Administrator's Guide

AudioCodes One Voice Operations Center (OVOC)

Device Manager Pro

Version 7.6.1000

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-24-2019

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
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

Document Name
Device Manager for Third-Party Vendor Products Administrator's Manual
Device Manager Agent Installation and Configuration Guide
One Voice Operations Center IOM Manual
One Voice Operations Center User's Manual
One Voice Resiliency Configuration Note

Document Revision Record

LTRT	Description
91080	Initial document release for Version 7.0 beta.
91081	7.0 GA. DHCP Option 160 changed. 'System' user added. New Device Status page features. Added img file management at device and tenant levels. Improved Template Placeholders. Installation procedure extended. New appendices. Enhanced alarm tables. New actions on multiple phones.
91082	Added support for the EMS to manage IP phones residing behind a NAT, though full management functionality support is still pending.
91083	HTTPS support when sending REST requests to phones. Option to use FQDN instead of IP (phones report to FQDN). Option to edit the initial DHCP Options 160 cfg file. Support for SBC HTTP Proxy. Show registered phones in the Users List. Open phone Web interface with HTTPS rather than HTTP. OVR. 405 model.
91084	7.2 GA. Zero Touch, administrator security level, tenant-specific administrator security level, viewing administrator security level per tenant, new GUI look & feel (new screenshots): Dashboard (new pie charts) and other pages.
91085	7.2.2000. REST requests from phones to EMS over HTTPS; from EMS server to phones are over HTTP. 3 new alarms. Telnet debug commands. Time Based License.
91087	7.2.3000. 450HD phone model. Full search. HTTP redirected to HTTPS.
91088	Updated EMS Platform Specifications
91089	Added new alarms for the Jabra speaker.
91090	Adjusted 'Required Ports for IP Phone Management'
91091	Access from OVOC. New look|feel. New name. New features.
91092	Setup Wizard. USB port. HRS.
91093	Provisioning Non Skype for Business IP Phones. Session Timeout. Update Firmware with Delay.
91094	7.6. Import only users. Update firmware for a batch of devices. Delay between batches. System Settings parameter. Polycom phone.

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: 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 AudioCodes' devices in an enterprise network from a single central point, using AudioCodes' Device Manager Pro.

- For information on third-party vendor products (for example Jabra and Polycom), 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 77
- 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.

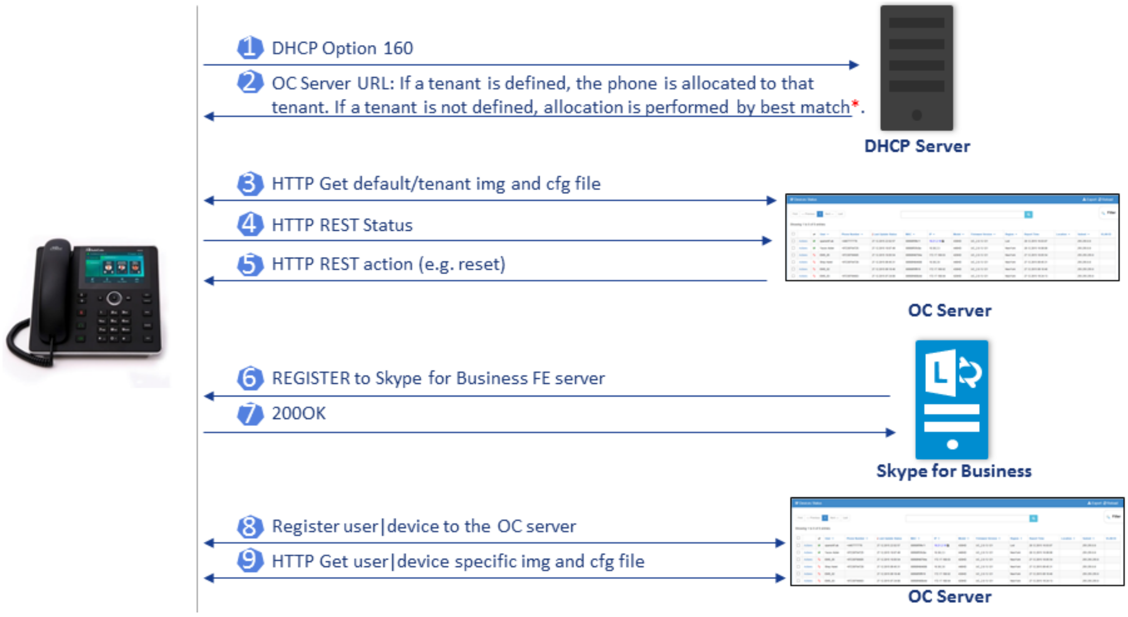
3. Choose the Zero Touch provisioning method. Either:
   - Configure the DHCP server to provision the phone with an IP address that is in the tenant/site range. Configure the phone to receive the IP address or subnet mask of the tenant/site.
   - Use DHCP Option 160.
4. Choose the default template for 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 25.

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

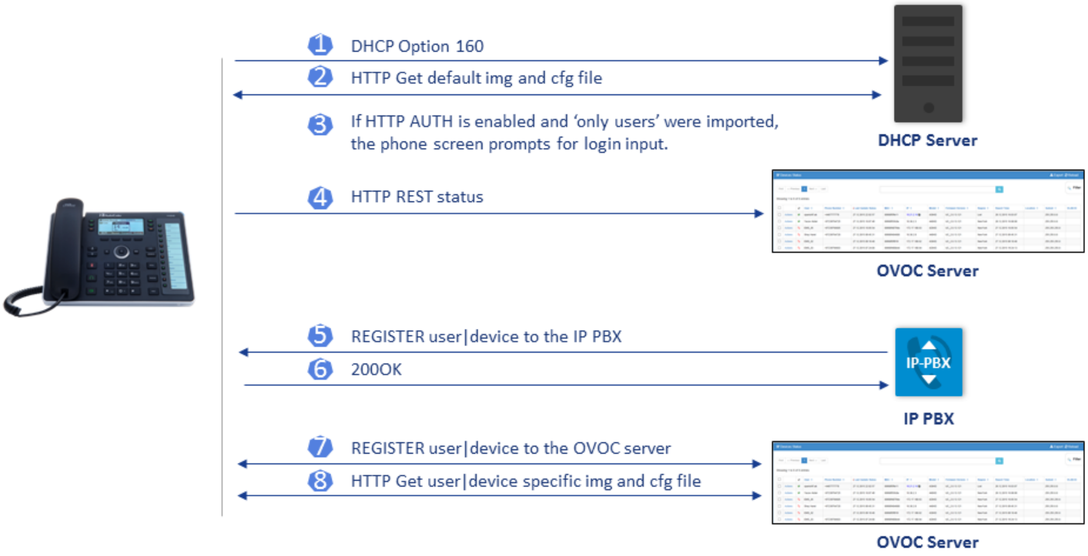

1 DHCP Option 160
2 OC Server URL: If a tenant is defined, the phone is allocated to that tenant. If a tenant is not defined, allocation is performed by best match*.
DHCP Server
3 HTTP Get default/tenant img and cfg file
4 HTTP REST Status
5 HTTP REST action (e.g. reset)
OC Server
6 REGISTER to Skype 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.

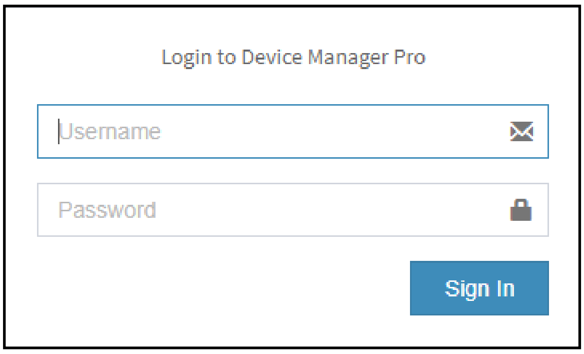
- To access the Device Manager Pro without running the OVOC, point your web browser to https://<OVOC_IP_Address>/ipp and then in the login screen that opens, log in. If the browser is pointed to HTTP, it will be redirected to HTTPS.
- Device Manager Pro is a secured web client that runs on any standard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

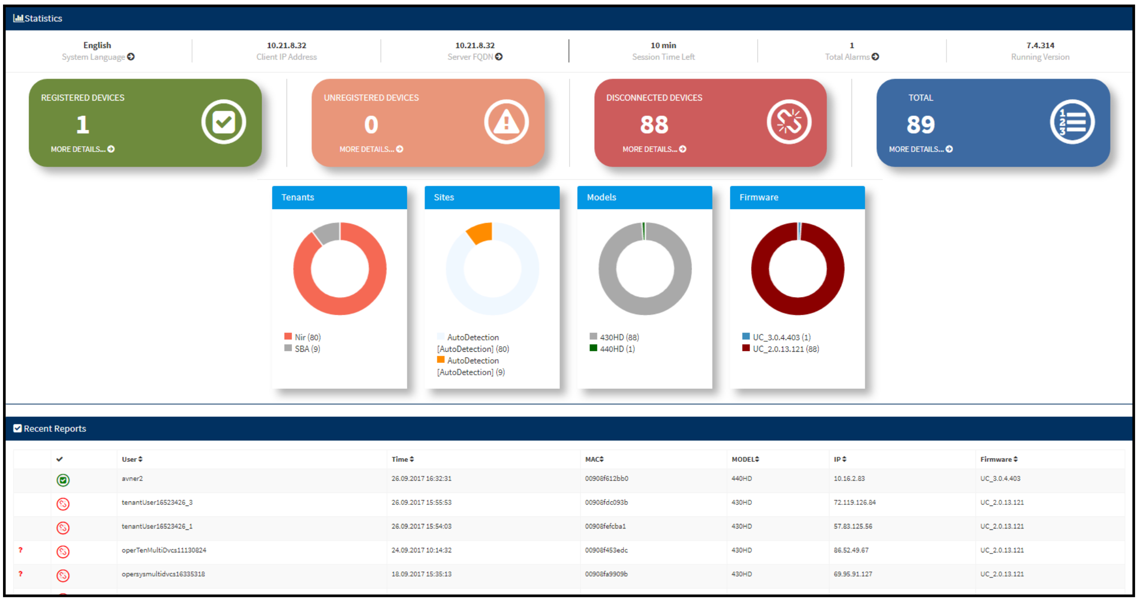
Figure 2-1: Login



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



Statistics

English	10.21.8.32	10.21.8.32	10 min	1	7.4.314
System Language	Client IP Address	Server FQDN	Session Time Left	Total Alarms	Running Version

REGISTERED DEVICES 1 MORE DETAILS...

UNREGISTERED DEVICES 0 MORE DETAILS...

DISCONNECTED DEVICES 88 MORE DETAILS...

TOTAL 89 MORE DETAILS...

Recent Reports

	✓	User	Time	MAC	MODEL	IP	Firmware
	✓	avner2	26.09.2017 16:32:31	00908f612bb0	440HD	10.16.2.83	UC_3.0.4.403
	⊘	tenantUser16523426_3	26.09.2017 15:55:53	00908fdc093b	430HD	72.119.126.84	UC_2.0.13.121
	⊘	tenantUser16523426_1	26.09.2017 15:54:03	00908fefcba1	430HD	57.83.125.56	UC_2.0.13.121
?	⊘	operTenMultiDvcs11130824	24.09.2017 10:14:32	00908f453edc	430HD	86.52.49.67	UC_2.0.13.121
?	⊘	opersysmultidvcs16335318	18.09.2017 15:35:13	00908fa9909b	430HD	69.95.91.127	UC_2.0.13.121

- See Monitoring and Maintaining the Phone Network on page 27 for more information about monitoring phones.
- The following topics show how to provision phones using Zero Touch.

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 8)
  - 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 10)
  - Import the csv file with users and devices back into Device Manager Pro (see Importing the csv File on page 10

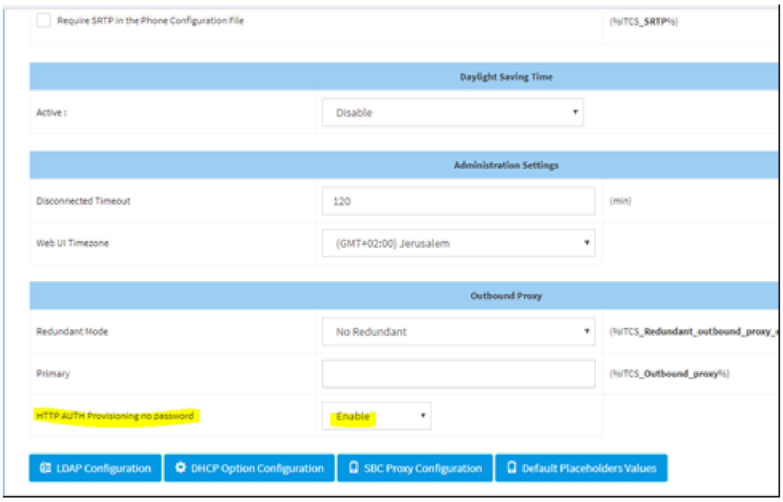
➢ To add *only* users:

> ⚠
> - 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



□ Require SRTP in the Phone Configuration File (%ITCS_SRTP%)

Daylight Saving Time

Active :	Disable	

Administration Settings

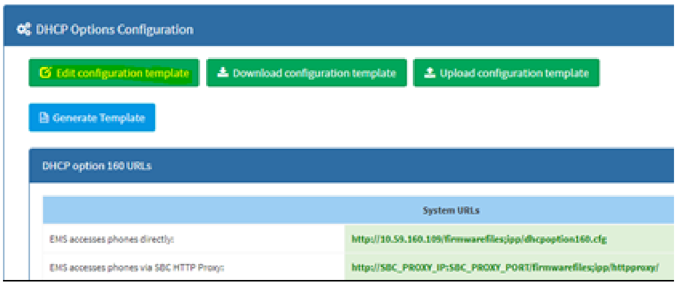
Disconnected Timeout	120	(min)
Web UI Timezone	(GMT+02:00) Jerusalem	

Outbound Proxy

Redundant Mode	No Redundant	(%ITCS_Redundant_outbound_proxy_
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** > **Devices Configuration** > **DHCP Options Configuration**)

Figure 3-2: DHCP Option Configuration



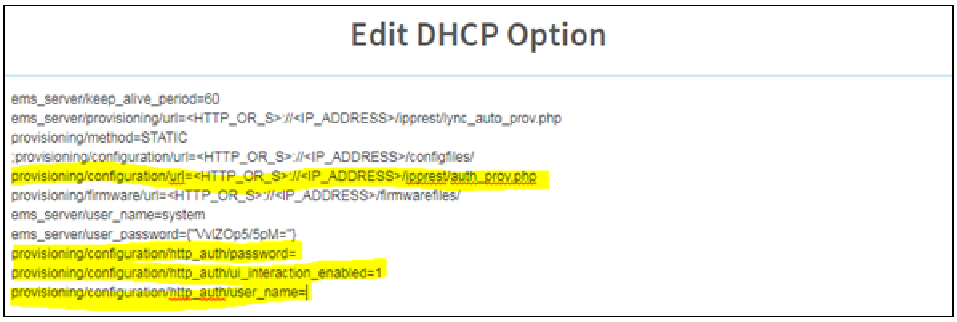
DHCP Options Configuration
Edit configuration template
Download configuration template
Upload configuration template
Generate Template
DHCP option 160 URLs

System URLs

EMS accesses phones directly:	http://10.59.160.109/firmwarefiles;ipp/dhcpoption160.cfg
EMS accesses phones via SBC HTTP Proxy:	http://SBC_PROXY_IP:SBC_PROXY_PORT/firmwarefiles;ipp/httpproxy/

6. Click **Edit configuration template**:

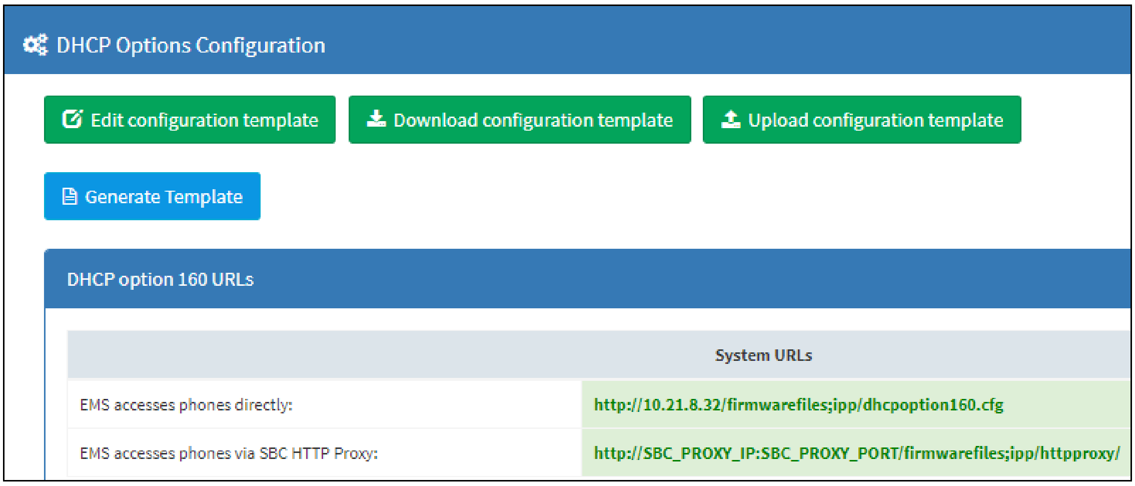
Figure 3-3: Edit DHCP Option



Edit DHCP Option

```
ems_server/keep_alive_period=60
ems_server/provisioning/url=<HTTP_OR_S>://<IP_ADDRESS>/ipprest/lync_auto_prov.php
provisioning/method=STATIC
;provisioning/configuration/url=<HTTP_OR_S>://<IP_ADDRESS>/configfiles/
provisioning/configuration/url=<HTTP_OR_S>://<IP_ADDRESS>/ipprest/auth_prov.php
provisioning/firmware/url=<HTTP_OR_S>://<IP_ADDRESS>/firmwarefiles/
ems_server/user_name=system
ems_server/user_password={"VvlZOp5/5pM="}
provisioning/configuration/http_auth/password=
provisioning/configuration/http_auth/ui_interaction_enabled=1
provisioning/configuration/http_auth/user_name=
```

7. Click **Generate Template**:



DHCP Options Configuration
Edit configuration template
Download configuration template
Upload configuration template
Generate Template
DHCP option 160 URLs

	System URLs
EMS accesses phones directly:	http://10.21.8.32/firmwarefiles;ipp/dhcpoption160.cfg
EMS accesses phones via SBC HTTP Proxy:	http://SBC_PROXY_IP:SBC_PROXY_PORT/firmwarefiles;ipp/httpproxy/

> ⚠ 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.

8. 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%
9. 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
10. 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**

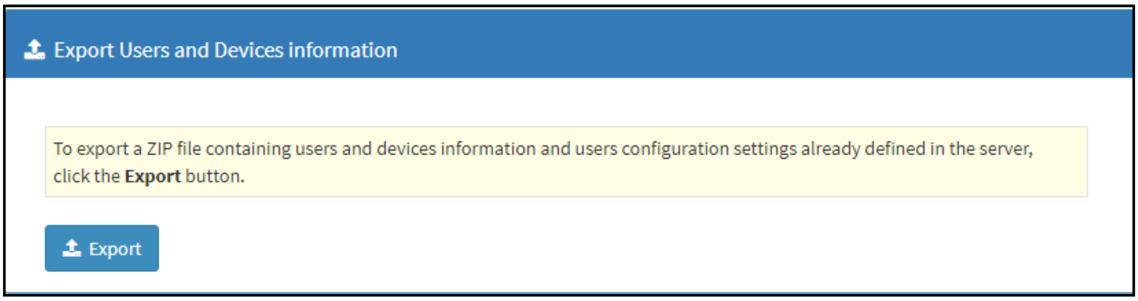
Exporting 'System User' to zip File

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

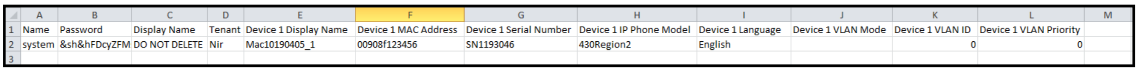


Export Users and Devices information

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.

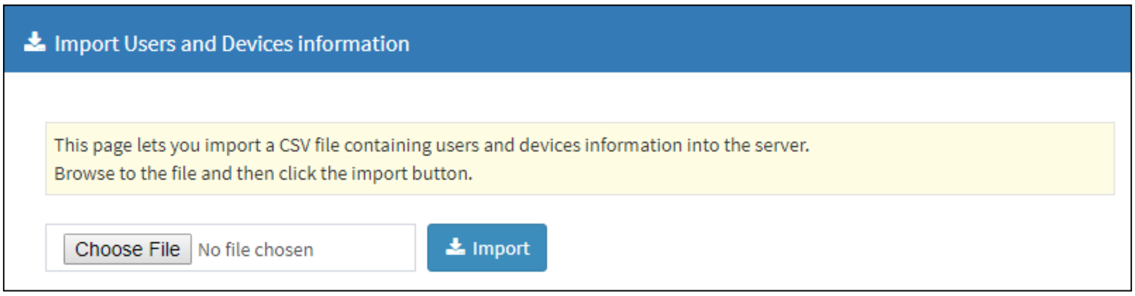
Importing the csv File

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.

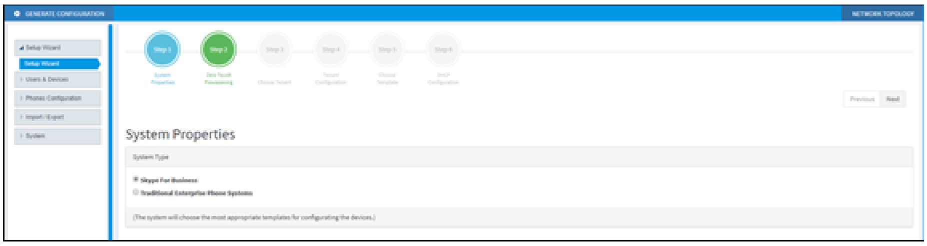
> Zero Touch provisioning *accelerates uptime* by enabling multiple users and phones to automatically be provisioned and added to the Manager.

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

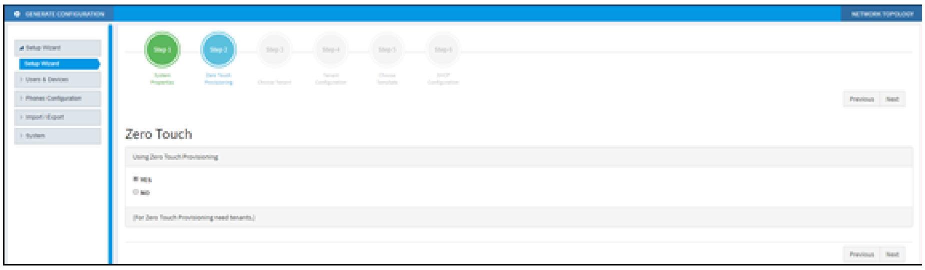
● Skype For Business
○ Traditional Enterprise Phone Systems

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

2. Select Skype for Business 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

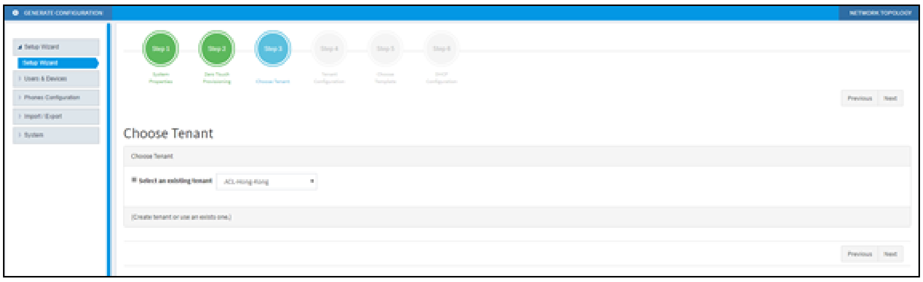
Using Zero Touch Provisioning

● YES
○ NO

(For Zero Touch Provisioning need tenants.)

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

Figure 4-3: Step 3 – Choose Tenant



Choose Tenant

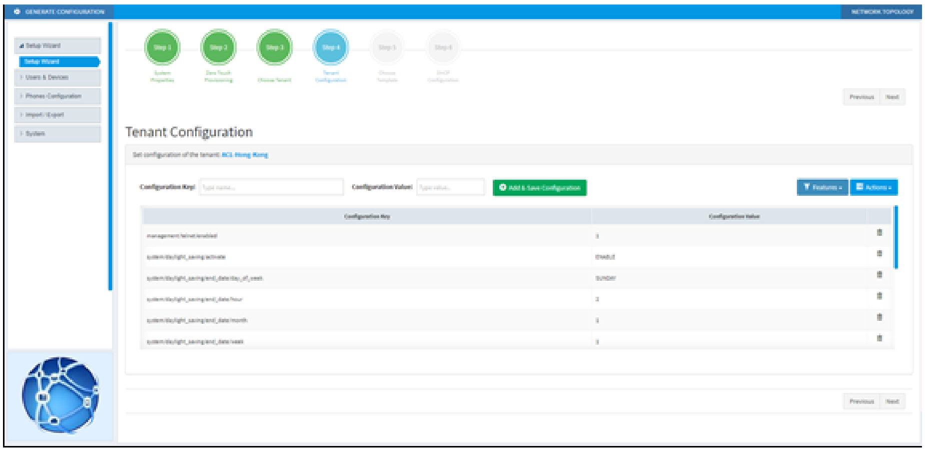
Choose Tenant

● 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

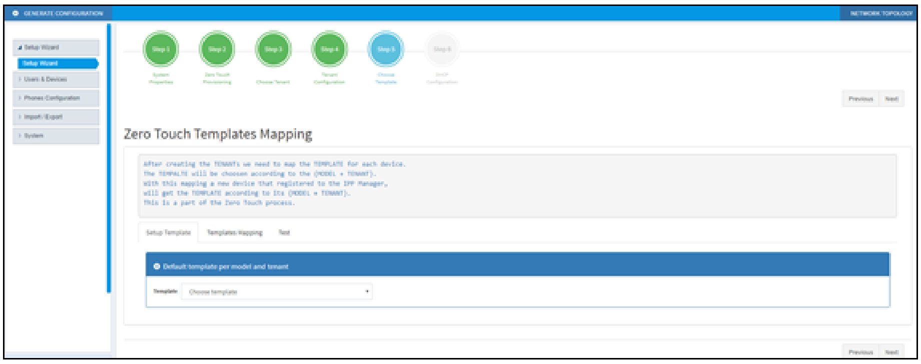
Set configuration of the tenant: ACL Hong Kong

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

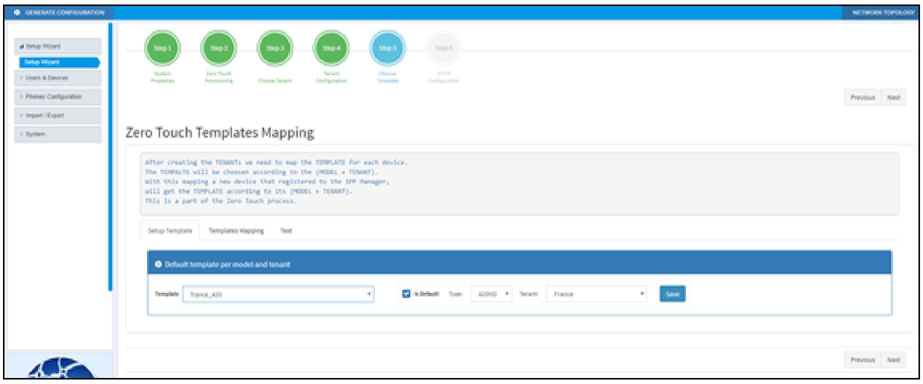
```
After creating the TENANTs we need to map the TEMPLATE for each device.
The TEMPALTE will be choosen according to the (MODEL + TENANT).
With this mapping a new device that registered to the IPP Manager,
will get the TEMPLATE according to its (MODEL + TENANT).
This is a part of the Zero Touch process.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

Default template per model and tenant

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 TEMPLATE 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.
```

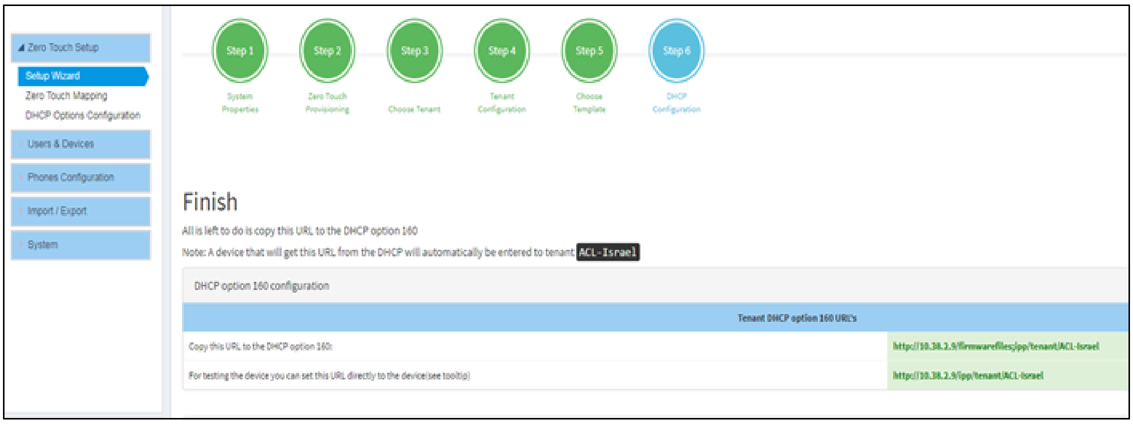
Default template per model and tenant

Template: France_420 ☑ Is Default Type: 420HD Tenant: France

This page is an alternative view to the Devices Configuration Templates page.

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. Define a tenant (see Defining a Tenant below).
2. Prepare a template per tenant (see Preparing a Template for a Tenant/Model on the next page).
3. Upload the firmware .img file to the server (see Uploading .img Firmware File to the Server on page 18).
4. 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 18).

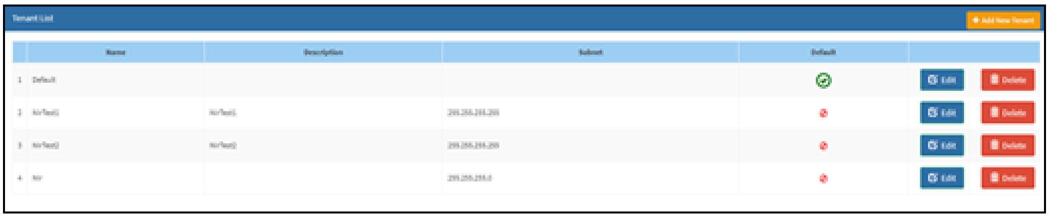
Defining a Tenant

You need to define a tenant before you can implement Zero Touch.

➢ **To define a tenant:**

1. Open the Tenant List page (Setup > System > Tenants).

Figure 5-1: Tenant List

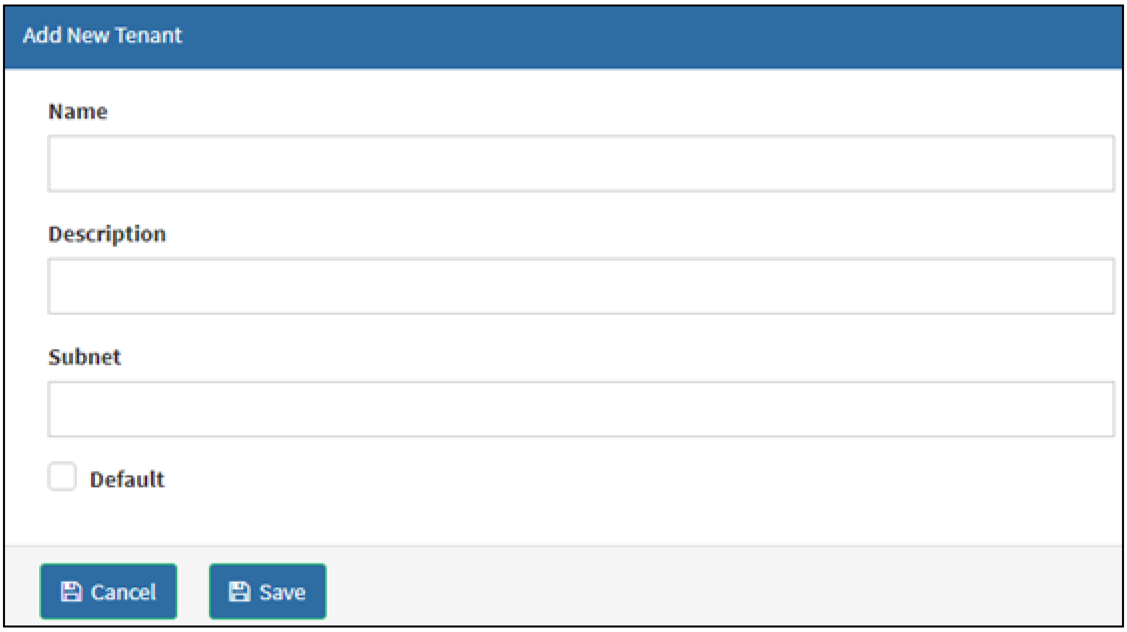


Tenant List

	Name	Description	Subnet	Default		
1	Default			✓	Edit	Delete
2	AirTest1	AirTest1	255.255.255.255	●	Edit	Delete
3	AirTest2	AirTest2	255.255.255.255	●	Edit	Delete
4	Air		255.255.255.0	●	Edit	Delete

2. Click the **+Add New Tenant** button.

Figure 5-2: Add New Tenant



Add New Tenant

Name

Description

Subnet

☐ Default

3. Use the table below as reference.

Table 5-1: Add New Tenant

Parameter	Description
Name	Enter an intuitive name to facilitate effective management later.
Description	Enter a tenant description to facilitate effective management later.
Subnet	Enter the tenant's subnet mask. Must be in prefix format x.x.x.x/y. For example: 255.255.0.0/16. For any region under the tenant, subnet mask is not mandatory, but if it is configured, its subnet mask must be within the tenant's, for example, 255.255.0.0/1.
Default	Defines the default tenant. Only this newly added tenant can be the default. The default is used for devices/endpoints auto-detection.

4. Click **Save**.

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

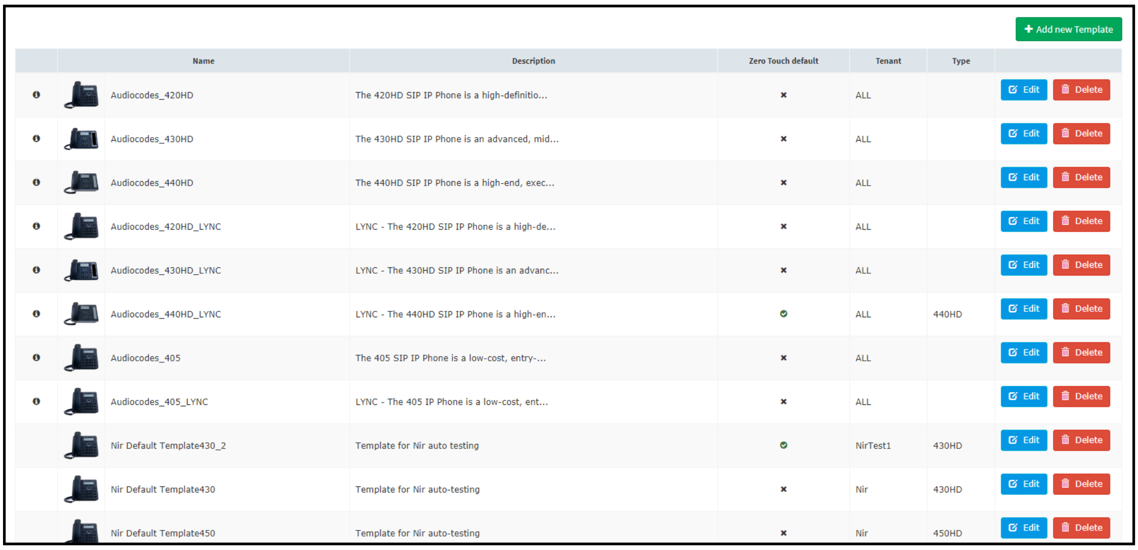
This saves the user from having to configure Speed Dials and Programmable Keys from the beginning. The user only needs to configure them once, initially.

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** > **Devices Configuration** > **Templates**).

Figure 5-3: Devices Configuration Templates



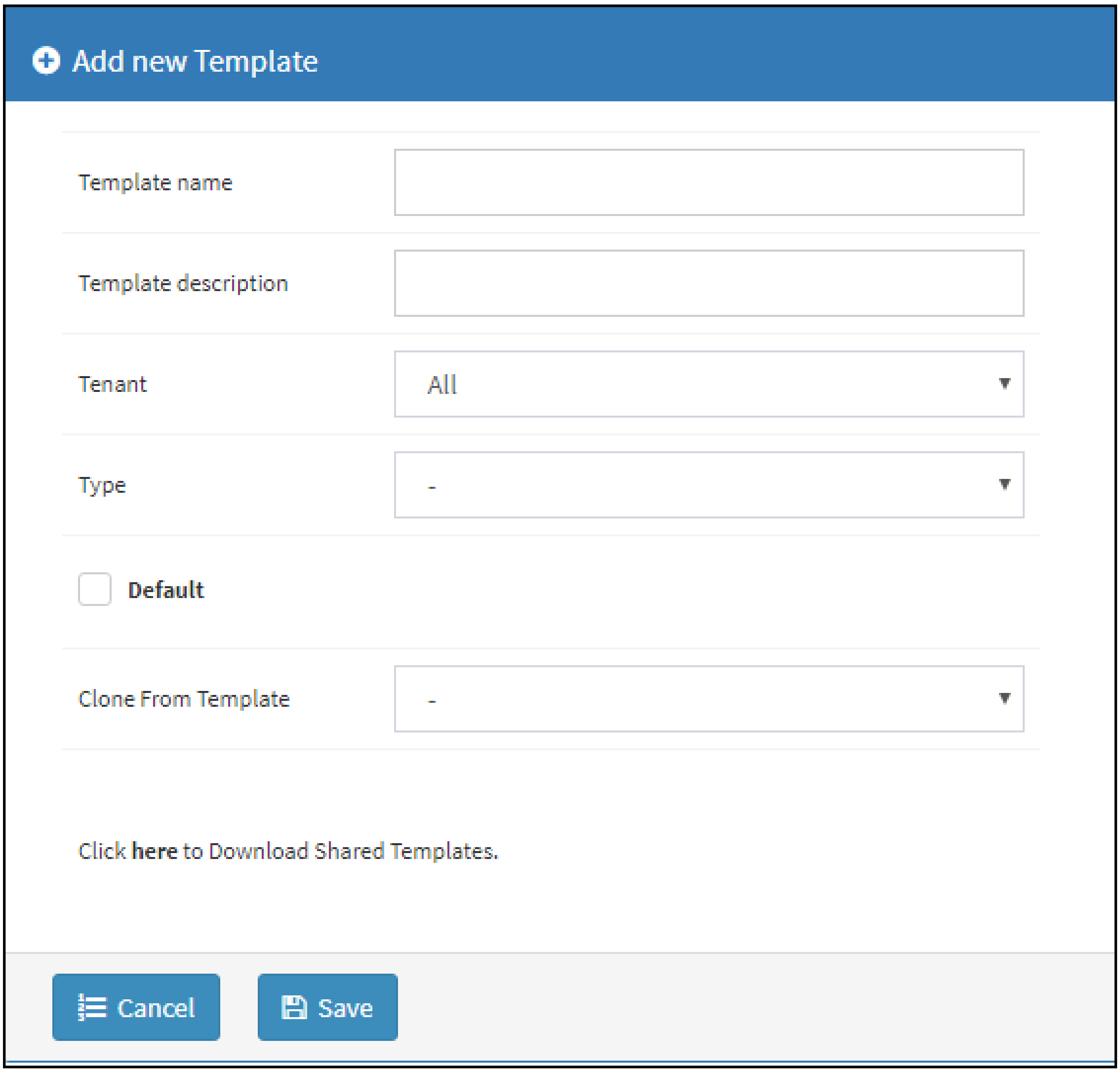
+ Add new Template

		Name	Description	Zero Touch default	Tenant	Type	
ℹ	☎	Audiocodes_420HD	The 420HD SIP IP Phone is a high-definitio...	✖	ALL		Edit Delete
ℹ	☎	Audiocodes_430HD	The 430HD SIP IP Phone is an advanced, mid...	✖	ALL		Edit Delete
ℹ	☎	Audiocodes_440HD	The 440HD SIP IP Phone is a high-end, exec...	✖	ALL		Edit Delete
ℹ	☎	Audiocodes_420HD_LYNC	LYNC - The 420HD SIP IP Phone is a high-de...	✖	ALL		Edit Delete
ℹ	☎	Audiocodes_430HD_LYNC	LYNC - The 430HD SIP IP Phone is an advanc...	✖	ALL		Edit Delete
ℹ	☎	Audiocodes_440HD_LYNC	LYNC - The 440HD SIP IP Phone is a high-en...	✓	ALL	440HD	Edit Delete
ℹ	☎	Audiocodes_405	The 405 SIP IP Phone is a low-cost, entry-...	✖	ALL		Edit Delete
ℹ	☎	Audiocodes_405_LYNC	LYNC - The 405 IP Phone is a low-cost, ent...	✖	ALL		Edit Delete
	☎	Nir Default Template430_2	Template for Nir auto testing	✓	NirTest1	430HD	Edit Delete
	☎	Nir Default Template430	Template for Nir auto-testing	✖	Nir	430HD	Edit Delete
	☎	Nir Default Template450	Template for Nir auto-testing	✖	Nir	450HD	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: - ▾

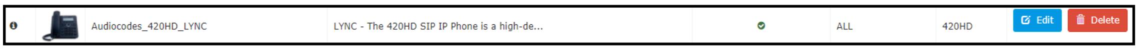
□ **Default**

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. 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



ℹ		Audiocodes_420HD_LYNC	LYNC - The 420HD SIP IP Phone is a high-de...	✓	ALL	420HD	Edit Delete

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.

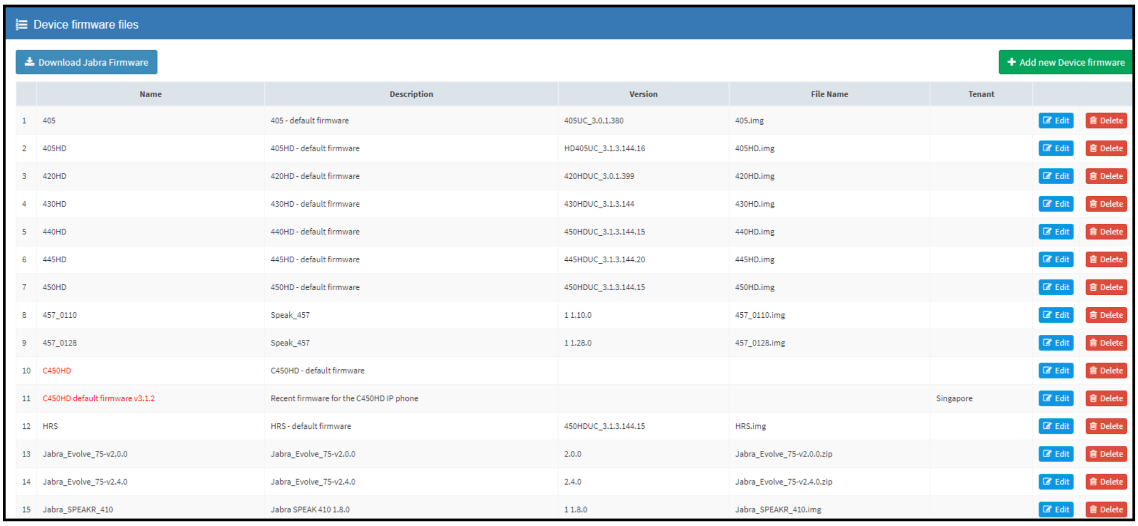
Uploading .img Firmware File to the Server

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** > **Devices Configuration** > **Firmware Files**).

Figure 5-6: Phone Firmware Files



	Name	Description	Version	File Name	Tenant	
1	405	405 - default firmware	405UC_3.0.1.380	405.img		Edit Delete
2	405HD	405HD - default firmware	HD405UC_3.1.3.144.16	405HD.img		Edit Delete
3	420HD	420HD - default firmware	420HDUC_3.0.1.399	420HD.img		Edit Delete
4	430HD	430HD - default firmware	430HDUC_3.1.3.144	430HD.img		Edit Delete
5	440HD	440HD - default firmware	450HDUC_3.1.3.144.15	440HD.img		Edit Delete
6	445HD	445HD - default firmware	445HDUC_3.1.3.144.20	445HD.img		Edit Delete
7	450HD	450HD - default firmware	450HDUC_3.1.3.144.15	450HD.img		Edit Delete
8	457_0110	Speak_457	1 1.10.0	457_0110.img		Edit Delete
9	457_0128	Speak_457	1 1.28.0	457_0128.img		Edit Delete
10	C450HD	C450HD - default firmware				Edit Delete
11	C450HD default firmware v3.1.2	Recent firmware for the C450HD IP phone			Singapore	Edit Delete
12	HRS	HRS - default firmware	450HDUC_3.1.3.144.15	HRS.img		Edit Delete
13	Jabra_Evolve_75-v2.0.0	Jabra_Evolve_75-v2.0.0	2.0.0	Jabra_Evolve_75-v2.0.0.zip		Edit Delete
14	Jabra_Evolve_75-v2.4.0	Jabra_Evolve_75-v2.4.0	2.4.0	Jabra_Evolve_75-v2.4.0.zip		Edit Delete
15	Jabra_SPEAKR_410	Jabra SPEAK 410 1.8.0	1 1.8.0	Jabra_SPEAKR_410.img		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

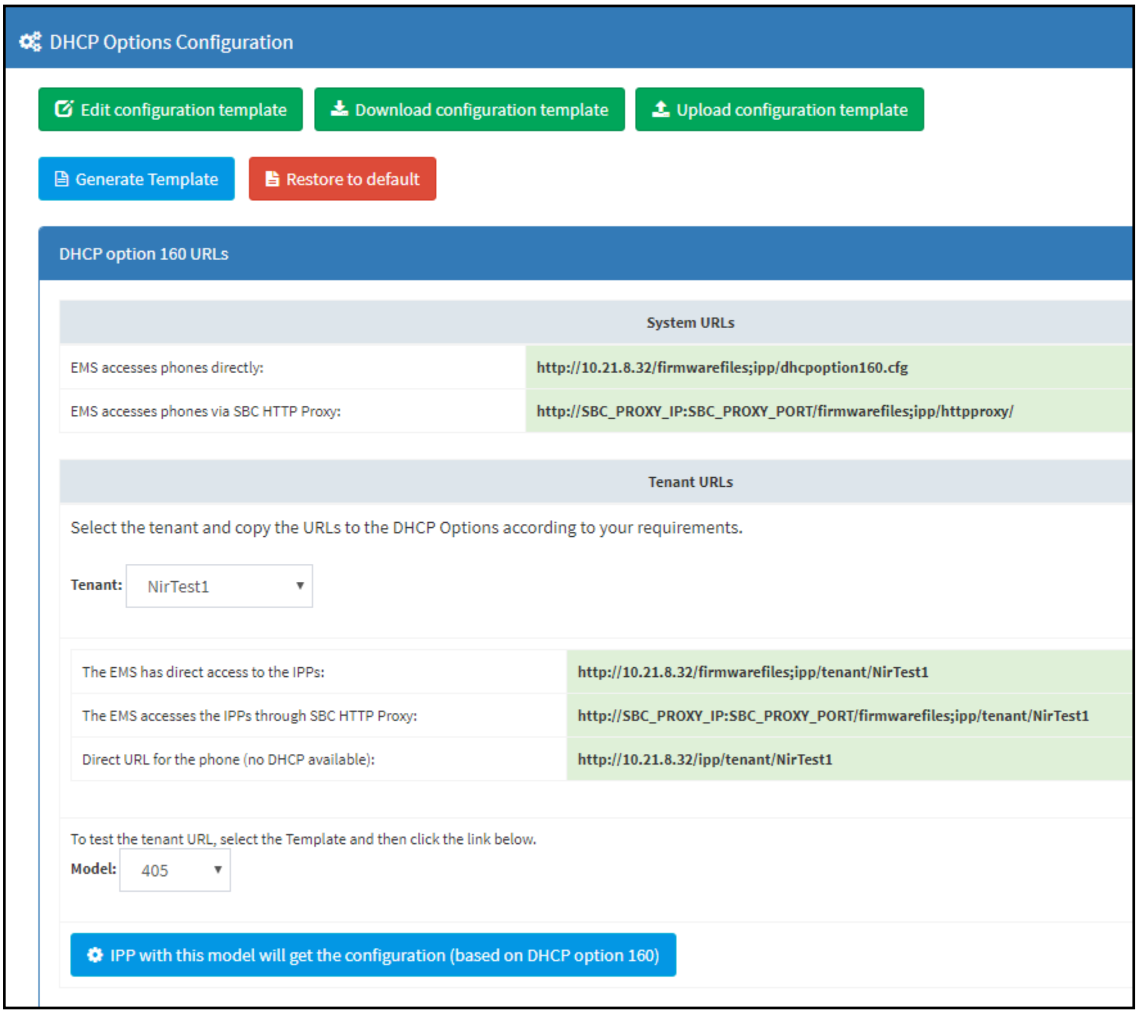
> ⚠ The Device Manager Pro supports backward compatibility so you can point DHCP Option 160 to a region URL. See the *Administrator's Manual* v7.2 and earlier.

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 System Settings page (**Setup** > **Devices Configuration** > **System Settings**).
2. Click the **DHCP Option Configuration** button.
3. In the DHCP Option Configuration dialog that opens, click the **DHCP Option 160 URLs** link located lowermost in the dialog; the dialog extends to display System URLs and Tenant URLs screen sections.
4. Under the Tenant URLs section, select the tenant (in which the phones are located) from the 'Tenant' dropdown list.

Figure 5-7: Tenant URL


DHCP Options Configuration
Edit configuration template
Download configuration template
Upload configuration template
Generate Template
Restore to default
DHCP option 160 URLs

System URLs	
EMS accesses phones directly:	http://10.21.8.32/firmwarefiles;ipp/dhcpoption160.cfg
EMS accesses phones via SBC HTTP Proxy:	http://SBC_PROXY_IP:SBC_PROXY_PORT/firmwarefiles;ipp/httpproxy/

Tenant URLs

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

Tenant: NirTest1

The EMS has direct access to the IPPs:	http://10.21.8.32/firmwarefiles;ipp/tenant/NirTest1
The EMS accesses the IPPs through SBC HTTP Proxy:	http://SBC_PROXY_IP:SBC_PROXY_PORT/firmwarefiles;ipp/tenant/NirTest1
Direct URL for the phone (no DHCP available):	http://10.21.8.32/ipp/tenant/NirTest1

To test the tenant URL, select the Template and then click the link below.

Model: 405

IPP with this model will get the configuration (based on DHCP option 160)

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.

1. 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>**
   - **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.

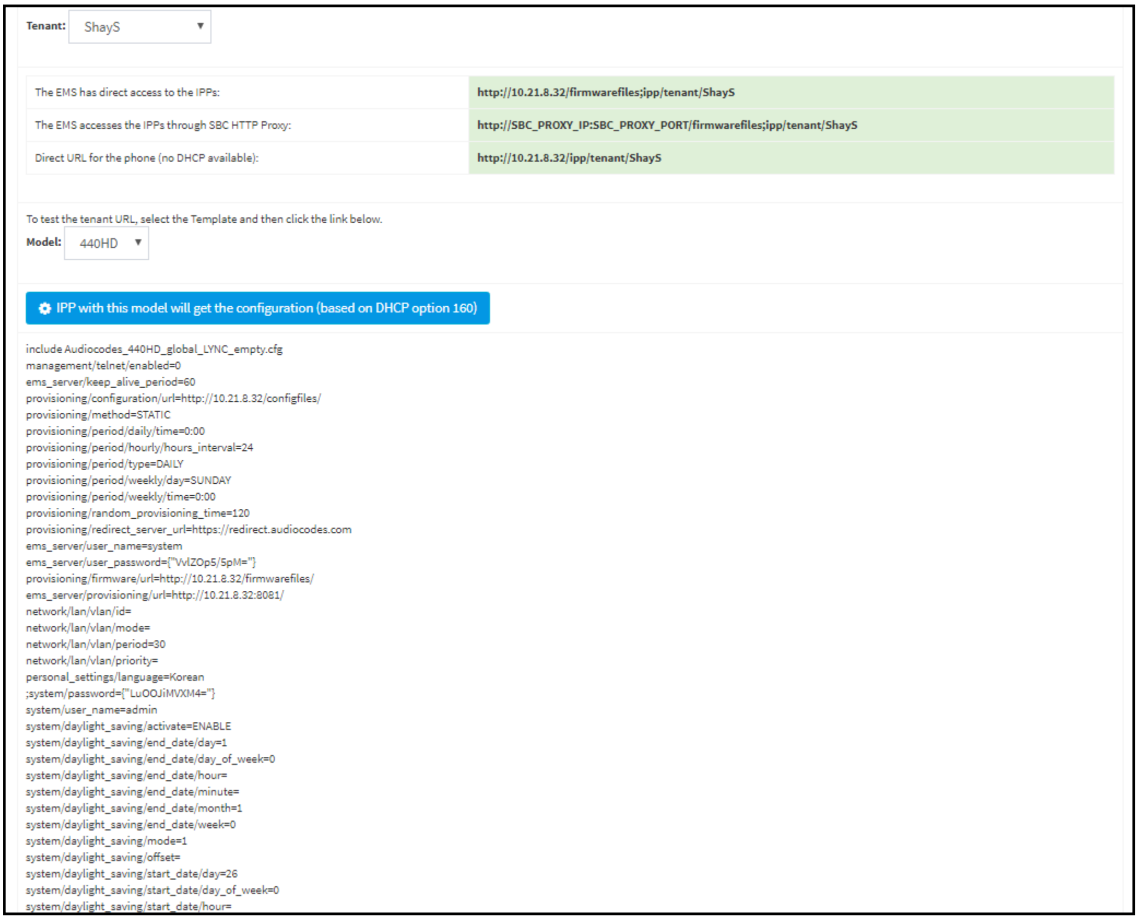
> - Configure DHCP Option 160 to point to the OVOC provisioning server's URL if the phones are not behind a NAT. DHCP Option 66/67 can also be used.
> - If the phones reside behind a NAT and an SBC HTTP proxy is available, configure DHCP Option 160 to point to the SBC HTTP proxy; phone-OVOC communications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

2. 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



Tenant: ShayS ▾

The EMS has direct access to the IPPs:	**http://10.21.8.32/firmwarefiles;ipp/tenant/ShayS**
The EMS accesses the IPPs through SBC HTTP Proxy:	**http://SBC_PROXY_IP:SBC_PROXY_PORT/firmwarefiles;ipp/tenant/ShayS**
Direct URL for the phone (no DHCP available):	**http://10.21.8.32/ipp/tenant/ShayS**

To test the tenant URL, select the Template and then click the link below.

Model: 440HD ▾

IPP with this model will get the configuration (based on DHCP option 160)

```
include Audiocodes_440HD_global_LYNC_empty.cfg
management/telnet/enabled=0
ems_server/keep_alive_period=60
provisioning/configuration/url=http://10.21.8.32/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=http://10.21.8.32/firmwarefiles/
ems_server/provisioning/url=http://10.21.8.32:8081/
network/lan/vlan/id=
network/lan/vlan/mode=
network/lan/vlan/period=30
network/lan/vlan/priority=
personal_settings/language=Korean
;system/password={"LuOOJiMVXM4="}
system/user_name=admin
system/daylight_saving/activate=ENABLE
system/daylight_saving/end_date/day=1
system/daylight_saving/end_date/day_of_week=0
system/daylight_saving/end_date/hour=
system/daylight_saving/end_date/minute=
system/daylight_saving/end_date/month=1
system/daylight_saving/end_date/week=0
system/daylight_saving/mode=1
system/daylight_saving/offset=
system/daylight_saving/start_date/day=26
system/daylight_saving/start_date/day_of_week=0
system/daylight_saving/start_date/hour=
```

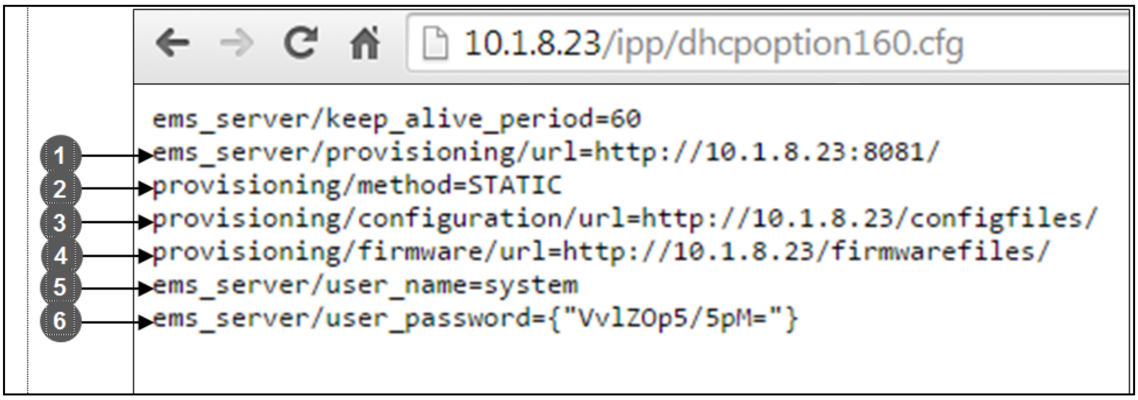
Zero Touch is supported for phones with sign-in capabilities only.

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



```
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.

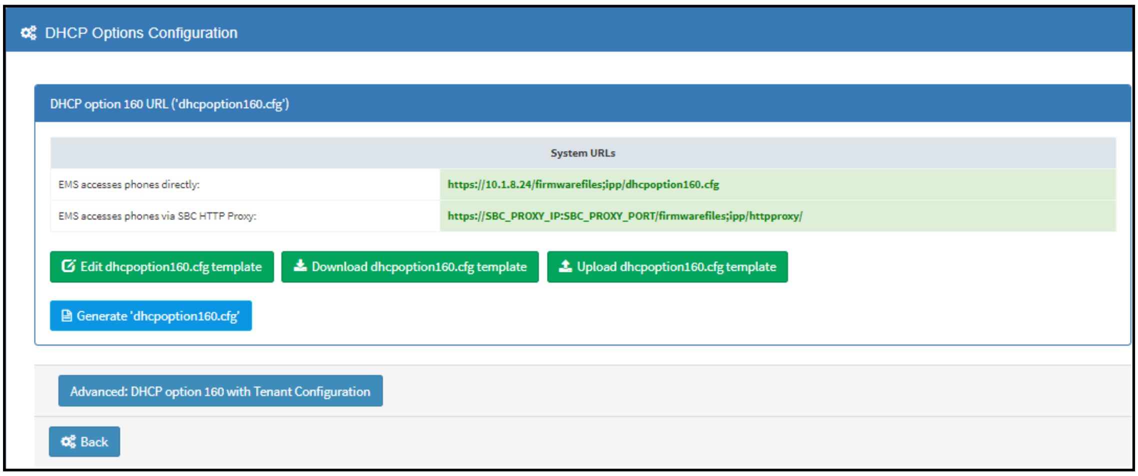
Editing the DHCP Option 160 cfg File

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** > **Devices Configuration** > **System Settings**).
2. Click the **DHCP Option Configuration** button.

Figure 5-10: DHCP Option Configuration

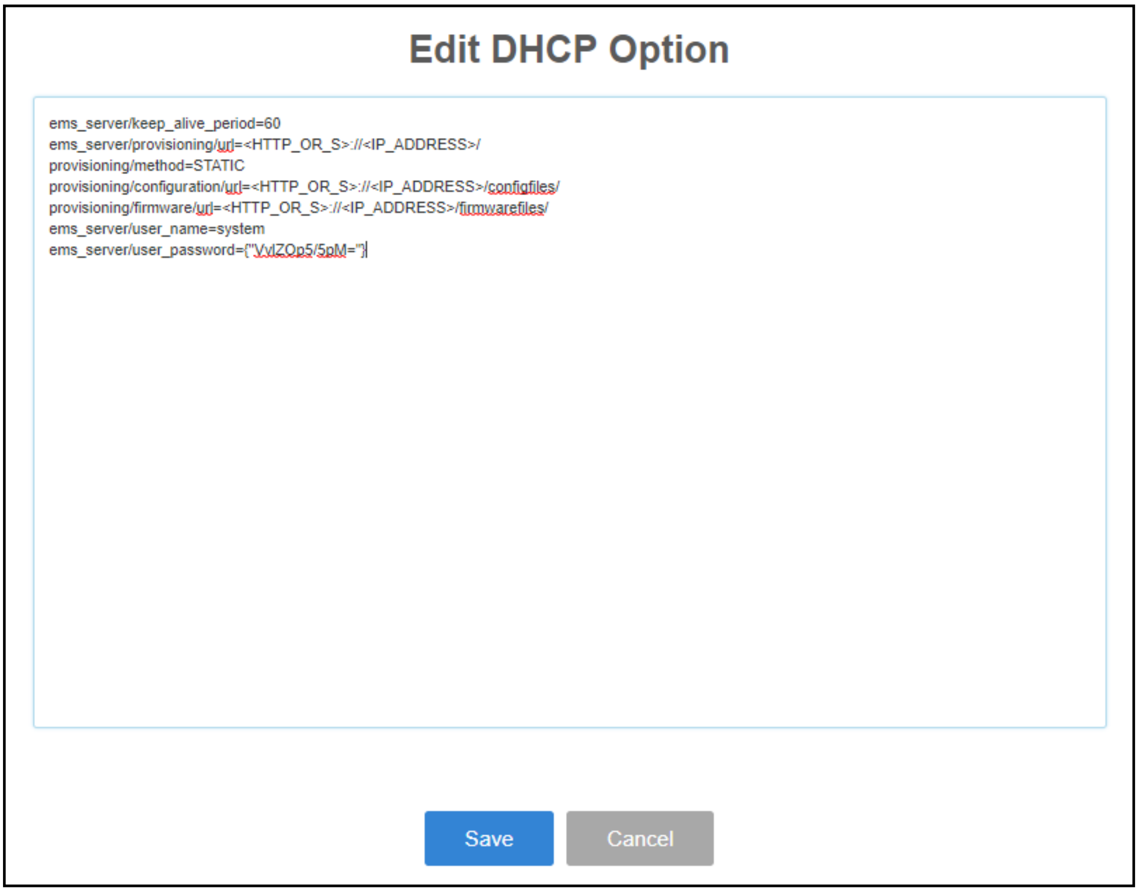


DHCP Options Configuration
DHCP option 160 URL ('dhcpoption160.cfg')
Edit dhcpoption160.cfg template
Download dhcpoption160.cfg template
Upload dhcpoption160.cfg template
Generate 'dhcpoption160.cfg'
Advanced: DHCP option 160 with Tenant Configuration
Back

System URLs	
EMS accesses phones directly:	https://10.1.8.24/firmwarefiles;ipp/dhcpoption160.cfg
EMS accesses phones via SBC HTTP Proxy:	https://SBC_PROXY_IP:SBC_PROXY_PORT/firmwarefiles;ipp/httpproxy/

3. Click the **Edit cfg template** button.

Figure 5-11: Edit DHCP Option



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="}
```

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

Table 5-2: 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).
Provisioning Firmware URL	Defines the URL of the location of the firmware files (including IP address and port) in the provisioning server (OVOC server).

Parameter	Description
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.

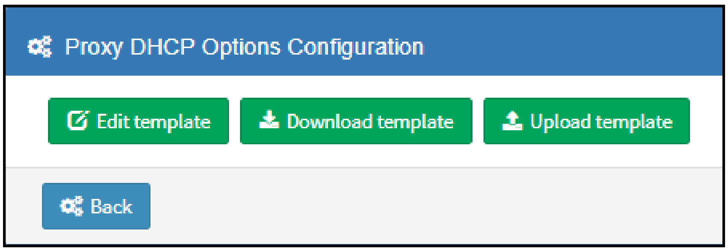
Editing the SBC HTTP Proxy

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** > **Devices Configuration** > **System Settings**) and then in the page click 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 in the previous section.
3. Click **Save**.

6 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:

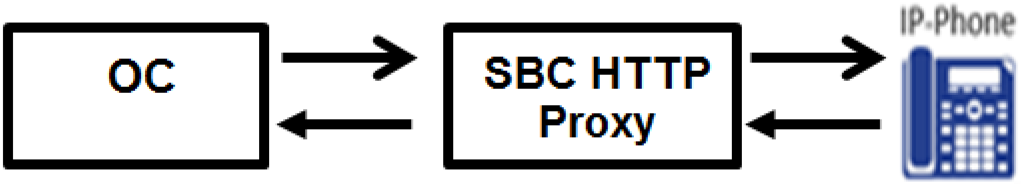
- Alarms and statuses can be sent from the phones to the Device Manager Pro, i.e., REST requests originate from the phone and the OVOC functions as a REST server.
- The Device Manager Pro can perform auto-discovery of the endpoints for the purpose of uploading configuration and firmware files.
- 'Actions' 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').

7 Monitoring and Maintaining the Phone Network

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

Monitoring the Network from the Dashboard

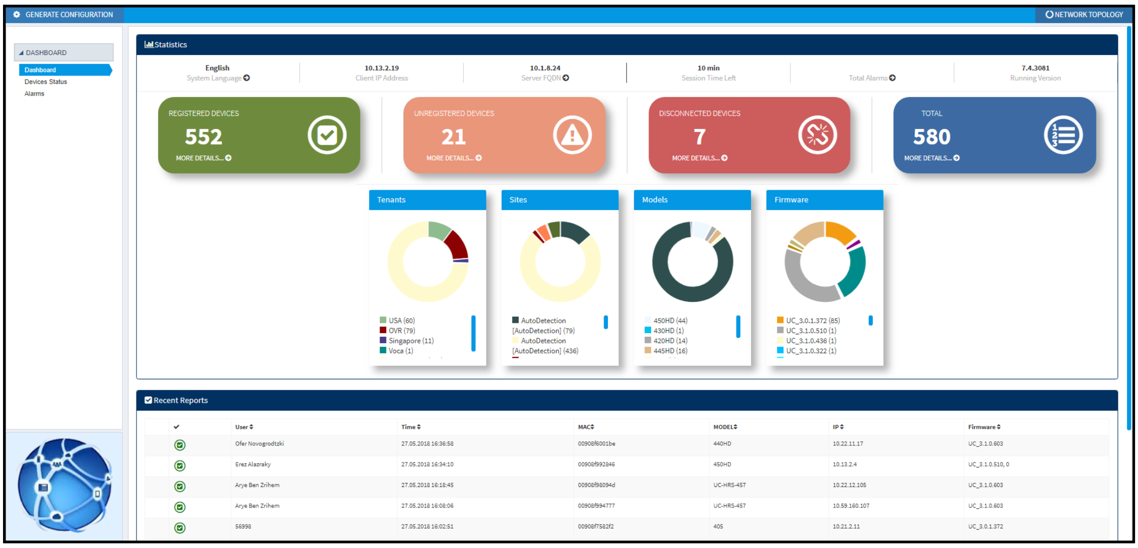
The Dashboard page lets you quickly identify

- 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:

- Under the **Monitor** tab, click **Dashboard** > **Dashboard**.

Figure 7-1: Dashboard



English	10.13.2.19	10.1.8.24	10 min		7.4.3081
System Language	Client IP Address	Server FQDN	Session Time Left	Total Alarms	Running Version

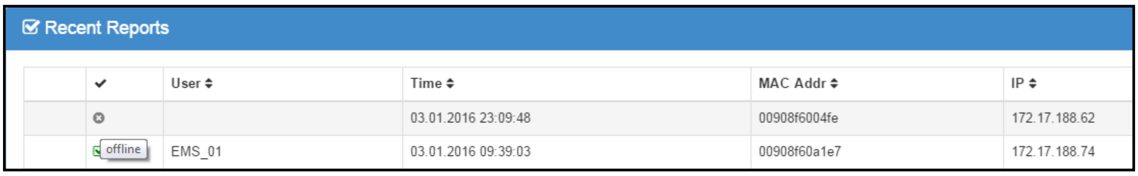
REGISTERED DEVICES 552 MORE DETAILS...
UNREGISTERED DEVICES 21 MORE DETAILS...
DISCONNECTED DEVICES 7 MORE DETAILS...
TOTAL 580 MORE DETAILS...

Recent Reports

✓	User	Time	MAC	MODEL	IP	Firmware
✓	Ofer Novogrodtzki	27.05.2018 16:36:58	00908f6001be	440HD	10.22.11.17	UC_3.1.0.603
✓	Erez Alazraky	27.05.2018 16:34:10	00908f992846	450HD	10.13.2.4	UC_3.1.0.510, 0
✓	Arye Ben Zrihem	27.05.2018 16:18:45	00908f98094d	UC-HRS-457	10.22.12.105	UC_3.1.0.603
✓	Arye Ben Zrihem	27.05.2018 16:08:06	00908f994777	UC-HRS-457	10.59.160.107	UC_3.1.0.603
✓	56998	27.05.2018 16:02:51	00908f7582f2	405	10.21.2.11	UC_3.0.1.372

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

Figure 7-2: Dashboard - Skype for Business IP Phone Offline

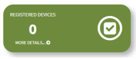
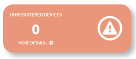
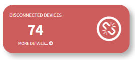
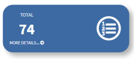
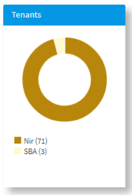
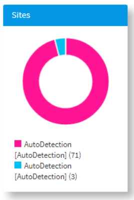
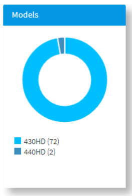
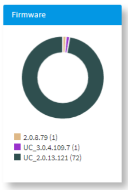


Recent Reports

	✓	User	Time	MAC Addr	IP
	⊗		03.01.2016 23:09:48	00908f6004fe	172.17.188.62
	offline	EMS_01	03.01.2016 09:39:03	00908f60a1e7	172.17.188.74

- 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 7-1: 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.
	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

A **Network Topology** link in the uppermost right corner of the Dashboard page allows administrators to view a snapshot of the network's tenants and subnets.

Figure 7-3: Network Topology Link

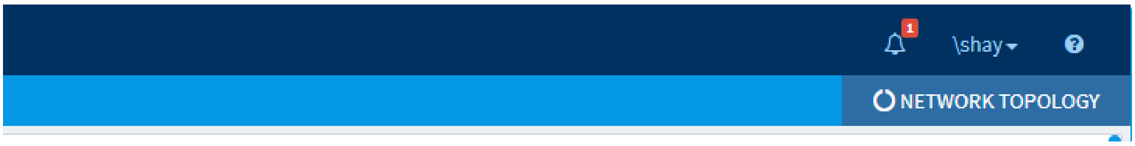
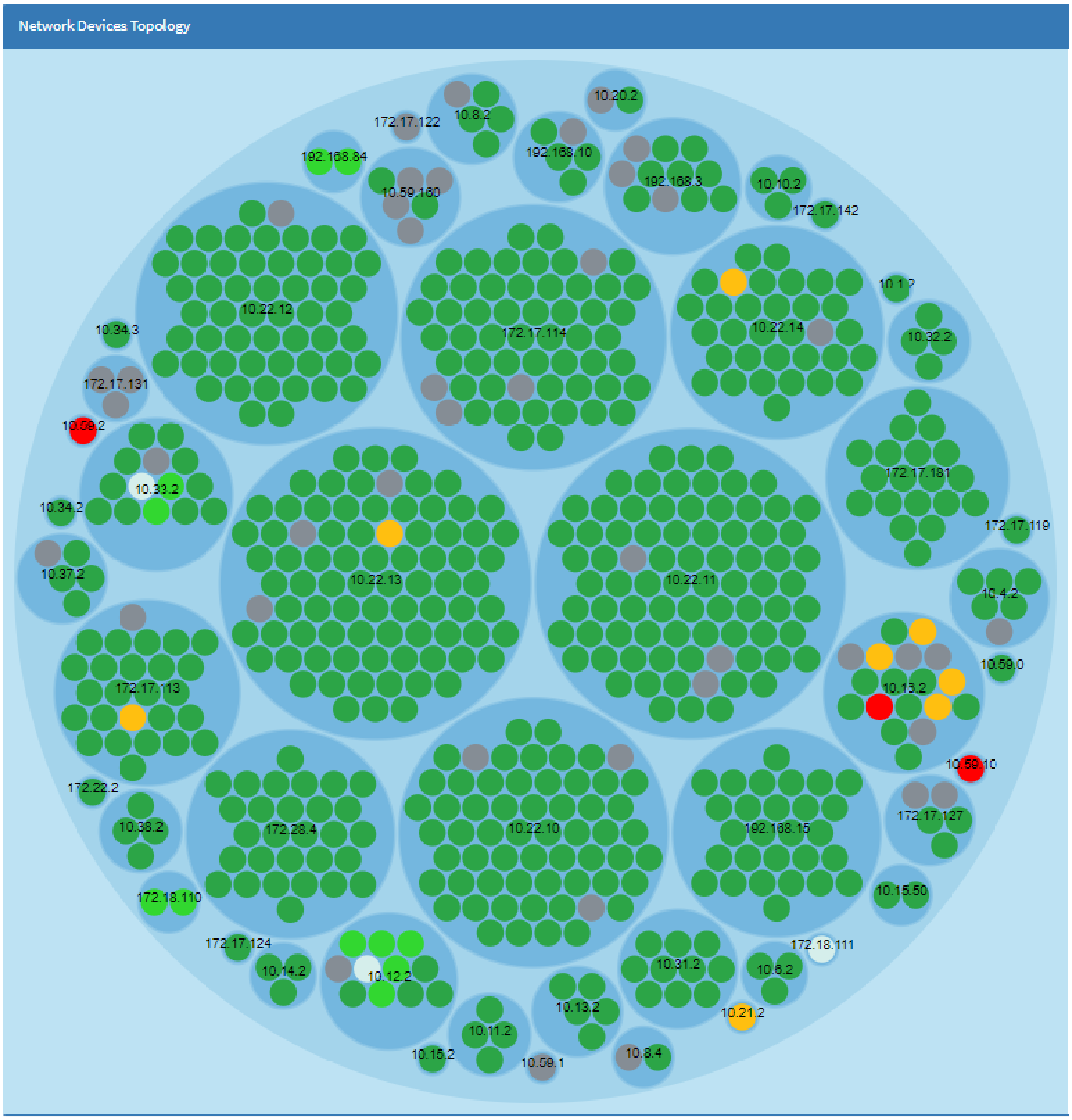


Figure 7-4: Network Topology Page



The page shown above displays a single-tenant network. Devices are divided according to subnets. The page allows administrators to determine at a glance which subnets are causing traffic overload (for example). Administrators can point their mouse at a device in a subnet to view information presented in a tool tip on that device.

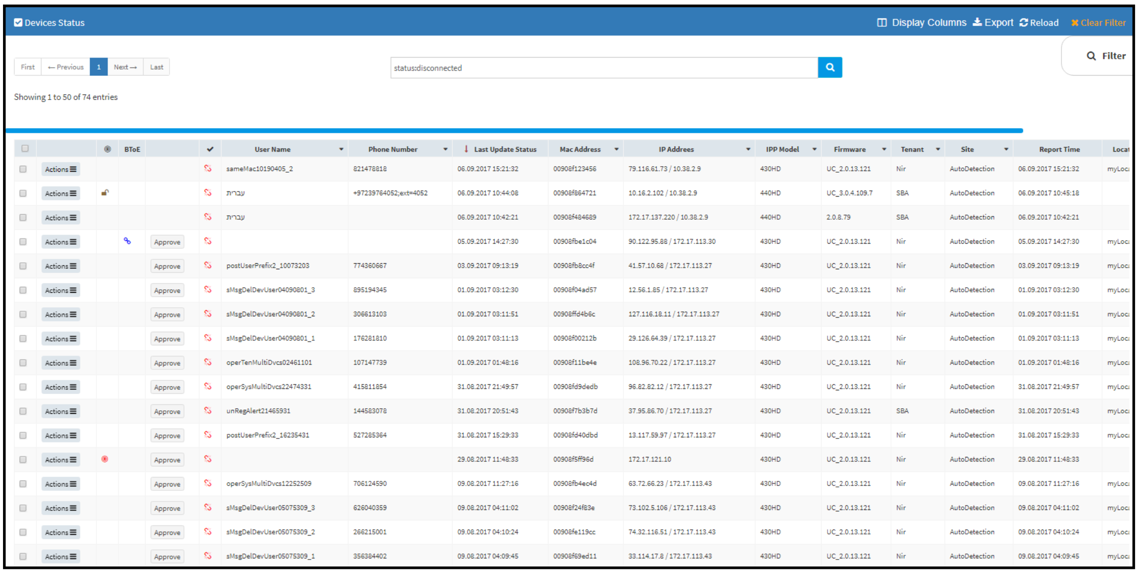
Checking Devices Status

The Devices Status page lets you check a device's status.

➢ **To check a device's status:**

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

Figure 7-5: Devices Status



☑ Devices Status

Display Columns Export Reload ✖ Clear Filter

First ← Previous 1 Next → Last

status:disconnected

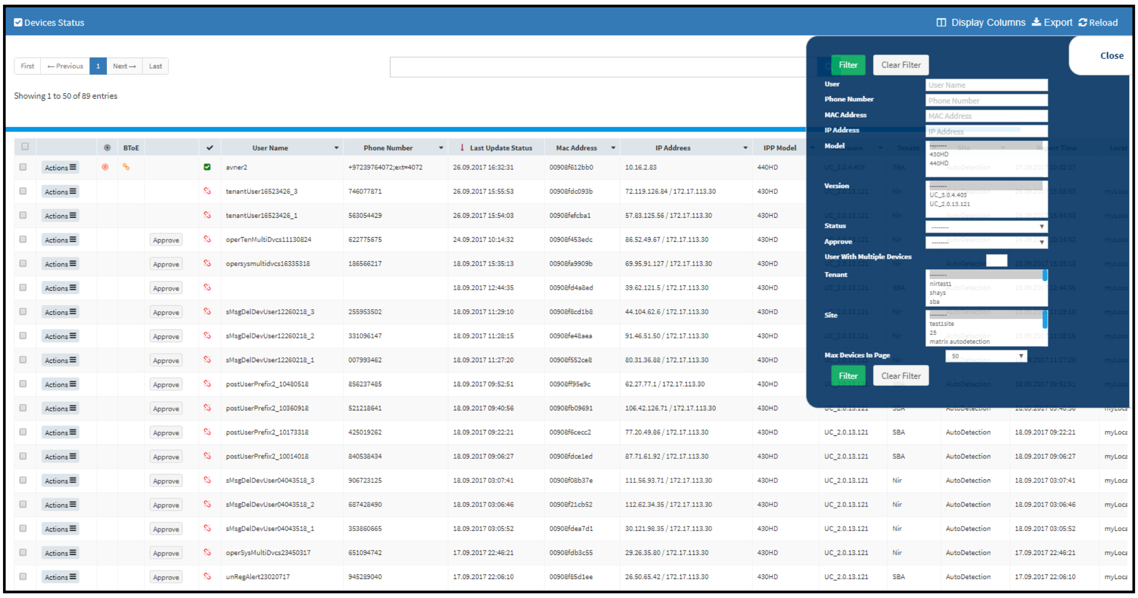
Filter

Showing 1 to 50 of 74 entries

□		⊛	BToE		✔	User Name	Phone Number	Last Update Status	Mac Address	IP Addrees	IPP Model	Firmware	Tenant	Site	Report Time	Locat
□	Actions ≡				✗	sameMac10190405_2	821478818	06.09.2017 15:21:32	00908f123456	79.116.61.73 / 10.38.2.9	430HD	UC_2.0.13.121	Nir	AutoDetection	06.09.2017 15:21:32	myLoca
□	Actions ≡	🔓			✗	עברית	+97239764052;ext=4052	06.09.2017 10:44:08	00908f864721	10.16.2.102 / 10.38.2.9	440HD	UC_3.0.4.109.7	SBA	AutoDetection	06.09.2017 10:45:18	
□	Actions ≡				✗	עברית		06.09.2017 10:42:21	00908f484689	172.17.137.220 / 10.38.2.9	440HD	2.0.8.79	SBA	AutoDetection	06.09.2017 10:42:21	
□	Actions ≡		🔗	Approve	✗			05.09.2017 14:27:30	00908fbe1c04	90.122.95.88 / 172.17.113.30	430HD	UC_2.0.13.121	Nir	AutoDetection	05.09.2017 14:27:30	myLoca
□	Actions ≡			Approve	✗	postUserPrefix2_10073203	774360667	03.09.2017 09:13:19	00908fb8cc4f	41.57.10.68 / 172.17.113.27	430HD	UC_2.0.13.121	Nir	AutoDetection	03.09.2017 09:13:19	myLoca
□	Actions ≡			Approve	✗	sMsgDelDevUser04090801_3	895194345	01.09.2017 03:12:30	00908f04ad57	12.56.1.85 / 172.17.113.27	430HD	UC_2.0.13.121	Nir	AutoDetection	01.09.2017 03:12:30	myLoca
□	Actions ≡			Approve	✗	sMsgDelDevUser04090801_2	306613103	01.09.2017 03:11:51	00908ffd4b6c	127.116.18.11 / 172.17.113.27	430HD	UC_2.0.13.121	Nir	AutoDetection	01.09.2017 03:11:51	myLoca
□	Actions ≡			Approve	✗	sMsgDelDevUser04090801_1	176281810	01.09.2017 03:11:13	00908f00212b	29.126.64.39 / 172.17.113.27	430HD	UC_2.0.13.121	Nir	AutoDetection	01.09.2017 03:11:13	myLoca
□	Actions ≡			Approve	✗	operTenMultiDvcs02461101	107147739	01.09.2017 01:48:16	00908f11be4e	108.96.70.22 / 172.17.113.27	430HD	UC_2.0.13.121	Nir	AutoDetection	01.09.2017 01:48:16	myLoca
□	Actions ≡			Approve	✗	operSysMultiDvcs22474331	415811854	31.08.2017 21:49:57	00908fd9dedb	96.82.82.12 / 172.17.113.27	430HD	UC_2.0.13.121	Nir	AutoDetection	31.08.2017 21:49:57	myLoca
□	Actions ≡			Approve	✗	unRegAlert21465931	144583078	31.08.2017 20:51:43	00908f7b3b7d	37.95.86.70 / 172.17.113.27	430HD	UC_2.0.13.121	SBA	AutoDetection	31.08.2017 20:51:43	myLoca
□	Actions ≡			Approve	✗	postUserPrefix2_16235431	527285364	31.08.2017 15:29:33	00908fd40dbd	13.117.59.97 / 172.17.113.27	430HD	UC_2.0.13.121	Nir	AutoDetection	31.08.2017 15:29:33	myLoca
□	Actions ≡	●		Approve	✗			29.08.2017 11:48:33	00908f5ff96d	172.17.121.10	430HD	UC_2.0.13.121	Nir	AutoDetection	29.08.2017 11:48:33	
□	Actions ≡			Approve	✗	operSysMultiDvcs12252509	706124590	09.08.2017 11:27:16	00908fb4ec4d	63.72.66.23 / 172.17.113.43	430HD	UC_2.0.13.121	Nir	AutoDetection	09.08.2017 11:27:16	myLoca
□	Actions ≡			Approve	✗	sMsgDelDevUser05075309_3	626040359	09.08.2017 04:11:02	00908f24f83e	73.102.5.106 / 172.17.113.43	430HD	UC_2.0.13.121	Nir	AutoDetection	09.08.2017 04:11:02	myLoca
□	Actions ≡			Approve	✗	sMsgDelDevUser05075309_2	266215001	09.08.2017 04:10:24	00908fe119cc	74.32.116.51 / 172.17.113.43	430HD	UC_2.0.13.121	Nir	AutoDetection	09.08.2017 04:10:24	myLoca
□	Actions ≡			Approve	✗	sMsgDelDevUser05075309_1	356384402	09.08.2017 04:09:45	00908f69ed11	33.114.17.8 / 172.17.113.43	430HD	UC_2.0.13.121	Nir	AutoDetection	09.08.2017 04:09:45	myLoca

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

Figure 7-6: Devices Status Filter



☑ Devices Status

Display Columns Export Reload

First ← Previous 1 Next → Last

Showing 1 to 50 of 89 entries

Filter Clear Filter Close

User User Name

Phone Number Phone Number

MAC Address MAC Address

IP Address IP Address

Model ---------
 430HD
 440HD

Version ---------
 UC_3.0.4.403
 UC_2.0.13.121

Status: ---------

Approve: ---------

User With Multiple Devices: □

Tenant: ---------
 nirtest1 <br> shays <br> sba

Site: ---------
 test1site
 25 <br> matrix autodetection

Max Devices In Page: 50

Filter Clear Filter

□		⊛	BToE		✔	User Name	Phone Number	Last Update Status	Mac Address	IP Addrees	IPP Model	Firmware	Tenant	Site	Report Time	Locat
□	Actions ≡	●	🔗		☑	avner2	+97239764072;ext=4072	26.09.2017 16:32:31	00908f612bb0	10.16.2.83	440HD	UC_3.0.4.403	SBA	AutoDetection	27.09.2017 10:32:37	
□	Actions ≡				✗	tenantUser16523426_3	746077871	26.09.2017 15:55:53	00908fdc093b	72.119.126.84 / 172.17.113.30	430HD	UC_2.0.13.121	Nir	AutoDetection	26.09.2017 15:55:53	myLoca
□	Actions ≡				✗	tenantUser16523426_1	563054429	26.09.2017 15:54:03	00908fefcba1	57.83.125.56 / 172.17.113.30	430HD	UC_2.0.13.121	Nir	AutoDetection	26.09.2017 15:54:03	myLoca
□	Actions ≡			Approve	✗	operTenMultiDvcs11130824	622775675	24.09.2017 10:14:32	00908f453edc	86.52.49.67 / 172.17.113.30	430HD	UC_2.0.13.121	Nir	AutoDetection	24.09.2017 10:14:32	myLoca
□	Actions ≡			Approve	✗	opersysmultidvcs16335318	186566217	18.09.2017 15:35:13	00908fa9909b	69.95.91.127 / 172.17.113.30	430HD	UC_2.0.13.121	Nir	AutoDetection	18.09.2017 15:35:13	myLoca
□	Actions ≡			Approve	✗			18.09.2017 12:44:35	00908fd4a8ed	39.62.121.5 / 172.17.113.30	430HD	UC_2.0.13.121	SBA	AutoDetection	18.09.2017 12:44:35	myLoca
□	Actions ≡			Approve	✗	sMsgDelDevUser12260218_3	255953502	18.09.2017 11:29:10	00908f8cd1b8	44.104.62.6 / 172.17.113.30	430HD	UC_2.0.13.121	Nir	AutoDetection	18.09.2017 11:29:10	myLoca
□	Actions ≡			Approve	✗	sMsgDelDevUser12260218_2	331096147	18.09.2017 11:28:15	00908fe48aea	91.46.51.50 / 172.17.113.30	430HD	UC_2.0.13.121	Nir	AutoDetection	18.09.2017 11:28:15	myLoca
□	Actions ≡			Approve	✗	sMsgDelDevUser12260218_1	007993462	18.09.2017 11:27:20	00908f552ce8	80.31.36.88 / 172.17.113.30	430HD	UC_2.0.13.121	Nir	AutoDetection	18.09.2017 11:27:20	myLoca
□	Actions ≡			Approve	✗	postUserPrefix2_10480518	856237485	18.09.2017 09:52:51	00908ff95e9c	62.27.77.1 / 172.17.113.30	430HD	UC_2.0.13.121	SBA	AutoDetection	18.09.2017 09:52:51	myLoca
□	Actions ≡			Approve	✗	postUserPrefix2_10360918	521218641	18.09.2017 09:40:56	00908fb09691	106.42.126.71 / 172.17.113.30	430HD	UC_2.0.13.121	SBA	AutoDetection	18.09.2017 09:40:56	myLoca
□	Actions ≡			Approve	✗	postUserPrefix2_10173318	425019262	18.09.2017 09:22:21	00908f6cecc2	77.20.49.86 / 172.17.113.30	430HD	UC_2.0.13.121	SBA	AutoDetection	18.09.2017 09:22:21	myLoca
□	Actions ≡			Approve	✗	postUserPrefix2_10014018	840538434	18.09.2017 09:06:27	00908fdce1ed	87.71.61.92 / 172.17.113.30	430HD	UC_2.0.13.121	SBA	AutoDetection	18.09.2017 09:06:27	myLoca
□	Actions ≡			Approve	✗	sMsgDelDevUser04043518_3	906723125	18.09.2017 03:07:41	00908f08b37e	111.56.93.71 / 172.17.113.30	430HD	UC_2.0.13.121	Nir	AutoDetection	18.09.2017 03:07:41	myLoca
□	Actions ≡			Approve	✗	sMsgDelDevUser04043518_2	687428490	18.09.2017 03:06:46	00908f21cb52	112.62.34.35 / 172.17.113.30	430HD	UC_2.0.13.121	Nir	AutoDetection	18.09.2017 03:06:46	myLoca
□	Actions ≡			Approve	✗	sMsgDelDevUser04043518_1	353860665	18.09.2017 03:05:52	00908fdea7d1	30.121.98.35 / 172.17.113.30	430HD	UC_2.0.13.121	Nir	AutoDetection	18.09.2017 03:05:52	myLoca
□	Actions ≡			Approve	✗	operSysMultiDvcs23450317	651094742	17.09.2017 22:46:21	00908fdb3c55	29.26.35.80 / 172.17.113.30	430HD	UC_2.0.13.121	Nir	AutoDetection	17.09.2017 22:46:21	myLoca
□	Actions ≡			Approve	✗	unRegAlert23020717	945289040	17.09.2017 22:06:10	00908f85d1ee	26.50.65.42 / 172.17.113.30	430HD	UC_2.0.13.121	SBA	AutoDetection	17.09.2017 22:06:10	myLoca

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, tenant, site, 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 'Location'; non-Skype for Business phones are not displayed under 'Location'.

7. View in the column 'IPP Model' the entries **Spectralink 8440, Polycom Trio 8800**, **Polycom VVX**, etc. if these phone models are connected; they can be monitored, configured and templates can be mapped.
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 7-7: Actions Menu - Single User

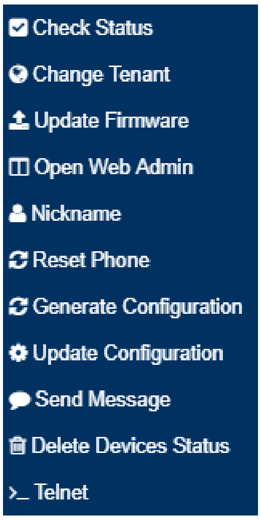
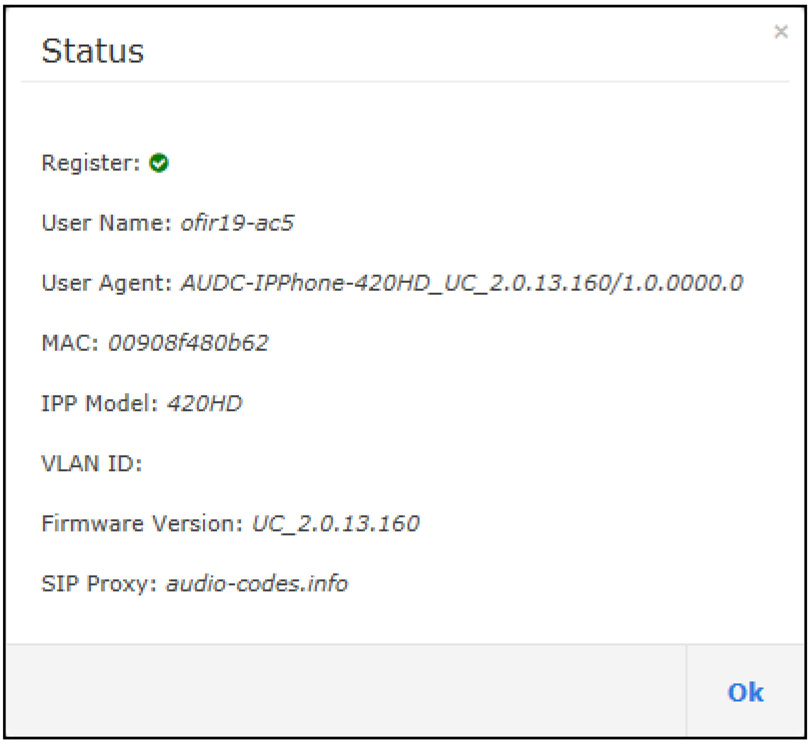
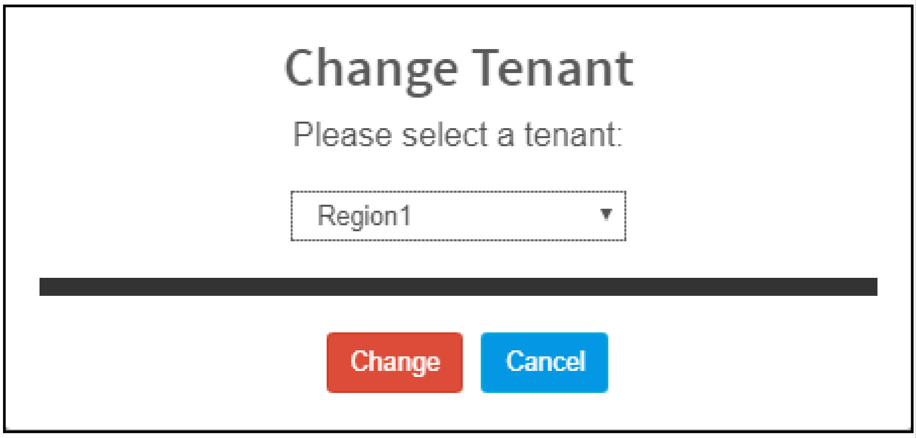
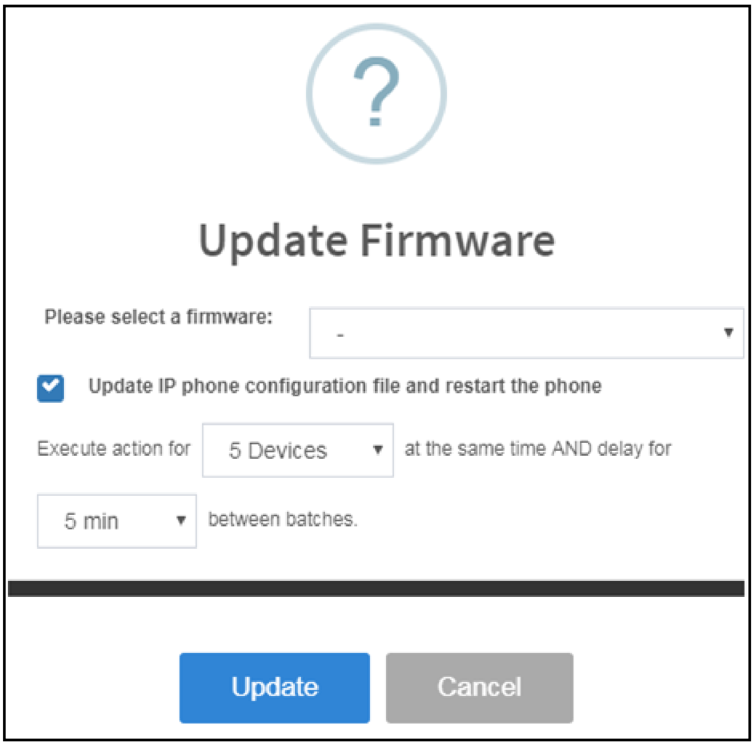


Table 7-2: Actions Menu

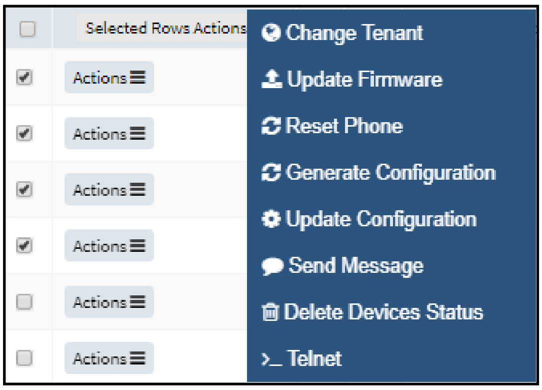
Action	Description
Check Status	Select the 'Check Status' option.  Status Register: ✓ User Name: *ofir19-ac5* User Agent: *AUDC-IPPhone-420HD_UC_2.0.13.160/1.0.0000.0* MAC: *00908f480b62* IPP Model: *420HD* VLAN ID: Firmware Version: *UC_2.0.13.160* SIP Proxy: *audio-codes.info* Ok

Action	Description
Change Tenant	Select the 'Change Tenant' option.  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 ■ update firmware simultaneously for a batch of devices, each batch containing 5 | 10 | 20 | 30 | 50 | 100 devices

Action	Description
	■ configure a 0 second | 2 second | 5 second | 10 second | 30 second | 2 minute | 5 minute delay between batches
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.
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.
Delete Devices Status	Deletes the devices from the Devices Status table.
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 7-8: Actions Menu - Selected Rows



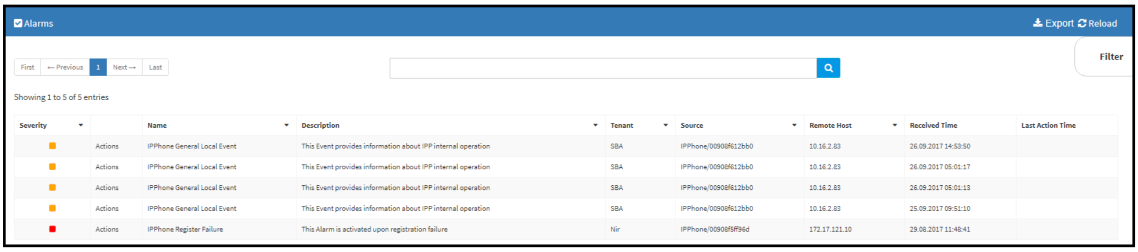
See the table above for descriptions. Any action you choose will apply to all selected rows. For example, select rows, click the **Selected Rows Actions** link, and then select the **Update Firmware** option; all selected devices will be updated with the firmware file you select.

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 7-9: Alarms



Showing 1 to 5 of 5 entries

Severity		Name	Description	Tenant	Source	Remote Host	Received Time	Last Action Time
🟧	Actions	IPPhone General Local Event	This Event provides information about IPP internal operation	SBA	IPPhone/00908f612bb0	10.16.2.83	26.09.2017 14:53:50	
🟧	Actions	IPPhone General Local Event	This Event provides information about IPP internal operation	SBA	IPPhone/00908f612bb0	10.16.2.83	26.09.2017 05:01:17	
🟧	Actions	IPPhone General Local Event	This Event provides information about IPP internal operation	SBA	IPPhone/00908f612bb0	10.16.2.83	26.09.2017 05:01:13	
🟧	Actions	IPPhone General Local Event	This Event provides information about IPP internal operation	SBA	IPPhone/00908f612bb0	10.16.2.83	25.09.2017 09:51:10	
🟥	Actions	IPPhone Register Failure	This Alarm is activated upon registration failure	Nir	IPPhone/00908f5ff96d	172.17.121.10	29.08.2017 11:48:41	

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.

The table below shows the five alarms that users can receive.

Table 7-3: Alarms

Alarm Name	Severity
Registration Failure	**Critical**
Survivable Mode Start	**Major**
Login Failure	**Critical**
Endpoint License Alarm	**Critical**
Endpoint Server Overloaded Alarm	**Critical**

Registration Failure Alarm

The table below describes the Registration Failure alarm. The alarm is issued if SIP registration, with the PBX, fails.

Table 7-4: IP Phone Registration Failure Alarm

Alarm	IPPhoneRegisterFailure
OID	.1.3.6.1.4.1.5003.9.20.3.2.0.39 is the OID used in the OVOC to forward the IPPhoneRegisterFailure alarm
Description	This alarm is activated when a registration failure occurs

Alarm	IPPhoneRegisterFailure
Alarm Title	Registration Failure
Alarm Type	communicationsAlarm(1)
Probable Cause	communicationsProtocolError(5)
Severity	Critical
Corrective Action	The problem is typically not related to the phone but to the server. The user/phone may not be defined, or may be incorrectly defined, or may previously have been defined but the username (for example) may have been changed, causing the registration to fail. Make sure the username and password credentials are the same in server and phone, and weren't changed; server-phone credentials must be synchronized. Make sure the server is responsive.

Survivable Mode Start Alarm

The table below describes the Survivable Mode Start alarm.

Table 7-5: IP Phone Survivable Mode Start Alarm

Alarm	IPPhoneSurvivableModeStart
OID	.1.3.6.1.4.1.5003.9.20.3.2.0.40 is the OID used in the OVOC to forward the IPPhoneSurvivableModeStart alarm
Description	This alarm is activated when entering survivable mode state with limited services
Alarm Title	Survivable Mode Start
Alarm Type	Other(0)
Probable Cause	other (0)
Severity	Major
Additional Info	
Corrective Action	The problem is typically not related to the phone but to the server or network. Make sure all servers in the enterprise network are up. If one is down, limited service will result.

Lync Login Failure Alarm

The table below describes the Skype for Business Login Failure alarm.

> ⚠ Microsoft rebranded Lync as Skype for Business so when the term Skype for Business appears in this document, it also applies to Microsoft Lync.

Table 7-6: IP Phone Lync Login Failure Alarm

Alarm	IPPhoneLyncLoginFailure
OID	.1.3.6.1.4.1.5003.9.20.3.2.0.41 is the OID used in the OVOC to forward the IPPhoneLyncLoginFailure alarm
Description	This alarm is activated when failing to connect to the Skype for Business server during sign in
Alarm Title	Lync Login Failure
Alarm Type	communicationsAlarm(1)
Probable Cause	communicationsProtocolError(5)
Severity	Critical
Additional Info	TlsConnectionFailure NtpServerError
Corrective Action	This alarm may typically occur if the user is not registered - or is registered incorrectly - in the Skype for Business server. Make sure in the server that the username, password and PIN code are correctly configured and valid. Try resetting them. Try redefine the user.

Endpoint License Alarm

The table below describes the Endpoint License alarm.

Table 7-7: Endpoint License Alarm

Description	This alarm is issued when the number of endpoints currently running on the OVOC server (Management of Endpoints in the Device Manager Pro) approaches or reaches license capacity.
SNMP Alarm	acEndpointLicenseAlarm
SNMP OID	1.3.6.1.4.1.5003.9.20.3.2.0.48
Alarm Title	Endpoint License Alarm
Alarm Source	OC Server
Alarm Type	Other
Probable Cause	Key Expired
Additional Info	Endpoint License capacity {0} devices.
Corrective Action	Contact your AudioCodes partner ASAP

Alarm Severity	Condition	Alarm Text	Corrective Action
Critical	100% of the period defined in the device's license is consumed	100% of the period defined in the currently running device's license has been consumed	Contact your AudioCodes partner.
Major	80% of the period defined in the device's license is consumed	80% of the period defined in the currently running device's license has been consumed	Contact your AudioCodes partner.
Clear	Clearing currently active alarm	Clear - Clearing currently active alarm.	Contact your AudioCodes partner.

If a license expires:

- Communications with all servers is suspended
- Users cannot log in
- New phones cannot be added
- Contact your AudioCodes partner

IP Phone Speaker Firmware Download Failure

The table below describes the IP Phone Speaker Firmware Download Failure alarm.

Table 7-8: IP Phone Speaker Firmware Download Failure Alarm

Description	This alarm is sent when the phone fails to download the speaker firmware from the server.
SNMP Alarm	IPPhoneSpeakerFirmDownloadFailure
SNMP OID	1.3.6.1.4.1.5003.9.20.3.2.0.54
Alarm Title	IP Phone Speaker Firmware Download Failure.
Alarm Source	IP Phone
Alarm Type	communicationsAlarm(1)
Probable Cause	communicationsProtocolError(5)
Additional Info	
Corrective Action	▪ Make sure the Device Manager Pro is correctly defined. ▪ Contact your network administrator (IT manager).

Alarm Severity	Condition	**Alarm Text**	**Corrective Action**

Minor		This alarm is sent when the phone fails to download the speaker firmware.	

IP Phone Speaker Firmware Upgrade Failure

The table below describes the IP Phone Speaker Firmware Upgrade failure alarm.

Table 7-9: IP Phone Speaker Firmware Upgrade Failure

<table>
<tr><td>Description</td><td colspan="3">This alarm is sent when the phone fails to load the firmware to the speaker. The new speaker firmware is already available on the phone. The phone downloaded the speaker firmware from an external server.</td></tr>
<tr><td>SNMP Alarm</td><td colspan="3">IPPhoneSpeakerFirmUpgradeFailure</td></tr>
<tr><td>SNMP OID</td><td colspan="3">1.3.6.1.4.1.5003.9.20.3.2.0.55</td></tr>
<tr><td>Alarm Title</td><td colspan="3">IP Phone Speaker Firmware Upgrade Failure</td></tr>
<tr><td>Alarm Source</td><td colspan="3"></td></tr>
<tr><td>Alarm Type</td><td colspan="3">communicationsAlarm(1)</td></tr>
<tr><td>Probable Cause</td><td colspan="3">communicationsProtocolError(5)</td></tr>
<tr><td>Additional Info</td><td colspan="3"></td></tr>
<tr><td>Corrective Action</td><td colspan="3">■ Make sure the speaker is properly connected to the phone.
■ Try again.
■ Contact your network administrator (IT manager) if the alarm persists.</td></tr>
<tr><th>Alarm Severity</th><th>Condition</th><th>Alarm Text</th><th>Corrective Action</th></tr>
<tr><td>Minor</td><td></td><td>This alarm is sent when the phone fails to load the firmware to the speaker.</td><td></td></tr>
</table>

IP Phone Conference Speaker Connection Failure

The table below describes the IP Phone Conference Speaker Connection Failure alarm.

Table 7-10: Conference IP Phone has no Connection to Speaker

Description	This alarm is sent when the USB connection between the phone and the speaker fails.
SNMP Alarm	IPPhoneConferSpeakerConnectFailure
SNMP OID	1.3.6.1.4.1.5003.9.20.3.2.0.56

Alarm Title	IP Phone Conference Speaker Connection Failure		
Alarm Source			
Alarm Type	communicationsAlarm(1)		
Probable Cause	communicationsProtocolError(5)		
Additional Info			
Corrective Action	■ Make sure the USB cable is properly connected. ■ After making sure, contact your network administrator (IT manager) if the alarm persists.		
Alarm Severity	Condition	Alarm Text	Corrective Action
Major		This alarm is sent when there is failure for the USB connection between the phone and the speaker	

IP Phone General Local Event

The table below describes the IP Phone General Local Event.

Table 7-11: IP Phone General Local Event

Description	This alarm provides information about the internal operation of the phone.
SNMP Alarm	IPPhoneGeneralLocalEvent
SNMP OID	1.3.6.1.4.1.5003.9.20.3.2.0.57
Alarm Title	IP Phone General Local Event
Alarm Source	The IP Phone
Alarm Type	Other(0)
Probable Cause	Other(0)
Severity	Major
Additional Info	4 digit code
Corrective Action	-

IP Phone Web Successive Login Failure

The table below describes the IP Phone Web Successive Login Failure alarm.

Table 7-12: IP Phone Web Successive Login Failure

<table>
<tr><td>Description</td><td colspan="3">This alarm is sent after five successive unsuccessful attempts are made to log in to the phone's Web interface.</td></tr>
<tr><td>SNMP Alarm</td><td colspan="3">IPPhoneWebSuccessiveLoginFailure</td></tr>
<tr><td>SNMP OID</td><td colspan="3">1.3.6.1.4.1.5003.9.20.3.2.0.59</td></tr>
<tr><td>Alarm Title</td><td colspan="3">IP Phone Web Successive Login Failure</td></tr>
<tr><td>Alarm Source</td><td colspan="3">The IP Phone</td></tr>
<tr><td>Alarm Type</td><td colspan="3">SecurityServiceOrMechanismViolation(9)</td></tr>
<tr><td>Probable Cause</td><td colspan="3">UnauthorizedAccessAttempt(73)</td></tr>
<tr><td>Additional Info</td><td colspan="3"></td></tr>
<tr><td>Alarm Severity</td><td>Condition</td><td>Alarm Text</td><td>Corrective Action</td></tr>
<tr><td>Major</td><td>Issued after the fifth successive attempt to log in to the phone's Web interface fails.</td><td></td><td>■ After the alarm is cleared, try to log in to the Web interface using the correct username and password.
■ If you forget the login credentials, inform the network administrator.</td></tr>
<tr><td>Clear</td><td>Issued if no additional unsuccessful Web login attempts are made during a specific time period (60 seconds) after a Major severity level alarm is sent.</td><td></td><td></td></tr>
</table>

Jabra Firmware Upgrade Failed

The table below describes the Jabra Firmware Upgrade Failed alarm.

Table 7-13: Jabra Firmware Upgrade Failed

Description	This alarm is sent when the firmware upgrade procedure for a Jabra device fails.
SNMP Alarm	JabraFirmwareUpgradeFailed
SNMP OID	1.3.6.1.4.1.5003.9.20.3.2.0.55
Alarm Title	JABRA FIRMWARE UPGRADE FAILED

Alarm Source	-		
Alarm Type	Communications Alarm		
Probable Cause	Communications Protocol Error		
Additional Info	-		
Corrective Action	■ Try again. ■ Contact your network administrator (IT manager) if the alarm persists.		
Alarm Severity	Condition	Alarm Text	Corrective Action
-	-	-	-

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 33 for more information.

Maintaining Users

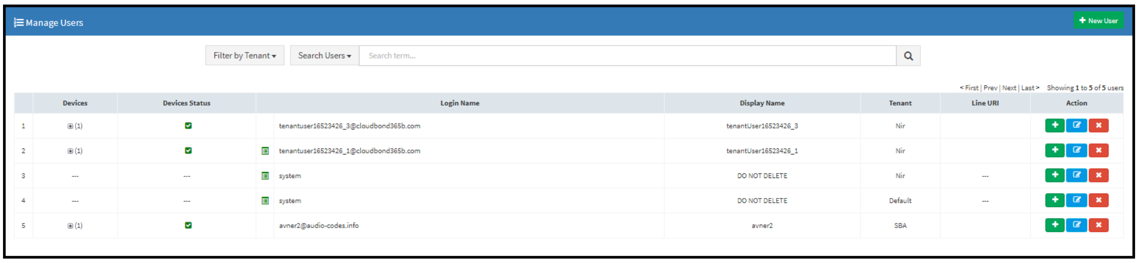
The Manage Users page lets you maintain users. You can

- 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 7-10: Searching for a User/Device



Manage Users

+ New User

Filter by Tenant ▾ | Search Users ▾ | Search term...

< First | Prev | Next | Last > Showing 1 to 5 of 5 users

	Devices	Devices Status		Login Name	Display Name	Tenant	Line URI	Action
1	⊞ (1)	✓		tenantuser16523426_3@cloudbond365b.com	tenantUser16523426_3	Nir		+ ✎ ✖
2	⊞ (1)	✓	▤	tenantuser16523426_1@cloudbond365b.com	tenantUser16523426_1	Nir		+ ✎ ✖
3	---	---	▤	system	DO NOT DELETE	Nir	---	+ ✎ ✖
4	---	---	▤	system	DO NOT DELETE	Default	---	+ ✎ ✖
5	⊞ (1)	✓		avner2@audio-codes.info	avner2	SBA		+ ✎ ✖

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 & Devices' 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.

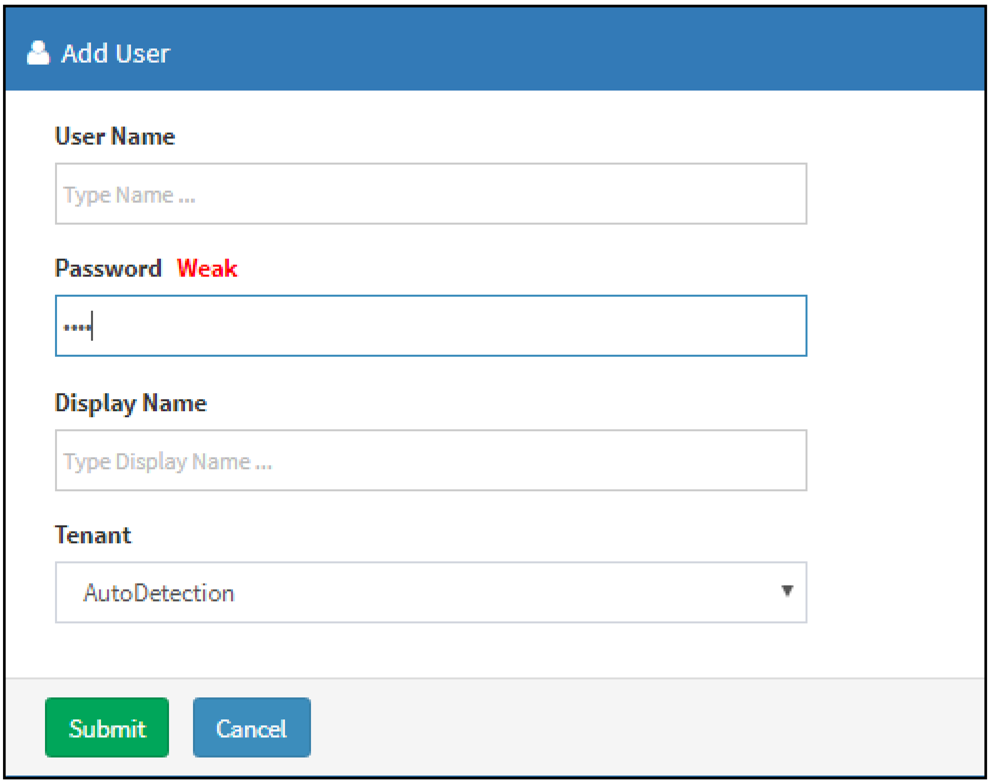
Adding a User

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 7-11: New User



Add User

User Name

Type Name ...

Password Weak

••••

Display Name

Type Display Name ...

Tenant

AutoDetection ▾

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.

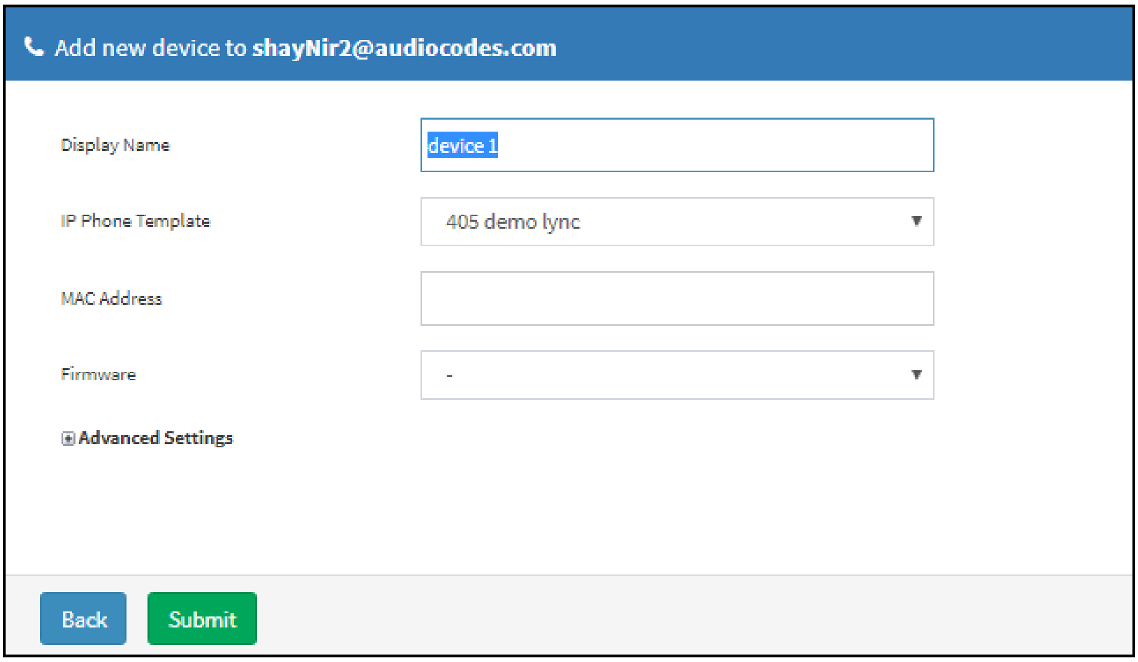
Adding a Phone

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 7-12: 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 57 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.

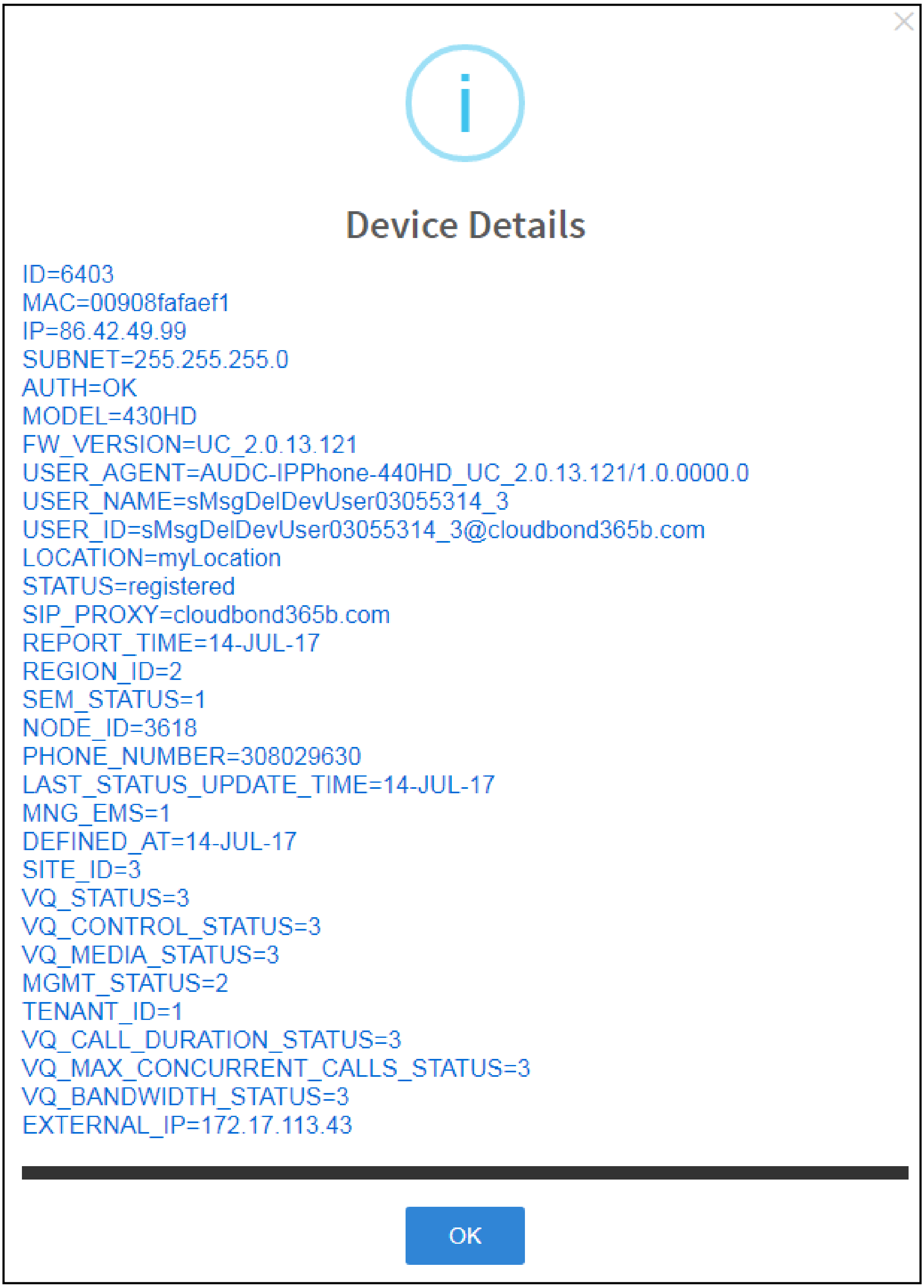
➢ To edit a user:

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

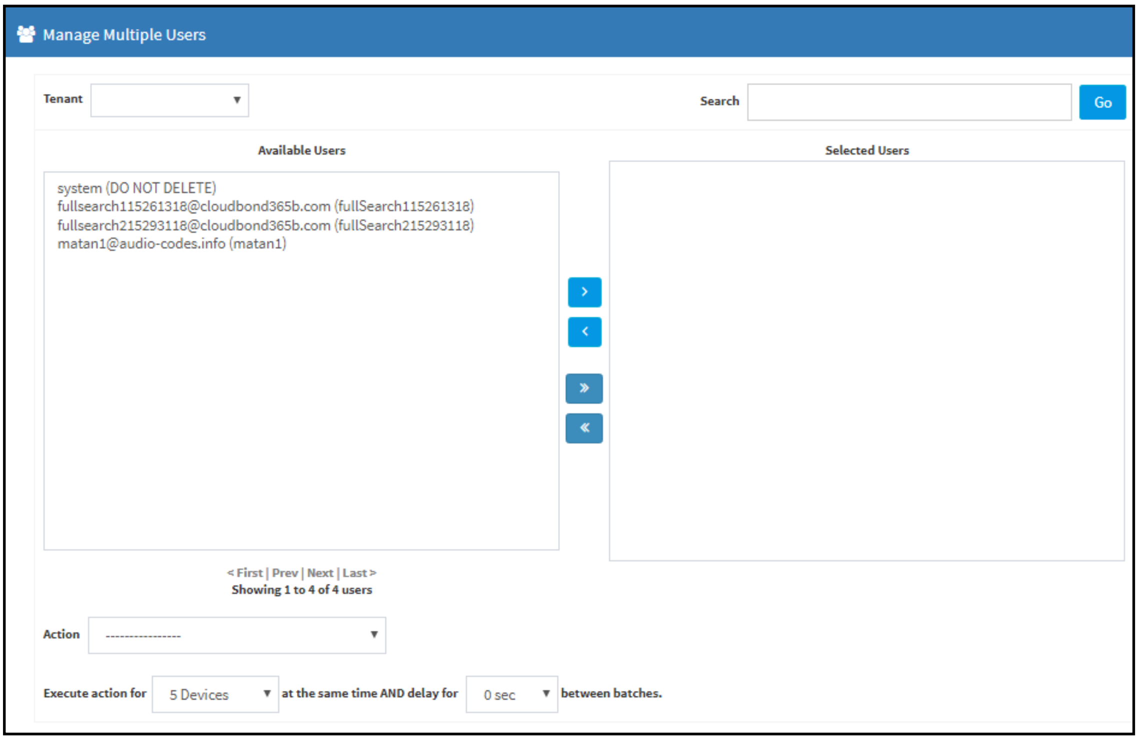
The Manage Multiple Users page lets you perform an action on a single user or on multiple users simultaneously:

- 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 7-13: Manage Multiple Users



system (DO NOT DELETE)
fullsearch115261318@cloudbond365b.com (fullSearch115261318)
fullsearch215293118@cloudbond365b.com (fullSearch215293118)
matan1@audio-codes.info (matan1)

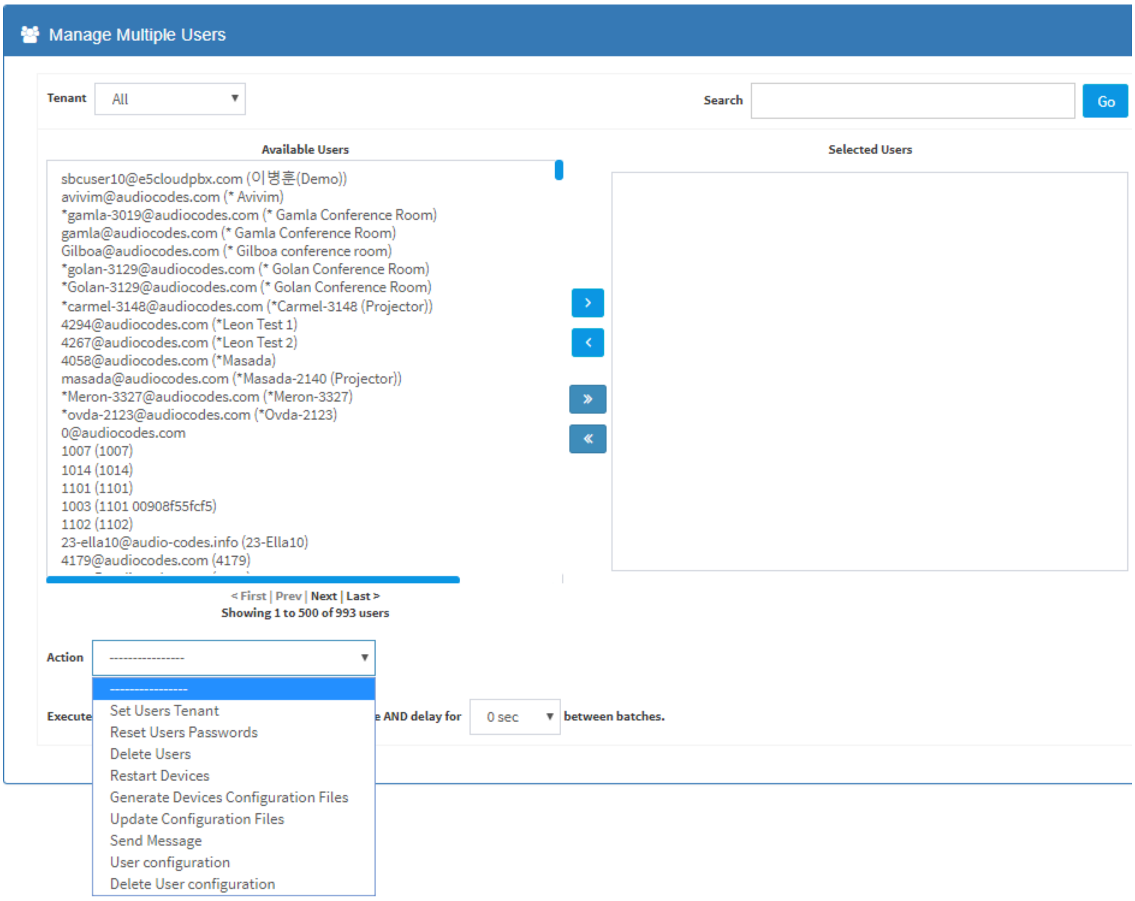
Showing 1 to 4 of 4 users

Action ----------------

Execute action for 5 Devices at the same time 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

Available Users

sbcuser10@e5cloudpbx.com (이병훈(Demo))
avivim@audiocodes.com (* Avivim)
gamla-3019@audiocodes.com (Gamla Conference Room)
gamla@audiocodes.com (* Gamla Conference Room)
Gilboa@audiocodes.com (* Gilboa conference room)
golan-3129@audiocodes.com (Golan Conference Room)
Golan-3129@audiocodes.com (Golan Conference Room)
*carmel-3148@audiocodes.com (*Carmel-3148 (Projector))
4294@audiocodes.com (*Leon Test 1)
4267@audiocodes.com (*Leon Test 2)
4058@audiocodes.com (*Masada)
masada@audiocodes.com (*Masada-2140 (Projector))
*Meron-3327@audiocodes.com (*Meron-3327)
*ovda-2123@audiocodes.com (*Ovda-2123)
0@audiocodes.com
1007 (1007)
1014 (1014)
1101 (1101)
1003 (1101 00908f55fcf5)
1102 (1102)
23-ella10@audio-codes.info (23-Ella10)
4179@audiocodes.com (4179)

Selected Users

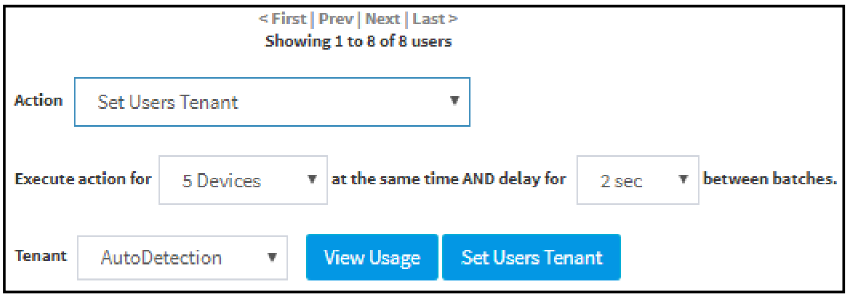
< First | Prev | Next | Last >
Showing 1 to 500 of 993 users

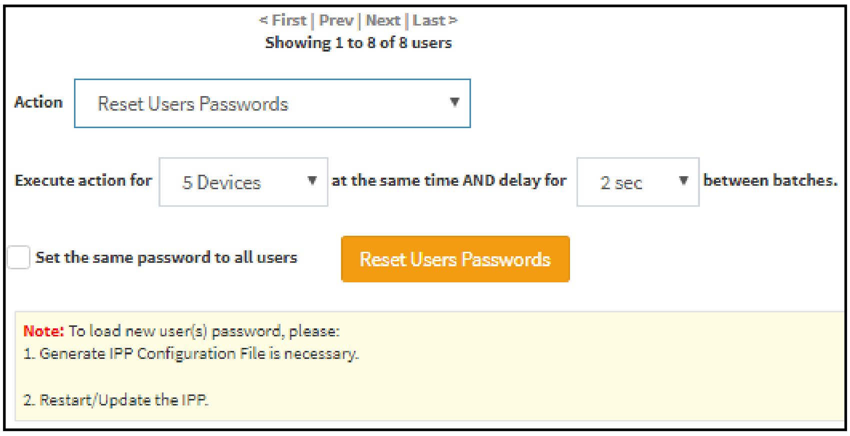
Action ----------------

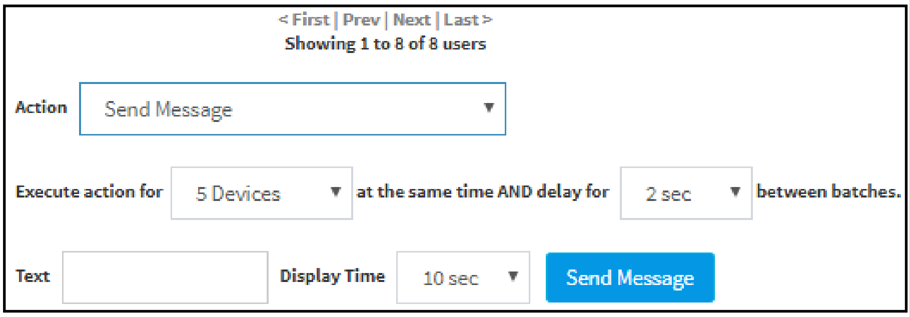
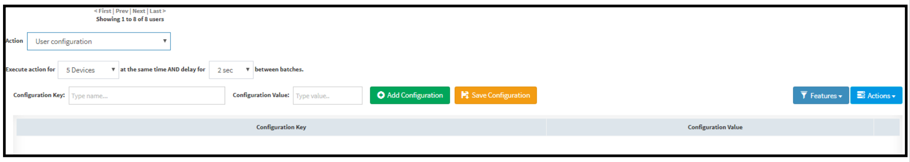
Execute ... e AND delay for 0 sec between batches.

- Use the table below as reference.

Table 7-14: Managing Multiple Users - Actions

Action	Description
Set Users Tenant	 < First | Prev | Next | Last > Showing 1 to 8 of 8 users Action Set Users Tenant Execute action for 5 Devices at the same time AND delay for 2 sec between batches. Tenant AutoDetection View Usage Set Users Tenant Sets the tenant for users selected.

Action	Description
Reset Users Passwords	 < First | Prev | Next | Last > Showing 1 to 8 of 8 users 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 Reset Users Passwords Note: To load new user(s) password, please: 1. Generate IPP 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 Files	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 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	Description
	 < First | Prev | Next | Last > Showing 1 to 8 of 8 users Action: Send Message Execute action for 5 Devices at the same time AND delay for 2 sec between batches. Text Display Time: 10 sec Send Message
User Configuration	 < First | Prev | Next | Last > Showing 1 to 8 of 8 users Action: User configuration Execute action for 5 Devices at the same time AND delay for 2 sec between batches. Configuration Key: Type name... Configuration Value: Type value.. Add Configuration Save Configuration Features Actions Configuration 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

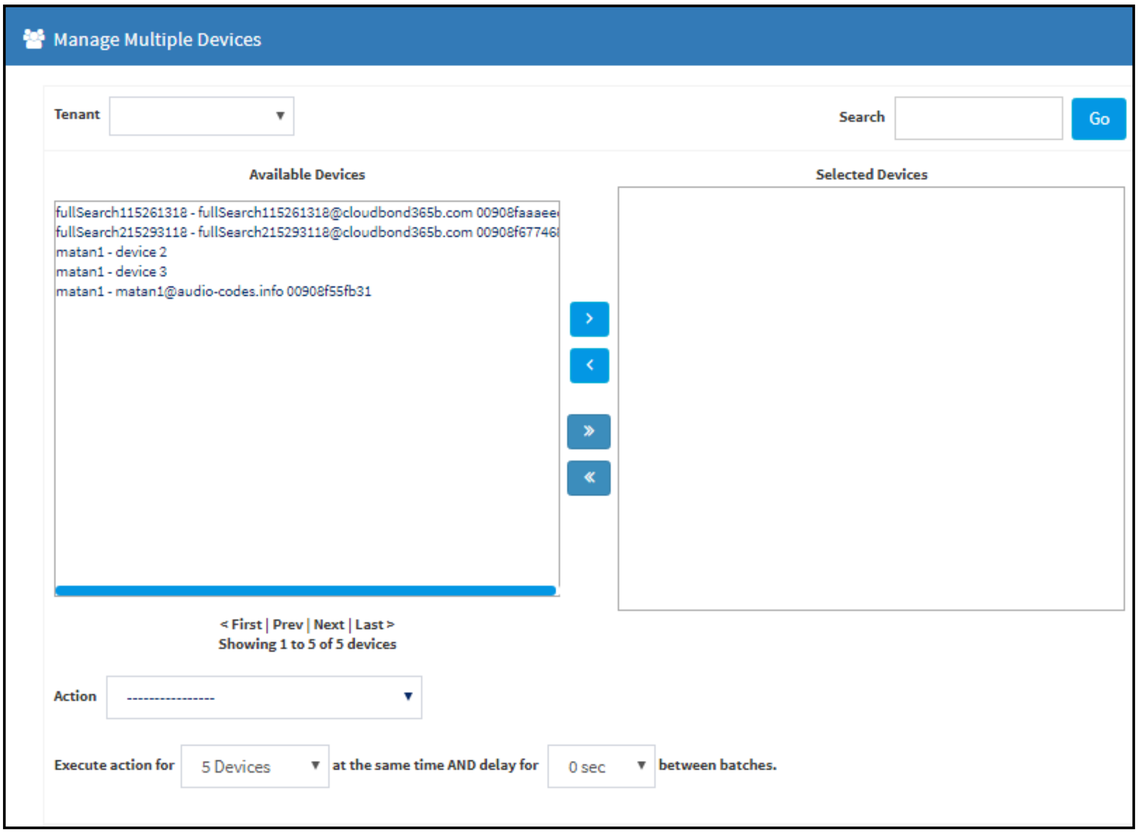
The Manage Multiple Devices page lets you perform a single operation on all or on many user devices. The page lets you

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

➢ To manage multiple devices:

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

Figure 7-14: Manage Multiple Devices



Manage Multiple Devices

Tenant

Search

Go

Available Devices

fullSearch115261318 - fullSearch115261318@cloudbond365b.com 00908faaaee
fullSearch215293118 - fullSearch215293118@cloudbond365b.com 00908f67746
matan1 - device 2
matan1 - device 3
matan1 - matan1@audio-codes.info 00908f55fb31

Selected Devices

< First | Prev | Next | Last >
Showing 1 to 5 of 5 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 7-15: 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.

Action	Description
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. 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.

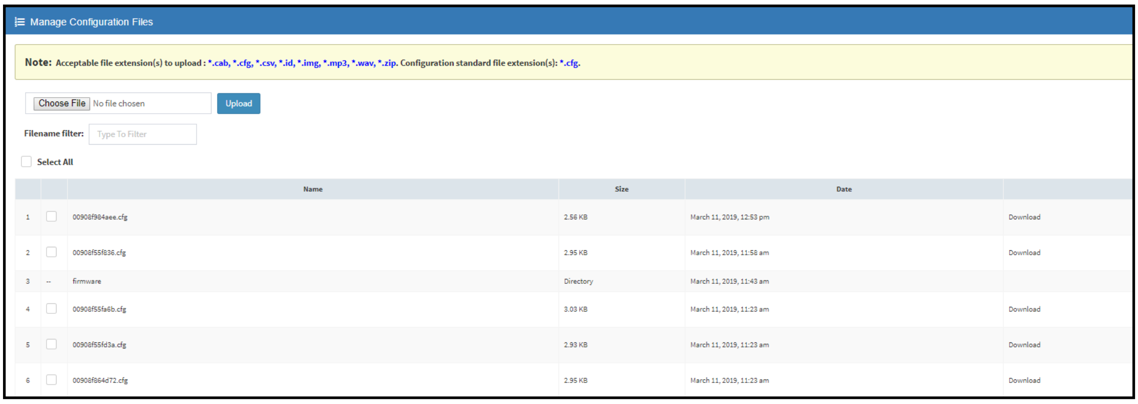
Managing Configuration Files

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** > **Devices Configuration** > **Generated Config Files**).

Figure 7-15: Manage Configuration Files



Manage Configuration Files

Note: Acceptable file extension(s) to upload : *.cab, *.cfg, *.csv, *.id, *.img, *.mp3, *.wav, *.zip. Configuration standard file extension(s): *.cfg.

Choose File No file chosen Upload

Filename filter: Type To Filter

□ Select All

		Name	Size	Date	
1	□	00908f984aee.cfg	2.56 KB	March 11, 2019, 12:53 pm	Download
2	□	00908f55f836.cfg	2.95 KB	March 11, 2019, 11:58 am	Download
3	--	firmware	Directory	March 11, 2019, 11:43 am	
4	□	00908f55fa6b.cfg	3.03 KB	March 11, 2019, 11:23 am	Download
5	□	00908f55fd3a.cfg	2.93 KB	March 11, 2019, 11:23 am	Download
6	□	00908f864d72.cfg	2.95 KB	March 11, 2019, 11:23 am	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)

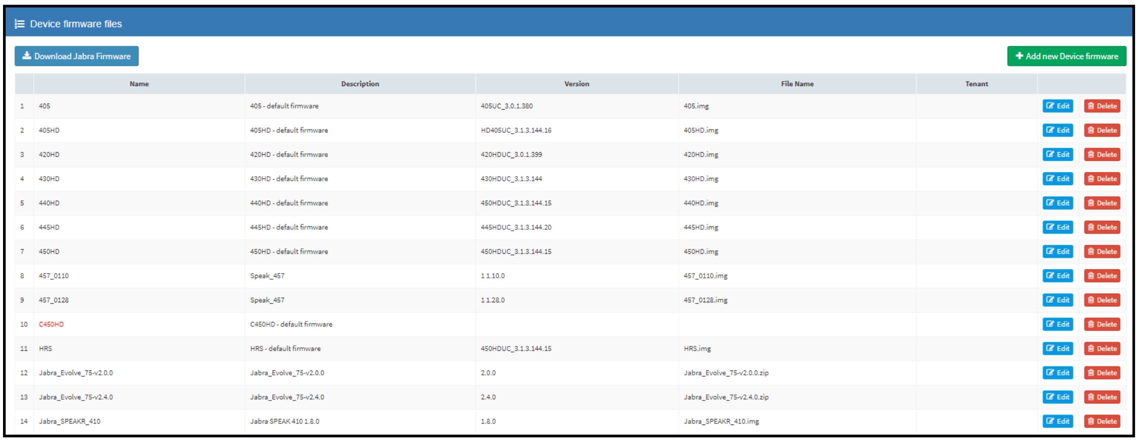
Managing Firmware Files

You can manage devices' .img firmware files.

➢ To manage the .img firmware files:

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

Figure 7-16: Device Firmware Files



Device firmware files

Download Jabra Firmware

Add new Device firmware

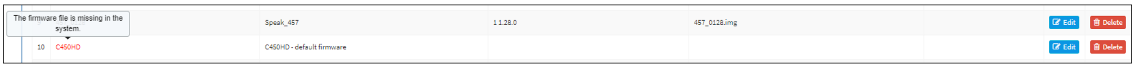
	Name	Description	Version	File Name	Tenant	
1	405	405 - default firmware	405UC_3.0.1.380	405.img		Edit Delete
2	405HD	405HD - default firmware	HD405UC_3.1.3.144.16	405HD.img		Edit Delete
3	420HD	420HD - default firmware	420HDUC_3.0.1.399	420HD.img		Edit Delete
4	430HD	430HD - default firmware	430HDUC_3.1.3.144	430HD.img		Edit Delete
5	440HD	440HD - default firmware	450HDUC_3.1.3.144.15	440HD.img		Edit Delete
6	445HD	445HD - default firmware	445HDUC_3.1.3.144.20	445HD.img		Edit Delete
7	450HD	450HD - default firmware	450HDUC_3.1.3.144.15	450HD.img		Edit Delete
8	457_0110	Speak_457	1 1.10.0	457_0110.img		Edit Delete
9	457_0128	Speak_457	1 1.28.0	457_0128.img		Edit Delete
10	C450HD	C450HD - default firmware				Edit Delete
11	HRS	HRS - default firmware	450HDUC_3.1.3.144.15	HRS.img		Edit Delete
12	Jabra_Evolve_75-v2.0.0	Jabra_Evolve_75-v2.0.0	2.0.0	Jabra_Evolve_75-v2.0.0.zip		Edit Delete
13	Jabra_Evolve_75-v2.4.0	Jabra_Evolve_75-v2.4.0	2.4.0	Jabra_Evolve_75-v2.4.0.zip		Edit Delete
14	Jabra_SPEAKR_410	Jabra SPEAK 410 1.8.0	1.8.0	Jabra_SPEAKR_410.img		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.



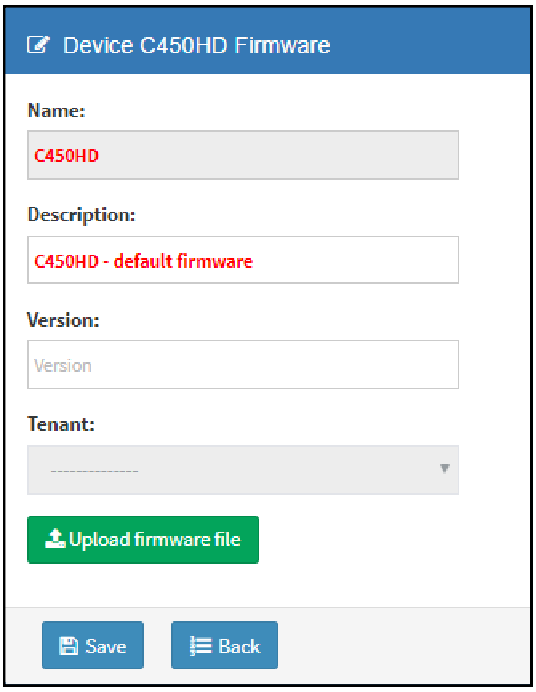
The firmware file is missing in the system.

		Speak_457	1 1.28.0	457_0128.img	Edit	Delete
10	C450HD	C450HD - default firmware			Edit	Delete

- 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 7-17: .img Firmware File Upload



Device C450HD Firmware

Name: C450HD

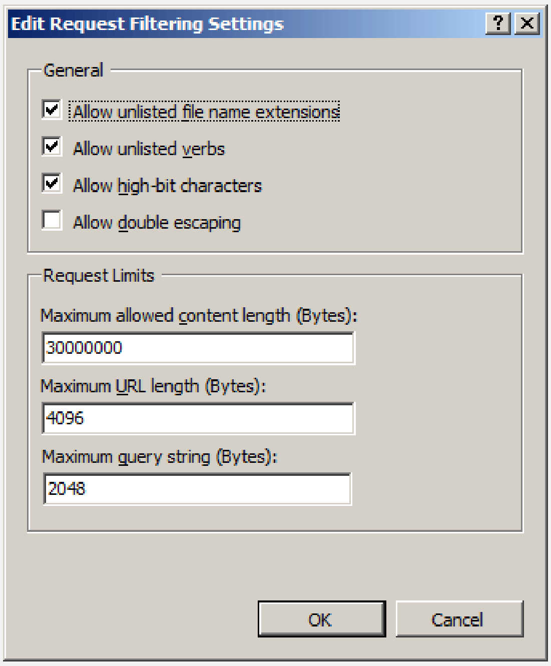
Description: C450HD - default firmware

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

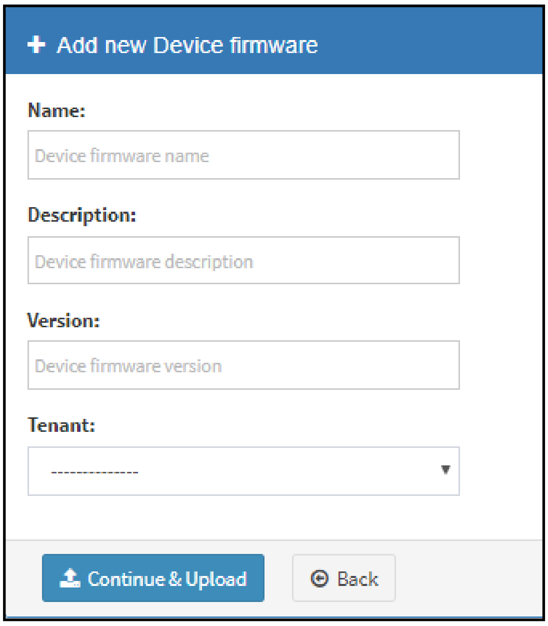
Request Limits

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. Click the **Add new Device firmware** button.



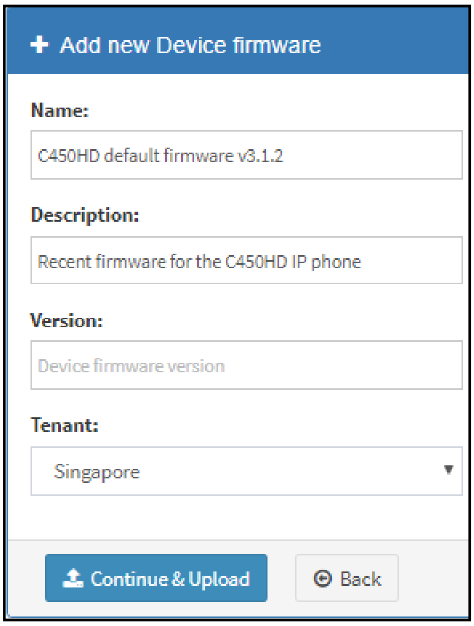
Name: Device firmware name

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**.

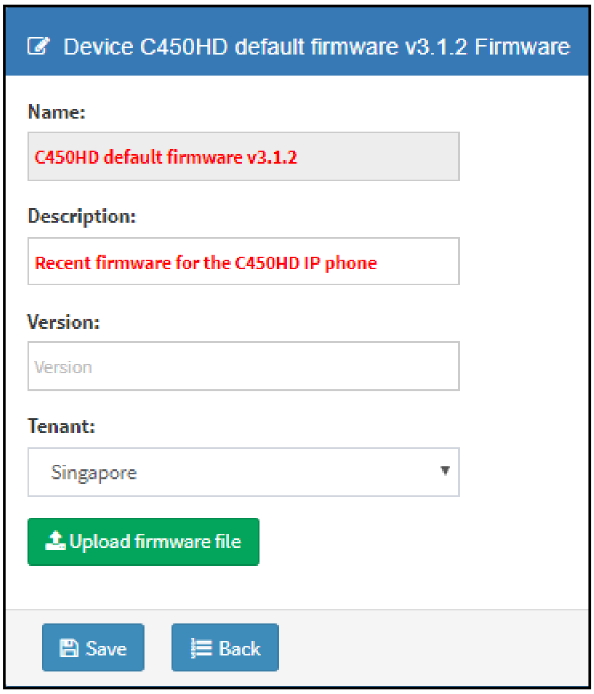


Name: C450HD default firmware v3.1.2

Description: Recent firmware for the C450HD IP phone

Version: Device firmware version

Tenant: Singapore



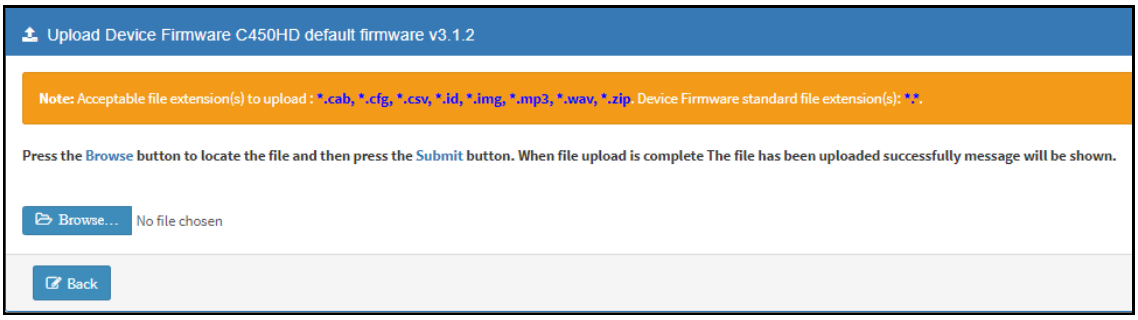
Name: C450HD default firmware v3.1.2

Description: Recent firmware for the C450HD IP phone

Version: Version

Tenant: Singapore

c. Click **Upload firmware file**:



Note: Acceptable file extension(s) to upload : *.cab, *.cfg, *.csv, *.id, *.img, *.mp3, *.wav, *.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.

8 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 8-1: License Properties

2. Use the table below as reference.

Table 8-1: License Properties

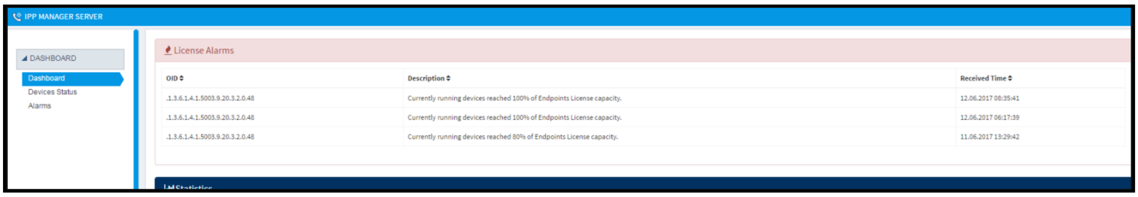
Action	Description
Status	Indicates the license's status (Enable or Disable). If enabled and the configured time expires, connection to the OVOC server platform is denied. When it expires, the Device Manager Pro is rendered non-usable. Contact your AudioCodes partner if the license expires.
Expiration 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 8-2: 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

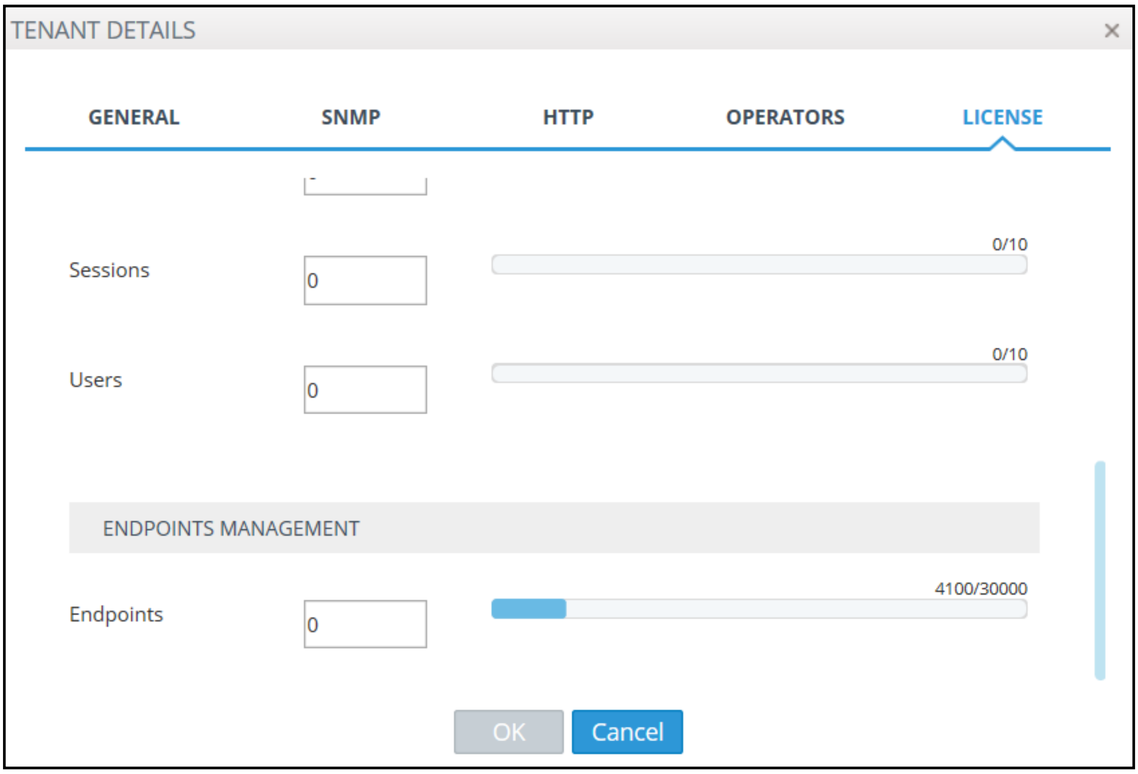
Licensing Endpoints

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 8-3: 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).

9 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.

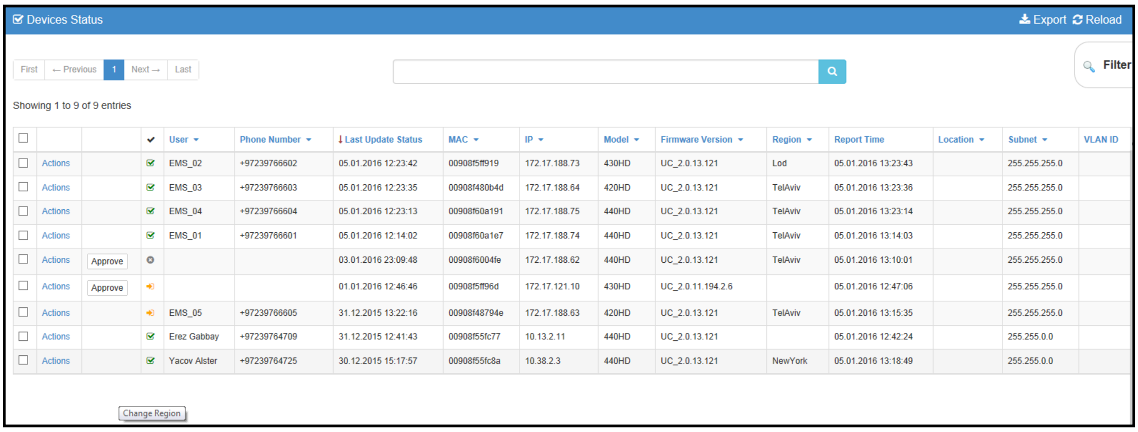
Skype for Business Environment

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 9-1: Devices Status



Showing 1 to 9 of 9 entries

□			✓	User	Phone Number	Last Update Status	MAC	IP	Model	Firmware Version	Region	Report Time	Location	Subnet	VLAN ID
□	Actions		☑	EMS_02	+97239766602	05.01.2016 12:23:42	00908f5ff919	172.17.188.73	430HD	UC_2.0.13.121	Lod	05.01.2016 13:23:43		255.255.255.0	
□	Actions		☑	EMS_03	+97239766603	05.01.2016 12:23:35	00908f480b4d	172.17.188.64	420HD	UC_2.0.13.121	TelAviv	05.01.2016 13:23:36		255.255.255.0	
□	Actions		☑	EMS_04	+97239766604	05.01.2016 12:23:13	00908f60a191	172.17.188.75	440HD	UC_2.0.13.121	TelAviv	05.01.2016 13:23:14		255.255.255.0	
□	Actions		☑	EMS_01	+97239766601	05.01.2016 12:14:02	00908f60a1e7	172.17.188.74	440HD	UC_2.0.13.121	TelAviv	05.01.2016 13:14:03		255.255.255.0	
□	Actions	Approve	⊗			03.01.2016 23:09:48	00908f6004fe	172.17.188.62	440HD	UC_2.0.13.121	TelAviv	05.01.2016 13:10:01		255.255.255.0	
□	Actions	Approve	➔			01.01.2016 12:46:46	00908f5ff96d	172.17.121.10	430HD	UC_2.0.11.194.2.6		05.01.2016 12:47:06		255.255.255.0	
□	Actions		➔	EMS_05	+97239766605	31.12.2015 13:22:16	00908f48794e	172.17.188.63	420HD	UC_2.0.13.121	TelAviv	05.01.2016 13:15:35		255.255.255.0	
□	Actions		☑	Erez Gabbay	+97239764709	31.12.2015 12:41:43	00908f55fc77	10.13.2.11	440HD	UC_2.0.13.121		05.01.2016 12:42:24		255.255.0.0	
□	Actions		☑	Yacov Alster	+97239764725	30.12.2015 15:17:57	00908f55fc8a	10.38.2.3	440HD	UC_2.0.13.121	NewYork	05.01.2016 13:18:49		255.255.0.0	

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.

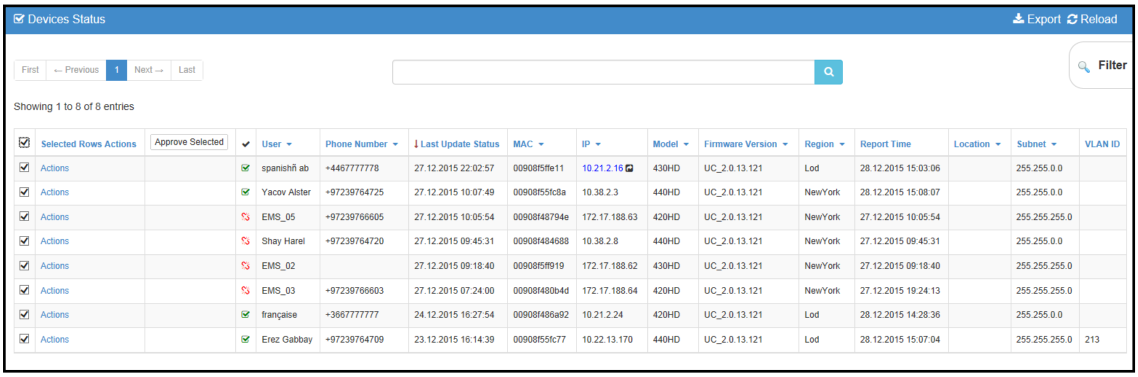
Other columns: User, Phone Number, MAC, IP, Model, Firmware Version, Report Time, Location, Subnet, VLAN ID

Search option

Smart **Filter(s)**

1. Select the upper left checkbox (in the figure below it's indicated in red); the **Selected Rows Actions** menu and the **Approve Selected** button are displayed.

Figure 9-2: Devices Status – Selected Rows Actions - Approve Selected



☑ Devices Status

Export Reload

First ← Previous 1 Next → Last

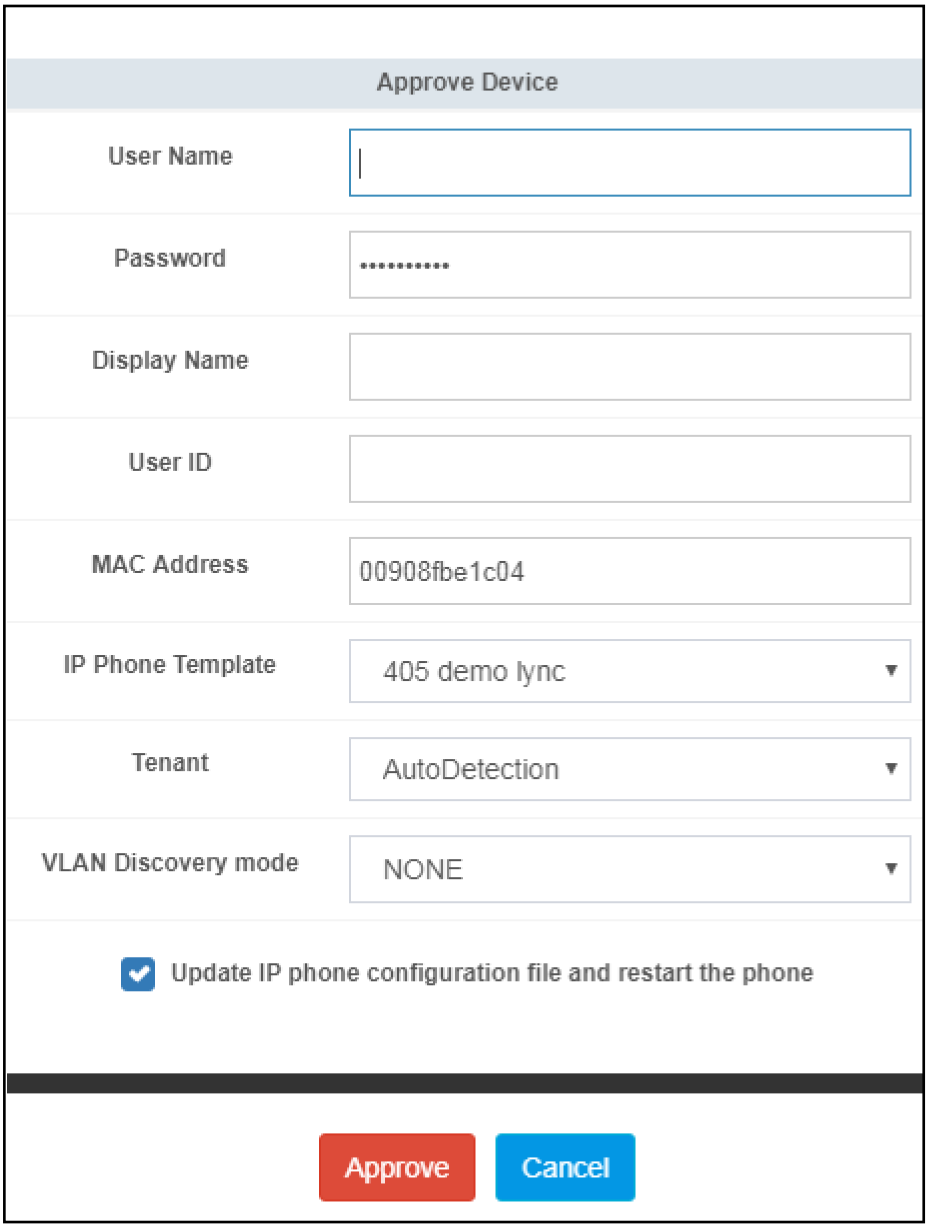
Filter

Showing 1 to 8 of 8 entries

☑	Selected Rows Actions	Approve Selected	✓	User	Phone Number	Last Update Status	MAC	IP	Model	Firmware Version	Region	Report Time	Location	Subnet	VLAN ID
☑	Actions		✓	spanishñ ab	+4467777778	27.12.2015 22:02:57	00908f5ffe11	10.21.2.16	430HD	UC_2.0.13.121	Lod	28.12.2015 15:03:06		255.255.0.0	
☑	Actions		✓	Yacov Alster	+97239764725	27.12.2015 10:07:49	00908f55fc8a	10.38.2.3	440HD	UC_2.0.13.121	NewYork	28.12.2015 15:08:07		255.255.0.0	
☑	Actions		✗	EMS_05	+97239766605	27.12.2015 10:05:54	00908f48794e	172.17.188.63	420HD	UC_2.0.13.121	NewYork	27.12.2015 10:05:54		255.255.255.0	
☑	Actions		✗	Shay Harel	+97239764720	27.12.2015 09:45:31	00908f484688	10.38.2.8	440HD	UC_2.0.13.121	NewYork	27.12.2015 09:45:31		255.255.0.0	
☑	Actions		✗	EMS_02		27.12.2015 09:18:40	00908f5ff919	172.17.188.62	430HD	UC_2.0.13.121	NewYork	27.12.2015 09:18:40		255.255.255.0	
☑	Actions		✗	EMS_03	+97239766603	27.12.2015 07:24:00	00908f480b4d	172.17.188.64	420HD	UC_2.0.13.121	NewYork	27.12.2015 19:24:13		255.255.255.0	
☑	Actions		✓	française	+3667777777	24.12.2015 16:27:54	00908f486a92	10.21.2.24	420HD	UC_2.0.13.121	Lod	28.12.2015 14:28:36		255.255.0.0	
☑	Actions		✓	Erez Gabbay	+97239764709	23.12.2015 16:14:39	00908f55fc77	10.22.13.170	440HD	UC_2.0.13.121	Lod	28.12.2015 15:07:04		255.255.255.0	213

2. Click the **Approve Selected** button; you're prompted to approve the phone/s selected.

Figure 9-3: 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

3. 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.

4. 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.

10 Managing Templates

This topic shows how to manage templates.

System Settings and Placeholders

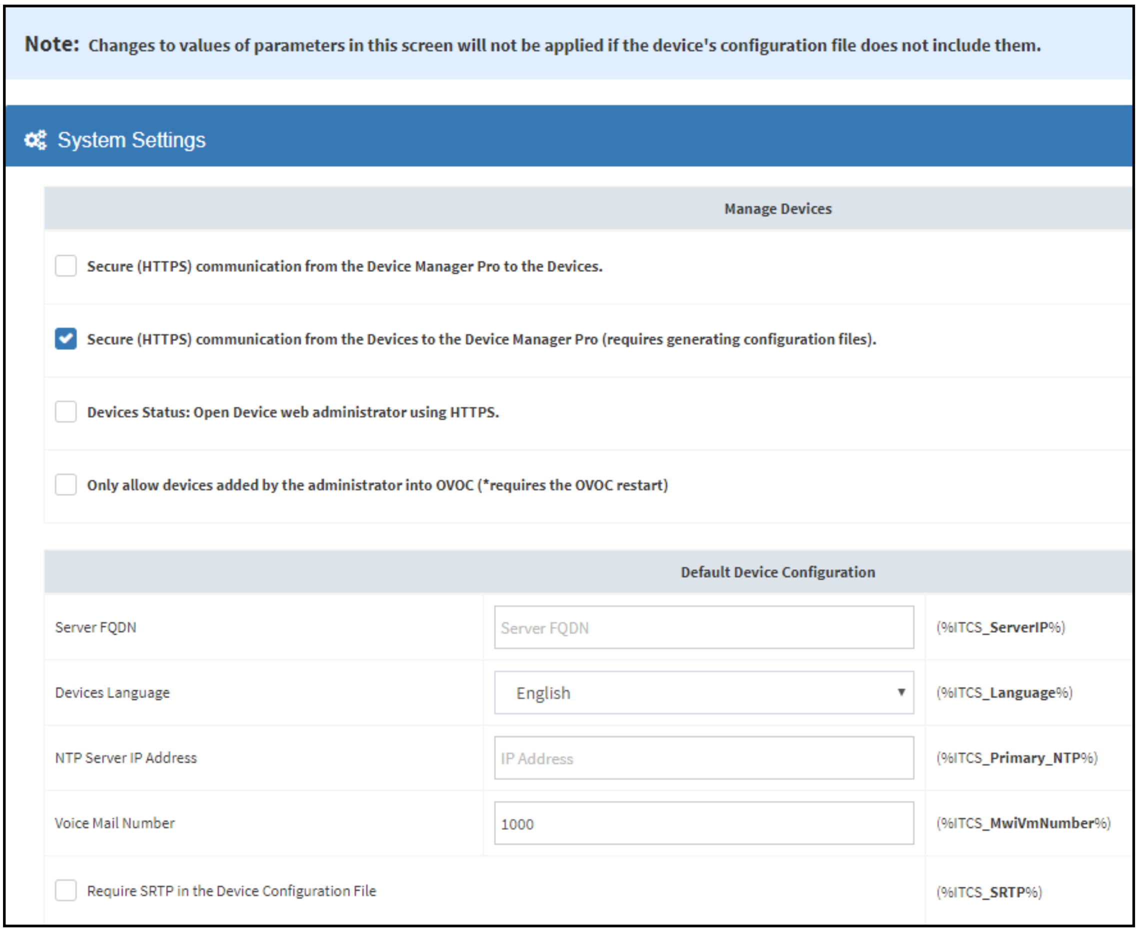
You can configure new placeholder values according to your enterprise's devices configuration requirements, in the System Settings screen .

You can view the default placeholders values in the Default Placeholders Values page.

➢ To configure new placeholder values:

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

Figure 10-1: System Settings



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

System Settings

Manage Devices

□ Secure (HTTPS) communication from the Device Manager Pro to the Devices.

☑ Secure (HTTPS) communication from the Devices to the Device Manager Pro (requires generating configuration files).

□ Devices Status: Open Device web administrator using HTTPS.

□ Only allow devices added by the administrator into OVOC (*requires the OVOC restart)

Default Device Configuration		
Server FQDN	Server FQDN	(%ITCS_ServerIP%)
Devices Language	English ▾	(%ITCS_Language%)
NTP Server IP Address	IP Address	(%ITCS_Primary_NTP%)
Voice Mail Number	1000	(%ITCS_MwiVmNumber%)
□ Require SRTP in the Device Configuration File		(%ITCS_SRTP%)

2. Configure values for available placeholders according to your enterprise's device configuration requirements. Use the table below as reference.

⚠ Except for parameters 'Devices Language' and 'Server FQDN', the parameters below only apply to enterprises whose environments are non Skype for Business.

Table 10-1: System Settings

Parameter	Description
Secure (HTTPS) communication from the IPP 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 here.
Secure (HTTPS) communication from the Devices to the IPP 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 here.
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 administrator into OVOC	Select this option to allow into the OVOC only those phones that were added by the network administrator. ■ 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.
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	

Parameter	Description
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.
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.
Administration Settings	
Disconnected Timeout	Default: 120 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.
Web UI Timezone	Sets the time zone for the Web interface. Used to determine if a device is disconnected when the keep-alive message for 'Disconnected Timeout' is not sent.
Outbound Proxy	
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.

Parameter	Description
Primary	Enter the primary PBX/Skype for Business server's IP address, i.e., the outbound proxy's.
Backup	Displayed only if you select the **Primary/Backup** option for the 'Redundant Mode' parameter (see above).
LDAP Configuration	Lightweight Directory Access Protocol lets you provide distributed directory information services to users in the enterprise. Not applicable in a Microsoft Skype for Business environment.
DHCP Option Configuration	Click this button if your phones are operating directly with a DHCP server without the mediation of an SBC HTTP proxy which is required when the phones are behind a NAT.
SBC Proxy Configuration	Click this button if your phones are operating with an SBC proxy. See also Editing the DHCP Option 160 cfg File on page 22.

3. Click **Save**.

Selecting a Template

Templates are available

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

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

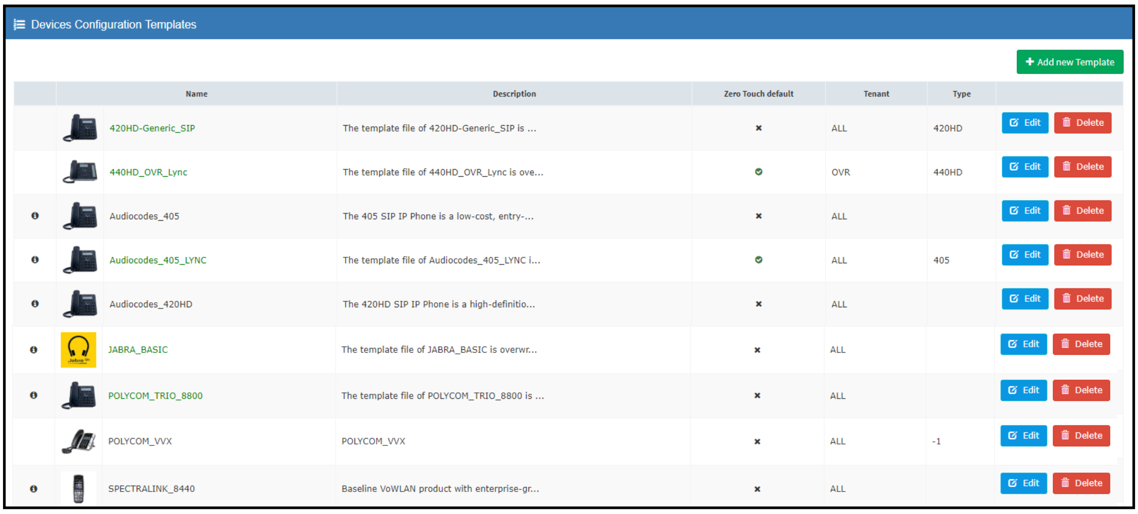
- AudioCodes 405
- AudioCodes 420HD
- AudioCodes 430HD
- AudioCodes 440HD
- AudioCodes 450HD
- AudioCodes 420HD Skype for Business
- AudioCodes 430HD Skype for Business
- AudioCodes 440HD Skype for Business
- AudioCodes 450HD Skype for Business

⚠ 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** > **Devices Configuration** > **Templates**):

Figure 10-2: Devices Configuration Templates



Devices Configuration Templates

		Name	Description	Zero Touch default	Tenant	Type	
		420HD-Generic_SIP	The template file of 420HD-Generic_SIP is ...	✗	ALL	420HD	Edit Delete
		440HD_OVR_Lync	The template file of 440HD_OVR_Lync is ove...	✓	OVR	440HD	Edit Delete
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		JABRA_BASIC	The template file of JABRA_BASIC is overwr...	✗	ALL		Edit Delete
ℹ		POLYCOM_TRIO_8800	The template file of POLYCOM_TRIO_8800 is ...	✗	ALL		Edit Delete
		POLYCOM_VVX	POLYCOM_VVX	✗	ALL	-1	Edit Delete
ℹ		SPECTRALINK_8440	Baseline VoWLAN product with enterprise-gr...	✗	ALL		Edit Delete

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

Editing a Configuration Template

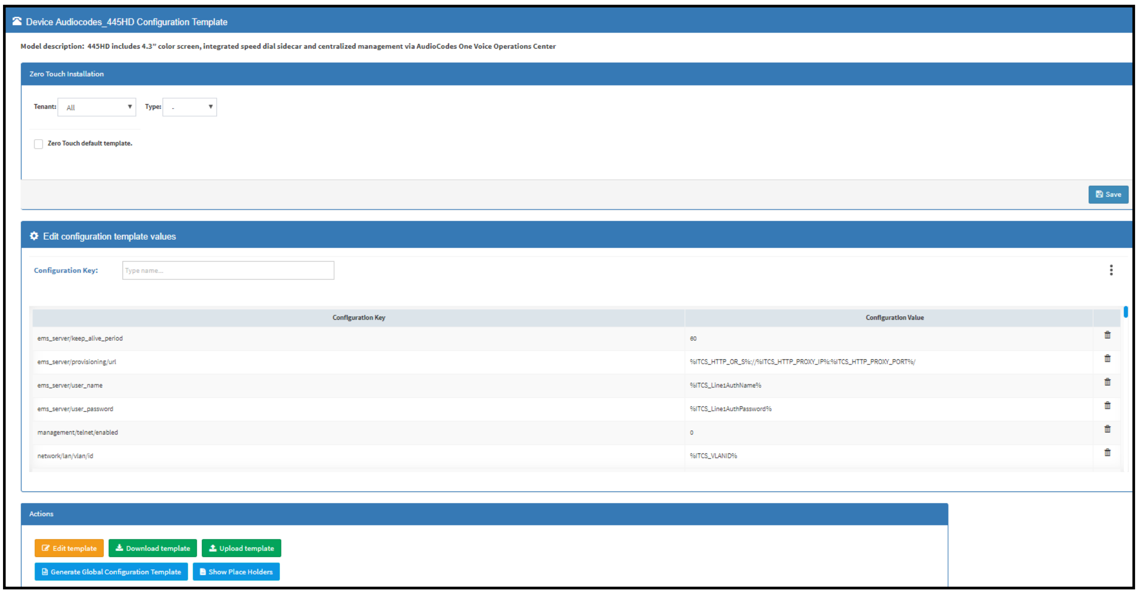
You can edit a device's template but typically it's unnecessary to change it.

> ⚠ 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** > **Devices Configuration** > **Templates**), click the link of the device or its **Edit** icon.

Figure 10-3: Device Configuration Template



Device Audiocodes_445HD Configuration Template

Model description: 445HD includes 4.3" color screen, integrated speed dial sidecar and centralized management via AudioCodes One Voice Operations Center

Zero Touch Installation

Tenant: All ▾ Type: - ▾

□ Zero Touch default template.

Edit configuration template values

Configuration Key: Type name...

Configuration Key	Configuration Value	
ems_server/keep_alive_period	60	🗑
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	🗑
network/lan/vlan/id	%ITCS_VLANID%	🗑

Actions

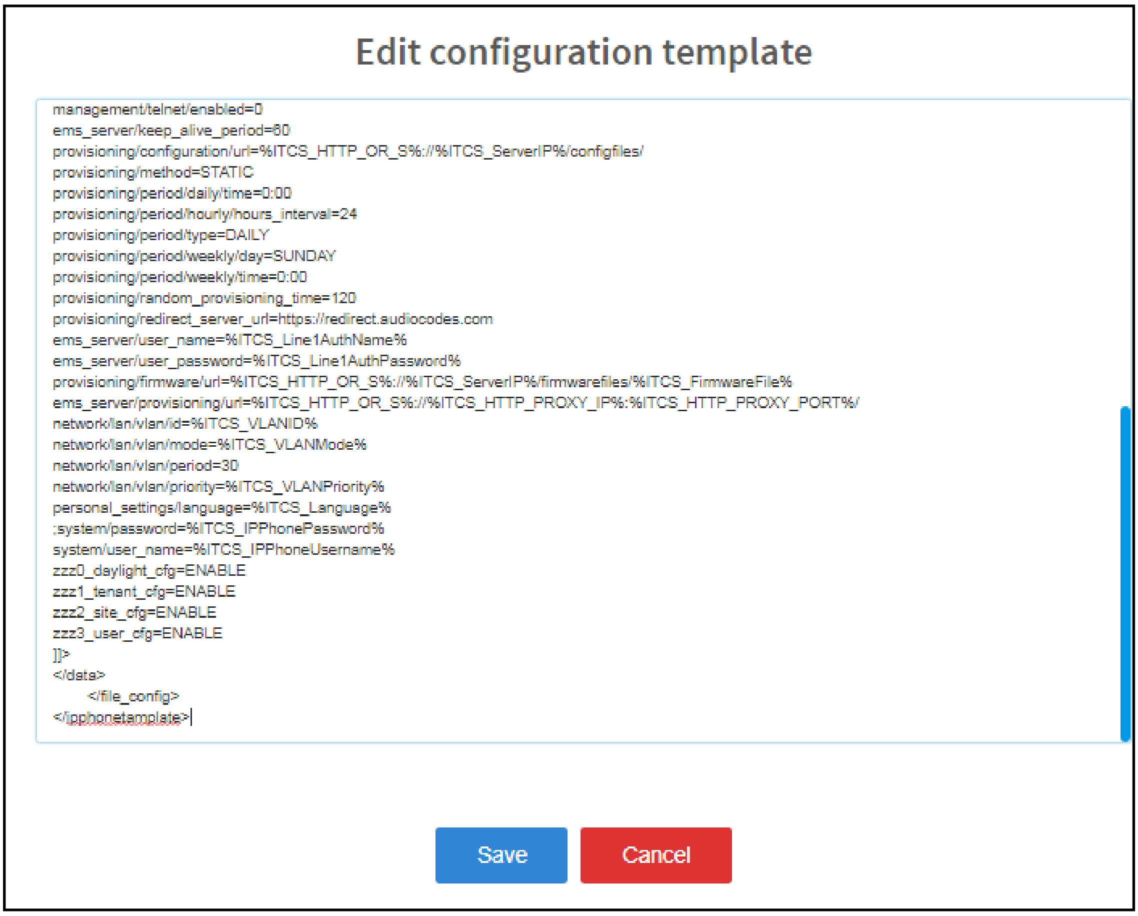
2. To use *this* template in the Zero Touch procedure:
   a. From the 'Tenant' dropdown under the Zero Touch Configuration screen section shown in the figure above, select the tenant.
   b. From the 'Type' dropdown, select the phone model.

c. Select the option Zero Touch default template.

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.

1. Click the **Edit configuration template** button; the template opens in an integral editor:

Figure 10-4: Edit Configuration Template



Edit configuration template

```
management/telnet/enabled=0
ems_server/keep_alive_period=60
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%/
network/lan/vlan/id=%ITCS_VLANID%
network/lan/vlan/mode=%ITCS_VLANMode%
network/lan/vlan/period=30
network/lan/vlan/priority=%ITCS_VLANPriority%
personal_settings/language=%ITCS_Language%
;system/password=%ITCS_IPPhonePassword%
system/user_name=%ITCS_IPPhoneUsername%
zzz0_daylight_cfg=ENABLE
zzz1_tenant_cfg=ENABLE
zzz2_site_cfg=ENABLE
zzz3_user_cfg=ENABLE
]]>
</data>
        </file_config>
</ipphonetamplate>
```

2. 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.

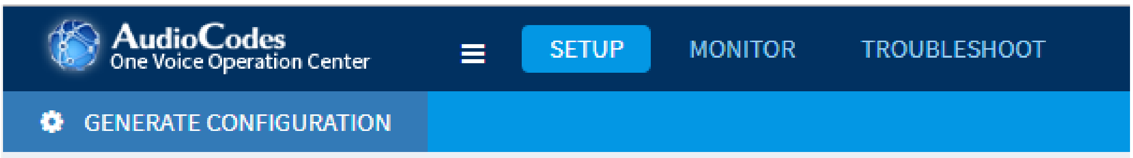
Generating an Edited Template

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:**

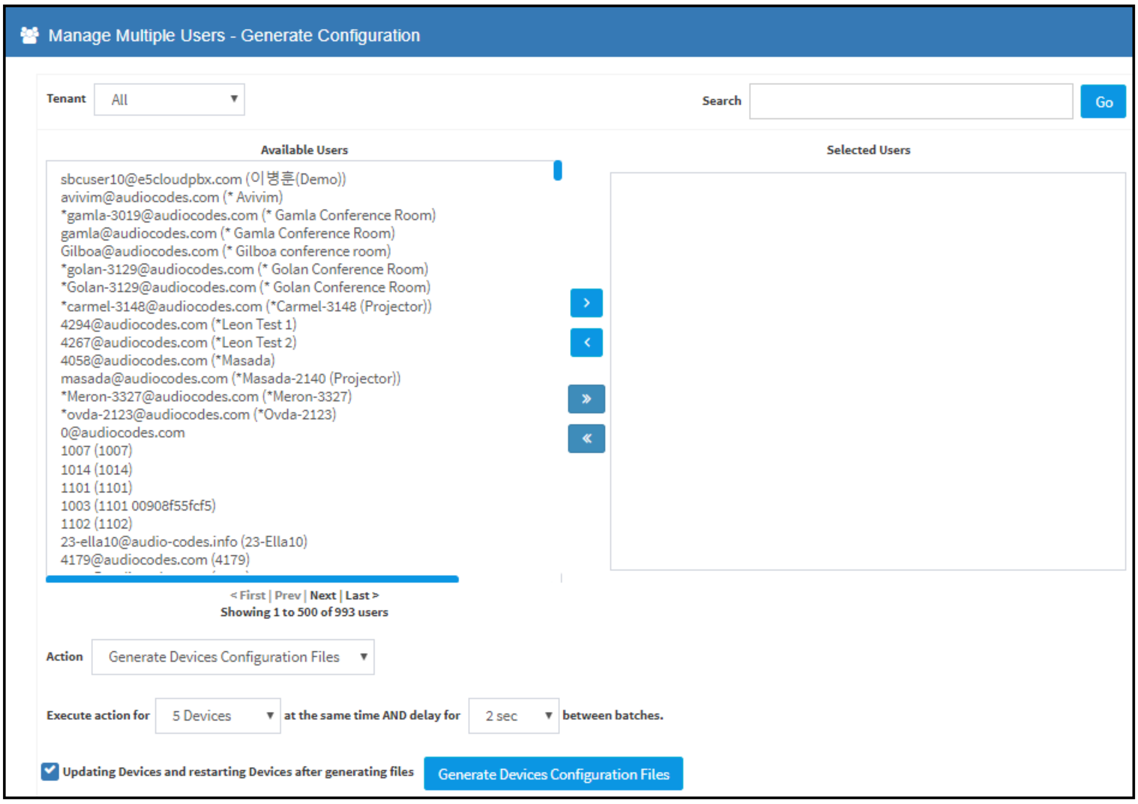
1. Click the **Generate Configuration** link located in the upper left corner of the screen, shown in the figure below.

Figure 10-5: Generate Configuration



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

Figure 10-6: Manage Multiple Users – Generate Configuration



Manage Multiple Users - Generate Configuration

Tenant: All

Search

Available Users

sbcuser10@e5cloudpbx.com (이병훈(Demo))
avivim@audiocodes.com (* Avivim)
gamla-3019@audiocodes.com (Gamla Conference Room)
gamla@audiocodes.com (* Gamla Conference Room)
Gilboa@audiocodes.com (* Gilboa conference room)
golan-3129@audiocodes.com (Golan Conference Room)
Golan-3129@audiocodes.com (Golan Conference Room)
*carmel-3148@audiocodes.com (*Carmel-3148 (Projector))
4294@audiocodes.com (*Leon Test 1)
4267@audiocodes.com (*Leon Test 2)
4058@audiocodes.com (*Masada)
masada@audiocodes.com (*Masada-2140 (Projector))
*Meron-3327@audiocodes.com (*Meron-3327)
*ovda-2123@audiocodes.com (*Ovda-2123)
0@audiocodes.com
1007 (1007)
1014 (1014)
1101 (1101)
1003 (1101 00908f55fcf5)
1102 (1102)
23-ella10@audio-codes.info (23-Ella10)
4179@audiocodes.com (4179)

Selected Users

< First | Prev | Next | Last >
Showing 1 to 500 of 993 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

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

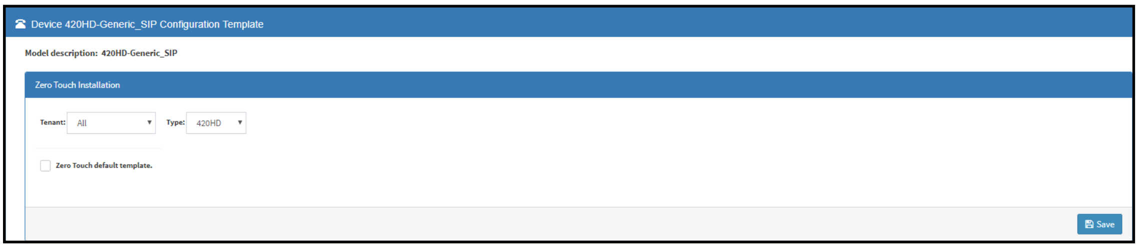
Defining Template Placeholders

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

Figure 10-7: Devices Configuration Template



Device 420HD-Generic_SIP Configuration Template

Model description: 420HD-Generic_SIP

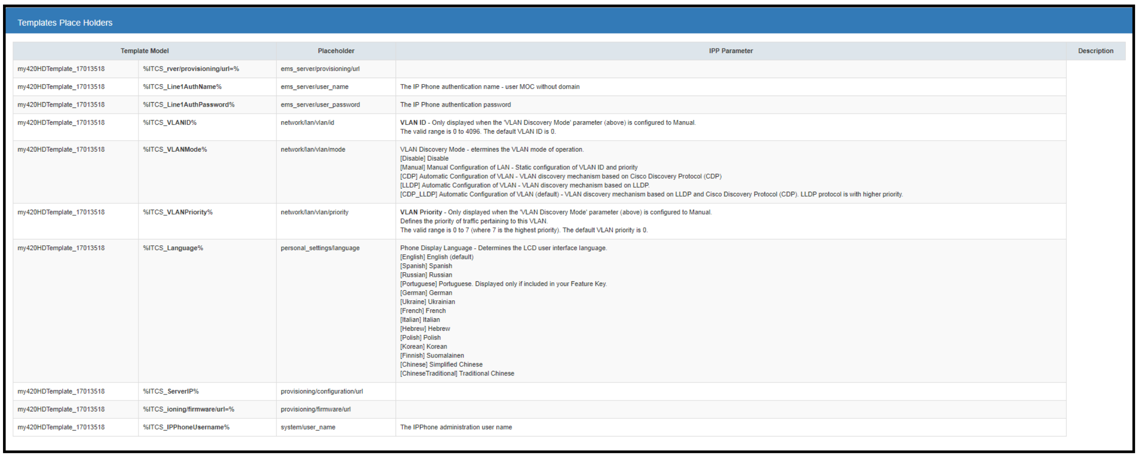
Zero Touch Installation

Tenant: All Type: 420HD

□ Zero Touch default template.

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

Figure 10-8: Templates Placeholders



Templates Place Holders

Template Model		Placeholder	IPP Parameter	Description
my420HDTemplate_17013518	%ITCS_**rver/provisioning/url=**%	ems_server/provisioning/url		
my420HDTemplate_17013518	%ITCS_**Line1AuthName**%	ems_server/user_name	The IP Phone authentication name - user MOC without domain	
my420HDTemplate_17013518	%ITCS_**Line1AuthPassword**%	ems_server/user_password	The IP Phone authentication password	
my420HDTemplate_17013518	%ITCS_**VLANID**%	network/lan/vlan/id	**VLAN ID** - Only displayed when the 'VLAN Discovery Mode' parameter (above) is configured to Manual. The valid range is 0 to 4096. The default VLAN ID is 0.	
my420HDTemplate_17013518	%ITCS_**VLANMode**%	network/lan/vlan/mode	VLAN Discovery Mode - etermines the VLAN mode of operation. [Disable] Disable [Manual] Manual Configuration of LAN - Static configuration of VLAN ID and priority [CDP] Automatic Configuration of VLAN - VLAN discovery mechanism based on Cisco Discovery Protocol (CDP) [LLDP] Automatic Configuration of VLAN - VLAN discovery mechanism based on LLDP. [CDP_LLDP] Automatic Configuration of VLAN (default) - VLAN discovery mechanism based on LLDP and Cisco Discovery Protocol (CDP). LLDP protocol is with higher priority.	
my420HDTemplate_17013518	%ITCS_**VLANPriority**%	network/lan/vlan/priority	**VLAN Priority** - Only displayed when the 'VLAN Discovery Mode' parameter (above) is configured to Manual. Defines the priority of traffic pertaining to this VLAN. The valid range is 0 to 7 (where 7 is the highest priority). The default VLAN priority is 0.	
my420HDTemplate_17013518	%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	
my420HDTemplate_17013518	%ITCS_**ServerIP**%	provisioning/configuration/url		
my420HDTemplate_17013518	%ITCS_**ioning/firmware/url=**%	provisioning/firmware/url		
my420HDTemplate_17013518	%ITCS_**IPPhoneUsername**%	system/user_name	The IPPhone administration user name	

The figure above shows placeholders currently defined in the xml Configuration Template file for the 420HD phone. There are four kinds of placeholders: (1) System (2) Template (3) Tenant (4) Devices.

- To manage an available placeholder, see here.
- To add/edit/delete a template placeholder, see here.
- To add/edit/delete a tenant placeholder, see here.
- To add/edit/delete a device placeholder, see here.

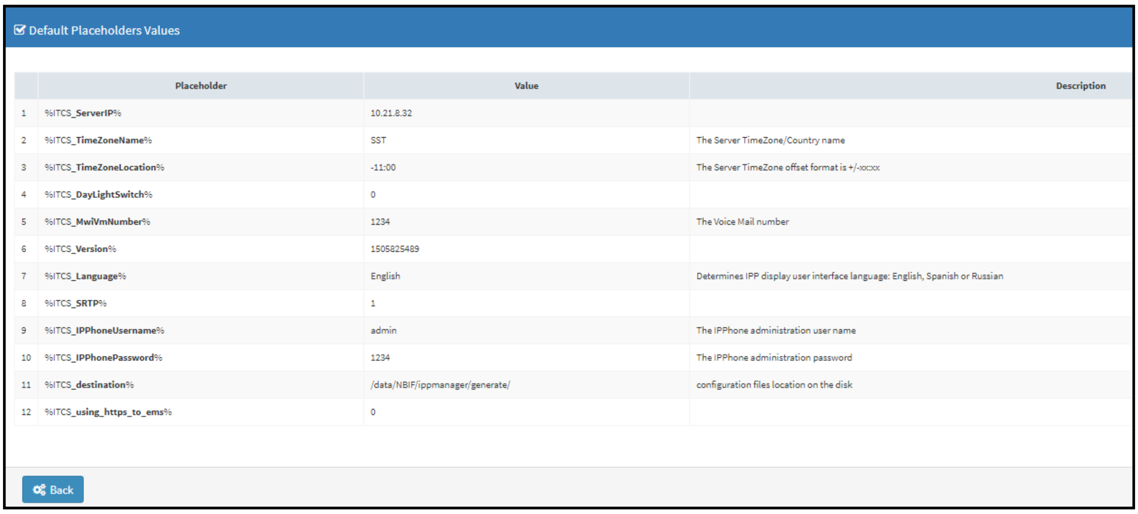
Viewing Default Placeholders Values

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

➢ To view default placeholders values:

- Open the Default Placeholders Values page (**Setup** > **Devices Configuration** > **System Settings**) and then click the **Default Placeholders Values** button located lowermost in the page.

Figure 10-9: Default Placeholders Values



☑ Default Placeholders Values

	Placeholder	Value	Description
1	%ITCS_**ServerIP**%	10.21.8.32	
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**%	1234	The Voice Mail number
6	%ITCS_**Version**%	1505825489	
7	%ITCS_**Language**%	English	Determines IPP display user interface language: English, Spanish or Russian
8	%ITCS_**SRTP**%	1	
9	%ITCS_**IPPhoneUsername**%	admin	The IPPhone administration user name
10	%ITCS_**IPPhonePassword**%	1234	The IPPhone administration password
11	%ITCS_**destination**%	/data/NBIF/ippmanager/generate/	configuration files location on the disk
12	%ITCS_**using_https_to_ems**%	0	

Template Placeholders

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

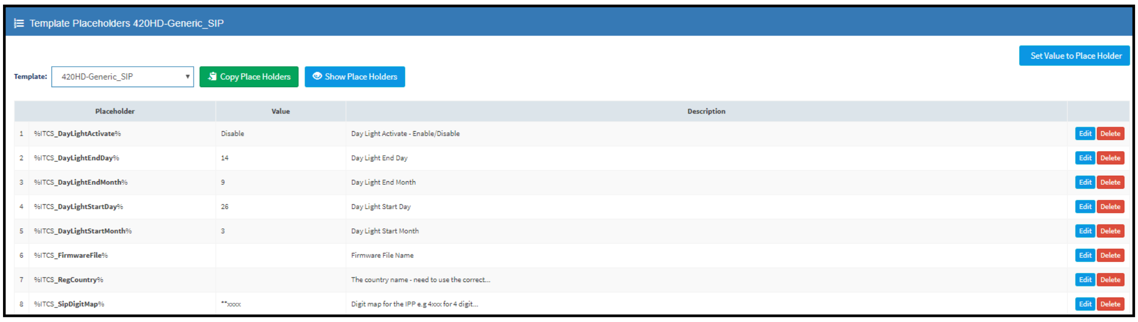
Editing Template Placeholders

You can edit the values for existing template placeholders.

➢ To edit values for existing template placeholders:

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

Figure 10-10: Template Placeholders



Template Placeholders 420HD-Generic_SIP
Set Value to Place Holder
Copy Place Holders
Show Place Holders

Template: 420HD-Generic_SIP

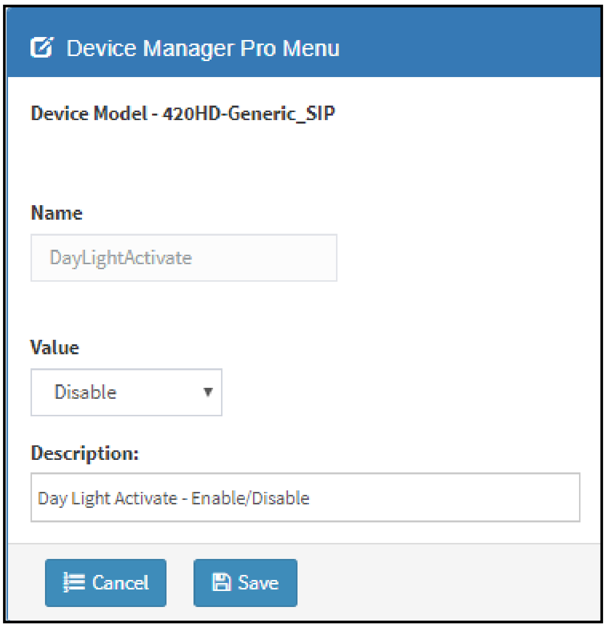
	Placeholder	Value	Description	
1	%ITCS_DayLightActivate%	Disable	Day Light Activate - Enable/Disable	Edit Delete
2	%ITCS_DayLightEndDay%	14	Day Light End Day	Edit Delete
3	%ITCS_DayLightEndMonth%	9	Day Light End Month	Edit Delete
4	%ITCS_DayLightStartDay%	26	Day Light Start Day	Edit Delete
5	%ITCS_DayLightStartMonth%	3	Day Light Start Month	Edit Delete
6	%ITCS_FirmwareFile%		Firmware File Name	Edit Delete
7	%ITCS_RegCountry%		The country name - need to use the correct...	Edit Delete
8	%ITCS_SipDigitMap%	**xxxx	Digit map for the IPP e.g 4xxx for 4 digit...	Edit Delete

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 10-11: Edit Template Placeholder



Device Model - 420HD-Generic_SIP

Name: DayLightActivate

Value: Disable

Description: Day Light Activate - Enable/Disable

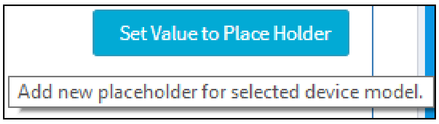
2. In the 'Name' field, you can edit the name of the placeholder.
3. In the 'Value' field, you can edit the value of the placeholder.
4. In the 'Description' field, you can edit the placeholder description.
5. Click **Save**; the edited placeholder is added to the table.

Adding a New Template Placeholder

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

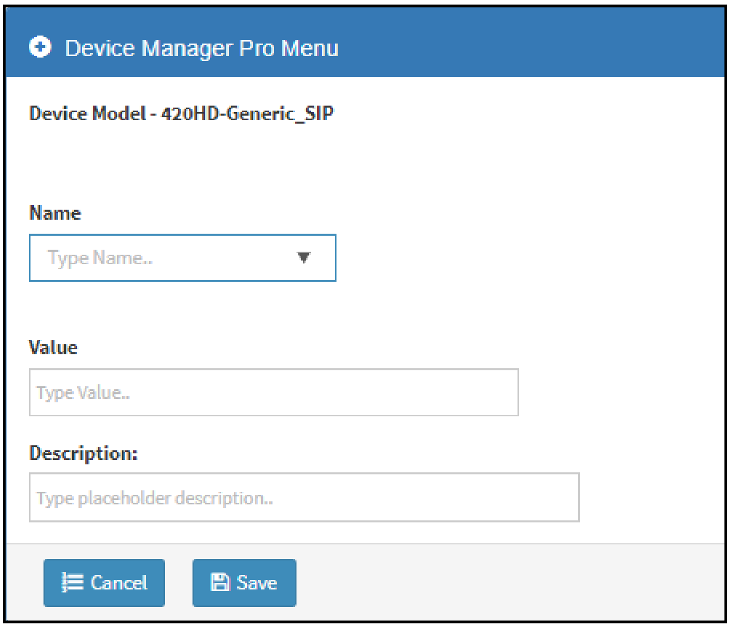
➢ To add a new template placeholder:

1. Open the Template Placeholders page (**Setup** > **Devices Configuration** > **Template Placeholders**):
2. From the **Template** dropdown, select the template , e.g., Audiocodes_420HD.
3. Click the **Set Value to Place Holder** button located in the upper right corner of the screen.



Set Value to Place Holder
Add new placeholder for selected device model.

Figure 10-12: Add New Template Placeholder



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.

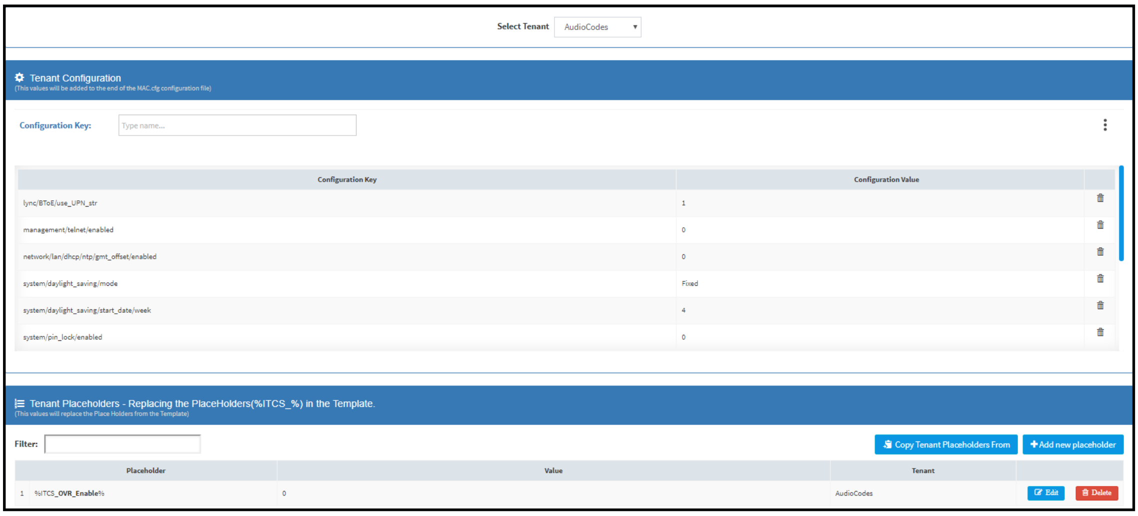
Editing Tenant Placeholders

You can edit the values for existing tenant placeholders.

➢ To edit values for existing tenant placeholders:

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

Figure 10-13: Tenant Configuration – Tenant Placeholders



Select Tenant: AudioCodes

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

Configuration Key: Type name...

Configuration Key	Configuration Value
lync/BToE/use_UPN_str	1
management/telnet/enabled	0
network/lan/dhcp/ntp/gmt_offset/enabled	0
system/daylight_saving/mode	Fixed
system/daylight_saving/start_date/week	4
system/pin_lock/enabled	0

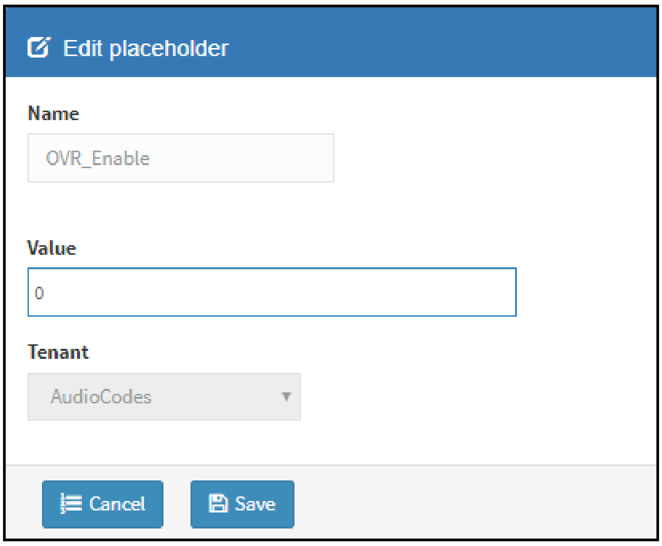
Tenant Placeholders - Replacing the PlaceHolders(%ITCS_%) in the Template.
(This values will replace the Place Holders from the Template)

Filter:

	Placeholder	Value	Tenant	
1	%ITCS_**OVR_Enable**%	0	AudioCodes	Edit Delete

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

Figure 10-14: Edit Placeholder



Edit placeholder

Name: OVR_Enable

Value: 0

Tenant: AudioCodes

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.

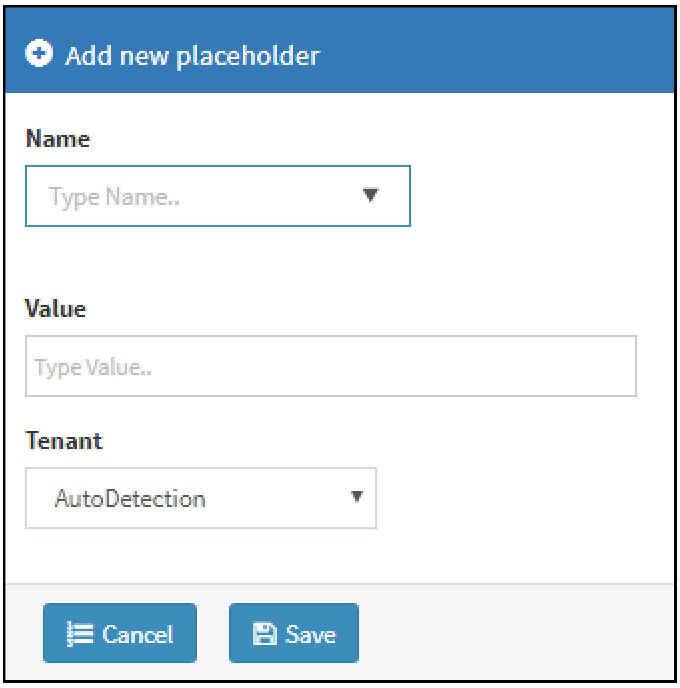
Adding a New Tenant Placeholder

You can add a new tenant placeholder.

➢ To add a new tenant placeholder:

1. Open the Tenant Configuration page (**Setup** > **Devices Configuration** > **Tenant Configuration**).
2. Under the Tenant Placeholders section of the page, click the **+Add new placeholder** button.

Figure 10-15: Add New Placeholder



Add new placeholder

Name

Type Name..

Value

Type Value..

Tenant

AutoDetection

3. In the 'Name' field, enter the name of the new placeholder.
4. In the 'Value' field, enter the value of the new placeholder.
5. From the 'Tenant' dropdown, select a new tenant.
6. Click **Save**; the new placeholder is added to the table.

Devices Placeholders

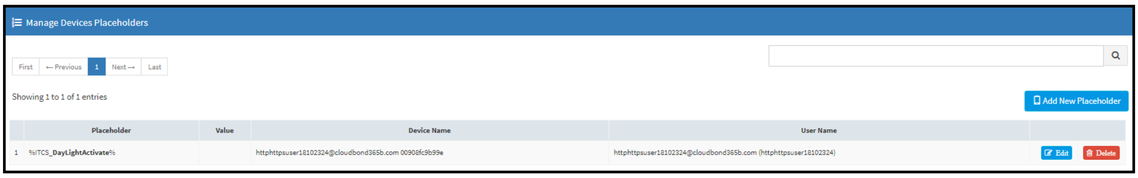
You can change placeholders values for specific phones, for example, you can change placeholders values for the CEO's phone. You can also edit a device's placeholders values.

Changing a Device Placeholder Value

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

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

Figure 10-16: Manage Devices Placeholders



Manage Devices Placeholders

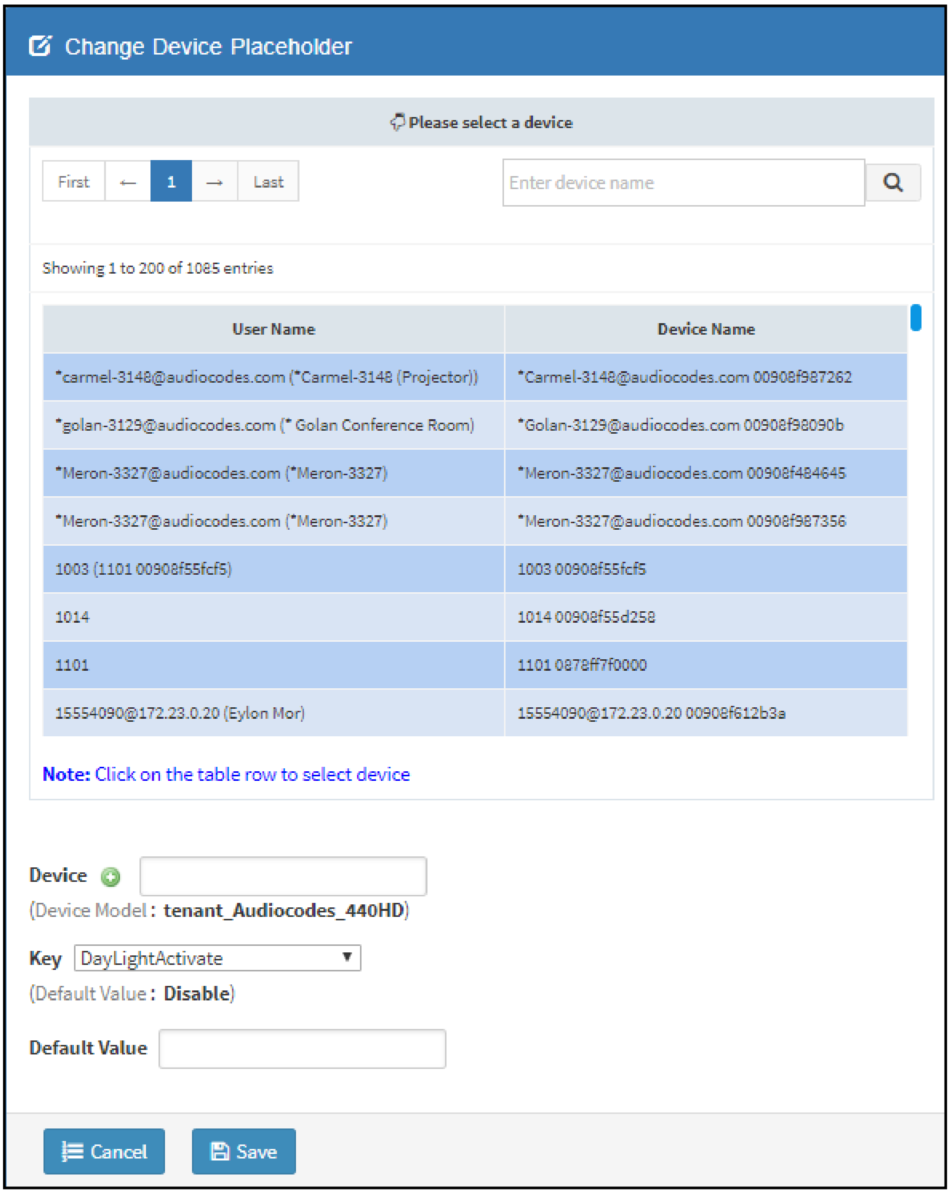
Showing 1 to 1 of 1 entries

	Placeholder	Value	Device Name	User Name	
1	%ITCS_DayLightActivate%		httphttpsuser18102324@cloudbond365b.com 00908fc9b99e	httphttpsuser18102324@cloudbond365b.com (httphttpsuser18102324)	Edit Delete

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 10-17: Change Device Placeholder



Change Device Placeholder

Please select a device

Showing 1 to 200 of 1085 entries

User Name	Device Name
*carmel-3148@audiocodes.com (*Carmel-3148 (Projector))	*Carmel-3148@audiocodes.com 00908f987262
golan-3129@audiocodes.com (Golan Conference Room)	*Golan-3129@audiocodes.com 00908f98090b
*Meron-3327@audiocodes.com (*Meron-3327)	*Meron-3327@audiocodes.com 00908f484645
*Meron-3327@audiocodes.com (*Meron-3327)	*Meron-3327@audiocodes.com 00908f987356
1003 (1101 00908f55fcf5)	1003 00908f55fcf5
1014	1014 00908f55d258
1101	1101 0878ff7f0000
15554090@172.23.0.20 (Eylon Mor)	15554090@172.23.0.20 00908f612b3a

Note: Click on the table row to select device

Device

(Device Model : **tenant_Audiocodes_440HD**)

Key DayLightActivate ▼

(Default Value : **Disable**)

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.

11 Configuring the LDAP Directory

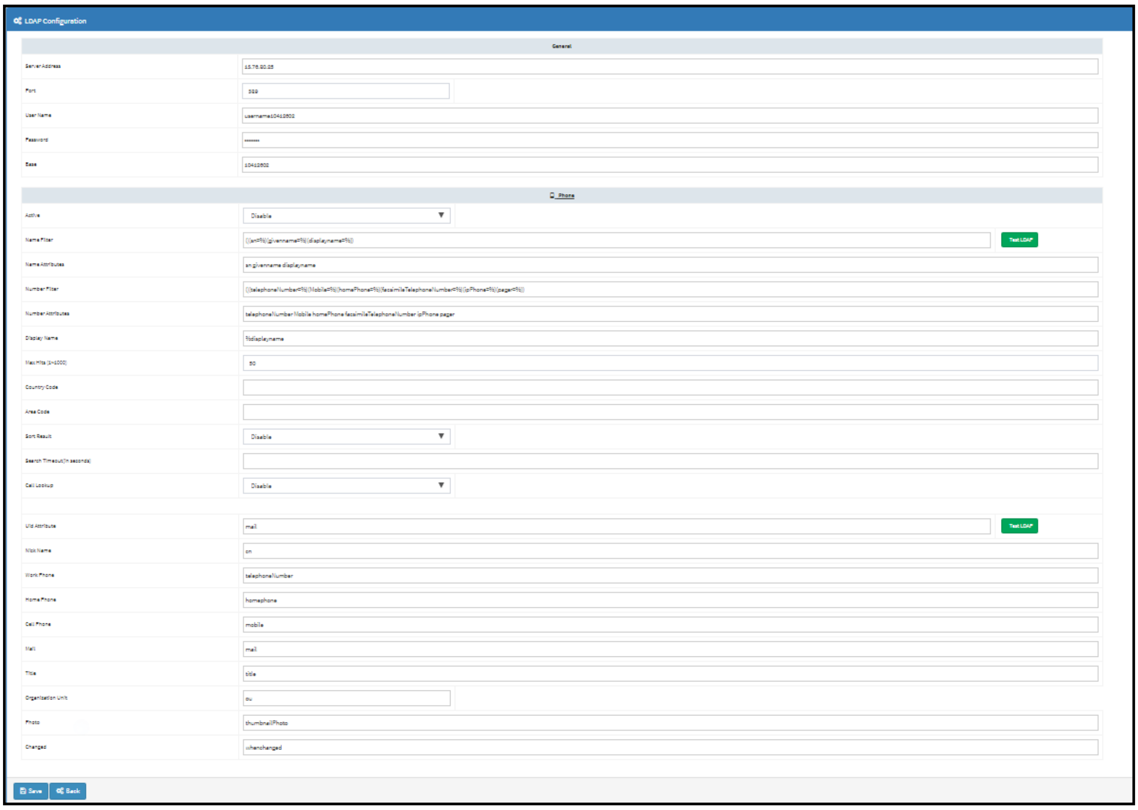
This section is inapplicable if you're operating in a Microsoft Skype for Business environment because Skype for Business uses its own Active Directory server.

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

➢ To access the LDAP directory:

1. Open the System Settings page (**Setup** > **Phones Configuration** > **System Settings**).
2. Click the **LDAP Configuration** button.

Figure 11-1: LDAP Configuration



Server Address: 15.76.90.25
Port: 389
User Name: username10412602
Password: ********
Base: 10412602
Active: Disable
Name Filter: (|(sn=%)(givenname=%)(displayname=%))
Name Attributes: sn givenname displayname
Number Filter: (|(telephoneNumber=%)(Mobile=%)(homePhone=%)(facsimileTelephoneNumber=%)(ipPhone=%)(pager=%))
Number Attributes: telephoneNumber Mobile homePhone facsimileTelephoneNumber ipPhone pager
Display Name: %displayname
Max Hits (1~1000): 50
Country Code:
Area Code:
Sort Result: Disable
Search Timeout(in seconds):
Call Lookup: Disable
Uid Attribute: mail
Nick Name: cn
Work Phone: telephoneNumber
Home Phone: homephone
Cell Phone: mobile
Mail: mail
Title: title
Organization Unit: ou
Photo: thumbnailPhoto
Changed: whenchanged

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

Table 11-1: 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.

Parameter	Description
Base	Enter the access point on the LDAP tree.
Active	From the dropdown, select **Disable** LDAP (default) or **Enable** LDAP. If **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 Code	Defines the country code prefix added for number search.
Area Code	Defines the area code prefix added for number search.
Sort Result	Sorts the search result by display name on the client side.

Parameter	Description
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**.

12 Managing Device Manager 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.

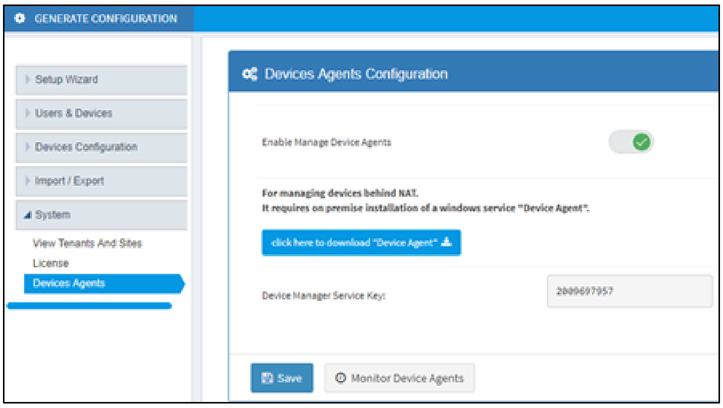
Enabling Device Manager to Support Agents

Network administrators must enable the Device Manager to support Agents.

➢ To enable the Device Manager to support Agents:

1. In the Device Manager, open the Devices Agents Configuration page (**Setup** > **System** > **Device Agents**).
2. Drag the **Enable Manager Device Agents** slider to the 'on' position.

Figure 13-1: Enabling Manager Device to Support Agents



Enable Manage Device Agents ✓

For managing devices behind NAT.
It requires on premise installation of a windows service "Device Agent".

Device Manager Service Key: 2009697957

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.

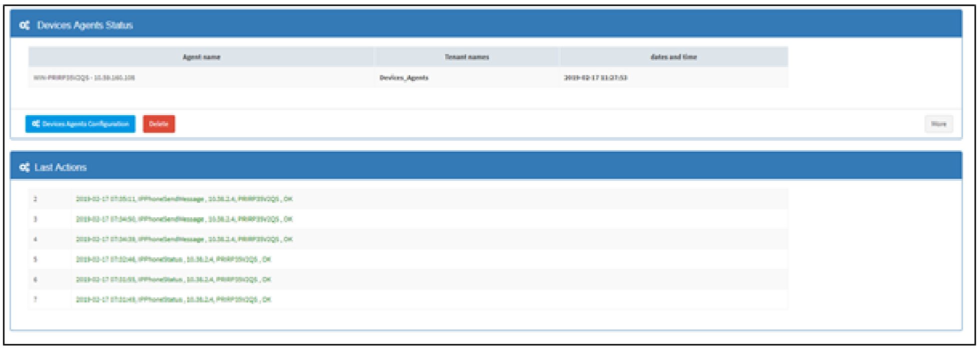
Monitoring Device Manager Agents

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.

Figure 14-1: Monitoring Device Manager Agents



Devices Agents Status

Agent name	Tenant names	dates and time
WIN-PRIRP35V2Q5 - 10.59.160.108	Devices_Agents	2019-02-17 11:27:53

Last Actions

2	2019-02-17 07:35:11, IPPhoneSendMessage , 10.38.2.4, PRIRP35V2Q5 , OK
3	2019-02-17 07:34:50, IPPhoneSendMessage , 10.38.2.4, PRIRP35V2Q5 , OK
4	2019-02-17 07:34:39, IPPhoneSendMessage , 10.38.2.4, PRIRP35V2Q5 , OK
5	2019-02-17 07:32:46, IPPhoneStatus , 10.38.2.4, PRIRP35V2Q5 , OK
6	2019-02-17 07:31:55, IPPhoneStatus , 10.38.2.4, PRIRP35V2Q5 , OK
7	2019-02-17 07:31:45, IPPhoneStatus , 10.38.2.4, PRIRP35V2Q5 , OK

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

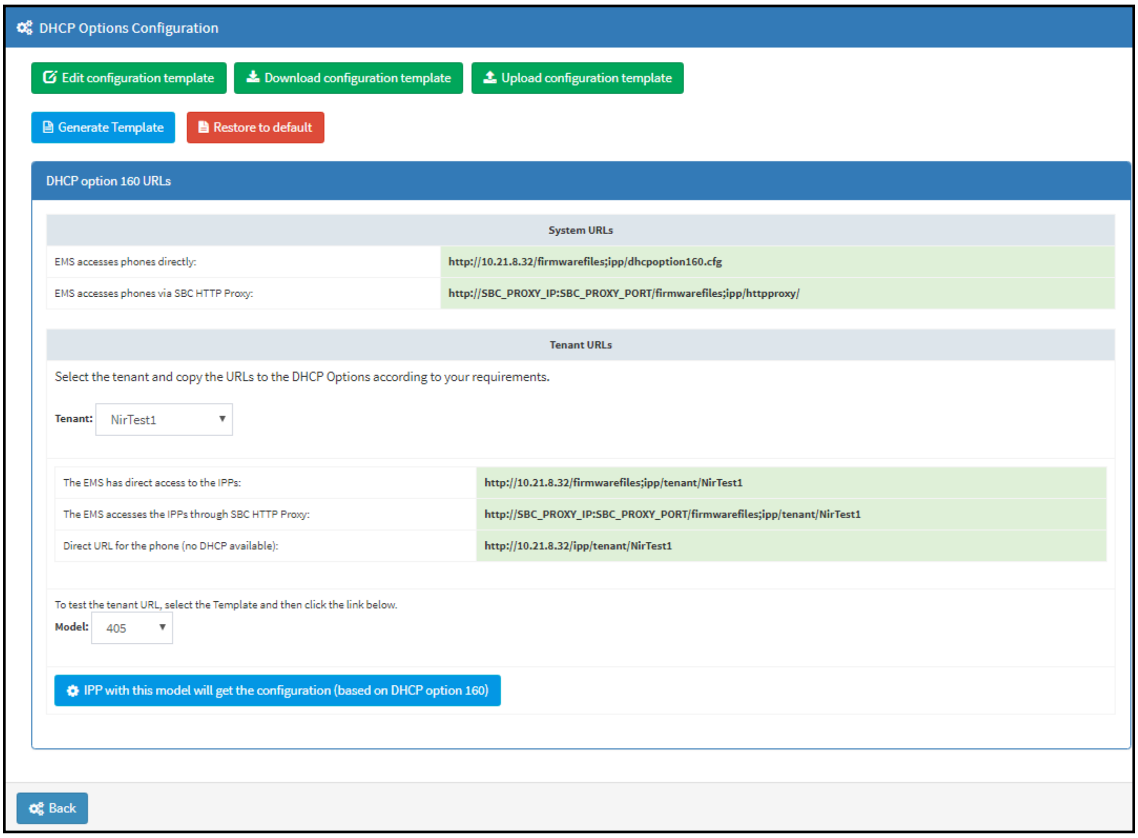
15 Configuring Phones to Operate in an OVR Deployment

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 System Settings page (**Setup** > **Phones Configuration** > **System Settings**) and then click the **DHCP Option Configuration** button.

Figure 15-1: Edit DHCP Option


DHCP Options Configuration
Edit configuration template
Download configuration template
Upload configuration template
Generate Template
Restore to default
DHCP option 160 URLs
IPP with this model will get the configuration (based on DHCP option 160)
Back

System URLs	
EMS accesses phones directly:	http://10.21.8.32/firmwarefiles;ipp/dhcpoption160.cfg
EMS accesses phones via SBC HTTP Proxy:	http://SBC_PROXY_IP:SBC_PROXY_PORT/firmwarefiles;ipp/httpproxy/

Tenant URLs

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

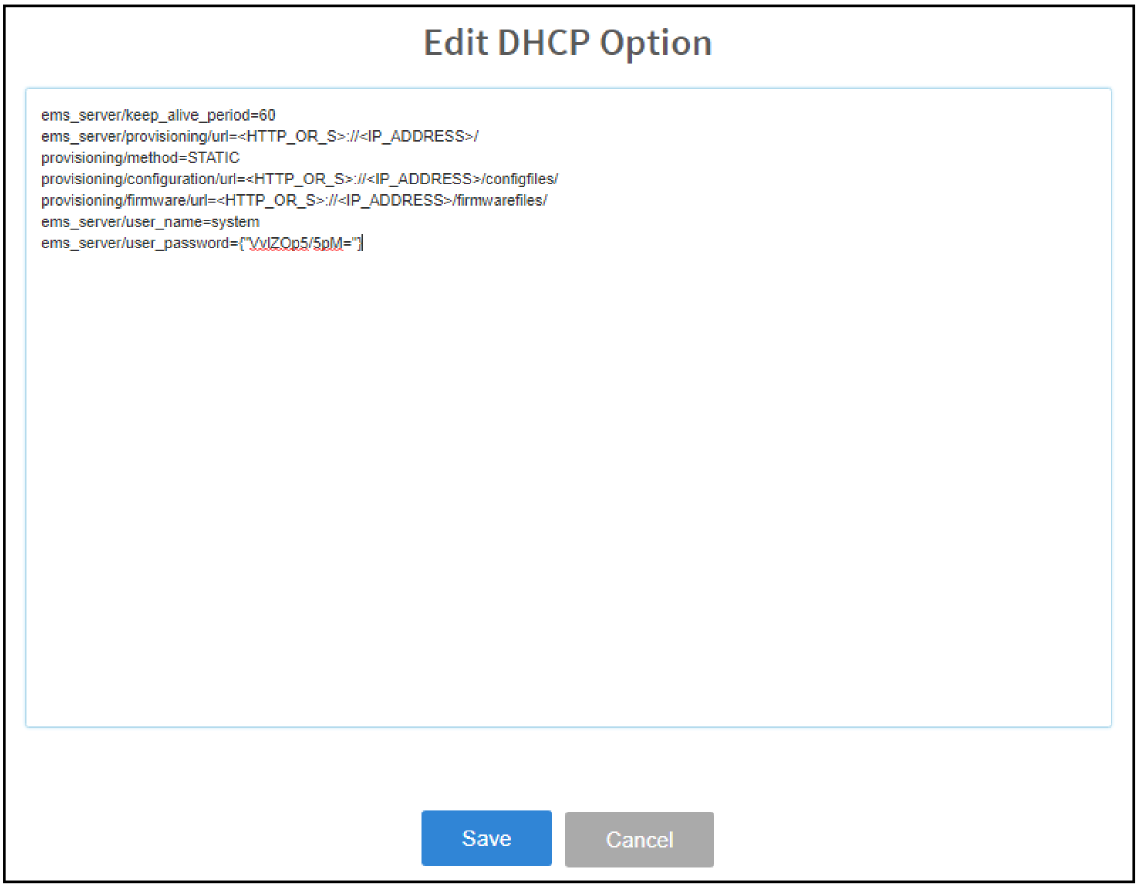
Tenant: NirTest1 ▾

The EMS has direct access to the IPPs:	http://10.21.8.32/firmwarefiles;ipp/tenant/NirTest1
The EMS accesses the IPPs through SBC HTTP Proxy:	http://SBC_PROXY_IP:SBC_PROXY_PORT/firmwarefiles;ipp/tenant/NirTest1
Direct URL for the phone (no DHCP available):	http://10.21.8.32/ipp/tenant/NirTest1

To test the tenant URL, select the Template and then click the link below.

Model: 405 ▾

2. Click the **Edit configuration template** button.



```
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={"VvlZOp5/5pM="}
```

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.

16 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.

17 Troubleshooting

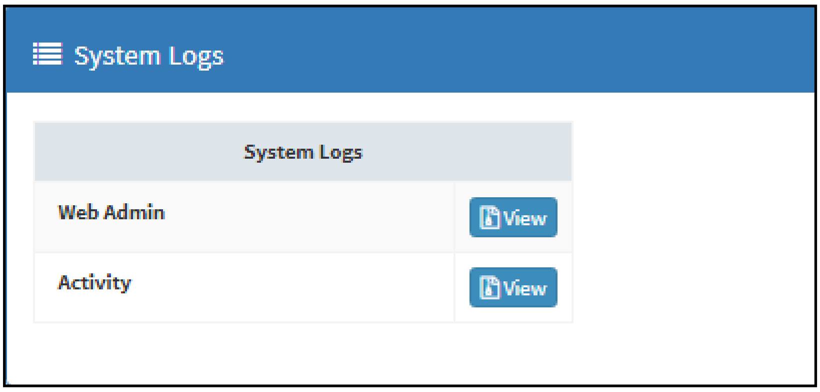
You can display system logs to help troubleshoot problems and determine cause. System logs comprise:

- 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 logs:**

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

Figure 17-1: System Logs



System Logs

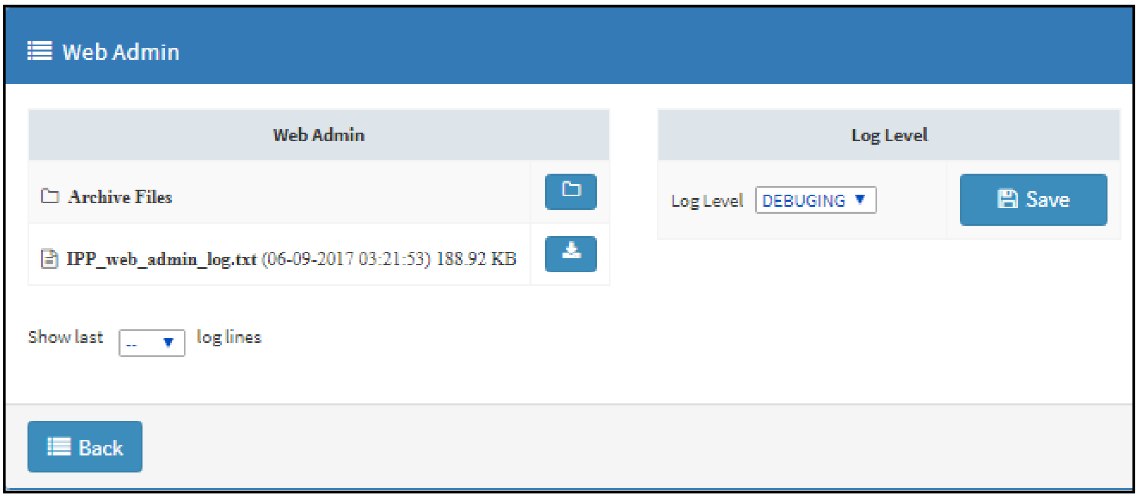
System Logs	
Web Admin	View
Activity	View

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 17-2: Web Admin



Web Admin

Web Admin	
Archive Files	
IPP_web_admin_log.txt (06-09-2017 03:21:53) 188.92 KB	

Log Level	
Log Level DEBUGING	Save

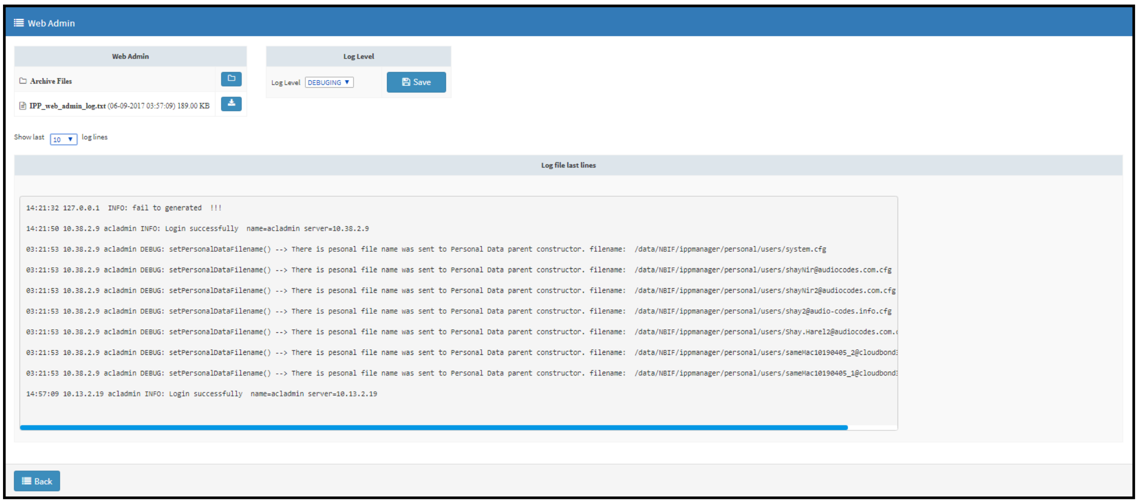
Show last -- log lines

Back

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 17-3: Last Activities Logged in the Web Interface



IPP_web_admin_log.txt (06-09-2017 03:57:09) 189.00 KB

Log Level DEBUGING

Show last 10 log lines

```
14:21:32 127.0.0.1  INFO: fail to generated  !!!

14:21:50 10.38.2.9 acladmin INFO: Login successfully  name=acladmin server=10.38.2.9

03:21:53 10.38.2.9 acladmin DEBUG: setPersonalDataFilename() --> There is pesonal file name was sent to Personal Data parent constructor. filename:  /data/NBIF/ippmanager/personal/users/system.cfg

03:21:53 10.38.2.9 acladmin DEBUG: setPersonalDataFilename() --> There is pesonal file name was sent to Personal Data parent constructor. filename:  /data/NBIF/ippmanager/personal/users/shayNir@audiocodes.com.cfg

03:21:53 10.38.2.9 acladmin DEBUG: setPersonalDataFilename() --> There is pesonal file name was sent to Personal Data parent constructor. filename:  /data/NBIF/ippmanager/personal/users/shayNir2@audiocodes.com.cfg

03:21:53 10.38.2.9 acladmin DEBUG: setPersonalDataFilename() --> There is pesonal file name was sent to Personal Data parent constructor. filename:  /data/NBIF/ippmanager/personal/users/shay2@audio-codes.info.cfg

03:21:53 10.38.2.9 acladmin DEBUG: setPersonalDataFilename() --> There is pesonal file name was sent to Personal Data parent constructor. filename:  /data/NBIF/ippmanager/personal/users/Shay.Harel2@audiocodes.com.

03:21:53 10.38.2.9 acladmin DEBUG: setPersonalDataFilename() --> There is pesonal file name was sent to Personal Data parent constructor. filename:  /data/NBIF/ippmanager/personal/users/sameMac10190405_2@cloudbond

03:21:53 10.38.2.9 acladmin DEBUG: setPersonalDataFilename() --> There is pesonal file name was sent to Personal Data parent constructor. filename:  /data/NBIF/ippmanager/personal/users/sameMac10190405_1@cloudbond

14:57:09 10.13.2.19 acladmin INFO: Login successfully  name=acladmin server=10.13.2.19
```

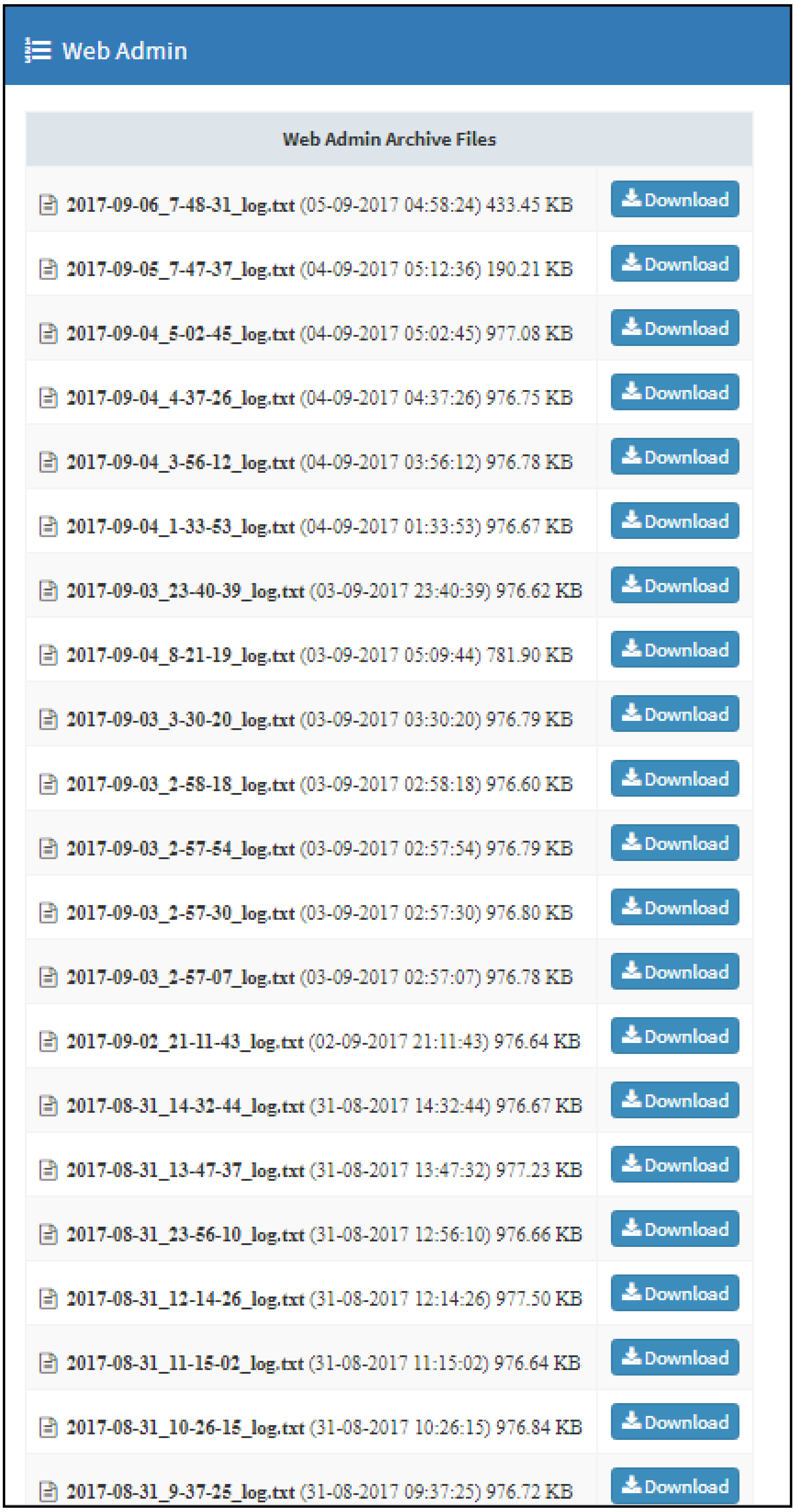
5. Click **Save** to save the last logged activities performed in the Web interface and share the log file with others.

Displaying Archived Activities Performed in the Web Interface

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

- In the System Logs page, click **View** next to **Web Admin** and then in the Web Admin page, click the icon next to **Archive Files**.

Figure 17-4: Archive Files



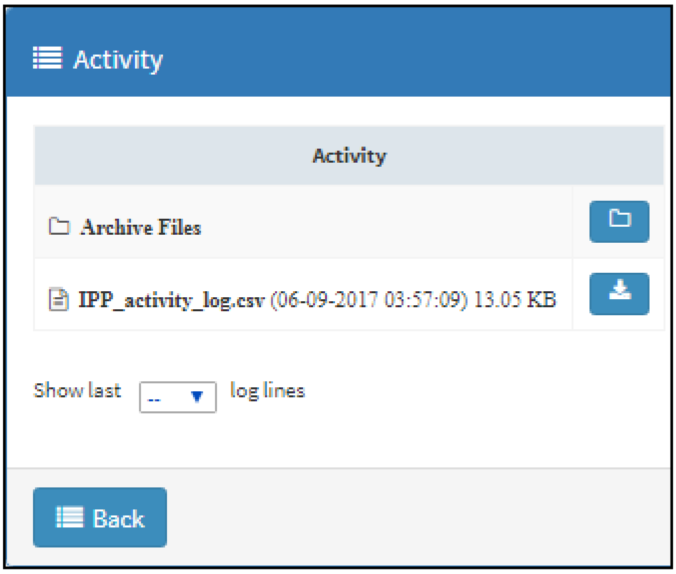
Web Admin Archive Files	
2017-09-06_7-48-31_log.txt (05-09-2017 04:58:24) 433.45 KB	Download
2017-09-05_7-47-37_log.txt (04-09-2017 05:12:36) 190.21 KB	Download
2017-09-04_5-02-45_log.txt (04-09-2017 05:02:45) 977.08 KB	Download
2017-09-04_4-37-26_log.txt (04-09-2017 04:37:26) 976.75 KB	Download
2017-09-04_3-56-12_log.txt (04-09-2017 03:56:12) 976.78 KB	Download
2017-09-04_1-33-53_log.txt (04-09-2017 01:33:53) 976.67 KB	Download
2017-09-03_23-40-39_log.txt (03-09-2017 23:40:39) 976.62 KB	Download
2017-09-04_8-21-19_log.txt (03-09-2017 05:09:44) 781.90 KB	Download
2017-09-03_3-30-20_log.txt (03-09-2017 03:30:20) 976.79 KB	Download
2017-09-03_2-58-18_log.txt (03-09-2017 02:58:18) 976.60 KB	Download
2017-09-03_2-57-54_log.txt (03-09-2017 02:57:54) 976.79 KB	Download
2017-09-03_2-57-30_log.txt (03-09-2017 02:57:30) 976.80 KB	Download
2017-09-03_2-57-07_log.txt (03-09-2017 02:57:07) 976.78 KB	Download
2017-09-02_21-11-43_log.txt (02-09-2017 21:11:43) 976.64 KB	Download
2017-08-31_14-32-44_log.txt (31-08-2017 14:32:44) 976.67 KB	Download
2017-08-31_13-47-37_log.txt (31-08-2017 13:47:32) 977.23 KB	Download
2017-08-31_23-56-10_log.txt (31-08-2017 12:56:10) 976.66 KB	Download
2017-08-31_12-14-26_log.txt (31-08-2017 12:14:26) 977.50 KB	Download
2017-08-31_11-15-02_log.txt (31-08-2017 11:15:02) 976.64 KB	Download
2017-08-31_10-26-15_log.txt (31-08-2017 10:26:15) 976.84 KB	Download
2017-08-31_9-37-25_log.txt (31-08-2017 09:37:25) 976.72 KB	Download

Displaying Last n Activities Performed in Device Manager Pro

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

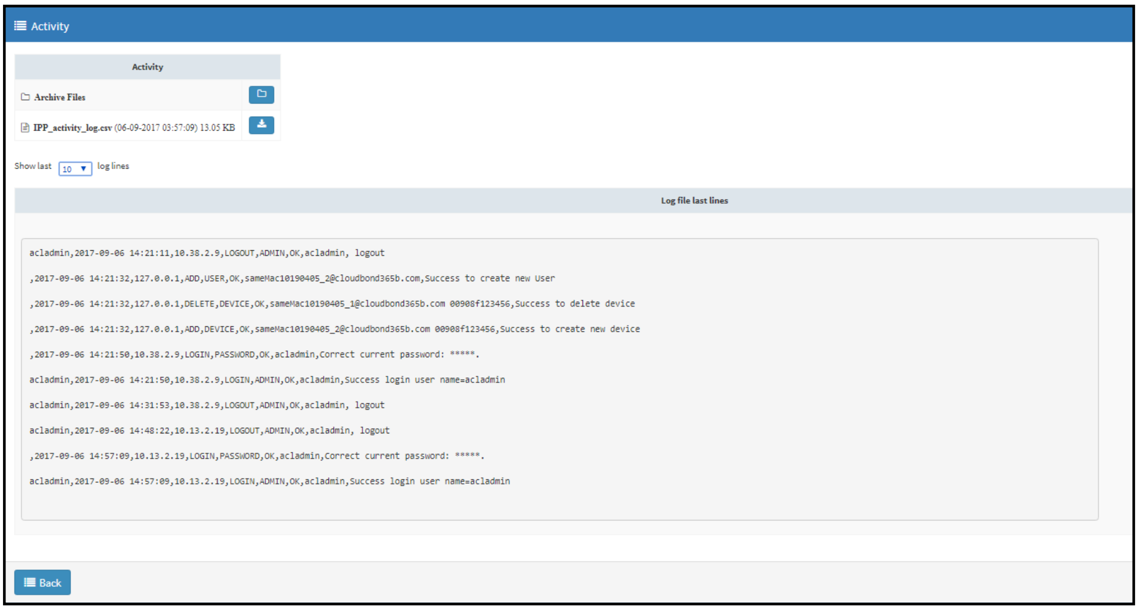
1. In the System Logs page, click **View** next to **Activity**.

Figure 17-5: Logged Activities Performed in Device Manager Pro



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

Figure 17-6: Logged Last Activities Performed in Device Manager Pro



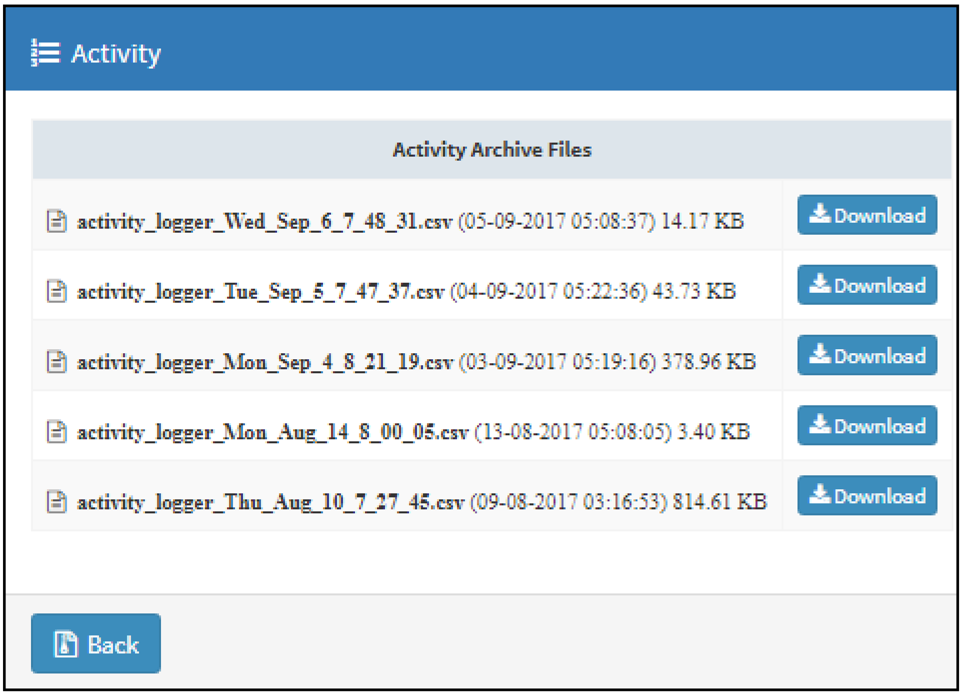
```
acladmin,2017-09-06 14:21:11,10.38.2.9,LOGOUT,ADMIN,OK,acladmin, logout

,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:**

- In the System Logs page, click **View** next to **Web Admin** and then in the Web Admin page, click the icon next to **Archive Files**.

Figure 17-7: Logged Archived Activities Performed in Device Manager Pro



Activity Archive Files	
activity_logger_Wed_Sep_6_7_48_31.csv (05-09-2017 05:08:37) 14.17 KB	Download
activity_logger_Tue_Sep_5_7_47_37.csv (04-09-2017 05:22:36) 43.73 KB	Download
activity_logger_Mon_Sep_4_8_21_19.csv (03-09-2017 05:19:16) 378.96 KB	Download
activity_logger_Mon_Aug_14_8_00_05.csv (13-08-2017 05:08:05) 3.40 KB	Download
activity_logger_Thu_Aug_10_7_27_45.csv (09-08-2017 03:16:53) 814.61 KB	Download

International Headquarters
1 Hayarden Street,
Airport City
Lod 7019900, Israel
Tel: +972-3-976-400s0
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/

Document #: LTRT-91094