Administrator's Guide

AudioCodes One Voice Operations Center (OVOC)

Device Manager Pro

Version 8.0.3000

audiocodes

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: March-13-2022

WEEE EU Directive

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

Customer Support

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

Documentation Feedback

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

Stay in the Loop with AudioCodes

Related Documentation

Document Name
400HD Series IP Phone User Manuals
400HD Series IP Phone with Microsoft Skype for Business User Manuals
400HD Series IP Phones Administrator's Manual

Document Name
400HD Series IP Phone with Microsoft Skype for Business Administrator's Manual
400HD Series IP Phone Quick Guides
400HD Series IP Phone with Microsoft Skype for Business Quick Guides
400HD Series IP Phone for Microsoft Teams User and Administrator Manuals
Device Manager for Third-Party Vendor Products Administrator's Manual
Device Manager Deployment Guide
Device Manager Agent Installation and Configuration Guide
One Voice Operations Center IOM Manual
One Voice Operations Center User's Manual

Document Revision Record

LTRT	Description
91097	Initial release for 7.8. Set as VIP. Network Topology page. Poly phones provisioned to sites. System Settings and tabs. Rearranged GUI.
91098	7.8.1000. Endpoints Groups. Configuring DHCP Option 160 - tenant and group. Filtering by group in Manage Multiple Devices. Zero Touch: URL to associate device w Tenant and Group.
91188	8.0.1000 New look and feel. Devices Status page: Enhanced Show Info feature. Teams phones and devices: RXV80, C435HD, C448HD, C470HD. Tenant / Site Configuration: provision devices using the 'Configuration Set' parameter and the corresponding 'Configuration Key' and 'Configuration Value' parameters auto-populated after selecting a device model. Parameters in configuration file commented to indicate template source.
91189	Polycom>Poly. EPOS. Poly CCX 500/600. RXV100 (MTR). 'Show Info' page includes detailed info reported by Teams devices (Status/Configuration). New 'Collect logs' link in 'Show Info' page; capability to collect logs on native Teams phones.
91190	EPOS. RXV100 (MTR). RXV90. DST.
91221	[8.0.3000 Fix 1] Microsoft SIP Gateway

Table of Contents

1 Introduction

AudioCodes' Device Manager Pro features a user interface that enables enterprise network administrators to effortlessly and effectively provision and maintain up to 30000 400HD Series IP phones and third-party vendor devices in globally distributed corporations.

The Device Manager Pro client, which network administrators can use to connect to the server, can be any standard web browser supporting HTML5: Microsoft's Edge, Internet Explorer version 11 and later, Chrome (recommended) or Firefox.

REST (Representational State Transfer) based architecture enables statuses, commands and alarms to be communicated between the devices and the server. The devices send their status to the server every hour for display in the user interface.

Accessed from AudioCodes' One Voice Operations Center (referred to as OVOC for short in this document), the Device Manager Pro enables network administrators to effortlessly load configuration files and firmware files on up to 30000 IP phones and third-party vendor devices.

Other actions administrators can perform on multiple phones are to upload a csv file with devices' MAC addresses and SIP credentials (supported in all environments except Skype for Business), approve devices at the press of a button (supported in Skype for Business environments only), send messages to phones' screens, reset phones, and move phones between tenants.

A configuration file template feature lets network administrators customize configuration files per phone model, tenant, and device.

Integrated into the OVOC, the Device Manager Pro server provides added value to AudioCodes' 400HD Series IP phones and third-party vendor devices.

About this Document

This document shows network administrators how to enable automatic provisioning (Zero Touch provisioning) of the AudioCodes devices in an enterprise network from a single central point.

- Network administrators are recommended to refer to AudioCodes' *Device Manager Deployment Guide* which focuses on *the critical steps* to be taken to deploy devices in the enterprise IP network (the guide currently covers deployment of Teams devices).
- For information on third-party vendor products (for example, EPOS, Jabra and Poly), see the Device Manager for Third-Party Vendor Products Administrator's Manual
- For information on the Device Manager Agent, see:
  - ✓ *Device Manager Agent Installation and Configuration Guide*
  - ✓ Managing Device Manager Agents on page 97
- For detailed descriptive information about the Agent, see the *Device Manager Agent Installation and Configuration Guide*.

Zero Touch Provisioning

AudioCodes' IP phones can be automatically provisioned when they are plugged in to the enterprise's network if Zero Touch provisioning has been implemented.

⚠ Applies to all phones irrespective of Skype for Business/non-Skype for Business.

➢ **To implement Zero Touch provisioning:**

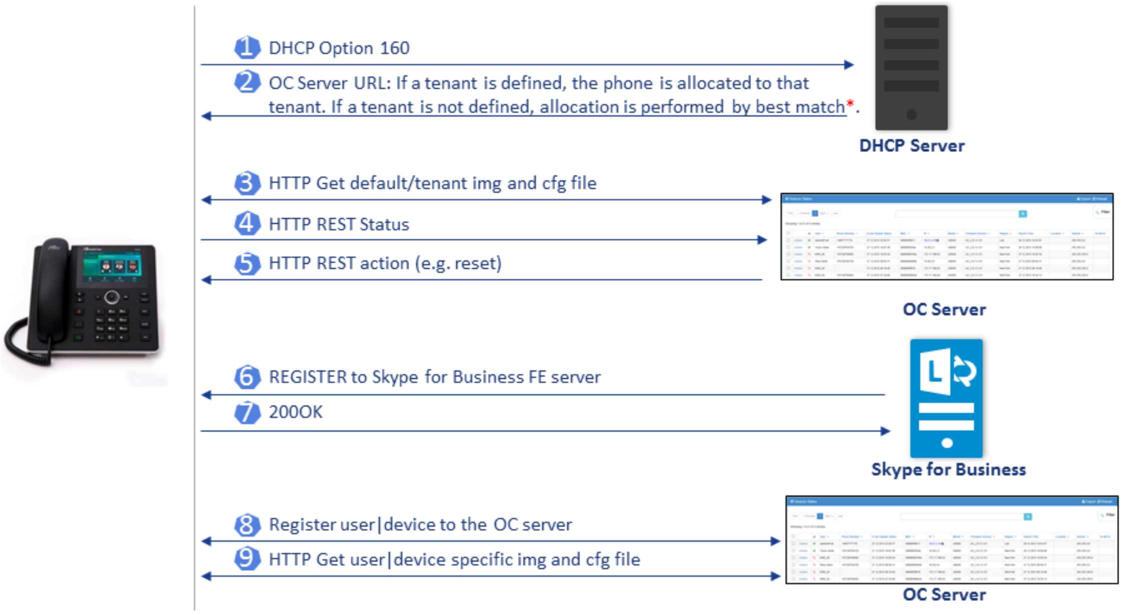
1. Build your network topology of tenants and sites using the One Voice Operations Center (see the *One Voice Operations Center User's Manual* for more information).
2. Start up and log into the Device Manager Pro.
3. Choose the Zero Touch provisioning method. Either:
   - Configure the DHCP server to provision the phone with an IP address that is in the tenant/site range. Configure the phone to receive the IP address or subnet mask of the tenant/site.
   - Use DHCP Option 160.
4. Choose the default template for each tenant and model.

⚠ Phones that reside behind a NAT and whose IP addresses are internal can be managed by the OVOC via SBC HTTP proxy. For more information, see Managing Devices Behind a NAT using SBC HTTP Proxy on page 36.

Zero Touch Provisioning Process - Skype for Business Phone

The figure below illustrates the 1-9 step provisioning process for AudioCodes' IP phones for Skype for Business when the Zero Touch feature is implemented.

Figure 1-1: Zero Touch Provisioning - Skype for Business Phone

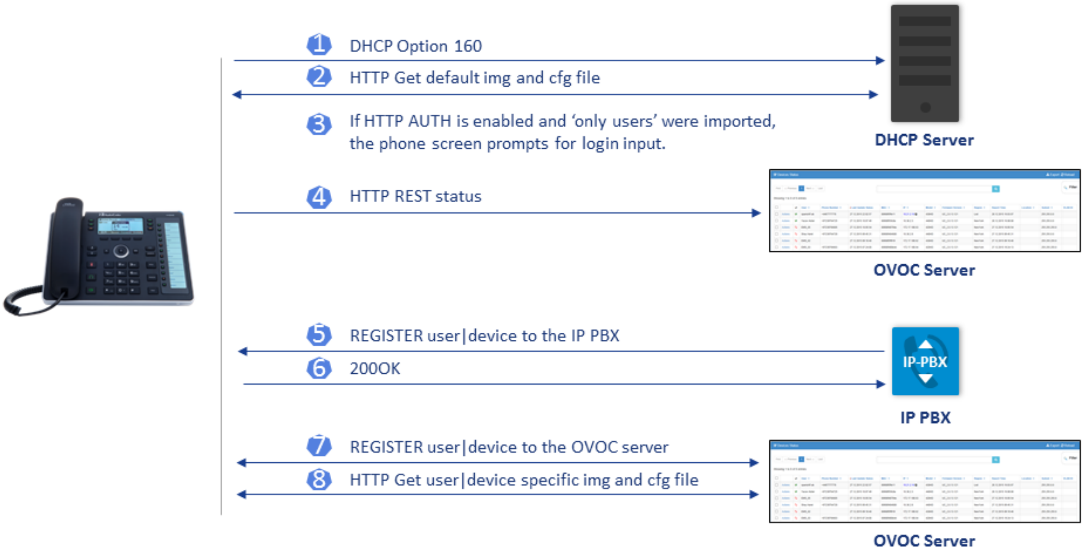

1 DHCP Option 160
2 OC Server URL: If a tenant is defined, the phone is allocated to that tenant. If a tenant is not defined, allocation is performed by best match*.
DHCP Server
3 HTTP Get default/tenant img and cfg file
4 HTTP REST Status
5 HTTP REST action (e.g. reset)
OC Server
6 REGISTER to Skype for Business FE server
7 200OK
Skype for Business
8 Register user|device to the OC server
9 HTTP Get user|device specific img and cfg file
OC Server

*If the network administrator does not define a tenant in the URL in DHCP Option 160, the phone is allocated a tenant/site according to *best match*, that is, according to either tenant Subnet Mask or site Subnet Mask configured in the OVOC. See the *One Voice Operations Center User's Manual* for more information.

Zero Touch Provisioning – non Skype for Business Phone

The figure below illustrates the 1-8 step provisioning process for AudioCodes' non Skype for Business phones when the Zero Touch feature is implemented.

Figure 1-2: Zero Touch Provisioning – non Skype for Business Phone


1 DHCP Option 160
2 HTTP Get default img and cfg file
3 If HTTP AUTH is enabled and 'only users' were imported, the phone screen prompts for login input.
DHCP Server
4 HTTP REST status
OVOC Server
5 REGISTER user|device to the IP PBX
6 200OK
IP-PBX
IP PBX
7 REGISTER user|device to the OVOC server
8 HTTP Get user|device specific img and cfg file
OVOC Server

2 Starting up and Logging in

After installation, start the Device Manager Pro and log in. Before logging in, you need to run the OVOC.

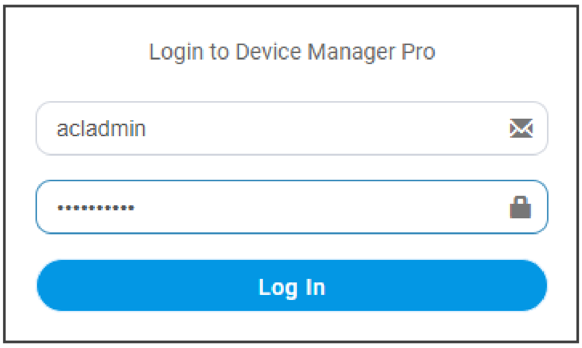
> ⚠
> - To access the Device Manager Pro without running the OVOC, point your web browser to https://<OVOC_IP_Address>/ipp and then in the login screen that opens, log in. If the browser is pointed to HTTP, it will be redirected to HTTPS.
> - Device Manager Pro is a secured web client that runs on any standard web browser supporting HTML5: Internet Explorer v11 and later, Chrome or Firefox.

For information on installing and operating the OVOC, see the *OVOC Server IOM Manual* and the *OVOC User's Manual*.

➢ To log in to the Device Manager Pro via the OVOC:

1. In the OVOC's Network page, click the **Endpoints** tab and from the dropdown select **Configuration** . The Login to Device Manager Pro screen opens.

Figure 2-1: Login



Login to Device Manager Pro

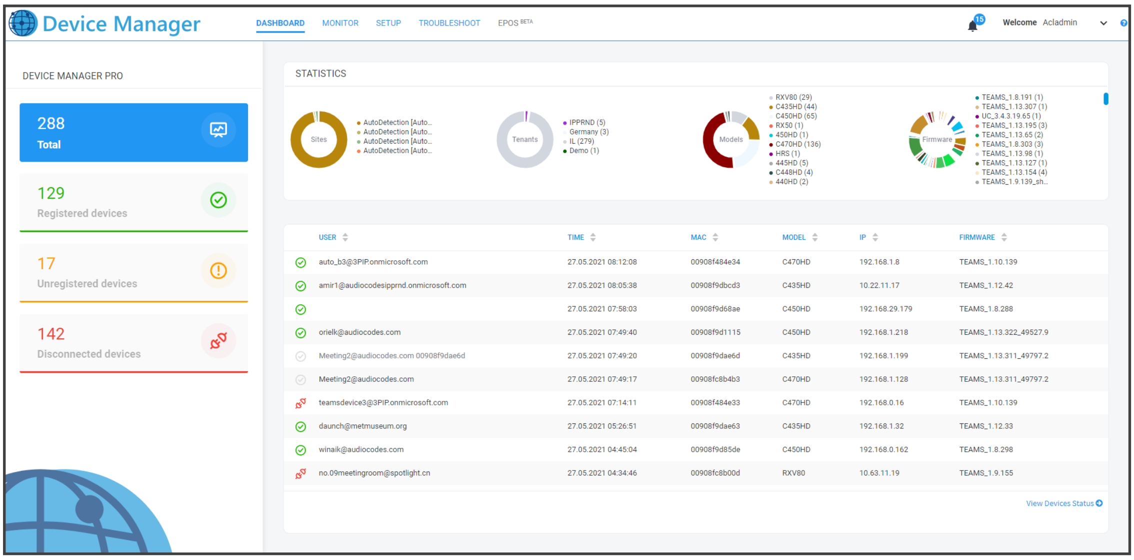
acladmin

••••••••••

> ⚠ The 'Username' and 'Password' used to log in to the Device Manager Pro are the same as those used to log in to the OVOC.

2. Enter your Username and Password (default = **acladmin** and **pass_1234**) and click **Sign In**; the application is launched and the Monitor Dashboard is displayed.

Figure 2-2: Monitor Dashboard



	USER	TIME	MAC	MODEL	IP	FIRMWARE
✓	auto_b3@3PIP.onmicrosoft.com	27.05.2021 08:12:08	00908f484e34	C470HD	192.168.1.8	TEAMS_1.10.139
✓	amir1@audiocodesipprnd.onmicrosoft.com	27.05.2021 08:05:38	00908f9dbcd3	C435HD	10.22.11.17	TEAMS_1.12.42
✓		27.05.2021 07:58:03	00908f9d68ae	C450HD	192.168.29.179	TEAMS_1.8.288
✓	orielk@audiocodes.com	27.05.2021 07:49:40	00908f9d1115	C450HD	192.168.1.218	TEAMS_1.13.322_49527.9
✓	Meeting2@audiocodes.com 00908f9dae6d	27.05.2021 07:49:20	00908f9dae6d	C435HD	192.168.1.199	TEAMS_1.13.311_49797.2
✓	Meeting2@audiocodes.com	27.05.2021 07:49:17	00908fc8b4b3	C470HD	192.168.1.128	TEAMS_1.13.311_49797.2
	teamsdevice3@3PIP.onmicrosoft.com	27.05.2021 07:14:11	00908f484e33	C470HD	192.168.0.16	TEAMS_1.10.139
✓	daunch@metmuseum.org	27.05.2021 05:26:51	00908f9dae63	C435HD	192.168.1.32	TEAMS_1.12.33
✓	winaik@audiocodes.com	27.05.2021 04:45:04	00908f9d85de	C450HD	192.168.0.162	TEAMS_1.8.298
	no.09meetingroom@spotlight.cn	27.05.2021 04:34:46	00908fc8b00d	RXV80	10.63.11.19	TEAMS_1.9.155

- See Monitoring and Maintaining the Phone Network on page 38 for more information about monitoring phones.
- The following topics show how to provision phones using Zero Touch.

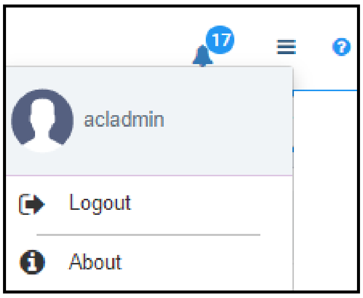
Viewing the About Screen

The About screen allows network administrators to access information about the Device Manager as well as to log out of the application from whatever page they're in. The screen is aligned with the About screen in the OVOC.

➢ To view the About screen:

- In any page in the Device Manager, click the icon ☰

Figure 2-3: About



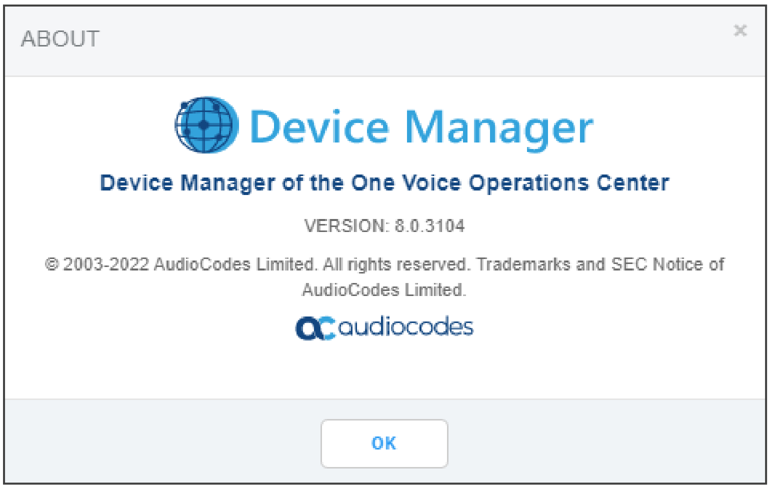
➢ To log out:

- Click the **Logout** option.

➢ To view version information:

- Click the **About** option.

Figure 2-4: About - Version



ABOUT

Device Manager

Device Manager of the One Voice Operations Center

VERSION: 8.0.3104

© 2003-2022 AudioCodes Limited. All rights reserved. Trademarks and SEC Notice of AudioCodes Limited.

3 Adding Users & Devices in Non-Skype for Business Environments

Administrators can import

- users *and* devices -or-
- only users

If the administrator imports users *and* devices, the association between users and devices was made before Version 7.6

- using the device's MAC address
- through user name and password
- via an imported CSV file
- before deployment

➢ To add users *and* devices with a version earlier than Version 7.6 of Device Manager Pro:

- After plugging the phones into the network, log in to Device Manager Pro and then (best practice):
  - Export the automatically created 'System User' to a zip file (see Exporting 'System User' to zip File on page 11)
  - Unzip the zip file, open the csv file and add users and devices in the same format (see Adding Users and Devices Information to the csv File on page 13)
  - Import the csv file with users and devices back into Device Manager Pro (see Importing the csv File on page 13

➢ To add *only* users:

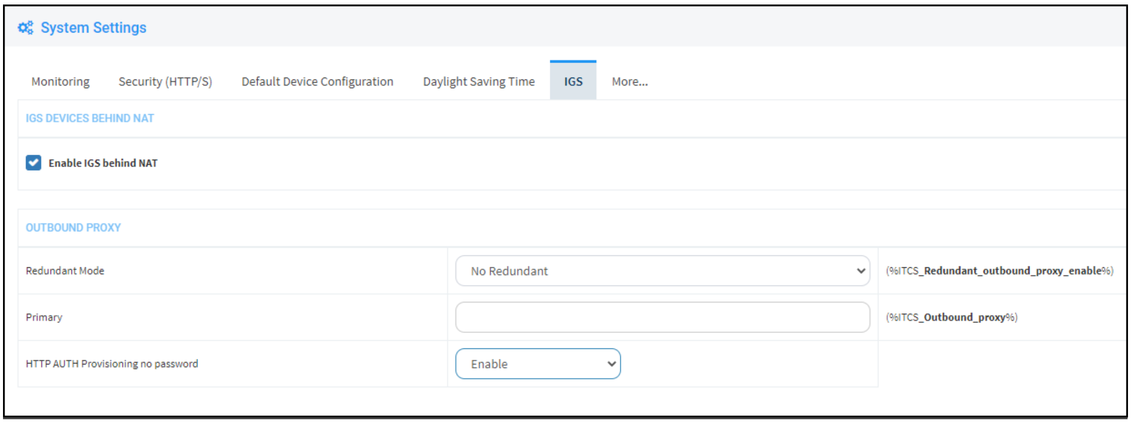
- Applies only to Version 7.6 and later
- The association is manually made after deployment, using the **Approve** button in the Devices Status page
- When the phone is connected to the network for the first time, the user is prompted to enter their username/password; it's matched with that on the Device Manager Pro. After the match, the Manager associates the device with the user. Usernames/ passwords are then uploaded to the Manager through the import CSV *without using MAC address*. After authentication, the Manager downloads the cfg file to the phone.

1. After installing the Device Manager Pro, add the HTTP authentication configuration properties to the initial configuration file (taken from DHCP Options 160) and to the templates.
2. Select an authentication mode. Two possibilities are available:

- With username/password
- Without password; only username or extension

> - The default authentication mode is username/password
> - The Login screen then allows the user to authenticate with username only, excluding password
> - If you want the user to use 'password only' for authentication, enable the 'no password' option

Figure 3-1: System Settings Page - HTTP AUTH Provisioning No Password



System Settings

IGS DEVICES BEHIND NAT

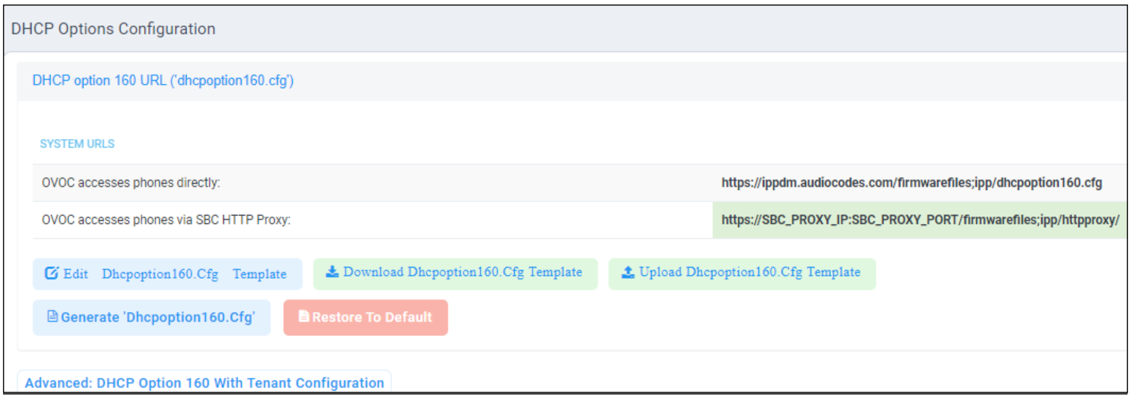
☑ Enable IGS behind NAT

OUTBOUND PROXY

Redundant Mode	No Redundant	(%ITCS_Redundant_outbound_proxy_enable%)
Primary		(%ITCS_Outbound_proxy%)
HTTP AUTH Provisioning no password	Enable	

3. Configure DHCP Options for HTTP Authentication. To prompt the user for username and password, add the following HTTP authentication parameters to the DHCP option 160 cfg file:
   - provisioning/configuration/http_auth/password=
   - provisioning/configuration/http_auth/ui_interaction_enabled=1
   - provisioning/configuration/http_auth/user_name=
4. Update the parameter 'provisioning/configuration/url'
   - provisioning/configuration/url=<HTTP_OR_S>://<IP_ADDRESS>/ip-p/admin/httpauth/auth_prov.php
5. Open the DHCP Option Configuration page (**Setup** > **Settings** > **DHCP Options Configuration**)

Figure 3-2: DHCP Options Configuration



DHCP Options Configuration

DHCP option 160 URL ('dhcpoption160.cfg')

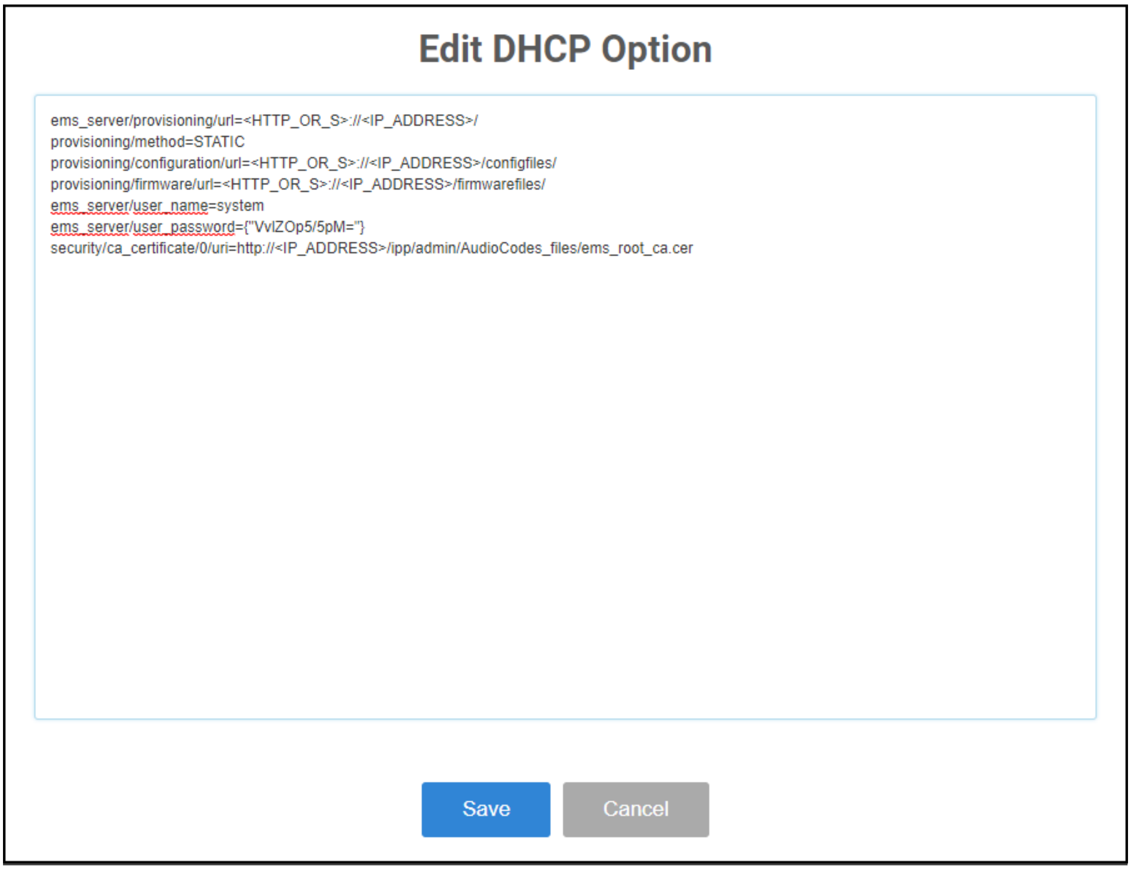
SYSTEM URLS

OVOC accesses phones directly:	https://ippdm.audiocodes.com/firmwarefiles;ipp/dhcpoption160.cfg
OVOC accesses phones via SBC HTTP Proxy:	https://SBC_PROXY_IP:SBC_PROXY_PORT/firmwarefiles;ipp/httpproxy/

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

6. Click **Edit configuration template**:

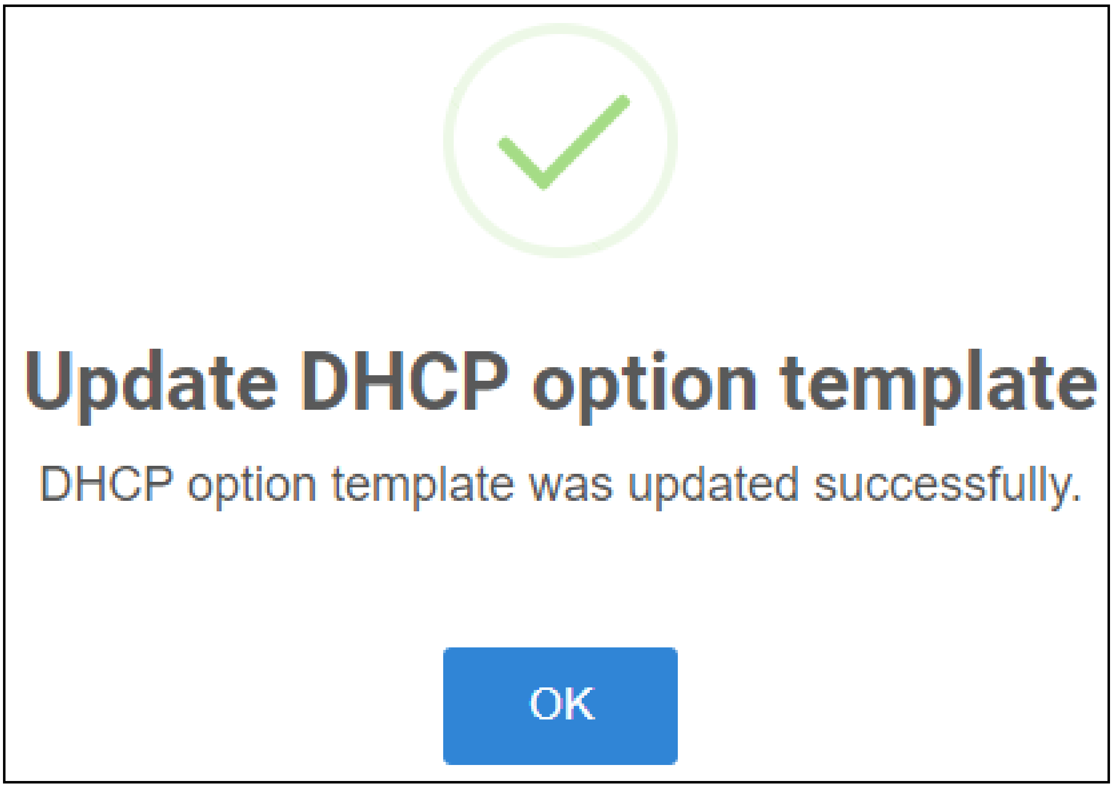
Figure 3-3: Edit DHCP Option



Edit DHCP Option

```
ems_server/provisioning/url=<HTTP_OR_S>://<IP_ADDRESS>/
provisioning/method=STATIC
provisioning/configuration/url=<HTTP_OR_S>://<IP_ADDRESS>/configfiles/
provisioning/firmware/url=<HTTP_OR_S>://<IP_ADDRESS>/firmwarefiles/
ems_server/user_name=system
ems_server/user_password={"VvlZOp5/5pM="}
security/ca_certificate/0/uri=http://<IP_ADDRESS>/ipp/admin/AudioCodes_files/ems_root_ca.cer
```

7. Click **Save**; you're prompted:



Update DHCP option template

DHCP option template was updated successfully.

8. Click **OK**.

⚠ If you want password to be excluded from HTTP user authentication, configure parameter 'provisioning/configuration/http_auth/password' to **1234**. Users will then not have to enter a password when performing authentication.

9. Configure each template to operate with HTTP authentication. Open each template you want to operate with HTTP authentication and add the following values to each:

   - provisioning/configuration/http_auth/password=%ITCS_Line1AuthPassword%
   - provisioning/configuration/http_auth/ui_interaction_enabled=1
   - provisioning/configuration/http_auth/user_name=%ITCS_Line1AuthName%

10. Update the parameter 'provisioning/configuration/url':

    - provisioning/configuration/url=%ITCS_HTTP_OR_S%://%ITCS_HTTP_PROXY_IP%:%ITCS_HTTP_PROXY_PORT%/ipp/admin/httpauth/auth_prov.php

11. Close the Directory 'configfiles'. For security reasons, it's preferable to close the 'configfiles' web directory as from now on all cfg files will be downloaded from the new location **http:<SERVER_IP_ADDRESS>/ipprest/lync_auto_prov.php** rather than from **http:<SERVER_IP_ADDRESS>/configfiles/MAC.cfg**

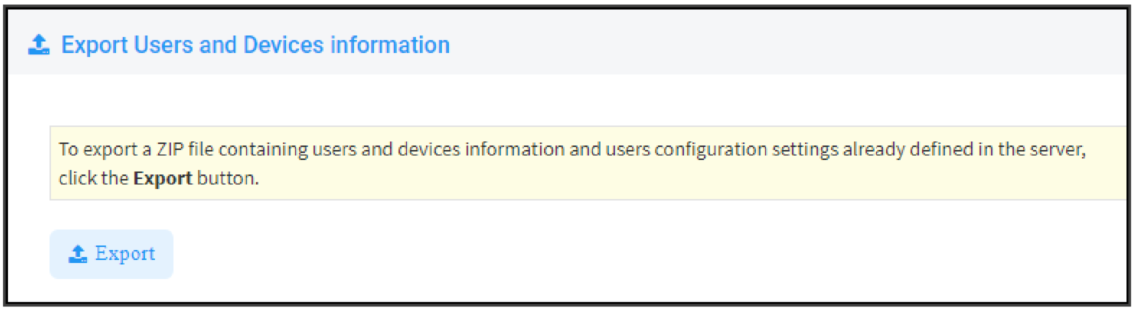
Exporting 'System User' to zip File

Here's how to export the 'system user' that is automatically created after you log in to Device Manager Pro, to a zip file.

➢ To export the 'system user' to a zip file:

1. Open the Export Users and Devices Information page (**Setup** > **Import/Export**).

Figure 3-4: Export Users and Devices Information

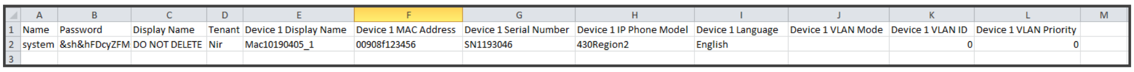


Export Users and Devices information

To export a ZIP file containing users and devices information and users configuration settings already defined in the server, click the **Export** button.

2. Click **Export**; a link to the *users.zip* file is added to the lowermost left corner of the page.
3. Click the link; the unzipped file opens displaying a csv file and a cfg file.
4. Open the csv (in Excel):

Figure 3-5: csv File in Excel



	A	B	C	D	E	F	G	H	I	J	K	L	M
1	Name	Password	Display Name	Tenant	Device 1 Display Name	Device 1 MAC Address	Device 1 Serial Number	Device 1 IP Phone Model	Device 1 Language	Device 1 VLAN Mode	Device 1 VLAN ID	Device 1 VLAN Priority	
2	system	&sh&hFDcyZFM	DO NOT DELETE	Nir	Mac10190405_1	00908f123456	SN1193046	430Region2	English		0	0	
3													

Excel displays the information related to 'system user'.

Adding Users and Devices Information to the csv File

You need to add to the csv file the information related to all the users and devices in your enterprise's network.

> ⚠ To facilitate this task, you can export a csv from your enterprise PBX and then edit it to conform to the 'system user' csv row shown in the figure above and the columns shown in the table below.

Table 3-1: csv File Information

Name	Password	Display Name	Tenant	Display Name	Serial	MAC Address	Phone Model	Language	VLAN Mode	VLAN ID	VLAN Priority

Up to 30000 users and devices can be defined in the csv file. After defining users and devices, save the csv file on your desktop from where you can import it into the Device Manager Pro.

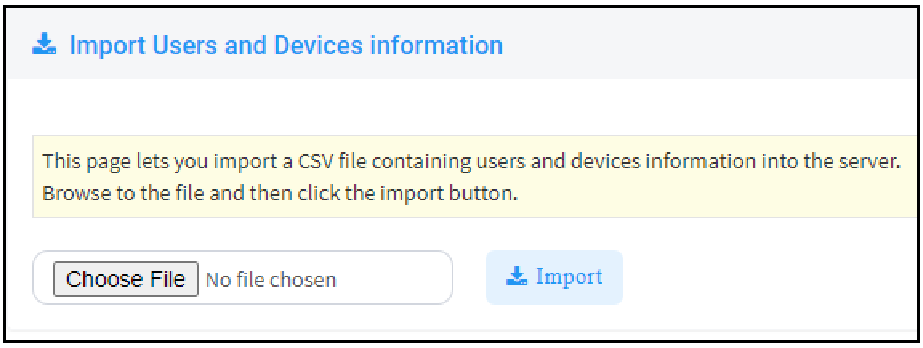
Importing the csv File

After adding to the csv file the information related to all the users and devices in your enterprise's network, import the new csv file into the Device Manager Pro.

➢ To import the new csv file into the Device Manager Pro:

1. Open the Import Users & Devices Information page (**Setup** > **Import/Export**).

Figure 3-6: Import Users & Devices Information



Import Users and Devices information

This page lets you import a CSV file containing users and devices information into the server. Browse to the file and then click the import button.

2. Click **Import** and then navigate to and select the csv file which you created and saved on your desktop previously; the file is imported into the Device Manager Pro.
3. Open the Manage Users page (**Setup** > **Users & Devices**) and make sure all enterprise users you imported are displayed.

4 Using the Zero Touch Setup Wizard to Provision Phones

When plugged in to the enterprise network, phones can automatically be provisioned through the Zero Touch feature.

- Zero Touch determines which *template* the phone will be allocated.
- The template is allocated *per phone model* and *per phone tenant*.
- The template determines which *firmware file* and *configuration file* the phone will be allocated.

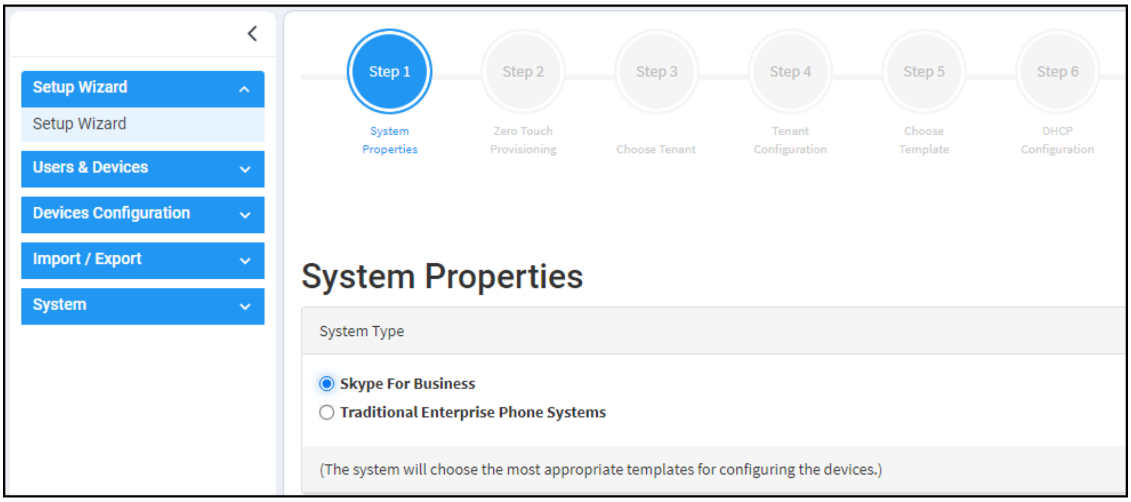
> ⚠ Zero Touch provisioning *accelerates uptime* by enabling multiple users and phones to automatically be provisioned and added to the Manager.

You can use the Setup Wizard feature to *set up* Zero Touch provisioning. The Wizard simplifies deployment of phones in the enterprise for network administrators. The Wizard's functions were already implemented in versions of Device Manager Pro earlier than Version 7.4, only now they're centralized in a single location for a friendlier deployment experience. Here're the steps to follow to provison phones using the Wizard.

➢ To provison phones using the Zero Touch Setup Wizard:

1. In the main screen, click the 'Setup' menu and then click the **Setup Wizard** option.

Figure 4-1: Step 1 – System Type



System Properties

System Type

● Skype For Business

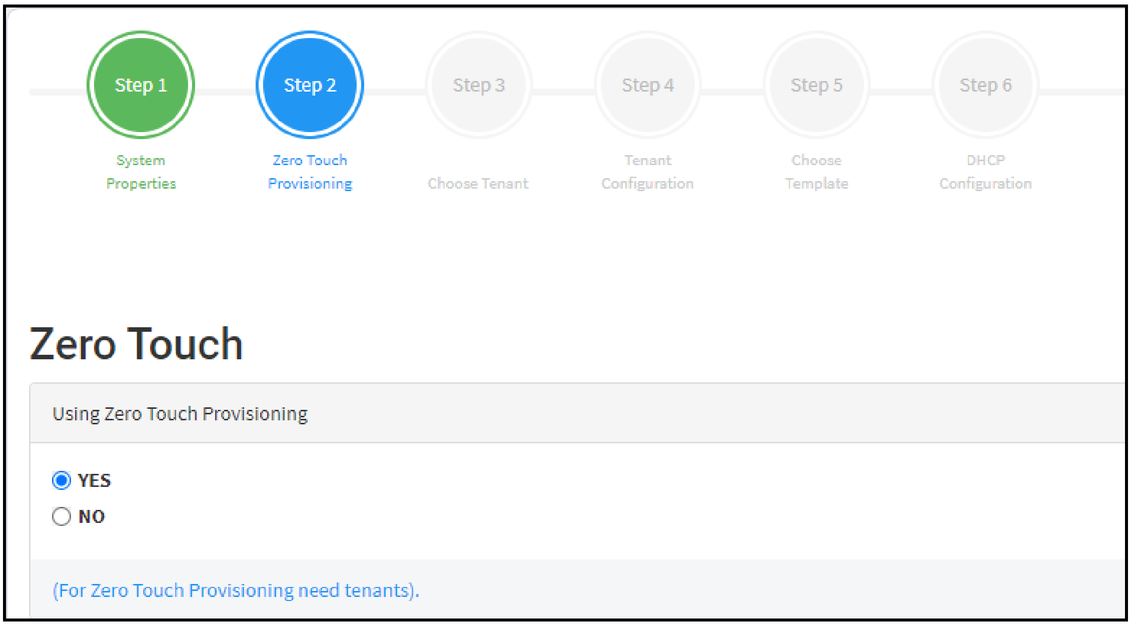
○ Traditional Enterprise Phone Systems

(The system will choose the most appropriate templates for configuring the devices.)

2. Select **Skype for Business** if it isn't selected already, and then click **Next**.

> ⚠ The Setup Wizard will be closed if you intend to use other PBXs besides Skype for Business. The Setup Wizard is intended exclusively for Skype for Business.

Figure 4-2: Step 2 - Zero Touch



Zero Touch

Using Zero Touch Provisioning

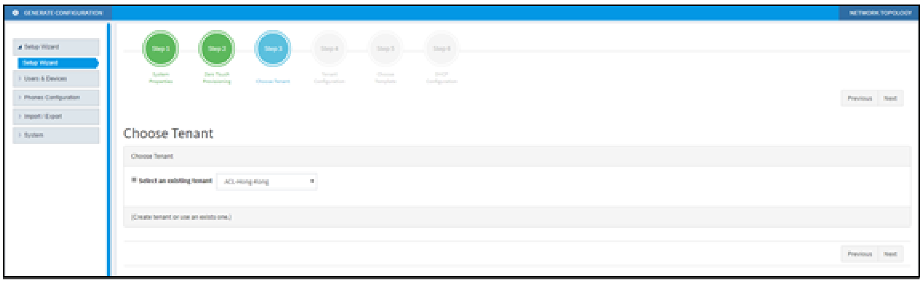
● YES

○ NO

(For Zero Touch Provisioning need tenants).

3. Select **Yes** and then click **Next**.

Figure 4-3: Step 3 – Choose Tenant



Choose Tenant

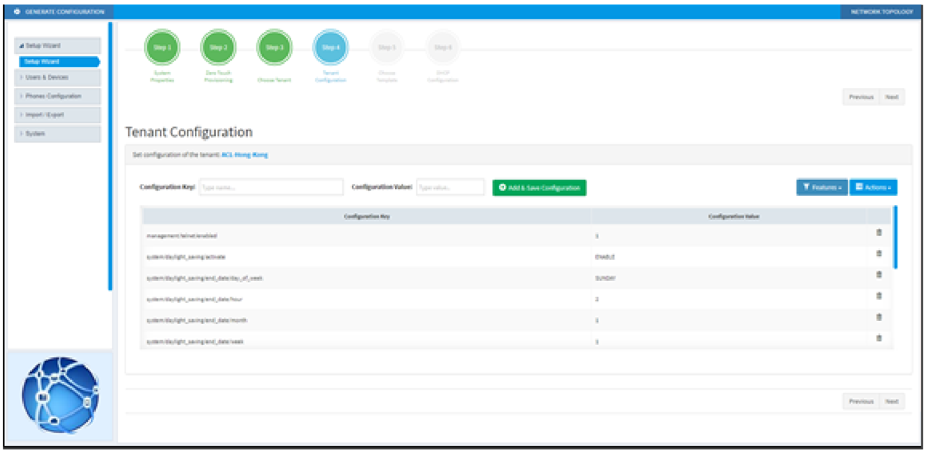
Choose Tenant

● Select an existing tenant: ACL Hong Kong

(Create tenant or use an exists one.)

4. Choose an existing tenant from the dropdown and click **Next**. If a tenant doesn't already exist, click **Next** and configure one. This is to be able to create a specific configuration for the tenant and configure the URL in DHCP Option 160 so devices will use this tenant. If there's no specific tenant configuration to configure, click **Next**.

Figure 4-4: Step 4 – Tenant Configuration



Tenant Configuration

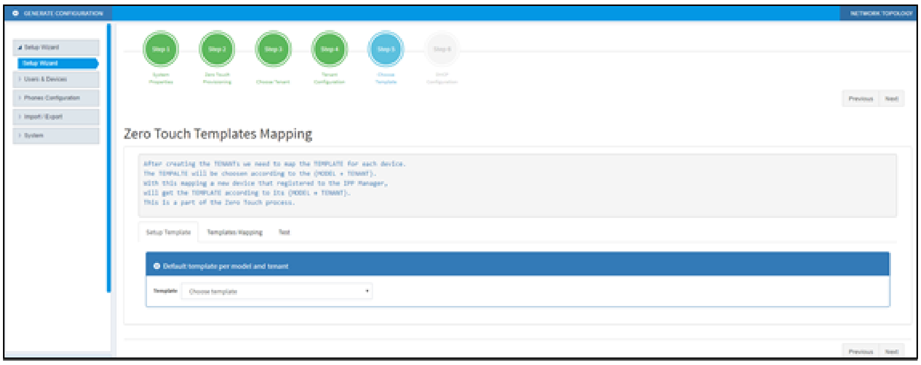
Set configuration of the tenant: ACL Hong Kong

Configuration Key: Type name... Configuration Value: Type value...

Configuration Key	Configuration Value
management/telnet/enabled	1
system/daylight_saving/activate	ENABLE
system/daylight_saving/end_date/day_of_week	SUNDAY
system/daylight_saving/end_date/hour	2
system/daylight_saving/end_date/month	1
system/daylight_saving/end_date/week	1

5. Click **Next**.

Figure 4-5: Step 5 – Templates Mapping



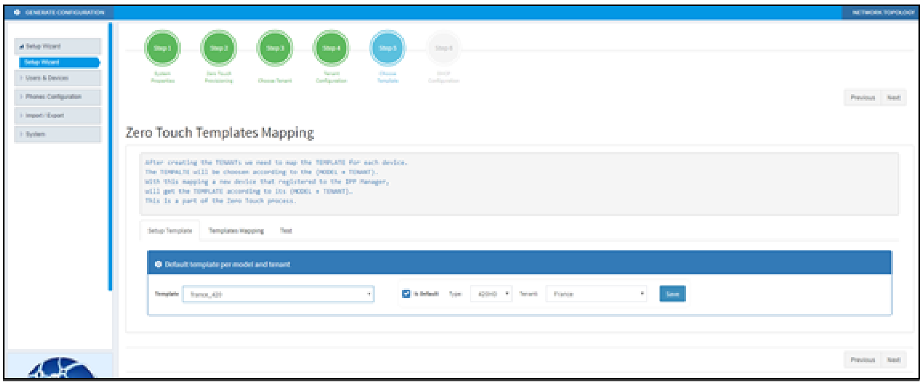
Zero Touch Templates Mapping

```
After creating the TENANTs we need to map the TEMPLATE for each device.
The TEMPALTE will be choosen according to the (MODEL + TENANT).
With this mapping a new device that registered to the IPP Manager,
will get the TEMPLATE according to its (MODEL + TENANT).
This is a part of the Zero Touch process.
```

Template: Choose template

6. From the 'Template' dropdown, choose a template.

Figure 4-6: Step 5 – Templates Mapping



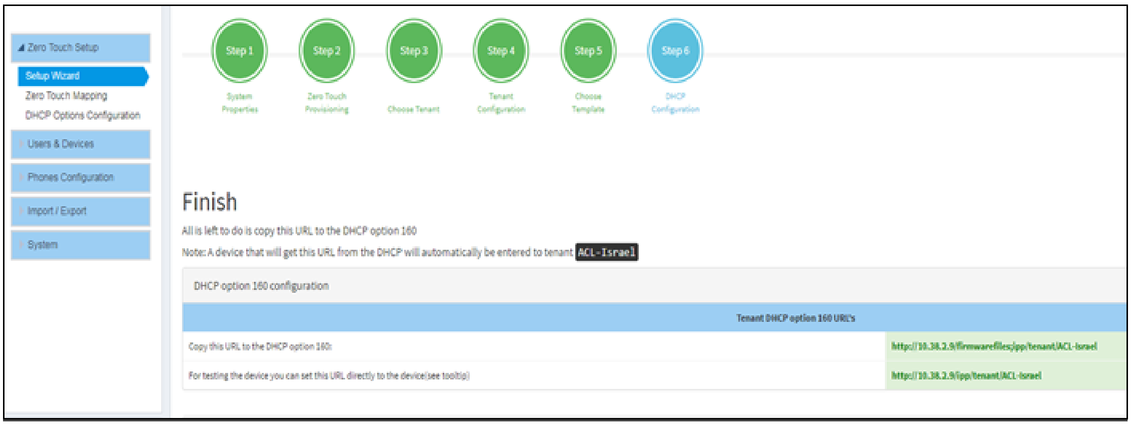
Zero Touch Templates Mapping

```
After creating the TENANTs we need to map the TEMPLATE for each device.
The TEMPALTE will be choosen according to the (MODEL + TENANT).
With this mapping a new device that registered to the IPP Manager,
will get the TEMPLATE according to its (MODEL + TENANT).
This is a part of the Zero Touch process.
```

Template: france_420 ☑ Is Default Type: 420HD Tenant: France

7. Associate a template according to the MODEL and TENANT. The page displays a mapping table in which you need to map {MODEL + TENANT} to TEMPLATE.
   a. Select 'IsDefault'; from this point on, the template chosen will be used.
   b. From the 'Phone' dropdown, select the model.
   c. From the 'Tenant' dropdown, select the tenant and then click **Next**.

Figure 4-7: Step 6 – DHCP Configuration



Finish

All is left to do is copy this URL to the DHCP option 160

Note: A device that will get this URL from the DHCP will automatically be entered to tenant ACL-Israel

DHCP option 160 configuration

Tenant DHCP option 160 URL's	
Copy this URL to the DHCP option 160:	http://10.38.2.9/firmwarefiles;ipp/tenant/ACL-Israel
For testing the device you can set this URL directly to the device(see tooltip)	http://10.38.2.9/ipp/tenant/ACL-Israel

8. Define the URL in DHCP Option 160.

5 Provisioning Phones without the Zero Touch Setup Wizard

You can set up zero touch provisioning in the Manager without using the Setup Wizard. When plugged in to the enterprise network, phones will then automatically be provisioned.

- Zero Touch determines with which *template* the phone will be provisioned.
- The template is provisioned *per phone model* and *per phone tenant*.
- The template determines with which *firmware file* (img) and *configuration file* (cfg) the phone will be provisioned.

> ⚠ Zero Touch accelerates uptime by enabling multiple users and phones to automatically be provisioned and added to the Manager.

Before Implementing Zero Touch

Before implementing Zero Touch, you need to prepare the network.

This applies to:

- the network administrator of the enterprise whose OVOC is installed on premises (in the enterprise's LAN)
- the system integrator of the Service Provider whose OVOC is installed in the cloud (WAN)

➢ **To prepare the network for Zero Touch provisioning:**

1. Prepare a template per tenant (see Preparing a Template for a Tenant/Model on page 20).
2. Upload the firmware .img file to the server (see Uploading .img Firmware File to the Server on page 22).
3. Configure the DHCP server's Option 160 to allocate the phone to the tenant/site URL (see Configuring DHCP Option 160 with a Tenant URL on page 23).

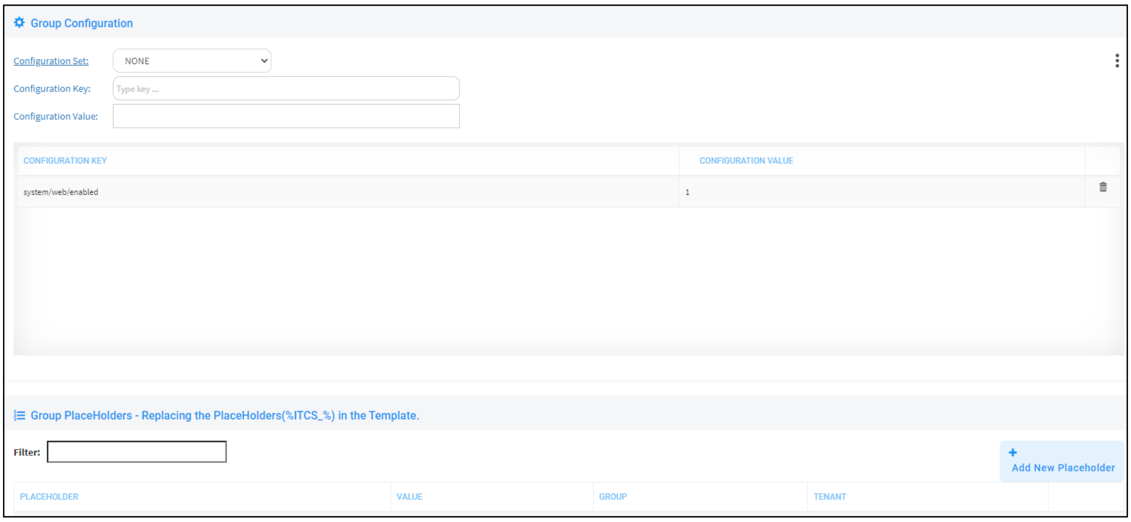
Configuring an Endpoints Group

After adding a group to the OVOC as shown in the *OVOC User's Manual*, you can add an end-point - or multiple endpoints - to that group as shown in Checking Devices Status on page 42 under the action **Change Group**, and then you can configure the endpoints in the group as shown here. The feature benefits a customer who wants for example 10 of 500 phones in a site in their enterprise organized in a group for a software upgrade to apply exclusively to the 10 phones in that group. In contrast to sites, groups are *logical* entities but configuration of both are identical; both are per tenant.

➢ To configure an endpoints group:

1. Open the Group Configuration page (**Setup** > **Configuration** > **Group Configuration**).

Figure 5-1: Group Configuration



Group Configuration

Configuration Set: NONE

Configuration Key: Type key ...

Configuration Value:

CONFIGURATION KEY	CONFIGURATION VALUE
system/web/enabled	1

Group PlaceHolders - Replacing the PlaceHolders(%ITCS_%) in the Template.

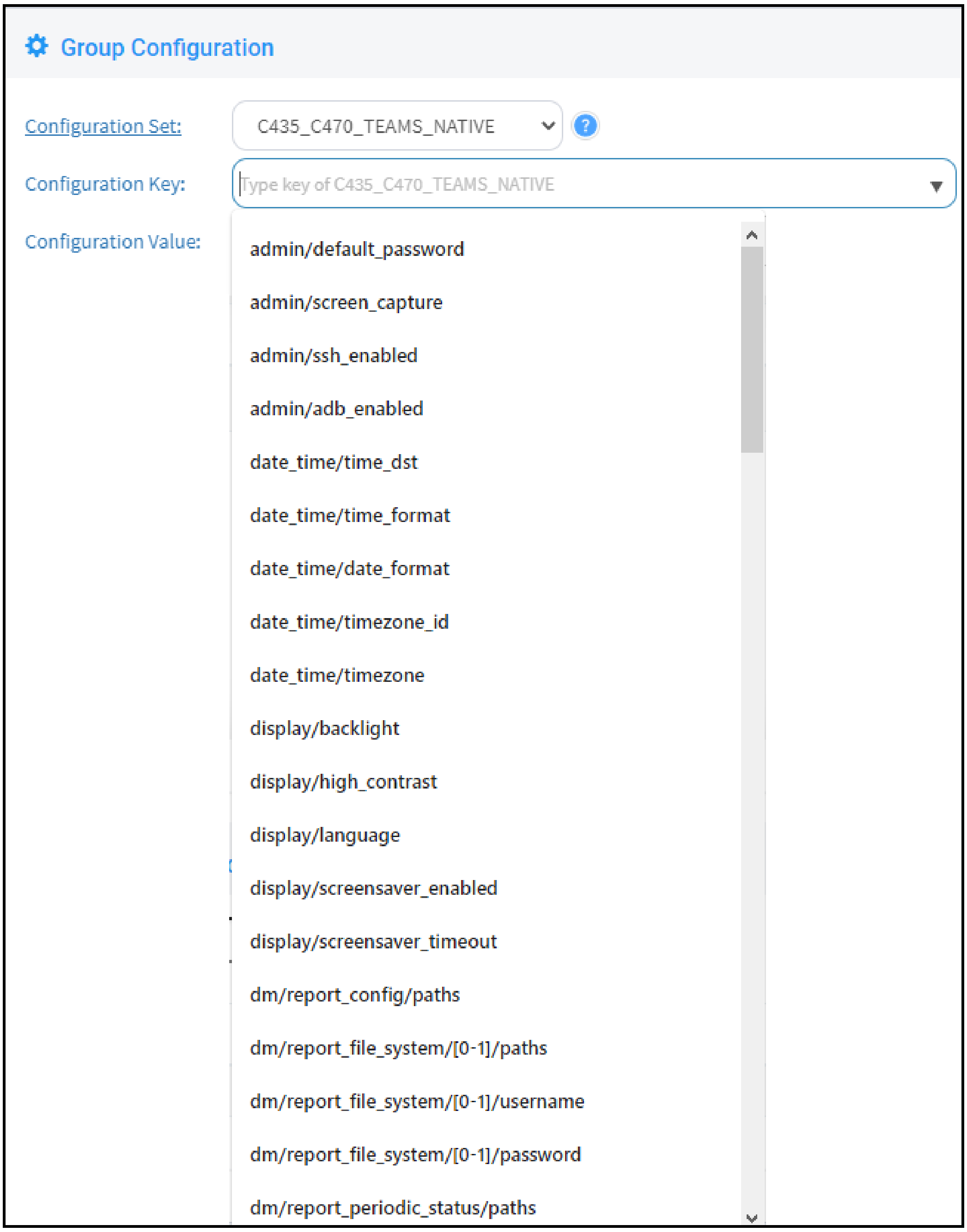
Filter:

PLACEHOLDER	VALUE	GROUP	TENANT

2. From the 'Select Group' drop-down, choose the group (added to the OVOC) under which you want to organize endpoints.

3. From the 'Configuration Key' drop-down, select a parameter to configure for the endpoints group.

Figure 5-2: Configuration Key



Group Configuration

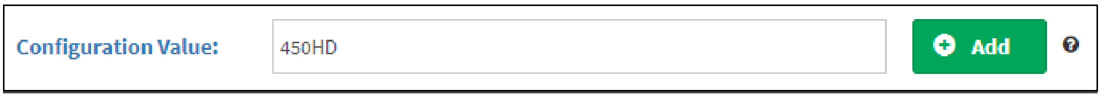
Configuration Set: C435_C470_TEAMS_NATIVE

Configuration Key: Type key of C435_C470_TEAMS_NATIVE

Configuration Value:

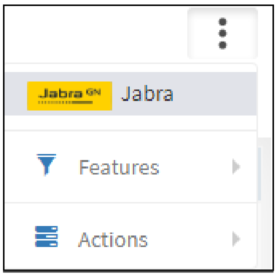
- admin/default_password
- admin/screen_capture
- admin/ssh_enabled
- admin/adb_enabled
- date_time/time_dst
- date_time/time_format
- date_time/date_format
- date_time/timezone_id
- date_time/timezone
- display/backlight
- display/high_contrast
- display/language
- display/screensaver_enabled
- display/screensaver_timeout
- dm/report_config/paths
- dm/report_file_system/[0-1]/paths
- dm/report_file_system/[0-1]/username
- dm/report_file_system/[0-1]/password
- dm/report_periodic_status/paths

4. In the 'Configuration Value' field displayed after a selection, provision the parameter with a value and then click **Add**. Click **?** for more information if necessary.

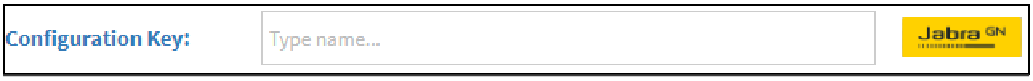


Configuration Value: 450HD

5. To configure Jabra endpoints group parameters, click ⋮ adjacent to the 'Configuration Key' field and select **Jabra**.

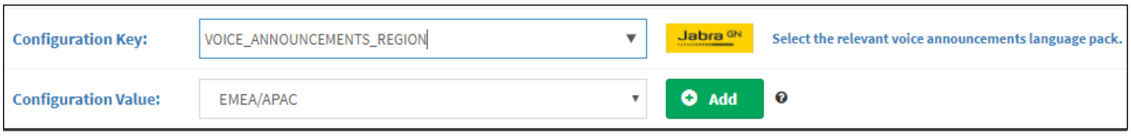


6. View the following:



Configuration Key: Type name...

7. From the 'Configuration Key' drop-down, select a Jabra parameter to configure for the Jabra endpoints group.



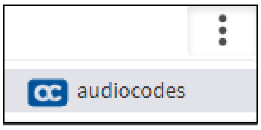
Configuration Key: VOICE_ANNOUNCEMENTS_REGION

Select the relevant voice announcements language pack.

Configuration Value: EMEA/APAC

8. In the 'Configuration Value' field displayed after a selection, provision the parameter with a value and then click **Add**. Click **?** for more information if necessary.

9. To switch back to an AudioCodes (non Jabra) endpoints group, click ⋮ adjacent to the 'Configuration Key' field and select **AudioCodes**.



Preparing a Template for a Tenant/Model

You need to prepare a template per tenant / type (phone model) in the deployment. The template informs the server how to generate the .cfg configuration file when the phones are plugged in to the network. When the phones are plugged in, the .cfg configuration file is downloaded to them from the server.

⚠ User-configured Speed Dials and Programmable Keys are saved in the device's cfg file and backed up on the server. After the user configures them (see the device's *User's Manual* for details), the phone automatically updates the cfg file on the server. They're downloaded to the phone after:

- they're deleted or some other 'crisis' occurs
- the phone is restored to factory defaults
- the user starts working with a new device
- the user deploys another device at their workstation
- the user's phone is upgraded

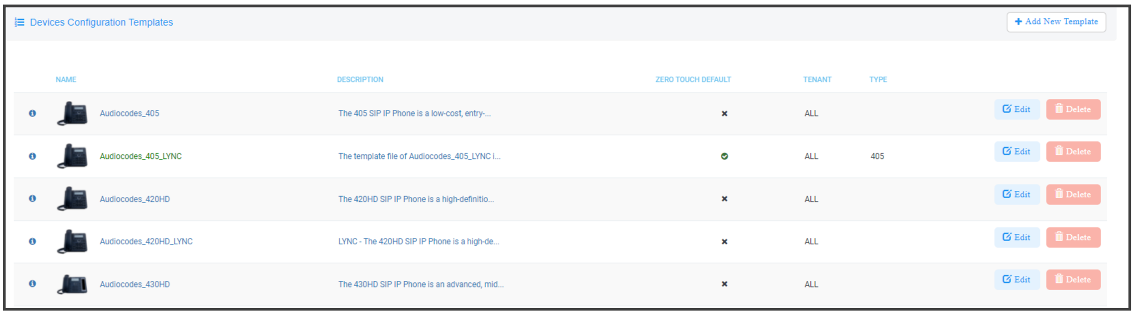
This saves the user from having to configure Speed Dials and Programmable Keys from the beginning. The user only needs to configure them once, initially.

If there is no cfg file on the server, the server gets the data from the phone.

➢ To prepare a template for a tenant / phone model:

1. Open the 'Add new template' screen (**Setup** > **Configuration** > **Templates**).

Figure 5-3: Devices Configuration Templates



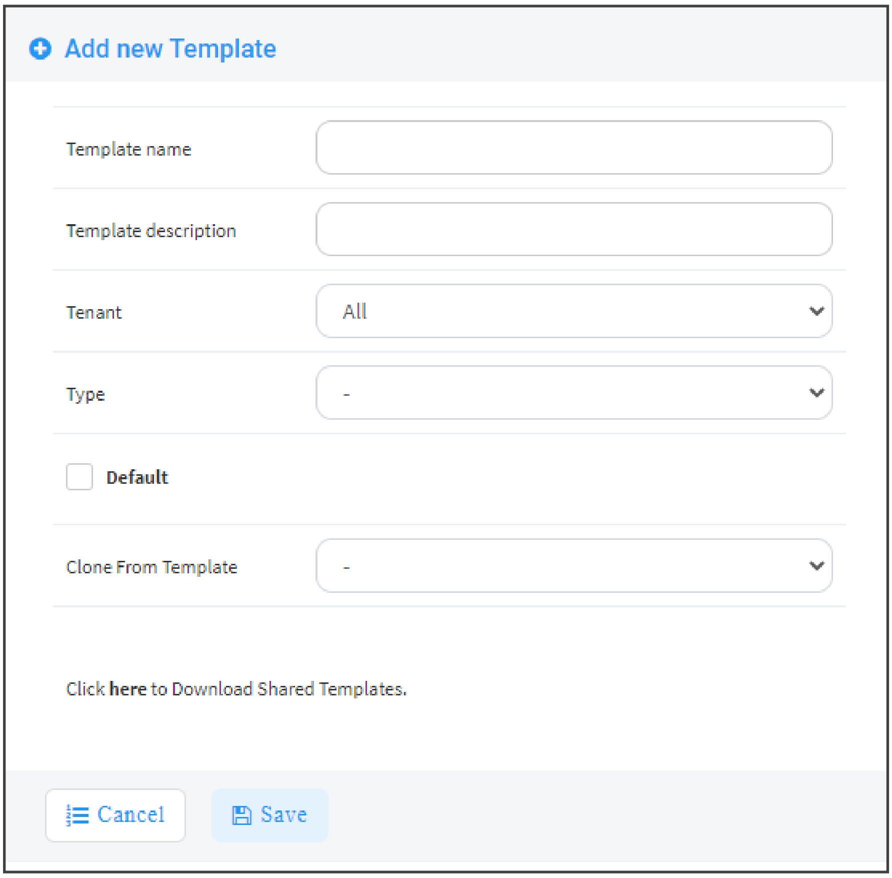
Devices Configuration Templates

		NAME	DESCRIPTION	ZERO TOUCH DEFAULT	TENANT	TYPE		
ℹ		Audiocodes_405	The 405 SIP IP Phone is a low-cost, entry-...	✖	ALL		Edit	Delete
ℹ		Audiocodes_405_LYNC	The template file of Audiocodes_405_LYNC i...	✓	ALL	405	Edit	Delete
ℹ		Audiocodes_420HD	The 420HD SIP IP Phone is a high-definitio...	✖	ALL		Edit	Delete
ℹ		Audiocodes_420HD_LYNC	LYNC - The 420HD SIP IP Phone is a high-de...	✖	ALL		Edit	Delete
ℹ		Audiocodes_430HD	The 430HD SIP IP Phone is an advanced, mid...	✖	ALL		Edit	Delete

⚠ For information on third-party vendor products, see the Device Manager for Third-Party Vendor Products Administrator's Manual

2. Click the **Add New Template** button.

Figure 5-4: Add New Template



Add new Template

Template name	
Template description	
Tenant	All
Type	-
□ **Default**	
Clone From Template	-

Click **here** to Download Shared Templates.

3. Enter a name for the template. Make the name intuitive. Include tenant *and* model aspects in it.

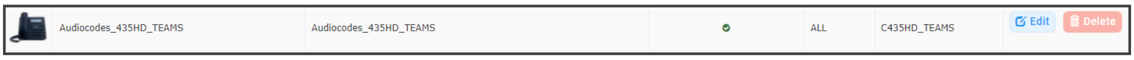
4. Provide a description of the template to enhance intuitive maintenance.

5. From the 'Tenant' dropdown list, select the tenant.

6. From the 'Type' dropdown list, select the phone model.

7. Select the **Default Tenant** option for the template to be the default for this tenant. More than one phone type can be in a tenant. All can have a common template. But only one template can be configured for a tenant. If a second template is configured for the tenant, it overrides the first. After a template is added, it's displayed as shown below in the Devices Configuration Template page (**Setup** > **Configuration** > **Templates**). When a phone is then connected to the network, if the phone is of this type and located in this tenant, it will automatically be provisioned via the DHCP server from the OVOC provisioning server (Zero Touch).

Figure 5-5: Default Template Indication



	Audiocodes_435HD_TEAMS	Audiocodes_435HD_TEAMS	✓	ALL	C435HD_TEAMS

8. From the 'Clone From Template' dropdown list, select a template to clone from. If the template is for phones in a tenant that are Microsoft Skype for Business phones, choose a Skype for Business template.

9. Do this for all tenants and types (phone models) in the network.

10. If necessary, click the **here** link in 'Click **here** to Download Shared Templates'; your browser opens displaying AudioCodes share file in which all templates are located, for example, the templates used with Genesys.

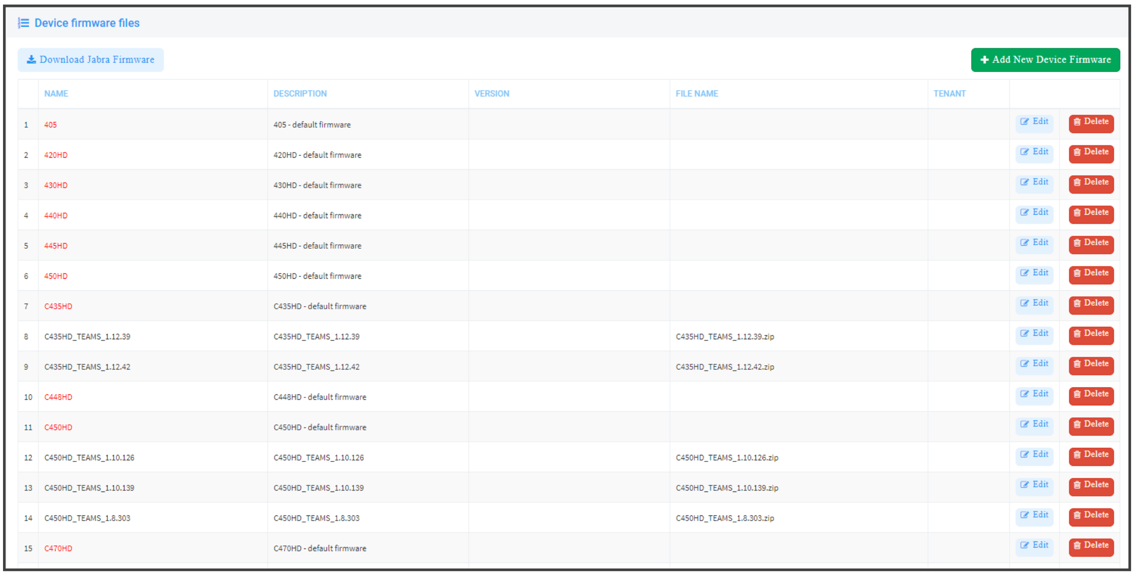
Uploading .img Firmware File to the Server

After obtaining the device's latest .img firmware file from AudioCodes, upload it to the OVOC provisioning server. When devices are later connected to the network, they're automatically provisioned with firmware from the server. You can also upload the .dfu firmware files for the speakers of the Huddle Room Solution (HRS).

➢ To upload the .img firmware file to the OVOC provisioning server:

1. In the Device Manager Pro, access the Firmware Files page (**Setup** > **Firmware** > **Firmware Files**).

Figure 5-6: Phone Firmware Files



	NAME	DESCRIPTION	VERSION	FILE NAME	TENANT		
1	405	405 - default firmware				Edit	Delete
2	420HD	420HD - default firmware				Edit	Delete
3	430HD	430HD - default firmware				Edit	Delete
4	440HD	440HD - default firmware				Edit	Delete
5	445HD	445HD - default firmware				Edit	Delete
6	450HD	450HD - default firmware				Edit	Delete
7	C435HD	C435HD - default firmware				Edit	Delete
8	C435HD_TEAMS_1.12.39	C435HD_TEAMS_1.12.39		C435HD_TEAMS_1.12.39.zip		Edit	Delete
9	C435HD_TEAMS_1.12.42	C435HD_TEAMS_1.12.42		C435HD_TEAMS_1.12.42.zip		Edit	Delete
10	C448HD	C448HD - default firmware				Edit	Delete
11	C450HD	C450HD - default firmware				Edit	Delete
12	C450HD_TEAMS_1.10.126	C450HD_TEAMS_1.10.126		C450HD_TEAMS_1.10.126.zip		Edit	Delete
13	C450HD_TEAMS_1.10.139	C450HD_TEAMS_1.10.139		C450HD_TEAMS_1.10.139.zip		Edit	Delete
14	C450HD_TEAMS_1.8.303	C450HD_TEAMS_1.8.303		C450HD_TEAMS_1.8.303.zip		Edit	Delete
15	C470HD	C470HD - default firmware				Edit	Delete

2. In the Firmware Files screen, click the **Add New Device Firmware** button.

3. Navigate to the .img file and/or .dfu firmware files for the HRS speakers, and upload to the OVOC provisioning server.

Configuring DHCP Option 160 with a Tenant URL

You need to point DHCP Option 160 to a tenant URL so that the phones will be automatically provisioned with their .img firmware file and cfg configuration file when they're plugged in to the network for the first time (Zero Touch provisioning).

Either of the following two methods can be used to implement Zero Touch:

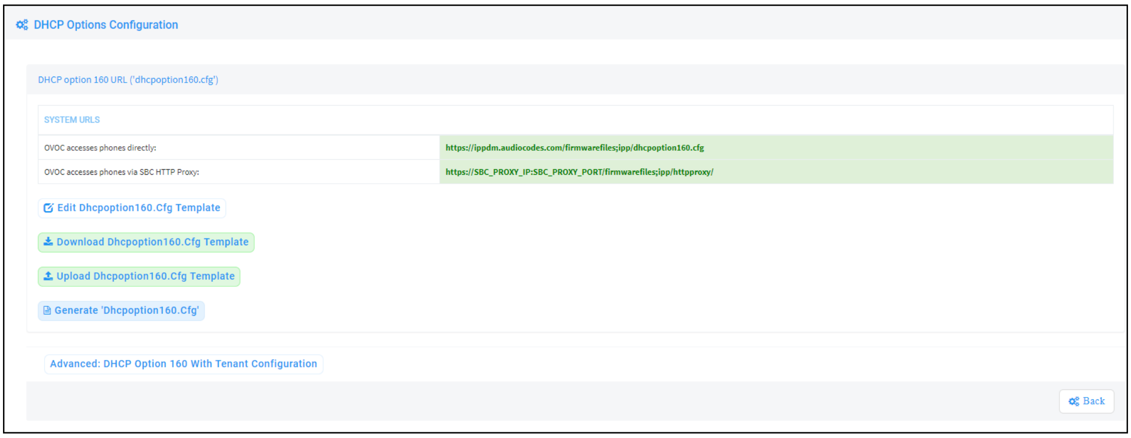
- Configure the DHCP server to provision the phone with an IP address that is in the tenant/site range. Configure the phone to receive the IP address or subnet mask of the tenant/site.
- Use DHCP Option 160

> ⚠ The Device Manager Pro supports backward compatibility so you can point DHCP Option 160 to a region URL. See the *Administrator's Manual* v7.2 and earlier.

Later when the (Skype for Business) phones are signed in, phones and users are automatically added to Device Manager Pro which loads their specific .cfg files to them.

➢ To point DHCP Option 160 to a tenant URL:

1. In the Device Manager Pro, open the DHCP Options Configuration page (**Setup** > **Settings** > **DHCP Options Configuration**).



DHCP Options Configuration

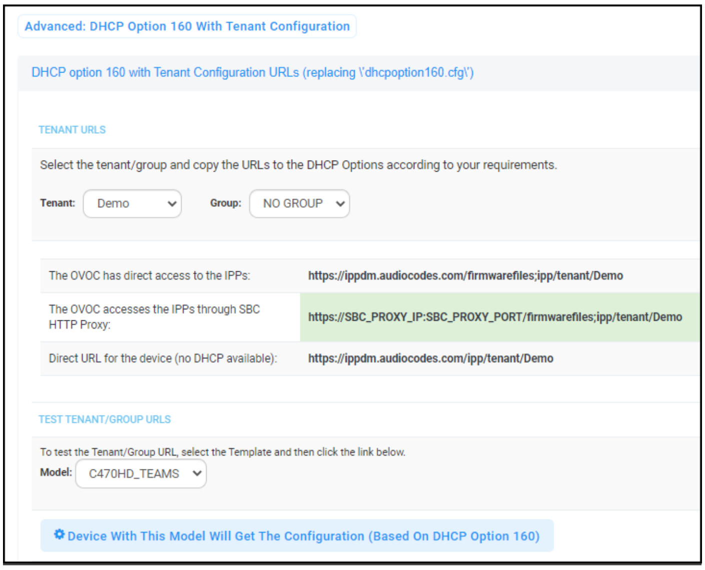
DHCP option 160 URL ('dhcpoption160.cfg')

SYSTEM URLS

OVOC accesses phones directly:	https://ippdm.audiocodes.com/firmwarefiles;ipp/dhcpoption160.cfg
OVOC accesses phones via SBC HTTP Proxy:	https://SBC_PROXY_IP:SBC_PROXY_PORT/firmwarefiles;ipp/httpproxy/

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

2. Click the **Advanced: DHCP option 160 with Tenant Configuration** link located lowermost.



Advanced: DHCP Option 160 With Tenant Configuration

DHCP option 160 with Tenant Configuration URLs (replacing \'dhcpoption160.cfg\')

TENANT URLS

Select the tenant/group and copy the URLs to the DHCP Options according to your requirements.

Tenant: Demo Group: NO GROUP

The OVOC has direct access to the IPPs:	https://ippdm.audiocodes.com/firmwarefiles;ipp/tenant/Demo
The OVOC accesses the IPPs through SBC HTTP Proxy:	https://SBC_PROXY_IP:SBC_PROXY_PORT/firmwarefiles;ipp/tenant/Demo
Direct URL for the device (no DHCP available):	https://ippdm.audiocodes.com/ipp/tenant/Demo

TEST TENANT/GROUP URLS

To test the Tenant/Group URL, select the Template and then click the link below.

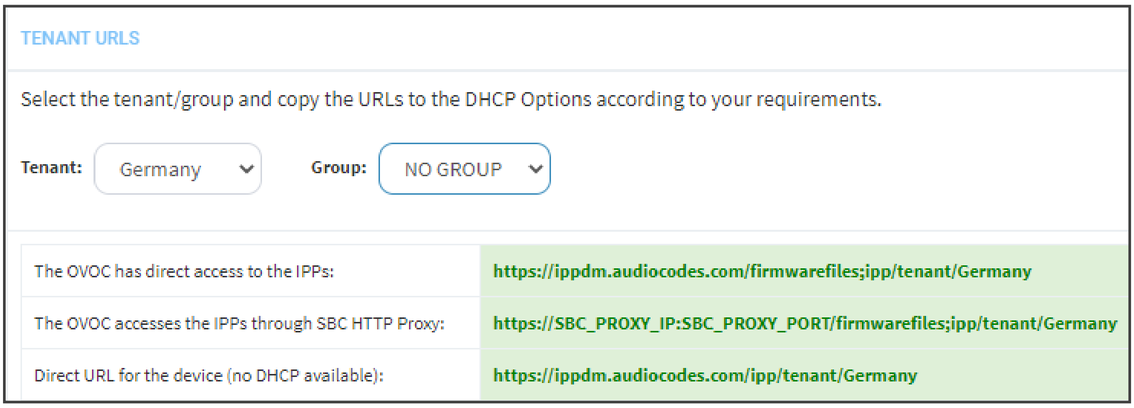
Model: C470HD_TEAMS

Device With This Model Will Get The Configuration (Based On DHCP Option 160)

3. Under the Tenant URLs section, select from the 'Tenant' dropdown a tenant with which to associate a new device, as shown in the next figure (Germany).

4. From the 'Group' dropdown list, select a group with which to associate a new device, as shown in the next figure (NO GROUP is selected).

Figure 5-7: Tenant URL



TENANT URLS

Select the tenant/group and copy the URLs to the DHCP Options according to your requirements.

Tenant: Germany Group: NO GROUP

The OVOC has direct access to the IPPs:	https://ippdm.audiocodes.com/firmwarefiles;ipp/tenant/Germany
The OVOC accesses the IPPs through SBC HTTP Proxy:	https://SBC_PROXY_IP:SBC_PROXY_PORT/firmwarefiles;ipp/tenant/Germany
Direct URL for the device (no DHCP available):	https://ippdm.audiocodes.com/ipp/tenant/Germany

You can configure the device's tenant URLs to retrieve files either directly from the OVOC server or via an SBC HTTP proxy. Using an SBC HTTP proxy server is useful for customers whose OVOC is installed in the cloud, or when phones are located behind a NAT.

5. Choose either:

    - **The OVOC has direct access to the phones**. The DHCP server will connect the phones directly to the OVOC server IP address.

        - Copy (Ctrl+C) the following URL and paste it into DHCP Option 160 in the enterprise's DHCP server: **HTTP://<OVOC_IP_Address>/firmwarefiles;ipp/tenant/<tenant selected in Step 1>/group/<group selected in step 1>**

    - **The OVOC access the IPP's through the SBC HTTP proxy**. The DHCP server directs the phones firstly to an SBC HTTP proxy server, which then redirects to the OVOC server.

        - If the phones communicate with an SBC HTTP proxy rather than directly with the OVOC server, copy (Ctrl+C) the following URL into DHCP Option 160 in the enterprise's DHCP server: **http://SBC_PROXY_IP:SBC_PROXY_PORT/firmwarefiles;ipp/tenant/Tenant**

    - **Direct URL for the IPP (No DHCP Available)** – typically used for debugging purposes when no DHCP is available.

- Configure DHCP Option 160 to point to the OVOC provisioning server's URL if the phones are not behind a NAT. DHCP Option 66/67 can also be used.
- If the phones reside behind a NAT and an SBC HTTP proxy is available, configure DHCP Option 160 to point to the SBC HTTP proxy; phone-OVOC communications will then be via the SBC HTTP proxy rather than direct.

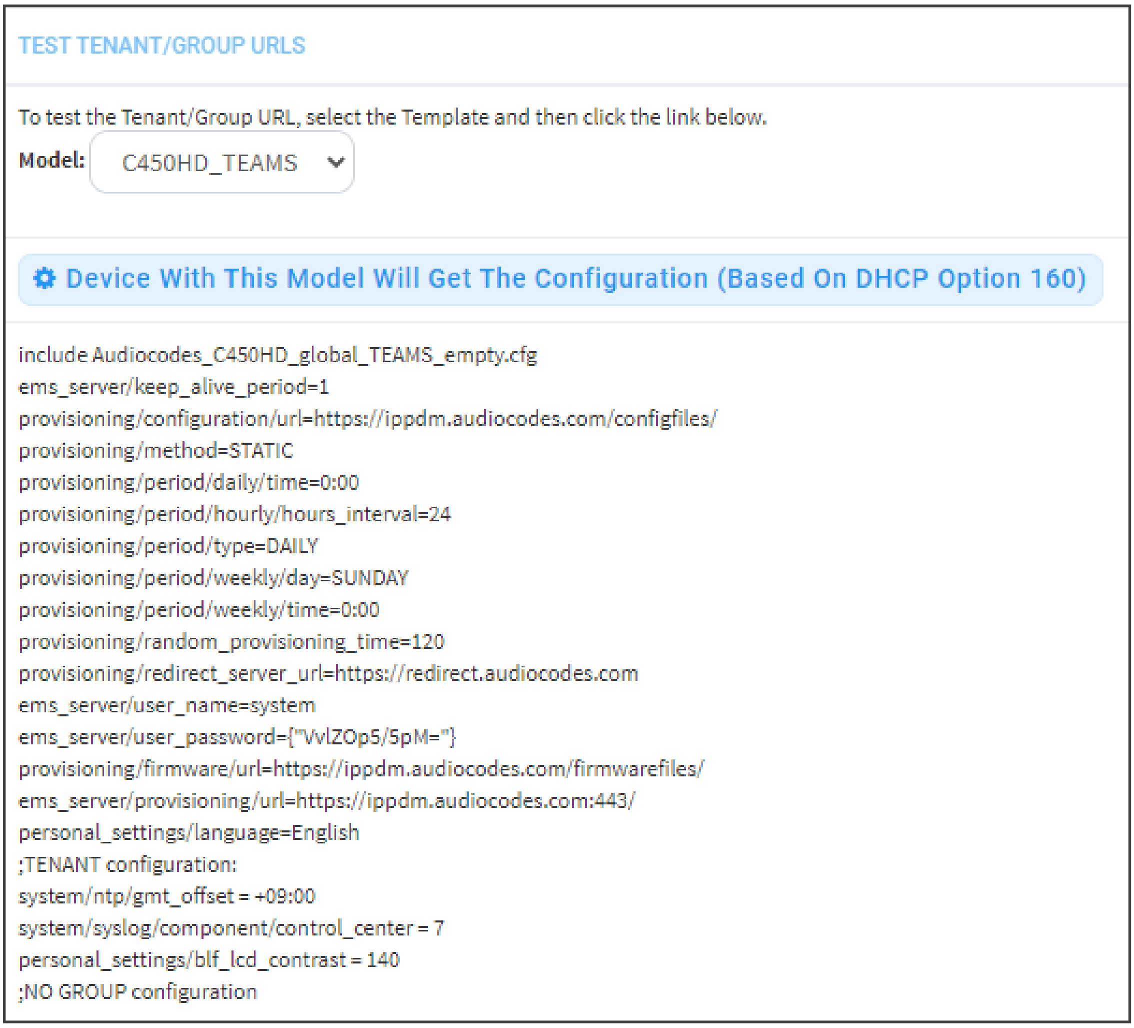
6. After copying the tenant URL (Ctrl+C) and pasting it into the enterprise's DHCP server's DHCP Option 160, select the phone model from the 'IPP Model' dropdown and then click the button **IPP with this model will get from the DHCP**; an output of the configuration file that you have configured to provision is displayed. Verify it before committing to provision multiple phones.

When a deployment covers multiple tenants, the tenants definition can be in two main hierarchies:

- DHCP server
- Subnet

For Zero Touch provisioning to function, tenant granularity must correspond with the number of DHCP servers/subnets already located within the enterprise network.

Figure 5-8: Verifying the device's Configuration File



TEST TENANT/GROUP URLS

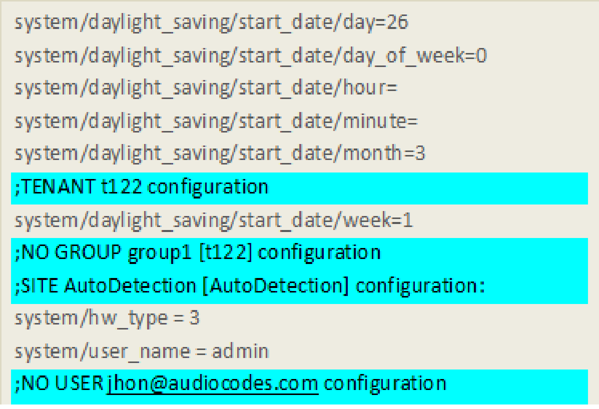
To test the Tenant/Group URL, select the Template and then click the link below.

Model: C450HD_TEAMS

Device With This Model Will Get The Configuration (Based On DHCP Option 160)

```
include Audiocodes_C450HD_global_TEAMS_empty.cfg
ems_server/keep_alive_period=1
provisioning/configuration/url=https://ippdm.audiocodes.com/configfiles/
provisioning/method=STATIC
provisioning/period/daily/time=0:00
provisioning/period/hourly/hours_interval=24
provisioning/period/type=DAILY
provisioning/period/weekly/day=SUNDAY
provisioning/period/weekly/time=0:00
provisioning/random_provisioning_time=120
provisioning/redirect_server_url=https://redirect.audiocodes.com
ems_server/user_name=system
ems_server/user_password={"VvlZOp5/5pM="}
provisioning/firmware/url=https://ippdm.audiocodes.com/firmwarefiles/
ems_server/provisioning/url=https://ippdm.audiocodes.com:443/
personal_settings/language=English
;TENANT configuration:
system/ntp/gmt_offset = +09:00
system/syslog/component/control_center = 7
personal_settings/blf_lcd_contrast = 140
;NO GROUP configuration
```

Comments in the configuration file's notation indicate a parameter's template source.



```
system/daylight_saving/start_date/day=26
system/daylight_saving/start_date/day_of_week=0
system/daylight_saving/start_date/hour=
system/daylight_saving/start_date/minute=
system/daylight_saving/start_date/month=3
;TENANT t122 configuration
system/daylight_saving/start_date/week=1
;NO GROUP group1 [t122] configuration
;SITE AutoDetection [AutoDetection] configuration:
system/hw_type = 3
system/user_name = admin
;NO USER jhon@audiocodes.com configuration
```

Template source can be:

- Device Specific
- Tenant Level
- Group Level
- Site Level

- User Level

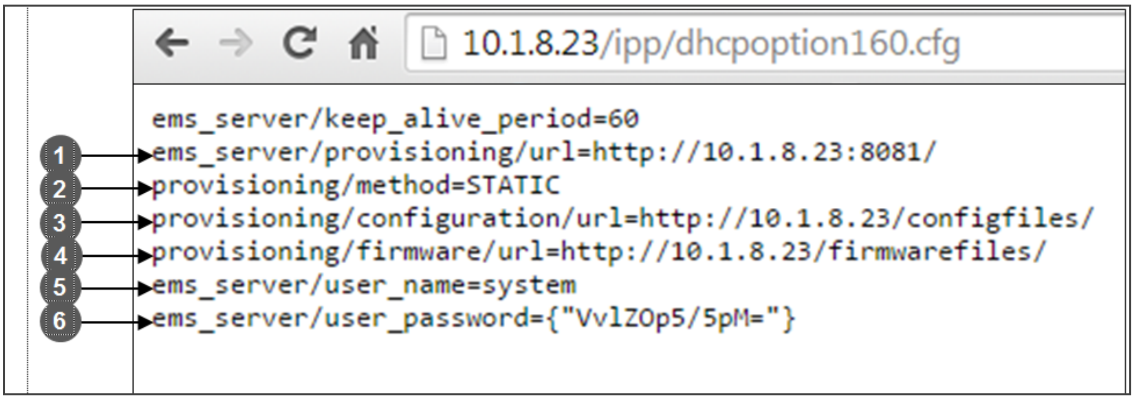
> Zero Touch is supported for phones with sign-in capabilities only.

Configuring DHCP Option 160 with System URL

> - This configuration is applicable when Zero Touch is not used to provision the phones.
> - The instructions below therefore describe a provisioning method that is not the choice method.

The figure below shows the file **dhcpoption160.cfg** located on the server.

Figure 5-9: cfg File Located on the Server



10.1.8.23/ipp/dhcpoption160.cfg

```
ems_server/keep_alive_period=60
ems_server/provisioning/url=http://10.1.8.23:8081/
provisioning/method=STATIC
provisioning/configuration/url=http://10.1.8.23/configfiles/
provisioning/firmware/url=http://10.1.8.23/firmwarefiles/
ems_server/user_name=system
ems_server/user_password={"VvlZOp5/5pM="}
```

Legend	Description
1	Points to the URL of the OVOC provisioning server.
2	STATIC provisioning method, so the cfg and img files are automatically pulled from the OVOC provisioning server rather than from the DHCP server.
3	Location of the cfg file, pulled by the phones when they're plugged into the network, on the OVOC provisioning server.
4	Location of the img file, pulled by the phones when they're plugged into the network, on the OVOC provisioning server.
5	Name of the 'system user', necessary for basic REST API authentication when the phones are plugged in to the network for the first time.
6	(Encrypted) Password of the 'system user', necessary for basic REST API authentication when the phones are plugged in to the network for the first time.

- The **dhcpoption160.cfg** file is created when logging in for the first time to the Device Manager Pro.
- The file is an internal OVOC file and cannot be manually modified.

After installation, the first, second and third lines in the file are automatically updated.

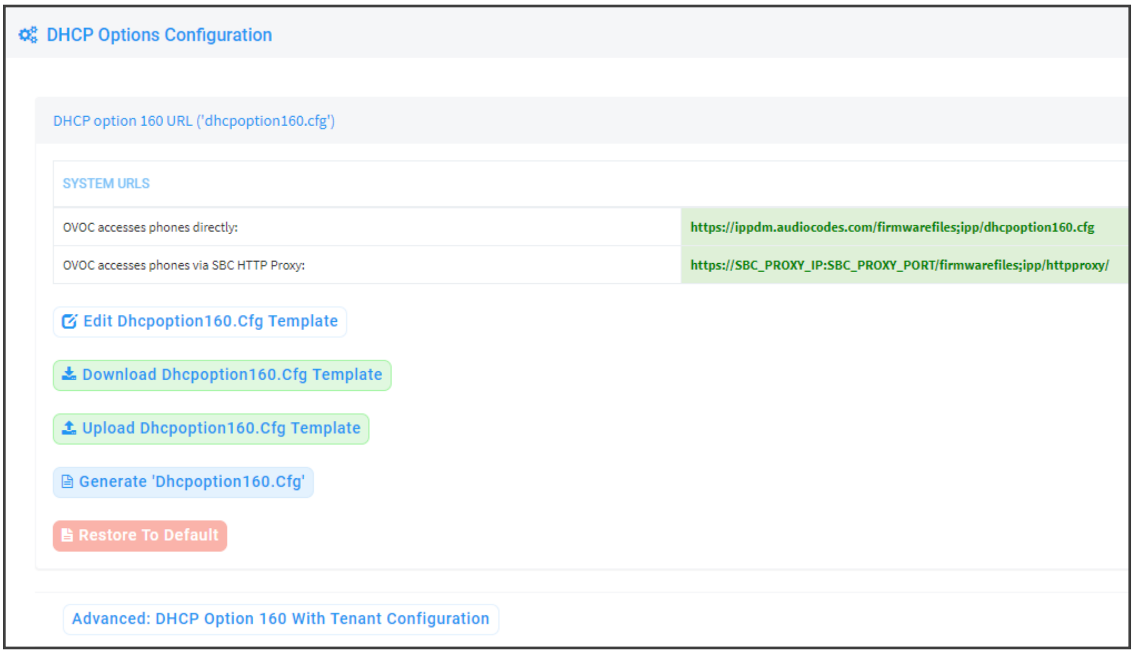
Editing the DHCP Option 160 cfg File

Administrators can opt to edit the initial DHCP Options 160 cfg file. Choose the **DHCP Option Configuration** button if your phones are communicating with a DHCP server. A DHCP server is mandatory if the phones are behind a NAT, or when communicating with an SBC HTTP proxy.

➢ To edit the DHCP Option 160 cfg File:

1. Open the System Settings page (**Setup** > **Settings** > **DHCP Options Configuration**).

Figure 5-10: DHCP Option Configuration



DHCP Options Configuration

DHCP option 160 URL ('dhcpoption160.cfg')

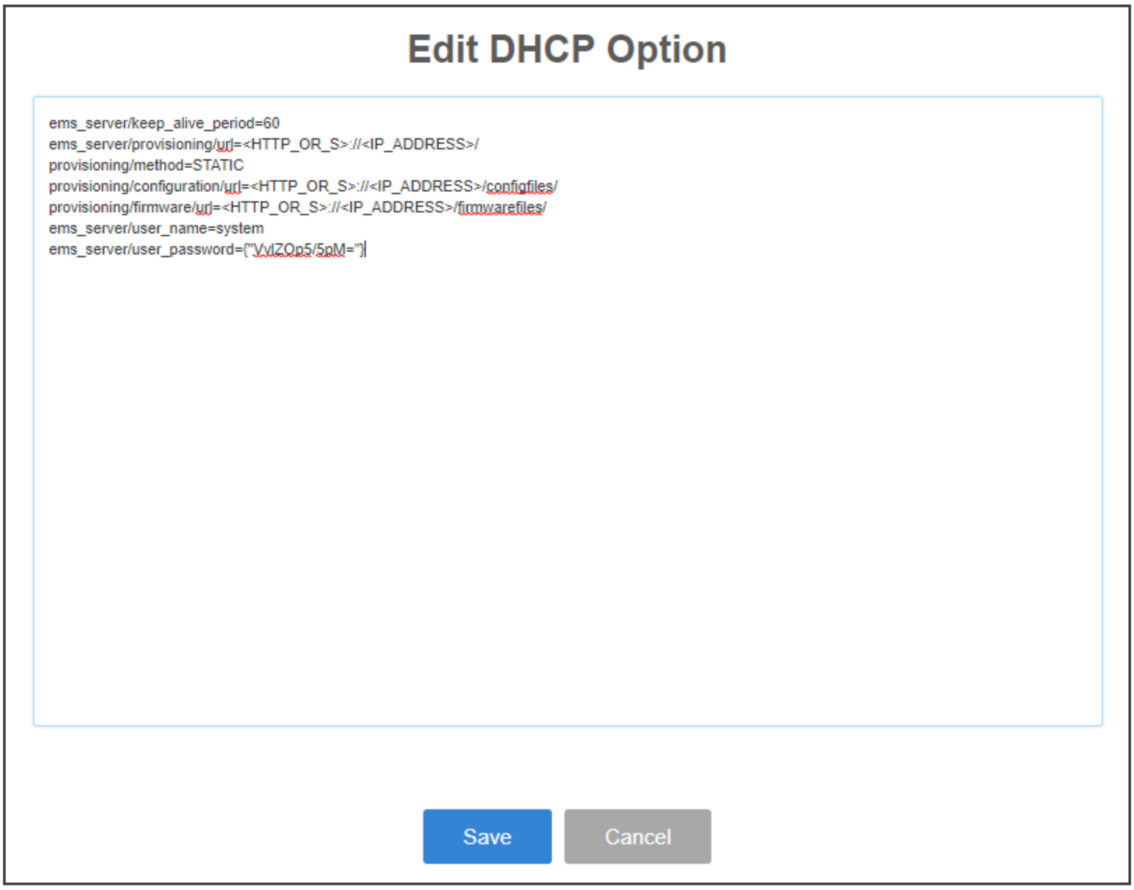
SYSTEM URLS

OVOC accesses phones directly:	https://ippdm.audiocodes.com/firmwarefiles;ipp/dhcpoption160.cfg
OVOC accesses phones via SBC HTTP Proxy:	https://SBC_PROXY_IP:SBC_PROXY_PORT/firmwarefiles;ipp/httpproxy/

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

2. Click the **Edit cfg Template** button.

Figure 5-11: Edit DHCP Option



```
ems_server/keep_alive_period=60
ems_server/provisioning/url=<HTTP_OR_S>://<IP_ADDRESS>/
provisioning/method=STATIC
provisioning/configuration/url=<HTTP_OR_S>://<IP_ADDRESS>/configfiles/
provisioning/firmware/url=<HTTP_OR_S>://<IP_ADDRESS>/firmwarefiles/
ems_server/user_name=system
ems_server/user_password={"VvIZOp5/5pM="}
```

3. Edit the DHCP option using the table below as reference.

Table 5-1: DHCP Option

Parameter	Description
Keep alive period	You can configure how often the phones generate a keep-alive trap towards the Device Manager Pro. Default: Every 60 minutes. It's advisable to configure a period that does not exceed an hour. The management system may incorrectly determine that the phone is disconnected if a period of more than an hour is configured.
Provisioning URL	Defines the URL (including IP address and port) of the provisioning server (OVOC server).
Provisioning Method	Defines the provisioning method, i.e., STATIC or Dynamic (DHCP). Do not change this setting. The setting must remain STATIC. If not, the phone will continuously perform restarts.
Provisioning Configuration URL	Defines the URL of the location of the configuration files (including IP address and port) in the provisioning server (OVOC server).

Parameter	Description
Provisioning Firmware URL	Defines the URL of the location of the firmware files (including IP address and port) in the provisioning server (OVOC server).
User Name	Defines the user name for the REST API. Default: **System**. Later, each phone receives its own unique user name.
User Password	Encrypted. Defines the user password for the REST API. Default: **System**. Later, each phone receives its own unique user password.

⚠ You can always restore these settings to their defaults if necessary by clicking the **Restore to default** button in the DHCP Option Configuration dialog, but it's advisable to leave these settings unchanged. The button is displayed only after the DHCP Option is changed.

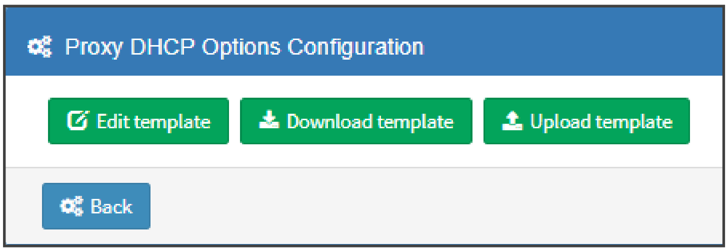
Editing the SBC HTTP Proxy

Administrators can opt to edit the initial DHCP Options 160 cfg file. Choose the **HTTP Proxy Configuration** button if your phones are communicating with an SBC HTTP proxy, which is required when the phones are behind a NAT.

➢ **To configure the SBC HTTP proxy:**

1. Open the System Settings page (**Setup** > **Settings** > **System Settings**) and then in the System Settings page click the **More** tab and then the **SBC Proxy Configuration** button.

Figure 5-12: Proxy DHCP Options Configuration



2. Click the **Edit template** button; the same Edit DHCP Option screen shown previously opens. Edit as described previously.

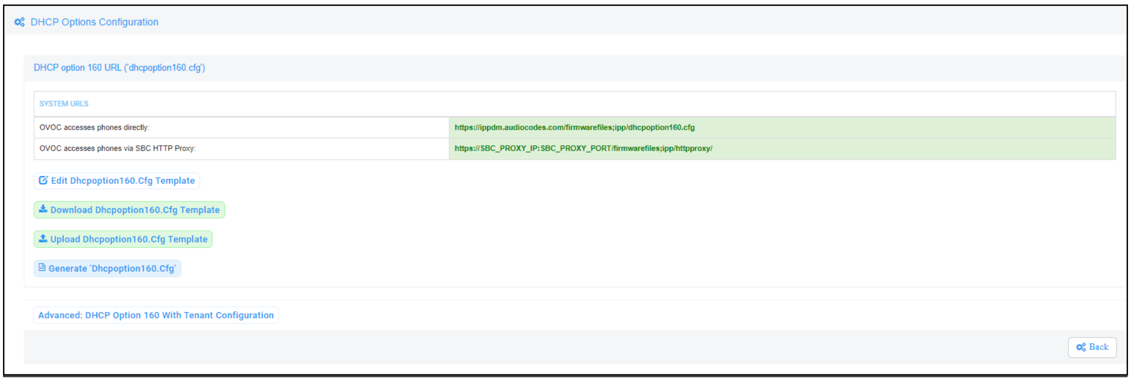
3. Click **Save**.

6 Provisioning Android-based Teams Phones

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

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

Table 6-1: DHCP Option 160 URL



DHCP Options Configuration

DHCP option 160 URL ('dhcpoption160.cfg')

SYSTEM URLS	
OVOC accesses phones directly:	https://ippdm.audiocodes.com/firmwarefiles;ipp/dhcpoption160.cfg
OVOC accesses phones via SBC HTTP Proxy:	https://SBC_PROXY_IP:SBC_PROXY_PORT/firmwarefiles;ipp/httpproxy/

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

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

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

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

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

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

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

Configuring a Periodic Provisioning Cycle

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

➢ To configure how often periodic provisioning cycles will occur:

- Use the following table as reference.

Table 6-2: Periodic Provisioning Cycle

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

Configuring TimeZone and Daylight Savings

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

➢ To configure TimeZone and Daylight Savings:

- Use the following table as reference.

Table 6-3: TimeZone And Daylight Savings

Parameter	Description
date_time/-timezone	Defines the Timezone. Valid values are: - +00:00 - +01:00 - +02:00 - Etc.
date_time/time_dst	[Boolean parameter]. Configuring **ENABLED** adds one hour to the configured time. Valid values are: - 1 - 0

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

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

date_time/time_dst=**1**

-OR-

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

date_time/time_dst=**0**

Managing Devices with HTTPS

Android-based Teams devices support an HTTPS connection.

➢ To establish an HTTPS connection:

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

  -OR-

- A root/intermediate CA certificate must be loaded to the device’s trust store either via 802.1x or configuration parameter ‘/security/ca_certificate/[0-4]/uri’

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

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

Supported Parameters

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

- general/silent_mode = 0 (default)/1
- general/power_saving = 0 (default)/1
- phone_lock/enabled = 0 (default)/1
- phone_lock/timeout = 900 (default) (in units of seconds)
- phone_lock/lock_pin = 123456
- display/language = English (default)
- display/screensaver_enabled = 0/1
- display/screensaver_timeout = 1800 (seconds)
- display/backlight = 80 (0-100)
- display/high_contrast = 0 (default) /1
- date_time/timezone = +02:00
- date_time/time_dst = 0 (default) /1
- date_time/time_format = 12 (default) / 24
- network/dhcp_enabled = 0/1
- network/ip_address =
- network/subnet_mask =
- network/default_gateway =
- network/primary_dns =
- network/pecondary_dns =
- network/pc_port = 0/1
- office_hours/start = 08:00
- office_hours/end = 17:00
- logging/enabled = 0/1
- logging/levels = VERBOSE, DEBUG, INFO, WARN, ERROR, ASSERT, SILENT
- admin/default_password = 1234
- admin/ssh_enabled=0/1 (default)
- security/SSLCertificateErrorsMode = IGNORE, NOTIFICATION, DISALLOW (default)
- security/ca_certificate/[0-4]/uri – uri to download costumer’s root-ca
- provisioning/period/daily/time
- provisioning/period/hourly/hours_interval
- provisioning/period/type = HOURLY, DAILY (default), WEEKLY, POWERUP, EVERY5MIN, EVERY15MIN

- provisioning/period/weekly/day
- provisioning/period/weekly/time
- provisioning/random_provisioning_time

7 Managing Devices Behind a NAT using SBC HTTP Proxy

Devices that reside behind a NAT and whose IP addresses are internal, can be managed by the OVOC via SBC HTTP proxy.

> ⚠ The SBC HTTP Proxy also supports HTTPS.

If the phones are located behind a NAT and the SBC HTTP proxy isn't used, then only partial management of the phones is possible:

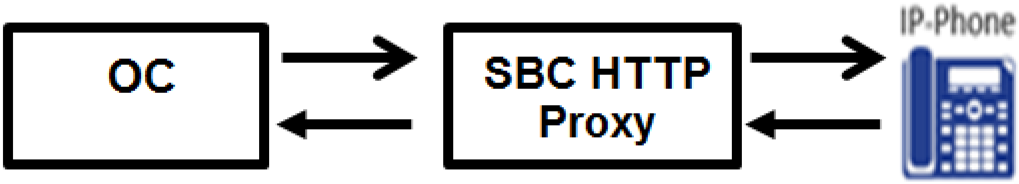
- Alarms and statuses can be sent from the phones to the Device Manager Pro, i.e., REST requests originate from the phone and the OVOC functions as a REST server.
- The Device Manager Pro can perform auto-discovery of the endpoints for the purpose of uploading configuration and firmware files.
- 'Actions' menu items cannot be applied, for example, **Reset Phone**, i.e., the OVOC functions as a REST client.

> ⚠ HTTP/S updates can be sent from the phones to the OVOC server across a NAT but requests cannot be sent from the OVOC server to the phones without the mediation of the SBC HTTP Proxy server.

If the phones are not behind a NAT, phone-OVOC server communications are direct, without the requirement of the SBC HTTP proxy.

The OVOC automatically updates phones' .cfg configuration file. The phone periodically checks whether there is a new file on the OVOC server (directly, or via the SBC HTTP proxy if the phones are behind a NAT). The frequency of the check is configurable: Every night, Every hour, etc. The default setting is **Every day at 00**:**00**. The administrator can change a value in the .cfg file using the management interface and view the result after the phone loads the new file.

The OVOC automatically updates phones' .img firmware file. The phone periodically checks whether there is a new .img file on the OVOC server (directly, or via SBC HTTP proxy if the phones are behind a NAT).



- When the OVOC communicates with the the SBC HTTP proxy, for example, when it communicates Actions (Check Status, Change Tenant, Update Firmware, Open Web Admin, Reset Phone, Update Configuration, Send Message, Delete Status and Telnet), communications are always over HTTPS. Similarly, when the SBC HTTP proxy communicates with the OVOC, communications can be over HTTPS (recommended).

- The string used to configure DHCP Option 160 for communication with the OVOC is different to the string used to configure DHCP Option 160 for communication with the SBC HTTP Proxy.
- A port firewall configuration must be defined for communication with the SBC HTTP Proxy.
  - The listening port (and IP) for HTTP/S must not collide with any other port such as SIP 5060/1 HTTP for AudioCodes' Web server 80/443.
  - If AudioCodes' Web server uses an interface other than SBC HTTP Proxy , the well-known ports 80 and 443 can be used.
- When a device uses the SBC HTTP Proxy, the Device Manager Pro indicates this with the following icon:
  172.17.113.98

The administrator can also view phones' online statuses (Started, Registered, Unregistered, etc.). The SBC HTTP Proxy also supports actions such as Send Message, Restart, Open Web Admin and Check Status.

> To support this feature, the SBC HTTP Proxy should be correctly configured. For more information, see the relevant device's *User's Manual* (Section 'HTTP-based Proxy Services').

8 Monitoring and Maintaining the Phone Network

You can monitor and maintain the enterprise's telephony network.

Monitoring the Network from the Dashboard

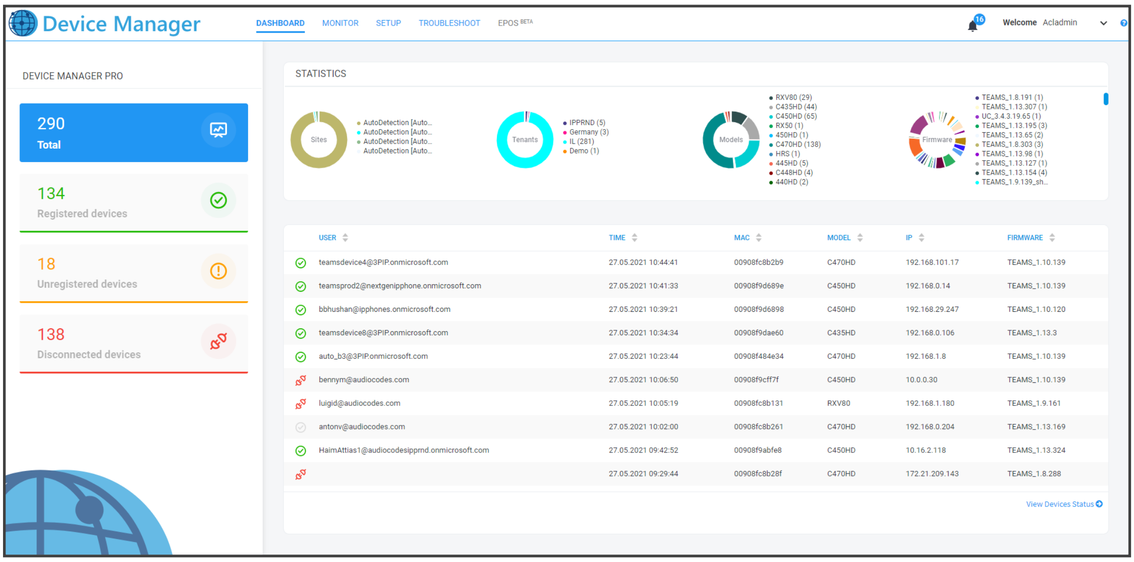
The Dashboard page lets you quickly identify

- which phones in the network are registered
- which phones in the network are non-registered
- # of registered and non-registered phones (in terms of SIP registration)
- % of registered phones
- MAC and IP address of each phone
- the time the information was reported
- the firmware version

➢ To open the Dashboard page:

- The page opens by default (under the **Dashboard** menu) after starting the Device Manager application.

Figure 8-1: Dashboard

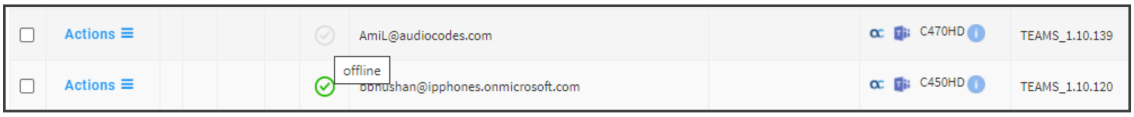


	USER	TIME	MAC	MODEL	IP	FIRMWARE
✓	teamsdevice4@3PIP.onmicrosoft.com	27.05.2021 10:44:41	00908fc8b2b9	C470HD	192.168.101.17	TEAMS_1.10.139
✓	teamsprod2@nextgenipphone.onmicrosoft.com	27.05.2021 10:41:33	00908f9d689e	C450HD	192.168.0.14	TEAMS_1.10.139
✓	bbhushan@ipphones.onmicrosoft.com	27.05.2021 10:39:21	00908f9d6898	C450HD	192.168.29.247	TEAMS_1.10.120
✓	teamsdevice8@3PIP.onmicrosoft.com	27.05.2021 10:34:34	00908f9dae60	C435HD	192.168.0.106	TEAMS_1.13.3
✓	auto_b3@3PIP.onmicrosoft.com	27.05.2021 10:23:44	00908f484e34	C470HD	192.168.1.8	TEAMS_1.10.139
🔌	bennym@audiocodes.com	27.05.2021 10:06:50	00908f9cff7f	C450HD	10.0.0.30	TEAMS_1.10.139
🔌	luigid@audiocodes.com	27.05.2021 10:05:19	00908fc8b131	RXV80	192.168.1.180	TEAMS_1.9.161
✓	antonv@audiocodes.com	27.05.2021 10:02:00	00908fc8b261	C470HD	192.168.0.204	TEAMS_1.13.169
✓	HaimAttias1@audiocodesipprnd.onmicrosoft.com	27.05.2021 09:42:52	00908f9abfe8	C450HD	10.16.2.118	TEAMS_1.13.324
🔌		27.05.2021 09:29:44	00908fc8b28f	C470HD	172.21.209.143	TEAMS_1.8.288

View Devices Status

- If a Skype for Business IP phone is signed out (offline, or not registered), you'll see an icon of a gray tick inside a gray circle, and the 'User' column will be blank, as shown in the figure below. It will be counted as a Non Registered Device.

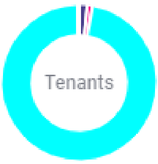
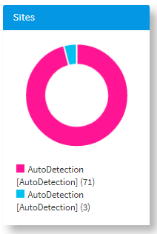
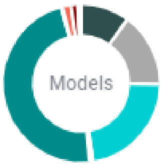
Figure 8-2: Dashboard - Skype for Business IP Phone Offline



□	Actions ≡	✓	AmiL@audiocodes.com	C470HD	TEAMS_1.10.139
□	Actions ≡	✓ offline	bbhushan@ipphones.onmicrosoft.com	C450HD	TEAMS_1.10.120

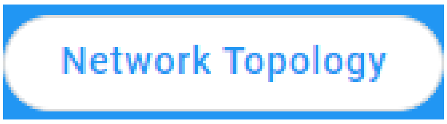
- Point your mouse over the icon to view the 'offline' tooltip.
- If the phone is not registered, you'll view a red triangle enclosing an exclamation mark.
- View the status thumbnails. Use this table as reference.

Table 8-1: Dashboard – Status Thumbnails

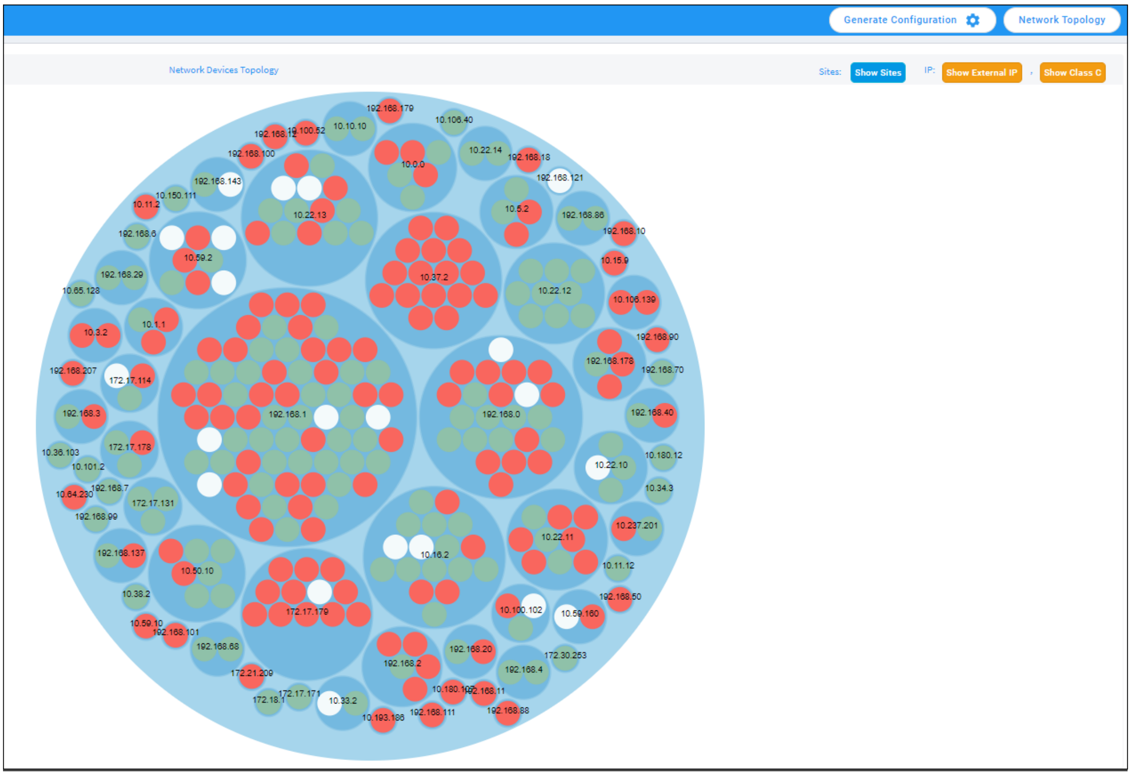
Status Thumbnail	Description
✓	Indicates the number of registered devices. Click **MORE DETAILS…** to quickly access the Devices Status page.
!	Indicates the number of unregistered devices. Click **MORE DETAILS…** to quickly access the Devices Status page.
🔌	Indicates the number of disconnected devices. Click **MORE DETAILS…** to quickly access the Devices Status page.
📈	Indicates the number of devices running the version stated above it. Click **MORE DETAILS…** to quickly access the Devices Status page.
	Pie chart showing the number of *devices per tenant* that are registered. Hover over a segment of the pie to view the tenant's name and the number of devices registered under it. Click a segment of the pie to open the Devices Status page displaying that tenant and the devices registered under it.
 Sites AutoDetection [AutoDetection] (71) AutoDetection [AutoDetection] (3)	Pie chart showing the number of *devices per site* that are registered. Click a segment of the pie to open the Devices Status page.
	Pie chart showing how many *phones of each model* are registered. Click a segment of the pie to open the Devices Status page.
	Pie chart showing how many *phones of each firmware version* are registered. Click a segment of the pie to open the Devices Status page.

Viewing Network Topology

Located in the uppermost right corner of the Dashboard page, the **Network Topology** button allows network administrators to view devices in their IP telephony networks according to sites, internal or external IP address, or IP address class.

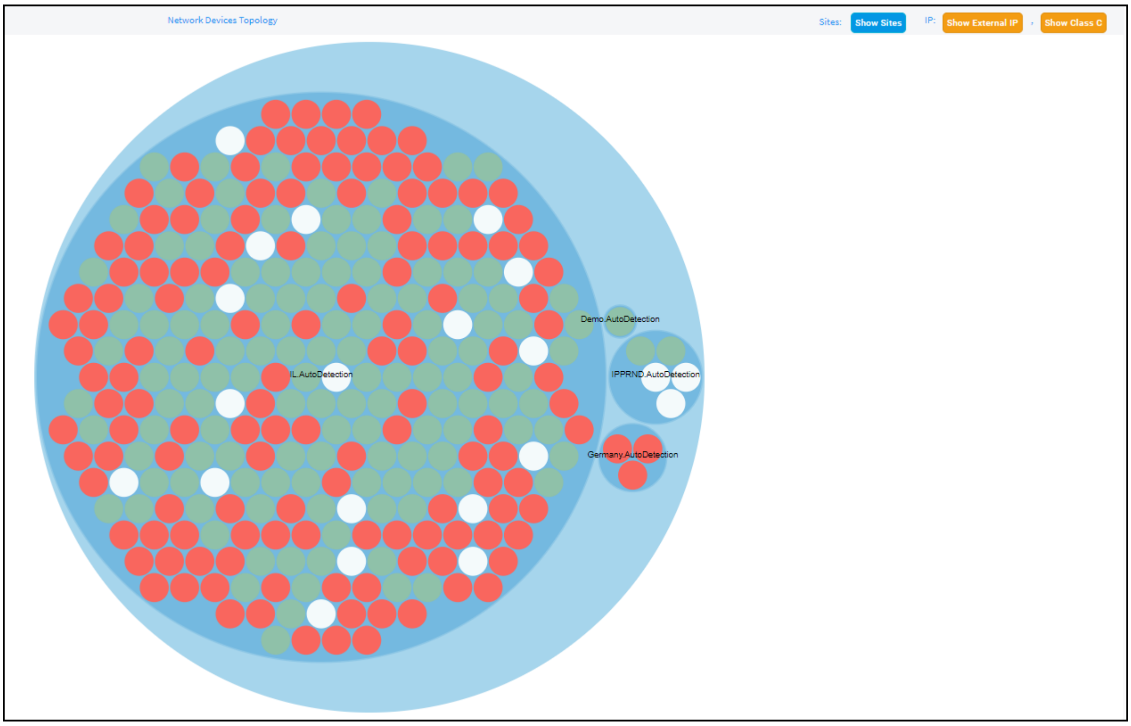


The Network Devices Topology page opens:



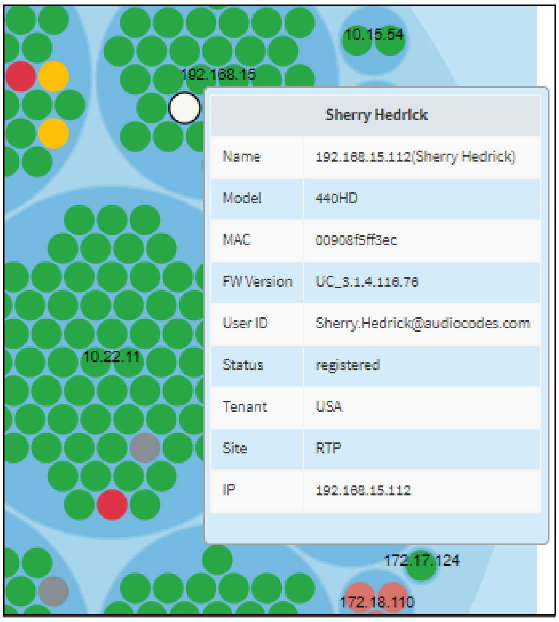
Click the **Show Sites** button to display the Network Devices Topology page *according to sites*.

Figure 8-3: Network Devices Topology page per sites



The preceding figure shows multiple sites in a single-tenant network. The page allows administrators to determine at a glance which sites are causing traffic overload (for example). Administrators can point their mouse at a device to view information on that device displayed in a tool tip.

Figure 8-4: Point your mouse at a device to view information on it



Sherry Hedrick

Name	192.168.15.112(Sherry Hedrick)
Model	440HD
MAC	00908f5ff3ec
FW Version	UC_3.1.4.116.76
User ID	Sherry.Hedrick@audiocodes.com
Status	registered
Tenant	USA
Site	RTP
IP	192.168.15.112

Click the **Show Internal IP** | **Show LAN IP** button to display devices in the page according to *internal IP address* or *LAN IP address*. Each device in the network has an *internal* IP address - the IP address of the device located *within the enterprise network*. Some devices also use a LAN

IP address - the IP address of a router via which calls transit (for example). The button displays devices according to the administrator's choice.

Click the **Show Class B** or **Show Class C** button. Every IP address in quad-dotted notation comprises four 'classes'. This button allows displaying devices according to IP addresses of Class B or Class C.

- **Show Class B** shows the first *two* classes, for example, 10.10
- **Show Class C** shows the first *three* classes, for example, 10.10.10.

A higher number of devices will be displayed if **Show Class B** is selected than if **Show Class C** is selected since more devices' IP addresses begin with 10.10 than with 10.10.10.

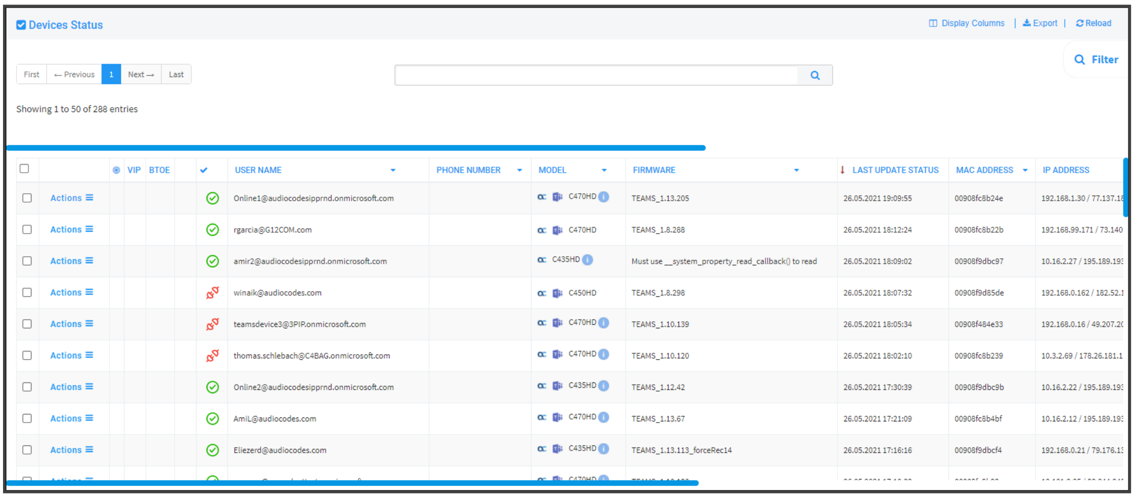
Checking Devices Status

The Devices Status page lets you check a device's status, for example, whether it's connected or not, as well as perform actions on an individual device or on multiple selected devices.

➢ To check a device's status:

1. Open the Devices Status page (**Monitor** > **Dashboard** > **Devices Status**)

Figure 8-5: Devices Status



☑ Devices Status

Display Columns | Export | Reload

First ← Previous 1 Next → Last

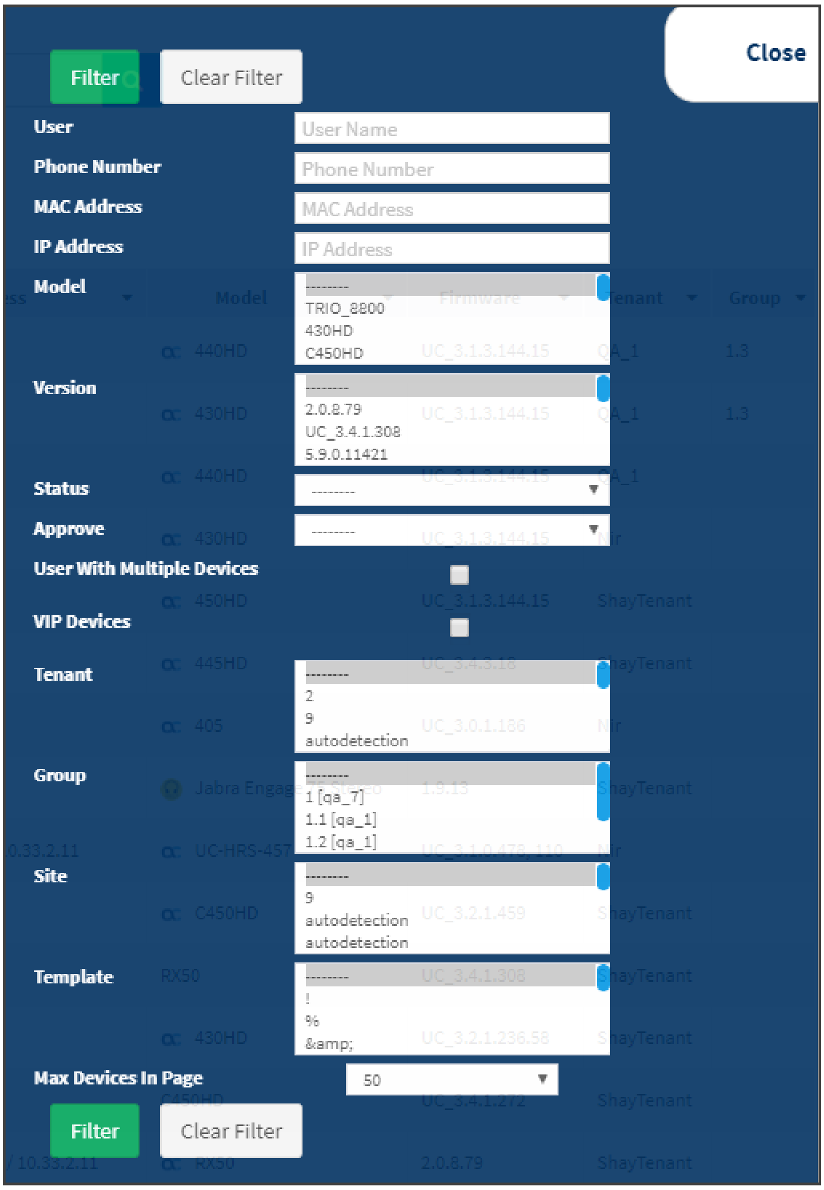
Filter

Showing 1 to 50 of 288 entries

□		◉	VIP	BTOE		✓	USER NAME	PHONE NUMBER	MODEL	FIRMWARE	LAST UPDATE STATUS	MAC ADDRESS	IP ADDRESS
□	Actions ≡					✓	Online1@audiocodesipprnd.onmicrosoft.com		C470HD	TEAMS_1.13.205	26.05.2021 19:09:55	00908fc8b24e	192.168.1.30 / 77.137.18
□	Actions ≡					✓	rgarcia@G12COM.com		C470HD	TEAMS_1.8.288	26.05.2021 18:12:24	00908fc8b22b	192.168.99.171 / 73.140
□	Actions ≡					✓	amir2@audiocodesipprnd.onmicrosoft.com		C435HD	Must use __system_property_read_callback() to read	26.05.2021 18:09:02	00908f9dbc97	10.16.2.27 / 195.189.19
□	Actions ≡					✗	winaik@audiocodes.com		C450HD	TEAMS_1.8.298	26.05.2021 18:07:32	00908f9d85de	192.168.0.162 / 182.52.1
□	Actions ≡					✗	teamsdevice3@3PIP.onmicrosoft.com		C470HD	TEAMS_1.10.139	26.05.2021 18:05:34	00908f484e33	192.168.0.16 / 49.207.2
□	Actions ≡					✗	thomas.schlebach@C4BAG.onmicrosoft.com		C470HD	TEAMS_1.10.120	26.05.2021 18:02:10	00908fc8b239	10.3.2.69 / 178.26.181.1
□	Actions ≡					✓	Online2@audiocodesipprnd.onmicrosoft.com		C435HD	TEAMS_1.12.42	26.05.2021 17:30:39	00908f9dbc9b	10.16.2.22 / 195.189.19
□	Actions ≡					✓	AmiL@audiocodes.com		C470HD	TEAMS_1.13.67	26.05.2021 17:21:09	00908fc8b4bf	10.16.2.12 / 195.189.19
□	Actions ≡					✓	Eliezerd@audiocodes.com		C435HD	TEAMS_1.13.113_forceRec14	26.05.2021 17:16:16	00908f9dbcf4	192.168.0.21 / 79.176.1

2. Click **Filter**; the filter lets you view specific information in the page, preventing information irrelevant to you from cluttering the page.

Figure 8-6: Devices Status Filter



3. You can filter per user, phone #, MAC, IP address, model, version, status (registered, offline or disconnected), approved or approval pending, users with multiple devices, VIP Devices, tenant, site, group, template or maximum devices shown in the page.

4. View in column 'USB Headset Type' if a headset is connected to a phone's USB port; in addition, column 'IPP Model' displays the USB icon.

5. View in column 'HRS Speaker Model' the Huddle Room Solution model (457 or 458) if an HRS is connected; in addition, you can view in column 'HRS Speaker FW' the speaker firmware version.

6. Non-Skype for Business phones are displayed differently to Skype for Business phones.

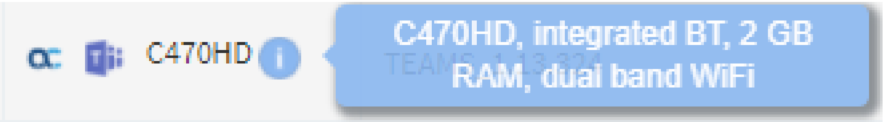
   - The format of 'User Agent' for non-Skype for Business phones is for example **AUDC-IPPhone/2.0.4.30 (430HD; 00908F4867AF)** while the format for Skype for Business phones is **AUDC-IPPhone-430HD_UC_2.0.7.70/1.0.0000.0**

- Only Skype for Business phones are displayed under the 'Location' column; non-Skype for Business phones are not displayed under the 'Location' column.

7. View in the column 'Model' the entries **Spectralink 8440, Poly Trio 8800**, **Poly VVX**, **Poly CCX 500/600**, etc. if these phone models are connected; they can be monitored, configured and templates can be mapped.

   You can also view in the 'Model' column an **i** icon:

   Point your mouse over it to display the device's vital hardware specifications:

   C470HD, integrated BT, 2 GB RAM, dual band WiFi

8. You can click the **Export** link to export all entries in the page - or a selected list of entries - to a csv file. This facilitates inventory management; it lets you easily obtain a list of phone MAC addresses or serial numbers, for example. After generating a csv file, a download option is displayed in the lower-left corner. You can save the csv file or open it directly in Excel which displays the same information as that on the page.

9. You can click an individual user's **Actions** link.

Figure 8-7: Actions Menu - Single User

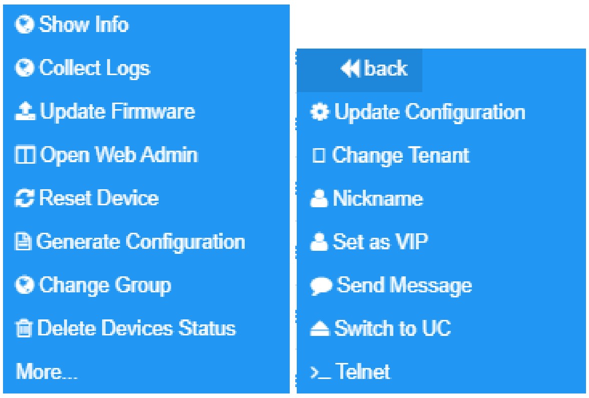
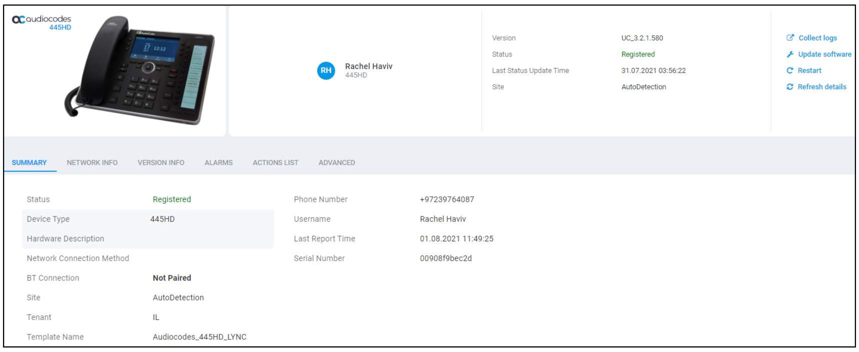
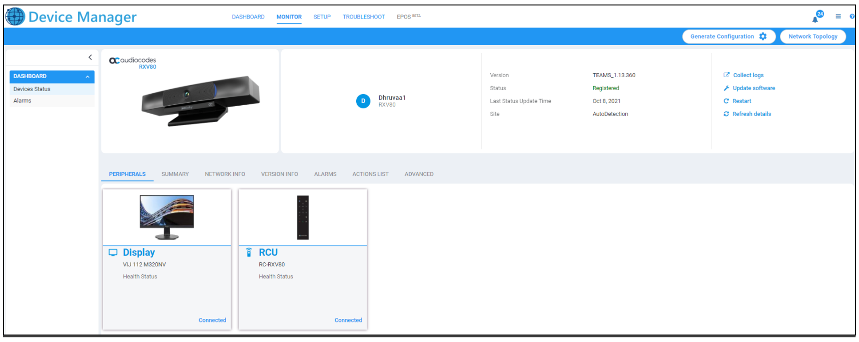
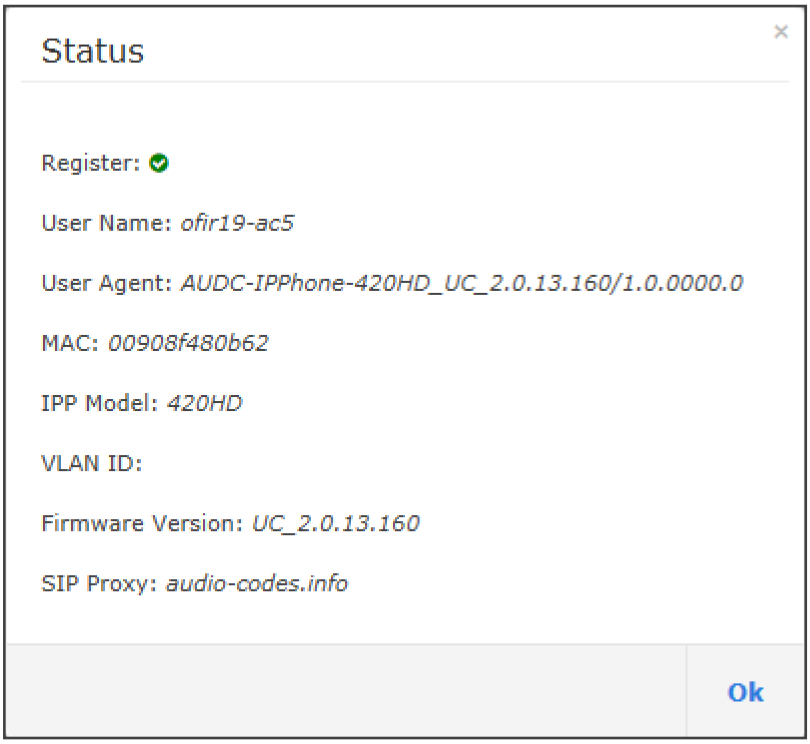
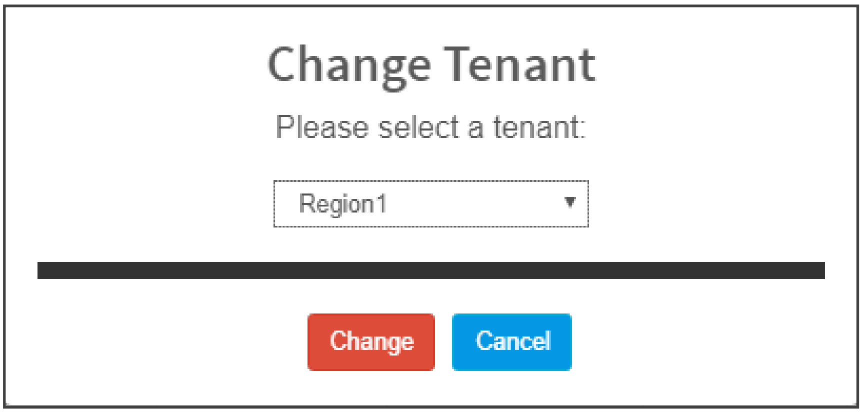
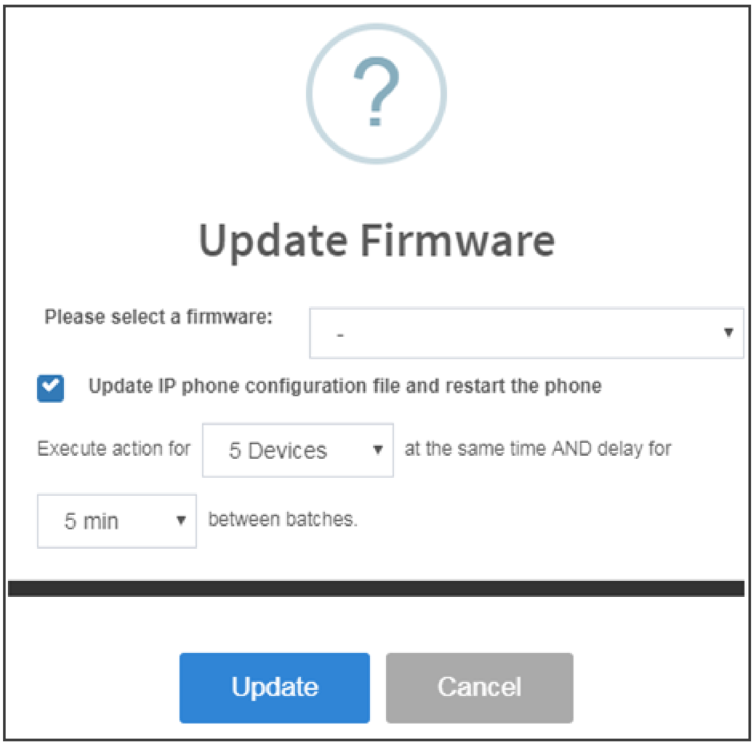
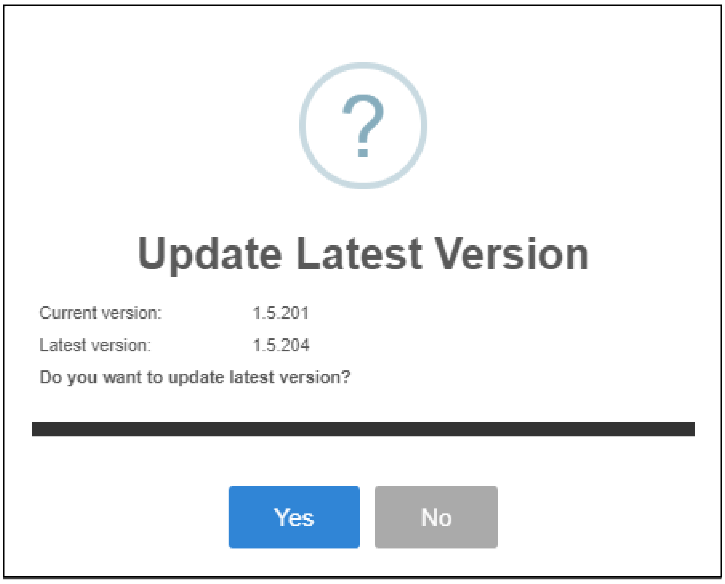


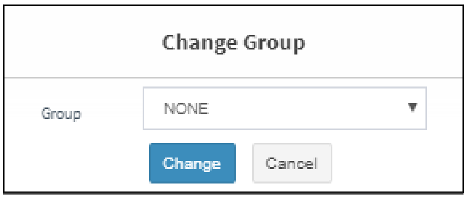
Table 8-2: Actions Menu

Action	Description
Show Info	Displays all the information about the device needed by the network administrator.  audiocodes 445HD Rachel Haviv 445HD Version UC_3.2.1.580 Status Registered Last Status Update Time 31.07.2021 03:56:22 Site AutoDetection Collect logs Update software Restart Refresh details SUMMARY NETWORK INFO VERSION INFO ALARMS ACTIONS LIST ADVANCED Status Registered Device Type 445HD Hardware Description Network Connection Method BT Connection Not Paired Site AutoDetection Tenant IL Template Name Audiocodes_445HD_LYNC Phone Number +97239764087 Username Rachel Haviv Last Report Time 01.08.2021 11:49:25 Serial Number 00908f9bec2d

Action	Description
	Information under tabs **Summary**, **Network Info**, **Version Info**, **Alarms**, **Actions List** and **Advanced** is available. All information that the peripheral device sends to the OVOC as raw data composes this GUI screen. The Show Info screen differs slightly from device to device. The RXV80, for example, displays the tab **Peripherals**, as shown in the next figure.  Device Manager DASHBOARD MONITOR SETUP TROUBLESHOOT EPOS BETA 24 Generate Configuration Network Topology DASHBOARD Devices Status Alarms audiocodes RXV80 D Collect logs Update software Restart Refresh details PERIPHERALS SUMMARY NETWORK INFO VERSION INFO ALARMS ACTIONS LIST ADVANCED Dhruvaa1 RXV80 Version TEAMS_1.13.360 Status Registered Last Status Update Time Oct 8, 2021 Site AutoDetection Display VIJ 112 M320NV Health Status Connected RCU RC-RXV80 Health Status Connected
Collect Logs	Allows network administrators to get logs without needing to go to the phone. See Getting Logs on page 116 for detailed information.
Check Status	[Only applies to UC phones] Select the 'Check Status' option.  Status Register: ✓ User Name: *ofir19-ac5* User Agent: *AUDC-IPPhone-420HD_UC_2.0.13.160/1.0.0000.0* MAC: *00908f480b62* IPP Model: *420HD* VLAN ID: Firmware Version: *UC_2.0.13.160* SIP Proxy: *audio-codes.info*
Change Tenant	Select the 'Change Tenant' option.

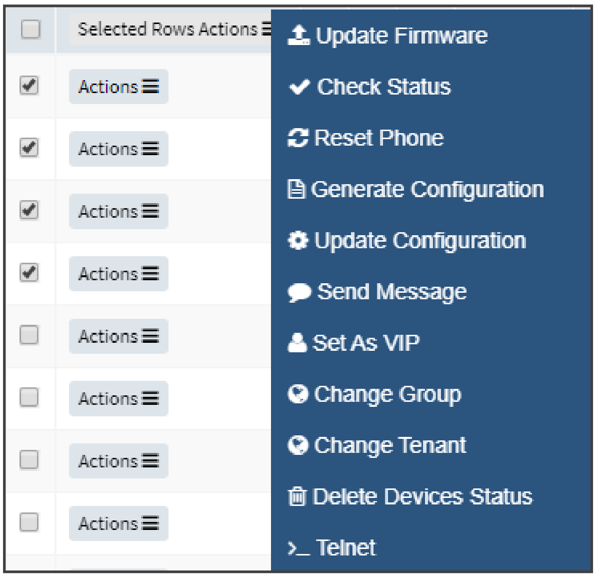
Action	Description
	 Change Tenant Please select a tenant: Region1 From the dropdown, select the tenant, and then click **Change**.
Update Firmware	You can update firmware per device, or for multiple selected devices. Choose the 'Update Firmware' menu option.  Update Firmware Please select a firmware: - ☑ Update IP phone configuration file and restart the phone Execute action for 5 Devices at the same time AND delay for 5 min between batches. The figure above shows the screen that opens after selecting *multiple* devices. The screen for a *single* device is *identical* but *without* the option to execute the action in batches. From the dropdown, select the firmware file, and then click **Update**; the firmware file is updated. You can simultaneously update the device's configuration file. If you select *multiple* devices and then click the **Selected Rows Actions** link in the title bar to choose 'Update Software' from the drop-down, the screen (as shown in the figure above) will include the option to

Action	Description
	■ update firmware simultaneously for a batch of devices, each batch containing 5 | 10 | 20 | 30 | 50 | 100 devices ■ configure a 0 second | 2 second | 5 second | 10 second | 30 second | 2 minute | 5 minute delay between batches Note that if the ↑ icon is displayed in the 'Firmware' column adjacent to a listed device in the Devices Status page, it indicates that that device's firmware is not the latest firmware available; you can click the icon to upload the device's latest firmware.  Update Latest Version Current version: 1.5.201 Latest version: 1.5.204 Do you want to update latest version?
Open Web Admin	Opens the Web interface (see the device's *Administrator's Manual*). By default, the Web interface opens in HTTPS.
Nickname	Allows you to provide a nickname for the enterprise employee to facilitate more effective user and phone management.
Reset Phone	Sends a reset command to the selected device/s. Note that some phone models wait for the user to finish an active call, while others may perform an immediate restart.
Generate configuration	Generates the device's configuration file according to its tenant, site and template. The user configuration will also be generated in case it will be needed.
Change Group	Allows you to add an endpoint to an endpoints group or to change end-points groups. Endpoints groups are added in the OVOC (see the *OVOC User's Manual* for more information). The feature benefits the customer who wants (for example) 10 of 500 phones in a site in the enterprise organized in a group for a software upgrade to apply exclusively to those

Action	Description
	10 phones. The groups are across sites, within a specific tenant. After clicking the **Actions** menu option, this prompt is displayed:  Change Group Group NONE Change Cancel - From the 'Group' drop-down, select the group and click **Change**. - Configure an endpoints group in the Group Configuration page as shown in Configuring an Endpoints Group on page 17.
Update configuration	Sends a command to the phone to check whether there is a new configuration file to upload and updates the phone after a configurable 'Delay Time' (Default = 2 seconds).
Send Message	Lets you send a message to the screen/s of the selected device/s. Enter the message in the 'Text' field. You can configure for how long the message will be displayed in the screen/s.
Set as VIP	Allows network administrators to configure the phone as a VIP phone; VIP phones feature a different disconnect time interval and support disconnect / unregistered alarms. A phone configured as a VIP phone is typically a Common Area Phone (CAP) located in the lobby of an enterprise, or a conference phone located in an enterprise's meeting rooms. It's important that it be continuously connected hence the different disconnect time interval and the disconnect / unregistered alarms.
Delete Devices Status	Deletes the devices from the Devices Status table.
Switch to UC	Applies to the two flavors of the C450HD phone: Microscope Teams Native and Microscope Teams Compatible. Select this option to switch the C450HD phone from the one flavor to the other.
Telnet	Allows administrators to send Telnet (CLI) debug commands to the phone for debugging purposes. Important: For this feature to function, Telnet must be enabled on the device. You can enable Telnet from the Web interface's Telnet page (**Management** > **Remote Management** > **Telnet**).

10. You can select multiple users and then click the **Selected Rows Actions** link.

Figure 8-8: Actions Menu - Selected Rows



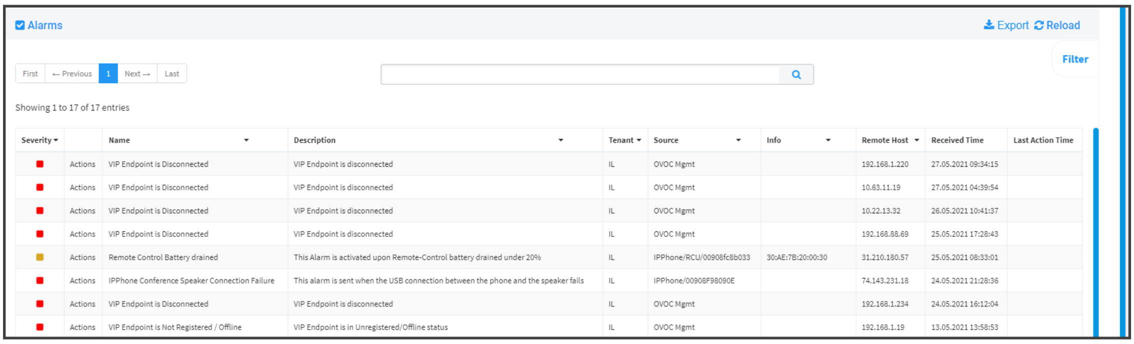
See the table above for descriptions. Any action you choose will apply to all selected rows. For example, select rows, click the **Selected Rows Actions** link, and then select the **Update Firmware** option; all selected devices will be updated with the firmware file you select.

Monitoring Alarms

Devices send alarms via the REST protocol. They're forwarded by the OVOC as mail, SNMP traps, etc. The Alarms page (**Monitor** > **Dashboard** > **Alarms**) shows you

- each device alarm in the network
- a description of each alarm
- MAC address of the device (source)
- alarm severity
- IP address of the device
- last action time
- date and time of receipt of the alarm

Figure 8-9: Alarms



Showing 1 to 17 of 17 entries

Severity		Name	Description	Tenant	Source	Info	Remote Host	Received Time	Last Action Time
🟥	Actions	VIP Endpoint is Disconnected	VIP Endpoint is disconnected	IL	OVOC Mgmt		192.168.1.220	27.05.2021 09:34:15	
🟥	Actions	VIP Endpoint is Disconnected	VIP Endpoint is disconnected	IL	OVOC Mgmt		10.63.11.19	27.05.2021 04:39:54	
🟥	Actions	VIP Endpoint is Disconnected	VIP Endpoint is disconnected	IL	OVOC Mgmt		10.22.13.32	26.05.2021 10:41:37	
🟥	Actions	VIP Endpoint is Disconnected	VIP Endpoint is disconnected	IL	OVOC Mgmt		192.168.88.69	25.05.2021 17:28:43	
🟧	Actions	Remote Control Battery drained	This Alarm is activated upon Remote-Control battery drained under 20%	IL	IPPhone/RCU/00908fc8b033	30:AE:7B:20:00:30	31.210.180.57	25.05.2021 08:33:01	
🟥	Actions	IPPhone Conference Speaker Connection Failure	This alarm is sent when the USB connection between the phone and the speaker fails	IL	IPPhone/00908F98090E		74.143.231.18	24.05.2021 21:28:36	
🟥	Actions	VIP Endpoint is Disconnected	VIP Endpoint is disconnected	IL	OVOC Mgmt		192.168.1.234	24.05.2021 16:12:04	
🟥	Actions	VIP Endpoint is Not Registered / Offline	VIP Endpoint is in Unregistered/Offline status	IL	OVOC Mgmt		192.168.1.19	13.05.2021 13:58:53	

The Device Manager Pro displays *active* alarms, not historical alarms.

Red indicates a severity level of Critical

Orange indicates a severity level of Major

After an alarm is cleared, it disappears from the Alarms screen.

See also AudioCodes' *One Voice Operations Center Monitoring Guide* for more information about each alarm.

Searching for Alarms

You can search for alarms in the Alarms page. The 'Search' field enables the functionality. You can search by

- alarm name
- a device's MAC address
- a device's IP address

Performing Actions on Alarms

You can perform actions on alarms in the Alarms page. Click the **Actions** link and from the popup menu select **Delete Alarm** or **Telnet**. The **Telnet** option lets administrators debug directly if an issue arises. See Telnet on page 48 for more information.

Maintaining Users

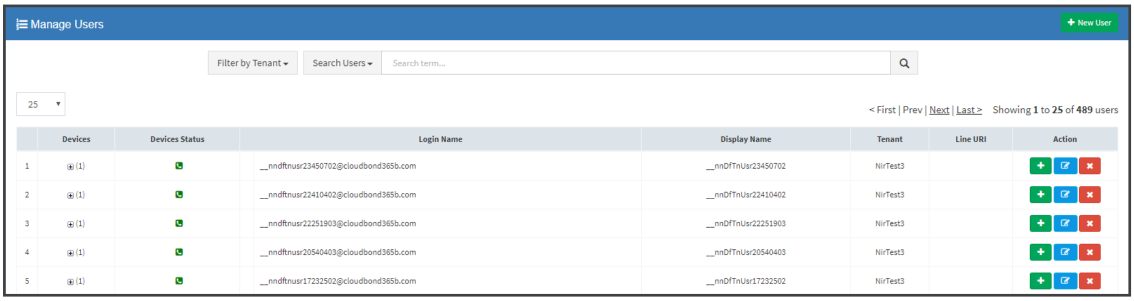
The Manage Users page lets you maintain users. You can

- search for a user/device
- add a user
- add a device to a user
- edit user/device
- view device status
- delete a user/device
- search for a device by tenant
- search for a device by name

Searching for Users/Devices

You can search for a user in the Manage Users page (**Setup** > **Users & Devices** > **Manage Users**).

Figure 8-10: Searching for a User/Device



Showing **1** to **25** of **489** users

	Devices	Devices Status	Login Name	Display Name	Tenant	Line URI	Action
1	⊞ (1)	☎	__nndftnusr23450702@cloudbond365b.com	__nnDfTnUsr23450702	NirTest3		+ ✎ ✖
2	⊞ (1)	☎	__nndftnusr22410402@cloudbond365b.com	__nnDfTnUsr22410402	NirTest3		+ ✎ ✖
3	⊞ (1)	☎	__nndftnusr22251903@cloudbond365b.com	__nnDfTnUsr22251903	NirTest3		+ ✎ ✖
4	⊞ (1)	☎	__nndftnusr20540403@cloudbond365b.com	__nnDfTnUsr20540403	NirTest3		+ ✎ ✖
5	⊞ (1)	☎	__nndftnusr17232502@cloudbond365b.com	__nnDfTnUsr17232502	NirTest3		+ ✎ ✖

When searching for a user or a device:

- From the 'Filter by Tenant' dropdown, select a tenant in which to search. This narrows the search.
- From the 'Search Users' dropdown, select **Search Users** and then in the 'Search Item' field enter the name of the user who you are trying to locate.
- From the 'Search Users' dropdown, select **Search Users & Devices** and then in the 'Search Item' field enter the name of the user you are trying to locate or the MAC address of the device you are trying to locate.
- From the '25' dropdown, select the number of users you want displayed per page. The default is 25.

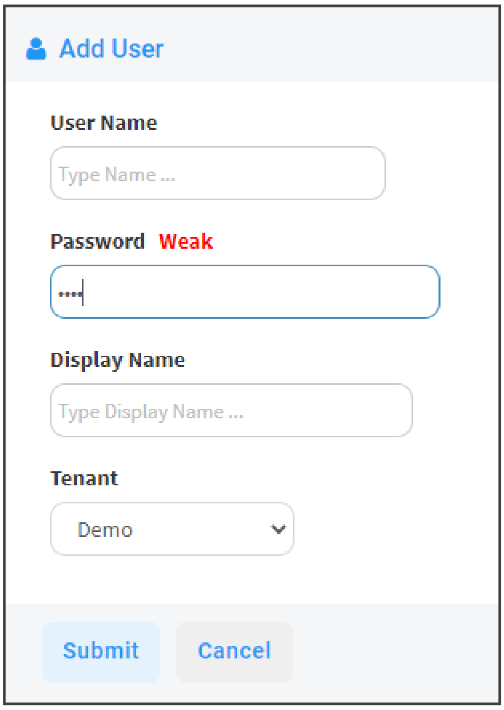
Adding a User

You can add a user to the Device Manager Pro.

➢ To add a user to the Device Manager Pro:

1. Open the Manage Users page (**Setup** > **Users & Devices** > **Manage Users**).
2. Click **+New User**. Before adding phones you need to add users.

Figure 8-11: New User



Add User

User Name

Type Name ...

Password Weak

••••

Display Name

Type Display Name ...

Tenant

Demo

3. Define a name and password for the user.
4. Define the 'Display Name' and select a tenant from the ' Tenant' dropdown.

> ⚠ Tenant/s must first be defined in the OVOC. See the *One Voice Operations Center User's Manual* for more information.

5. Click **Submit**; you're returned to the Manage Users page. Locate the added user.

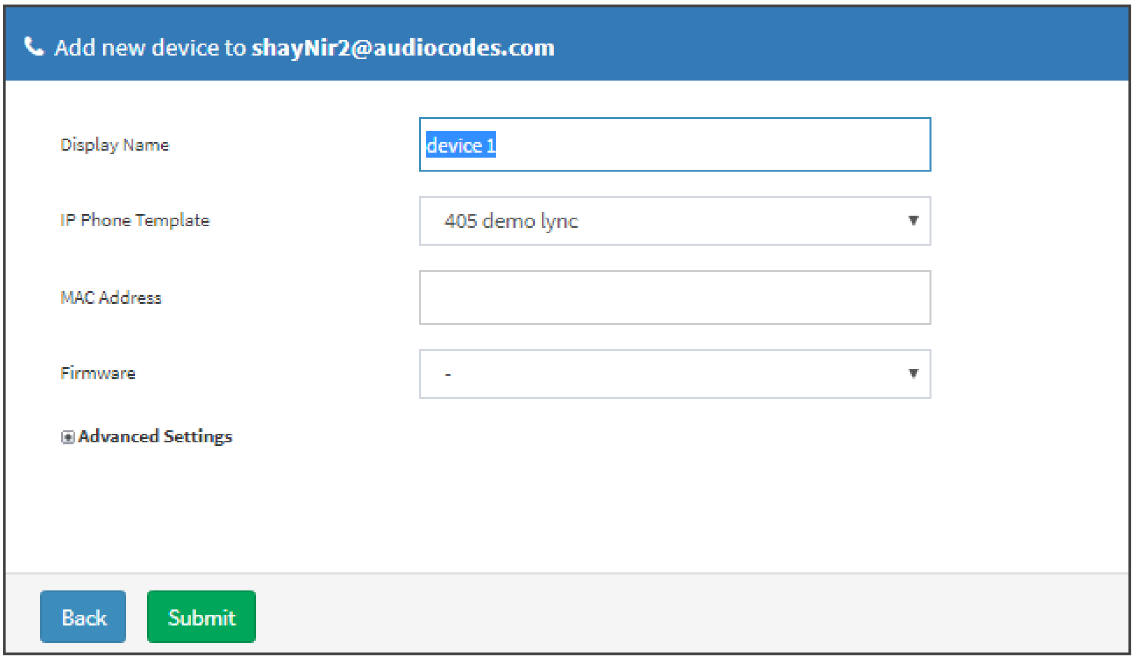
Adding a Phone

You can manually add a single phone to the server.

➢ **To add a phone:**

1. In the Manage Users page, click **+** in the row of the listed added user.

Figure 8-12: Add New Device to User



☎ Add new device to **shayNir2@audiocodes.com**

Display Name: device 1

IP Phone Template: 405 demo lync

MAC Address:

Firmware: -

2. Enter the 'Display Name', i.e., the device's name to be displayed in the Device Manager Pro.
3. From the 'Device Template' dropdown, select a template.
4. Enter the 'MAC Address'.
5. From the 'Firmware' dropdown, select the firmware relevant to the phone.
6. [Optional] Expand **+Advanced Settings**.
   - From the 'Devices Language' dropdown, select the language you want the phone interface to display.
   - From the 'VLAN Discovery mode' dropdown, select Manual / CDP / LLDP / CDP_LLDP. See under Appendix Skype for Business Environment on page 72 for more information.
7. Click **Submit** and then click **Back** to see the added device in the Manage Users page under the Devices column (click **+**).

Editing a User

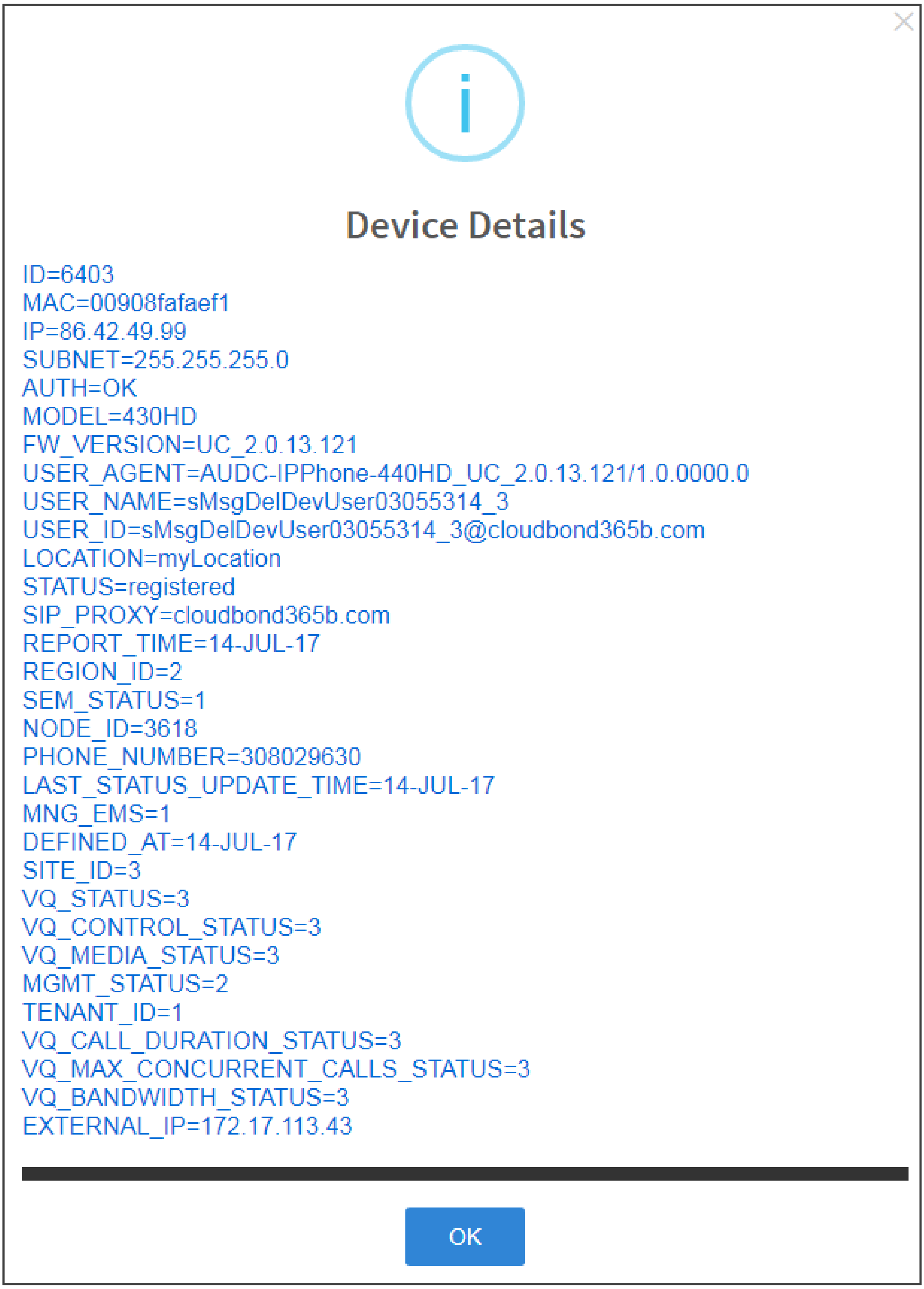
You can edit a user if (for example) they relocate to another tenant or if they are given another phone.

➢ To edit a user:

1. Click the **Edit** button in the row adjacent to the user; the Edit User screen opens.
2. Edit the same fields as when adding the device.

Viewing Device Status

You can quickly assess a device's status from the Manage Users page by clicking the ✓ icon in the Devices Status column.



Device Details

```
ID=6403
MAC=00908fafaef1
IP=86.42.49.99
SUBNET=255.255.255.0
AUTH=OK
MODEL=430HD
FW_VERSION=UC_2.0.13.121
USER_AGENT=AUDC-IPPhone-440HD_UC_2.0.13.121/1.0.0000.0
USER_NAME=sMsgDelDevUser03055314_3
USER_ID=sMsgDelDevUser03055314_3@cloudbond365b.com
LOCATION=myLocation
STATUS=registered
SIP_PROXY=cloudbond365b.com
REPORT_TIME=14-JUL-17
REGION_ID=2
SEM_STATUS=1
NODE_ID=3618
PHONE_NUMBER=308029630
LAST_STATUS_UPDATE_TIME=14-JUL-17
MNG_EMS=1
DEFINED_AT=14-JUL-17
SITE_ID=3
VQ_STATUS=3
VQ_CONTROL_STATUS=3
VQ_MEDIA_STATUS=3
MGMT_STATUS=2
TENANT_ID=1
VQ_CALL_DURATION_STATUS=3
VQ_MAX_CONCURRENT_CALLS_STATUS=3
VQ_BANDWIDTH_STATUS=3
EXTERNAL_IP=172.17.113.43
```

Deleting a User

You can delete a user if, for example, they leave the company.

➢ **To delete a user:**

- Click the **Delete** button in the row adjacent to the user; the user and device are removed.

Managing Multiple Users

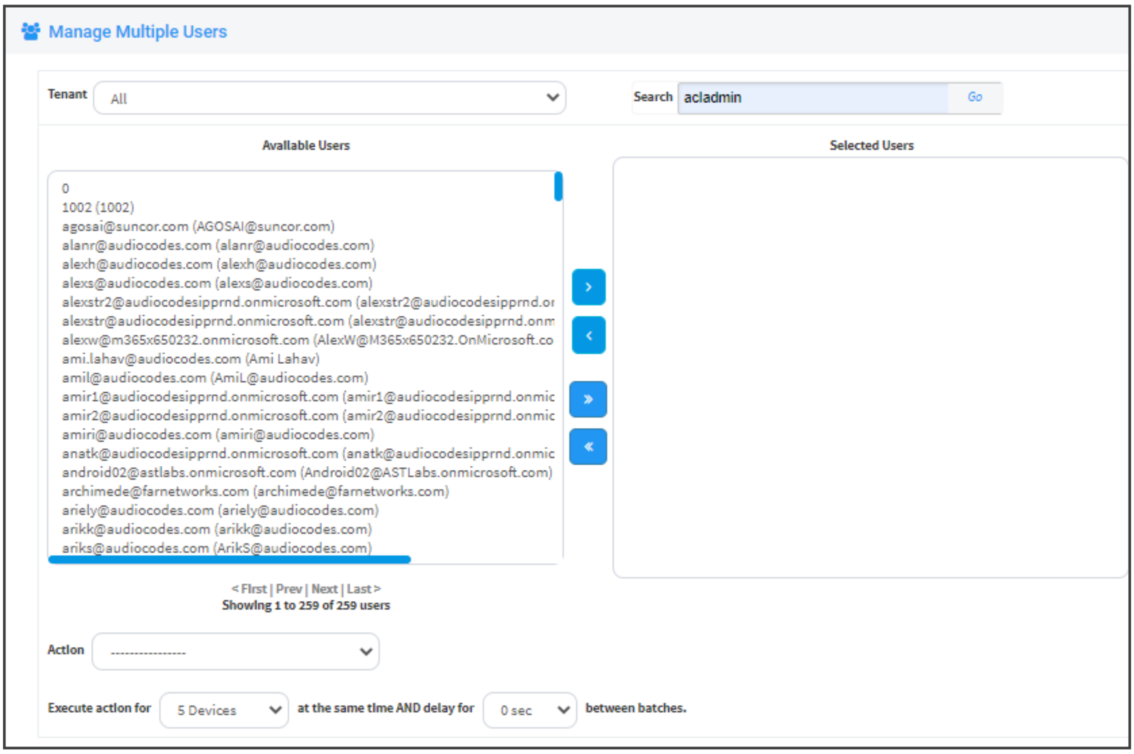
The Manage Multiple Users page lets you perform an action on a single user or on multiple users simultaneously:

- reset passwords
- delete users
- restart devices
- generate devices configuration files
- update configuration files
- send a message to multiple phones

➢ **To manage multiple users:**

1. Open the Manage Multiple Users page (**Setup** > **Users & Devices** > **Manage Multiple Users**):

Figure 8-13: Manage Multiple Users



Manage Multiple Users

Tenant: All

Search: acladmin

Avallable Users

0
1002 (1002)
agosai@suncor.com (AGOSAI@suncor.com)
alanr@audiocodes.com (alanr@audiocodes.com)
alexh@audiocodes.com (alexh@audiocodes.com)
alexs@audiocodes.com (alexs@audiocodes.com)
alexstr2@audiocodesipprnd.onmicrosoft.com (alexstr2@audiocodesipprnd.or
alexstr@audiocodesipprnd.onmicrosoft.com (alexstr@audiocodesipprnd.onm
alexw@m365x650232.onmicrosoft.com (AlexW@M365x650232.OnMicrosoft.co
ami.lahav@audiocodes.com (Ami Lahav)
amil@audiocodes.com (AmiL@audiocodes.com)
amir1@audiocodesipprnd.onmicrosoft.com (amir1@audiocodesipprnd.onmic
amir2@audiocodesipprnd.onmicrosoft.com (amir2@audiocodesipprnd.onmic
amiri@audiocodes.com (amiri@audiocodes.com)
anatk@audiocodesipprnd.onmicrosoft.com (anatk@audiocodesipprnd.onmic
android02@astlabs.onmicrosoft.com (Android02@ASTLabs.onmicrosoft.com)
archimede@farnetworks.com (archimede@farnetworks.com)
ariely@audiocodes.com (ariely@audiocodes.com)
arikk@audiocodes.com (arikk@audiocodes.com)
ariks@audiocodes.com (ArikS@audiocodes.com)

Selected Users

Showlng 1 to 259 of 259 users

Actlon: ----------------

Execute actlon for 5 Devices at the same tlme AND delay for 0 sec between batches.

2. In the Available Users pane, select a user or select multiple users on whom to perform an action.

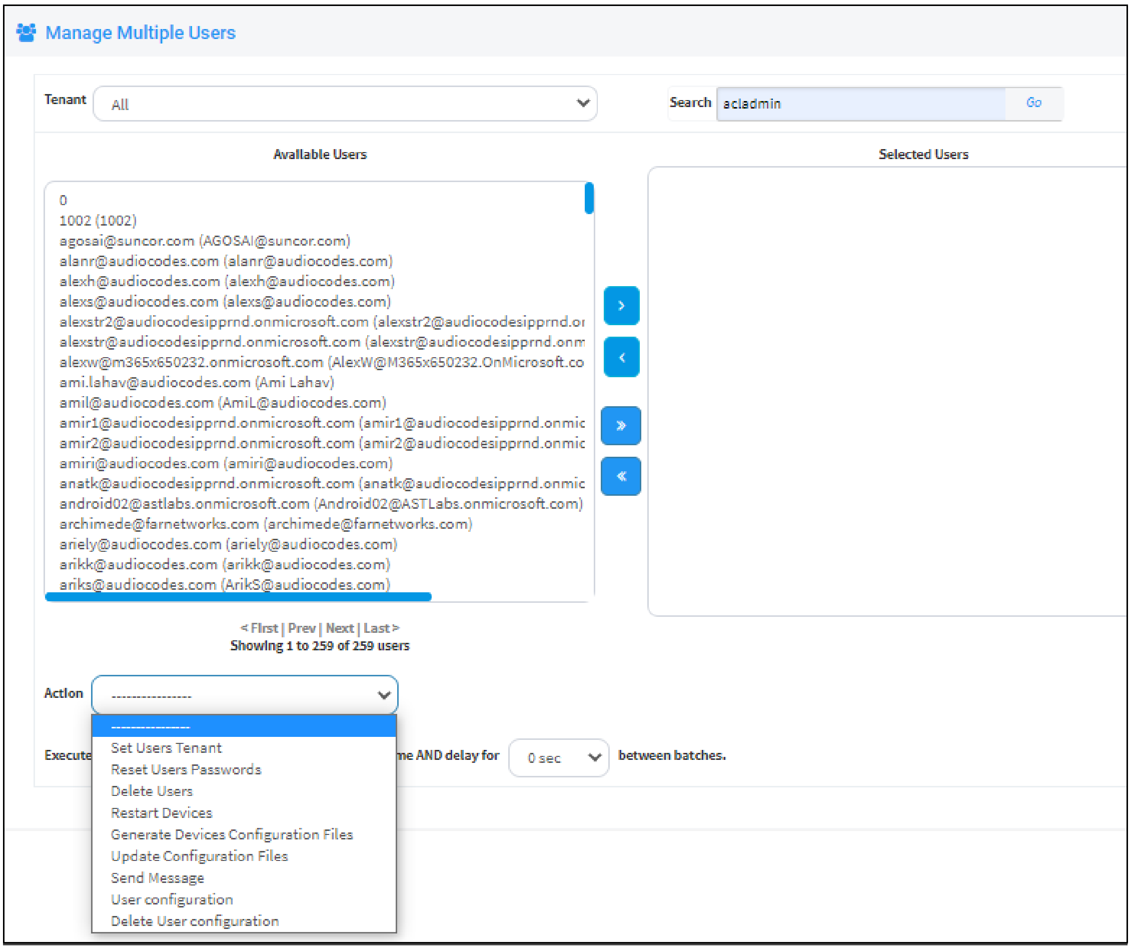
3. Click > to add a single user to the Selected Users pane.

4. Click >> to add multiple users to the Selected Users pane.

5. Click **<** to remove a single user from the Selected Users pane - after selecting them in the pane.

6. Click **<<** to remove multiple users from the Selected Users pane - after selecting them in the pane.

7. From the **Action** dropdown, select the required action.



Manage Multiple Users

Tenant: All

Search: acladmin

0
1002 (1002)
agosai@suncor.com (AGOSAI@suncor.com)
alanr@audiocodes.com (alanr@audiocodes.com)
alexh@audiocodes.com (alexh@audiocodes.com)
alexs@audiocodes.com (alexs@audiocodes.com)
alexstr2@audiocodesipprnd.onmicrosoft.com (alexstr2@audiocodesipprnd.or
alexstr@audiocodesipprnd.onmicrosoft.com (alexstr@audiocodesipprnd.onm
alexw@m365x650232.onmicrosoft.com (AlexW@M365x650232.OnMicrosoft.co
ami.lahav@audiocodes.com (Ami Lahav)
amil@audiocodes.com (AmiL@audiocodes.com)
amir1@audiocodesipprnd.onmicrosoft.com (amir1@audiocodesipprnd.onmic
amir2@audiocodesipprnd.onmicrosoft.com (amir2@audiocodesipprnd.onmic
amiri@audiocodes.com (amiri@audiocodes.com)
anatk@audiocodesipprnd.onmicrosoft.com (anatk@audiocodesipprnd.onmic
android02@astlabs.onmicrosoft.com (Android02@ASTLabs.onmicrosoft.com)
archimede@farnetworks.com (archimede@farnetworks.com)
ariely@audiocodes.com (ariely@audiocodes.com)
arikk@audiocodes.com (arikk@audiocodes.com)
ariks@audiocodes.com (ArikS@audiocodes.com)

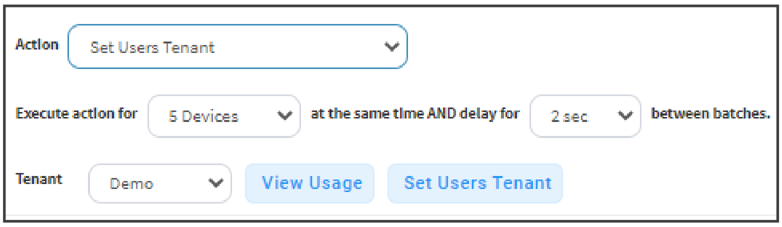
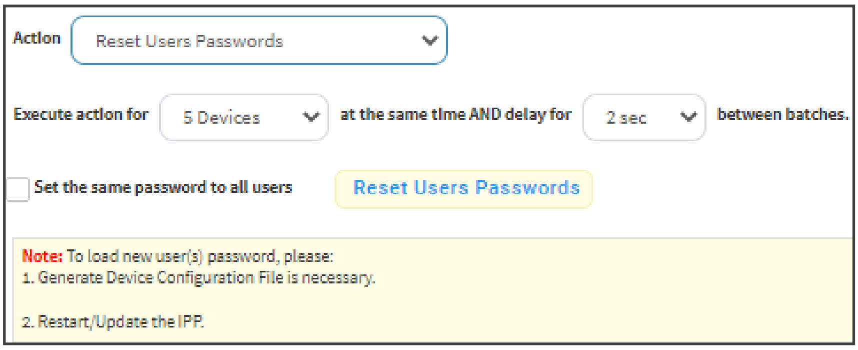
Showing 1 to 259 of 259 users

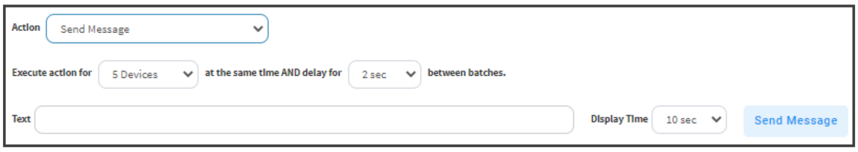
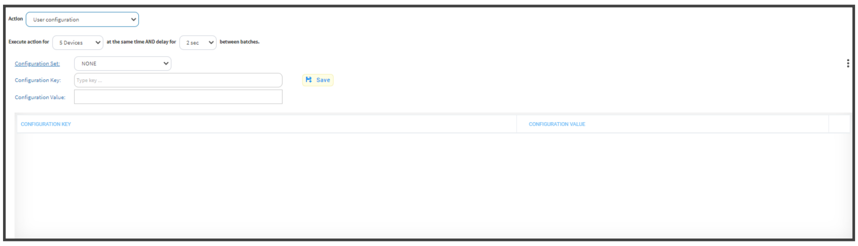
Action: ----------------

Execute ... me AND delay for 0 sec between batches.

- Use the table below as reference.

Table 8-3: Managing Multiple Users - Actions

Action	Description
Set Users Tenant	 Action: Set Users Tenant Execute action for 5 Devices at the same time AND delay for 2 sec between batches. Tenant: Demo Sets the tenant for users selected.
Reset Users Passwords	 Action: Reset Users Passwords Execute action for 5 Devices at the same time AND delay for 2 sec between batches. ☐ Set the same password to all users Note: To load new user(s) password, please: 1. Generate Device Configuration File is necessary. 2. Restart/Update the IPP. Resets users passwords. A random password is generated for each user. To generate a single password for all users selected, select the **Set the same password to all users** option. To load the new user passwords: ■ Generate the device's configuration file ■ Restart/Update the device
Delete Users	Deletes users and applies a configurable 'Delay Time' (Default = 2 seconds) after each delete is performed.
Restart Devices	Restarts devices. A reset command is sent to all selected devices. The commands are sent in batches; each batch contains 5 devices with a delay of 2 minutes between each batch. From the dropdown, choose the type of restart: ■ Graceful (default) ■ Force ■ Scheduled Before restarting, some models wait for the user to finish an active call while others may perform an immediate restart.
Generate Devices Configuration	Generates new configuration files. Updates each device with the newly generated configuration files after a configurable 'Delay Time' (default = 2 seconds) - if you select the **Updating Devices and restarting**

Action	Description
Files	**Devices after generating files** option. You can generate a private configuration file per user group, device group, or specific tenants.
Update Configuration Files	Updates each device after a configurable 'Delay Time' (default = 2 seconds).
Send Message	Lets you send a message to the screens of all user devices selected. Enter the message in the 'Text' field. You can configure the length of time the message will be displayed in the screens. Phones beep to alert users when messages come in.  Action: Send Message Execute action for 5 Devices at the same time AND delay for 2 sec between batches. Text: Display Time: 10 sec
User Configuration	 Action: User configuration Execute action for 5 Devices at the same time AND delay for 2 sec between batches. Configuration Set: NONE Configuration Key: Type key ... Configuration Value: Configures the values that will be added to the *mac.cfg* file for the selected users. Note that you can copy from one user to multiple users.
Delete User Configuration	Deletes the user configuration for the selected users.

The page also lets you

- filter per tenant before selecting users on whom to perform an action
- configure performing the action on a batch of 1 | 5 | 10 | 20 | 30 | 50 | 100 devices simultaneously
- configure a 0 second | 2 second | 5 second | 10 second | 30 second | 2 minute | 5 minute delay between batches

Maintaining Multiple Devices

The Manage Multiple Devices page lets you perform a single operation on all or on many user devices. The page lets you

- delete multiple devices
- change devices type

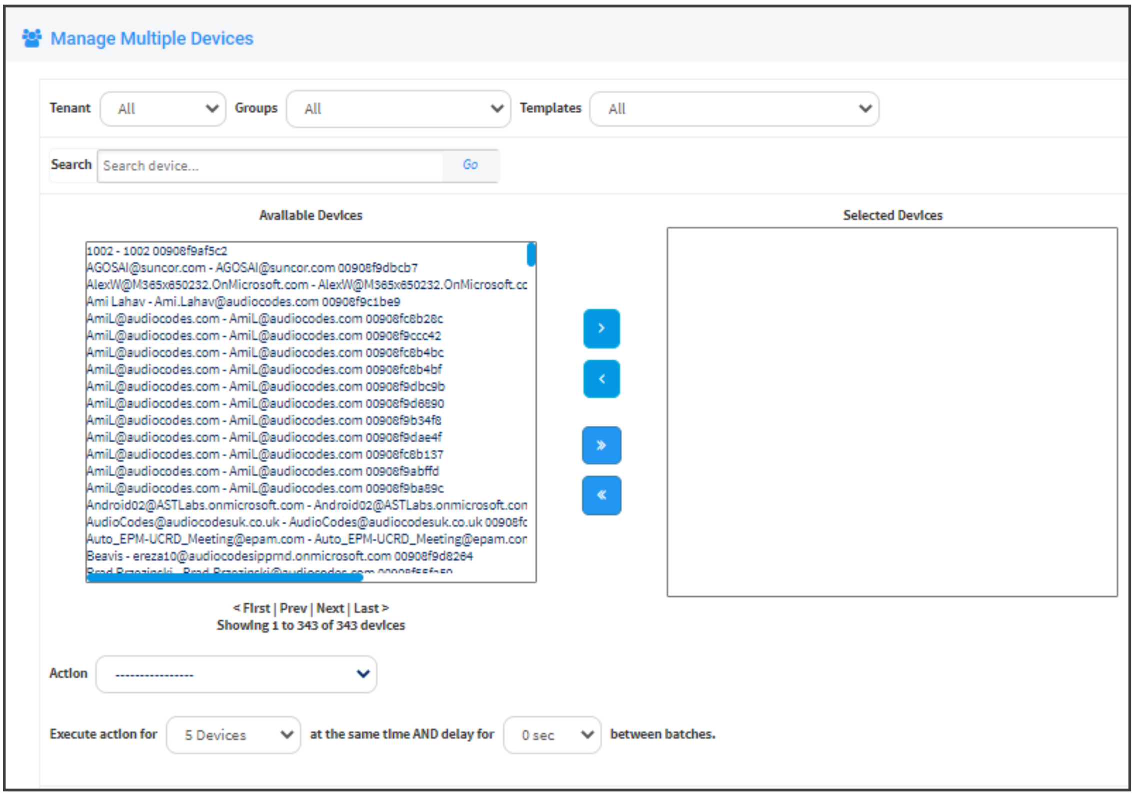
- change language
- restart multiple devices
- generate devices configuration files
- update configuration files
- send a message to multiple phones

> ⚠ These operations can also be performed on an endpoints group or on all endpoints groups; from the 'Groups' drop-down in the Manage Multiple Devices page shown in the figure below, select a single endpoints group, or **All**. For more information about *adding an endpoint to a group*, see under Checking Devices Status on page 42. For more information about *configuring an endpoints group* , see Configuring an Endpoints Group on page 17.

➢ To manage multiple devices:

1. Open the Manage Multiple Devices page (**Setup** > **Users & Devices** > **Manage Multiple Devices**):

Figure 8-14: Manage Multiple Devices



Manage Multiple Devices

Tenant: All

Groups: All

Templates: All

Search: Search device... Go

Available Devices

1002 - 1002 00908f9af5c2
AGOSAI@suncor.com - AGOSAI@suncor.com 00908f9dbcb7
AlexW@M365x650232.OnMicrosoft.com - AlexW@M365x650232.OnMicrosoft.cc
Ami Lahav - Ami.Lahav@audiocodes.com 00908f9c1be9
AmiL@audiocodes.com - AmiL@audiocodes.com 00908fc8b28c
AmiL@audiocodes.com - AmiL@audiocodes.com 00908f9ccc42
AmiL@audiocodes.com - AmiL@audiocodes.com 00908fc8b4bc
AmiL@audiocodes.com - AmiL@audiocodes.com 00908fc8b4bf
AmiL@audiocodes.com - AmiL@audiocodes.com 00908f9dbc9b
AmiL@audiocodes.com - AmiL@audiocodes.com 00908f9d6890
AmiL@audiocodes.com - AmiL@audiocodes.com 00908f9b34f8
AmiL@audiocodes.com - AmiL@audiocodes.com 00908f9dae4f
AmiL@audiocodes.com - AmiL@audiocodes.com 00908fc8b137
AmiL@audiocodes.com - AmiL@audiocodes.com 00908f9abffd
AmiL@audiocodes.com - AmiL@audiocodes.com 00908f9ba89c
Android02@ASTLabs.onmicrosoft.com - Android02@ASTLabs.onmicrosoft.con
AudioCodes@audiocodesuk.co.uk - AudioCodes@audiocodesuk.co.uk 00908fc
Auto_EPM-UCRD_Meeting@epam.com - Auto_EPM-UCRD_Meeting@epam.cor
Beavis - ereza10@audiocodesipprnd.onmicrosoft.com 00908f9d8264

< First | Prev | Next | Last >
Showing 1 to 343 of 343 devices

Selected Devices

Action: ----------------

Execute action for 5 Devices at the same time AND delay for 0 sec between batches.

2. You can filter devices per tenant, before selecting those to perform an action on.
3. You can enter a string in the 'Search' field and then click **Go** to search for devices.

4. In the Available Devices pane, select a device on which to perform an action and then click **>** to add it to the Selected Devices pane -or- select multiple devices on which to perform an action and then click **>>** to add them to the Selected Devices pane.

5. In the Selected Devices pane, select a single device and then click < to remove it, or select multiple Selected Devices and then click **<<** to remove them.

6. From the **Action** dropdown, select an action. Use the table below as reference.

Table 8-4: Managing Multiple Devices - Actions

Action	Description
Delete Devices	Deletes selected devices from the server applying a configurable 'Delay Time' (default = 2 seconds) in the process.
Change Template	This action will update the device template in the database. To finish the action, you need to: 1. Generate the device's Configuration File 2. Restart/Update the phone.
Change Language	Changes the phone language. Select the language from the **Language** dropdown and click **Change**. To view the usage of a language, click **View Usage**. To load a new language: 1. Generate the device's configuration file. 2. Restart/update the phone.
Restart Devices	Restarts online devices. Before restarting, some models wait for the user to finish an active call while others may perform an immediate restart. From the dropdown, choose the type of restart: ■ Graceful (default) ■ Force ■ Scheduled
Generate Devices Configuration Files	Generates new configuration files. Updates each phone with the newly generated configuration files after a configurable 'Delay Time' (default = 2 seconds) - if you selected the **Updating Devices and restarting Devices after generating files** option (by default it is selected).
Update Configuration File	Updates each phone after a configurable 'Delay Time' (default = 2 seconds).
Send Message	Lets you send a message to the screens of all user phones selected.

Action	Description
	Enter the message in the 'Text' field. You can configure the length of time the message will be displayed in the screen. Phones beep to alert users when messages come in.
Change Firmware	Lets you upload a different .img firmware file to the phone.
Change VLAN Discovery Mode	Used to change the virtual phone network's mode of operation. Go to Skype for Business Environment.htm for the options descriptions [Manual/CDP/LLDP/CDP_LLDP]

➢ To update all existing configuration files according to the new template:

- After selecting devices, select from the 'Action' dropdown the **Generate Devices Configuration Files** option in the Manage Multiple Devices page.

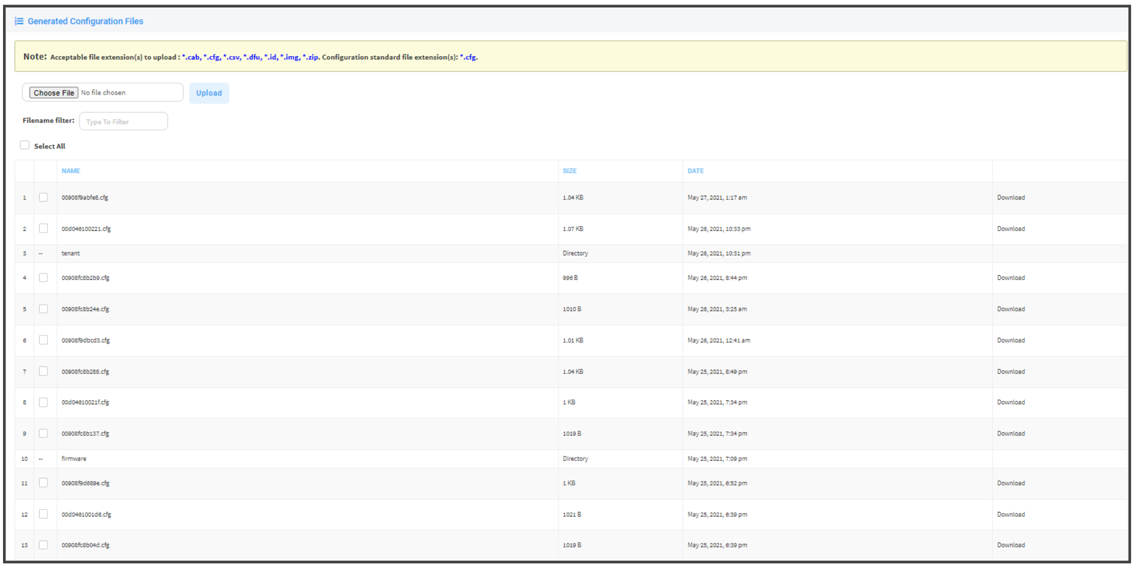
Managing Configuration Files

You can manage devices' configuration files. All cfg files are created and located on the OVOC server. You can view and manage storage, and upload and delete files from storage. To avoid network congestion, a delay feature enables an interval between each installation.

➢ To manage devices' configuration files:

- Open the Manage Configuration Files page (**Setup** > **Configuration** > **Generated Config Files**).

Figure 8-15: Manage Configuration Files



Generated Configuration Files

Note: Acceptable file extension(s) to upload : *.cab, *.cfg, *.csv, *.dfu, *.id, *.img, *.zip. Configuration standard file extension(s): *.cfg.

		NAME	SIZE	DATE	
1	□	00908f9abfe8.cfg	1.04 KB	May 27, 2021, 1:17 am	Download
2	□	00d046100221.cfg	1.07 KB	May 26, 2021, 10:33 pm	Download
3	--	tenant	Directory	May 26, 2021, 10:31 pm	
4	□	00908fc8b2b9.cfg	996 B	May 26, 2021, 8:44 pm	Download
5	□	00908fc8b24e.cfg	1010 B	May 26, 2021, 3:25 am	Download
6	□	00908f9dbcd3.cfg	1.01 KB	May 26, 2021, 12:41 am	Download
7	□	00908fc8b288.cfg	1.04 KB	May 25, 2021, 8:49 pm	Download
8	□	00d04610021f.cfg	1 KB	May 25, 2021, 7:34 pm	Download
9	□	00908fc8b137.cfg	1019 B	May 25, 2021, 7:34 pm	Download
10	--	firmware	Directory	May 25, 2021, 7:09 pm	
11	□	00908f9d689e.cfg	1 KB	May 25, 2021, 6:52 pm	Download
12	□	00d0461001d6.cfg	1021 B	May 25, 2021, 6:39 pm	Download
13	□	00908fc8b04d.cfg	1019 B	May 25, 2021, 6:39 pm	Download

The page lets you

- Filter the .cfg configuration files listed by name

- Browse to a location on your PC and upload a .cfg configuration file
- Select and delete any or all of the .cfg configuration files listed
- Open any of the .cfg configuration files listed in an editor
- Save any of the .cfg configuration files listed
- Download any of the .cfg configuration files listed
- View all configuration files currently located on the server (global configuration files, company directory configuration files, and IP phone configuration files and third-party vendor product configuration files)

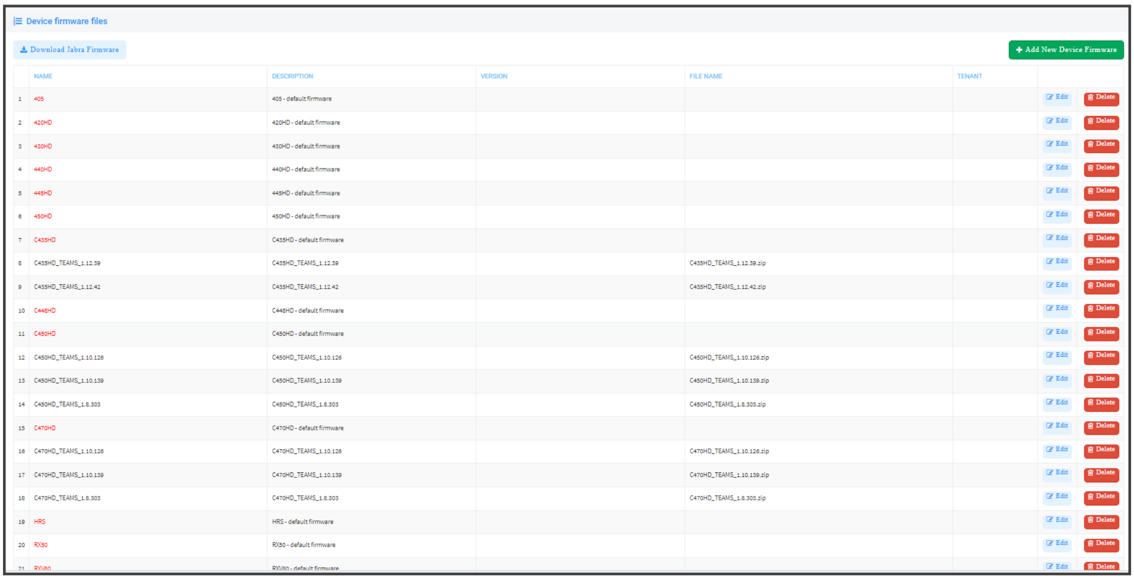
Managing Firmware Files

The 'Device firmware files' page allows network administrators to download, edit, delete and add devices' .img firmware files.

➢ To manage the .img firmware files:

- Open the Device Firmware Files page (**Setup** > **Firmware** > **Firmware Files**).

Figure 8-16: Device Firmware Files



Device firmware files

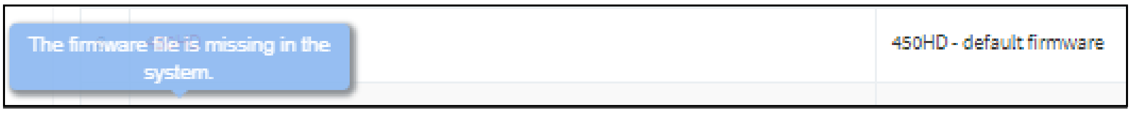
	NAME	DESCRIPTION	VERSION	FILE NAME	TENANT		
1	405	405 - default firmware				Edit	Delete
2	420HD	420HD - default firmware				Edit	Delete
3	430HD	430HD - default firmware				Edit	Delete
4	440HD	440HD - default firmware				Edit	Delete
5	445HD	445HD - default firmware				Edit	Delete
6	450HD	450HD - default firmware				Edit	Delete
7	C435HD	C435HD - default firmware				Edit	Delete
8	C435HD_TEAMS_1.12.39	C435HD_TEAMS_1.12.39		C435HD_TEAMS_1.12.39.zip		Edit	Delete
9	C435HD_TEAMS_1.12.42	C435HD_TEAMS_1.12.42		C435HD_TEAMS_1.12.42.zip		Edit	Delete
10	C448HD	C448HD - default firmware				Edit	Delete
11	C450HD	C450HD - default firmware				Edit	Delete
12	C450HD_TEAMS_1.10.126	C450HD_TEAMS_1.10.126		C450HD_TEAMS_1.10.126.zip		Edit	Delete
13	C450HD_TEAMS_1.10.139	C450HD_TEAMS_1.10.139		C450HD_TEAMS_1.10.139.zip		Edit	Delete
14	C450HD_TEAMS_1.8.303	C450HD_TEAMS_1.8.303		C450HD_TEAMS_1.8.303.zip		Edit	Delete
15	C470HD	C470HD - default firmware				Edit	Delete
16	C470HD_TEAMS_1.10.126	C470HD_TEAMS_1.10.126		C470HD_TEAMS_1.10.126.zip		Edit	Delete
17	C470HD_TEAMS_1.10.139	C470HD_TEAMS_1.10.139		C470HD_TEAMS_1.10.139.zip		Edit	Delete
18	C470HD_TEAMS_1.8.303	C470HD_TEAMS_1.8.303		C470HD_TEAMS_1.8.303.zip		Edit	Delete
19	HRS	HRS - default firmware				Edit	Delete
20	RX50	RX50 - default firmware				Edit	Delete
21	RXV80	RXV80 - default firmware				Edit	Delete

⚠ For information on third-party vendor products, see the Device Manager for Third-Party Vendor Products Administrator's Manual

In this page you can

- View all .img firmware files currently located on the server
- Add a new device firmware file. Note that if default names are used (e.g., 420HD.img), all devices of this type will automatically use it.
- Manage the .dfu firmware files of the Huddle Room Solution (HRS) speakers.

- Filter by filename the .img firmware files listed
- Determine if the device has firmware or not. If the device does not have firmware, its name will be red-coded and a tool tip will indicate a missing firmware file when you point the cursor at it.



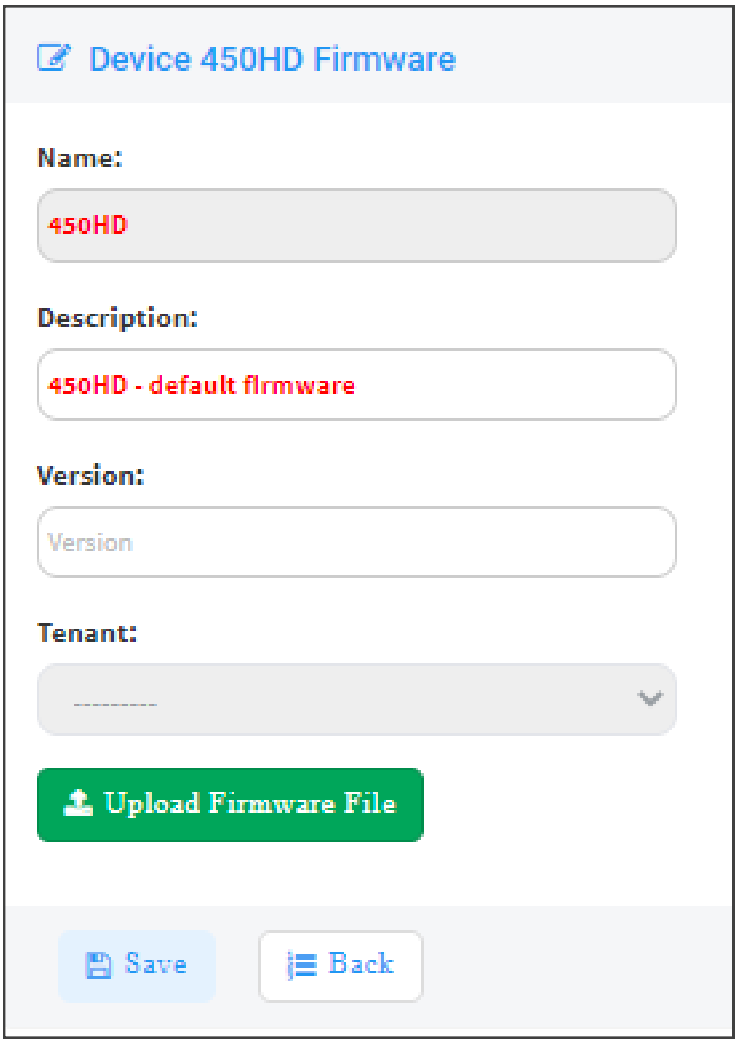
The firmware file is missing in the system.

450HD - default firmware

- If this is the case, upload the device's .img firmware file that you obtained from AudioCodes, to the OVOC provisioning server:

  a. Click the red-coded name of the phone.

Figure 8-17: .img Firmware File Upload



Device 450HD Firmware

Name:

450HD

Description:

450HD - default firmware

Version:

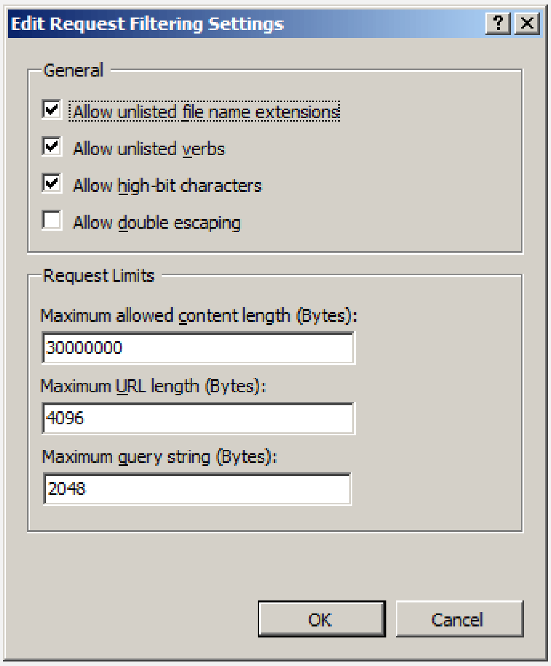
Version

Tenant:

----

  b. Click the **Upload firmware file** button and then navigate to the .img file you received from AudioCodes and put on the OVOC provisioning server. You can perform this part of the installation procedure before or after configuring your enterprise's DHCP Server with DHCP Option 160.

- If Microsoft's Internet Information Services (IIS) web server is deployed in the network, you need to change the default value of the parameter 'Max allowed content length (Bytes)' (shown in the following figure) to the size of the .img file (at least) before uploading the .img file of the 445HD or 440HD phone to the Device Manager Pro.
- If it's left unchanged at the Microsoft default, the .img file for the 445HD and 440HD phone will not be uploaded to the Device Manager Pro because it's heavier than the Microsoft default.



Edit Request Filtering Settings

General

☑ Allow unlisted file name extensions

☑ Allow unlisted verbs

☑ Allow high-bit characters

☐ Allow double escaping

Request Limits

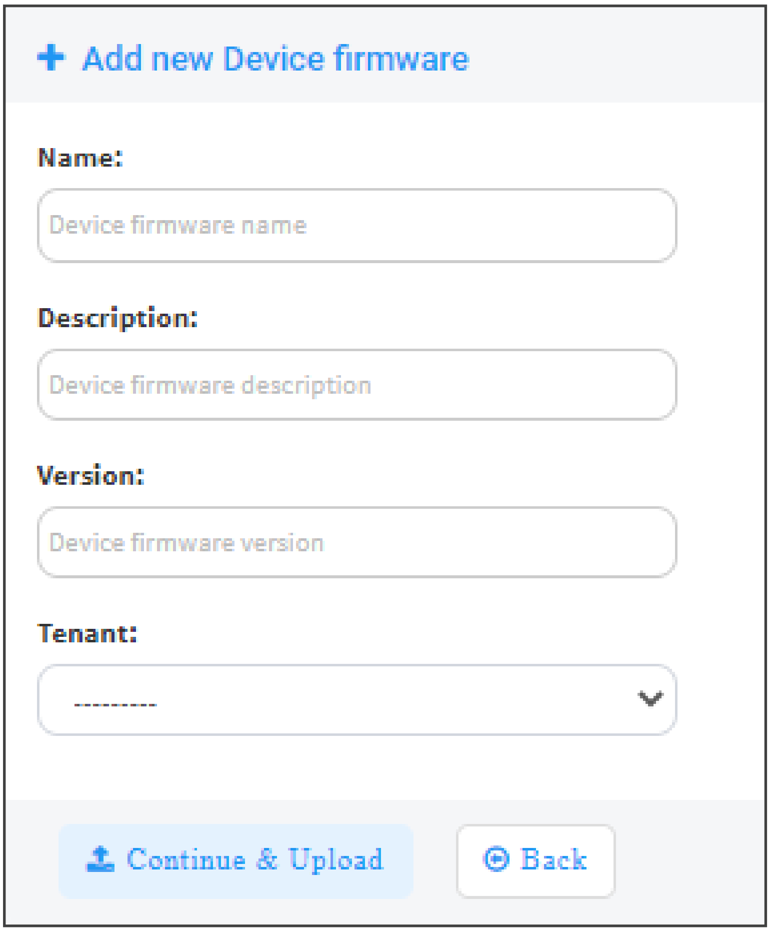
Maximum allowed content length (Bytes): 30000000

Maximum URL length (Bytes): 4096

Maximum query string (Bytes): 2048

- After an .img firmware file has been uploaded to a phone, you can download it to your pc. Click the device's name and then in the screen that opens, click the **Download firmware file** button.
- Edit a device's .img firmware file. Click the name or click the **Edit** button in the row.
- Delete any .img firmware file listed. Click the **Delete** button in the row.
- Manage .img firmware files by grouping them.

  a. In the 'Device firmware files' page, click the **Add New Device Firmware** button located in the upper right corner.



Add new Device firmware

Name:

Device firmware name

Description:

Device firmware description

Version:

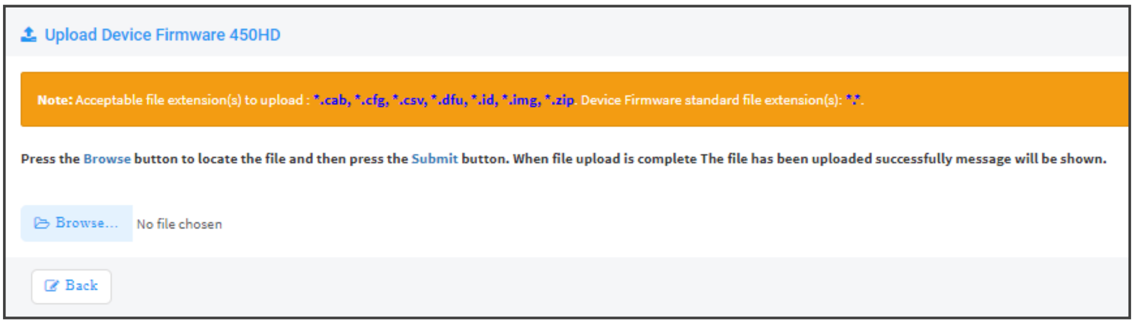
Device firmware version

Tenant:

----

b. Define an intuitive 'Name' and 'Description' to facilitate easy identification. You can leave the 'Version' field empty, and then click **Continue & Upload**.

c. Click **Upload firmware file**:



Upload Device Firmware 450HD

Note: Acceptable file extension(s) to upload : *.cab, *.cfg, *.csv, *.dfu, *.id, *.img, *.zip. Device Firmware standard file extension(s): *.*.

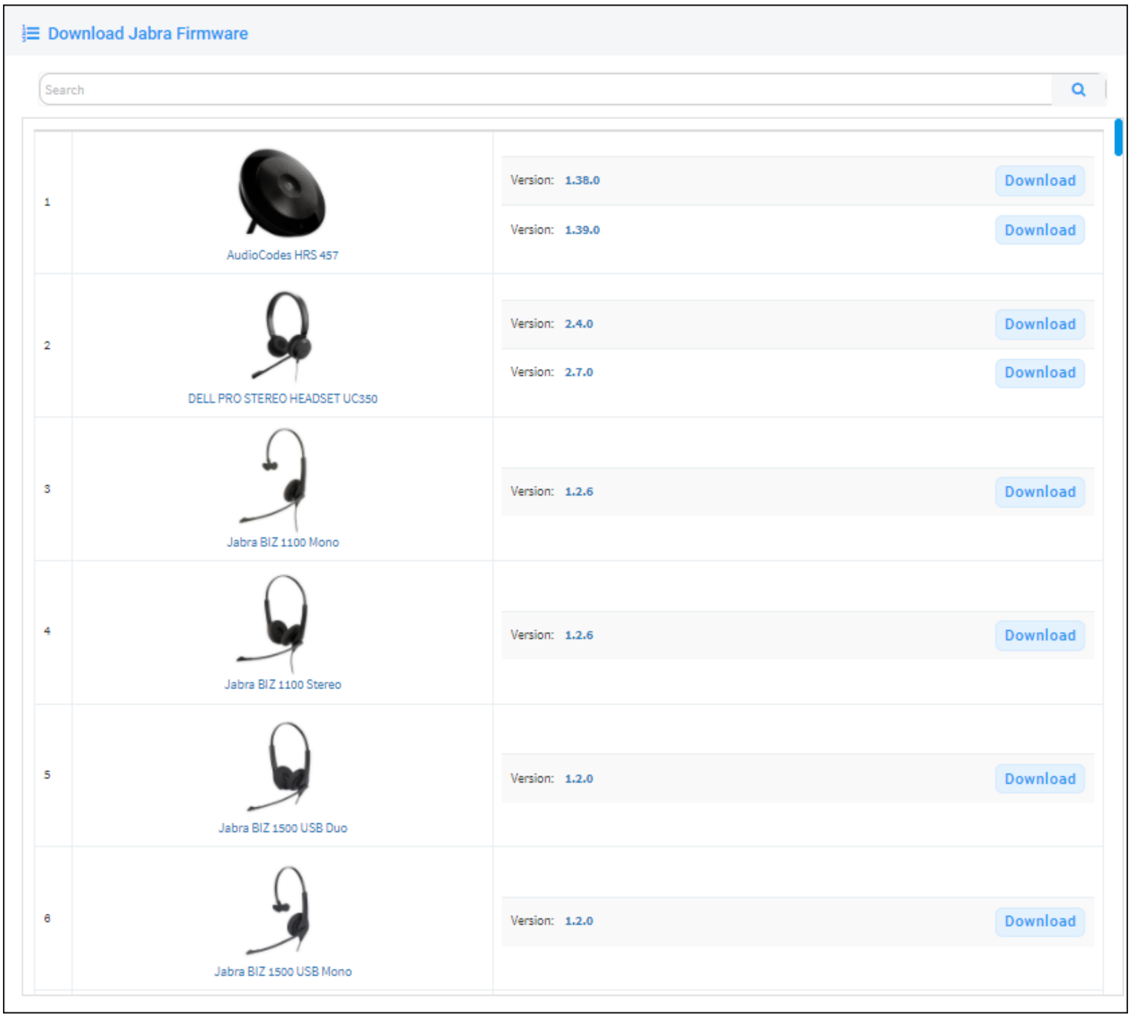
Press the Browse button to locate the file and then press the Submit button. When file upload is complete The file has been uploaded successfully message will be shown.

No file chosen

d. Click **Browse**, navigate to the .img file, and then click **Save**; the 'Version' field is populated and the .img file is uploaded to the phone.

➢ To download Jabra firmware files:

1. In the 'Device firmware files' page, click the **Download Jabra Firmware** button.



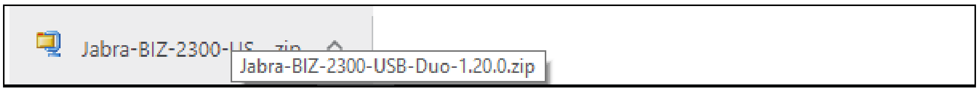
Download Jabra Firmware

Search

1	AudioCodes HRS 457	Version: 1.38.0 Version: 1.39.0	Download Download
2	DELL PRO STEREO HEADSET UC350	Version: 2.4.0 Version: 2.7.0	Download Download
3	Jabra BIZ 1100 Mono	Version: 1.2.6	Download
4	Jabra BIZ 1100 Stereo	Version: 1.2.6	Download
5	Jabra BIZ 1500 USB Duo	Version: 1.2.0	Download
6	Jabra BIZ 1500 USB Mono	Version: 1.2.0	Download

2. Locate the device firmware you require; point your cursor over each entry for detailed information on each device to be displayed, and then click the **Download** button adjacent to the device whose firmware you require.

3. After the download, view the downloaded file indication in the lowermost left corner of the page.



Jabra-BIZ-2300-US...zip

Jabra-BIZ-2300-USB-Duo-1.20.0.zip

4. To upload the file to the device, follow the same procedure as that described for uploading phone firmware.

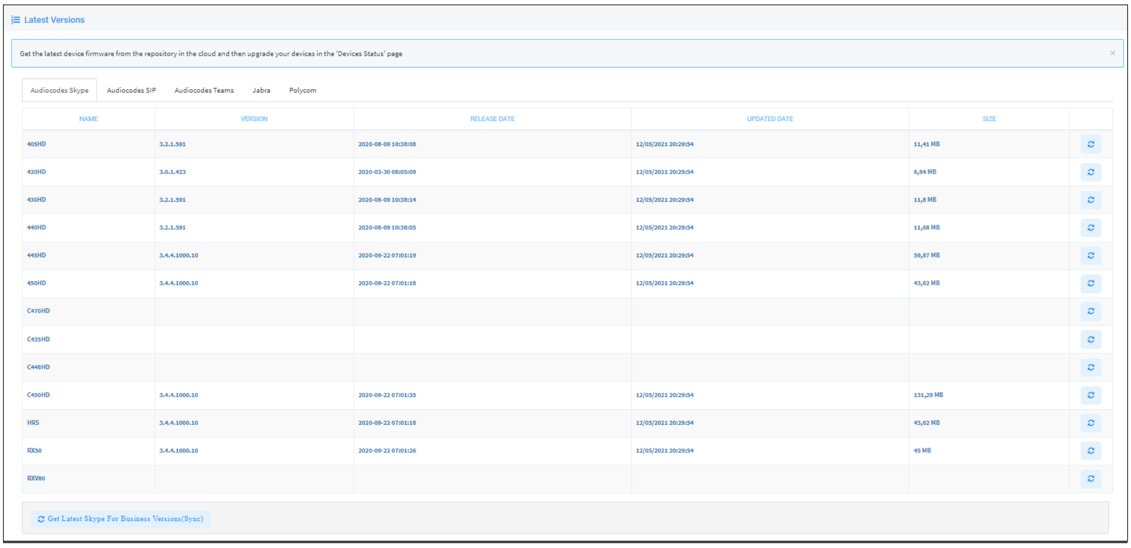
Upgrading Devices to the Latest Firmware Versions

The Device Manager's 'Latest versions' page allows network administrators to get the latest device firmware files from AudioCodes' firmware repository located in the cloud, before upgrading the devices in the 'Devices Status' page. The 'Latest versions' page allows network administrators to 'sync' with the repository before performing the upgrade.

➢ To sync with the repository:

1. Open the 'Latest versions' page (**Setup** > **Firmware** > **Latest Firmware Versions**).

Figure 8-18: Latest Versions



Latest Versions

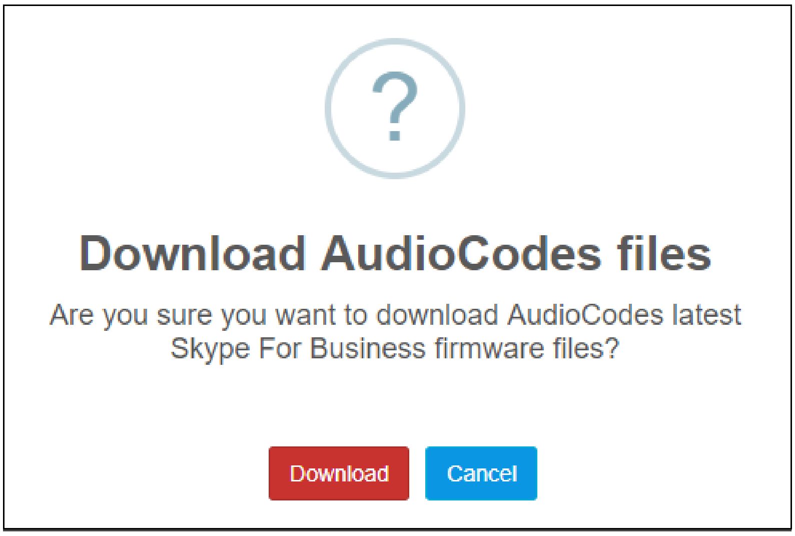
Get the latest device firmware from the repository in the cloud and then upgrade your devices in the 'Devices Status' page

NAME	VERSION	RELEASE DATE	UPDATED DATE	SIZE	
405HD	3.2.1.591	2020-08-09 10:38:08	12/05/2021 20:29:54	11,41 MB	↻
420HD	3.0.1.423	2020-03-30 08:05:09	12/05/2021 20:29:54	6,84 MB	↻
430HD	3.2.1.591	2020-08-09 10:38:14	12/05/2021 20:29:54	11,8 MB	↻
440HD	3.2.1.591	2020-08-09 10:38:05	12/05/2021 20:29:54	11,68 MB	↻
445HD	3.4.4.1000.10	2020-09-22 07:01:19	12/05/2021 20:29:54	59,87 MB	↻
450HD	3.4.4.1000.10	2020-09-22 07:01:18	12/05/2021 20:29:54	43,62 MB	↻
C470HD					↻
C435HD					↻
C448HD					↻
C450HD	3.4.4.1000.10	2020-09-22 07:01:35	12/05/2021 20:29:54	131,29 MB	↻
HRS	3.4.4.1000.10	2020-09-22 07:01:18	12/05/2021 20:29:54	43,62 MB	↻
RX50	3.4.4.1000.10	2020-09-22 07:01:26	12/05/2021 20:29:54	45 MB	↻
RXV80					↻

2. Click the **Get latest Skype for Business versions (Sync)** button or the **Get latest Generic SIP versions (Sync)** button.

> ⚠ Very few deployments, if any, feature both Skype for Business phones *and* generic SIP phones, so when performing a sync, do so for either one or the other, never for both.

Figure 8-19: Sync



Download AudioCodes files

Are you sure you want to download AudioCodes latest Skype For Business firmware files?

3. Click the **Download** button; the latest firmware files for the selected phone type are pulled from the repository in the cloud and displayed in the 'Latest Versions' page.

4. Open the 'Devices Status' page (**Monitor** > **Dashboard** > **Devices Status**) and from the 'Actions' button adjacent to a phone, select **Update Firmware**; the phone will use the firmware file listed in the 'Latest Versions' page.

- The same procedure applies to Jabra firmware files viewed under the **Jabra** tab in the 'Latest Versions' page.
- See also Checking Devices Status on page 42.

9 Viewing Your License

Use of OVOC server platform processes is managed by a license that controls the time period validity for the use of the platform.

The License page displays the license's properties, including the number of days remaining until it expires.

➢ To view your license's properties:

1. Open the License Properties page (**Setup** > **System** > **License**).

Figure 9-1: License Properties

2. Use the table below as reference.

Table 9-1: License Properties

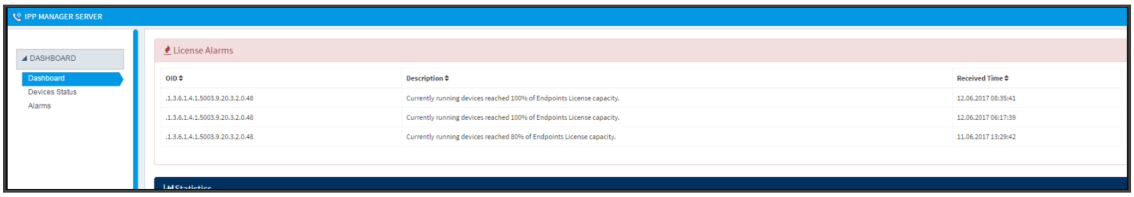
Action	Description
Status	Indicates the license's status (Enable or Disable). If enabled and the configured time expires, connection to the OVOC server platform is denied. When it expires, the Device Manager Pro is rendered non-usable. Contact your AudioCodes partner if the license expires.
Expiration Date	Displays **DD:MM:YY**.
Days Left	The number of days remaining until your license expires. Minus indicates your license has expired. Contact your AudioCodes partner if the license expires.
Number of devices	The total number of devices deployed in your enterprise network.

> ⚠ If a license expires, communications with all servers will be suspended; users will not be able to log in, and it will not be possible to add new phones.

The time zone is determined by the OVOC server's Date & Time menu settings. If an expiration date is not configured, the 'Expiration Date' field displays **Unlimited**.

- As the license's expiration date approaches, warning alarms are issued:
  - ✓ A Major alarm is sent when 80% of the period defined in the currently running device's license is consumed
  - ✓ A Critical alarm is sent when 100% of the period defined in the currently running device's license is consumed
- When the maximum number of devices reporting to the OVOC is exceeded, the OVOC server blocks them and sends an alert that is displayed in the Home page.

Figure 9-2: 100% of Endpoints License Capacity Reached



License Alarms

OID	Description	Received Time
.1.3.6.1.4.1.5003.9.20.3.2.0.48	Currently running devices reached 100% of Endpoints License capacity.	12.06.2017 08:35:41
.1.3.6.1.4.1.5003.9.20.3.2.0.48	Currently running devices reached 100% of Endpoints License capacity.	12.06.2017 06:17:39
.1.3.6.1.4.1.5003.9.20.3.2.0.48	Currently running devices reached 80% of Endpoints License capacity.	11.06.2017 13:29:42

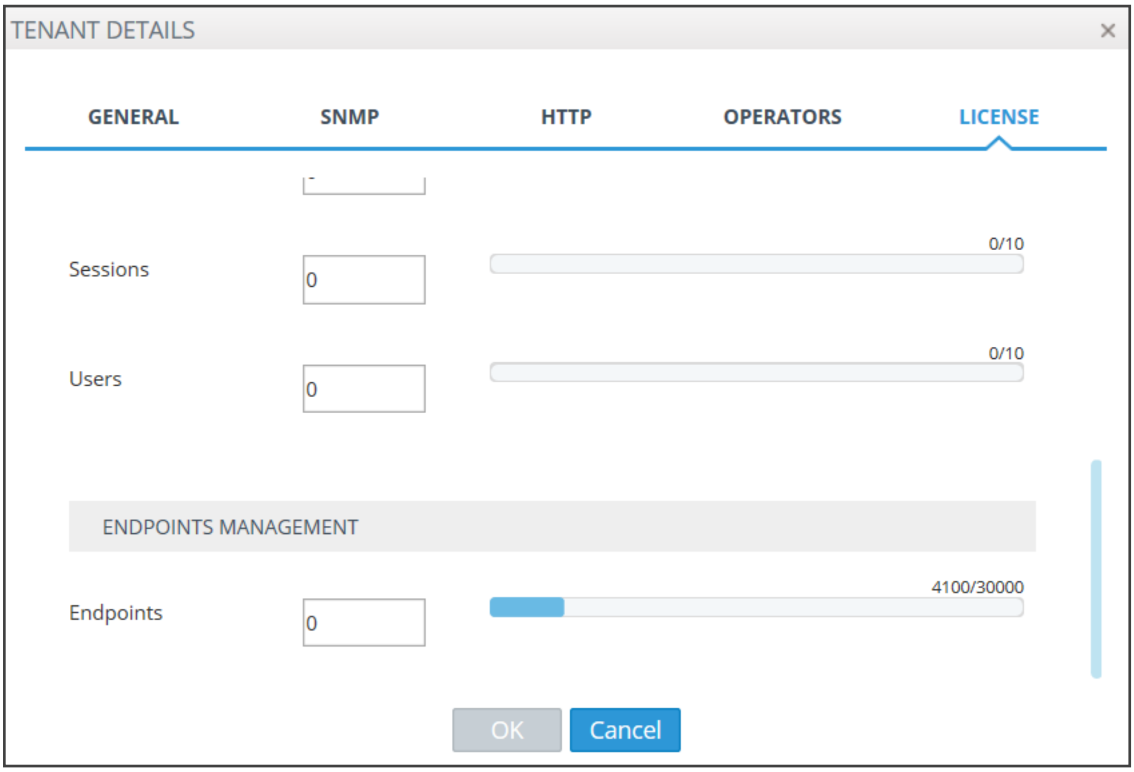
Licensing Endpoints

You can license endpoints using the One Voice Operations Center (see also the *One Voice Operations Center User's Manual*).

➢ To license endpoints:

1. When adding a new tenant in the One Voice Operations Center, click the **License** tab in the Tenant Details screen and then scroll down to the Endpoints Management section.

Figure 9-3: One Voice Operations Center: Endpoints Management



Sessions 0 0/10

Users 0 0/10

ENDPOINTS MANAGEMENT

Endpoints 0 4100/30000

2. In the Endpoints field, enter the number of endpoints the Device Manager Pro application supports for this tenant (30000 maximum).

10 Approving Users

> Approving users is not necessary
> - when using the Zero Touch provisioning method
> - when importing a csv file containing devices (as well as users)

If you are *not* using the Zero Touch provisioning method or importing a csv file, then after plugging the phones into the network you need to approve the users.

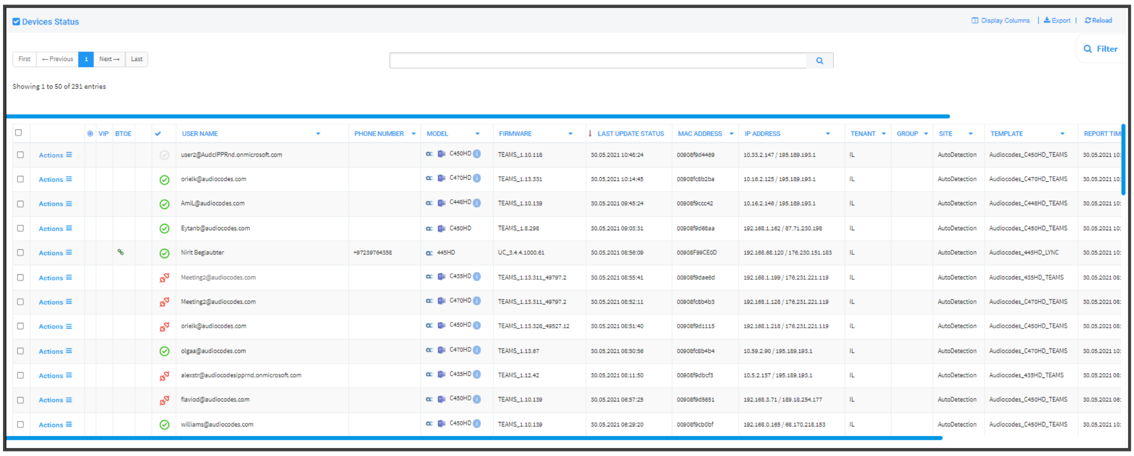
Skype for Business Environment

After plugging the phones in, they report to the Device Manager Pro which does not display user name in the UI until sign-in is performed or, until users are approved in the UI.

➢ To approve users in a Skype for Business environment:

1. In the Device Manager Pro UI, open the Devices Status page (**Dashboard** > **Devices Status**).

Figure 10-1: Devices Status



☑ Devices Status

Display Columns | Export | Reload

Filter

First | ← Previous | 1 | Next → | Last

Showing 1 to 50 of 291 entries

□		⊛	VIP	BTOE		✓	USER NAME	PHONE NUMBER	MODEL	FIRMWARE	LAST UPDATE STATUS	MAC ADDRESS	IP ADDRESS	TENANT	GROUP	SITE	TEMPLATE	REPORT TIM
□	Actions ≡					○	user2@AudcIPPRnd.onmicrosoft.com		C450HD	TEAMS_1.10.118	30.05.2021 10:48:24	00908f9d4469	10.33.2.147 / 195.189.193.1	IL		AutoDetection	Audiocodes_C450HD_TEAMS	30.05.2021 10:
□	Actions ≡					✓	orielk@audiocodes.com		C470HD	TEAMS_1.13.331	30.05.2021 10:14:45	00908fc8b2ba	10.16.2.125 / 195.189.193.1	IL		AutoDetection	Audiocodes_C470HD_TEAMS	30.05.2021 10:
□	Actions ≡					✓	AmiL@audiocodes.com		C448HD	TEAMS_1.10.139	30.05.2021 09:45:24	00908f9ccc42	10.16.2.146 / 195.189.193.1	IL		AutoDetection	Audiocodes_C448HD_TEAMS	30.05.2021 10:
□	Actions ≡					✓	Eytanb@audiocodes.com		C450HD	TEAMS_1.8.298	30.05.2021 09:03:31	00908f9d68aa	192.168.1.162 / 87.71.230.198	IL		AutoDetection	Audiocodes_C450HD_TEAMS	30.05.2021 10:
□	Actions ≡			🔗		✓	Nirit Beglaubter	+97239764358	445HD	UC_3.4.4.1000.61	30.05.2021 08:56:09	00908F99CE0D	192.168.68.120 / 176.230.151.183	IL		AutoDetection	Audiocodes_445HD_LYNC	30.05.2021 10:
□	Actions ≡					✗	Meeting2@audiocodes.com		C435HD	TEAMS_1.13.311_49797.2	30.05.2021 08:55:41	00908f9dae6d	192.168.1.199 / 176.231.221.119	IL		AutoDetection	Audiocodes_435HD_TEAMS	30.05.2021 08:
□	Actions ≡					✗	Meeting2@audiocodes.com		C470HD	TEAMS_1.13.311_49797.2	30.05.2021 08:52:11	00908fc8b4b3	192.168.1.128 / 176.231.221.119	IL		AutoDetection	Audiocodes_C470HD_TEAMS	30.05.2021 08:
□	Actions ≡					✗	orielk@audiocodes.com		C450HD	TEAMS_1.13.328_49527.12	30.05.2021 08:51:40	00908f9d1115	192.168.1.218 / 176.231.221.119	IL		AutoDetection	Audiocodes_C450HD_TEAMS	30.05.2021 08:
□	Actions ≡					✓	olgaa@audiocodes.com		C470HD	TEAMS_1.13.67	30.05.2021 08:50:56	00908fc8b4b4	10.59.2.90 / 195.189.193.1	IL		AutoDetection	Audiocodes_C470HD_TEAMS	30.05.2021 10:
□	Actions ≡					✗	alexstr@audiocodesipprnd.onmicrosoft.com		C435HD	TEAMS_1.12.42	30.05.2021 08:11:50	00908f9dbcf3	10.5.2.157 / 195.189.193.1	IL		AutoDetection	Audiocodes_435HD_TEAMS	30.05.2021 08:
□	Actions ≡					✗	flaviod@audiocodes.com		C450HD	TEAMS_1.10.139	30.05.2021 06:57:25	00908f9d5651	192.168.3.71 / 189.18.254.177	IL		AutoDetection	Audiocodes_C450HD_TEAMS	30.05.2021 06:
□	Actions ≡					✓	williams@audiocodes.com		C450HD	TEAMS_1.10.139	30.05.2021 06:29:20	00908f9cb0bf	192.168.0.165 / 68.170.218.153	IL		AutoDetection	Audiocodes_C450HD_TEAMS	30.05.2021 10:

Screen functions:

You can click the **Export** link; a csv file is generated; a download option is displayed in the lower-left corner. The same information on the page, e.g., Serial Number which allows administrators to efficiently manage devices stocktaking, is displayed in Excel format.

Actions: Check status, Change Tenant, Update Firmware, Open Web Admin (opens in HTTPS), Reset Phone, Update Configuration, Send Message (to the phone), Delete Status, Telnet.

Approve button. Displayed if the System URL is configured for the DHCP Option because the OVOC will then not know the tenant in which the device is located. If the Tenant URL is configured for the DHCP Option, the **Approve** button will not be displayed.

Last Update Status. Indicates the last time the status of the device changed.

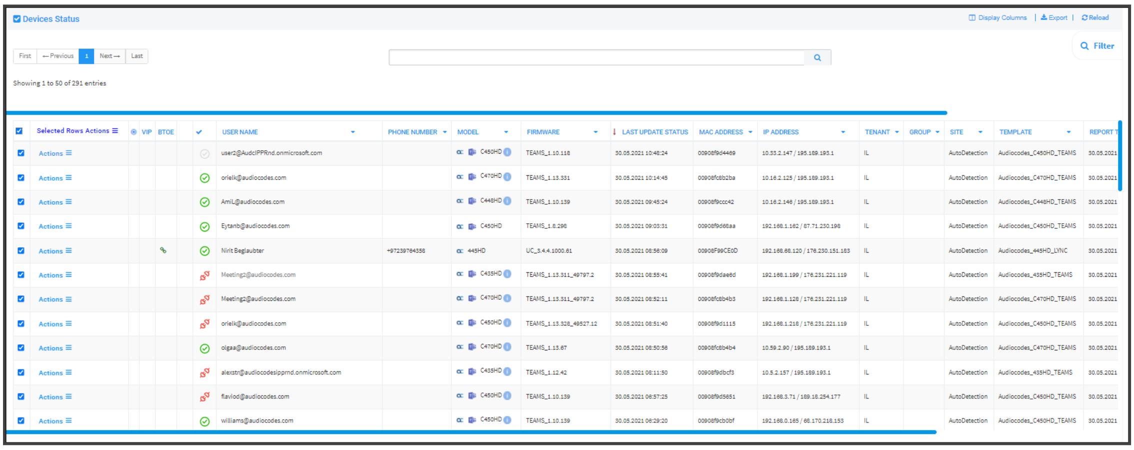
Other columns: User, Phone Number, MAC, IP, Model, Firmware Version, Report Time, Location, Subnet, VLAN ID

Search option

Smart **Filter(s)**

2. Select the upper left checkbox; the **Selected Rows Actions** menu is displayed.

Figure 10-2: Devices Status – Selected Rows Actions - Approve Selected

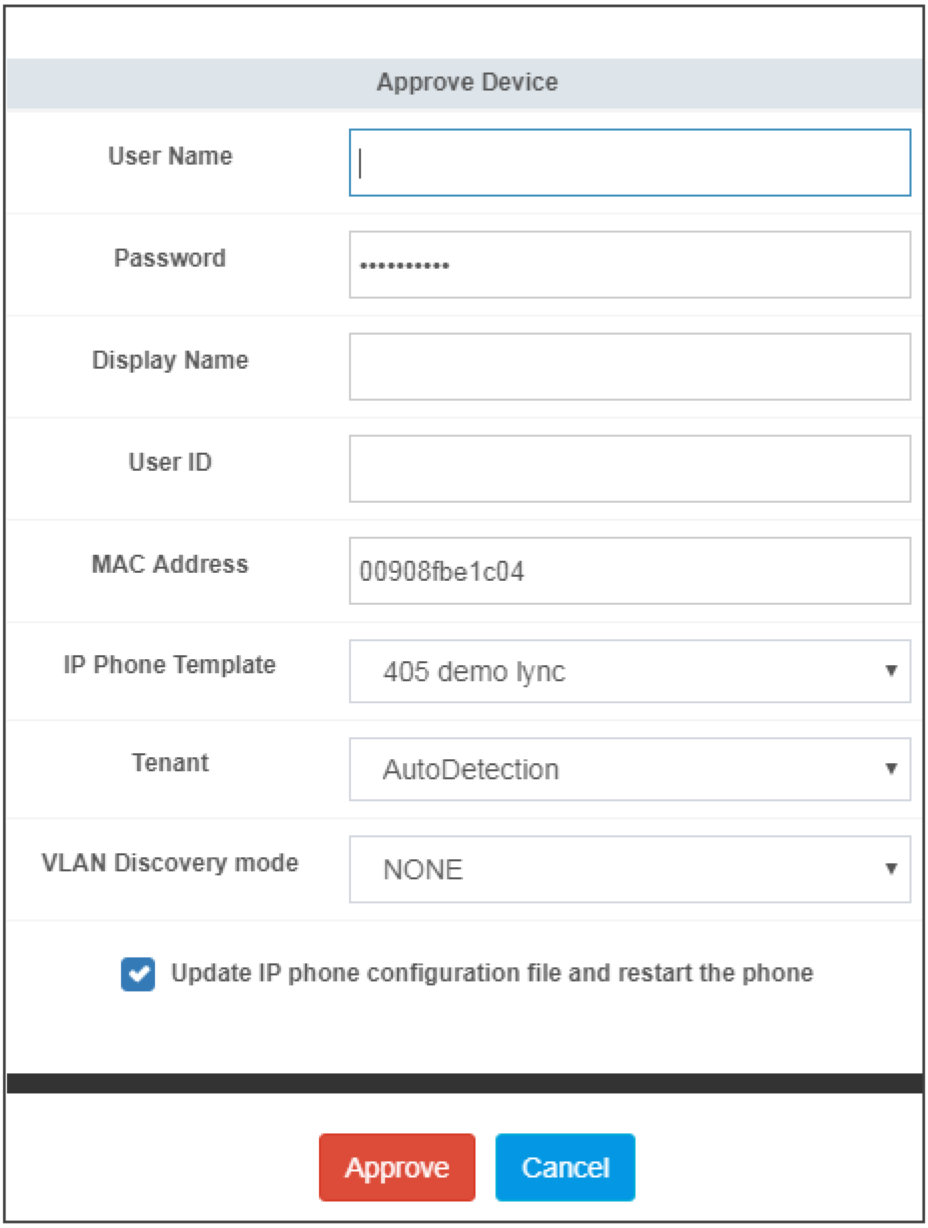


Showing 1 to 50 of 291 entries

☑	Selected Rows Actions ☰		VIP	BTOE		✓	USER NAME	PHONE NUMBER	MODEL	FIRMWARE	LAST UPDATE STATUS	MAC ADDRESS	IP ADDRESS	TENANT	GROUP	SITE	TEMPLATE	REPORT T
☑	Actions ☰					✓	user2@AudcIPPRnd.onmicrosoft.com		C450HD	TEAMS_1.10.118	30.05.2021 10:48:24	00908f9d4469	10.33.2.147 / 195.189.193.1	IL		AutoDetection	Audiocodes_C450HD_TEAMS	30.05.2021
☑	Actions ☰					✓	orielk@audiocodes.com		C470HD	TEAMS_1.13.331	30.05.2021 10:14:45	00908fc8b2ba	10.16.2.125 / 195.189.193.1	IL		AutoDetection	Audiocodes_C470HD_TEAMS	30.05.2021
☑	Actions ☰					✓	AmiL@audiocodes.com		C448HD	TEAMS_1.10.139	30.05.2021 09:45:24	00908f9ccc42	10.16.2.146 / 195.189.193.1	IL		AutoDetection	Audiocodes_C448HD_TEAMS	30.05.2021
☑	Actions ☰					✓	Eytanb@audiocodes.com		C450HD	TEAMS_1.8.298	30.05.2021 09:03:31	00908f9d68aa	192.168.1.162 / 87.71.230.198	IL		AutoDetection	Audiocodes_C450HD_TEAMS	30.05.2021
☑	Actions ☰			🔗		✓	Nirit Beglaubter	+97239764358	445HD	UC_3.4.4.1000.61	30.05.2021 08:56:09	00908F99CE0D	192.168.68.120 / 176.230.151.183	IL		AutoDetection	Audiocodes_445HD_LYNC	30.05.2021
☑	Actions ☰					✗	Meeting2@audiocodes.com		C435HD	TEAMS_1.13.311_49797.2	30.05.2021 08:55:41	00908f9dae6d	192.168.1.199 / 176.231.221.119	IL		AutoDetection	Audiocodes_435HD_TEAMS	30.05.2021
☑	Actions ☰					✗	Meeting2@audiocodes.com		C470HD	TEAMS_1.13.311_49797.2	30.05.2021 08:52:11	00908fc8b4b3	192.168.1.128 / 176.231.221.119	IL		AutoDetection	Audiocodes_C470HD_TEAMS	30.05.2021
☑	Actions ☰					✗	orielk@audiocodes.com		C450HD	TEAMS_1.13.328_49527.12	30.05.2021 08:51:40	00908f9d1115	192.168.1.218 / 176.231.221.119	IL		AutoDetection	Audiocodes_C450HD_TEAMS	30.05.2021
☑	Actions ☰					✓	olgaa@audiocodes.com		C470HD	TEAMS_1.13.67	30.05.2021 08:50:56	00908fc8b4b4	10.59.2.90 / 195.189.193.1	IL		AutoDetection	Audiocodes_C470HD_TEAMS	30.05.2021
☑	Actions ☰					✗	alexstr@audiocodesipprnd.onmicrosoft.com		C435HD	TEAMS_1.12.42	30.05.2021 08:11:50	00908f9dbcf3	10.5.2.157 / 195.189.193.1	IL		AutoDetection	Audiocodes_435HD_TEAMS	30.05.2021
☑	Actions ☰					✗	flaviod@audiocodes.com		C450HD	TEAMS_1.10.139	30.05.2021 06:57:25	00908f9d5651	192.168.3.71 / 189.18.254.177	IL		AutoDetection	Audiocodes_C450HD_TEAMS	30.05.2021
☑	Actions ☰					✓	williams@audiocodes.com		C450HD	TEAMS_1.10.139	30.05.2021 06:29:20	00908f9cb0bf	192.168.0.165 / 68.170.218.153	IL		AutoDetection	Audiocodes_C450HD_TEAMS	30.05.2021

3. (Applies only to SIP devices, not to Teams devices) Click the **Approve Selected** button; you're prompted to approve the selected device/s.

Figure 10-3: Approve Device



Approve Device

User Name	
Password	••••••••••
Display Name	
User ID	
MAC Address	00908fbe1c04
IP Phone Template	405 demo lync ▾
Tenant	AutoDetection ▾
VLAN Discovery mode	NONE ▾

☑ Update IP phone configuration file and restart the phone

4. In the prompt, select the tenant and then click **Approve**; all selected users are approved; all phones restart; the cfg file is automatically uploaded to the phones from the OVOC provisioning server, which the DHCP server points them to.

5. From the 'VLAN Discovery mode' dropdown, select either:

   - **NONE**
   - **Disabled**
   - **Manual Configuration** [of the LAN; static configuration of VLAN ID and priority]
   - **Automatic - CDP** [automatic configuration of the VLAN - VLAN discovery mechanism based on Cisco Discovery Protocol]
   - **Automatic - LLDP** [automatic configuration of VLAN - VLAN discovery mechanism based on LLDP]

- **Automatic - CDP_LLDP** [automatic configuration of VLAN (default) - VLAN discovery mechanism based on LLDP and Cisco Discovery Protocol. LLDP protocol is with higher priority].

Non-Skype for Business Environment

Unlike Skype for Business phones, the network administrator in a non Skype for Business environment needs to log in users phones. The network administrator can do this by importing a csv/zip file with the phones properties, or by approving the phones users one at a time.

> ⚠
> - In contact centers, where multiple users may use a particular phone, a 'user' is sometimes made the equivalent of the Direct Inward Dialing (DID) number associated with the phone.
> - After plugging in phones, the phones report to the Device Manager Pro, which does not display user names whose MAC address are unknown.

➢ To approve users:

1. In the Device Manager Pro, open the Devices Status page (**Monitor** > **Dashboard**); the non Skype for Business screen is identical to the Skype for Business screen.
2. Click **Approve** next to the user; the Approve Device dialog opens – the non Skype for Business screen is identical to the Skype for Business screen.
3. Enter the User Name and the Display Name, and then click **Approve**; the user name is displayed in the Device Manager Pro and the user is approved.

   The User Name and Password will function as the SIP user name and password.

> ⚠
> - This procedure only applies when connecting phones for the first time. After first-time connection, the cfg file - containing user name and password - is automatically uploaded to the phones from the OVOC provisioning server, which the DHCP server points them to.
> - In some non-Skype for Business environments, for example, in Genesys contact centers, Password is not specified.

11 Managing Templates

This topic shows how to manage templates.

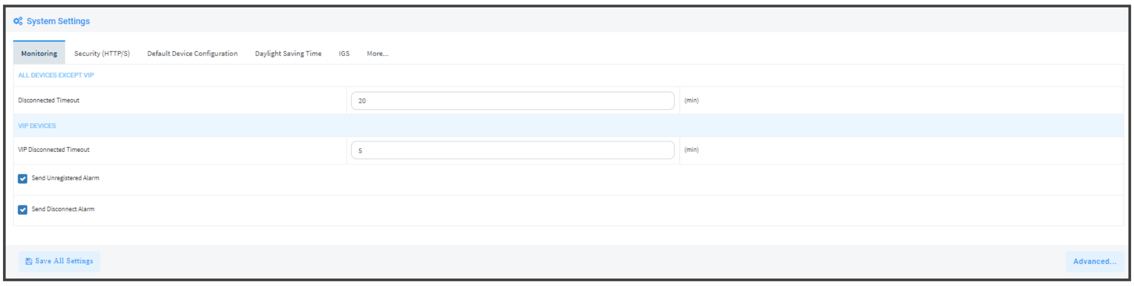
System Settings and Placeholders

The System Settings screen allows you to configure devices according to enterprise requirements. Settings under some tabs also include placeholders so that when you generate a template, the settings values will be applied to the template. Default placeholder values can be viewed in the Default Placeholders Values page.

➢ To configure system settings:

1. Open the System Settings page (**Setup** > **Settings** > **System Settings**).

Figure 11-1: System Settings



ALL DEVICES EXCEPT VIP

Disconnected Timeout 20 (min)

VIP DEVICES

VIP Disconnected Timeout 5 (min)

☑ Send Unregistered Alarm

☑ Send Disconnect Alarm

2. Use the table below as reference.

⚠ The tab **Generic SIP** applies only to enterprises whose environments are non Skype for Business. All other tabs in the screen apply to both Skype for Business and non Skype for Business environments.

Table 11-1: System Settings

Tab/Parameter	Description
Monitoring	
Disconnected Timeout	Determines how long, in minutes, a device's status will be indicated as 'Disconnected' if not reported otherwise. Default: 20 minutes. The phone reports its status to the server every hour. If it does not report its status before 'Disconnect Timeout' lapses, i.e., if the parameter is left at its default and two hours pass without a status report, the status will change from **Registered** to **Disconnected** and the device's 'Status' column in the Devices Status screen will be red-coded.
Send KEEP-ALIVE Every	[Only displayed after clicking **Advanced**] Determines how often, in minutes, a KEEP-ALIVE message is sent from the device.

Tab/Parameter	Description
VIP Disconnected Timeout	Determines how long, in minutes, a VIP device's status will be indicated as 'Disconnected' if not reported otherwise. An alarm can be sent to the network administrator if the timeout is exceeded. Default: 5 minutes. A VIP device is typically a Common Area Phone (CAP) located in the lobby of an enterprise, or a conference phone located in an enterprise's meeting rooms. It's important for a VIP device to be connected, hence the default timeout of 5 minutes compared to the default of 20 minutes for a non VIP device.
VIP Send KEEP-ALIVE Every	[Only displayed after clicking **Advanced**] Determines how often, in minutes, a KEEP-ALIVE message is sent from the VIP device.
Send Unregistered alarm	Select this option for an alarm to be sent when VIP device status changes to 'Unregistered'.
Send Disconnect Alarm	Select this option for an alarm to be sent when VIP device status changes to 'Disconnected'. It's important for a VIP device to be connected, hence the default Disconnected Timeout of 5 minutes compared to the default of 20 minutes for a non VIP device.
Security (HTTP/S)	
Secure (HTTPS) communication from the Device Manager to the Devices	Sends secured (HTTPS) requests from the Device Manager Pro server to the phone. If the option is selected, communications and REST actions such as Restart, Send Message, etc., will be carried out over HTTPS. Not relevant when using an SBC proxy (see Editing the SBC HTTP Proxy on page 30).
Secure (HTTPS) communication from the Devices to the Device Manager	Sends secured (HTTPS) requests from the phone to the Device Manager Pro server. If the option is selected, communications and REST updates such as keep-alive, alarms and statuses between phone and server will be carried out over HTTPS. Also used for loading firmware and configuration files, and when there is an SBC proxy (see Editing the SBC HTTP Proxy on page 30).
Devices Status: Open Device Web Administrator using HTTPS	The browser immediately opens the device's Web interface, over HTTPS, without prompting that there is a problem with the website's security certificate and that it is not recommended to continue to the website.
Only allow devices added by the	Select this option to allow into the OVOC only those phones that were added by the network administrator.

Tab/Parameter	Description
administrator into OVOC	- Phones that were not added by the network administrator will be blocked by the OVOC. - If a device's Mac Address is not listed in the 'Manage Users & Devices' page, it will be blocked by the OVOC. The OVOC must be restarted for the parameter to take effect.
Default Device Configuration	
Server FQDN	[Recommended] Points phones to the OVOC server using the server's name rather than its IP address. If phones are pointed to the OVOC server's IP address, then if the server is moved due to organizational changes within the enterprise, all phones are disconnected from it. Pointing using the server's name prevents this, making organizational changes easier.
Devices Language	From the dropdown select the language you want displayed in the phones' screens: **English** (default), **French**, **German**, **Hebrew**, **Italian**, **Polish**, **Portuguese**, **Russian**, **Spanish** or **Ukraine**.
NTP Server IP Address	Enter the IP address of the Network Time Protocol (NTP) server from which the phones can get the time.
Voice Mail Number	Enter the number of the enterprise's exchange. Configuration depends on the enterprise environment, specifically, on which exchange the enterprise has. If the enterprise has a Skype for Business environment, ignore this parameter. Default=1000.
Require SRTP in the Phone Configuration File	Select this option for *Secure* RTP. Real-time Transport Protocol (RTP) is the standard packet format for delivering voice over IP.
Daylight Saving Time	
Active	Determines whether the phone automatically detects the Daylight Saving Time for the selected Time Zone. - Disable - Enable (default)
Date Format	Configures the date format. Valid values are: - FIXED. Date is specified as: Month, Day of month. - Day of Week. Date is specified as Month, Week of month, Day of week.

Tab/Parameter	Description
Start Time	Defines precisely when to start the daylight saving offset. - month - defines the specific month in the year - week – defines the specific week in the month (first – fourth) - day - defines the specific day in the week - hour - defines the specific hour in the day - minute - defines the specific minute after the hour Configures the precise moment the phone will start daylight savings with a specific offset.
End Time	Defines precisely when to end the daylight saving offset. - month - defines the specific month in the year - week – defines the specific week in the month (first – fourth) - day - defines the specific day in the week - hour - defines the specific hour in the day - minute - defines the specific minute after the hour Configures the precise moment the phone will end daylight savings with a specific offset.
Offset	The offset value for the daylight saving. Range: 0 to 180.
Generic SIP	
Redundant Mode	From the dropdown select **No Redundant** (default) or **Primary/Backup**. Allows the administrator to set the primary PBX / Skype for Business server to which the phone registers and the fallback option if the server is unavailable. Primary/Backup, or 'outbound proxy', is a feature that enables the phone to operate with a primary or backup PBX/Skype for Business server. If the primary falls, the other backs it up.
Primary	Enter the primary PBX/Skype for Business server's IP address, i.e., the outbound proxy's IP address.
HTTP AUTH Provisioning no password	If set to **Enabled**, only the extension number will be used for provisioning HTTP authentication. The default HTTP AUTH password will be **1234**. In DHCP option 160 and on the templates, the setting 'provisioning/configuration/http_auth/password' must be configured to **1234** to activate the feature.

3. Click the **More...** tab and if necessary, in the 'Accept Extensions' field define file extensions you'll require which aren't already defined, then click **Save**.
   - For information about the **LDAP Configuration** button, see Configuring the LDAP Directory on page 94
   - For information about the **SBC Proxy Configuration** button, see Editing the SBC HTTP Proxy on page 30
   - For information about the **Default Placeholders Values** button, see Viewing Default Placeholders Values on page 85
   - For information about the **SCEP** button, see under Adding Users & Devices in Non-Skype for Business Environments on page 8
4. Click **Save All Settings**.

Selecting a Template

Templates are available

- per tenant
- per phone model
- per model for Microsoft Skype for Business phones
- per model for Microsoft Teams phones
- per model for regular (non-Skype for Business) third-party phones

Depending on the tenant, model and the server in the enterprise, select a template for:

- AudioCodes 405
- AudioCodes 420HD
- AudioCodes 430HD
- AudioCodes 440HD
- AudioCodes 450HD
- AudioCodes 420HD Skype for Business
- AudioCodes 430HD Skype for Business
- AudioCodes 440HD Skype for Business
- AudioCodes 450HD Skype for Business
- AudioCodes C435HD Teams
- AudioCodes C448HD Teams
- AudioCodes C450HD Teams
- AudioCodes C455HD Teams
- AudioCodes C470HD Teams

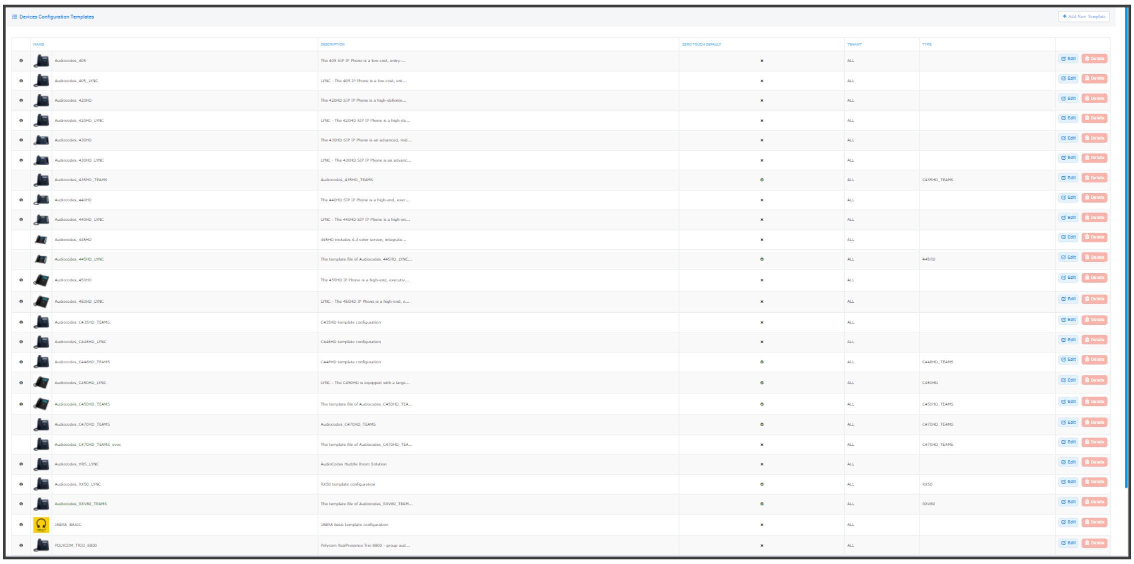
- AudioCodes RXV80 Standalone Video Collaboration Bar for Teams
- AudioCodes RXV90 Meeting Room Solution for Microsoft Teams
- AudioCodes RXV100 Meeting Room Solution for Microsoft Teams
- Jabra
- Poly Trio 8800
- Poly VVX
- Poly CCX 500/600
- Spectralink 8440

> For information on third-party vendor products, see the Device Manager for Third-Party Vendor Products Administrator's Manual

➢ **To select a template:**

- Open the Devices Configuration Templates page (**Setup** > **Configuration** > **Templates**):

Figure 11-2: Devices Configuration Templates



Devices Configuration Templates

+ Add New Template

	NAME	DESCRIPTION	ZERO TOUCH DEFAULT	TENANT	TYPE	
ⓘ	Audiocodes_405	The 405 SIP IP Phone is a low-cost, entry-...	×	ALL		Edit Delete
ⓘ	Audiocodes_405_LYNC	LYNC - The 405 IP Phone is a low-cost, ent...	×	ALL		Edit Delete
ⓘ	Audiocodes_420HD	The 420HD SIP IP Phone is a high-definitio...	×	ALL		Edit Delete
ⓘ	Audiocodes_420HD_LYNC	LYNC - The 420HD SIP IP Phone is a high-de...	×	ALL		Edit Delete
ⓘ	Audiocodes_430HD	The 430HD SIP IP Phone is an advanced, mid...	×	ALL		Edit Delete
ⓘ	Audiocodes_430HD_LYNC	LYNC - The 430HD SIP IP Phone is an advanc...	×	ALL		Edit Delete
	Audiocodes_435HD_TEAMS	Audiocodes_435HD_TEAMS	✓	ALL	C435HD_TEAMS	Edit Delete
ⓘ	Audiocodes_440HD	The 440HD SIP IP Phone is a high-end, exec...	×	ALL		Edit Delete
ⓘ	Audiocodes_440HD_LYNC	LYNC - The 440HD SIP IP Phone is a high-en...	×	ALL		Edit Delete
	Audiocodes_445HD	445HD includes 4.3 color screen, integrate...	×	ALL		Edit Delete
	Audiocodes_445HD_LYNC	The template file of Audiocodes_445HD_LYNC...	✓	ALL	445HD	Edit Delete
ⓘ	Audiocodes_450HD	The 450HD IP Phone is a high-end, executiv...	×	ALL		Edit Delete
ⓘ	Audiocodes_450HD_LYNC	LYNC - The 450HD IP Phone is a high-end, e...	×	ALL		Edit Delete
ⓘ	Audiocodes_C435HD_TEAMS	C435HD template configuration	×	ALL		Edit Delete
ⓘ	Audiocodes_C448HD_LYNC	C448HD template configuration	×	ALL		Edit Delete
ⓘ	Audiocodes_C448HD_TEAMS	C448HD template configuration	✓	ALL	C448HD_TEAMS	Edit Delete
ⓘ	Audiocodes_C450HD_LYNC	LYNC - The C450HD is equipped with a large...	✓	ALL	C450HD	Edit Delete
ⓘ	Audiocodes_C450HD_TEAMS	The template file of Audiocodes_C450HD_TEA...	✓	ALL	C450HD_TEAMS	Edit Delete
	Audiocodes_C470HD_TEAMS	Audiocodes_C470HD_TEAMS	✓	ALL	C470HD_TEAMS	Edit Delete
	Audiocodes_C470HD_TEAMS_ovoc	The template file of Audiocodes_C470HD_TEA...	×	ALL	C470HD_TEAMS	Edit Delete
ⓘ	Audiocodes_HRS_LYNC	AudioCodes Huddle Room Solution	×	ALL		Edit Delete
ⓘ	Audiocodes_RX50_LYNC	RX50 template configuration	✓	ALL	RX50	Edit Delete
ⓘ	Audiocodes_RXV80_TEAMS	The template file of Audiocodes_RXV80_TEAM...	✓	ALL	RXV80	Edit Delete
ⓘ	JABRA_BASIC	JABRA basic template configuration	×	ALL		Edit Delete
ⓘ	POLYCOM_TRIO_8800	Polycom RealPresence Trio 8800 - group aud...	×	ALL		Edit Delete

- Click ⓘ for more information about the phone whose template is displayed.
- Click **Edit** to modify a template.

Editing a Configuration Template

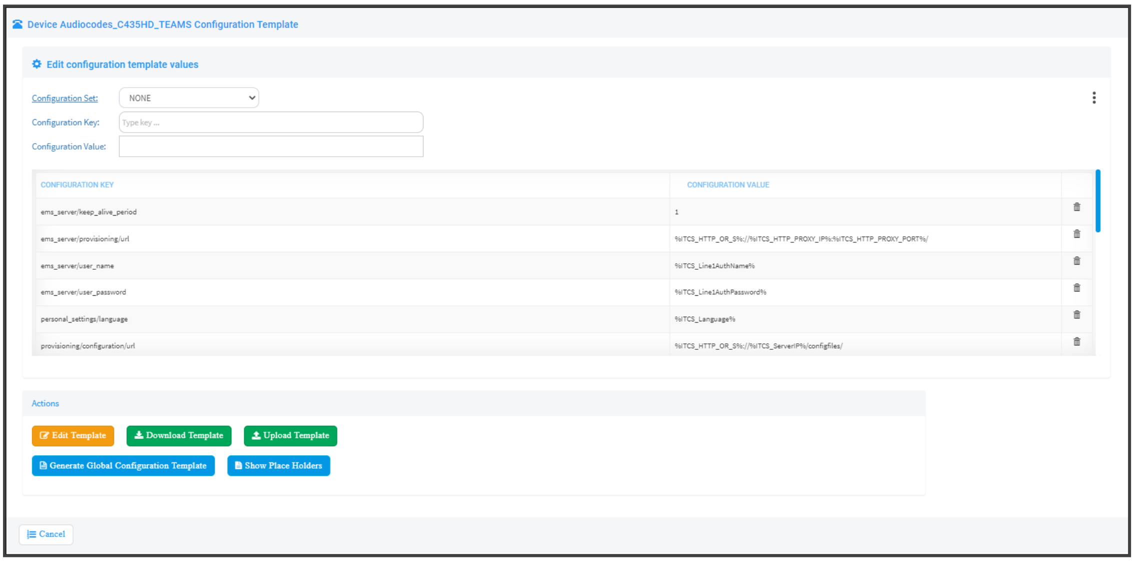
You can edit a device's template but typically it's unnecessary to change it.

> For information on third-party vendor products, see the Device Manager for Third-Party Vendor Products Administrator's Manual

➢ To edit a template:

1. In the Devices Configuration Templates page (**Setup** > **Configuration** > **Templates**), click the link of the device or its **Edit** icon.

Figure 11-3: Device Configuration Template



Device Audiocodes_C435HD_TEAMS Configuration Template

Edit configuration template values

Configuration Set: NONE

Configuration Key: Type key ...

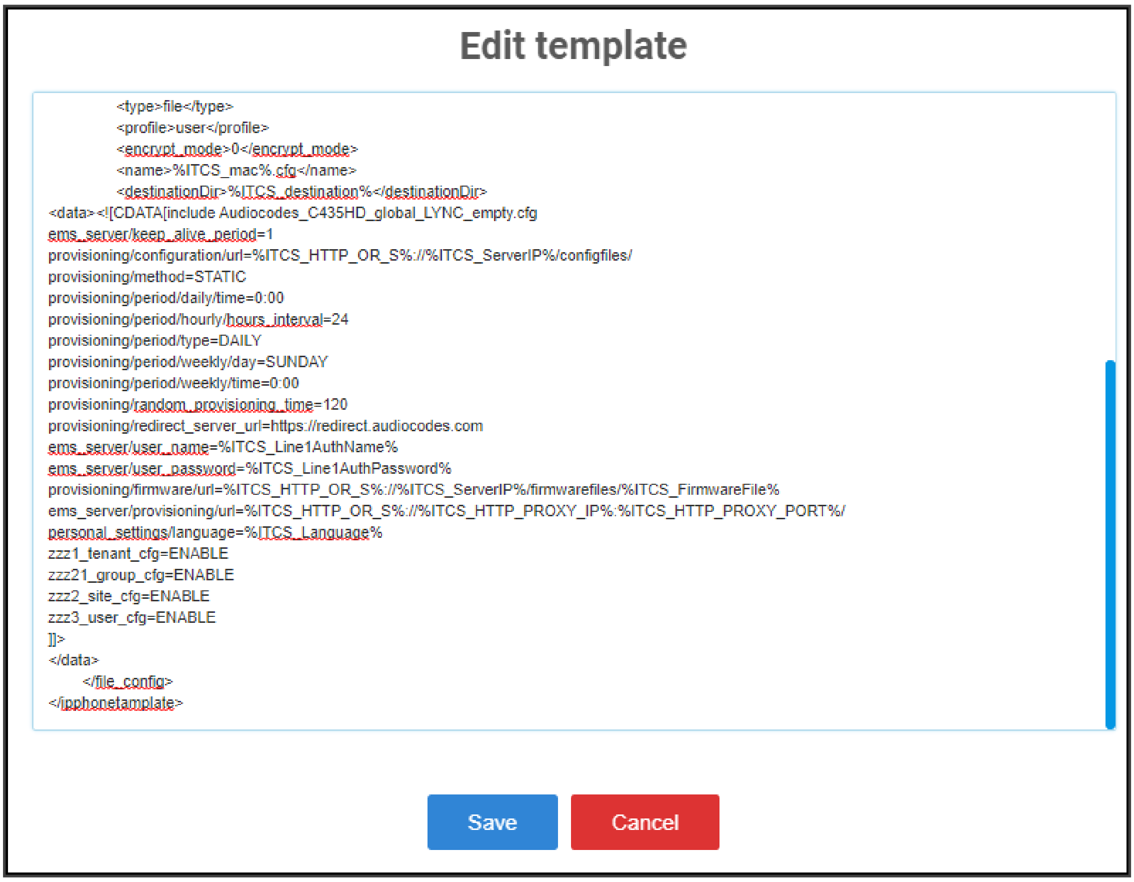
Configuration Value:

CONFIGURATION KEY	CONFIGURATION VALUE
ems_server/keep_alive_period	1
ems_server/provisioning/url	%ITCS_HTTP_OR_S%://%ITCS_HTTP_PROXY_IP%:%ITCS_HTTP_PROXY_PORT%/
ems_server/user_name	%ITCS_Line1AuthName%
ems_server/user_password	%ITCS_Line1AuthPassword%
personal_settings/language	%ITCS_Language%
provisioning/configuration/url	%ITCS_HTTP_OR_S%://%ITCS_ServerIP%/configfiles/

When a new device of model x and tenant y will be connected for the first time to the network, it will use this template.

2. Click the **Edit Template** button; the template opens in an integral editor:

Figure 11-4: Edit Configuration Template



Edit template

```
            <type>file</type>
            <profile>user</profile>
            <encrypt_mode>0</encrypt_mode>
            <name>%ITCS_mac%.cfg</name>
            <destinationDir>%ITCS_destination%</destinationDir>
<data><![CDATA[include Audiocodes_C435HD_global_LYNC_empty.cfg
ems_server/keep_alive_period=1
provisioning/configuration/url=%ITCS_HTTP_OR_S%://%ITCS_ServerIP%/configfiles/
provisioning/method=STATIC
provisioning/period/daily/time=0:00
provisioning/period/hourly/hours_interval=24
provisioning/period/type=DAILY
provisioning/period/weekly/day=SUNDAY
provisioning/period/weekly/time=0:00
provisioning/random_provisioning_time=120
provisioning/redirect_server_url=https://redirect.audiocodes.com
ems_server/user_name=%ITCS_Line1AuthName%
ems_server/user_password=%ITCS_Line1AuthPassword%
provisioning/firmware/url=%ITCS_HTTP_OR_S%://%ITCS_ServerIP%/firmwarefiles/%ITCS_FirmwareFile%
ems_server/provisioning/url=%ITCS_HTTP_OR_S%://%ITCS_HTTP_PROXY_IP%:%ITCS_HTTP_PROXY_PORT%/
personal_settings/language=%ITCS_Language%
zzz1_tenant_cfg=ENABLE
zzz21_group_cfg=ENABLE
zzz2_site_cfg=ENABLE
zzz3_user_cfg=ENABLE
]]>
</data>
     </file_config>
</ipphonetamplate>
```

3. Edit the template and then click **Save**; in the Devices Configuration Templates page, the name of an edited template is displayed in green. See the device's *Administrator's Manual* for parameter descriptions.

About the Template File

The template is an xml file. It defines how a device's configuration file will be generated. The template shows two sections.

- The upper section defines the *global* parameters that will be in the *global* configuration file
- The lower section defines the *private user* parameters that will be in the *device* configuration file

Restoring a Template to the Default

You can restore a template to the factory default at any time.

➢ **To restore a template to the default:**

- Click the **Restore to default** button (displayed only if a change was made); the template and its description are displayed.

Downloading a Template

You can download a template, for example, in order to edit it in a PC-based editor.

➢ **To download a template:**

- Click the **Download configuration template** button and save the *xml* file in a folder on your PC.

Uploading an Edited Template

You can upload a template, for example, after editing it in a PC-based editor.

➢ **To upload an edited template:**

- Click the **Upload configuration template** button and browse to the *xml* template file on your PC. The file will be the new template for the phone model.

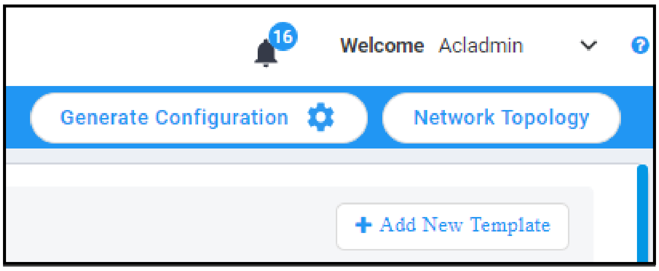
Generating an Edited Template

After editing a template, you must generate the cfg files for the users/devices with whom/which the template is associated.

➢ **To generate an edited template:**

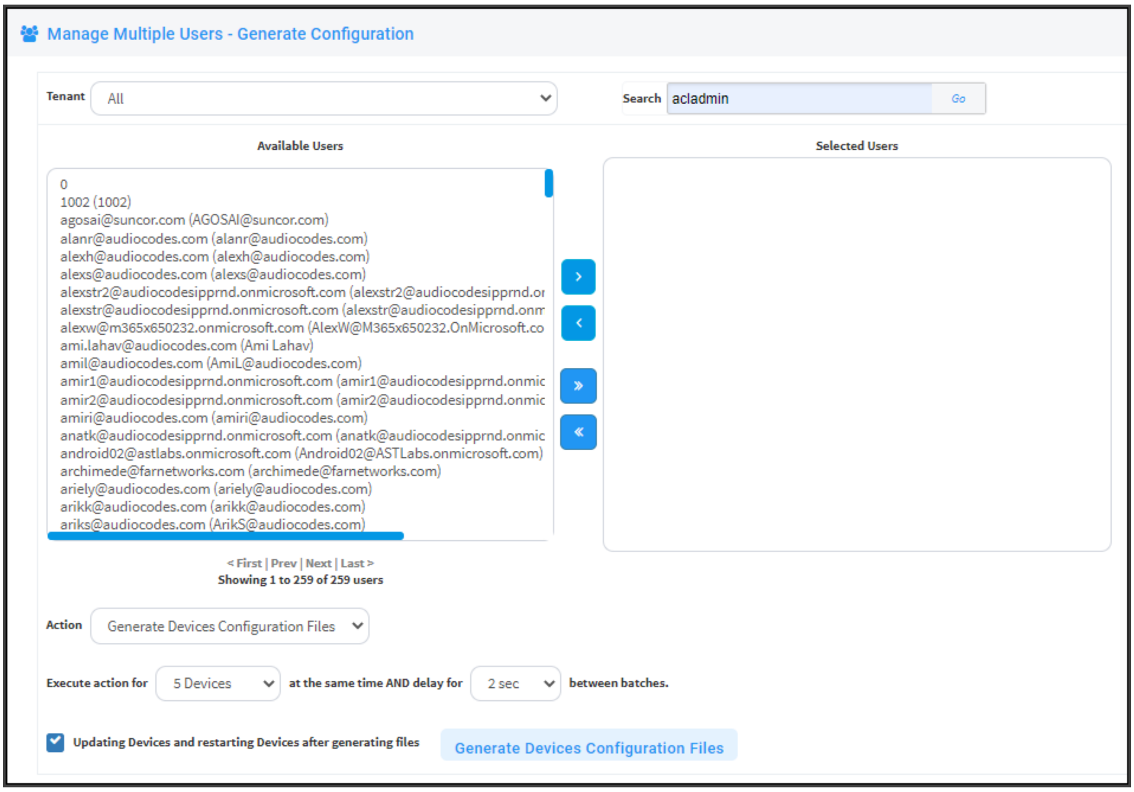
1. Click the **Generate Configuration** link located in the upper right corner of the screen, shown in the figure below.

Figure 11-5: Generate Configuration



2. In the Manage Multiple Users – Generate Configuration screen that opens shown in the figure below, select the relevant users.

Figure 11-6: Manage Multiple Users – Generate Configuration



Manage Multiple Users - Generate Configuration

Tenant: All

Search: acladmin Go

Available Users

0
1002 (1002)
agosai@suncor.com (AGOSAI@suncor.com)
alanr@audiocodes.com (alanr@audiocodes.com)
alexh@audiocodes.com (alexh@audiocodes.com)
alexs@audiocodes.com (alexs@audiocodes.com)
alexstr2@audiocodesipprnd.onmicrosoft.com (alexstr2@audiocodesipprnd.or
alexstr@audiocodesipprnd.onmicrosoft.com (alexstr@audiocodesipprnd.onm
alexw@m365x650232.onmicrosoft.com (AlexW@M365x650232.OnMicrosoft.co
ami.lahav@audiocodes.com (Ami Lahav)
amil@audiocodes.com (AmiL@audiocodes.com)
amir1@audiocodesipprnd.onmicrosoft.com (amir1@audiocodesipprnd.onmic
amir2@audiocodesipprnd.onmicrosoft.com (amir2@audiocodesipprnd.onmic
amiri@audiocodes.com (amiri@audiocodes.com)
anatk@audiocodesipprnd.onmicrosoft.com (anatk@audiocodesipprnd.onmic
android02@astlabs.onmicrosoft.com (Android02@ASTLabs.onmicrosoft.com)
archimede@farnetworks.com (archimede@farnetworks.com)
ariely@audiocodes.com (ariely@audiocodes.com)
arikk@audiocodes.com (arikk@audiocodes.com)
ariks@audiocodes.com (ArikS@audiocodes.com)

Selected Users

< First | Prev | Next | Last >
Showing 1 to 259 of 259 users

Action: Generate Devices Configuration Files

Execute action for 5 Devices at the same time AND delay for 2 sec between batches.

☑ Updating Devices and restarting Devices after generating files

Generate Devices Configuration Files

3. After selecting users, click the **Generate Devices Configuration Files** button

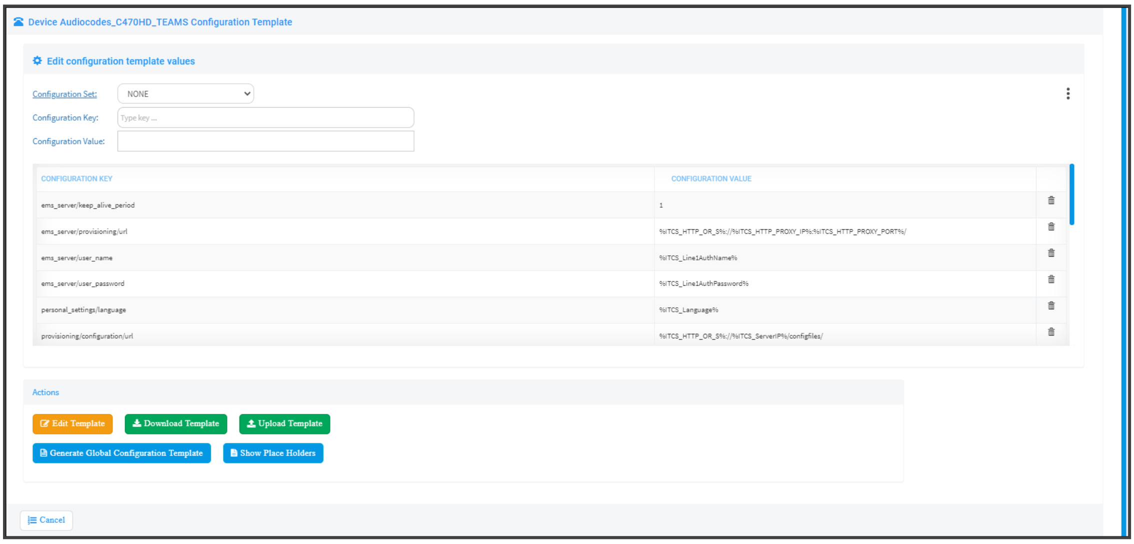
Defining Template Placeholders

Templates include *placeholders* whose values you can define. After defining values, the placeholders are automatically resolved when you generate the template. For example, placeholder **%ITCS_TimeZoneLocation%** is replaced with local time. Placeholders can be defined per tenant, model, etc. The cfg file includes default values and overwritten values according to configured placeholders. If no placeholder is configured, the cfg file will include only default values.

➢ To show placeholders:

1. In the Device Configuration Templates page (**Setup** > **Configuration** > **Templates**), click the **Edit** button in the same row as the device model.

Figure 11-7: Devices Configuration Template



☎ Device Audiocodes_C470HD_TEAMS Configuration Template

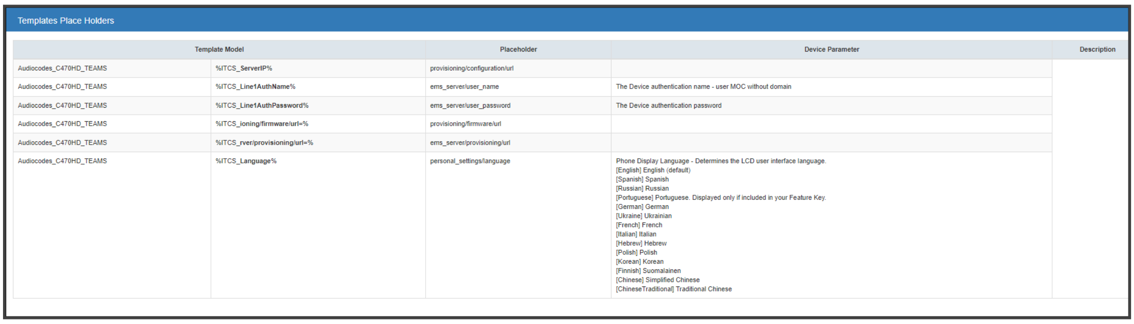
Edit configuration template values

Configuration Set: NONE
Configuration Key: Type key ...
Configuration Value:

CONFIGURATION KEY	CONFIGURATION VALUE	
ems_server/keep_alive_period	1	🗑
ems_server/provisioning/url	%ITCS_HTTP_OR_S%://%ITCS_HTTP_PROXY_IP%:%ITCS_HTTP_PROXY_PORT%/	🗑
ems_server/user_name	%ITCS_Line1AuthName%	🗑
ems_server/user_password	%ITCS_Line1AuthPassword%	🗑
personal_settings/language	%ITCS_Language%	🗑
provisioning/configuration/url	%ITCS_HTTP_OR_S%://%ITCS_ServerIP%/configfiles/	🗑

2. Click the **Show Placeholders** button.

Figure 11-8: Templates Placeholders



Templates Place Holders

Template Model		Placeholder	Device Parameter	Description
Audiocodes_C470HD_TEAMS	%ITCS_ServerIP%	provisioning/configuration/url		
Audiocodes_C470HD_TEAMS	%ITCS_Line1AuthName%	ems_server/user_name	The Device authentication name - user MOC without domain	
Audiocodes_C470HD_TEAMS	%ITCS_Line1AuthPassword%	ems_server/user_password	The Device authentication password	
Audiocodes_C470HD_TEAMS	%ITCS_ioning/firmware/url=%	provisioning/firmware/url		
Audiocodes_C470HD_TEAMS	%ITCS_rver/provisioning/url=%	ems_server/provisioning/url		
Audiocodes_C470HD_TEAMS	%ITCS_Language%	personal_settings/language	Phone Display Language - Determines the LCD user interface language. [English] English (default) [Spanish] Spanish [Russian] Russian [Portuguese] Portuguese. Displayed only if included in your Feature Key. [German] German [Ukraine] Ukrainian [French] French [Italian] Italian [Hebrew] Hebrew [Polish] Polish [Korean] Korean [Finnish] Suomalainen [Chinese] Simplified Chinese [ChineseTraditional] Traditional Chinese	

The figure above shows placeholders currently defined in the xml Configuration Template file for the C470HD Teams phone. There are four kinds of placeholders: (1) System (2) Template (3) Tenant (4) Devices.

- To add/edit/delete a template placeholder, see Adding a New Template Placeholder on page 88 and Adding a New Template Placeholder on page 88
- To add/edit/delete a tenant placeholder, see Adding a New Tenant Placeholder on page 89 and Editing a Configuration Template on page 81.
- To add/edit/delete a device placeholder, see Devices Placeholders on page 92 and Changing a Device Placeholder Value on page 92

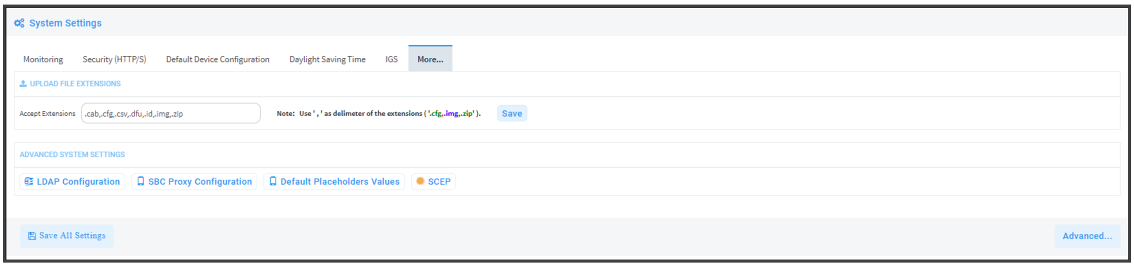
Viewing Default Placeholders Values

Before defining values for placeholders, you can view the default placeholders values.

➢ To view default placeholders values:

1. Open the Default Placeholders Values page (**Setup** > **Settings** > **System Settings** and then click the **More...** option).

Figure 11-9: System Settings - More...

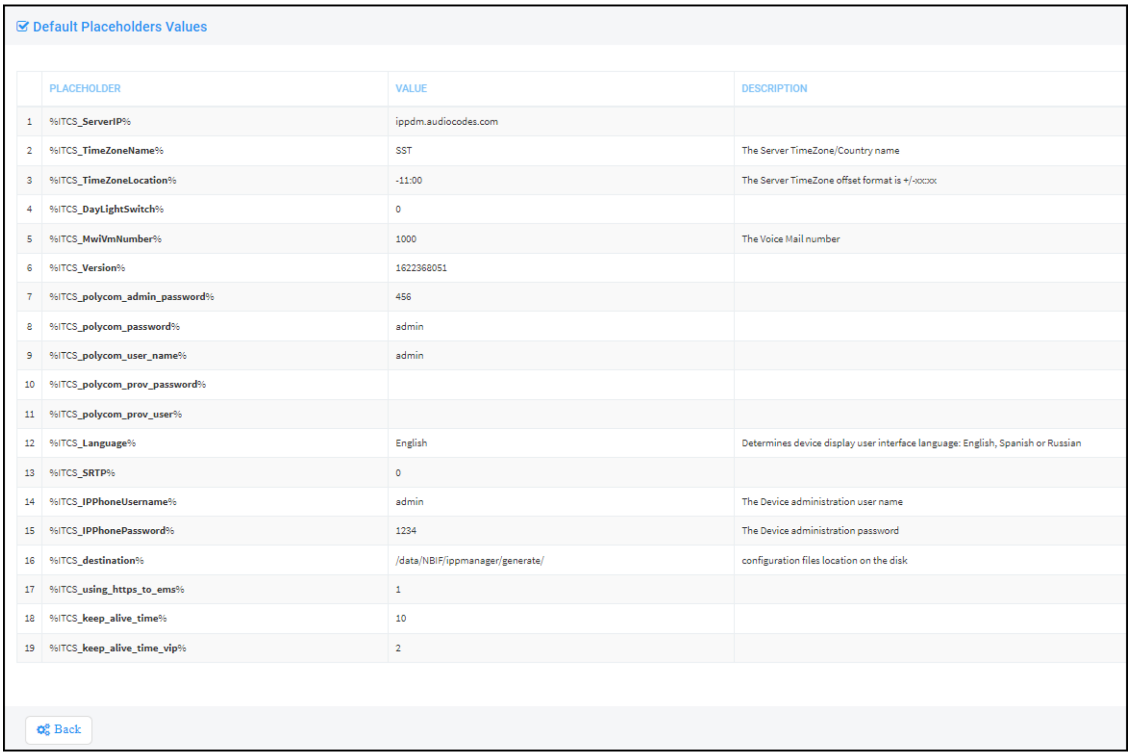


Accept Extensions .cab,.cfg,.csv,.dfu,.id,.img,.zip

Note: Use ' , ' as delimeter of the extensions ('.cfg,.img,.zip').

2. Click the **Default Placeholders Values** button.

Figure 11-10: Default Placeholders Values



	PLACEHOLDER	VALUE	DESCRIPTION
1	%ITCS_**ServerIP**%	ippdm.audiocodes.com	
2	%ITCS_**TimeZoneName**%	SST	The Server TimeZone/Country name
3	%ITCS_**TimeZoneLocation**%	-11:00	The Server TimeZone offset format is +/-xx:xx
4	%ITCS_**DayLightSwitch**%	0	
5	%ITCS_**MwiVmNumber**%	1000	The Voice Mail number
6	%ITCS_**Version**%	1622368051	
7	%ITCS_**polycom_admin_password**%	456	
8	%ITCS_**polycom_password**%	admin	
9	%ITCS_**polycom_user_name**%	admin	
10	%ITCS_**polycom_prov_password**%		
11	%ITCS_**polycom_prov_user**%		
12	%ITCS_**Language**%	English	Determines device display user interface language: English, Spanish or Russian
13	%ITCS_**SRTP**%	0	
14	%ITCS_**IPPhoneUsername**%	admin	The Device administration user name
15	%ITCS_**IPPhonePassword**%	1234	The Device administration password
16	%ITCS_**destination**%	/data/NBIF/ippmanager/generate/	configuration files location on the disk
17	%ITCS_**using_https_to_ems**%	1	
18	%ITCS_**keep_alive_time**%	10	
19	%ITCS_**keep_alive_time_vip**%	2	

Template Placeholders

You can edit the values defined for an existing template placeholder and/or you can add a new template placeholder.

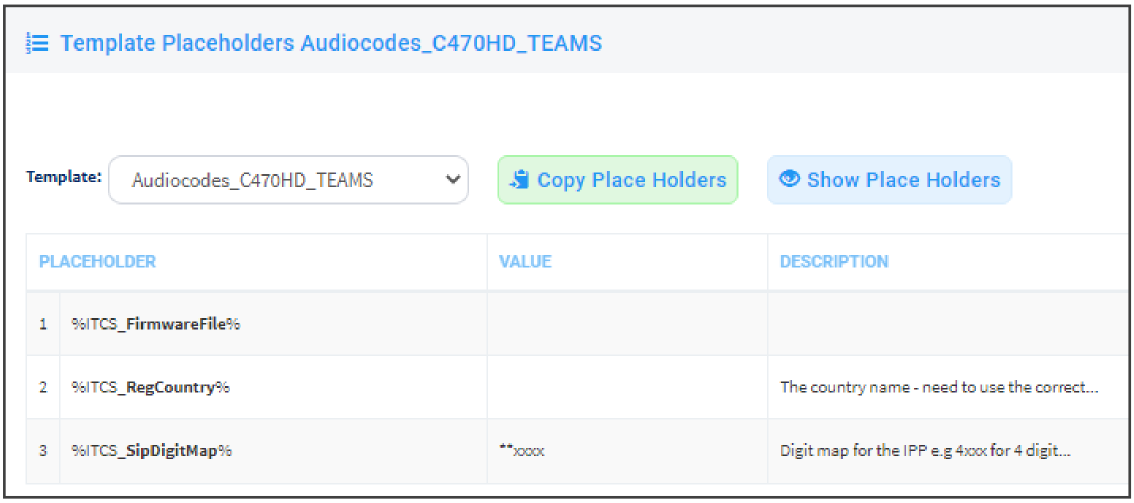
Editing Template Placeholders

You can edit the values for existing template placeholders.

➢ To edit values for existing template placeholders:

- Open the Template Placeholders page (**Setup** > **Configuration** > **Template Placeholders**):

Figure 11-11: Template Placeholders



Template Placeholders Audiocodes_C470HD_TEAMS

Template: Audiocodes_C470HD_TEAMS

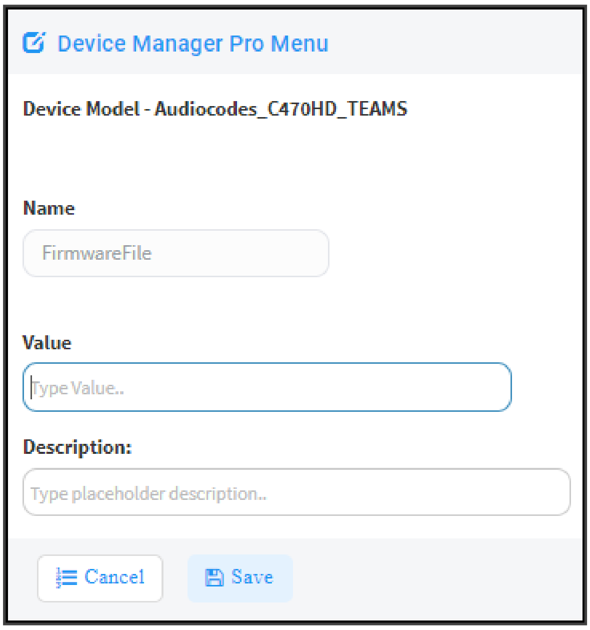
	PLACEHOLDER	VALUE	DESCRIPTION
1	%ITCS_FirmwareFile%		
2	%ITCS_RegCountry%		The country name - need to use the correct...
3	%ITCS_SipDigitMap%	**xxxx	Digit map for the IPP e.g 4xxx for 4 digit...

The page shows the placeholders and their values defined for a template.

➢ To edit a value of an existing template placeholder:

1. Click the adjacent **Edit** button.

Figure 11-12: Edit Template Placeholder



Device Manager Pro Menu

Device Model - Audiocodes_C470HD_TEAMS

Name: FirmwareFile

Value: Type Value..

Description: Type placeholder description..

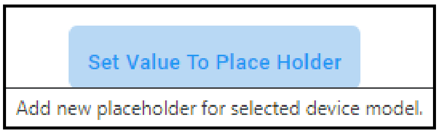
2. In the 'Name' field, you can edit the name of the placeholder.
3. In the 'Value' field, you can edit the value of the placeholder.
4. In the 'Description' field, you can edit the placeholder description.
5. Click **Save**; the edited placeholder is added to the table.

Adding a New Template Placeholder

You can add a new template placeholder. A new placeholder can be added and assigned with a new value.

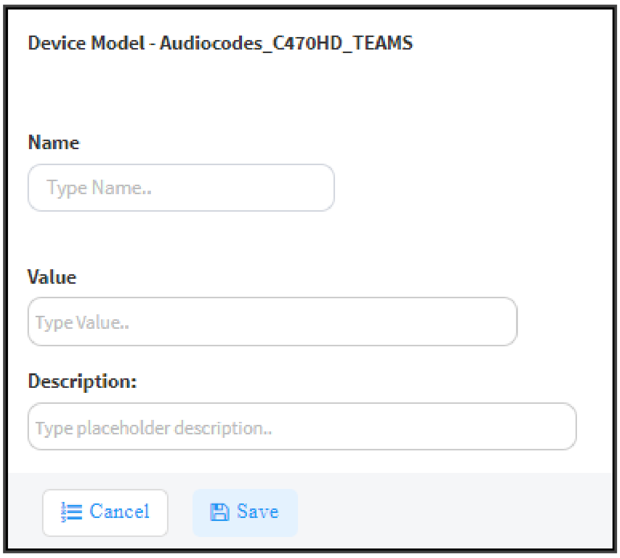
➢ **To add a new template placeholder:**

1. Open the Template Placeholders page (**Setup** > **Configuration** > **Template Placeholders**):
2. From the **Template** dropdown, select the template , e.g., Audiocodes_C470HD_TEAMS.
3. Click the **Set Value to Place Holder** button located in the upper right corner of the screen.



Add new placeholder for selected device model.

Figure 11-13: Add New Template Placeholder


Device Model - Audiocodes_C470HD_TEAMS
Name
Type Name..
Value
Type Value..
Description:
Type placeholder description..
Cancel
Save

4. In the 'Name' field, enter the name of the new placeholder.
5. In the 'Value' field, enter the value of the new placeholder.
6. In the 'Description' field, enter a short description for the new placeholder.
7. Click **Save**; the new placeholder is added to the table.

Tenant Placeholders

You can edit values for existing tenant placeholders and/or add new tenant placeholders.

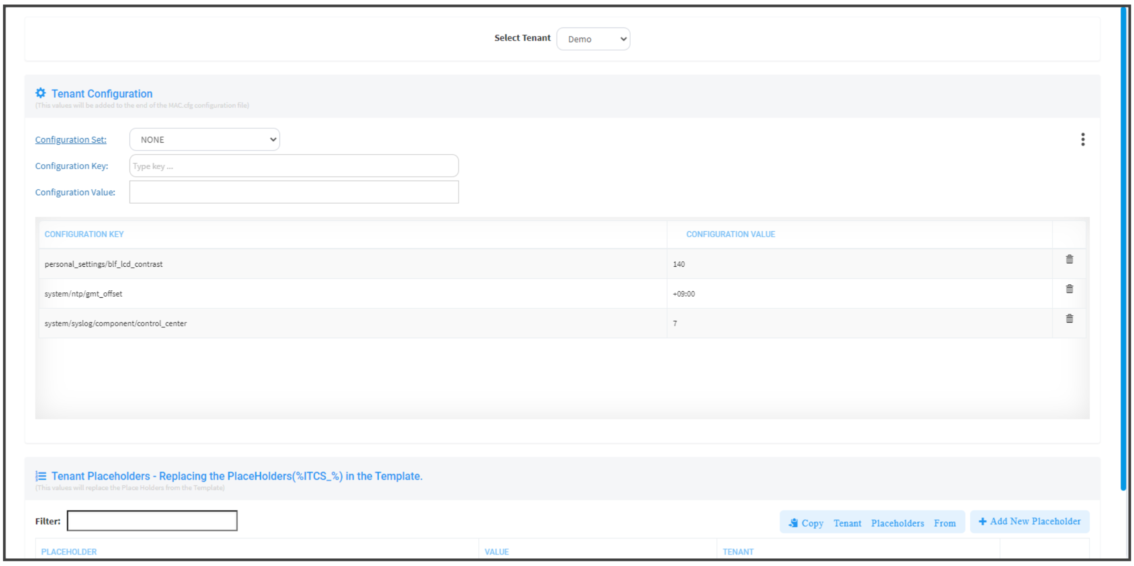
Editing Tenant Placeholders

You can edit the values for existing tenant placeholders.

➢ **To edit values for existing tenant placeholders:**

1. Open the Tenant Configuration page (**Setup** > **Configuration** > **Tenant Configuration**):

Figure 11-14: Tenant Configuration – Tenant Placeholders



Select Tenant: Demo

Tenant Configuration
(This values will be added to the end of the MAC.cfg configuration file)

Configuration Set: NONE
Configuration Key: Type key ...
Configuration Value:

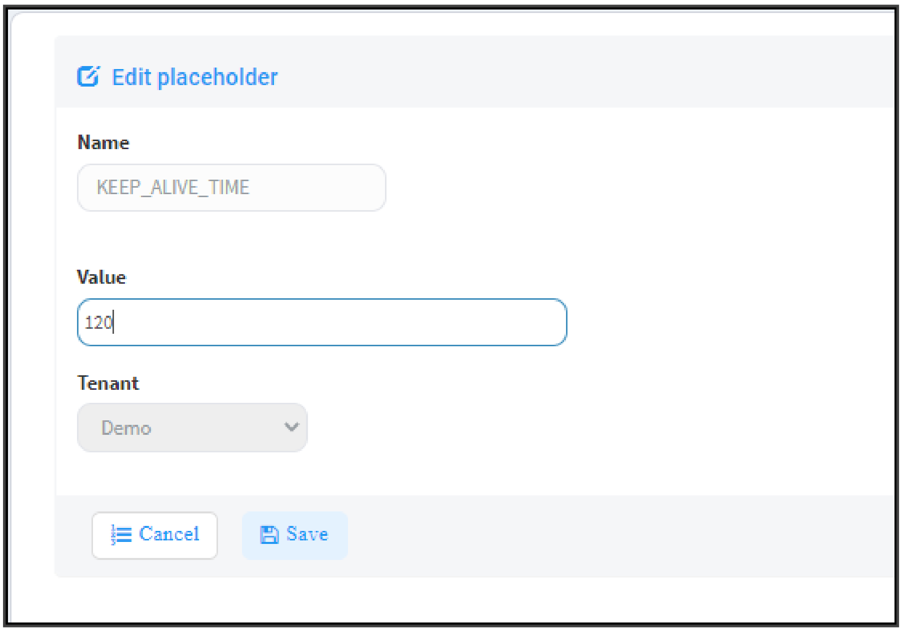
CONFIGURATION KEY	CONFIGURATION VALUE
personal_settings/blf_lcd_contrast	140
system/ntp/gmt_offset	+09:00
system/syslog/component/control_center	7

Tenant Placeholders - Replacing the PlaceHolders(%ITCS_%) in the Template.
(This values will replace the Place Holders from the Template)

Filter:

2. Under the Tenant Placeholders section, select the placeholder and then click the **Edit** button.

Figure 11-15: Edit Placeholder



Edit placeholder

Name: KEEP_ALIVE_TIME

Value: 120

Tenant: Demo

3. In the 'Name' field, you can edit the name of the placeholder.
4. In the 'Value' field, you can edit the value of the placeholder.
5. From the 'Tenant' dropdown, you can select another tenant.
6. Click **Save**; the edited placeholder is added to the table.

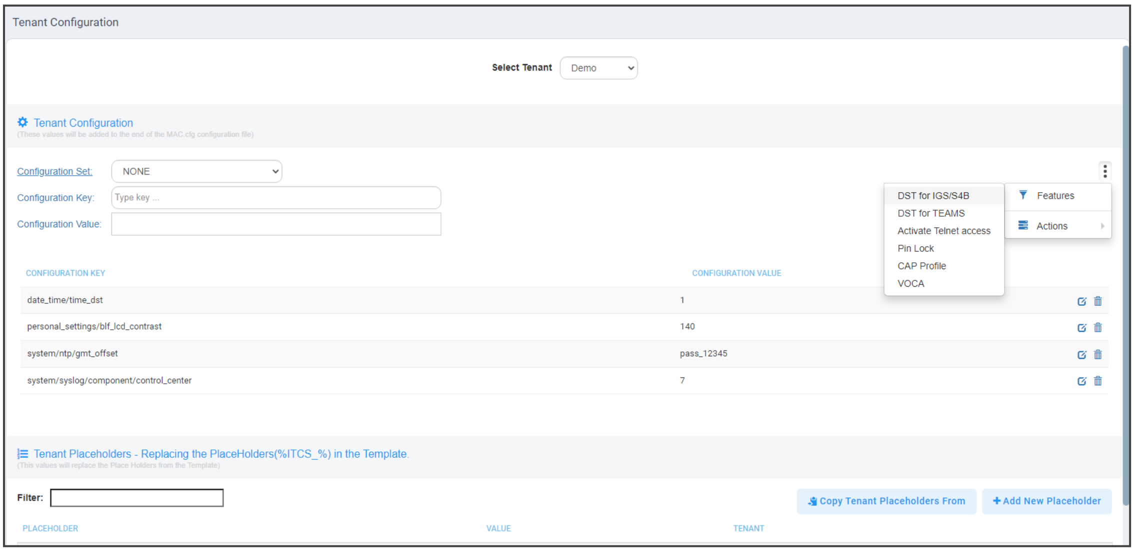
Adding a New Tenant Placeholder

You can add a new tenant placeholder.

➢ To add a new tenant placeholder:

1. Open the Tenant Configuration page (**Setup** > **Configuration** > **Tenant Configuration**).

Figure 11-16: Tenant Configuration



Tenant Configuration

Select Tenant: Demo

Tenant Configuration
(These values will be added to the end of the MAC.cfg configuration file)

Configuration Set: NONE
Configuration Key: Type key ...
Configuration Value:

CONFIGURATION KEY	CONFIGURATION VALUE
date_time/time_dst	1
personal_settings/blf_lcd_contrast	140
system/ntp/gmt_offset	pass_12345
system/syslog/component/control_center	7

Tenant Placeholders - Replacing the PlaceHolders(%ITCS_%) in the Template.
(This values will replace the Place Holders from the Template)

Filter:

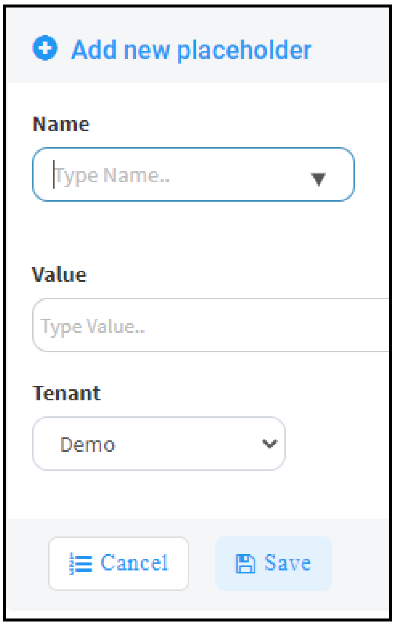
PLACEHOLDER	VALUE	TENANT

2. Under Tenant Configuration, provision devices using the 'Configuration Set' parameter and the corresponding 'Configuration Key' and 'Configuration Value' parameters that are auto-populated after selecting a device model.

   - On the right side of the page, click the vertical ellipsis ⋮ and from the menu that pops up shown in the preceding figure, select **DST for IGS/SFB** or **DST for Teams** and then select **AUTO**, **ENABLE** or **DISABLE**. This menu provides a quick and friendly way to configure Daylight Saving Time (DST) for Generic SIP / Skype for Business phones and for Native Teams phones.

3. Under the lowermost Tenant Placeholders section of the page, click the **+Add New Placeholder** button.

Figure 11-17: Add New Placeholder



Add new placeholder

Name: Type Name..

Value: Type Value..

Tenant: Demo

4. In the 'Name' field, enter / select the name of the new placeholder.

5. In the 'Value' field, enter the value of the new placeholder.

6. From the 'Tenant' dropdown, select a new tenant.

7. Click **Save**; the new placeholder is added to the table.

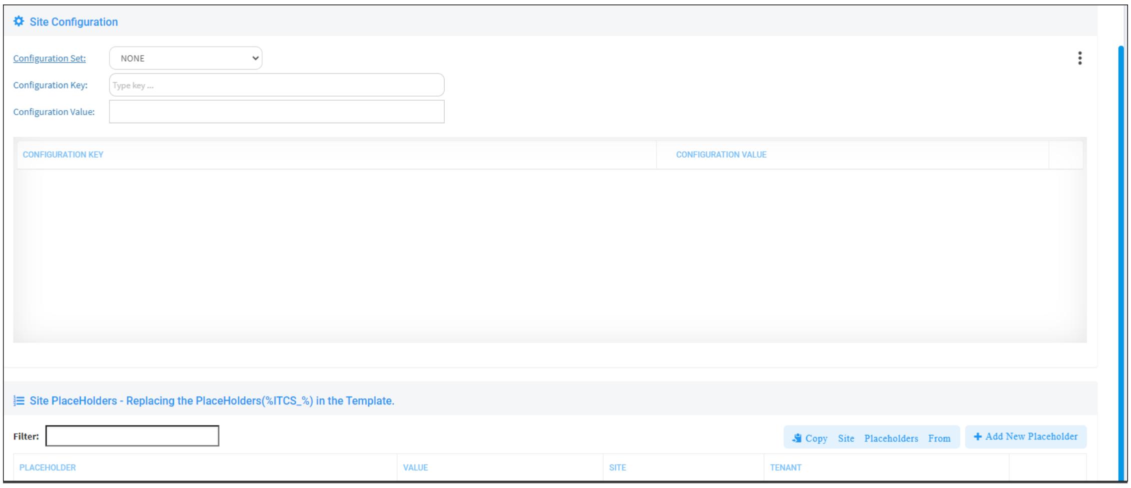
Adding a New Site Placeholder

You can add a new site placeholder.

➢ To add a new site placeholder:

1. Open the Site Configuration page (**Setup** > **Configuration** > **Site Configuration**).

Figure 11-18: Site Configuration



Configuration Set: NONE

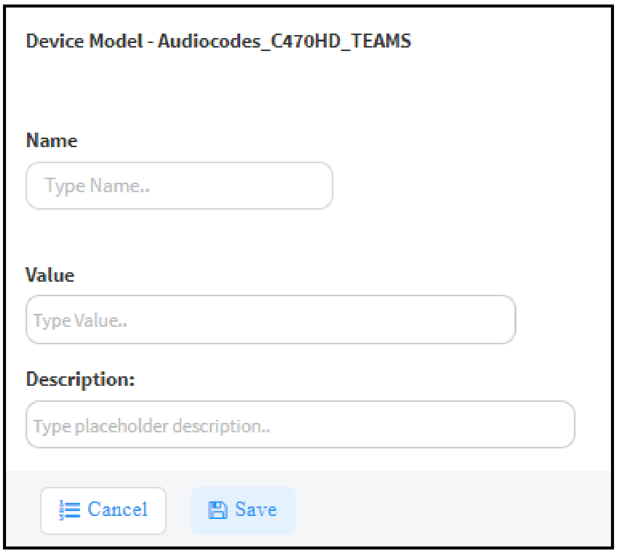
Configuration Key: Type key ...

Configuration Value:

2. Under Site Configuration, provision devices using the 'Configuration Set' parameter and the corresponding 'Configuration Key' and 'Configuration Value' parameters that are auto-populated after selecting a device model.

3. Under the Site Placeholders section of the page, click the **+Add new placeholder** button.

Figure 11-19: Add New Placeholder



Device Model - Audiocodes_C470HD_TEAMS

Name

Type Name..

Value

Type Value..

Description:

Type placeholder description..

4. From the 'Name' field drop-down, select the name of the new placeholder.
5. In the 'Value' field, enter the value of the new placeholder.
6. From the 'Site' drop-down, select a site to which the phone will automatically be provisioned.

> ⚠ Prior to version 7.8, Poly phones could only be provisioned to 'AutoDetection' by default. As of version 7.8, the 'Site' drop-down allows selecting a site to which Poly phones will also be automatically provisioned.

7. Click **Save**; the new placeholder is added to the table.

Devices Placeholders

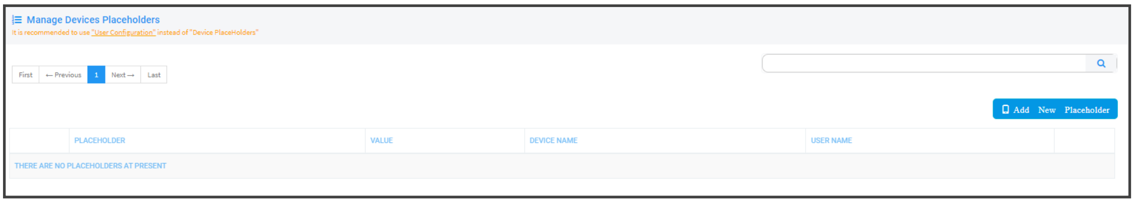
You can change placeholders values for specific phones, for example, you can change placeholders values for the CEO's phone. You can also edit a device's placeholders values.

Changing a Device Placeholder Value

➢ **To change a device placeholder value:**

1. Open the Manage Devices Placeholders page (**Setup** > **Configuration** > **Devices Placeholders**):

Figure 11-20: Manage Devices Placeholders



Manage Devices Placeholders

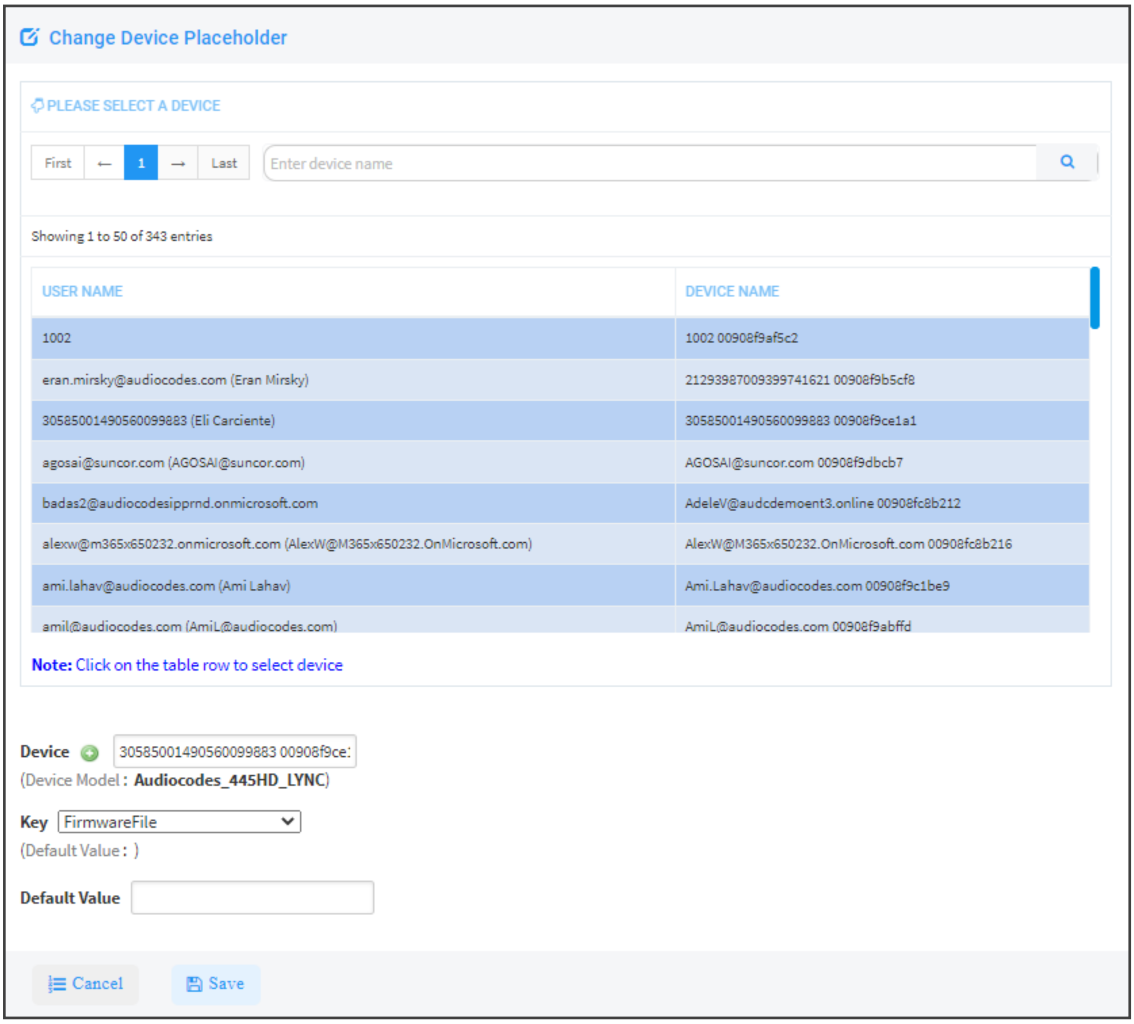
It is recommended to use "User Configuration" instead of "Device PlaceHolders"

	PLACEHOLDER	VALUE	DEVICE NAME	USER NAME	
THERE ARE NO PLACEHOLDERS AT PRESENT					

Use the 'Filter' field to quickly find a specific device if many are listed. You can search for a device by its name or by its extension

2. Select the device whose placeholder value you want to change and click **Edit**.

Figure 11-21: Change Device Placeholder



Change Device Placeholder

PLEASE SELECT A DEVICE

Showing 1 to 50 of 343 entries

USER NAME	DEVICE NAME
1002	1002 00908f9af5c2
eran.mirsky@audiocodes.com (Eran Mirsky)	21293987009399741621 00908f9b5cf8
30585001490560099883 (Eli Carciente)	30585001490560099883 00908f9ce1a1
agosai@suncor.com (AGOSAI@suncor.com)	AGOSAI@suncor.com 00908f9dbcb7
badas2@audiocodesipprnd.onmicrosoft.com	AdeleV@audcdemoent3.online 00908fc8b212
alexw@m365x650232.onmicrosoft.com (AlexW@M365x650232.OnMicrosoft.com)	AlexW@M365x650232.OnMicrosoft.com 00908fc8b216
ami.lahav@audiocodes.com (Ami Lahav)	Ami.Lahav@audiocodes.com 00908f9c1be9
amil@audiocodes.com (AmiL@audiocodes.com)	AmiL@audiocodes.com 00908f9abffd

Note: Click on the table row to select device

Device 30585001490560099883 00908f9ce:
(Device Model : **Audiocodes_445HD_LYNC**)

Key FirmwareFile
(Default Value :)

Default Value

3. Make sure the correct device is selected; the read-only 'Device' field is filled.

4. From the **Key** dropdown, choose the phone configuration key.

5. Enter the device's default value in the 'Default Value' field, and then click **Save**; the edited device placeholder is added to the table.

⚠ The new default value is not automatically generated in the device's configuration file. To generate it, choose the relevant device and then click the **Generate Configuration** link located in the upper left corner of the page.

12 Configuring the LDAP Directory

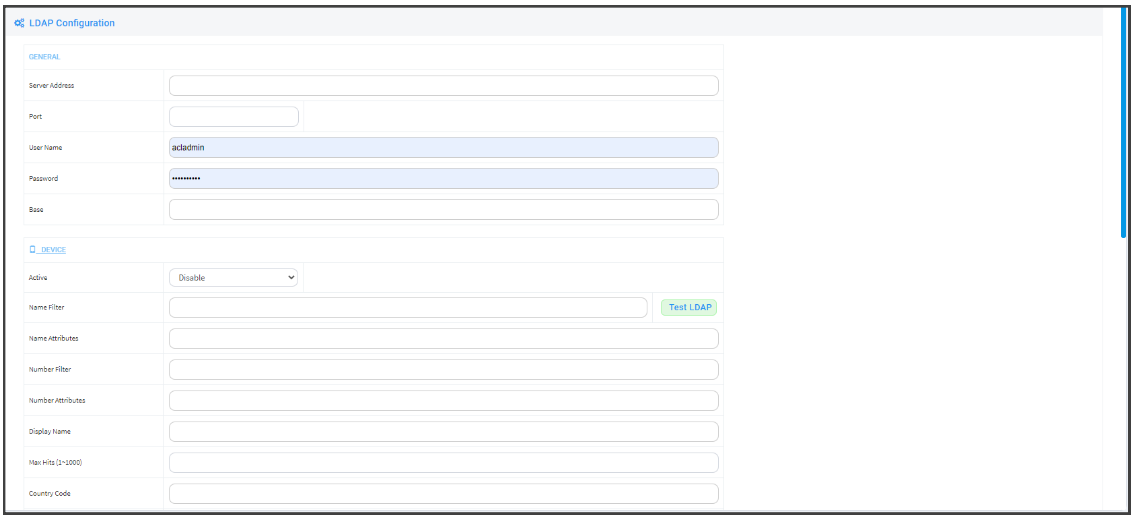
⚠ This section is inapplicable if you're operating in a Microsoft Skype for Business environment because Skype for Business uses its own Active Directory server.

The Device Manager Pro lets you configure an enterprise's LDAP directory.

➢ To access the LDAP directory:

1. Open the System Settings page (**Setup** > **Settings** > **System Settings**).
2. Click **More...** and then click the **LDAP Configuration** button that is then displayed.

Figure 12-1: LDAP Configuration



LDAP Configuration

GENERAL

Server Address	
Port	
User Name	acladmin
Password	••••••••••
Base	

DEVICE

Active	Disable
Name Filter	
Name Attributes	
Number Filter	
Number Attributes	
Display Name	
Max Hits (1~1000)	
Country Code	

3. From the 'Active' parameter dropdown, select **Enable**.
4. Configure the parameters using the table below as reference.

Table 12-1: LDAP Configuration

Parameter	Description
Server address	Enter the IP address, or URL, of the LDAP server.
Port	Enter the LDAP service port.
User Name	Enter the user name used for the LDAP search request.
Password	Enter the password of the search requester.
Base	Enter the access point on the LDAP tree.
Active	From the dropdown, select **Disable** LDAP (default) or **Enable** LDAP. If

Parameter	Description
	Enable is selected, the parameters below are displayed.
Name Filter	Specify your search pattern for name look ups. For example, when you type in the *(&(telephoneNumber=*)(sn=%))* field*,* the search result includes all LDAP records which have the 'telephoneNumber' field set, and the '(“sn”-->surname)' field starting with the entered prefix. When you type in the *(|(cn=%)(sn=%))* field*,* the search result includes all LDAP records which have the '(“cn”-->CommonName)' OR the '(“sn”-->Surname)' field starting with the entered prefix. When you type in the *(!(cn=%))* field*,* the search result includes all LDAP records which “do not” have the 'cn' field starting with the entered prefix.
Name Attributes	Specifies the LDAP name attributes setting, which can be used to specify the “name” attributes of each record which is returned in the LDAP search results. When you type in the following field, for example, *cn sn displayName*”, this requires you to specify 'cn-->commonName'. This is the Full name of the user, sn-->Surname, last name or family name and “displayName” fields for each LDAP record.
Number Filter	Specifies your search pattern for number look ups. When you type in the following field, for example, *(|(telephoneNumber=%)(Mobile=%)(ipPhone=%))*, the search result is all LDAP records which have the “telephoneNumber” OR “Mobile” OR “ipPhone”field match the number being searched. When you type in the *(&(telephoneNumber=%)(sn=*))* field, the search result is all LDAP records which have the 'sn' field set and the “telephoneNumber” match the number being searched.
Number Attributes	Specifies the LDAP number attributes setting, which can be used to specify the “number” attributes of each record which is returned in the LDAP search results. When you type in the following field, for example, *Mobile telephoneNumber ipPhone*, you must specify 'Mobile', 'telephoneNumber' and 'ipPhone' fields for each LDAP record.
Display Name	Specifies the format in which the “name, e.g. “Mike Black” of each returned search result is displayed on the IPPHONE. When you type in the following field, for example, %sn, %givenName, the displayed result returned should be “Black, Mike”.
Max Hits (1~1000)	Specifies the maximum number of entries expected to be sent by the LDAP server (this parameter is sent to the LDAP server).
Country	Defines the country code prefix added for number search.

Parameter	Description
Code	
Area Code	Defines the area code prefix added for number search.
Sort Result	Sorts the search result by display name on the client side.
Search Timeout	The timeout value (in seconds) for LDAP search (sent to the LDAP server).
Call Lookup	Defines the user name used for the LDAP search request.

5. Click **Save**.

13 Managing Device Manager Agents

⚠ Network administrators can skip this documentation. Configuring Agents is no longer necessary with AudioCodes' new Microsoft Teams devices and Jabra devices. They don't require this feature. They pass through a NAT without requiring Agents.

An Agent enables devices located behind a NAT | Firewall in a local enterprise network to be managed from a global cloud network. The application allows the Device Manager to send actions directly to devices. Deployed on an enterprise's premises, the Agent opens a communications channel with the Device Manager located in the global cloud network. The Device Manager is then able to send commands to devices in the local network.

The Device Manager consequently allows

- Internet Telephony Service Providers (ITSPs) to remotely manage devices in enterprise customer networks, through cloud services
- Software as a Service (SaaS) by a centralized hosting business
- Enterprise network administrators to manage devices located within their own network

⚠ For information on how to install and configure a Device Manager Agent, see the *Device Manager Agent Installation and Configuration Guide*. See this same guide for more detailed descriptive information about the Device Manager Agent.

Enabling Device Manager to Support Agents

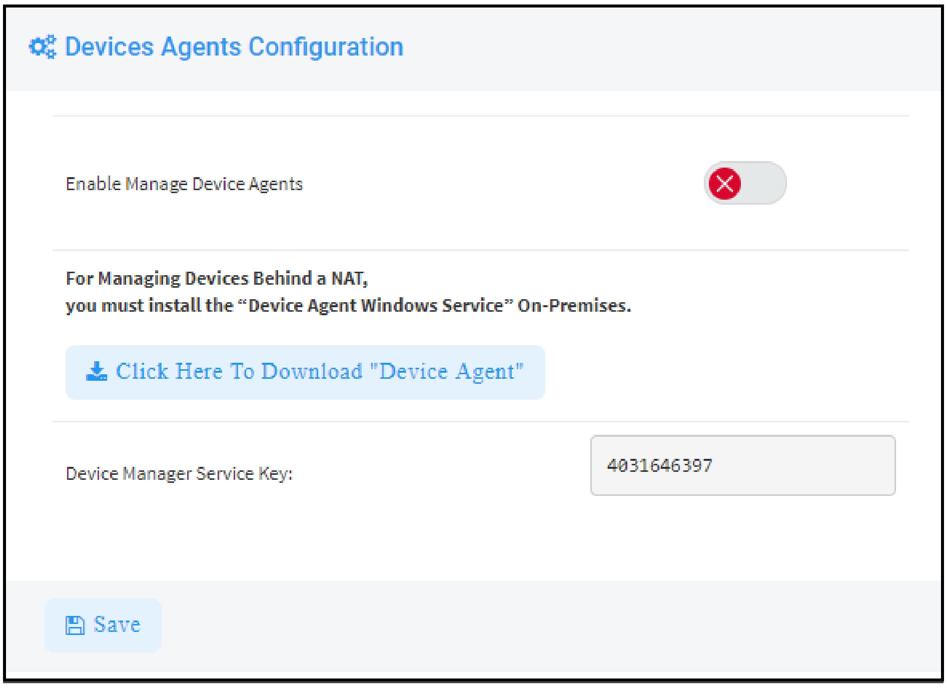
Network administrators must enable the Device Manager to support Agents.

⚠ Network administrators can skip this documentation. Configuring Agents is no longer necessary with AudioCodes' new Microsoft Teams devices and Jabra devices. They don't require this feature. They pass through a NAT without requiring Agents.

➢ **To enable the Device Manager to support Agents:**

1. In the Device Manager, open the Devices Agents Configuration page (**Setup** > **System** > **Devices Agents**).

Figure 13-1: Enabling Manager Device to Support Agents



Devices Agents Configuration

Enable Manage Device Agents ☒

For Managing Devices Behind a NAT,
you must install the "Device Agent Windows Service" On-Premises.

Click Here To Download "Device Agent"

Device Manager Service Key: 4031646397

Save

2. Drag the **Enable Manager Device Agents** slider to the 'on' position.

3. Click **Save**.

4. Make sure the icon ⚙ is displayed in the uppermost right corner of the Device Manager GUI.

5. If it isn't displayed, log out and log in again.

Monitoring Device Manager Agents

⚠ Network administrators can skip this documentation. Configuring Agents is no longer necessary with AudioCodes' new Microsoft Teams devices and Jabra devices. They don't require this feature. They pass through a NAT without requiring Agents.

The Device Manager allows network administrators to view a list of Device Manager Agents registered in the deployment, as well as view the last action each Agent performed for its devices.

➢ To monitor Agents:

1. In the Device Agents Configuration page (**Setup** > **System** > **Device Agents**), click the ⊙ Monitor Device Agents button or click the icon ⚙ displayed in the uppermost right corner of the page.

2. In the Devices Agents Status page that opens, view the list of Devices Agents Status registered in the deployment and view the last action each Agent performed for its devices.

13 Converting a Phone to a Microsoft Teams Phone

Microsoft's SIP Gateway allows users with AudioCodes' phones to convert them to Microsoft Teams phones using the Device Manager to make the conversion.

> For information on how to configure the Microsoft SIP Gateway, see here.

AudioCodes phone models that can be converted to Teams phones are: 405, 405HD, 420HD, 440HD, 445HD, 450HD and C450HD. (Version 3.4.4.1000.61 and later is supported for the 445HD, 450HD and C450HD models).

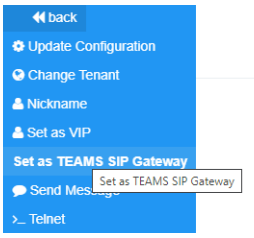
After adding Microsoft's SIP Gateway to an enterprise's IP telephony network, users can connect these non Teams-certified AudioCodes phone models to the Microsoft telephony environment and reuse / re-purpose them with the Microsoft Teams cloud telephony service.

> The phones must be running MPP (multi-party platform) firmware / software. If connecting a phone to on-premise, you'll need to get the MPP firmware which you'll need to connect to WebEx. Once you run the MPP software, then you can connect to Teams.

➢ To convert an AudioCodes phone model to a Teams phone:

1. Define the SIP Gateway URL as shown in Configuring Microsoft Teams SIP Gateway URL below for SIP Gateway - Device Manager connectivity.
2. In the Monitor page, click the **Actions** link adjacent to the phone to convert and then in the menu that opens click **More...**

Figure 13-2: Actions - More



3. Click the **Set as TEAMS SIP Gateway** option.

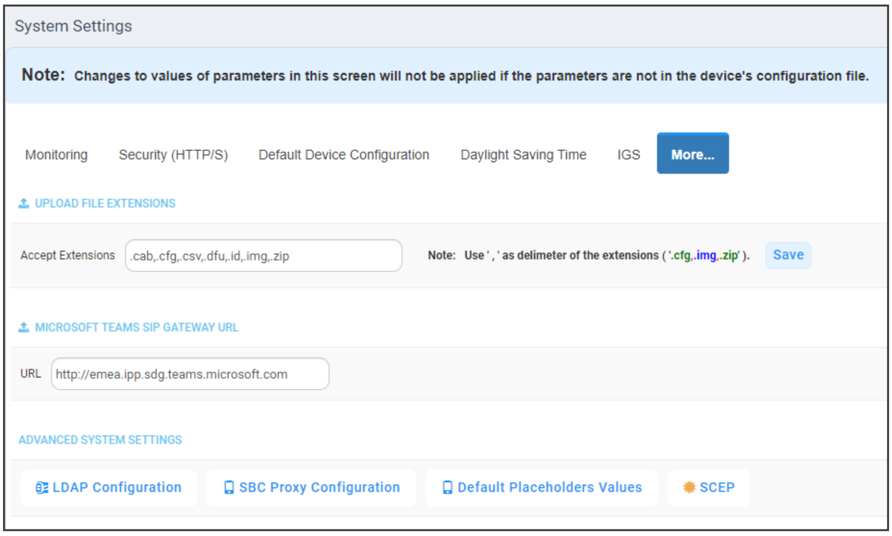
Configuring Microsoft Teams SIP Gateway URL

Network administrators must configure the Microsoft SIP Gateway URL for SIP Gateway - Device Manager connectivity.

➢ To configure the Microsoft SIP Gateway URL:

1. In the Device Manager, open the System Settings page (**Setup** > **Settings** > **System Settings**) and then click the **More...** tab.

Figure 13-3: System Settings page


System Settings

Note: Changes to values of parameters in this screen will not be applied if the parameters are not in the device's configuration file.

UPLOAD FILE EXTENSIONS

Accept Extensions: .cab,.cfg,.csv,.dfu,.id,.img,.zip

Note: Use ' , ' as delimeter of the extensions ('.cfg,.img,.zip').

MICROSOFT TEAMS SIP GATEWAY URL

URL: http://emea.ipp.sdg.teams.microsoft.com

ADVANCED SYSTEM SETTINGS

2. In the 'Microsoft Teams SIP Gateway URL' field shown in the preceding figure, enter the Microsoft SIP Gateway's URL and then click **Save all Settings** in the lowermost right corner (not shown in the figure).

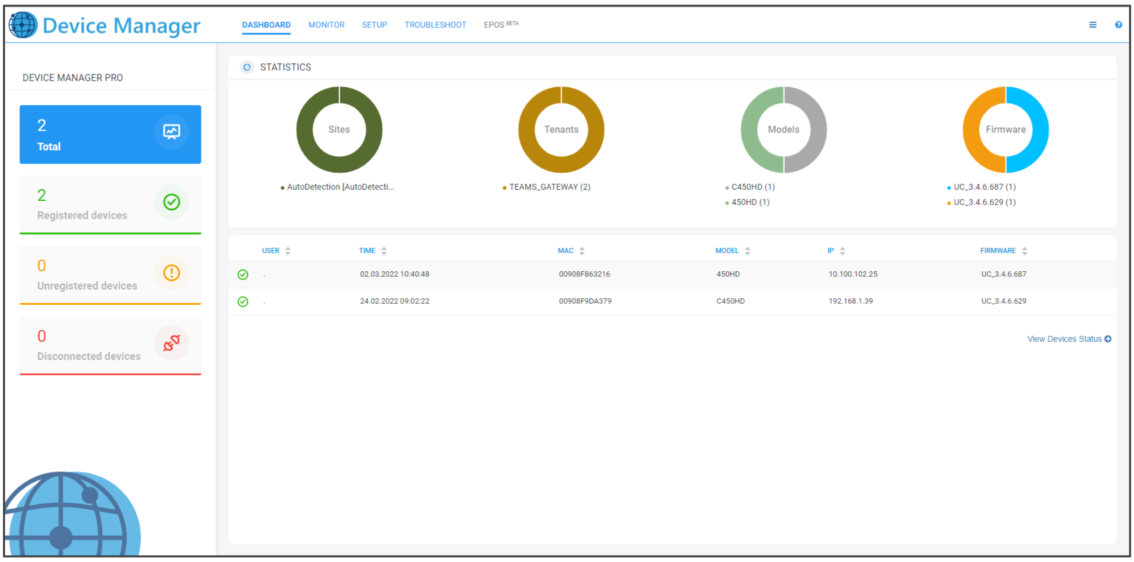
Verifying that Microsoft SIP Gateway was Added

After adding in the Device Manager Microsoft's SIP Gateway to an enterprise's IP telephony network, verify connectivity.

➢ To verify that Microsoft's SIP Gateway has been added to the IP network:

- In the Device Manager, open the Dashboard page and view TEAMS_GATEWAY displayed:

Figure 13-4: Dashboard page: Teams Gateway



	USER	TIME	MAC	MODEL	IP	FIRMWARE
✓	.	02.03.2022 10:40:48	00908F863216	450HD	10.100.102.25	UC_3.4.6.687
✓	.	24.02.2022 09:02:22	00908F9DA379	C450HD	192.168.1.39	UC_3.4.6.629

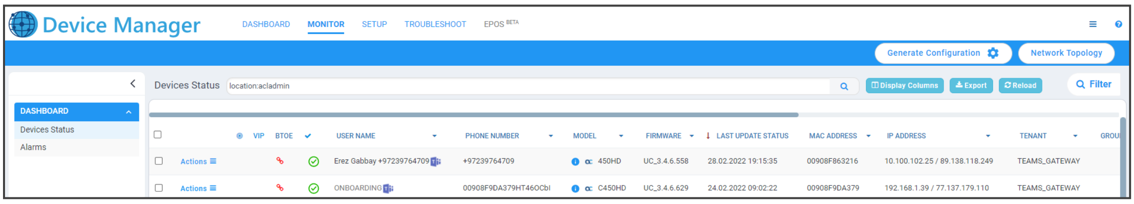
Monitoring the Microsoft Teams Phone

After converting a non Teams-certified AudioCodes phone model to a Microsoft Teams phone, the device can be monitored.

➢ To monitor an AudioCodes phone converted to a Microsoft Teams phone:

1. In the Device Manager, open the Devices Status page (**Monitor** > **Devices Status**).

Figure 13-5: Devices Status page



Devices Status location:acladmin

☐		VIP	BTOE	✓	USER NAME	PHONE NUMBER	MODEL	FIRMWARE	LAST UPDATE STATUS	MAC ADDRESS	IP ADDRESS	TENANT	GROU
☐	Actions ≡			✓	Erez Gabbay +97239764709	+97239764709	450HD	UC_3.4.6.558	28.02.2022 19:15:35	00908F863216	10.100.102.25 / 89.138.118.249	TEAMS_GATEWAY	
☐	Actions ≡			✓	ONBOARDING	00908F9DA379HT46OCbl	C450HD	UC_3.4.6.629	24.02.2022 09:02:22	00908F9DA379	192.168.1.39 / 77.137.179.110	TEAMS_GATEWAY	

2. View the Teams icon . displayed adjacent to the phone.

3. View the phone's status:

   - Onboarding (waiting for the user to sign in)
   - Registered (sign-in was performed)

14 Performing Poly Configuration

Poly Trio devices, Poly VVX devices and Poly CCX 500/600 devices can be *automatically provisioned with templates per model* from AudioCodes' provisioning server. The feature is an AudioCodes proprietary feature configured from the Poly Configuration page in the AudioCodes Device Manager (**Setup** > **Configuration** > **Poly Configuration**).

For more information, see the *Device Manager for Third-Party Vendor Products Administrator's Manual* available from AudioCodes.

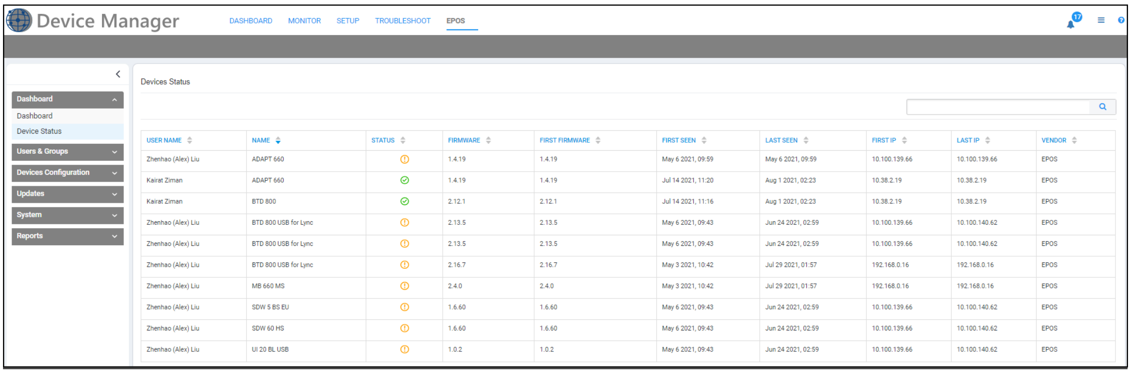
15 Performing EPOS Configuration

The Device Manager enables network administrators to manage and monitor EPOS (Sennheiser) headset devices (beta version). EPOS have a cloud-based EPOS Manager. AudioCodes' Device Manager reflects the EPOS Manager.

➢ To configure EPOS device settings:

- From any page in the Device Manager, click the **EPOS** menu.

Figure 15-1: EPOS



Devices Status

USER NAME	NAME	STATUS	FIRMWARE	FIRST FIRMWARE	FIRST SEEN	LAST SEEN	FIRST IP	LAST IP	VENDOR
Zhenhao (Alex) Liu	ADAPT 660	!	1.4.19	1.4.19	May 6 2021, 09:59	May 6 2021, 09:59	10.100.139.66	10.100.139.66	EPOS
Kairat Ziman	ADAPT 660	✓	1.4.19	1.4.19	Jul 14 2021, 11:20	Aug 1 2021, 02:23	10.38.2.19	10.38.2.19	EPOS
Kairat Ziman	BTD 800	✓	2.12.1	2.12.1	Jul 14 2021, 11:16	Aug 1 2021, 02:23	10.38.2.19	10.38.2.19	EPOS
Zhenhao (Alex) Liu	BTD 800 USB for Lync	!	2.13.5	2.13.5	May 6 2021, 09:43	Jun 24 2021, 02:59	10.100.139.66	10.100.140.62	EPOS
Zhenhao (Alex) Liu	BTD 800 USB for Lync	!	2.13.5	2.13.5	May 6 2021, 09:43	Jun 24 2021, 02:59	10.100.139.66	10.100.140.62	EPOS
Zhenhao (Alex) Liu	BTD 800 USB for Lync	!	2.16.7	2.16.7	May 3 2021, 10:42	Jul 29 2021, 01:57	192.168.0.16	192.168.0.16	EPOS
Zhenhao (Alex) Liu	MB 660 MS	!	2.4.0	2.4.0	May 3 2021, 10:42	Jul 29 2021, 01:57	192.168.0.16	192.168.0.16	EPOS
Zhenhao (Alex) Liu	SDW 5 BS EU	!	1.6.60	1.6.60	May 6 2021, 09:43	Jun 24 2021, 02:59	10.100.139.66	10.100.140.62	EPOS
Zhenhao (Alex) Liu	SDW 60 HS	!	1.6.60	1.6.60	May 6 2021, 09:43	Jun 24 2021, 02:59	10.100.139.66	10.100.140.62	EPOS
Zhenhao (Alex) Liu	UI 20 BL USB	!	1.0.2	1.0.2	May 6 2021, 09:43	Jun 24 2021, 02:59	10.100.139.66	10.100.140.62	EPOS

⚠ For detailed information about configuring EPOS device settings, see the following documents:

- *EPOS Manager Admin Manual* available here.
- *Device Manager for Third-Party Vendor Products Administrator's Manual* available on AudioCodes' website here.

16 Enabling Calls to Emergency Numbers

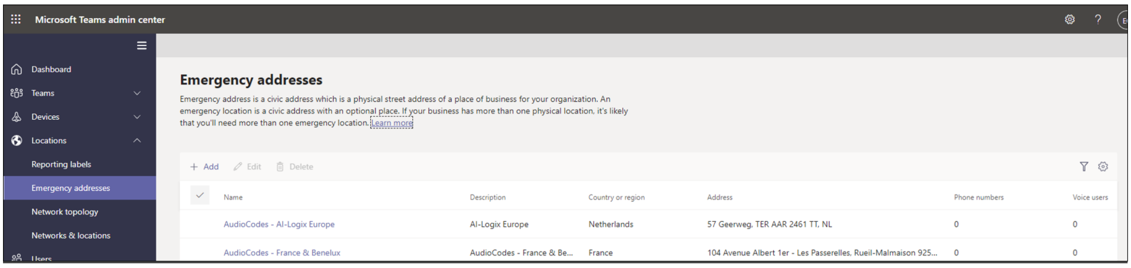
The documentation here shows how to enable users to make emergency calls to emergency numbers (E911) from Skype for Business IP phones. It'll help you get started with configuring the infrastructure elements and call routing needed for making dynamic emergency calls.

- 'Dynamic' means the Teams client gets the emergency address/location based on the network location it is at and transmits it directly to the Public Safety Answering Point (PSAP), bypassing the Emergency Call Relay Center (ECRC).
- Based on the network topology that the tenant administrator defines, the Teams client provides network connectivity information in a request to the Teams Location Information Service (LIS). If there's a match, the Teams LIS returns a location to the client. This location data is transmitted back to the client. See here for more on configuring dynamic emergency calling.
- 'Infrastructure elements' refers to information about the physical address of the building in which the devices are located and the network elements and their locations within it.

➢ To configure emergency locations in Microsoft Teams admin center:

1. In the admin center, open the 'Emergency addresses' page.

Figure 16-1: Microsoft Teams admin center: Emergency addresses

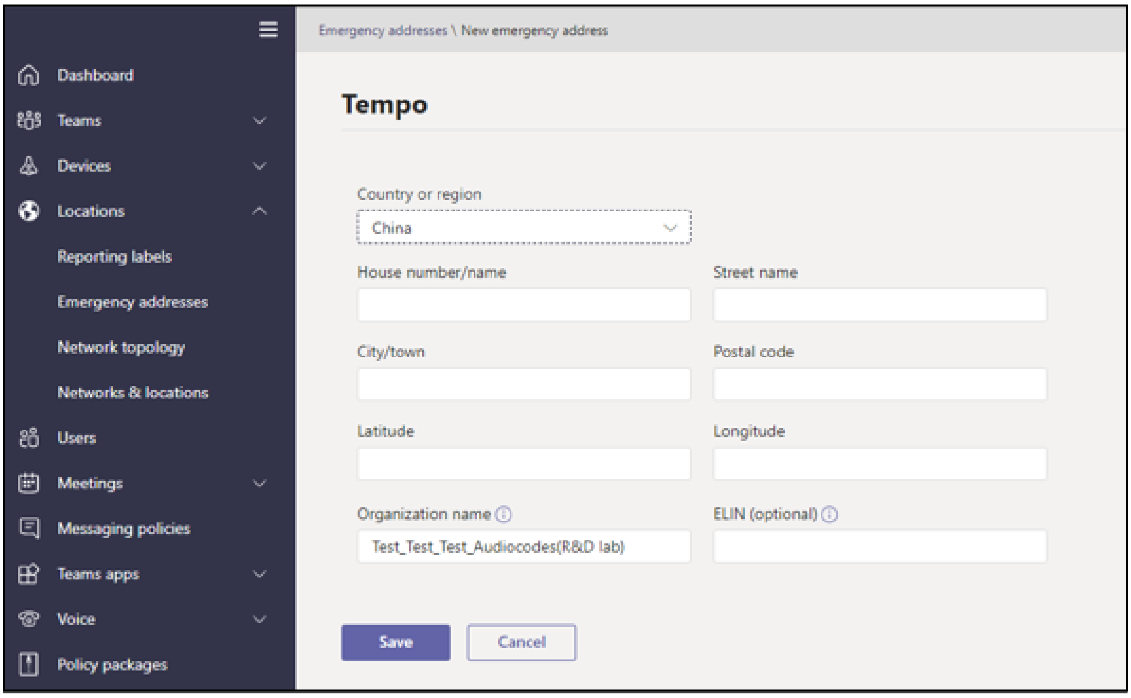


Emergency addresses

Emergency address is a civic address which is a physical street address of a place of business for your organization. An emergency location is a civic address with an optional place. If your business has more than one physical location, it's likely that you'll need more than one emergency location. Learn more

Name	Description	Country or region	Address	Phone numbers	Voice users
AudioCodes - Al-Logix Europe	Al-Logix Europe	Netherlands	57 Geerweg, TER AAR 2461 TT, NL	0	0
AudioCodes - France & Benelux	AudioCodes - France & Be...	France	104 Avenue Albert 1er - Les Passerelles, Rueil-Malmaison 925...	0	0

2. Add addresses using the preceding and next figure as reference.



Emergency addresses \ New emergency address

Tempo

Country or region: China

House number/name:

Street name:

City/town:

Postal code:

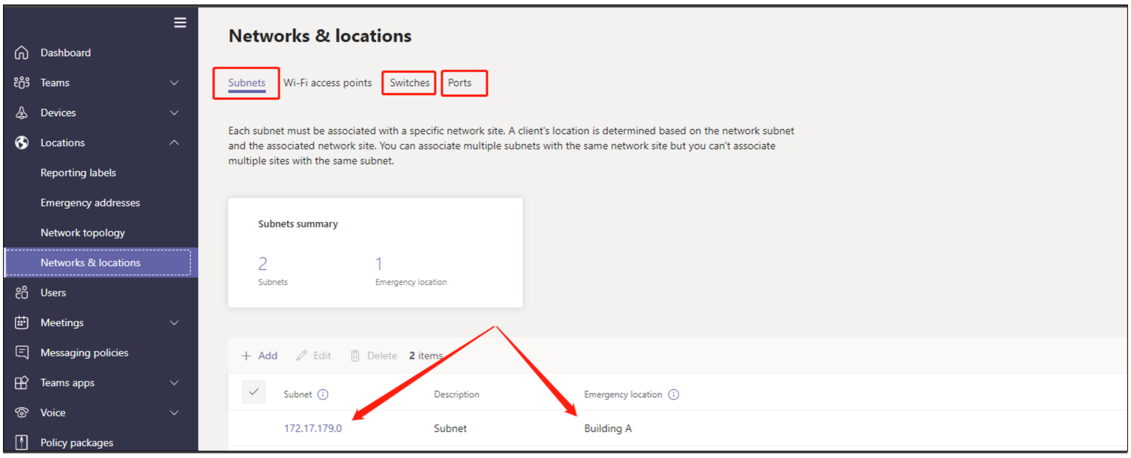
Latitude:

Longitude:

Organization name: Test_Test_Test_Audiocodes(R&D lab)

ELIN (optional):

3. Click **Save** and then open the 'Networks & locations' page.



Networks & locations

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

Subnets summary

2 Subnets

1 Emergency location

2 items

Subnet	Description	Emergency location
172.17.179.0	Subnet	Building A

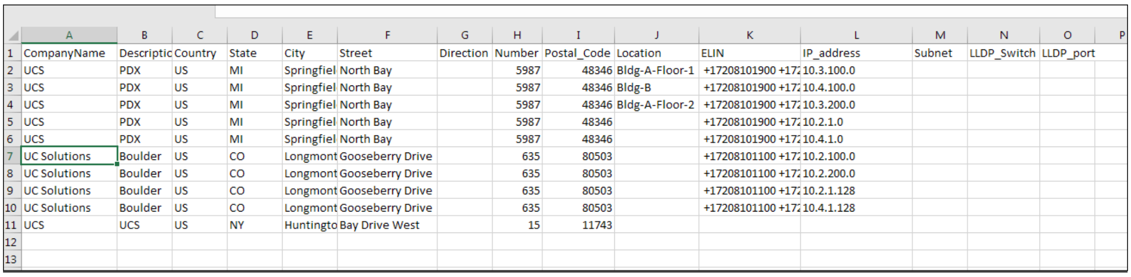
4. Assign an emergency address to the network site using the preceding figure as reference.

> After configuring the emergency locations in the Microsoft Teams admin center, you can import them into the Device Manager.

➢ To import emergency locations into the Device Manager:

1. After configuring emergency locations in Microsoft Teams admin center, open the Emergency Locations page in the Device Manager (**Setup** > **System** > **Emergency Locations**).
2. Click the **Import** button; a script exports the emergency locations from the Microsoft Teams admin center into the OVOC from where they're imported into the Device Manager.
3. Navigate to the folder in which the CSV file is saved.

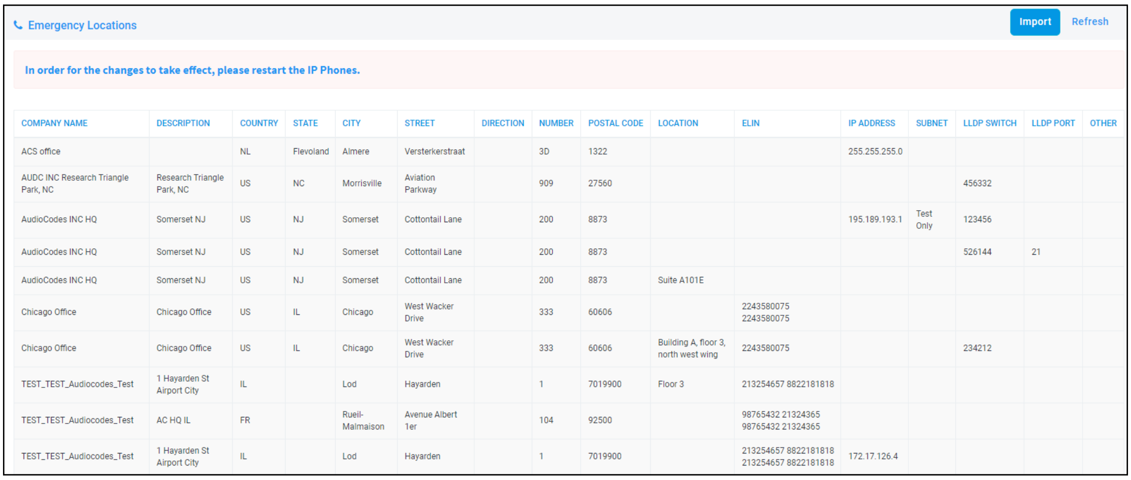
Figure 16-2: Example CSV File



	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
1	CompanyName	Descriptic	Country	State	City	Street	Direction	Number	Postal_Code	Location	ELIN	IP_address	Subnet	LLDP_Switch	LLDP_port	
2	UCS	PDX	US	MI	Springfiel	North Bay		5987	48346	Bldg-A-Floor-1	+17208101900 +172	10.3.100.0				
3	UCS	PDX	US	MI	Springfiel	North Bay		5987	48346	Bldg-B	+17208101900 +172	10.4.100.0				
4	UCS	PDX	US	MI	Springfiel	North Bay		5987	48346	Bldg-A-Floor-2	+17208101900 +172	10.3.200.0				
5	UCS	PDX	US	MI	Springfiel	North Bay		5987	48346		+17208101900 +172	10.2.1.0				
6	UCS	PDX	US	MI	Springfiel	North Bay		5987	48346		+17208101900 +172	10.4.1.0				
7	UC Solutions	Boulder	US	CO	Longmont	Gooseberry Drive		635	80503		+17208101100 +172	10.2.100.0				
8	UC Solutions	Boulder	US	CO	Longmont	Gooseberry Drive		635	80503		+17208101100 +172	10.2.200.0				
9	UC Solutions	Boulder	US	CO	Longmont	Gooseberry Drive		635	80503		+17208101100 +172	10.2.1.128				
10	UC Solutions	Boulder	US	CO	Longmont	Gooseberry Drive		635	80503		+17208101100 +172	10.4.1.128				
11	UCS	UCS	US	NY	Huntingto	Bay Drive West		15	11743							
12																
13																

After the CSV file is imported, the locations are displayed in the Device Manager's Emergency Locations table. The Device Manager adds the values from the CSV without any manipulation except for removing leading / trailing white spaces.

Figure 16-3: Emergency Locations page in the Device Manager



In order for the changes to take effect, please restart the IP Phones.

COMPANY NAME	DESCRIPTION	COUNTRY	STATE	CITY	STREET	DIRECTION	NUMBER	POSTAL CODE	LOCATION	ELIN	IP ADDRESS	SUBNET	LLDP SWITCH	LLDP PORT	OTHER
ACS office		NL	Flevoland	Almere	Versterkerstraat		3D	1322			255.255.255.0				
AUDC INC Research Triangle Park, NC	Research Triangle Park, NC	US	NC	Morrisville	Aviation Parkway		909	27560					456332		
AudioCodes INC HQ	Somerset NJ	US	NJ	Somerset	Cottontail Lane		200	8873			195.189.193.1	Test Only	123456		
AudioCodes INC HQ	Somerset NJ	US	NJ	Somerset	Cottontail Lane		200	8873					526144	21	
AudioCodes INC HQ	Somerset NJ	US	NJ	Somerset	Cottontail Lane		200	8873	Suite A101E						
Chicago Office	Chicago Office	US	IL	Chicago	West Wacker Drive		333	60606		2243580075 2243580075					
Chicago Office	Chicago Office	US	IL	Chicago	West Wacker Drive		333	60606	Building A, floor 3, north west wing	2243580075			234212		
TEST_TEST_Audiocodes_Test	1 Hayarden St Airport City	IL		Lod	Hayarden		1	7019900	Floor 3	213254657 8822181818					
TEST_TEST_Audiocodes_Test	AC HQ IL	FR		Rueil-Malmaison	Avenue Albert 1er		104	92500		98765432 21324365 98765432 21324365					
TEST_TEST_Audiocodes_Test	1 Hayarden St Airport City	IL		Lod	Hayarden		1	7019900		213254657 8822181818 213254657 8822181818	172.17.126.4				

4. View the following columns in the newly created Emergency Locations table:

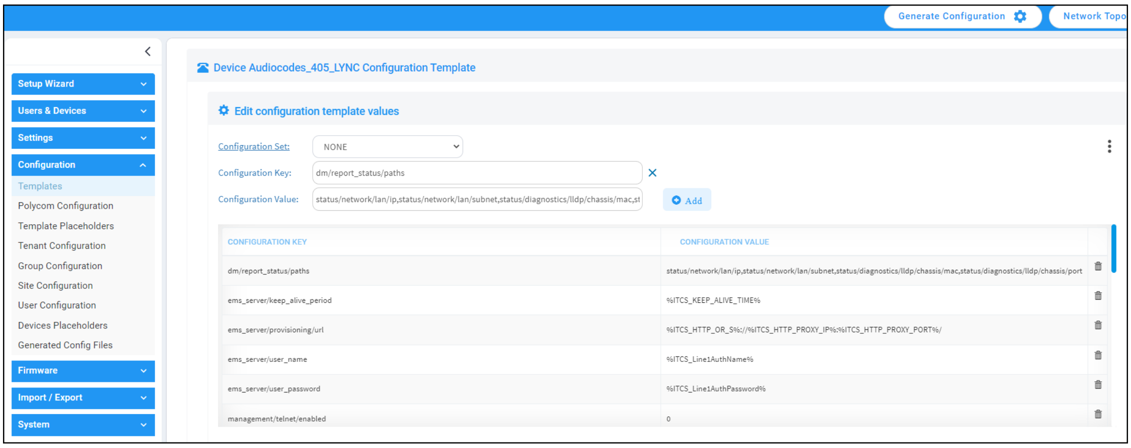
- Company Name - the name of the company in which the devices are deployed
- Description - a description of the company in which the devices are deployed
- Country - the name of the country in which the company is located
- State - the name of the state in which the company is located
- City - the name of the city in which the company is located
- Street - the name of the street in which the company is located
- Direction
- Number - the street number of the company
- Postal Code - the postal code of the company
- Location - the company's department in which the devices are deployed
- ELIN - Emergency Location Identification Number. A 10-digit DID number that can be obtained from the local exchange carrier (LEC). Provide it to the public safety answering point (PSAP) for 911 calls.
- IP address - the device's IP address in the network

- Subnet - the subnet in which the device is deployed
- LLDP Switch - Link Layer Discovery Protocol switch. Devices use this link layer protocol to advertize their identity, capabilities and neighbors in a LAN based on IEEE 802.
- LLDP port - Link Layer Discovery Protocol port.
- OTHER

> ⚠ Make sure two rows (or more) in the Emergency Locations table do not contain same combination of:
>
> - LLDP Switch Chassis number + LLDP port
> - LLDP Switch Chassis number + EMPTY LLDP port
> - IP address

5. After importing the CSV file, edit the configuration template in the Configuration Template page (**Setup** > **Configuration** > **Templates**).

Figure 16-4: Configuration Template



Device Audiocodes_405_LYNC Configuration Template

Edit configuration template values

Configuration Set: NONE

Configuration Key: dm/report_status/paths

Configuration Value: status/network/lan/ip,status/network/lan/subnet,status/diagnostics/lldp/chassis/mac,st

CONFIGURATION KEY	CONFIGURATION VALUE
dm/report_status/paths	status/network/lan/ip,status/network/lan/subnet,status/diagnostics/lldp/chassis/mac,status/diagnostics/lldp/chassis/port
ems_server/keep_alive_period	%ITCS_KEEP_ALIVE_TIME%
ems_server/provisioning/url	%ITCS_HTTP_OR_S%://%ITCS_HTTP_PROXY_IP%:%ITCS_HTTP_PROXY_PORT%/
ems_server/user_name	%ITCS_Line1AuthName%
ems_server/user_password	%ITCS_Line1AuthPassword%
management/telnet/enabled	0

6. Configure the following (refer to the preceding figure):

- Set the parameter 'Configuration Key' to **dm/report_status/paths**
- Set the parameter 'Configuration Value' to

  dm/report_status/paths=status/network/lan/*,

  status/diagnostics/lldp/chassis/chassisId,

  status/diagnostics/lldp/chassis/portId

> ⚠
>
> - Configuration of these two parameters is mandatory for the feature to function.
> - The configuration can be performed at either the device level, Tenant level, Group level or Site level.

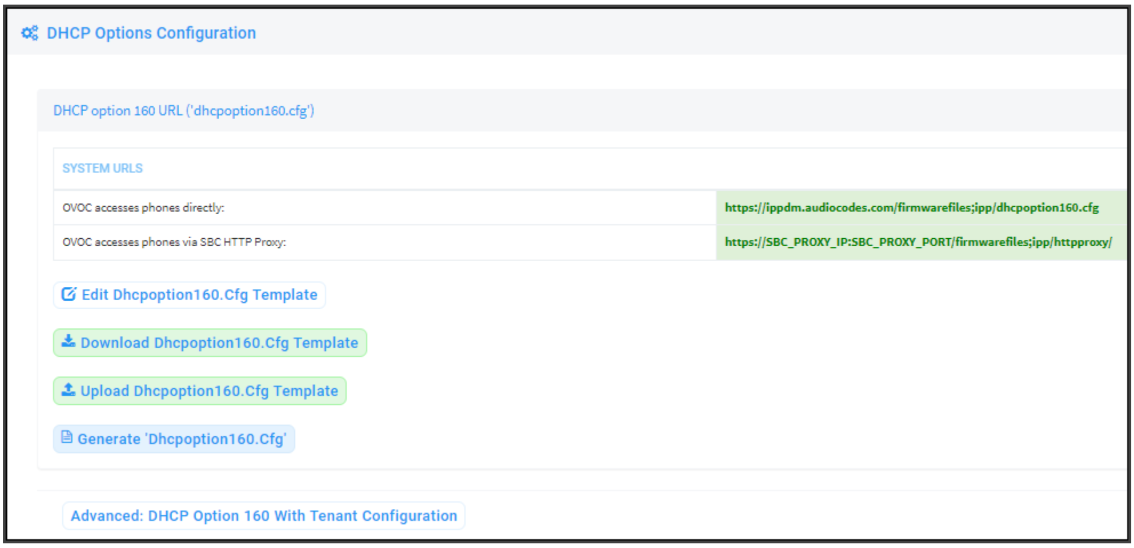
17 Configuring Phones to Operate in an OVR Deployment

You can configure phones to operate in an OVR (One Voice Resiliency) deployment. See the *One Voice Resiliency Configuration Note* for a detailed description of OVR.

➢ To configure phones to operate in an OVR deployment:

1. Open the DHCP Options Configuration page (**Setup** > **Settings** > **DHCP Options Configuration**).

Figure 17-1: DHCP Options Configuration



DHCP Options Configuration

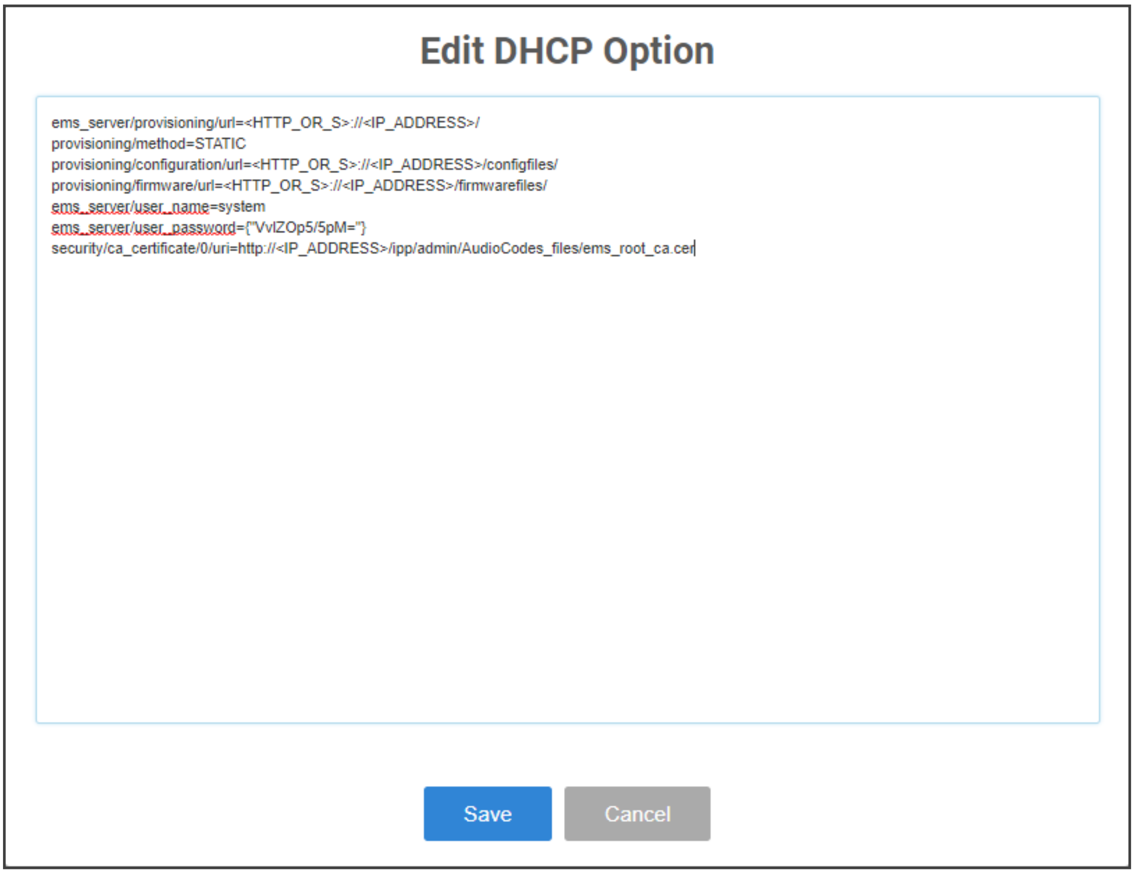
DHCP option 160 URL ('dhcpoption160.cfg')

SYSTEM URLS

OVOC accesses phones directly:	https://ippdm.audiocodes.com/firmwarefiles;ipp/dhcpoption160.cfg
OVOC accesses phones via SBC HTTP Proxy:	https://SBC_PROXY_IP:SBC_PROXY_PORT/firmwarefiles;ipp/httpproxy/

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

2. Click the **Edit dhcpoption160.cfg template** button.



```
ems_server/provisioning/url=<HTTP_OR_S>://<IP_ADDRESS>/
provisioning/method=STATIC
provisioning/configuration/url=<HTTP_OR_S>://<IP_ADDRESS>/configfiles/
provisioning/firmware/url=<HTTP_OR_S>://<IP_ADDRESS>/firmwarefiles/
ems_server/user_name=system
ems_server/user_password={"VvlZOp5/5pM="}
security/ca_certificate/0/uri=http://<IP_ADDRESS>/ipp/admin/AudioCodes_files/ems_root_ca.cer
```

3. Customize dhcpoption160.cfg. Add the following lines:

```
outbound_proxy_address=<SBC IP address>
lync/sign_in/fixed_outbound_proxy_port=<SBC listening port>
lync/sign_in/use_hosting_outbound_proxy=1
```

4. Click **Save**; the phones are configured to operate in an OVR environment.

⚠ After configuring phones to operate in an OVR environment, you must configure their template with the same settings.

18 Signing in to a Phone into which Another User is Signed

If user B signs in to a phone that user A is signed in to, user A's phone is deleted from the Manage Users page and the newly signed-in phone is added to User A.

The Devices Status page is updated with the newly signed-in phone.

Before version 7.2, the GUI remained unchanged, irrespective of the new sign in.

⚠ Applies only if the Zero Touch provisioning method was used.

19 Troubleshooting

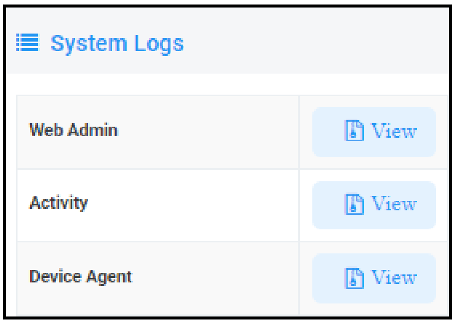
You can display system diagnostics to help troubleshoot problems and determine cause. System diagnostics comprise:

- Logged activities performed in the Web interface
    - Last logged activities
    - Archived activities
- Logged activities performed in the Device Manager Pro
    - Last logged activities
    - Archived activities

➢ **To display system diagnostics:**

1. Open the System Logs page (**Troubleshoot** > **System Diagnostics**).

Figure 19-1: System Logs



System Logs

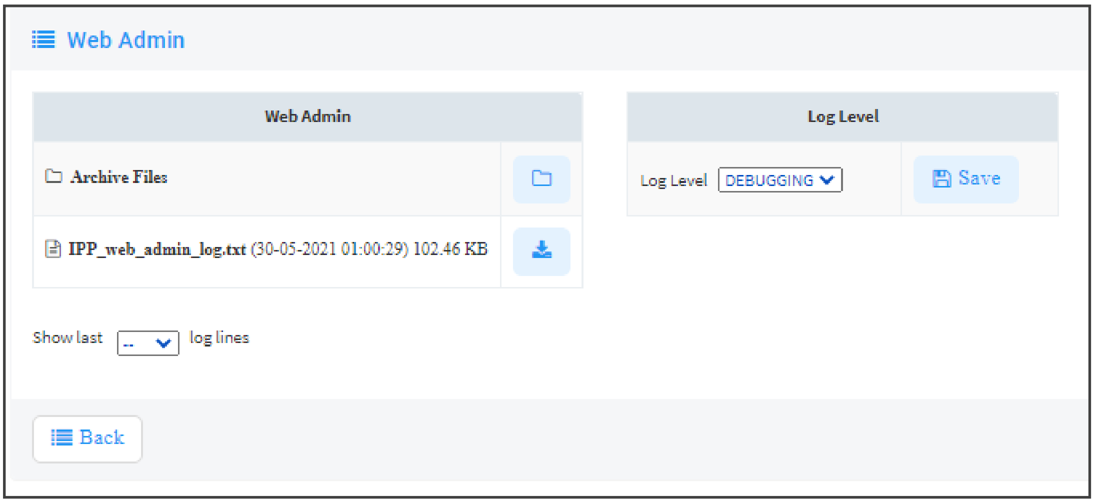
Web Admin	View
Activity	View
Device Agent	View

Displaying Last n Activities Performed in the Web Interface

➢ **To display logged activities performed in the Web interface:**

1. Click the **View** button next to **Web Admin**.

Figure 19-2: Web Admin



IPP_web_admin_log.txt (30-05-2021 01:00:29) 102.46 KB

Log Level DEBUGGING

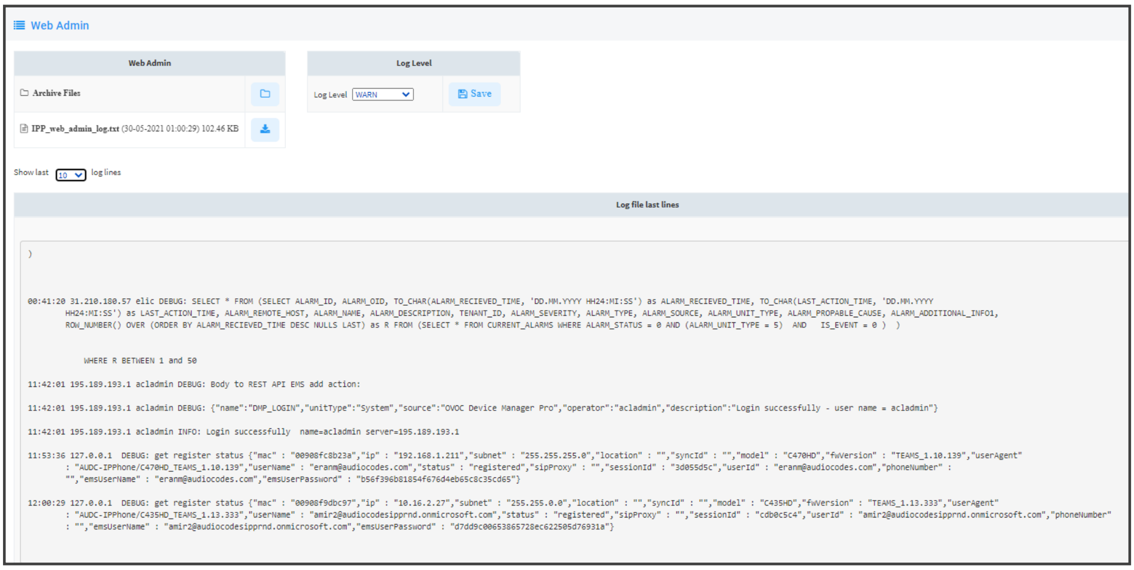
Show last -- log lines

2. From the 'Log Level' dropdown select ERROR, WARN, INFO, DEBUGGING (default) or VERBOSE – All Levels (Detailed).

3. From the 'Show last log lines' dropdown select 10, 20, 30, 40, 50 or 100.

4. View the generated *IPP_web_admin_log.txt* file.

Figure 19-3: Last Activities Logged in the Web Interface



IPP_web_admin_log.txt (30-05-2021 01:00:29) 102.46 KB

Log Level WARN

Show last 10 log lines

```
)


00:41:20 31.210.180.57 elic DEBUG: SELECT * FROM (SELECT ALARM_ID, ALARM_OID, TO_CHAR(ALARM_RECIEVED_TIME, 'DD.MM.YYYY HH24:MI:SS') as ALARM_RECIEVED_TIME, TO_CHAR(LAST_ACTION_TIME, 'DD.MM.YYYY
        HH24:MI:SS') as LAST_ACTION_TIME, ALARM_REMOTE_HOST, ALARM_NAME, ALARM_DESCRIPTION, TENANT_ID, ALARM_SEVERITY, ALARM_TYPE, ALARM_SOURCE, ALARM_UNIT_TYPE, ALARM_PROPABLE_CAUSE, ALARM_ADDITIONAL_INFO1,
        ROW_NUMBER() OVER (ORDER BY ALARM_RECIEVED_TIME DESC NULLS LAST) as R FROM (SELECT * FROM CURRENT_ALARMS WHERE ALARM_STATUS = 0 AND (ALARM_UNIT_TYPE = 5)  AND   IS_EVENT = 0 )  )


            WHERE R BETWEEN 1 and 50

11:42:01 195.189.193.1 acladmin DEBUG: Body to REST API EMS add action:

11:42:01 195.189.193.1 acladmin DEBUG: {"name":"DMP_LOGIN","unitType":"System","source":"OVOC Device Manager Pro","operator":"acladmin","description":"Login successfully - user name = acladmin"}

11:42:01 195.189.193.1 acladmin INFO: Login successfully  name=acladmin server=195.189.193.1

11:53:36 127.0.0.1  DEBUG: get register status {"mac" : "00908fc8b23a","ip" : "192.168.1.211","subnet" : "255.255.255.0","location" : "","syncId" : "","model" : "C470HD","fwVersion" : "TEAMS_1.10.139","userAgent"
        : "AUDC-IPPhone/C470HD_TEAMS_1.10.139","userName" : "eranm@audiocodes.com","status" : "registered","sipProxy" : "","sessionId" : "3d055d5c","userId" : "eranm@audiocodes.com","phoneNumber" :
        "","emsUserName" : "eranm@audiocodes.com","emsUserPassword" : "b56f396b81854f676d4eb65c8c35cd65"}

12:00:29 127.0.0.1  DEBUG: get register status {"mac" : "00908f9dbc97","ip" : "10.16.2.27","subnet" : "255.255.0.0","location" : "","syncId" : "","model" : "C435HD","fwVersion" : "TEAMS_1.13.333","userAgent"
        : "AUDC-IPPhone/C435HD_TEAMS_1.13.333","userName" : "amir2@audiocodesipprnd.onmicrosoft.com","status" : "registered","sipProxy" : "","sessionId" : "cdb0c5c4","userId" : "amir2@audiocodesipprnd.onmicrosoft.com","phoneNumber"
        : "","emsUserName" : "amir2@audiocodesipprnd.onmicrosoft.com","emsUserPassword" : "d7dd9c00653865728ec622505d76931a"}
```

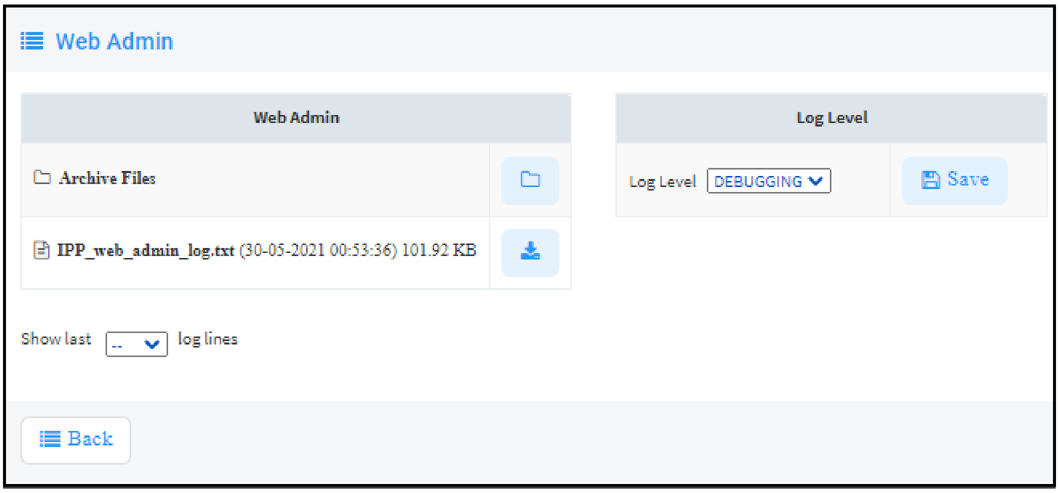
5. Click **Save** to save the last logged activities performed in the Web interface and share the log file with others.

Displaying Archived Activities Performed in the Web Interface

➢ **To display archived activities performed in the Web interface:**

1. Open the Web Admin page (**Troubleshoot** > **System Diagnostics** > **Web Admin Logs**).

Figure 19-4: System Logs



Web Admin

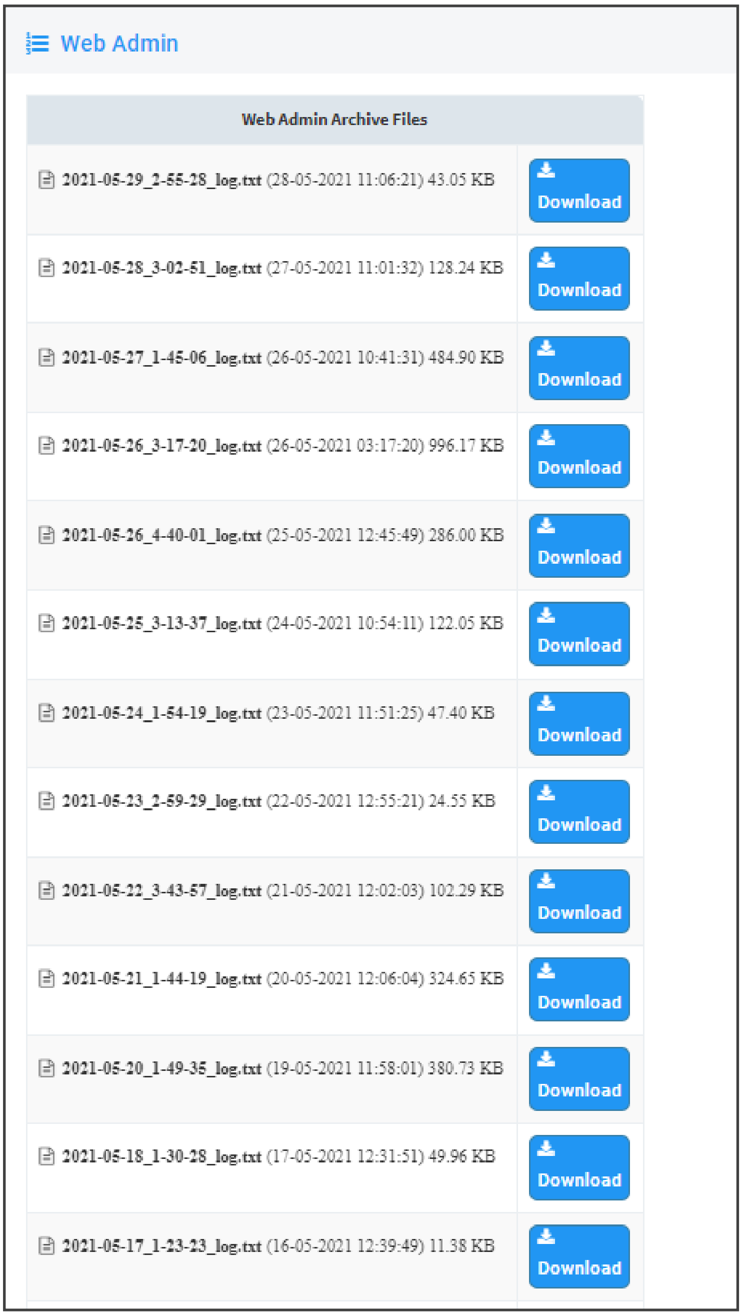
Web Admin	
Archive Files	
IPP_web_admin_log.txt (30-05-2021 00:53:36) 101.92 KB	

Log Level	
Log Level DEBUGGING	Save

Show last -- log lines

2. Click the icon next to **Archive Files**.

Figure 19-5: Archive Files



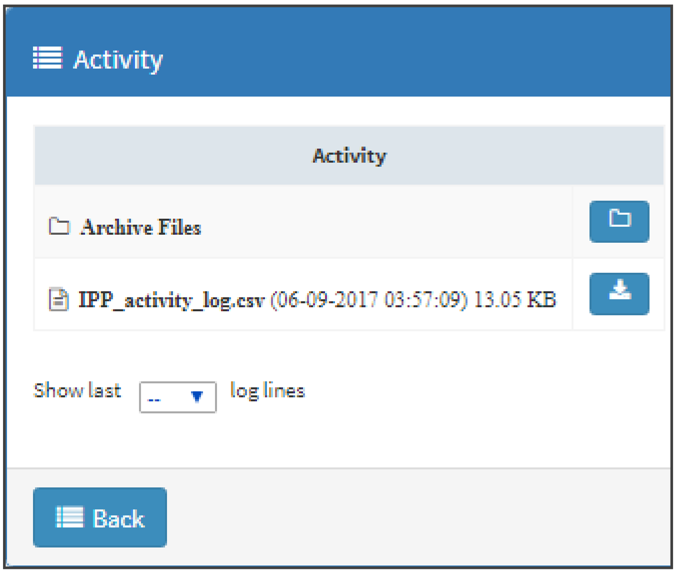
Web Admin Archive Files	
🗎 **2021-05-29_2-55-28_log.txt** (28-05-2021 11:06:21) 43.05 KB	Download
🗎 **2021-05-28_3-02-51_log.txt** (27-05-2021 11:01:32) 128.24 KB	Download
🗎 **2021-05-27_1-45-06_log.txt** (26-05-2021 10:41:31) 484.90 KB	Download
🗎 **2021-05-26_3-17-20_log.txt** (26-05-2021 03:17:20) 996.17 KB	Download
🗎 **2021-05-26_4-40-01_log.txt** (25-05-2021 12:45:49) 286.00 KB	Download
🗎 **2021-05-25_3-13-37_log.txt** (24-05-2021 10:54:11) 122.05 KB	Download
🗎 **2021-05-24_1-54-19_log.txt** (23-05-2021 11:51:25) 47.40 KB	Download
🗎 **2021-05-23_2-59-29_log.txt** (22-05-2021 12:55:21) 24.55 KB	Download
🗎 **2021-05-22_3-43-57_log.txt** (21-05-2021 12:02:03) 102.29 KB	Download
🗎 **2021-05-21_1-44-19_log.txt** (20-05-2021 12:06:04) 324.65 KB	Download
🗎 **2021-05-20_1-49-35_log.txt** (19-05-2021 11:58:01) 380.73 KB	Download
🗎 **2021-05-18_1-30-28_log.txt** (17-05-2021 12:31:51) 49.96 KB	Download
🗎 **2021-05-17_1-23-23_log.txt** (16-05-2021 12:39:49) 11.38 KB	Download

Displaying Last n Activities Performed in Device Manager Pro

➢ **To display last activities logged in the Device Manager Pro:**

1. In the System Logs page, click **View** next to **Activity**.

Figure 19-6: Logged Activities Performed in Device Manager Pro

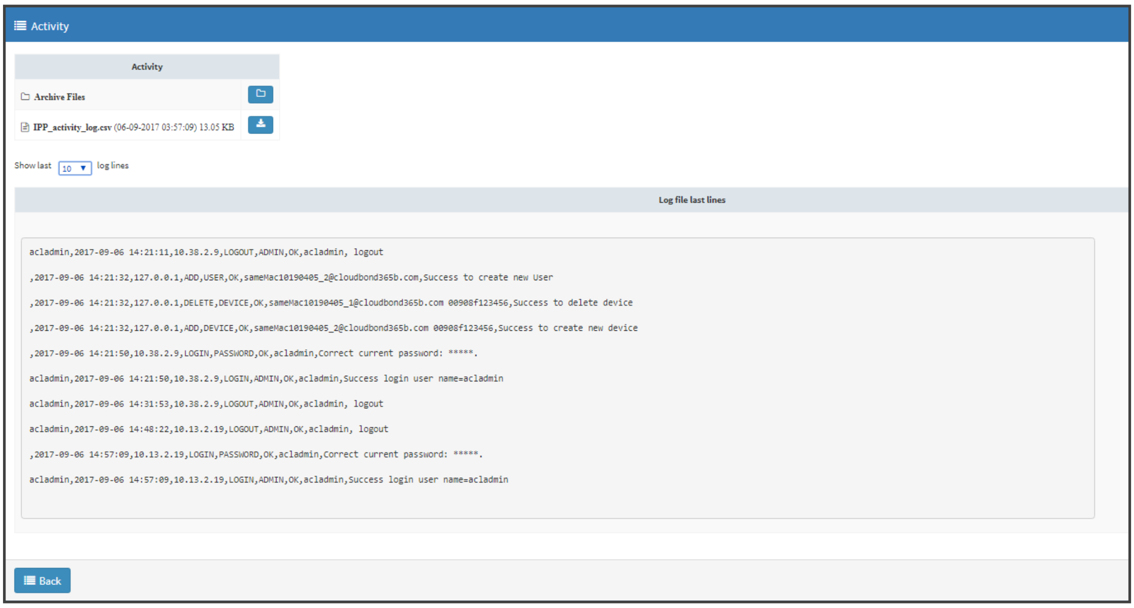


IPP_activity_log.csv (06-09-2017 03:57:09) 13.05 KB

Show last -- log lines

2. From the 'Show last log lines' dropdown select 10, 20, 30, 40, 50 or 100.

Figure 19-7: Logged Last Activities Performed in Device Manager Pro



IPP_activity_log.csv (06-09-2017 03:57:09) 13.05 KB

Show last 10 log lines

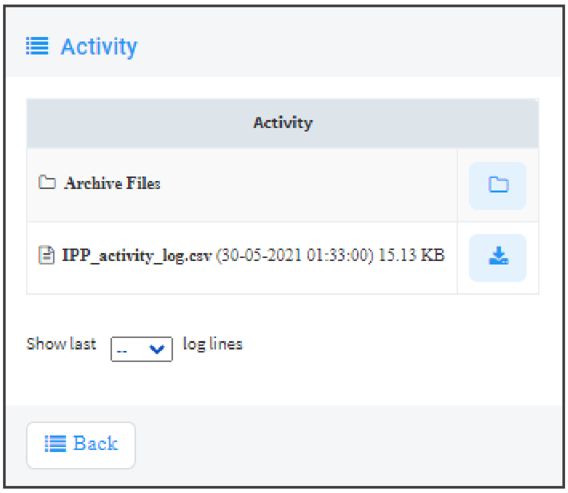
```
acladmin,2017-09-06 14:21:11,10.38.2.9,LOGOUT,ADMIN,OK,acladmin, logout

,2017-09-06 14:21:32,127.0.0.1,ADD,USER,OK,sameMac10190405_2@cloudbond365b.com,Success to create new User

,2017-09-06 14:21:32,127.0.0.1,DELETE,DEVICE,OK,sameMac10190405_1@cloudbond365b.com 00908f123456,Success to delete device

,2017-09-06 14:21:32,127.0.0.1,ADD,DEVICE,OK,sameMac10190405_2@cloudbond365b.com 00908f123456,Success to create new device

,2017-09-06 14:21:50,10.38.2.9,LOGIN,PASSWORD,OK,acladmin,Correct current password: *****.

acladmin,2017-09-06 14:21:50,10.38.2.9,LOGIN,ADMIN,OK,acladmin,Success login user name=acladmin

acladmin,2017-09-06 14:31:53,10.38.2.9,LOGOUT,ADMIN,OK,acladmin, logout

acladmin,2017-09-06 14:48:22,10.13.2.19,LOGOUT,ADMIN,OK,acladmin, logout

,2017-09-06 14:57:09,10.13.2.19,LOGIN,PASSWORD,OK,acladmin,Correct current password: *****.

acladmin,2017-09-06 14:57:09,10.13.2.19,LOGIN,ADMIN,OK,acladmin,Success login user name=acladmin
```

Displaying Archived Activities Performed in Device Manager Pro

➢ **To display logged archived activities performed in the Device Manager Pro:**

- Open the Activity page (**Troubleshoot** > **Activity Logs**).

Figure 19-8: Logged Archived Activities Performed in Device Manager Pro



Activity

Activity	
Archive Files	
IPP_activity_log.csv (30-05-2021 01:33:00) 15.13 KB	

Show last -- log lines

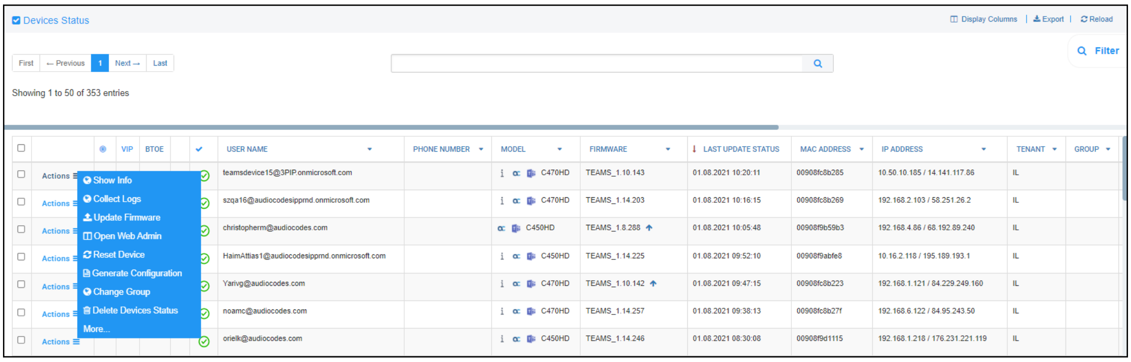
Getting Logs

The Device Manager enables network administrators to get logs for debugging purposes without needing to go to the phone.

➢ To get logs:

1. In the Monitor page (**Monitor** > **Devices Status**), click **Actions** adjacent to the listed phone from which you want to get logs and then select the **Collect Logs** option from the pop-up menu.

Figure 19-9: Actions > Collect Logs



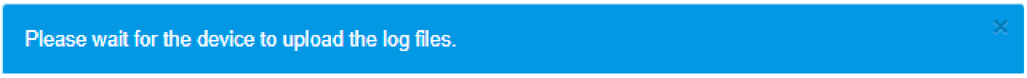
Devices Status

Display Columns | Export | Reload
Filter
First ← Previous 1 Next → Last

Showing 1 to 50 of 353 entries

□		◉	VIP	BTOE	✓	USER NAME	PHONE NUMBER	MODEL	FIRMWARE	LAST UPDATE STATUS	MAC ADDRESS	IP ADDRESS	TENANT	GROUP
□	Actions ☰				✓	teamsdevice15@3PIP.onmicrosoft.com		C470HD	TEAMS_1.10.143	01.08.2021 10:20:11	00908fc8b285	10.50.10.185 / 14.141.117.86	IL	
□	Actions ☰				✓	szqa16@audiocodesipprnd.onmicrosoft.com		C470HD	TEAMS_1.14.203	01.08.2021 10:16:15	00908fc8b269	192.168.2.103 / 58.251.26.2	IL	
□	Actions ☰				✓	christopherm@audiocodes.com		C450HD	TEAMS_1.8.288 ↑	01.08.2021 10:05:48	00908f9b59b3	192.168.4.86 / 68.192.89.240	IL	
□	Actions ☰				✓	HaimAttias1@audiocodesipprnd.onmicrosoft.com		C450HD	TEAMS_1.14.225	01.08.2021 09:52:10	00908f9abfe8	10.16.2.118 / 195.189.193.1	IL	
□	Actions ☰				✓	Yarivg@audiocodes.com		C470HD	TEAMS_1.10.142 ↑	01.08.2021 09:47:15	00908fc8b223	192.168.1.121 / 84.229.249.160	IL	
□	Actions ☰				✓	noamc@audiocodes.com		C470HD	TEAMS_1.14.257	01.08.2021 09:38:13	00908fc8b27f	192.168.6.122 / 84.95.243.50	IL	
□	Actions ☰				✓	orielk@audiocodes.com		C450HD	TEAMS_1.14.246	01.08.2021 08:30:08	00908f9d1115	192.168.1.218 / 176.231.221.119	IL	

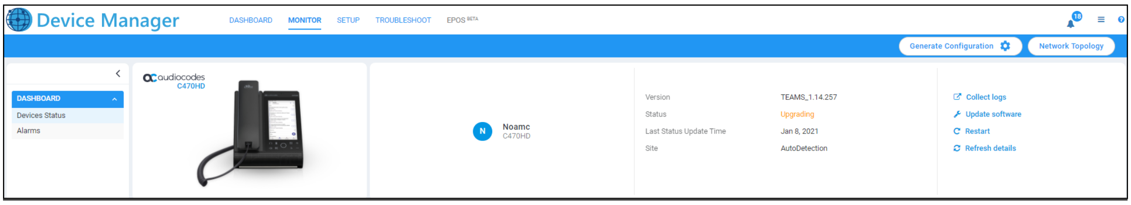
2. View the following notification:



Please wait for the device to upload the log files.

3. Alternatively, select the **Show Info** option and after making sure of the phone's identity, click the **Collect Logs** link on the right side of the screen.

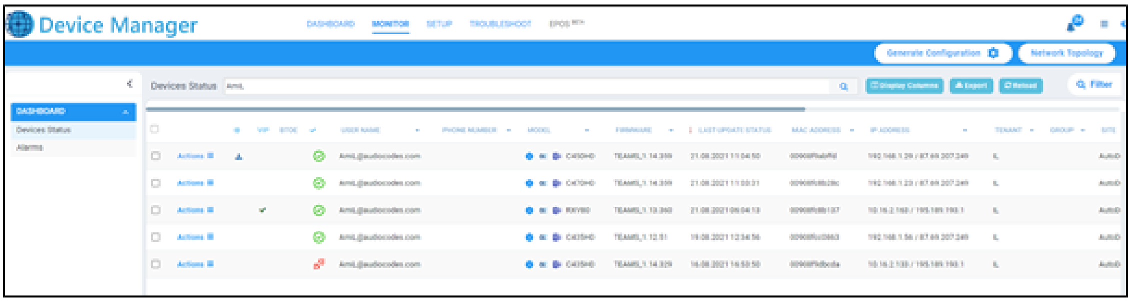
Figure 19-10: Show Info > Collect Logs



Version	TEAMS_1.14.257
Status	Upgrading
Last Status Update Time	Jan 8, 2021
Site	AutoDetection

4. After the logs are collected, the Devices Status page displays ⤓ in the same row as the device from which logs were collected as shown in the next figure.

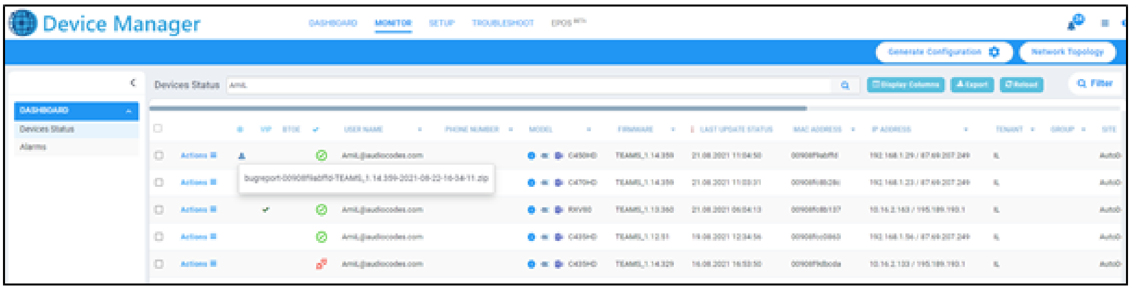
Figure 19-11: Devices Status > Download Logs



			VIP	E TOE		USER NAME	PHONE NUMBER	MODEL	FIRMWARE	LAST UPDATE STATUS	MAC ADDRESS	IP ADDRESS	TENANT	GROUP	SITE
□	Actions	⤓			✓	AmiL@audiocodes.com		C450HD	TEAMS_1.14.359	21.08.2021 11:04:50	00908f9abffd	192.168.1.29 / 87.69.207.249	IL		AutoD
□	Actions				✓	AmiL@audiocodes.com		C470HD	TEAMS_1.14.359	21.08.2021 11:03:21	00908fc8b28c	192.168.1.23 / 87.69.207.249	IL		AutoD
□	Actions		✓		✓	AmiL@audiocodes.com		RXV80	TEAMS_1.13.360	21.08.2021 06:04:13	00908fc8b137	10.16.2.163 / 195.189.193.1	IL		AutoD
□	Actions				✓	AmiL@audiocodes.com		C435HD	TEAMS_1.12.51	19.08.2021 12:34:56	00908fcc0863	192.168.1.56 / 87.69.207.249	IL		AutoD
□	Actions				✗	AmiL@audiocodes.com		C435HD	TEAMS_1.14.329	16.08.2021 16:53:50	00908f9dbcda	10.16.2.133 / 195.189.193.1	IL		AutoD

5. Click the icon to download the logs.

Figure 19-12: Devices Status > Download Logs



bugreport-00908f9abffd-TEAMS_1.14.359-2021-08-22-16-34-11.zip

			VIP	E TOE		USER NAME	PHONE NUMBER	MODEL	FIRMWARE	LAST UPDATE STATUS	MAC ADDRESS	IP ADDRESS	TENANT	GROUP	SITE
□	Actions	⤓			✓	AmiL@audiocodes.com		C450HD	TEAMS_1.14.359	21.08.2021 11:04:50	00908f9abffd	192.168.1.29 / 87.69.207.249	IL		AutoD
□	Actions							C470HD	TEAMS_1.14.359	21.08.2021 11:03:21	00908fc8b28c	192.168.1.23 / 87.69.207.249	IL		AutoD
□	Actions		✓		✓	AmiL@audiocodes.com		RXV80	TEAMS_1.13.360	21.08.2021 06:04:13	00908fc8b137	10.16.2.163 / 195.189.193.1	IL		AutoD
□	Actions				✓	AmiL@audiocodes.com		C435HD	TEAMS_1.12.51	19.08.2021 12:34:56	00908fcc0863	192.168.1.56 / 87.69.207.249	IL		AutoD
□	Actions				✗	AmiL@audiocodes.com		C435HD	TEAMS_1.14.329	16.08.2021 16:53:50	00908f9dbcda	10.16.2.133 / 195.189.193.1	IL		AutoD

6. Network administrators can click the icon to download the logs.

This page is intentionally left blank.

International Headquarters

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

AudioCodes Inc.

200 Cottontail Lane
Suite A101E
Somerset NJ 08873
Tel: +1-732-469-0880
Fax: +1-732-469-2298

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

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

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

Document #: LTRT-91221