

# IP Phone Manager Pro

IP Phone Manager Pro

Version 7.4

## 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: June-07-2018

## WEEE EU Directive

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

## Customer Support

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

## Abbreviations and Terminology

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

## Regulatory Information

The Regulatory Information can be viewed at <https://www.audiocodes.com/library/technical-documents>.

## Related Documentation

Document Name
420HD IP Phone User's Manual
430HD and 440HD IP Phone User's Manual
405HD IP Phone User's Manual
400HD Series IP Phones Administrator's Manual
400HD Series IP Phone with Microsoft Skype for Business Administrator's Guide
420HD IP Phone Quick Guide
430HD IP Phone Quick Guide

Document Name
440HD IP Phone Quick Guide
405 IP Phone Quick 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.

## Documentation Feedback

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

---

## Table of Contents

---

<b>1 Introduction</b>	<b>1</b>
1.1 About this Document	1
1.2 Zero Touch Provisioning	1
1.2.1 Zero Touch Provisioning Process - Skype for Business Phone	2
1.2.2 Zero Touch Provisioning – non Skype for Business Phone	2
<b>2 Starting up and Logging in</b>	<b>4</b>
<b>3 Adding Users &amp; Devices in Non-Skype for Business Environments</b>	<b>6</b>
3.1 Exporting 'System User' to zip File	6
3.2 Adding Users and Devices Information to the csv File	7
3.3 Importing the csv File	7
<b>4 Using the Zero Touch Setup Wizard to Provision Phones</b>	<b>8</b>
<b>4 Provisioning Phones without the Zero Touch Setup Wizard</b>	<b>11</b>
4.1 Before Implementing Zero Touch	11
4.2 Defining a Tenant	11
4.3 Preparing a Template for a Tenant/Model	12
4.4 Uploading .img Firmware File to the Server	13
4.5 Configuring DHCP Option 160 with a Tenant URL	13
4.5.1 Configuring DHCP Option 160 with System URL	14
4.5.1.1 Editing the DHCP Option 160 cfg File	15
4.5.1.2 Editing the SBC HTTP Proxy	16
<b>5 Managing IP Phones Behind a NAT using SBC HTTP Proxy</b>	<b>17</b>
<b>6 Monitoring and Maintaining the Phone Network</b>	<b>19</b>
6.1 Monitoring the Network from the Dashboard	19
6.2 Viewing Network Topology	21
6.3 Checking Devices Status	21
6.4 Monitoring Alarms	23
6.4.1 Registration Failure Alarm	23
6.4.2 Survivable Mode Start Alarm	24
6.4.3 Lync Login Failure Alarm	24
6.4.4 Endpoint License Alarm	25
6.4.5 IP Phone Speaker Firmware Download Failure	26
6.4.6 IP Phone Speaker Firmware Upgrade Failure	27
6.4.7 IP Phone Conference Speaker Connection Failure	27
6.4.8 IP Phone General Local Event	28
6.4.9 IP Phone Web Successive Login Failure	28
6.5 Searching for Alarms	29
6.6 Performing Actions on Alarms	29
6.7 Maintaining Users	29
6.7.1 Searching for Users/Devices	30
6.7.2 Adding a User	30
6.7.3 Adding a Phone	30
6.7.4 Editing a User	31

6.7.5 Viewing Device Status .....	31
6.7.6 Deleting a User .....	31
6.8 Managing Multiple Users .....	31
6.9 Maintaining Multiple Devices .....	33
6.10 Managing Configuration Files .....	35
6.11 Managing Firmware Files .....	35
<b>7 Viewing Your License .....</b>	<b>37</b>
7.1 Licensing Endpoints .....	37
<b>8 Approving Users .....</b>	<b>39</b>
8.1 Skype for Business Environment .....	39
8.2 Non-Skype for Business Environment .....	40
<b>9 Managing Templates .....</b>	<b>41</b>
9.1 System Settings and Placeholders .....	41
9.2 Selecting a Template .....	43
9.3 Editing a Configuration Template .....	44
9.4 About the Template File .....	44
9.4.1 Restoring a Template to the Default .....	44
9.4.2 Downloading a Template .....	44
9.4.3 Uploading an Edited Template .....	45
9.4.4 Generating an Edited Template .....	45
9.4.5 Defining Template Placeholders .....	45
9.4.5.1 Viewing Default Placeholders Values .....	45
9.4.5.2 Template Placeholders .....	45
9.4.5.3 Tenant Placeholders .....	46
9.4.5.4 Devices Placeholders .....	47
<b>10 Configuring the LDAP Directory .....</b>	<b>48</b>
<b>11 Configuring Phones to Operate in an OVR Deployment .....</b>	<b>50</b>
<b>12 Signing in to a Phone into which Another User is Signed .....</b>	<b>51</b>
<b>13 Troubleshooting .....</b>	<b>52</b>
13.1 Displaying Last n Activities Performed in the Web Interface .....	52
13.2 Displaying Archived Activities Performed in the Web Interface .....	52
13.3 Displaying Last n Activities Performed in IP Phone Manager Pro .....	52
13.4 Displaying Archived Activities Performed in IP Phone Manager Pro .....	52

# 1 Introduction

AudioCodes' IP Phone 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 in globally distributed corporations.

The IP Phone 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 IP phones and the server. The IP phones 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 IP Phone Manager Pro enables network administrators to effortlessly load configuration files and firmware files on up to 30000 IP phones.

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 IP Phone Manager Pro server provides added value to AudioCodes' 400HD Series IP phones.

## 1.1 About this Document

This document shows network administrators how to enable automatic provisioning (Zero Touch provisioning) of AudioCodes' IP phones in an enterprise network from a single central point, using AudioCodes' IP Phone Manager Pro.

## 1.2 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 IP Phone 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.

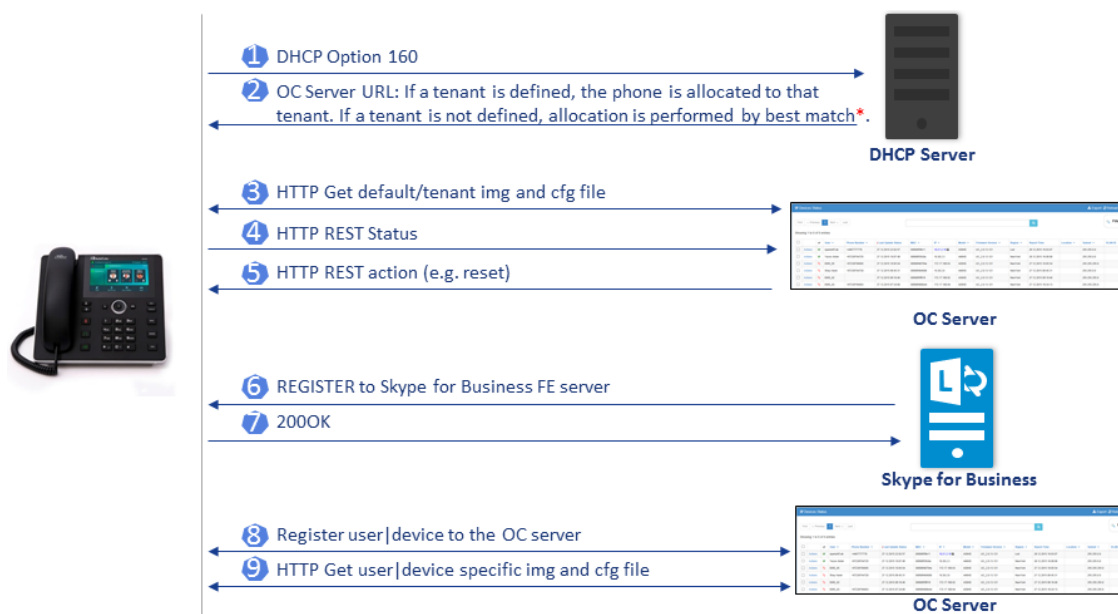


Phones that reside behind a NAT and whose IP addresses are internal can be managed by the OVOC via SBC HTTP proxy. For more information, see [Managing IP Phones Behind a NAT](#).

## 1.2.1 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.

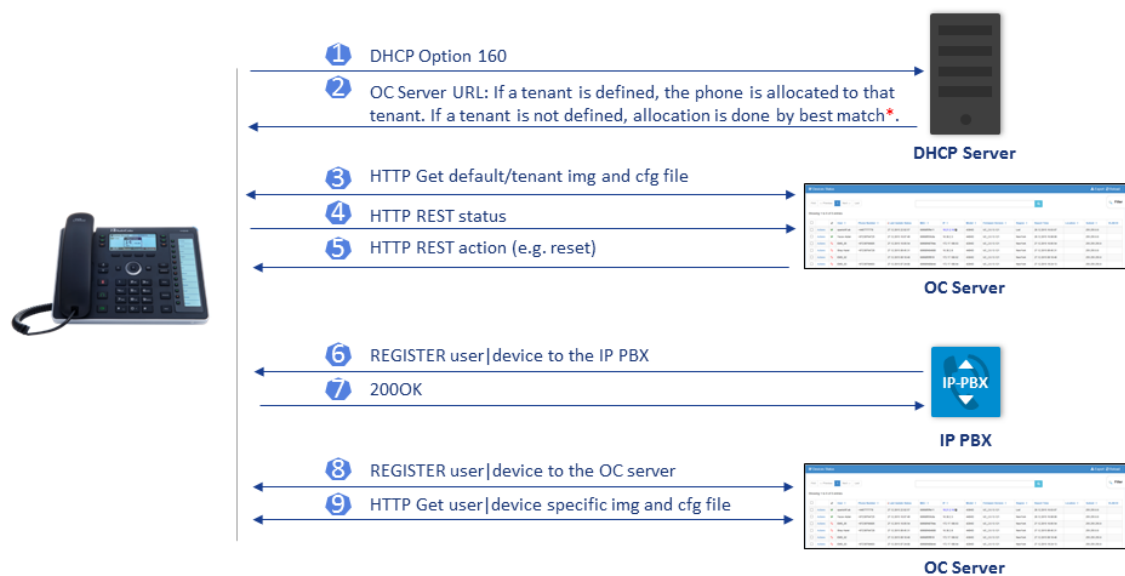
**Figure 1-1: Zero Touch Provisioning - Skype for Business Phone**



\*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.

## 1.2.2 Zero Touch Provisioning – non Skype for Business Phone

The figure below illustrates the 1-9 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**



## 2 Starting up and Logging in

This section shows how to start the IP Phone Manager Pro and log in. Before logging in, you need to run the OVOC.



- To access the IP Phone 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.
- IP Phone 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 IP Phone 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 IP Phone Manager Pro screen opens.

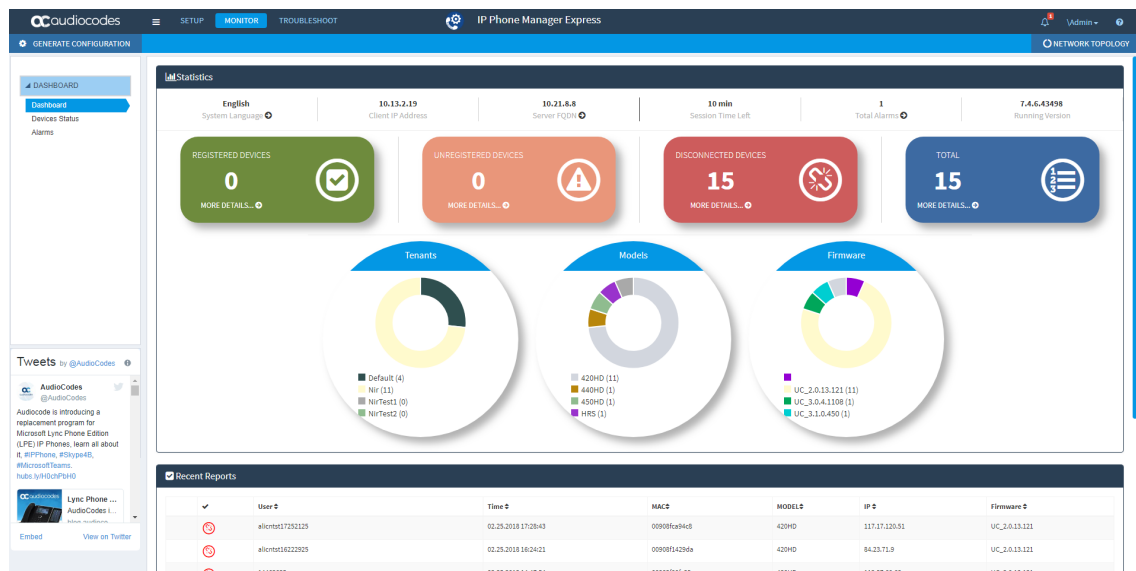
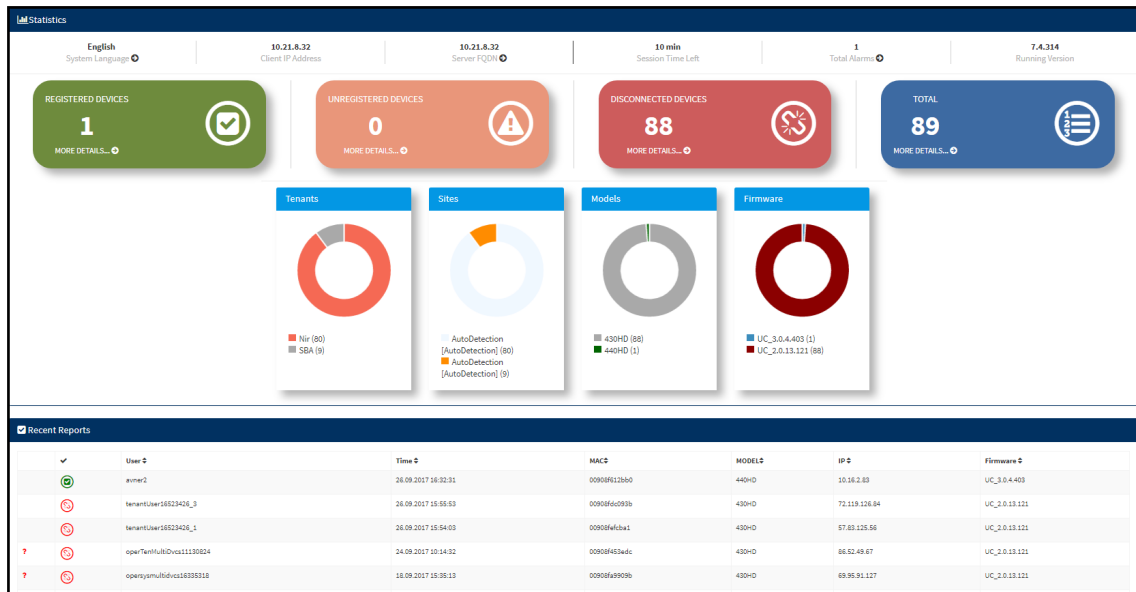
Figure 2-1 shows the login interface for IP Phone Manager Pro. The interface is titled 'Login to IP Phone Manager Pro'. It contains two input fields: 'Username' and 'Password'. The 'Username' field has an eye icon on the right, and the 'Password' field has a lock icon on the right. Below these fields is a blue button labeled 'Sign In'.



The 'Username' and 'Password' used to log in to the IP Phone Manager Pro are the same as those used to log in to the OVOC.

**Figure 2-1: Login**

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**

- See "Monitoring and Maintaining the Phone Network" on page 19 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

This section shows how to add users and devices to the IP Phone Manager Pro in non-Skype for Business environments. After plugging the phones into the network, log in to IP Phone Manager Pro and then (best practice):

1. Export the automatically created 'System User' to a zip file.
2. Unzip the zip file, open the csv file and add users and devices in the same format.
3. Import the csv file with users and devices back into IP Phone Manager Pro.

### 3.1 Exporting 'System User' to zip File

This section shows how to export the 'system user' that is automatically created after you log in to IP Phone 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**).
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):

Excel displays the information related to 'system user'.

## 3.2 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	VL-AN Mode	VL-AN 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 IP Phone Manager Pro.

## 3.3 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 IP Phone Manager Pro.

➤ **To import the new csv file into the IP Phone Manager Pro:**

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



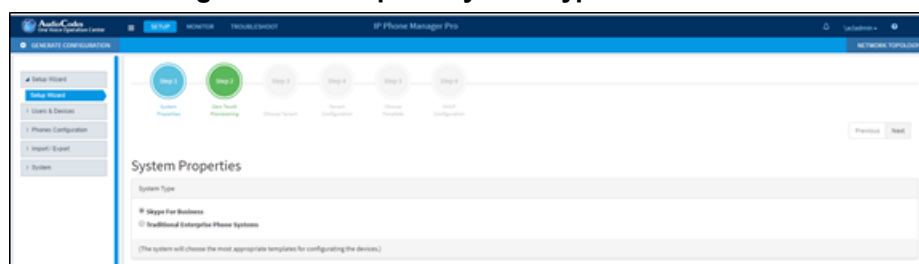
Zero Touch provisioning *accelerates uptime* by enabling multiple users and phones to automatically be provisioned and added to the Manager.

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 IP Phone 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 provision phones using the Wizard.

### ➤ To provision 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**

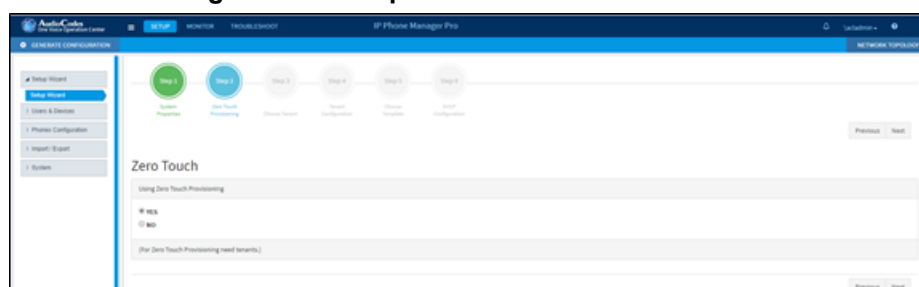


2. Select Skype for Business and then click Next.

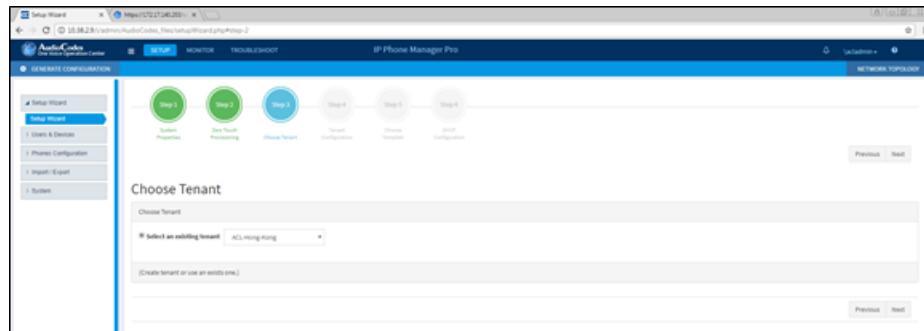


The Setup Wizard will be closed if you intend to use other PBXs besides Skype for Business. The Setup Wizard is intended exclusively for Skype for Business.

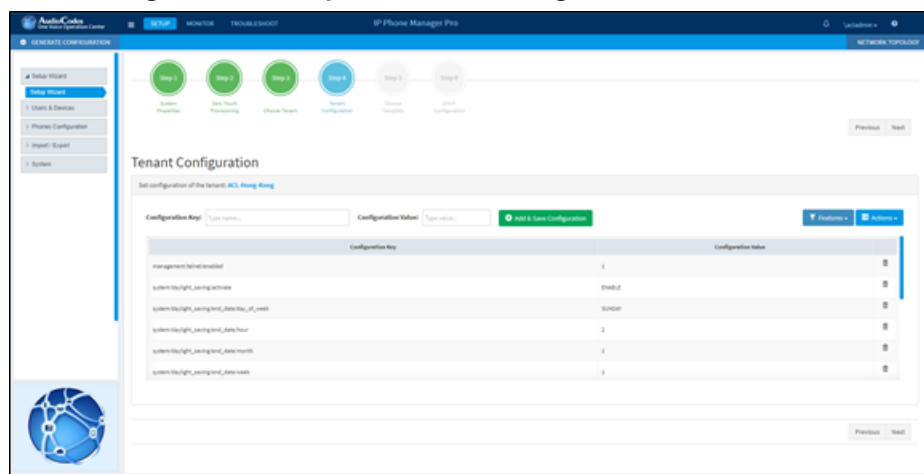
**Figure 4-2: Step 2 - Zero Touch**



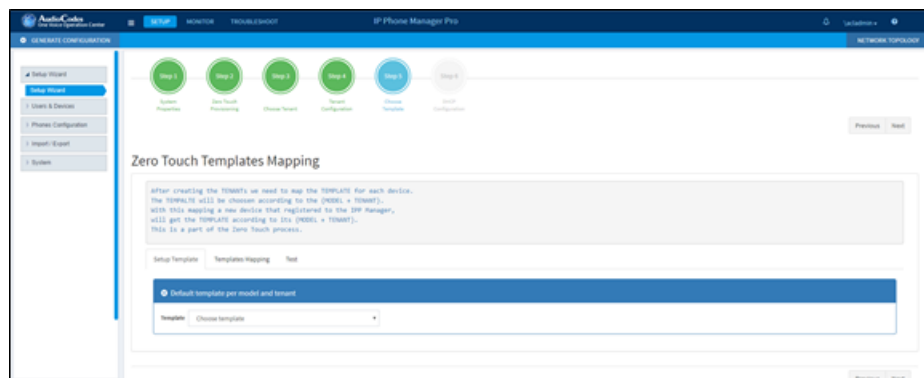
3. Select **Yes** and then click **Next**.

**Figure 4-3: Step 3 – Choose Tenant**

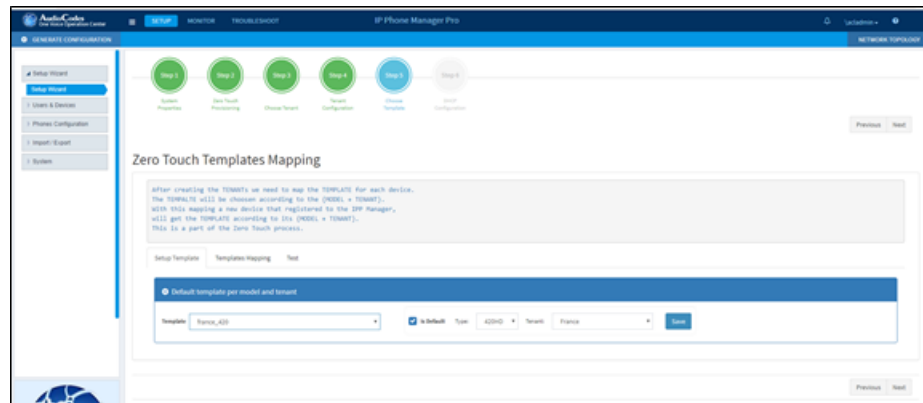
4. Choose an existing tenant from the dropdown and click **Next**. If a tenant doesn't already exist, click **Next** and configure one. This is to be able to create a specific configuration for the tenant and configure the URL in DHCP Option 160 so devices will use this tenant. If there's no specific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

**Figure 4-4: Step 4 – Tenant Configuration**

5. Click **Next**.

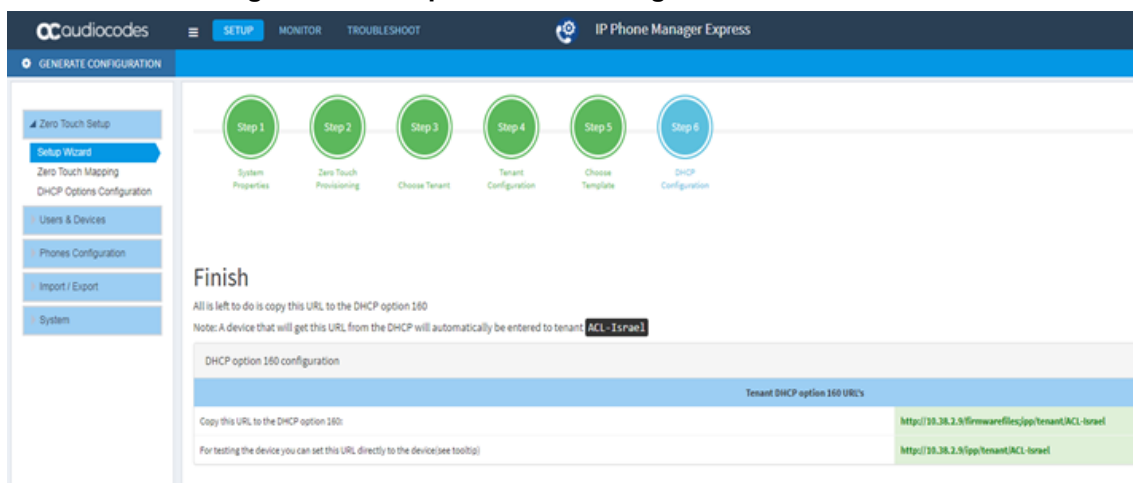
**Figure 4-5: Step 5 – Templates Mapping**

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

**Figure 4-6: Step 5 – Templates Mapping**

This page is an alternative view to the IP Phone 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**

8. Define the URL in DHCP Option 160.

## 4 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.

### 4.1 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 13).
  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 13).

### 4.2 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).
2. Click the **+Add New Tenant** button.
3. Use the table below as reference.

**Table 4-1: 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.



Parameter	Description
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**.

## 4.3 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 phone's cfg file and backed up on the server. After the user configures them (see the phone'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 > Phones Configuration > Templates > Add New Template button).
2. Enter a name for the template. Make the name intuitive. Include tenant *and* model aspects in it.
3. Provide a description of the template to enhance intuitive maintenance.
4. From the 'Tenant' dropdown list, select the tenant.
5. From the 'Type' dropdown list, select the phone model.
6. 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 IP Phones 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).
7. 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.
8. Do this for all tenants and types (phone models) in the network.
9. 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.

## 4.4 Uploading .img Firmware File to the Server

After obtaining the phone's latest .img firmware file from AudioCodes, upload it to the OVOC provisioning server. When phones 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 IP Phone Manager Pro, access the Phone Firmware Files page (**Setup > Phones Configuration > Phone Firmware Files**).
2. In the Phone Firmware Files screen, click the **Add new IP Phone firmware** button.
3. Navigate to the .img file and/or .dfu firmware files for the HRS speakers, and upload to the OVOC provisioning server.

## 4.5 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 IP Phone 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 IP Phone Manager Pro which loads their specific .cfg files to them.

➤ **To point DHCP Option 160 to a tenant URL:**

1. In the IP Phone Manager Pro, open the System Settings page (**Setup > Phones 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.

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

5. Choose either:
  - **The OVOC has direct access to the phones.** The DHCP server will connect the phones directly to the OVOC server IP address.
    - ◆ Copy (Ctrl+C) the following URL and paste it into DHCP Option 160 in the enterprise's DHCP server:  
`HTTP://<OVOC_IP_Address>/firmwarefiles;ipp/tenant/<tenant selected in Step 1>`
  - **The OVOC access the IPP's through the SBC HTTP proxy.** The DHCP server directs the phones firstly to an SBC HTTP proxy server, which then redirects to the OVOC server.

- ◆ If the phones communicate with an SBC HTTP proxy rather than directly with the OVOC server, copy (Ctrl+C) the following URL into DHCP Option 160 in the enterprise's DHCP server: **http://SBC\_PROXY\_IP:SBC\_PROXY\_PORT/firmwarefiles;ipp/tenant/Tenant**
- **Direct URL for the IPP (No DHCP Available)** – typically used for debugging purposes when no DHCP is available.



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

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



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

- DHCP server
- Subnet

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



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

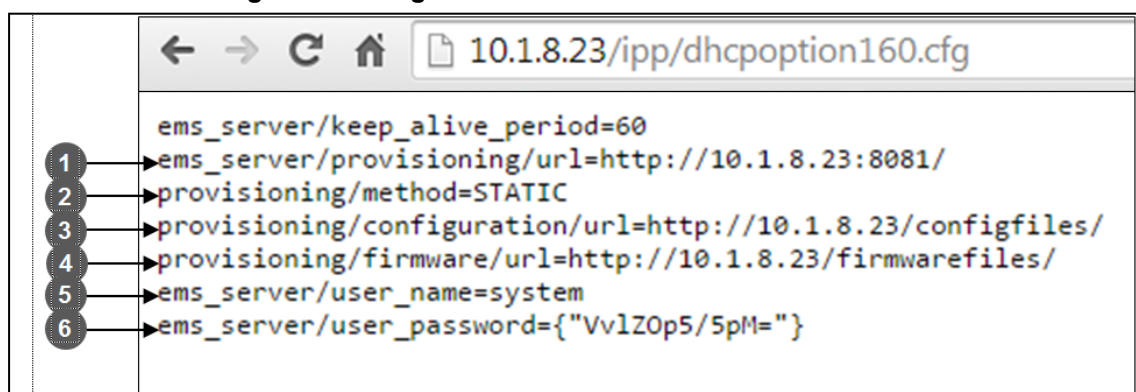
### 4.5.1 Configuring DHCP Option 160 with System URL



- This section is applicable when Zero Touch is not used to provision the phones.
- The section thus describes a provisioning method that is not the choice method.

The figure below shows the file **dhcption160.cfg** located on the server.

**Figure 4-8: cfg File Located on the Server**



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 **dhcption160.cfg** file is created when logging in for the first time to the IP Phone 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.

#### 4.5.1.1 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 > Phones Configuration > System Settings**).
2. Click the **DHCP Option Configuration** button.
3. Click the **Edit configuration template** button.
4. Edit the DHCP option using the table below as reference.

**Table 4-2: DHCP Option**

Parameter	Description
Keep alive period	You can configure how often the phones generate a keep-alive trap towards the IP Phone 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.

Parameter	Description
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).
User Name	Defines the user name for the REST API. Default: <b>System</b> . Later, each phone receives its own unique user name.
User Password	Encrypted. Defines the user password for the REST API. Default: <b>System</b> . 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.

#### 4.5.1.2 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 > Phones Configuration > System Settings**).
2. Click the **SBC Proxy Configuration** button.
3. Click the **Edit configuration template** button; the same Edit DHCP Option screen shown in the previous section opens. Edit as described in the previous section.
4. Click **Save**.

## 5 Managing IP Phones Behind a NAT using SBC HTTP Proxy

Phones 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 IP Phone Manager Pro, i.e., REST requests originate from the phone and the OVOC functions as a REST server.
- The IP Phone 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 an IP phone is using the SBC HTTP Proxy, the IP Phone Manager Pro indicates this with the following icon: 

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 SIP User's Manual.

## 6 Monitoring and Maintaining the Phone Network

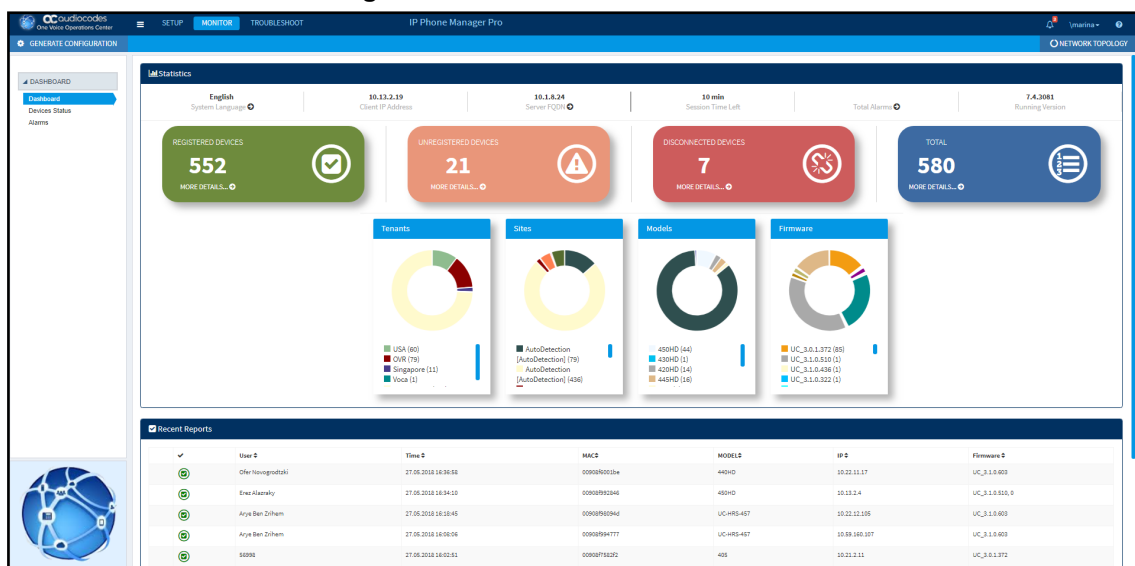
This section shows how to monitor and maintain the phone network in the enterprise.

### 6.1 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 6-1: Dashboard**



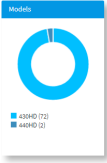
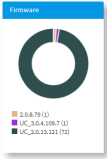




- If a Skype for Business IP phone is signed out (offline, or not registered), you'll see an x icon inside a grey circle, and the 'User' column will be blank, as shown in the figure below. It will be counted as a Non Registered Device.
- Point your mouse over the icon to view the 'offline' tooltip.
- 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 6-1: Dashboard – Status Thumbnails**

Status Thumbnail	Description
	Indicates the number of registered devices. Click <b>MORE DETAILS...</b> to quickly access the Devices Status page.
	Indicates the number of unregistered devices. Click <b>MORE DETAILS...</b> to quickly access the Devices Status page.
	Indicates the number of disconnected devices. Click <b>MORE DETAILS...</b> to quickly access the Devices Status page.
	Indicates the number of devices running the version stated above it. Click <b>MORE DETAILS...</b> to quickly access the Devices Status page.
	Pie chart showing the number of <i>devices per tenant</i> 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 <i>devices per site</i> that are registered. Click a segment of the pie to open the Devices Status page.

Status Thumbnail	Description
	Pie chart showing how many <i>phones of each model</i> are registered. Click a segment of the pie to open the Devices Status page.
	Pie chart showing how many <i>phones of each firmware version</i> are registered. Click a segment of the pie to open the Devices Status page.

## 6.2 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.

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 tooltip on that device.

## 6.3 Checking Devices Status

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

### ➤ To check a phone's status:

1. Open the Devices Status page (**Monitor > Dashboard > Devices Status**)
2. Click **Filter**; the filter lets you view specific information in the page, preventing information irrelevant to you from cluttering the page.
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. In the column 'IPP Model', view **Spectralink 8440**, **Polycom Trio 8800**, 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.

**Table 6-2: Actions Menu**

Action	Description
Check Status	Select the 'Check Status' option.
Change Tenant	Select the 'Change Tenant' option. From the dropdown, select the tenant, and then click <b>Change</b> .
Update Firmware	You can update firmware per device, or for multiple selected devices (see the next step, below the table). Select the 'Update Firmware' menu option. From the dropdown, select the firmware file, and then click <b>Update</b> ; the firmware file is updated. You can simultaneously update the phone's configuration file.
Open Web Admin	Opens the Web interface (see the phone's <i>Administrator's Manual</i> ). 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 ( <b>Management &gt; Remote Management &gt; Telnet</b> ).

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

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.

## 6.4 Monitoring Alarms

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

The IP Phone 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 6-3: Alarms**

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

### 6.4.1 Registration Failure Alarm

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

**Table 6-4: 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 IPhoneRegisterFailure alarm
Description	This alarm is activated when a registration failure occurs
Alarm Title	Registration Failure
Alarm Type	communicationsAlarm(1)

Alarm	IPPhoneRegisterFailure
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.

### 6.4.2 Survivable Mode Start Alarm

The table below describes the Survivable Mode Start alarm.

**Table 6-5: 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.

### 6.4.3 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 6-6: 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.

#### 6.4.4 Endpoint License Alarm

The table below describes the Endpoint License alarm.

**Table 6-7: IP Phone Endpoint License Alarm**

Description	This alarm is issued when the number of endpoints currently running on the OVOC server (Management of Endpoints in the IP Phone Manager) 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

### 6.4.5 IP Phone Speaker Firmware Download Failure

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

**Table 6-8: 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	<ul style="list-style-type: none"> <li>■ Make sure the IP Phone Manager Pro is correctly defined.</li> <li>■ Contact your network administrator (IT manager).</li> </ul>		
Alarm Severity	Condition	Alarm Text	Corrective Action
Minor		This alarm is sent when the phone fails to download the speaker firmware.	

## 6.4.6 IP Phone Speaker Firmware Upgrade Failure

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

**Table 6-9: IP Phone Speaker Firmware Upgrade Failure**

Description	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.		
SNMP Alarm	IPPhoneSpeakerFirmUpgradeFailure		
SNMP OID	1.3.6.1.4.1.5003.9.20.3.2.0.55		
Alarm Title	IP Phone Speaker Firmware Upgrade Failure		
Alarm Source			
Alarm Type	communicationsAlarm(1)		
Probable Cause	communicationsProtocolError(5)		
Additional Info			
Corrective Action	<ul style="list-style-type: none"> <li>■ Make sure the speaker is properly connected to the phone.</li> <li>■ Try again.</li> <li>■ Contact your network administrator (IT manager) if the alarm persists.</li> </ul>		
Alarm Severity	Condition	Alarm Text	Corrective Action
Minor		This alarm is sent when the phone fails to load the firmware to the speaker.	

## 6.4.7 IP Phone Conference Speaker Connection Failure

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

**Table 6-10: 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	<ul style="list-style-type: none"> <li>■ Make sure the USB cable is properly connected.</li> <li>■ After making sure, contact your network administrator (IT manager) if the alarm persists.</li> </ul>		
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	

### 6.4.8 IP Phone General Local Event

The table below describes the IP Phone General Local Event.

**Table 6-11: 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	-

### 6.4.9 IP Phone Web Successive Login Failure

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

**Table 6-12: IP Phone Web Successive Login Failure**

Description	This alarm is sent after five successive unsuccessful attempts are made to log in to the phone's Web interface.
SNMP Alarm	IPPhoneWebSuccessiveLoginFailure

SNMP OID	1.3.6.1.4.1.5003.9.20.3.2.0.59		
Alarm Title	IP Phone Web Successive Login Failure		
Alarm Source	The IP Phone		
Alarm Type	SecurityServiceOrMechanismViolation(9)		
Probable Cause	UnauthorizedAccessAttempt(73)		
Additional Info			
Alarm Severity	Condition	Alarm Text	Corrective Action
Major	Issued after the fifth successive attempt to log in to the phone's Web interface fails.		<ul style="list-style-type: none"> <li>■ After the alarm is cleared, try to log in to the Web interface using the correct username and password.</li> <li>■ If you forget the login credentials, inform the network administrator.</li> </ul>
Clear	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.		

## 6.5 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 phone's MAC address
- a phone's IP address

## 6.6 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 22 for more information.

## 6.7 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

### 6.7.1 Searching for Users/Devices

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

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.

### 6.7.2 Adding a User

You can add a user to the IP Phone Manager Pro.

➤ **To add a user to the IP Phone 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.
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.

### 6.7.3 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.
2. Enter the 'Display Name', i.e., the device's name to be displayed in the IP Phone Manager Pro.
3. From the 'IP Phone 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 'IP Phones 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 39 for more information.

7. Click **Submit** and then click **Back** to see the added phone in the Manage Users page under the Devices column (click +).

### 6.7.4 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.

### 6.7.5 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.

### 6.7.6 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.

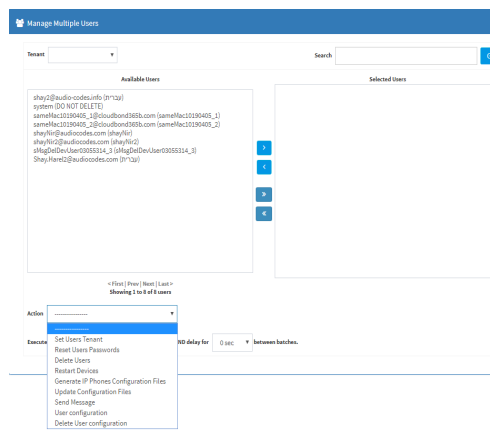
## 6.8 Managing Multiple Users

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 IP phones configuration files
- update configuration files
- send a message to multiple phones

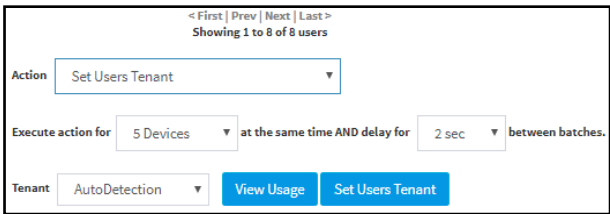
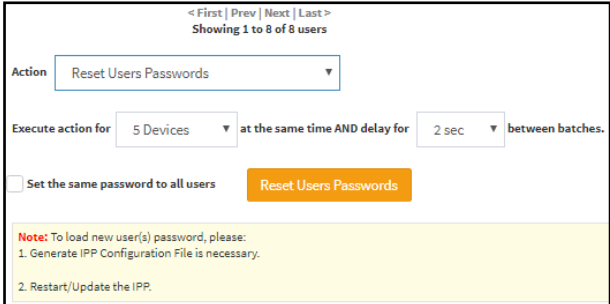
➤ **To manage multiple users:**

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



- Use the table below as reference.

**Table 6-13: Managing Multiple Users - Actions**

Action	Description
Set Users Tenant	 <p>Sets the tenant for users selected.</p>
Reset Users Passwords	 <p>Resets users passwords. A random password is generated for each user. To generate a single password for all users selected, select the <b>Set the same password to all users</b> option.</p> <p>To load the new user passwords:</p> <ul style="list-style-type: none"> <li>■ Generate the phone's configuration file</li> <li>■ Restart/Update the phone</li> </ul>
Delete Users	Deletes users and applies a configurable 'Delay Time' (Default = 2 seconds) after each delete is performed.
Restart Devices	<p>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.</p> <p>From the dropdown, choose the type of restart:</p> <ul style="list-style-type: none"> <li>■ Graceful (default)</li> <li>■ Force <ul style="list-style-type: none"> <li>■ Scheduled</li> </ul> </li> </ul>

Action	Description
	Before restarting, some models wait for the user to finish an active call while others may perform an immediate restart.
Generate IP Phones 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 select the <b>Updating IP Phones after generating files</b> option. You can generate a private configuration file per user group, device group, or specific tenants.
Update Configuration Files	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 screens. Phones beep to alert users when messages come in. <div data-bbox="497 810 1104 1019" data-label="Form"> </div>
User Configuration	<div data-bbox="497 1057 1412 1209" data-label="Form"> </div> <p>Configures the values that will be added to the <i>mac.cfg</i> file for the selected users. Note that you can copy from one user to multiple users.</p>
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

## 6.9 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 IP phone type
- change language
- restart multiple devices
- generate IP phones 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 6-2: Manage Multiple Devices**

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 6-14: 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: <ol style="list-style-type: none"> <li>1. Generate the phone's Configuration File</li> <li>2. Restart/Update the phone.</li> </ol>
Change Language	Changes the phone language. Select the language from the <b>Language</b> dropdown and click <b>Change</b> . To view the usage of a language, click <b>View Usage</b> . To load a new language: <ol style="list-style-type: none"> <li>3. Generate the phone's configuration file.</li> <li>4. Restart/update the phone.</li> </ol>
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: <ul style="list-style-type: none"> <li>■ Graceful (default)</li> <li>■ Force</li> <li>■ Scheduled</li> </ul>
Generate IP Phone 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 <b>Updating IP Phones after generating files</b> option.
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.

Action	Description
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 <a href="#">Skype for Business Environment.htm</a> 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 IP Phones Configuration Files** option in the Manage Multiple Devices page.

## 6.10 Managing Configuration Files

You can manage IP phones 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 IP phone configuration files:**

- Open the Manage Configuration Files page (**Setup > Phones Configuration > Phone Configuration Files**).

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)

## 6.11 Managing Firmware Files

You can manage the phones' .img firmware files.

➤ **To manage the .img firmware files:**

- Open the Phone Firmware Files page (**Setup > Phones Configuration > Phone Firmware Files**).

In this page you can

- View all .img firmware files currently located on the server
- Add a new IP phone 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 from the phone's name if the phone has firmware or not. The name will be red-coded if the phone does not have firmware and black if it does have. If it doesn't have, you must upload the phone's .img firmware file that you obtained from AudioCodes, to the OVOC provisioning server:
  - a. Click the red-coded name of the phone; this screen opens:



- 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.
- After an .img firmware file has been uploaded to a phone, you can download it to your pc. Click the phone's name and then in the screen that opens, click the **Download firmware file** button.
- Edit a phone'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 IP Phone firmware** button.
  - b.** Define an intuitive 'Name' and 'Description' to facilitate easy identification. You can leave the 'Version' field empty, and then click **Save**.
  - c.** Click **Upload firmware file**:
  - 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.

## 7 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**).
2. Use the table below as reference.

**Table 7-1: 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 IP Phone Manager Pro is rendered non-usable. Contact your AudioCodes partner if the license expires.
Expiration Date	Displays <b>DD:MM:YY</b> .
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.

### 7.1 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.

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

## 8 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.

### 8.1 Skype for Business Environment

After plugging the phones in, they report to the IP Phone 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 IP Phone Manager Pro UI, open the Devices Status page (**Dashboard > Devices Status**).

Screen functions:

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

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

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

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

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

**Search** option

Smart **Filter(s)**

2. Select the upper left checkbox (in the figure below it's indicated in red); the **Selected Rows Actions** menu and the **Approve Selected** button are displayed.
3. Click the **Approve Selected** button; you're prompted to approve the phone/s selected.
4. In the prompt, select the tenant and then click **Approve**; all selected users are approved; all phones restart; the cfg file is automatically uploaded to the phones from the OVOC provisioning server, which the DHCP server points them to.
5. From the 'VLAN Discovery mode' dropdown, select either:
  - **NONE**
  - **Disabled**
  - **Manual Configuration** [of the LAN; static configuration of VLAN ID and priority]
  - **Automatic - CDP** [automatic configuration of the VLAN - VLAN discovery mechanism based on Cisco Discovery Protocol]
  - **Automatic - LLDP** [automatic configuration of VLAN - VLAN discovery mechanism based on LLDP]
  - **Automatic - CDP\_LLDP** [automatic configuration of VLAN (default) - VLAN discovery mechanism based on LLDP and Cisco Discovery Protocol. LLDP protocol is with higher priority].

## 8.2 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 IP Phone Manager Pro, which does not display user names whose MAC address are unknown.

➤ **To approve users:**

1. In the IP Phone 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 IP Phone 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.

## 9 Managing Templates

This topic shows how to manage templates.

### 9.1 System Settings and Placeholders

You can configure new placeholder values according to your enterprise's IP phone 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 > Phones Configuration > System Settings**).
2. Configure values for available placeholders according to your enterprise's IP phone configuration requirements. Use the table below as reference.



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

**Table 9-1: System Settings**

Parameter	Description
Secure (HTTPS) communication from the IPP Manager to the Devices	Sends secured (HTTPS) requests from the IP Phone 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 IP Phone 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 IP Phone 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.
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.
IP Phones Language	From the dropdown select the language you want displayed in the phones' screens: <b>English</b> (default), <b>French</b> , <b>German</b> , <b>Hebrew</b> , <b>Italian</b> , <b>Polish</b> , <b>Portuguese</b> , <b>Russian</b> , <b>Spanish</b> or <b>Ukraine</b> .

Parameter	Description
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 <i>Secure</i> RTP. Real-time Transport Protocol (RTP) is the standard packet format for delivering voice over IP.
Daylight Saving Time	
Active	Determines whether the phone automatically detects the Daylight Saving Time for the selected Time Zone. <ul style="list-style-type: none"> <li>■ Disable</li> <li>■ Enable (default)</li> </ul>
Date Format	Configures the date format. Valid values are: <ul style="list-style-type: none"> <li>■ FIXED. Date is specified as: Month, Day of month.</li> <li>■ Day of Week. Date is specified as Month, Week of month, Day of week.</li> </ul>
Start Time	Defines precisely when to start the daylight saving offset. <ul style="list-style-type: none"> <li>■ month - defines the specific month in the year</li> <li>■ week – defines the specific week in the month (first – fourth)</li> <li>■ day - defines the specific day in the week</li> <li>■ hour - defines the specific hour in the day</li> <li>■ minute - defines the specific minute after the hour</li> </ul> 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. <ul style="list-style-type: none"> <li>■ month - defines the specific month in the year</li> <li>■ week – defines the specific week in the month (first – fourth)</li> <li>■ day - defines the specific day in the week</li> <li>■ hour - defines the specific hour in the day</li> <li>■ minute - defines the specific minute after the hour</li> </ul> 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	

Parameter	Description
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 <b>Registered</b> to <b>Disconnected</b> and the phone'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 <b>No Redundant</b> (default) or <b>Primary/Backup</b> . Allows the administrator to set the primary PBX / Skype for Business server to which the phone registers and the fallback option if the server is unavailable. Primary/Backup, or 'outbound proxy', is a feature that enables the phone to operate with a primary or backup PBX/Skype for Business server. If the primary falls, the other backs it up.
Primary	Enter the primary PBX/Skype for Business server's IP address, i.e., the outbound proxy's.
Backup	Displayed only if you select the <b>Primary/Backup</b> 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 15.

3. Click **Save**.

## 9.2 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
- **To select a template:**
- Open the IP Phones Configuration Templates page (**Setup > Phones Configuration > Templates**):
- Click ⓘ for more information about the phone whose template is displayed.
- Click **Edit** to modify a template.

## 9.3 Editing a Configuration Template

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

➤ **To edit a template:**

1. In the IP Phones Configuration Templates page, click the link of the IP phone model or its **Edit** icon.
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.

3. Click the **Edit configuration template** button; the template opens in an integral editor:
4. Edit the template and then click **Save**; in the IP Phones Configuration Templates page, the name of an edited template is displayed in green. See the IP phone's *Administrator's Manual* for parameter descriptions.

## 9.4 About the Template File

The template is an xml file. It defines how a phone'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

### 9.4.1 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.

### 9.4.2 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.

### 9.4.3 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.

### 9.4.4 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.
2. In the Manage Multiple Users – Generate Configuration screen that opens shown in the figure below, select the relevant users.
3. After selecting users, click the **Generate IP Phones Configuration Files** button

### 9.4.5 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 IP Phones Configuration Template page (**Setup > Phones Configuration > Templates**), click the **Edit** button in the same row as the phone model.
2. Click **Show Placeholders**.

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.

#### 9.4.5.1 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 > Phones Configuration > System Settings > Default Placeholders Values** button):

#### 9.4.5.2 Template Placeholders

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

##### 9.4.5.2.1 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 > Phones Configuration > Template Placeholders**):

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

➤ **To edit a value of an existing template placeholder:**

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

#### 9.4.5.2.2 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 > Phones Configuration > Template Placeholders**):
2. From the **Template** dropdown, select the template , e.g., IP Phone Model – Audiocodes\_420HD.
3. Click the **+Add new placeholder** button located in the upper right corner of the screen.
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.

#### 9.4.5.3 Tenant Placeholders

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

##### 9.4.5.3.1 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 > Phones Configuration > Tenant Configuration**):

➤ **To edit a value of an existing tenant placeholder:**

1. Under the Tenant Placeholders section, select the placeholder and then click the **Edit** button.
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. From the 'Tenant' dropdown, you can select another tenant.
5. Click **Save**; the edited placeholder is added to the table.

##### 9.4.5.3.2 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 > Phones Configuration > Tenant Configuration**).

2. Under the Tenant Placeholders section of the page, click the **+Add new placeholder** button.
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.

#### 9.4.5.4 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 phone's placeholders values.

##### 9.4.5.4.1 Changing a Device Placeholder Value

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

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

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. Click **Edit**.
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 IP phone 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.

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

**Table 10-1: LDAP Configuration**

Parameter	Description
Server address	Enter the IP address, or URL, of the LDAP server.
Port	Enter the LDAP service port.
User Name	Enter the user name used for the LDAP search request.
Password	Enter the password of the search requester.
Base	Enter the access point on the LDAP tree.
Active	From the dropdown, select <b>Disable</b> LDAP (default) or <b>Enable</b> LDAP. If <b>Enable</b> is selected, the parameters below are displayed.
Name Filter	Specify your search pattern for name look ups. For example, when you type in the <code>(&amp;(telephoneNumber=*)(sn=*))</code> 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 <code>((cn=%)(sn=*))</code> 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 <code>(!(cn=*))</code> 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, <code>cn sn displayName</code> , 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, <code>((telephoneNumber=%)(Mobile=%)(ipPhone=*))</code> , the search result is all LDAP records which have the “telephoneNumber” OR “Mobile” OR “ipPhone” field match the number being searched.

Parameter	Description
	When you type in the <code>(&amp;(telephoneNumber=%)(sn=*))</code> 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, <i>Mobile telephoneNumber ipPhone</i> , 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.
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**.

## 11 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.
2. Click the **Edit configuration template** button.
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.

## 12 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.



## 13 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 IP Phone Manager Pro
  - Last logged activities
  - Archived activities

➤ **To display system logs:**

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

### 13.1 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**.
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.
5. Click **Save** to save the last logged activities performed in the Web interface and share the log file with others.

### 13.2 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**.

### 13.3 Displaying Last n Activities Performed in IP Phone Manager Pro

➤ **To display last activities logged in the IP Phone Manager Pro:**

1. In the System Logs page, click **View** next to **Activity**.
2. From the 'Show last log lines' dropdown select 10, 20, 30, 40, 50 or 100.

### 13.4 Displaying Archived Activities Performed in IP Phone Manager Pro

➤ **To display logged archived activities performed in the IP Phone 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**.

**This page is intentionally left blank.**

**International Headquarters**

1 Hayarden Street,  
Airport City  
Lod 7019900, Israel  
Tel: +972-3-976-400s0  
Fax: +972-3-976-4040

**AudioCodes Inc.**

27 World's Fair Drive,  
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/>

©2018 AudioCodes Ltd. All rights reserved. AudioCodes, AC, HD VoIP, HD VoIP Sounds Better, IPmedia, Mediant, MediaPack, What's Inside Matters, OSN, SmartTAP, User Management Pack, VMAS, VoIPerfect, VoIPerfectHD, Your Gateway To VoIP, 3GX, VocaNom, AudioCodes One Voice and CloudBond are trademarks or registered trademarks of AudioCodes Limited. All other products or trademarks are property of their respective owners. Product specifications are subject to change without notice.

Document #: LTRT-91092

