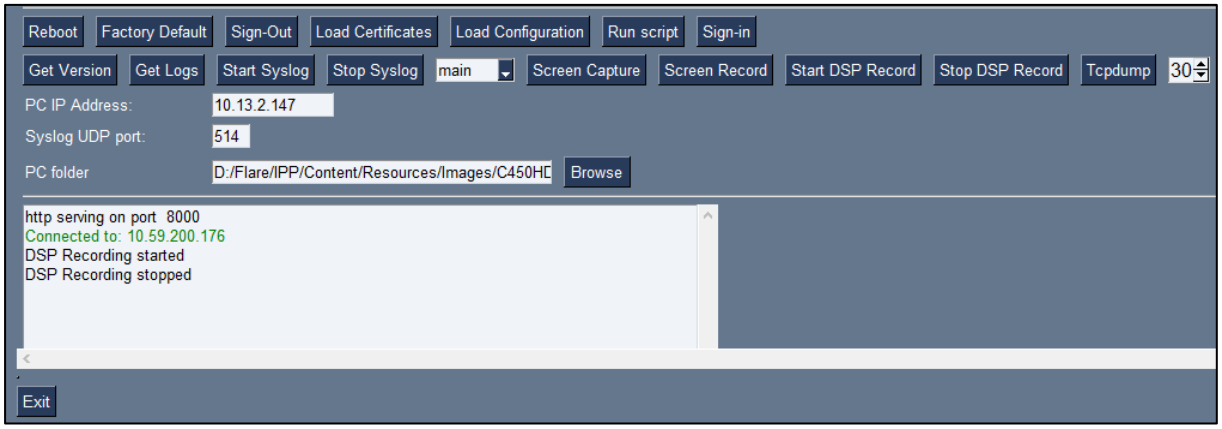
```
SCP admin@<DeviceIP>:/sdcard/logs/bugreports/<log file name>
C:\<destination Directory>
```

4.7 Activating DSP Recording

Admins can activate DSP recording using the utility.

➢ **To activate DSP Recording:**

1. Enter the device's IP address and then click **SSH Connect**.
2. Click the **Browse** button next to the field 'PC folder' to configure a folder on the PC to which to send the recording.
3. In the 'PC IP Address' field, enter the IP address of the PC on which the utility is installed and then click the **Start DSP Record** button.
4. After a period of recording, click **Stop DSP Record**.



5. Run Wireshark and capture packets on the interface that you selected in the 'PC IP Address' drop-down.
6. Admins can alternatively activate a DSP recording using SSH protocol, as shown next.

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

Applies to C448HD, C450HD and C455HD phones:

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

Applies to C435HD and C470HD phones:

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

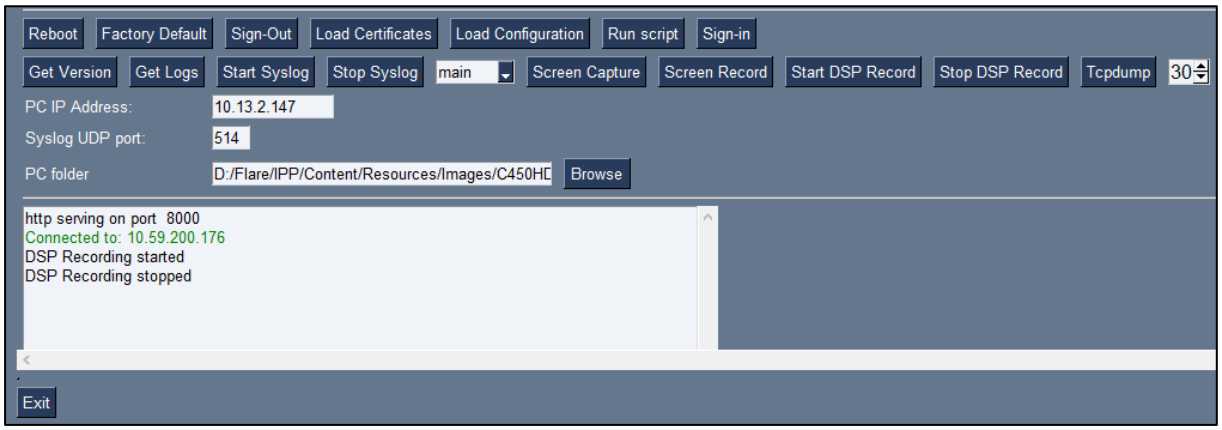
Note: DSP recording can be activated on the fly without needing to reset the phone.

4.8 Deactivating DSP Recording

Admins can deactivate DSP recording using the utility.

➢ **To deactivate DSP Recording:**

1. In the utility, click **Stop DSP Record** after a period of recording (see here how to start).



2. Alternatively, deactivate a DSP recording using SSH protocol, as shown next.

➢ **To deactivate DSP recording using SSH protocol, type the following at the shell prompt:**

```
setprop ac.dr_voice_enable false
```

Note: DSP recording can be deactivated on the fly without needing to reset the phone.

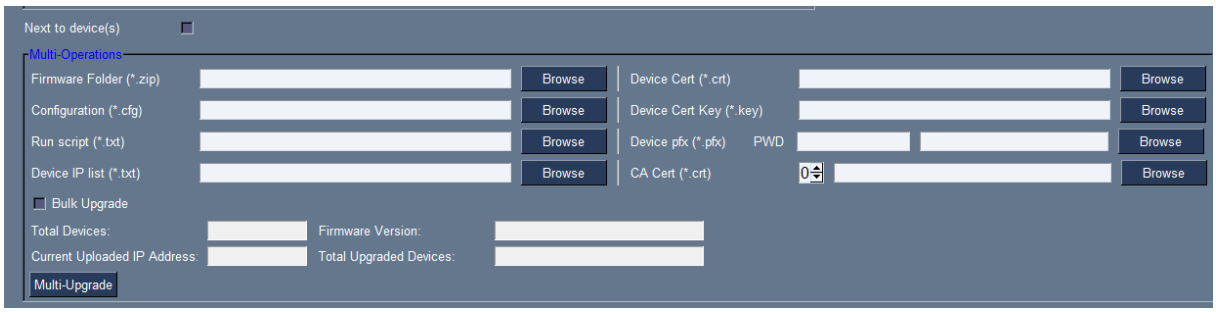
5 Inputting Data into Devices

Admins can load a firmware file, configuration file, certificate file, etc., to up to three devices simultaneously. Admins can run a script to load - for example - a configuration to an unlimited number of devices simultaneously.

The 'Command' field sends SSH commands to a device to get a response from the device. The field is useful for debugging.

5.1 Uploading Firmware Folder (*.ZIP)

Admins can load a zipped firmware folder to up to three devices simultaneously.



➢ **To load a zip firmware file:**

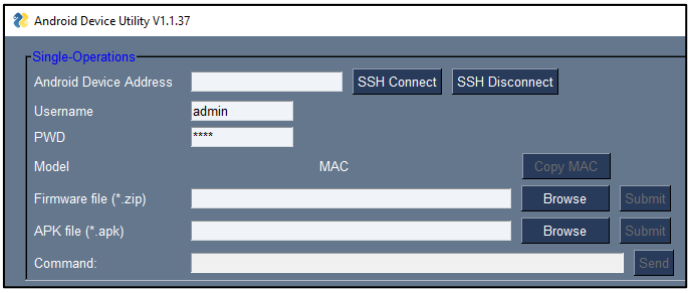
Note:

- Before loading, make sure you entered the IP addresses of the device(s) in the 'Android Device Address' field.
- For multiple devices, make sure you enter each IP address on a separate line.

1. Click the **Browse** button adjacent to the 'Firmware Folder (*.zip) field shown in the previous figure and then navigate to the folder to load.
   - Select the **Bulk Upgrade** option to *simultaneously* load the folder to multiple devices.
   - Clear the **Bulk Upgrade** option to load the folder to *one device after another*.
2. Click the **Multi-Upgrade** button to perform the upload.

5.2 Uploading an Android Package Kit (APK) File

Admins can upload an APK file to one device at a time.



➢ **To load an APK file from the GUI:**

Note: Before loading, make sure you enter the IP address of the device in the 'Android Device Address' field.

1. Click the **Browse** button adjacent to the 'APK file' field and navigate to the file to load.
2. Click the adjacent **Submit** button.

➢ **To upgrade the APK using SSH commands:**

1. Download the required APK to sdcard/teamszoom.apk. For example, use the following:
```
SCP <file name> admin@<DeviceIP>>:/sdcard/teams.apk
```
2. Update the APK using the following:
```
pm install -r -g /sdcard/<filename>
```
3. Delete the old APK using the following:
```
pm uninstall com.microsoft.skype.teams.ipphone
```
4. If the new APK is older than the existing one, delete the existing APK before installing the new one.

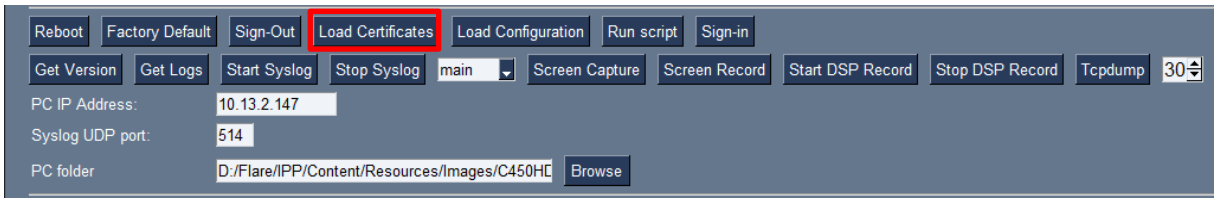
5.3 Uploading a Certificate

Certificates can be loaded to a phone or to multiple phones using the utility.

➢ **To load certificates to a single device:**

1. Enter the device's IP address, the username and password and click **SSH Connect**.
2. Click the **Browse** button next to the field 'Device Cert' shown in the next figure and then navigate to and select the certificate file to download.

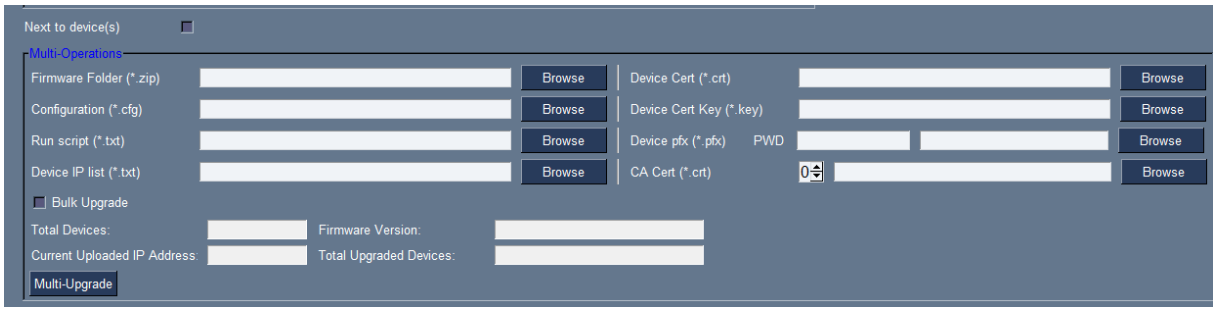
3. Click the **Load Certificates** button shown in the next figure, to add the certificate.



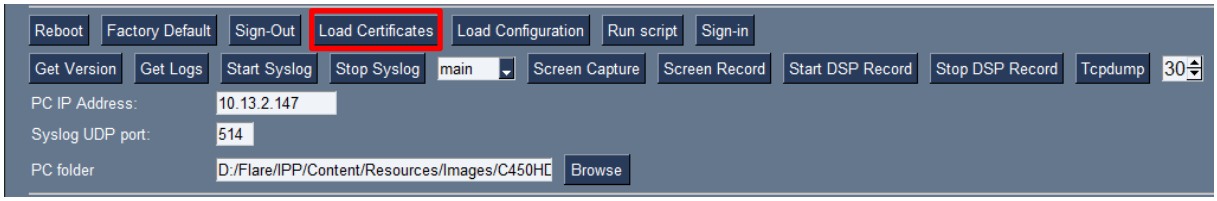
4. After a short period, view in the results pane 'Cert Successfully Installed'.

➢ **To load certificates to multiple devices:**

1. Create a txt file and enter into it the IP addresses of the devices. Each IP address must receive its own line in the list; the IP addresses are listed one under the other; no notation between them is required.



2. Adjacent to the field 'Devices IP list' shown in the preceding figure, click the **Browse** button and then navigate to and select the txt file listing the IP addresses of the devices to which to download the certificates.
3. Click **SSH Connect**.
4. Adjacent to the field 'Device Cert', click the **Browse** button and then navigate to and select the certificate file to download.
5. Click the now-activated **Load Certificates** button shown in the next figure, to add the certificates to the phones.



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

5.4 Uploading a Certificate Key

Each certificate has a key. The certificate file is paired with the certificate key file. They must both be loaded to the device. Use the instructions here as reference.

5.5 Uploading a Device PFX

Device certificates can be provisioned in Personal Information Exchange (PFX) format combining .crt and key. Use the instructions here as reference.

This password-protected file certificate is typically used for code signing an application. It stores multiple cryptographic objects within a single file: X.509 public key certificates.

Additionally, the following parameter values can be configured in the Configuration File which can be loaded to the device using the utility:

- /security/device_certificate_url = <url>/certificate.pfx
- /security/device_private_key_url = NULL
- security/device_certificate/password=<pfx password>

5.6 Uploading a CA Certificate

The utility enables IT admins to load a digital certificate authority (CA)-issued file to the device. The CA verifies trusted certificates for trusted roots. Use the instructions here as reference.

This page is intentionally left blank.

6 Changing Device Status

The utility enables IT admins to change a device's status with operations such as rebooting and restoring to factory defaults.

6.1 Rebooting a Device

IT admins can remotely reboot a device after debugging it or after changing its configuration for example.

If a device gets stuck for example, rebooting can correct the issue.

After clicking the **Reboot** button, the utility reboots the device over SSH.

6.2 Restoring to Factory Defaults

IT admins can remotely restore a device to factory defaults if for example it gets stuck.

Other examples of when to use the feature:

- to calibrate a device
- to demo a device
- to give a device to another user

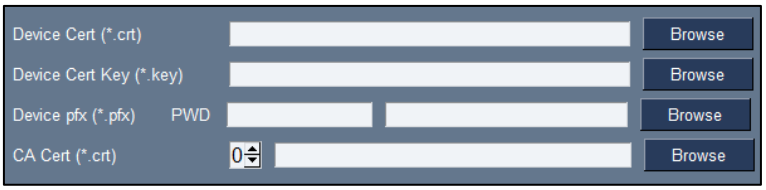
Click the **Factory Default** button to restore a device to factory defaults.

6.3 Signing out

The IT admin can remotely sign out from a device when registering for example a user to Teams. The admin does not need to be next to the device to perform the sign-out. Remotely signing out from a device can save admins time and inconvenience.

6.4 Loading Certificates

The **Load Certificates** button can only be used after selecting the certificate here:



See also:

Uploading a Certificate

Uploading a Certificate Key

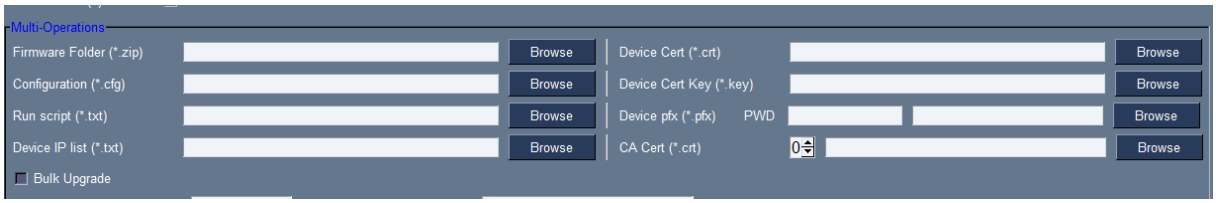
Uploading a Device PFX

Uploading a CA Certificate

IT admins can load a new certificate to a device to replace the factory certificate for example.

6.5 Loading a Configuration

Use the **Load Configuration** button after browsing to and selecting the *.cfg configuration file in the 'Configuration (*.cfg)' field:



➢ **To load a *.cfg file to multiple devices:**

1. Create a txt file and enter into it the IP addresses of the devices. Each IP address must receive its own line in the list.
2. Click the **Browse** button next to the 'Device IP List (*.txt)' field and navigate to and select the txt file.
3. Click Load Configuration

Note: If you don't create a *.txt file and you don't configure the 'Device IP List (*.txt)' field, then the utility loads the *.cfg file to the device it's connected to.

6.6 Running a Script

A script is a set of commands in a *.txt file that any IT admin can create and use for internal purposes.

IT admins can for example create and run a script to convert devices from Android to Zoom or to convert devices from Teams to Zoom.

Note: Every command in the txt file must be on a different line, i.e., separated.

➢ **To run a script:**

1. Click the **Browse** button next to the 'Run script (*.txt)' field and navigate to and select the *.txt file.
2. Click Run script

6.7 Signing in

The IT admin can remotely sign in to a device when registering for example a user to Teams. The admin does not need to be next to the device to perform sign-in. Remotely signing in to a device can save admins time and inconvenience. Related: Signing out.

This page is intentionally left blank.

International Headquarters
1 Hayarden Street,
Airport City
Lod 7019900, Israel
Tel: +972-3-976-4000
Fax: +972-3-976-4040

AudioCodes Inc.
80 Kingsbridge Rd
Piscataway, NJ 08854, USA
Tel: +1-732-469-0880
Fax: +1-732-469-2298

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

©2023 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, VocaNom, 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-21951