Administrator's Manual

400HD IP Phones Series

IP Phone Management Server

Version 7.2

AudioCodes

Table of Contents

List of Figures

List of Tables

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. In cases where there are discrepancies between this document and the Release Notes, the information in the Release Notes supersedes that in this document. Updates to this document and other documents as well as software files can be downloaded by registered customers at http://www.audiocodes.com/downloads.

This document is subject to change without notice.

Date Published: May-15-2017

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 www.audiocodes.com/support.

Documentation Feedback

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

Abbreviations and Terminology

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

Related Documentation

Manual Name
420HD IP Phone User’s Manual
430HD and 440HD IP Phone User’s Manual
405 IP Phone User's Manual
400HD Series IP Phones Administrator's Manual
400HD Series IP Phone with Microsoft Lync Administrator’s Guide
420HD IP Phone Quick Guide
430HD IP Phone Quick Guide
440HD IP Phone Quick Guide
405 IP Phone Quick Guide
EMS and SEM Server IOM Manual
EMS 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 region 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, region-specific administrator security level, viewing administrator security level per region, 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 cmnds. 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'

This page is intentionally left blank.

1 Introduction

AudioCodes' IP Phone Management Server features a user interface that enables enterprise network administrators to effortlessly and effectively provision and maintain up to 10000 400HD Series IP phones in globally distributed corporations.

The IP Phone Management Server 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 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' Element Manager Server (EMS), the IP Phone Management Server user interface enables network administrators to effortlessly load configuration files and firmware files on up to 10000 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 Lync), approve devices at the press of a button (supported in Lync environments only), send messages to phones' LCDs, reset phones, and move phones between regions.

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

Integrated into the EMS, the IP Phone Management Server provides added value to AudioCodes 400HD Series IP phones.

1.1 About this Manual

This *Administrator's Manual* shows network administrators how to use the IP Phone Management Server to set up, configure, and maintain AudioCodes IP phones in an enterprise network, from a single centralized point.

1.2 EMS Platforms Specifications

EMS 7.2 must run on one of these platforms to support the IP Phone Management Server:

- Dedicated hardware platform (HP ProLiant DL360p Gen8 Server) -OR-
- VMware ESXi Hypervisor virtual environment -OR-
- Microsoft Hyper-V virtual environment

These platforms must comply with the following specifications:

Table 1-1: EMS Platforms Specifications

EMS Platform	Platform Description	# of Managed IP Phones
HP ProLiant DL360p Gen8 Server	CPU: E5-2690 (8 cores X 2.9 GHz) Memory: 32 GB Disk: 2 disks X 1.2 TG in RAID 0 (SAS 10K RPM)	10000
VMware ESXi bare metal hypervisor / Microsoft Hyper-V (minimum)	CPU: 1 core x 2 GHz Memory: 8 GB Disk: 500 GB	1000
VMware ESXi bare metal hypervisor / Microsoft Hyper-V (maximum)	CPU: 6 cores X 2.0 GHz Memory: 32 GB Disk: 1.2 TB (SAS 10K RPM)	5000

For details on installing the EMS, see the *EMS and SEM Server IOM Manual*.

Note:

- The EMS can manage IP phones residing behind a NAT via an SBC HTTP proxy – see Section 1.3 below.

1.3 Ports Required for IP Phone Management

The table below shows the ports required for IP phone management. The table summarizes the firewall ports, protocols and direction that administrators must open.

Table 1-2: Ports Required for IP Phone Management

Connection	Port Type	Port Number	Purpose	Port Side / Flow Direction
IP Phones > EMS Server	HTTP (TCP)	80	HTTP connection used by phones for downloading firmware and configuration files from the EMS server. Initiator: IP phone	EMS server side / Receive only
	HTTP (TCP)	8081	HTTP connection for REST requests from the EMS server to the IP phone Initiator: EMS Server	EMS server side / Receive only
EMS Server > IP Phone	HTTP (TCP)	80	HTTP connection from admin PC to the EMS server and IP phone Initiator: Admin PC	IP Phone / Receive only
Web Browser > EMS Server / IP Phone	HTTP (TCP)	80	HTTPS connection from admin PC to the EMS server and IP phone Initiator: Admin PC	EMS Server & IP Phone / Receive only
	HTTPS (TLS)	443	HTTPS connection used by endpoints for downloading firmware and configuration files from the EMS server. Initiator: Endpoints	EMS Server & IP Phone / Receive only

Note: For the connection between the Web browser and the EMS server / IP phone, the firewall can only be configured to port 80 or port 443.

1.4 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 EMS via SBC HTTP proxy.

Note: 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:

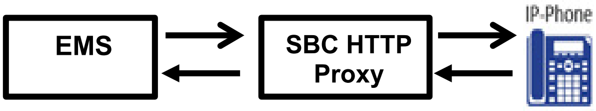
- Alarms and statuses can be sent from the phones to the IP Phone Management Server, i.e., REST requests originate from the phone and the EMS functions as a REST server.
- The IP Phone Management Server can perform auto-discovery of the endpoints for the purpose of uploading configuration and firmware files.
- 'Actions' menu items cannot be applied (see Table 8-2), for example, **Reset Phone**, i.e., the EMS functions as a REST client.

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

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

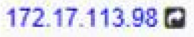
The EMS automatically updates phones' .cfg configuration file. The phone periodically checks whether there is a new file on the EMS server (directly, or via the SBC HTTP proxy if the phones are behind a NAT). The frequency of the check is configurable: Every night, Every hour, etc. The default setting 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 EMS automatically updates phones' .img firmware file. The phone periodically checks whether there is a new .img file on the EMS server (directly, or via SBC HTTP proxy if the phones are behind a NAT).



- When the EMS communicates with the the SBC HTTP proxy, for example, when it communicates Actions (Check Status, Change Region, Update Firmware, Open Web Admin, Reset Phone, Update Configuration, Send Message, Delete Status and Telnet – see Figure 8-6), communications are always over HTTPS. Similarly, when the SBC HTTP proxy communicates with the EMS, communications can be over HTTPS (recommended).
- The string used to configure DHCP Option 160 for communication with the EMS 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 management server interface indicates this with the following icon: 

172.17.113.98

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

Note: To support this feature, the SBC HTTP Proxy should be correctly configured. For more information, see the relevant *SIP User's Manual*.

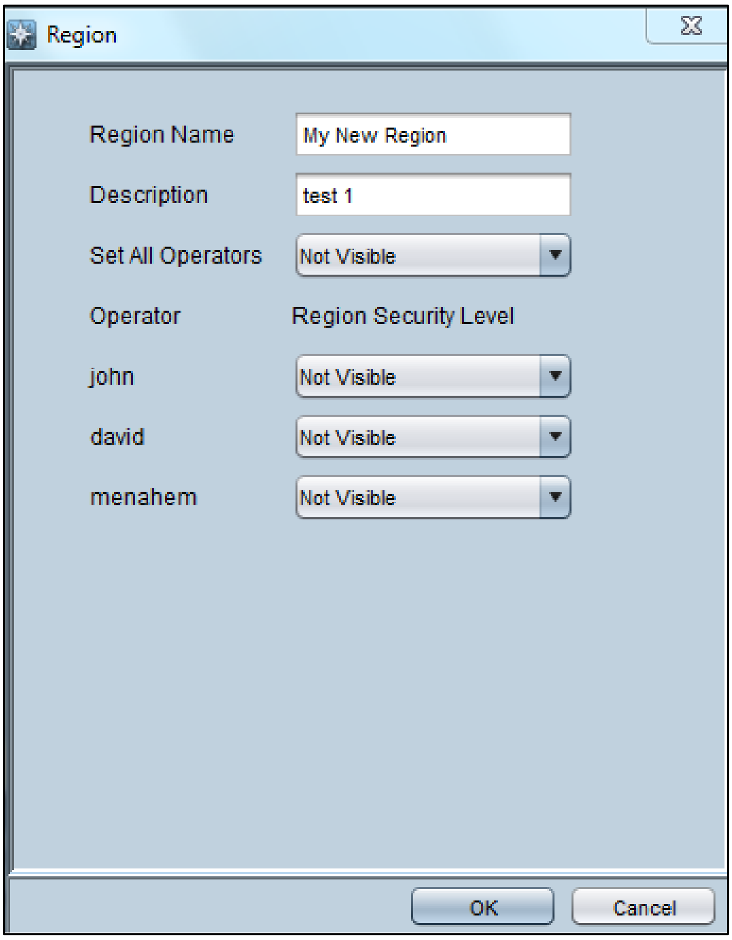
1.5 Configuring Regions in the EMS

Before provisioning phones using Zero Touch, you need to configure regions in the EMS. If there is only one region in the network you're managing, you must still configure at least one region. The number of defined regions must correlate with the number of DHCP servers/subnets in the network for Zero Touch provisioning to function, because the DHCP server/subnet redirects the phone to the relevant regional configuration template.

➢ **To configure a region in the EMS:**

1. Access the EMS (see the *EMS User's Manual* for more information if necessary).
2. Right-click Globe (the root) in the MG Tree and choose **Add Region** from the sub-menu; the following screen appears:

Figure 5-1: Configuring a Region



Region

Region Name: My New Region

Description: test 1

Set All Operators: Not Visible

Operator	Region Security Level
john	Not Visible
david	Not Visible
menahem	Not Visible

3. Define the region's name and type in an optional description.
4. From the 'Set All Operators' dropdown you can select the same security level for all administrators.
5. From under the 'Operator Region Security Level' you can select the security rights for each operator. See also Appendix F.
6. Click **OK**; the region is configured.

Note: Setting security level for other administrators applies only to Operator/Monitoring administrators. If no such administrator is defined, the option is not displayed.

1.6 Preparing the Network for Zero Touch Provisioning

This section shows how to prepare the network for Zero Touch provisioning. Zero Touch enables phones to be automatically provisioned when plugged in to the network.

Note: Applies to all IP phones irrespective of Lync/non-Lync.

This section targets

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

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

- Follow the procedure shown in the table below.

Table 1-3: Zero Touch Flow

Flow	Description
1	Define regions in the EMS (see the previous section). If there is only one region in the network, that region will define the entire network.
2	Configure a 'system' user (see Section 3)
3	Prepare a template per region (see Section 4)
4	Upload the firmware .img file to the EMS provisioning server (see Section 5)
5	Configure DHCP Option 160 with Regional URL (see Section 6)

2 Starting up and Logging in

This section shows how to start the IP Phone Management Server GUI and log in. Before logging in, run the EMS.

Note:

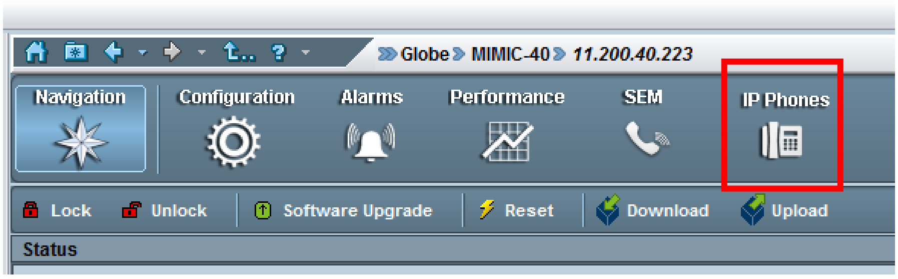
- To access the IP Phone Management Server without running the EMS, point your web browser to **https://<EMS_IP_Address>/ipp** and then in the login screen that opens, log in. If the browser is pointed to HTTP, it will be redirected to HTTPS.
- The IP Phone Management Server UI is a secured web client that runs on any standard web browser supporting HTML5: Internet Explorer version 11 and later, Chrome or Firefox.

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

➢ **To log in to the IP Phone Management Server via the EMS:**

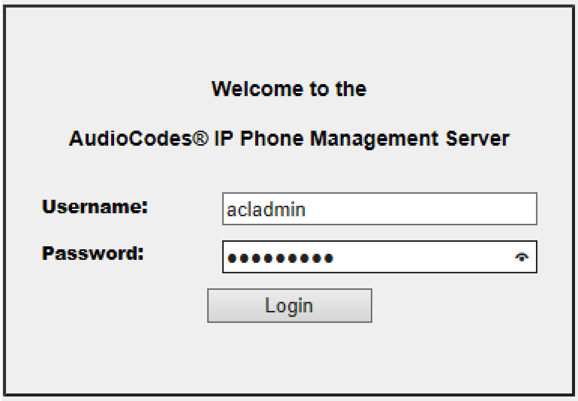
1. Open the EMS and in the main screen toolbar, click the **IP Phones** button.

Figure 2-1: EMS - IP Phone Management Server button



The Welcome to the IP Phone Management Server screen opens:

Figure 2-2: Welcome to the IP Phone Management Server



Welcome to the

AudioCodes® IP Phone Management Server

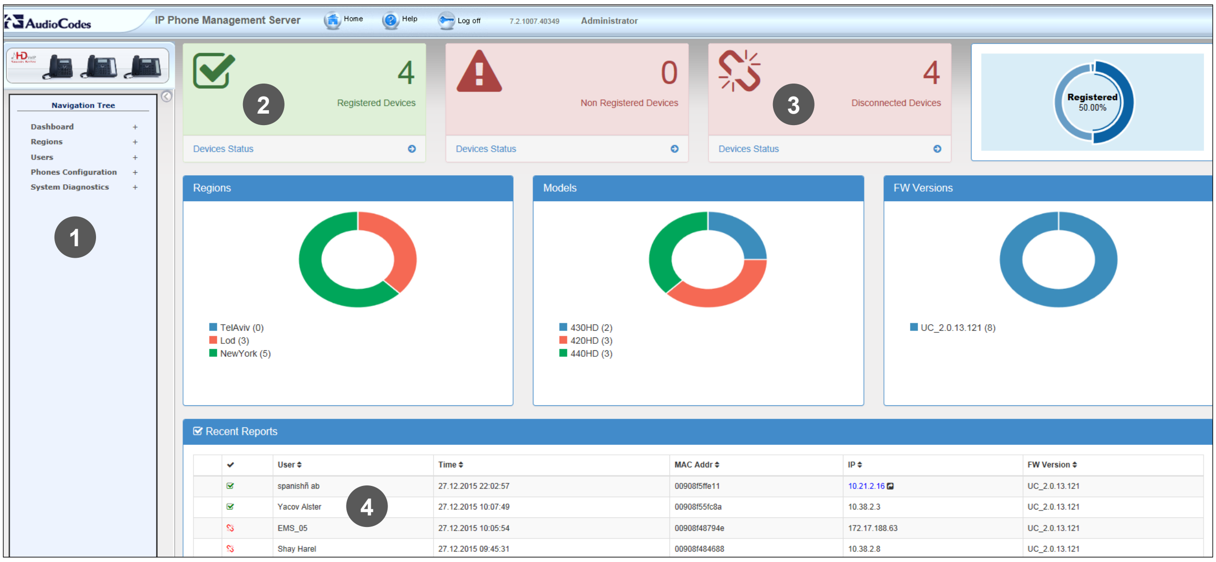
Username: acladmin

Password: ●●●●●●●●●

Note: The 'Username' and 'Password' used to log in to the IP Phone Management Server are the same as those used to log in to the EMS.

2. Enter your Username and Password (default = **acladmin** and **pass_1234**) and click **Login**; the application is launched and the homepage displayed.

Figure 2-3: IP Phone Management Server User Interface - Homepage



✓	User	Time	MAC Addr	IP	FW Version
✓	spanishñ ab	27.12.2015 22:02:57	00908f5ffe11	10.21.2.16	UC_2.0.13.121
✓	Yacov Alster	27.12.2015 10:07:49	00908f55fc8a	10.38.2.3	UC_2.0.13.121
	EMS_05	27.12.2015 10:05:54	00908f48794e	172.17.188.63	UC_2.0.13.121
	Shay Harel	27.12.2015 09:45:31	00908f484688	10.38.2.8	UC_2.0.13.121

1 = Navigation pane
2 = Network registration status
3 = Network health status
4 = List of users and their current status

Note: After first-time login, no users and devices are displayed in the Home page.

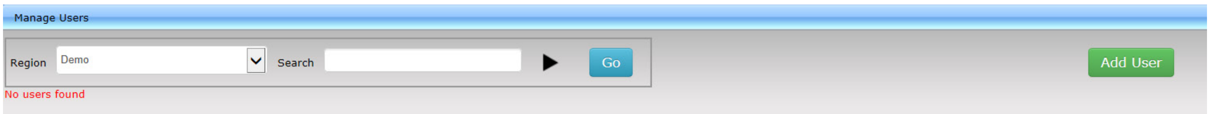
3 Configuring a 'System User'

This section shows how to configure a 'system user' whose user name is **system** and whose password is **system**. This is necessary for *basic REST API authentication*, after the phones are plugged in to the network for the first time.

➢ To configure a 'system user':

1. From the IP Phone Management Server navigation tree, access the Manage Users page (**Users** > **Manage Users**).

Figure 3-1: Manage Users



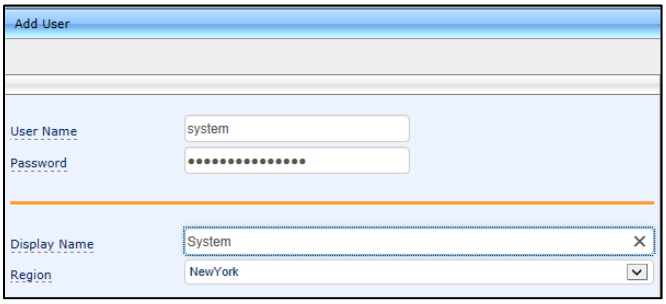
Manage Users

Region: Demo   Search:

No users found

2. Click the **Add User** button; the Add User screen opens.

Figure 3-2: Add User



Add User

User Name: system

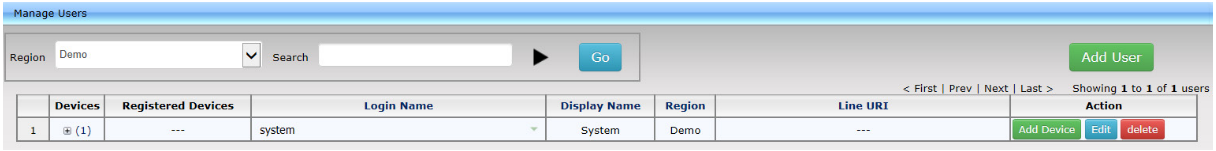
Password: •••••••••••••••

Display Name: System

Region: NewYork

3. Configure the 'User Name' field as **system** and the 'Password' field as **system**.
4. From the dropdown, select the 'Region' you want, and then click the **Submit** button.
5. Make sure in the Manage Users screen that the user is added.

Figure 3-3: Manage Users Screen Displaying Added User



Manage Users

Region: Demo   Search:

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

	Devices	Registered Devices	Login Name	Display Name	Region	Line URI	Action
1	⊕ (1)	---	system	System	Demo	---	Add Device Edit delete

This page is intentionally left blank.

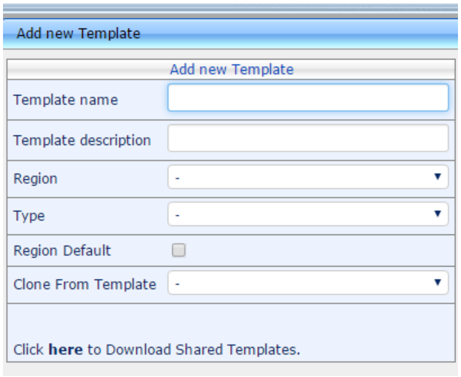
4 Preparing a Template per Region/Model

You need to prepare a template for each region / type (phone mode) in the deployment. The template informs the EMS how to generate the .cfg configuration file when the phones are plugged in to the network. After the phones are plugged in to the network, the .cfg configuration file is downloaded to them from the EMS provisioning server.

➢ **To prepare a template for a region / phone model:**

1. Open the 'Add new template' screen (**Phones Configuration** > **Templates** > **Add New Template** button).

Figure 4-1: Add New Template



Add new Template

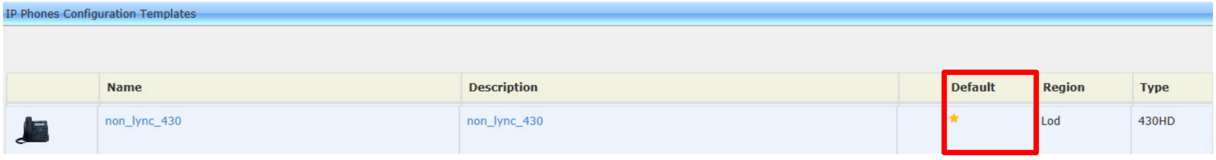
Add new Template

Template name	
Template description	
Region	- ▾
Type	- ▾
Region Default	□
Clone From Template	- ▾

Click **here** to Download Shared Templates.

2. Enter a name for the template. Make the name intuitive. Include region *and* model aspects in it.
3. Provide a description of the template to enhance intuitive maintenance.
4. From the 'Region' dropdown list, select the region.
5. From the 'Type' dropdown list, select the phone model.
6. Select the **Default Region** option for the template to be the default for this region. More than one phone type can be in the same region. All can have a common template. But only one template can be configured per region. If a second template is configured for the region, it overrides the first. After a template is added, it's displayed as shown below in the IP Phones Configuration Template page. The gold asterisk in the Default column indicates that this template is the default. Then when a phone is connected to the network, if the phone is of this type and located in this region, it'll automatically be provisioned via DHCP server from the EMS provisioning server (Zero Touch).

Figure 4-2: Default Template Indicated by Gold Asterisk



IP Phones Configuration Templates

	Name	Description	Default	Region	Type
☎	non_lync_430	non_lync_430	★	Lod	430HD

7. From the 'Clone From Template' dropdown list, select a template to clone from. If the template is for phones in a region that are Microsoft Lync phones, choose a Lync template.
8. Do this for all regions 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.

This page is intentionally left blank.

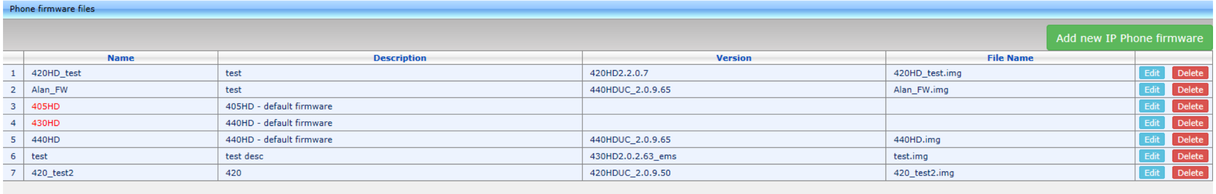
5 Uploading .img Firmware File to EMS Provisioning Server

After obtaining the latest .img firmware file from AudioCodes, upload it to the EMS provisioning server. When phones are later connected to the network, they're automatically provisioned with firmware from the server.

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

1. In the IP Phone Management Server, access the Phone Firmware Files page (**Phones Configuration** > **Phone Firmware Files**).

Figure 5-1: Phone Firmware Files



Phone firmware files

	Name	Description	Version	File Name		
1	420HD_test	test	420HD2.2.0.7	420HD_test.img	Edit	Delete
2	Alan_FW	test	440HDUC_2.0.9.65	Alan_FW.img	Edit	Delete
3	405HD	405HD - default firmware			Edit	Delete
4	430HD	440HD - default firmware			Edit	Delete
5	440HD	440HD - default firmware	440HDUC_2.0.9.65	440HD.img	Edit	Delete
6	test	test desc	430HD2.0.2.63_ems	test.img	Edit	Delete
7	420_test2	420	420HDUC_2.0.9.50	420_test2.img	Edit	Delete

2. In the Phone Firmware Files screen, click the **Add new IP Phone firmware** button.
3. Navigate to the .img file and upload it to the EMS provisioning server.

This page is intentionally left blank.

6 Configuring DHCP Option 160 with Regional URL

You need to point DHCP Option 160 to a Regional 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).

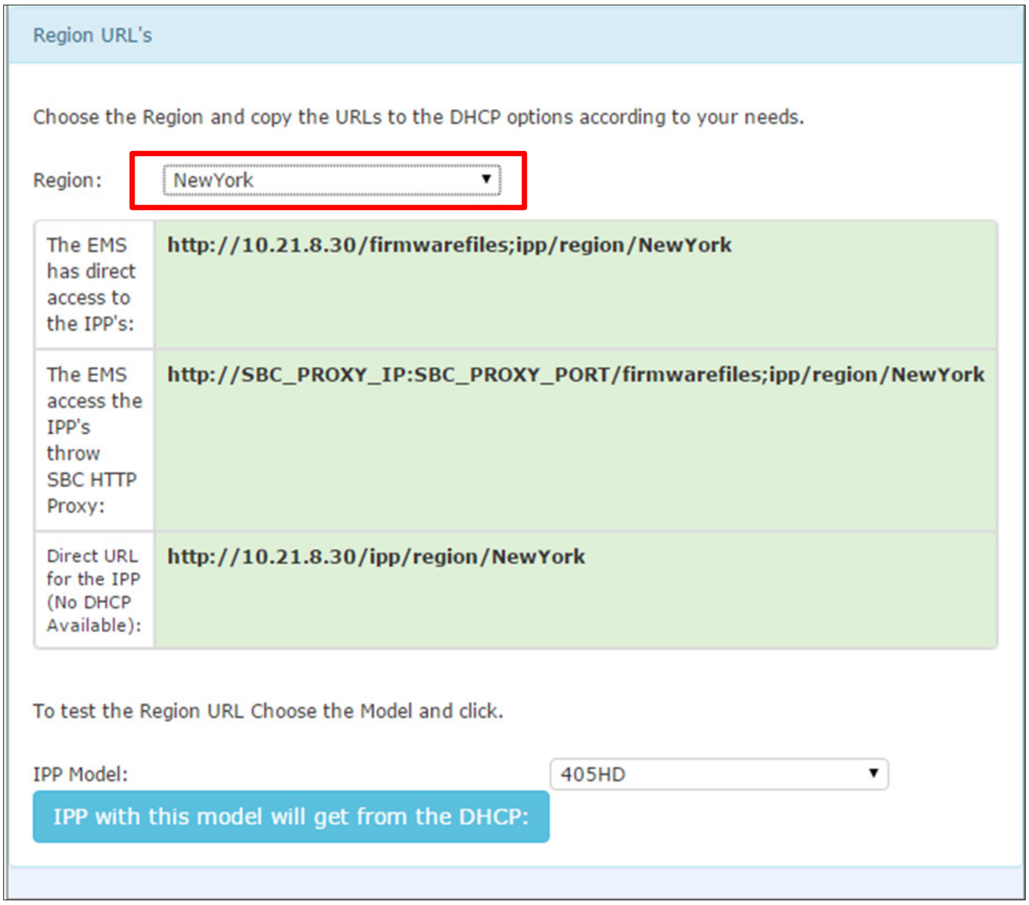
Later when the (Lync) phones are signed in, the phones and users are automatically added to IP Phone Management Server and downloads the phones' private .cfg configuration file to them.

Note: The Zero Touch feature significantly accelerates uptime by enabling multiple users and phones to automatically be provisioned and added to the IP Phone Management Server.

➢ To point DHCP Option 160 to a Regional URL:

1. In the IP Phone Management Server, open the System Settings page (**Phones Configuration** > **System Settings**).
2. Click the **DHCP Option Template** button.
3. In the DHCP Option Template dialog that opens, click the **DHCP Option 160 URLs** link located lowermost in the dialog; the dialog extends to display System URLs and Region URLs screen sections.
4. Under the Region URLs section, select the region (in which the phones are located) from the 'Region' dropdown list. The Region URLs options are displayed:

Figure 6-1: Regional URLs



Region URL's

Choose the Region and copy the URLs to the DHCP options according to your needs.

Region: NewYork

The EMS has direct access to the IPP's:	http://10.21.8.30/firmwarefiles;ipp/region/NewYork
The EMS access the IPP's throw SBC HTTP Proxy:	http://SBC_PROXY_IP:SBC_PROXY_PORT/firmwarefiles;ipp/region/NewYork
Direct URL for the IPP (No DHCP Available):	http://10.21.8.30/ipp/region/NewYork

To test the Region URL Choose the Model and click.

IPP Model: 405HD

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

5. Choose either:
   - **The EMS has direct access to the phones**. The DHCP server will connect the phones directly to the EMS server IP address.
     - Copy (Ctrl+C) the URL **HTTP://<EMS IP>/firmwarefiles;ipp/region/<region selected in Step 1>** and paste it into DHCP Option 160 in the enterprise's DHCP server
   - **The EMS 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 EMS server.
     - If the phones communicate with an SBC HTTP proxy rather than directly with the EMS server, copy (Ctrl+C) the URL **http://SBC_PROXY_IP:SBC_PROXY_PORT/firmwarefiles;ipp/region/Region** into DHCP Option 160 in the enterprise's DHCP server.
   - **Direct URL for the IPP (No DHCP Available)** – usually used for debugging purposes when no DHCP is available.

Note:

- Configure DHCP option 160 to point to the EMS 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-EMS communications will then be via the SBC HTTP proxy rather than direct.

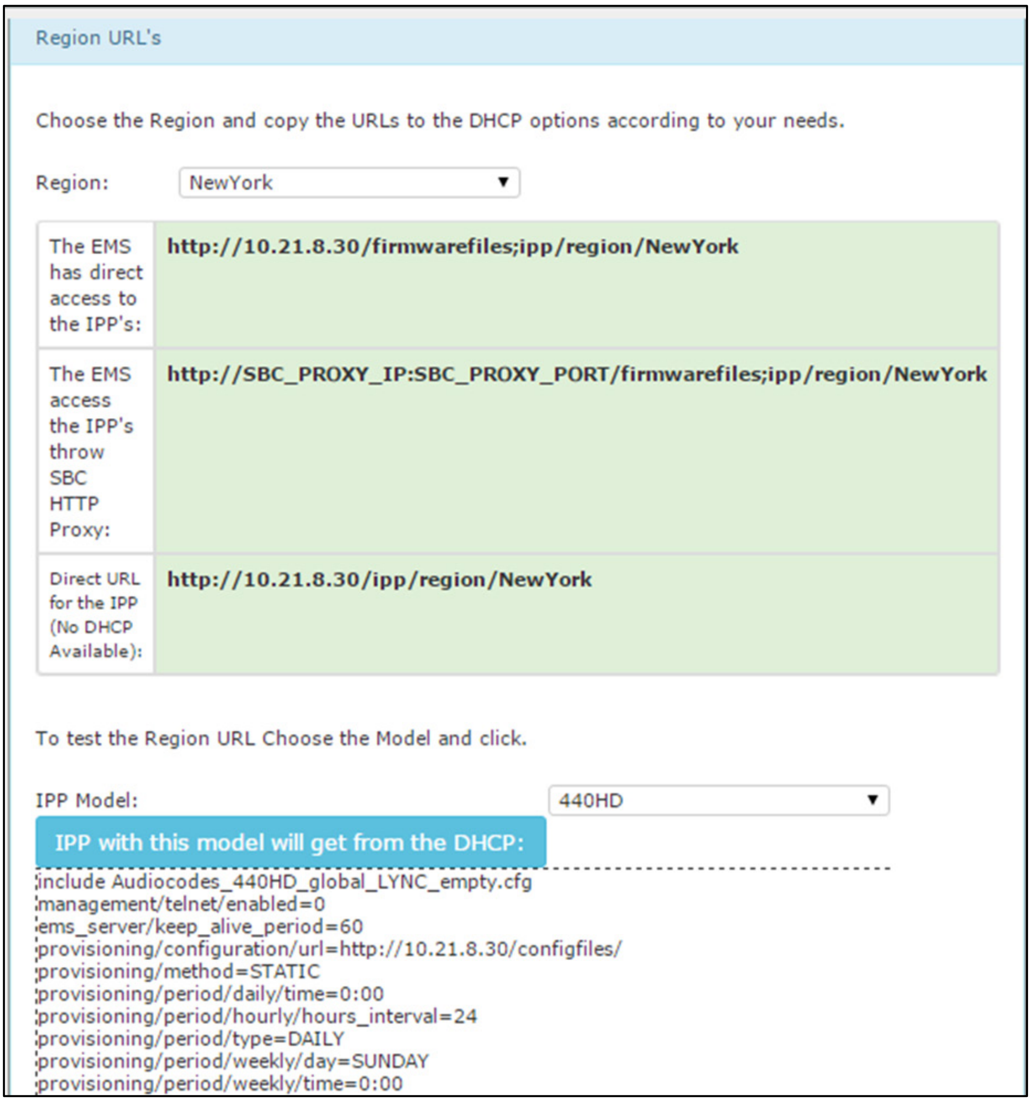
6. After copying the Regional URL (Ctrl+C) and pasting it into the enterprise's DHCP server's DHCP Option 160, select the phone model from the 'IPP Model' dropdown and then click the button **IPP with this model will get from the DHCP**; an output of the configuration file that you have configured to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

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

- DHCP server
- Subnet

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

Figure 6-2: Verifying the Phone's Configuration File



Region URL's

Choose the Region and copy the URLs to the DHCP options according to your needs.

Region: NewYork ▾

The EMS has direct access to the IPP's:	http://10.21.8.30/firmwarefiles;ipp/region/NewYork
The EMS access the IPP's throw SBC HTTP Proxy:	http://SBC_PROXY_IP:SBC_PROXY_PORT/firmwarefiles;ipp/region/NewYork
Direct URL for the IPP (No DHCP Available):	http://10.21.8.30/ipp/region/NewYork

To test the Region URL Choose the Model and click.

IPP Model: 440HD ▾

IPP with this model will get from the DHCP:

```
include Audiocodes_440HD_global_LYNC_empty.cfg
management/telnet/enabled=0
ems_server/keep_alive_period=60
provisioning/configuration/url=http://10.21.8.30/configfiles/
provisioning/method=STATIC
provisioning/period/daily/time=0:00
provisioning/period/hourly/hours_interval=24
provisioning/period/type=DAILY
provisioning/period/weekly/day=SUNDAY
provisioning/period/weekly/time=0:00
```

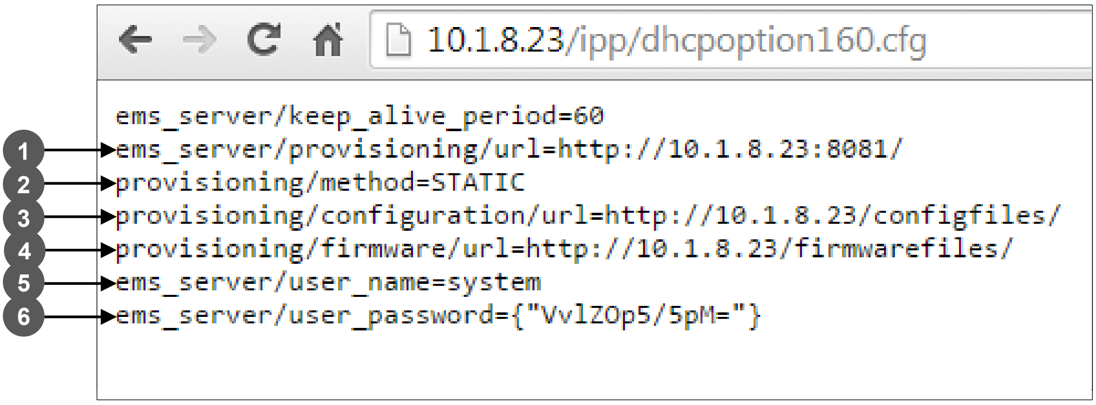
Note: Zero Touch is supported for phones with sign-in capabilities only.

6.1 Configuring DHCP Option 160 with System URL

> **Note:**
> - 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 **dhcpoption160.cfg** file.

Figure 6-3: cfg File Located on the EMS Provisioning Server



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

Legend	Description
1	Points to the URL of the EMS provisioning server.
2	STATIC provisioning method, so the cfg and img files are automatically pulled from the EMS 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 EMS provisioning server.
4	Location of the img file, pulled by the phones when they're plugged into the network, on the EMS 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.

> **Note:**
> - The **dhcpoption160.cfg** file is created when logging in for the first time to the IP Phone Management Server.
> - The file is an internal EMS file and cannot be manually modified.
> - After installation, the first, second and third lines in the file are automatically updated.

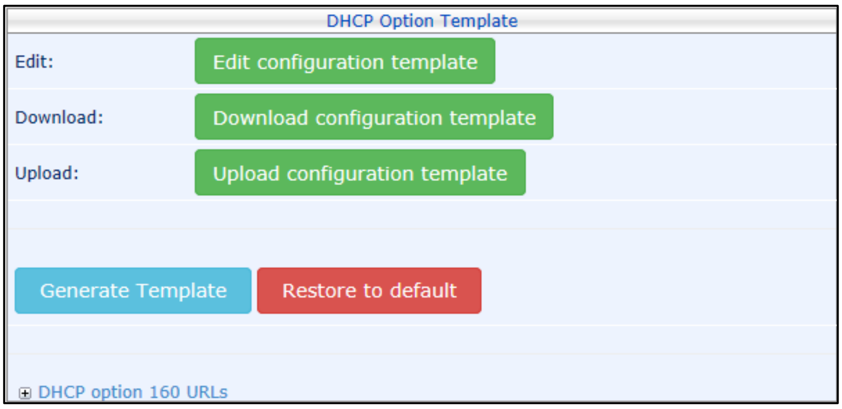
6.1.1 Editing the DHCP Option 160 cfg File

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:**

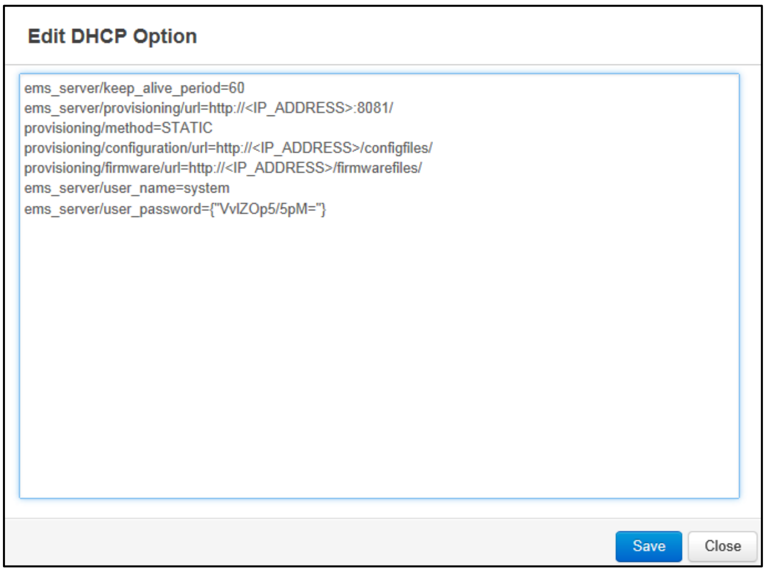
1. Access the System Settings page (**Phones Configuration** > **System Settings**).
2. Click the **DHCP Option Configuration** button; this dialog opens:

Figure 6-4: DHCP Option Template



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

Figure 6-5: Edit DHCP Option



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

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

Table A-1: DHCP Option

Parameter	Description
Keep alive period	You can configure how often the phones generate a keep-alive trap towards the IP Phone Management Server. 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 (EMS server).
Provisioning Method	Defines the provisining method, i.e., STATIC or Dynamic (DHCP). Do not change this setting. The setting must remain STATIC. If not, the phone will continuously perform restarts.
Provisioning Configuration URL	Defines the URL of the location of the configuration files (including IP address and port) in the provisioning server (EMS server).
Provisioning Firmware URL	Defines the URL of the location of the firmware files (including IP address and port) in the provisioning server (EMS server).
User Name	Defines the user name for the REST API. Default: **System**. Later, each phone receives its own unique user name.
User Password	Encrypted. Defines the user password for the REST API. Default: **System**. Later, each phone receives its own unique user password.

Note: You can always restore these settings to their defaults if necessary by clicking the **Restore to default** button in the DHCP Option Template dialog, but it's advisable to leave these settings unchanged.

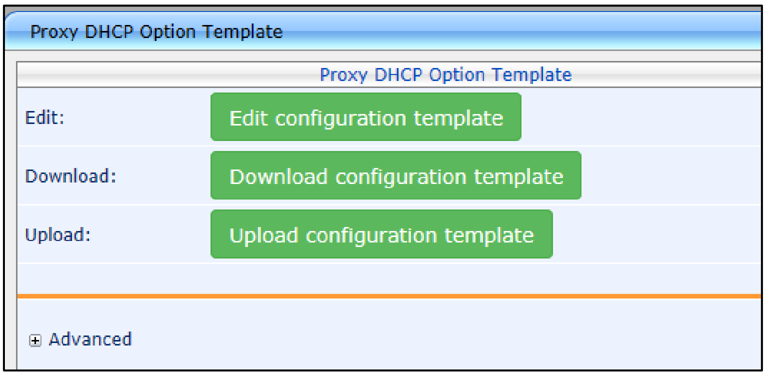
6.1.2 Editing the SBC HTTP Proxy

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. Access the System Settings page (**Phones Configuration** > **System Settings**).
2. Click the **SBC Proxy Configuration** button; the Proxy DHCP Option Template screen opens.

Figure 6-6: Proxy DHCP Option Template


Proxy DHCP Option Template
Proxy DHCP Option Template
Edit:
Edit configuration template
Download:
Download configuration template
Upload:
Upload configuration template
⊞ Advanced

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**.

This page is intentionally left blank.

7 Importing a CSV File [Non-Lync Phones]

In non-Lync environments, after configuring 'system user' you can plug the phones into the network, but *before* plugging in the phones, it's recommended to:

1. Import a CSV file with users and devices. Best practice is to create one or more users with devices and export them to a CSV file, add new users and devices in the same format to the CSV file, and import it (see Appendix A).
2. Use the **Approve** button to add a device manually if you don't know it's MAC address. After importing, approve users (see Appendix B).

Note: Approving users is not necessary when using Zero Touch or when importing a CSV file. For details about approving users, see Appendix B.

3. Generate a cfg configuration file and apply it to users. After this, the phones pull the cfg configuration file containing usernames and passwords from the EMS provisioning server.

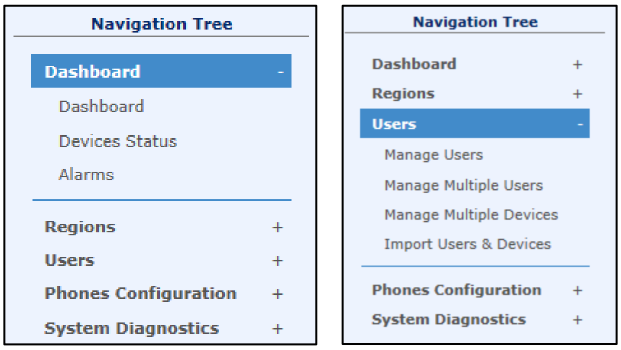
This page is intentionally left blank.

8 Monitoring and Maintaining the Phone Network

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

The following Dashboard and Users pages let you monitor and maintain the phone network:

Figure 8-1: Dashboard and Users



The sections below show what each page lets you do.

8.1 Monitoring the Network from the Dashboard

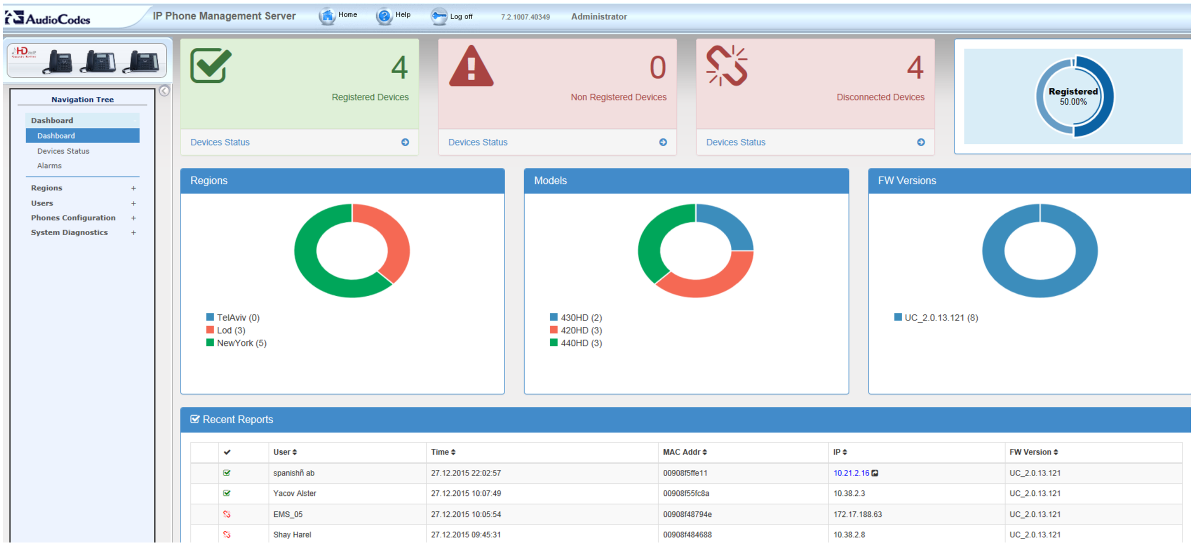
The Dashboard page lets you quickly identify

- 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:**

- In the navigation tree, click **Dashboard** > **Dashboard**.

Figure 8-2: Dashboard

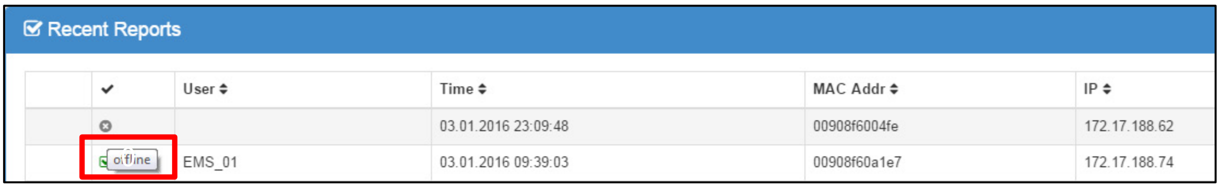


Recent Reports

	✓	User	Time	MAC Addr	IP	FW Version
	✓	spanishñ ab	27.12.2015 22:02:57	00908f5ffe11	10.21.2.16	UC_2.0.13.121
	✓	Yacov Alster	27.12.2015 10:07:49	00908f55fc8a	10.38.2.3	UC_2.0.13.121
	✗	EMS_05	27.12.2015 10:05:54	00908f48794e	172.17.188.63	UC_2.0.13.121
	✗	Shay Harel	27.12.2015 09:45:31	00908f484688	10.38.2.8	UC_2.0.13.121

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

Figure 8-3: Dashboard - Lync IP Phone Not Registered

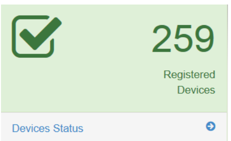
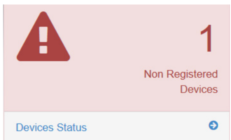
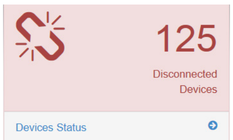
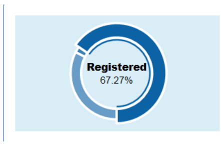
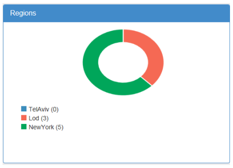
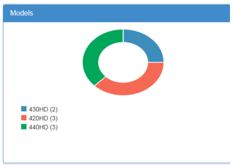
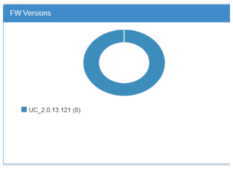


Recent Reports

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

- Point your mouse over the icon to view the 'offline' indication (see the figure above).
- If the phone is a generic model, a red triangle enclosing an exclamation mark will be displayed, as shown in the figure above.
- View the following status thumbnails on the Dashboard (left to right, top down):

Table 8-1: Dashboard – Status Thumbnails

Status Thumbnail	Description
	The number of registered devices. Click the **Devices Status** link to quickly access the Devices Status page.
	The number of non-registered devices. Click the **Devices Status** link to quickly access the Devices Status page.
	The number of disconnected devices. Click the **Devices Status** link to quickly access the Devices Status page.
	The percentage of registered devices.
	Pie chart showing the number of devices per region that are registered.
	Pie chart showing how many phones of each model are registered.
	Pie chart showing how many phones of each firmware version are registered.

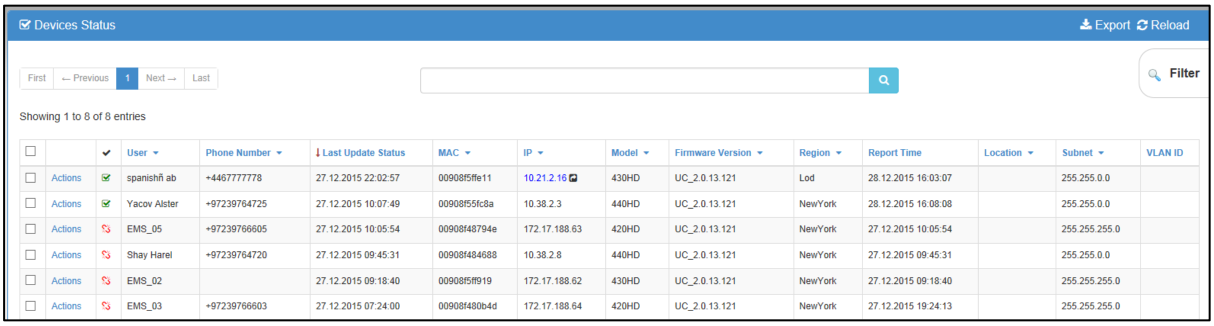
8.2 Checking Devices Status

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

➢ To check a phone's status:

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

Figure 8-4: Devices Status



Devices Status

Export Reload

First ← Previous 1 Next → Last

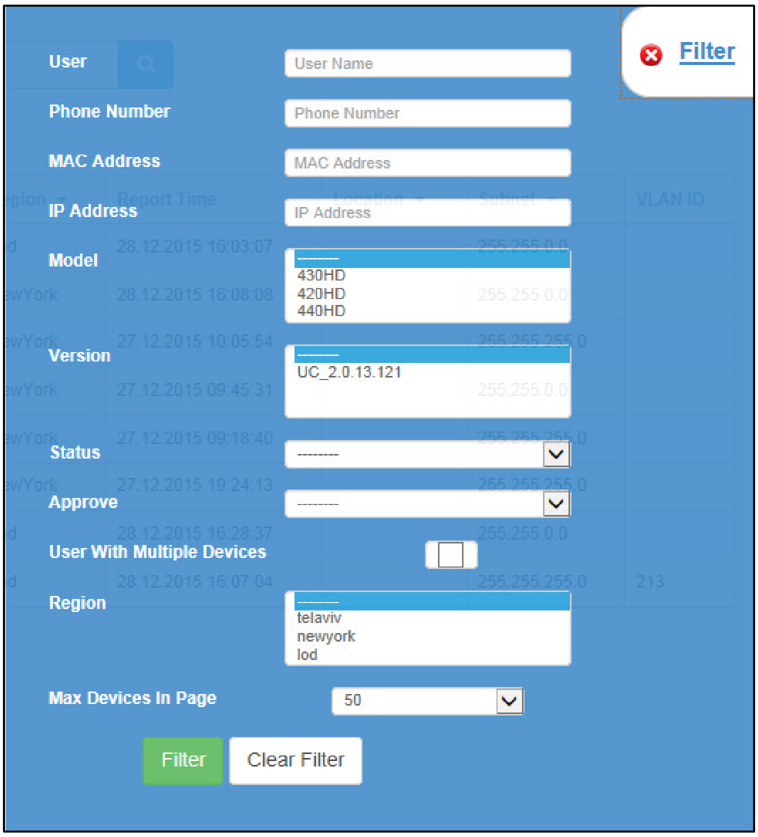
Filter

Showing 1 to 8 of 8 entries

☐		✓	User	Phone Number	Last Update Status	MAC	IP	Model	Firmware Version	Region	Report Time	Location	Subnet	VLAN ID
☐	Actions	☑	spanishñ ab	+4467777778	27.12.2015 22:02:57	00908f5ffe11	10.21.2.16	430HD	UC_2.0.13.121	Lod	28.12.2015 16:03:07		255.255.0.0	
☐	Actions	☑	Yacov Alster	+97239764725	27.12.2015 10:07:49	00908f55fc8a	10.38.2.3	440HD	UC_2.0.13.121	NewYork	28.12.2015 16:08:08		255.255.0.0	
☐	Actions	✗	EMS_05	+97239766605	27.12.2015 10:05:54	00908f48794e	172.17.188.63	420HD	UC_2.0.13.121	NewYork	27.12.2015 10:05:54		255.255.255.0	
☐	Actions	✗	Shay Harel	+97239764720	27.12.2015 09:45:31	00908f484688	10.38.2.8	440HD	UC_2.0.13.121	NewYork	27.12.2015 09:45:31		255.255.0.0	
☐	Actions	✗	EMS_02		27.12.2015 09:18:40	00908f5ff919	172.17.188.62	430HD	UC_2.0.13.121	NewYork	27.12.2015 09:18:40		255.255.255.0	
☐	Actions	✗	EMS_03	+97239766603	27.12.2015 07:24:00	00908f480b4d	172.17.188.64	420HD	UC_2.0.13.121	NewYork	27.12.2015 19:24:13		255.255.255.0	

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

Figure 8-5: Devices Status Filter



Filter

User: User Name

Phone Number: Phone Number

MAC Address: MAC Address

IP Address: IP Address

Model: --------
430HD
420HD
440HD

Version: --------
UC_2.0.13.121

Status: --------

Approve: --------

User With Multiple Devices: ☐

Region: --------
telaviv
newyork
lod

Max Devices In Page: 50

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, region, or maximum devices shown in the page.

4. Non-Lync and Lync phones are displayed differently. The format of 'User Agent' for non-Lync phones is for example **AUDC-IPPhone/2.0.4.30 (430HD; 00908F4867AF)** while the format for Lync phones is **AUDC-IPPhone-430HD_UC_2.0.7.70/1.0.0000.0** Only Lync phones are displayed under 'Location', non-Lync phones are not.

5. You can click the **Export** link to export all entries in the Device Status page - or a selected list of entries in the page - to a csv file. The feature facilitates inventory management; it lets you easily obtain a list of phone MAC address or Serial Numbers, for example. After generating a csv file, a download option is displayed in the lower-left corner. You can either save the csv file or open it directly in Excel. The same information displayed in the page is displayed in the Excel file in Excel format.
6. You can click an individual user's **Actions** link; the following menu is displayed:

Figure 8-6: Actions Menu - Single User

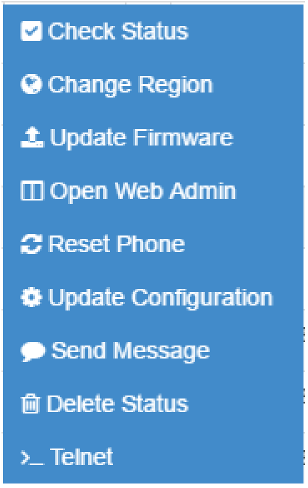
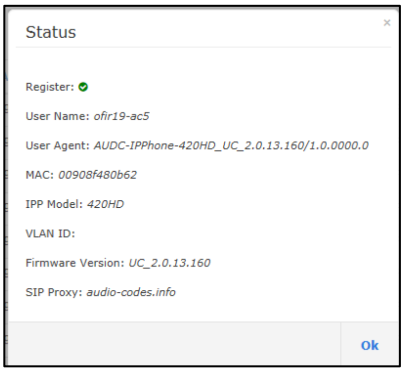
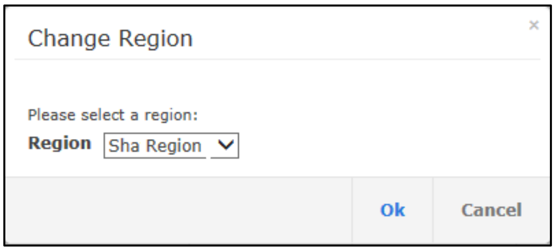
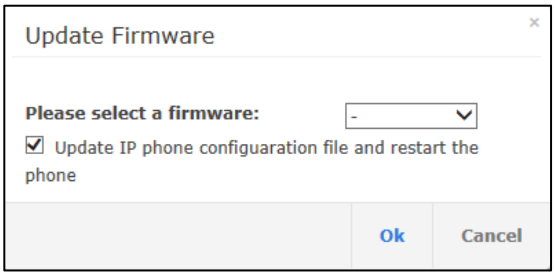


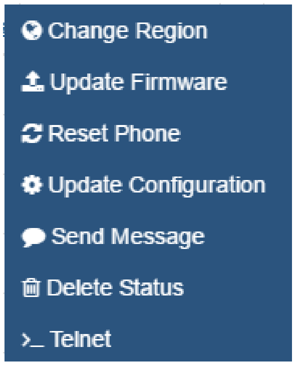
Table 8-2: Actions Menu

Action	Description
Check Status	Select the 'Check Status' option; the status is displayed:  Status Register: ✓ User Name: *ofir19-ac5* User Agent: *AUDC-IPPhone-420HD_UC_2.0.13.160/1.0.0000.0* MAC: *00908f480b62* IPP Model: *420HD* VLAN ID: Firmware Version: *UC_2.0.13.160* SIP Proxy: *audio-codes.info* Ok
Change Region	Select the 'Change Region' option:  Change Region Please select a region: **Region** Sha Region Ok Cancel From the dropdown, select the region, and then click **Ok**.

Action	Description
Update Firmware	You can update firmware per device, or for multiple selected devices (see step 7 below). Select the 'Update Firmware' menu option:  Update Firmware × Please select a firmware: - ☑ Update IP phone configuaration file and restart the phone Ok Cancel From the dropdown, select the firmware file, and then click **Ok**.; the firmware file is updated.
Open Web Admin	Opens the Web interface (see the phone's *Administrator's Manual*). By default, the Web interface opens in HTTPS.
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.
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 LCD/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 LCD/s.
Delete Status	Deletes the devices from the Status table.
Telnet	Allows administrators to send Telnet (CLI) debug commands to the phone for debugging purposes. Important: For this feature to function, Telnet must be enabled on the device. You can enable Telnet from the Web interface's Telnet page (**Management** > **Remote Management** > **Telnet**).

7. You can select multiple users and then click the **Selected Rows Actions** link; the following menu is displayed:

Figure 8-7: Actions Menu - Selected Rows



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

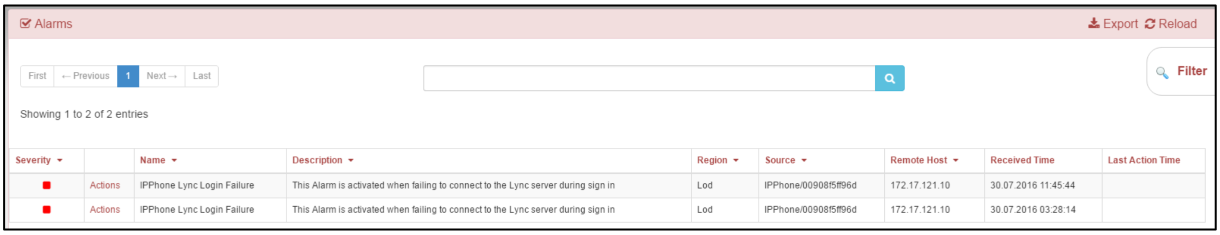
8.3 Monitoring Alarms

AudioCodes IP phones send alarms via the REST protocol. The EMS forwards them as mail, SNMP traps, etc.

The Alarms page (**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

Figure 8-8: Alarms



Showing 1 to 2 of 2 entries

Severity		Name	Description	Region	Source	Remote Host	Received Time	Last Action Time
🟥	Actions	IPPhone Lync Login Failure	This Alarm is activated when failing to connect to the Lync server during sign in	Lod	IPPhone/00908f5ff96d	172.17.121.10	30.07.2016 11:45:44	
🟥	Actions	IPPhone Lync Login Failure	This Alarm is activated when failing to connect to the Lync server during sign in	Lod	IPPhone/00908f5ff96d	172.17.121.10	30.07.2016 03:28:14	

The management server displays *active* alarms, not historical alarms.

Red indicates a severity level of Critical

Orange indicates a severity level of Major

Click ⓘ for more information about the alarm

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

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

Table 8-3: Alarms

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

8.3.1 Registration Failure Alarm

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

Table 8-4: 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 EMS to forward the IPPhoneRegisterFailure alarm
Description	This alarm is activated when a registration failure occurs
Alarm Title	Registration Failure
Alarm Type	communicationsAlarm(1)
Probable Cause	communicationsProtocolError(5)
Severity	Critical
Corrective Action	The problem is typically not related to the phone but to the server. The user/phone may not be defined, or may be incorrectly defined, or may previously have been defined but the username (for example) may have been changed, causing the registration to fail. Make sure the username and password credentials are the same in server and phone, and weren't changed; server-phone credentials must be synchronized. Make sure the server is responsive.

8.3.2 Survivable Mode Start Alarm

The table below describes the Survivable Mode Start alarm.

Table 8-5: 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 EMS 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.

8.3.3 Lync Login Failure Alarm

The table below describes the Lync Login Failure alarm.

Table 8-6: 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 EMS to forward the IPPhoneLyncLoginFailure alarm
Description	This alarm is activated when failing to connect to the Lync 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 Lync 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.

8.3.4 Endpoint License Alarm

The table below describes the Endpoint License alarm.

Table 8-7: IP Phone Endpoint License Alarm

Description	This alarm is issued when the number of endpoints currently running on the EMS 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	EMS 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.

Note: If a license expires:

- Communications with all servers is suspended
- Users cannot log in
- New phones cannot be added

Note: Contact your AudioCodes partner if the license expires.

8.3.5 IP Phone Speaker Firmware Download Failure

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

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

<table>
<tr><td><b>Description</b></td><td colspan="3">This alarm is sent when the phone fails to download the speaker firmware from the server.</td></tr>
<tr><td><b>SNMP Alarm</b></td><td colspan="3">IPPhoneSpeakerFirmDownloadFailure</td></tr>
<tr><td><b>SNMP OID</b></td><td colspan="3">1.3.6.1.4.1.5003.9.20.3.2.0.54</td></tr>
<tr><td><b>Alarm Title</b></td><td colspan="3">IP Phone Speaker Firmware Download Failure.</td></tr>
<tr><td><b>Alarm Source</b></td><td colspan="3">IP Phone</td></tr>
<tr><td><b>Alarm Type</b></td><td colspan="3">communicationsAlarm(1)</td></tr>
<tr><td><b>Probable Cause</b></td><td colspan="3">communicationsProtocolError(5)</td></tr>
<tr><td><b>Additional Info</b></td><td colspan="3"></td></tr>
<tr><td><b>Corrective Action</b></td><td colspan="3">▪ Make sure the IP Phone Management Server is correctly defined.
▪ Contact your network administrator (IT manager).</td></tr>
<tr><td><b>Alarm Severity</b></td><td><b>Condition</b></td><td><b>Alarm Text</b></td><td><b>Corrective Action</b></td></tr>
<tr><td>Minor</td><td></td><td>This alarm is sent when the phone fails to download the speaker firmware.</td><td></td></tr>
<tr><td></td><td></td><td></td><td></td></tr>
<tr><td></td><td></td><td></td><td></td></tr>
</table>

8.3.6 IP Phone Speaker Firmware Upgrade Failure

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

Table 8-9: IP Phone Speaker Firmware Upgrade Failure

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

8.3.7 IP Phone Conference Speaker Connection Failure

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

Table 8-10: Conference IPPhone has no Connection to Speaker

Description	This alarm is sent when the USB connection between the phone and the speaker fails.		
SNMP Alarm	IPPhoneConferSpeakerConnectFailure		
SNMP OID	1.3.6.1.4.1.5003.9.20.3.2.0.56		
Alarm Title	IP Phone Conference Speaker Connection Failure		
Alarm Source			
Alarm Type	communicationsAlarm(1)		
Probable Cause	communicationsProtocolError(5)		
Additional Info			
Corrective Action	• Make sure the USB cable is properly connected. • After making sure, contact your network administrator (IT manager) if the alarm persists.		
Alarm Severity	**Condition**	**Alarm Text**	**Corrective Action**
Major		This alarm is sent when there is failure for the USB connection between the phone and the speaker	

8.4 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

8.5 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 above for more information.

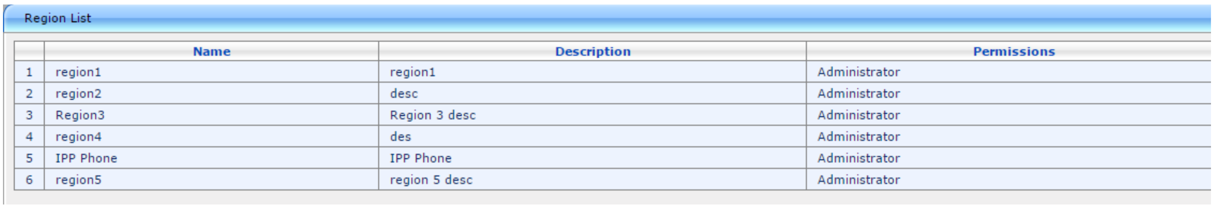
8.6 Viewing Security Levels per Region

You can view the administrator security levels for each region that has been configured in the EMS. See also the *EMS User's Manual* for detailed information.

➢ **To view security levels per region:**

- Open the Region List page (**Regions** > **Manage Regions**).

Figure 8-9: Region List



Region List

	Name	Description	Permissions
1	region1	region1	Administrator
2	region2	desc	Administrator
3	Region3	Region 3 desc	Administrator
4	region4	des	Administrator
5	IPP Phone	IPP Phone	Administrator
6	region5	region 5 desc	Administrator

8.7 Maintaining Users

The Manage Users page lets you maintain users. You can

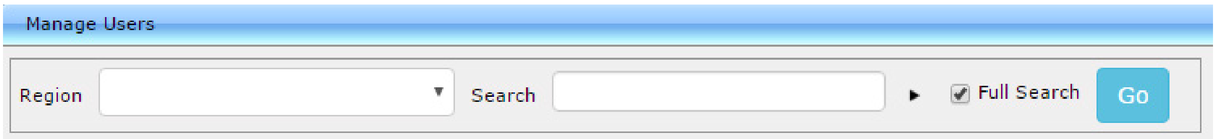
- search for a user/device
- add a user
- add a device to a user
- edit user/device
- view device status
- delete a user/device
- search for a device by region
- search for a device by name

8.7.1 Searching for Users/Devices

Two search methods are available to you when searching for a user or a device:

- Regular search, i.e., you can seach by name, display name
- Full search, i.e., you can click ► and search in all fields, including MAC address.

Figure 8-10: Searching for a User/Device

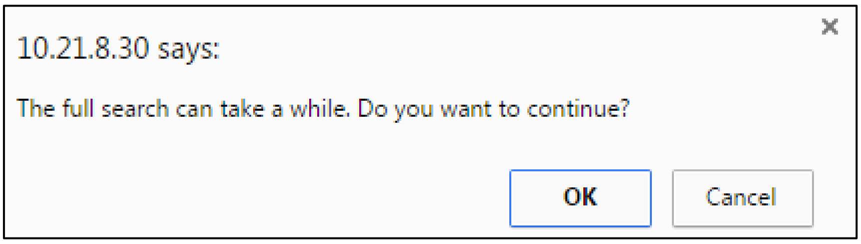


Manage Users

Region ▼ Search ► ☑ Full Search

- If you perform a full seach and there are more than 5000 users in the network, the messge shown below pops up. Click **OK**.

Figure 8-11: Searching in a Network of More than 5000 Users



10.21.8.30 says:

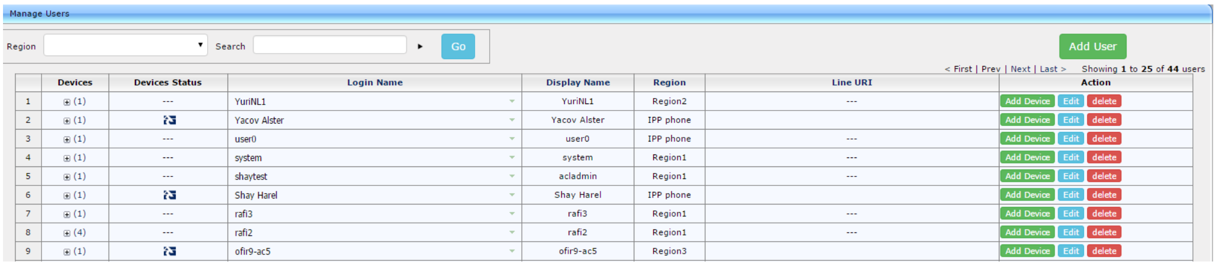
The full search can take a while. Do you want to continue?

8.7.2 Adding a User

➢ To add a user to the Management Server:

1. Access the ‘Manage Users’ page (**Users** > **Manage Users**):

Figure 8-12: Manage Users



Manage Users

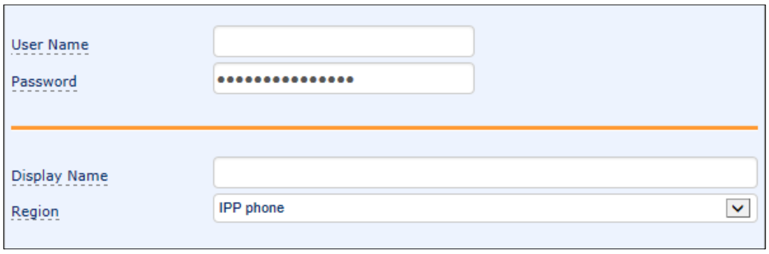
Region ▾ Search ▸ Go

< First | Prev | Next | Last > Showing **1** to **25** of **44** users

	Devices	Devices Status	Login Name	Display Name	Region	Line URI	Action
1	⊞ (1)	---	YuriNL1	YuriNL1	Region2	---	Add Device Edit delete
2	⊞ (1)	☎	Yacov Alster	Yacov Alster	IPP phone		Add Device Edit delete
3	⊞ (1)	---	user0	user0	IPP phone	---	Add Device Edit delete
4	⊞ (1)	---	system	system	Region1	---	Add Device Edit delete
5	⊞ (1)	---	shaytest	acladmin	Region1	---	Add Device Edit delete
6	⊞ (1)	☎	Shay Harel	Shay Harel	IPP phone		Add Device Edit delete
7	⊞ (1)	---	rafi3	rafi3	Region1	---	Add Device Edit delete
8	⊞ (4)	---	rafi2	rafi2	Region1	---	Add Device Edit delete
9	⊞ (1)	☎	ofir9-ac5	ofir9-ac5	Region3		Add Device Edit delete

2. Click the **Add User** button (before adding phones to the IP phone management server you must add users); the following screen is displayed:

Figure 8-13: Add User

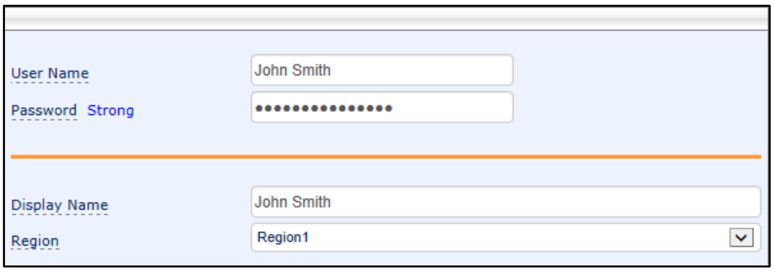


User Name	
Password	•••••••••••••••
Display Name	
Region	IPP phone

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

Note: Region/s must first be defined in the EMS.

Figure 8-14: Add User Definitions



User Name	John Smith
Password Strong	•••••••••••••••
Display Name	John Smith
Region	Region1

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

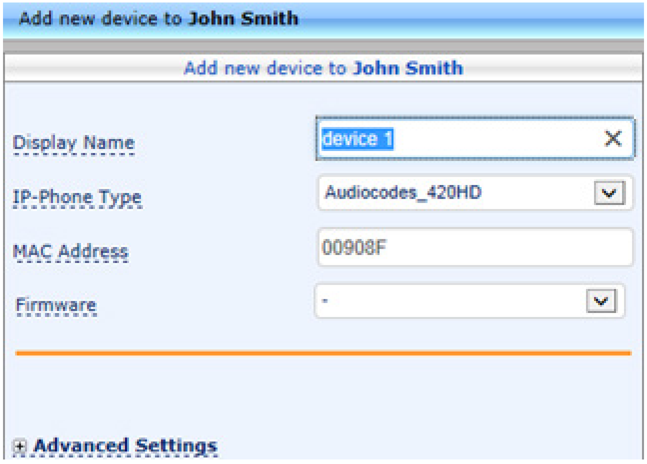
8.7.3 Adding a Phone

You can manually add a single phone to the server.

➢ **To add a phone:**

1. In the Manage Users page, click the **Add Device** button in the row of the listed added user; the following screen opens:

Figure 8-15: Add New Device to User



Add new device to John Smith

Add new device to John Smith

Display Name: device 1

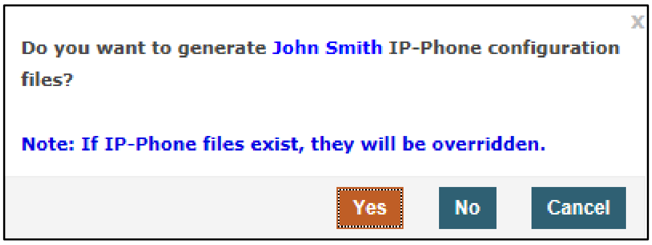
IP-Phone Type: Audiocodes_420HD

MAC Address: 00908F

Firmware: -

2. Enter the 'Display Name'. This is the name that will be displayed in the management server interface.
3. Click the **Submit** button.
4. Click **Add Device** (to associate the employee's name/line with the IP phone).
5. Enter the remaining characters of the 'MAC Address'. The prefix characters are displayed by default.
6. Click the **Submit** button; the following prompt is displayed:

Figure 8-16: Prompt: Do you want to generate configuration files?

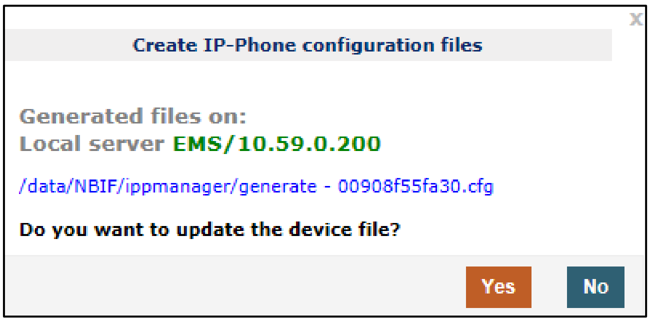


Do you want to generate John Smith IP-Phone configuration files?

Note: If IP-Phone files exist, they will be overridden.

7. Click **Yes**; the following prompt is displayed:

Figure 8-17: Prompt: Do you want to update the device file?



Create IP-Phone configuration files

Generated files on:
Local server EMS/10.59.0.200

/data/NBIF/ippmanager/generate - 00908f55fa30.cfg

Do you want to update the device file?

8. Click **Yes**.

8.7.4 Editing a User

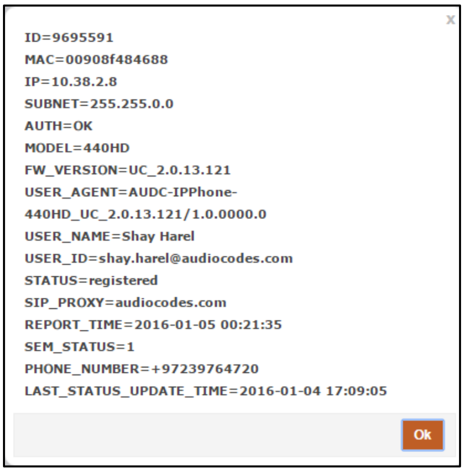
You can edit a user if, for example, they relocate to another region, or if they are given another phone.

➢ **To edit a user:**

1. Click the **Edit** button in the row adjacent to the user; the Edit User screen opens, identical to that shown in Figure 8-13.
2. Edit the same fields as when adding the device (see Section 0).

8.7.5 Viewing Device Status

You can quickly assess a device's status by clicking the icon under the Devices Status column; the following is displayed:



```
ID=9695591
MAC=00908f484688
IP=10.38.2.8
SUBNET=255.255.0.0
AUTH=OK
MODEL=440HD
FW_VERSION=UC_2.0.13.121
USER_AGENT=AUDC-IPPhone-
440HD_UC_2.0.13.121/1.0.0000.0
USER_NAME=Shay Harel
USER_ID=shay.harel@audiocodes.com
STATUS=registered
SIP_PROXY=audiocodes.com
REPORT_TIME=2016-01-05 00:21:35
SEM_STATUS=1
PHONE_NUMBER=+97239764720
LAST_STATUS_UPDATE_TIME=2016-01-04 17:09:05
```

8.7.6 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.

8.8 Managing Multiple Users

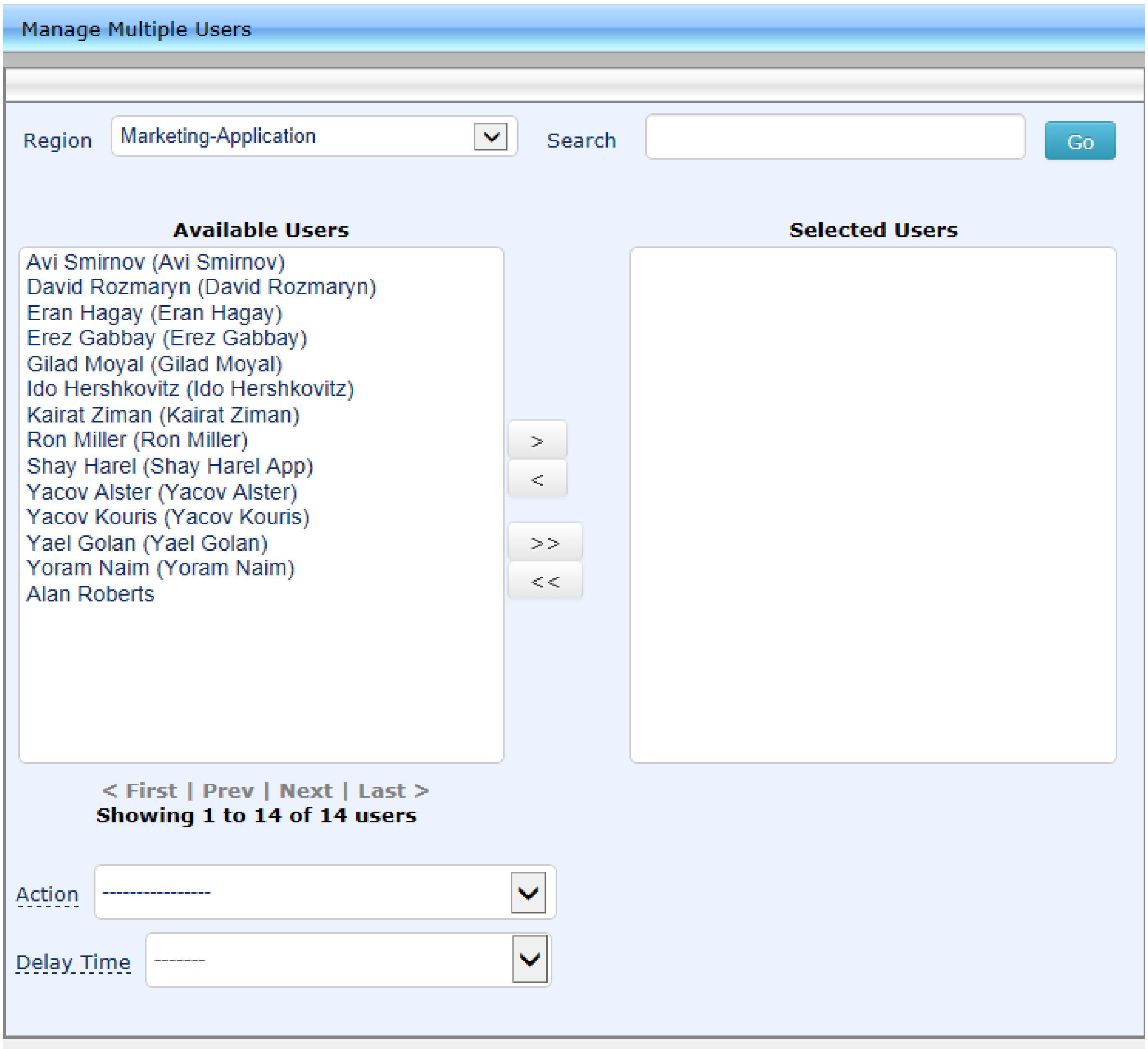
The Manage Multiple Users page lets you easily perform a single operation on all or on many users simultaneously:

- 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. Access the ‘Manage Multiple Users’ page (**Users** > **Manage Multiple Users**):

Figure 8-18: Manage Multiple Users



Manage Multiple Users

Region: Marketing-Application

Search:

Available Users:

Avi Smirnov (Avi Smirnov)
David Rozmaryn (David Rozmaryn)
Eran Hagay (Eran Hagay)
Erez Gabbay (Erez Gabbay)
Gilad Moyal (Gilad Moyal)
Ido Hershkovitz (Ido Hershkovitz)
Kairat Ziman (Kairat Ziman)
Ron Miller (Ron Miller)
Shay Harel (Shay Harel App)
Yacov Alster (Yacov Alster)
Yacov Kouris (Yacov Kouris)
Yael Golan (Yael Golan)
Yoram Naim (Yoram Naim)
Alan Roberts

Selected Users:

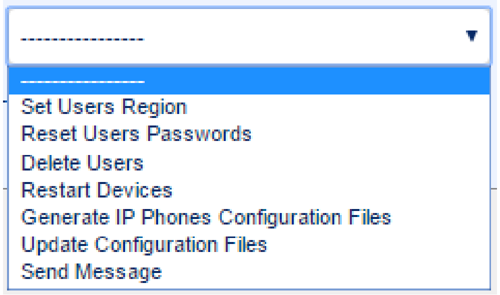
Showing 1 to 14 of 14 users

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

Delay Time: --------

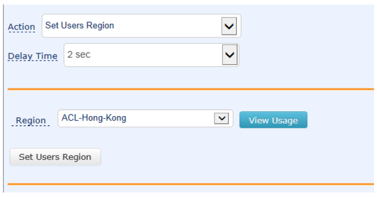
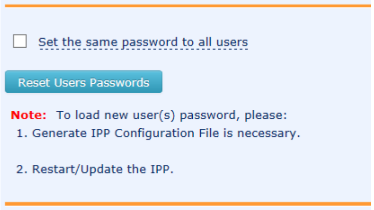
2. In the **Available Users** pane, select the users on which to perform the operation.
3. Click the right arrow (**>**) to add new users to the Selected Users pane. Click the left arrow (**<**) to remove selected users.

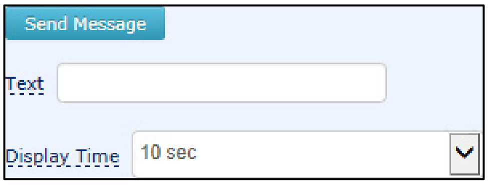
4. From the **Action** dropdown, select the required action.



Use the table below as reference.

Table 8-11: Managing Multiple Users - Actions

Action	Description
Set Users Region	 Action: Set Users Region Delay Time: 2 sec Region: ACL-Hong-Kong Sets the region for users selected.
Reset Users Passwords	 □ Set the same password to all users Note: To load new user(s) password, please: 1. Generate IPP Configuration File is necessary. 2. Restart/Update the IPP. Resets users passwords. A random password is generated for each user. To generate a single password for all users selected, select the **Set the same password to all users** option. To load the new user passwords: ▪ Generate the phone's configuration file ▪ Restart/Update the phone
Delete Users	Deletes users and applies a configurable 'Delay Time' (Default = 2 seconds) after each delete is performed.
Restart Devices	Restarts devices. A reset command is sent to all selected devices. The commands are sent in batches; each batch contains 5 devices with a delay of 2 minutes between each batch. From the dropdown, choose the type of restart: ▪ Graceful (default) ▪ Force ▪ Scheduled Before restarting, some models wait for the user to finish an active call while others may perform an immediate restart.
Generate 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 **Updating IP Phones after generating files** option. You can generate a private configuration file per user group, device group, or specific regions.
Update Configuration Files	Updates each phone after a configurable 'Delay Time' (default = 2 seconds).

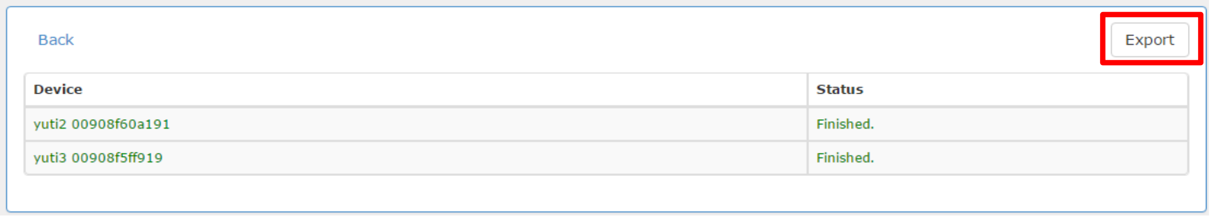
Action	Description
Send Message	Lets you send a message to the LCDs of all user phones selected. Enter the message in the 'Text' field. You can configure the length of time the message will be displayed in the LCD. Phones beep to alert users when messages come in.  Send Message Text Display Time: 10 sec

The page also lets you

- filter per region, before selecting the users on which to perform an action

5. Show results by clicking the **Export** link:

Figure 8-19: Export



Device	Status
yuti2 00908f60a191	Finished.
yuti3 00908f5ff919	Finished.

8.9 Maintaining Multiple Devices

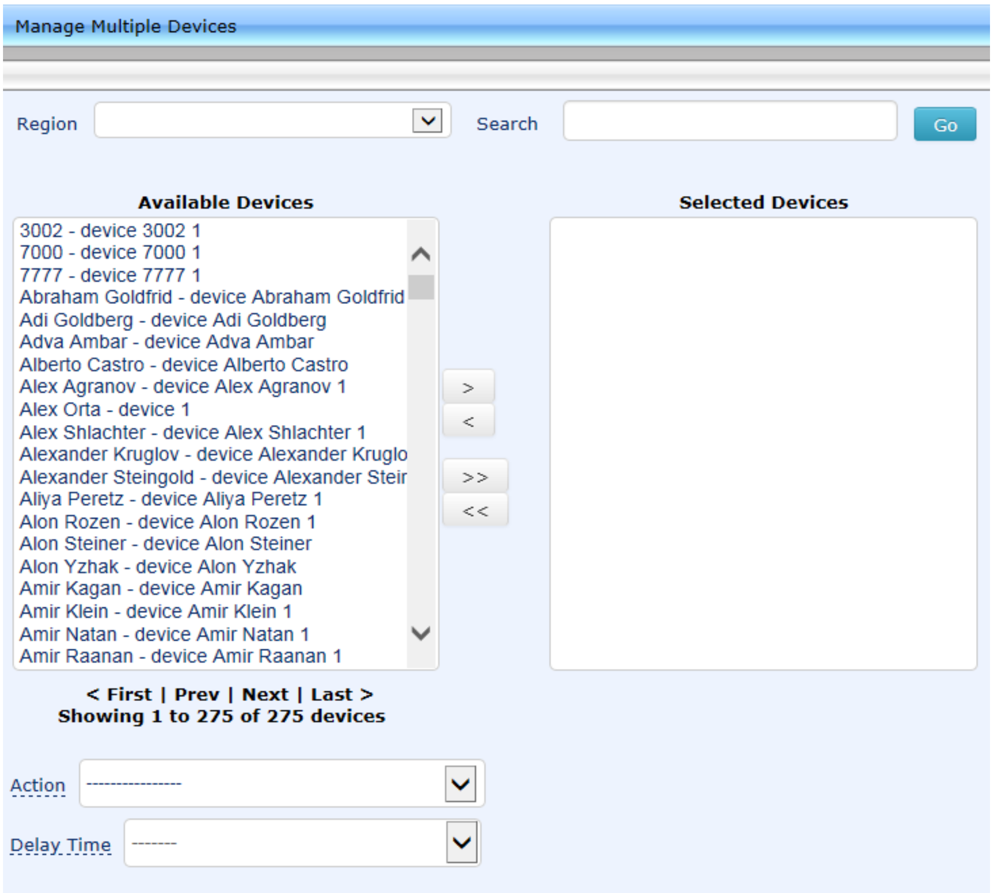
The Manage Multiple Devices page lets you perform a single operation on all or on many user devices. The page lets you

- 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. Access the 'Manage Multiple Devices' page (**Users** > **Manage Multiple Devices**):

Figure 8-20: Manage Multiple Devices



3002 - device 3002 1
7000 - device 7000 1
7777 - device 7777 1
Abraham Goldfrid - device Abraham Goldfrid
Adi Goldberg - device Adi Goldberg
Adva Ambar - device Adva Ambar
Alberto Castro - device Alberto Castro
Alex Agranov - device Alex Agranov 1
Alex Orta - device 1
Alex Shlachter - device Alex Shlachter 1
Alexander Kruglov - device Alexander Kruglo
Alexander Steingold - device Alexander Steir
Aliya Peretz - device Aliya Peretz 1
Alon Rozen - device Alon Rozen 1
Alon Steiner - device Alon Steiner
Alon Yzhak - device Alon Yzhak
Amir Kagan - device Amir Kagan
Amir Klein - device Amir Klein 1
Amir Natan - device Amir Natan 1
Amir Raanan - device Amir Raanan 1

Showing 1 to 275 of 275 devices

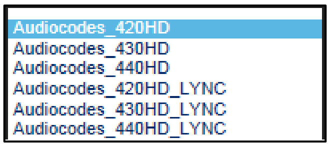
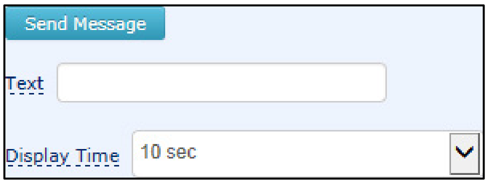
Action: ----------------

Delay Time: --------

The devices are displayed in the following format:

1. You can search for devices by entering a string in the 'Search' field and then clicking **Go**.
2. You can filter the devices per region, before selecting those on which to perform an action.
3. In the Available Devices pane, select the devices on which to perform the action.
4. Click the right arrow → to add new devices to the Selected Devices pane, or use the left arrow ← to remove selected devices.
5. From the **Action** dropdown, select an action. Use the table below as reference.

Table 8-12: 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 IP Phone Type	You can change the phone model:  Audiocodes_420HD Audiocodes_430HD Audiocodes_440HD Audiocodes_420HD_LYNC Audiocodes_430HD_LYNC Audiocodes_440HD_LYNC To view the usage of a model, click **View Usage**. To load a new phone model: 1 Generate the phone's configuration file. 2 Restart/update the phone.
Change Language	Changes the phone language. Select the language from the **Language** dropdown and click **Change**. To view the usage of a language, click **View Usage**. To load a new language: 1 Generate the phone's configuration file. 2 Restart/update the phone.
Restart Devices	Restarts online devices. Before restarting, some models wait for the user to finish an active call while others may perform an immediate restart. From the dropdown, choose the type of restart: - Graceful (default) - Force - Scheduled
Generate 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 **Updating IP Phones after generating files** option.
Update Configuration Files	Updates each phone after a configurable 'Delay Time' (default = 2 seconds).
Send Message	Lets you send a message to the LCDs 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 LCD. Phones beep to alert users when messages come in.  Send Message Text Display Time 10 sec
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. See under Appendix B.1 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.

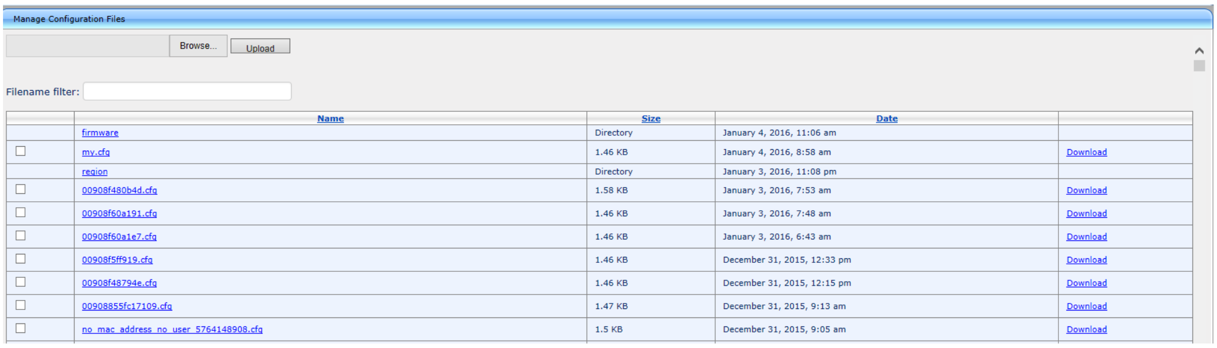
8.10 Managing Configuration Files

You can manage IP phones configuration files. All cfg files are created and located on the EMS 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:**

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

Figure 8-21: Manage Configuration Files



Filename filter:

	Name	Size	Date	
	firmware	Directory	January 4, 2016, 11:06 am	
□	my.cfg	1.46 KB	January 4, 2016, 8:58 am	Download
	region	Directory	January 3, 2016, 11:08 pm	
□	00908f480b4d.cfg	1.58 KB	January 3, 2016, 7:53 am	Download
□	00908f60a191.cfg	1.46 KB	January 3, 2016, 7:48 am	Download
□	00908f60a1e7.cfg	1.46 KB	January 3, 2016, 6:43 am	Download
□	00908f5ff919.cfg	1.46 KB	December 31, 2015, 12:33 pm	Download
□	00908f48794e.cfg	1.46 KB	December 31, 2015, 12:15 pm	Download
□	00908855fc17109.cfg	1.47 KB	December 31, 2015, 9:13 am	Download
□	no_mac_address_no_user_5764148908.cfg	1.5 KB	December 31, 2015, 9:05 am	Download

The page lets you

- Filter by filename the .cfg configuration files listed
- 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)

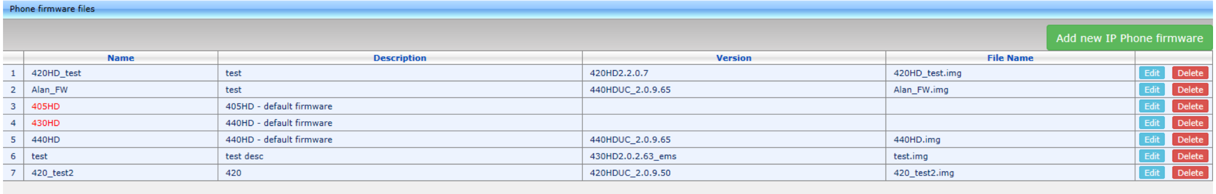
8.11 Managing Firmware Files

You can manage the phones' .img firmware files.

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

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

Figure 8-22: Phone Firmware Files



Phone firmware files

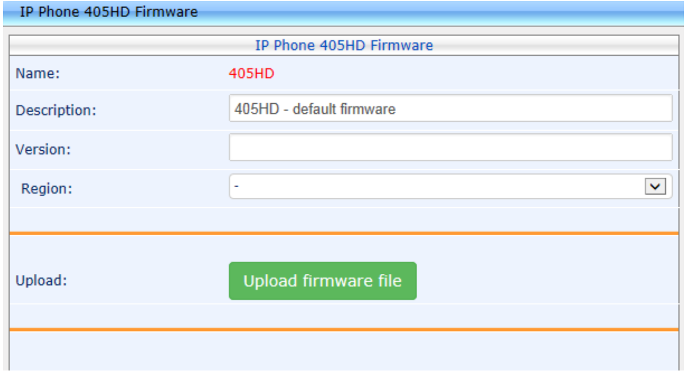
	Name	Description	Version	File Name	
1	420HD_test	test	420HD2.2.0.7	420HD_test.img	Edit Delete
2	Alan_FW	test	440HDUC_2.0.9.65	Alan_FW.img	Edit Delete
3	405HD	405HD - default firmware			Edit Delete
4	430HD	440HD - default firmware			Edit Delete
5	440HD	440HD - default firmware	440HDUC_2.0.9.65	440HD.img	Edit Delete
6	test	test desc	430HD2.0.2.63_ems	test.img	Edit Delete
7	420_test2	420	420HDUC_2.0.9.50	420_test2.img	Edit Delete

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.
- 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 has. If it doesn't have, you must upload the phone's .img firmware file that you obtained from AudioCodes, to the EMS Provisioning Server:

  a. Click the **red**-coded name of the phone; this screen opens:

  Figure 8-23: .img Firmware File Upload

  IP Phone 405HD Firmware

  IP Phone 405HD Firmware

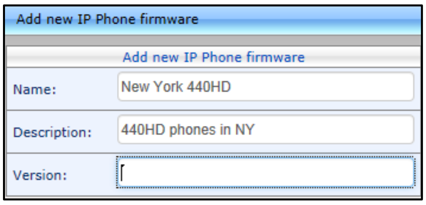
Name:	405HD
Description:	405HD - default firmware
Version:	
Region:	-
Upload:	Upload firmware file

  b. Click the **Upload firmware** button, and then navigate to the .img file you received from AudioCodes and put on the EMS 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** 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.



Add new IP Phone firmware

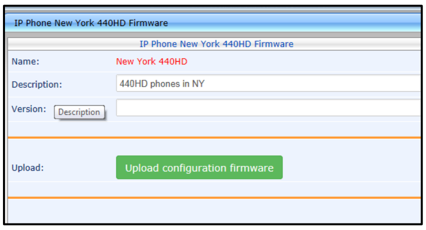
Add new IP Phone firmware

Name: New York 440HD

Description: 440HD phones in NY

Version:

b. Define an intuitive 'Name' and 'Description' to facilitate easy identification. You can leave the 'Version' field empty, and then click the **Submit** button; this screen is displayed:



IP Phone New York 440HD Firmware

IP Phone New York 440HD Firmware

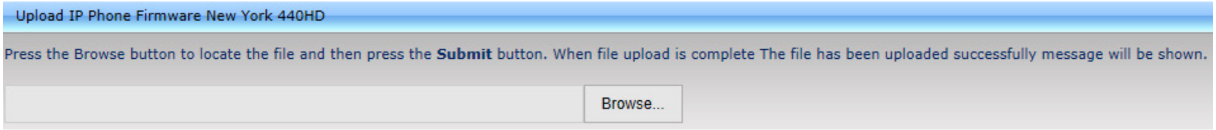
Name: New York 440HD

Description: 440HD phones in NY

Version:

Upload:

c. Click **Upload firmware**; this screen is displayed:



Upload IP Phone Firmware New York 440HD

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

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

9 Viewing Your License

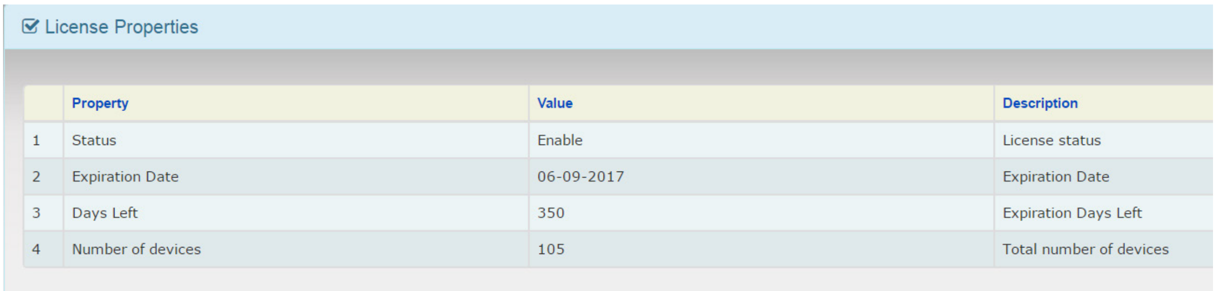
Use of EMS server platform processes is managed by a license that controls the time period validity for the use of the platform.

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 (**License** > **System License**).

Figure 9-1: License Properties



☑ License Properties

	Property	Value	Description
1	Status	Enable	License status
2	Expiration Date	06-09-2017	Expiration Date
3	Days Left	350	Expiration Days Left
4	Number of devices	105	Total number of devices

2. Use the table below as reference.

Table 9-1: License Properties

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

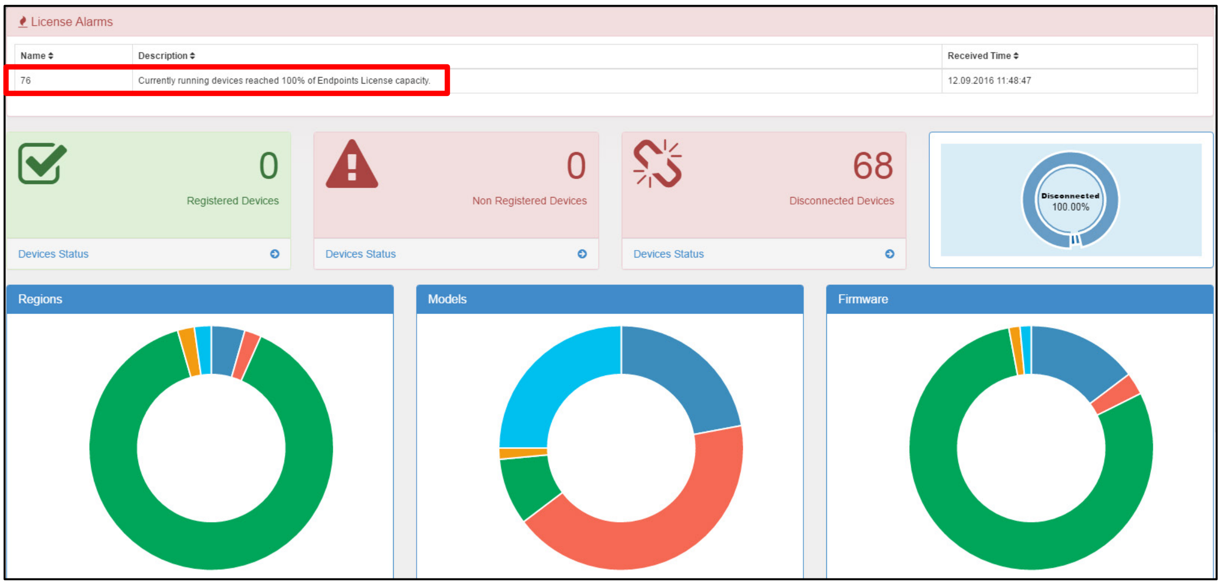
Note: If a license expires, communications with all servers will be suspended; users will not be able to log in; and it will not be possible to add new phones.

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

Note:

- 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 (see Section 8.3.4 for more information)
  - √ A Critical alarm is sent when 100% of the period defined in the currently running device's license is consumed (see also Section 8.3.4 for more information)
- When the maximum number of devices reporting to the EMS is exceeded, the EMS server blocks them and sends an alert that is displayed in the Home page, shown in Figure 9-2 on the next page.

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



License Alarms

Name	Description	Received Time
76	Currently running devices reached 100% of Endpoints License capacity.	12.09.2016 11:48:47

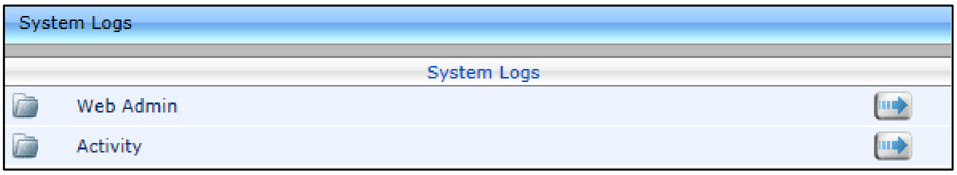
10 Troubleshooting

You can display log files to help troubleshoot problems and determine cause.

➢ **To display log files:**

1. Access the System Logs page (**System Diagnostics** > **System Logs**):

Figure 10-1: System Logs



2. Click the **Web Admin** arrow or the **Activity** arrow link.

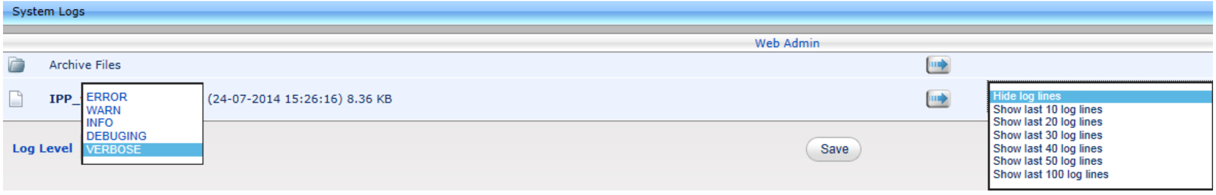
Note:

- The Web Admin log displays recent actions performed in the user interface
- The Activity log displays recent activities performed with the EMS server

➢ **To display Web Admin log files:**

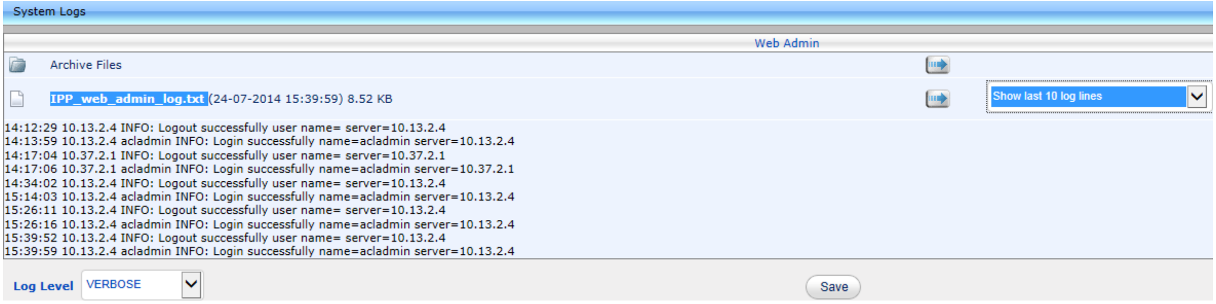
1. Click the **Web Admin** arrow link; the System Logs – Web Admin page opens:

Figure 10-2: System Logs – Web Admin Level Log



2. From the 'Log Level' dropdown select
   - ERROR
   - WARN
   - INFO
   - DEBUGGING
   - VERBOSE (default) – All Levels (Detailed)
3. From the 'Hide log lines' dropdown select
   - Hide log lines
   - Show last 10 log lines
   - Show last 20 log lines
   - Show last 30 log lines
   - Show last 40 log lines
   - Show last 50 log lines
   - Show last 100 log lines
4. View the generated IPP_web_admin_log.txt file.

Figure 10-3: System Logs – Web Admin Level txt Log File Displayed



```
14:12:29 10.13.2.4 INFO: Logout successfully user name= server=10.13.2.4
14:13:59 10.13.2.4 acladmin INFO: Login successfully name=acladmin server=10.13.2.4
14:17:04 10.37.2.1 INFO: Logout successfully user name= server=10.37.2.1
14:17:06 10.37.2.1 acladmin INFO: Login successfully name=acladmin server=10.37.2.1
14:34:02 10.13.2.4 INFO: Logout successfully user name= server=10.13.2.4
15:14:03 10.13.2.4 acladmin INFO: Login successfully name=acladmin server=10.13.2.4
15:26:11 10.13.2.4 INFO: Logout successfully user name= server=10.13.2.4
15:26:16 10.13.2.4 acladmin INFO: Login successfully name=acladmin server=10.13.2.4
15:39:52 10.13.2.4 INFO: Logout successfully user name= server=10.13.2.4
15:39:59 10.13.2.4 acladmin INFO: Login successfully name=acladmin server=10.13.2.4
```

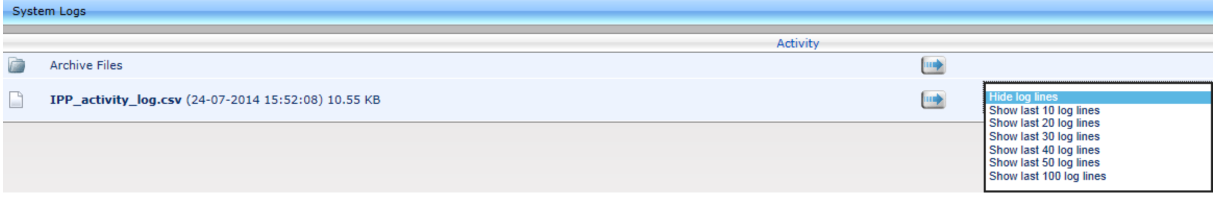
Log Level: VERBOSE

5. Click **Save** to save the file and share it with others.

➢ To display Activity log files:

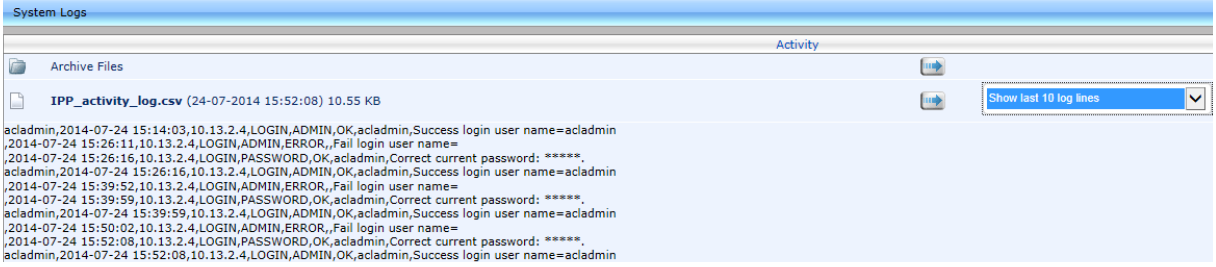
1. Click the **Activity** arrow; the System Logs – Activity page opens:

Figure 10-4: System Logs – Activity Log



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

Figure 10-5: System Logs – Activity Level txt Log File Displayed



```
acladmin,2014-07-24 15:14:03,10.13.2.4,LOGIN,ADMIN,OK,acladmin,Success login user name=acladmin
,2014-07-24 15:26:11,10.13.2.4,LOGIN,ADMIN,ERROR,,Fail login user name=
,2014-07-24 15:26:16,10.13.2.4,LOGIN,PASSWORD,OK,acladmin,Correct current password: *****.
acladmin,2014-07-24 15:26:16,10.13.2.4,LOGIN,ADMIN,OK,acladmin,Success login user name=acladmin
,2014-07-24 15:39:52,10.13.2.4,LOGIN,ADMIN,ERROR,,Fail login user name=
,2014-07-24 15:39:59,10.13.2.4,LOGIN,PASSWORD,OK,acladmin,Correct current password: *****.
acladmin,2014-07-24 15:39:59,10.13.2.4,LOGIN,ADMIN,OK,acladmin,Success login user name=acladmin
,2014-07-24 15:50:02,10.13.2.4,LOGIN,ADMIN,ERROR,,Fail login user name=
,2014-07-24 15:52:08,10.13.2.4,LOGIN,PASSWORD,OK,acladmin,Correct current password: *****.
acladmin,2014-07-24 15:52:08,10.13.2.4,LOGIN,ADMIN,OK,acladmin,Success login user name=acladmin
```

A Importing Users into the IP Phone Management Server

Note: Applies to non-Lync environments.

You can import up to 10000 users or phones, defined in a CSV file, into the IP Phone Management Server. Before you import the CSV file into the server, you need to make it.

A.1 Making a CSV File

This section shows how to make a CSV file. To make the CSV file:

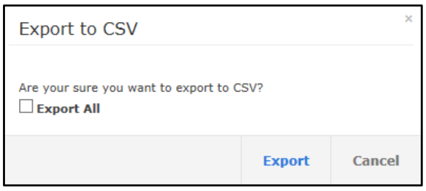
1. Configure a 'system user' (it can be any other user as well) (see Section 3)
2. Add a device to this user ('system user' or any other user)
3. Export the 'system user' to a CSV file (see Section A.1.1 below)
4. Define in Excel the other users in the enterprise (see Section A.1.2)
5. Import the new CSV into the server.

A.1.1 Export the 'System User' to a CSV File

This section shows how to export the 'system user' to a CSV file. You can export from either the Devices Status page or from the Import Users & Devices page.

➢ **To export the 'system user' to a CSV file from the Devices Status page:**

1. Access the Devices Status page (see Figure 8-4).
2. Select the 'system user', and then click the **Export** link in the top right corner:



Export to CSV

Are your sure you want to export to CSV?

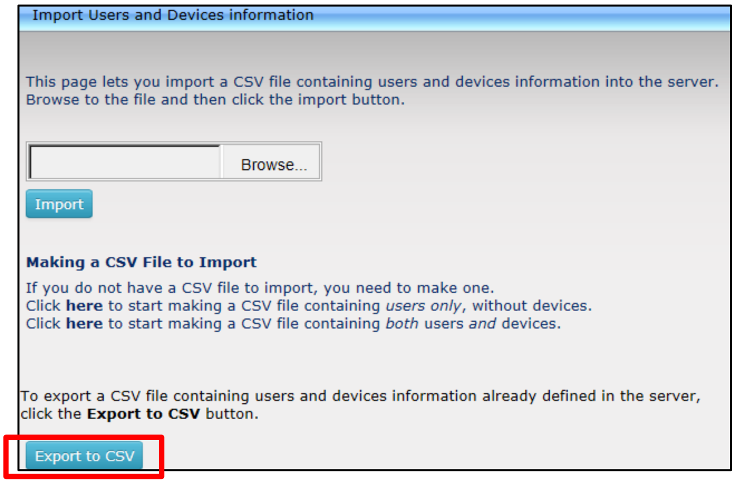
□ Export All

3. Click the **Export** button

➢ **To export the 'system user' to a CSV file from the Import Users & Devices page:**

1. Access the Import Users and Devices page (**Users** > **Import Users & Devices**):

Figure A-1: Import Users – Export to CSV



Import Users and Devices information

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

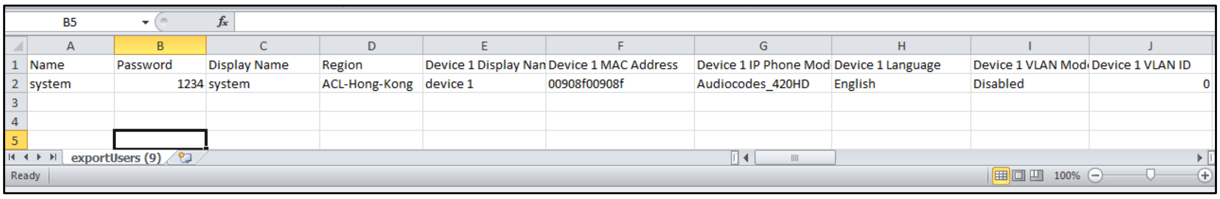
Making a CSV File to Import

If you do not have a CSV file to import, you need to make one.
Click **here** to start making a CSV file containing *users only*, without devices.
Click **here** to start making a CSV file containing *both* users *and* devices.

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

2. Click the **Export to CSV** button shown in Figure A-1, and then open the CSV in Excel; the 'system user' you configured previously is displayed:

Figure A-2: CSV File in Excel



	A	B	C	D	E	F	G	H	I	J
1	Name	Password	Display Name	Region	Device 1 Display Nan	Device 1 MAC Address	Device 1 IP Phone Mod	Device 1 Language	Device 1 VLAN Mod	Device 1 VLAN ID
2	system	1234	system	ACL-Hong-Kong	device 1	00908f00908f	Audiocodes_420HD	English	Disabled	0
3										
4										
5										

Table A-1: CSV File

Name	Password	Display Name	Region	Device 1 Display Name	Device 1 MAC Address	Device 1 IP Phone Model
system	system	system	ACL-Hong Kong			

A.1.2 Defining Users in the CSV File

You need to define users in the CSV file.

> **Tip:** 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.

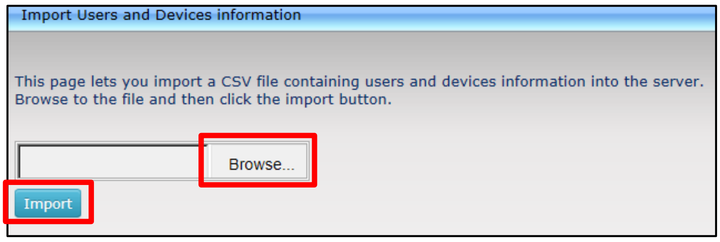
A.2 Importing the New CSV File into the Server

After making the CSV file, import the new CSV file into the IP Phone Management Server.

➢ To import the new CSV file into the IP Phone Management Server:

1. Access the Import Users page (**Users** > **Import Users & Devices**).

Figure A-3: Import Users



Import Users and Devices information

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

2. Click the **Browse** button and then navigate to and select the CSV file which you created and saved on your Desktop previously.
3. Click the **Import** button; the file is imported into the IP Phone Management Server.
4. Click the **Home** icon; verify that all enterprise users that you imported are displayed.
5. Plug in the phones; the cfg configuration file is automatically uploaded to the phones from the EMS provisioning server, which the DHCP server points them to.

This page is intentionally left blank.

B Approving Users

Note: 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 Zero Touch provisioning method or importing a CSV file, then after plugging the phones into the network you need to approve the users.

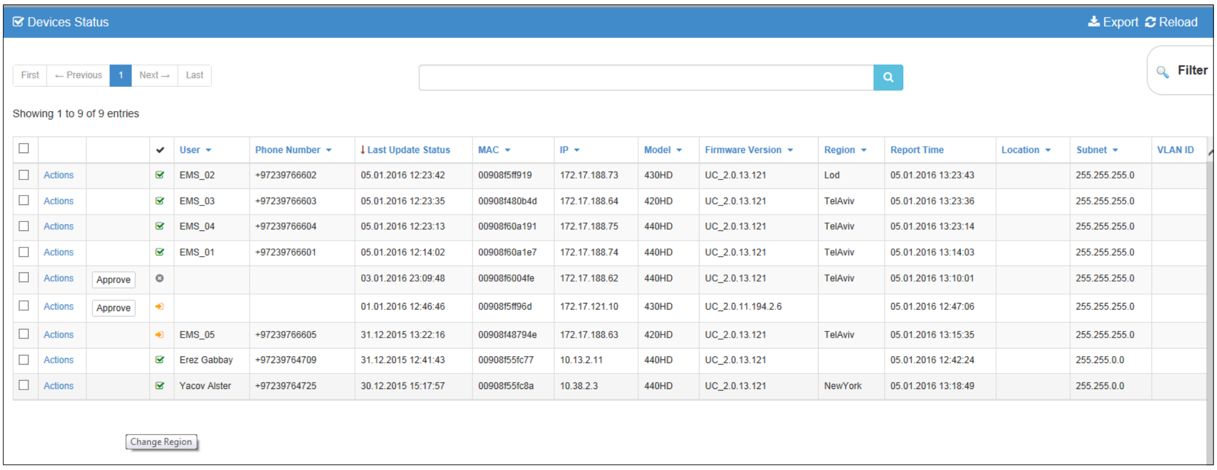
B.1 Lync Environment

After plugging the phones in, they report to the Management Server 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 Lync environment:

1. In the IP Phone Management Server UI, open the Devices Status page (**Dashboard** > **Devices Status**).

Figure B-1: Devices Status



Showing 1 to 9 of 9 entries

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

Screen functions:

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

Actions: Check status, Change Region, 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 EMS will then not know the region in which the device is located. If the Region URL is configured for the DHCP Option, the **Approve** button will not be displayed. See also Section 6.1.

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

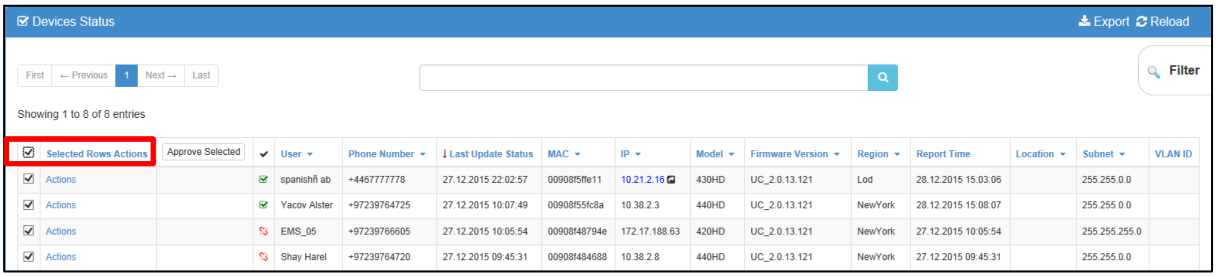
Other columns: User, Phone Number, MAC, IP, Model, Firmware Version, Report Time, Location, Subnet, VLAN ID

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.

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



☑ Devices Status

Export | Reload

First | ← Previous | 1 | Next → | Last

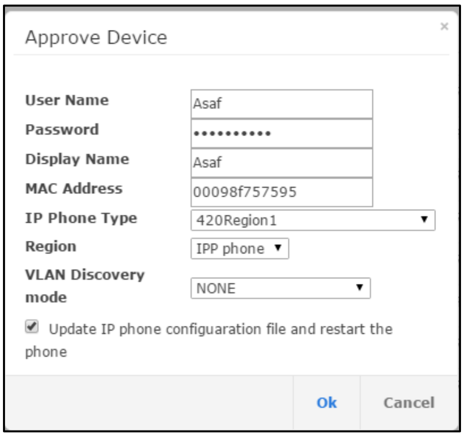
Filter

Showing 1 to 8 of 8 entries

☑	Selected Rows Actions	Approve Selected	✓	User	Phone Number	Last Update Status	MAC	IP	Model	Firmware Version	Region	Report Time	Location	Subnet	VLAN ID
☑	Actions		✓	spanishñ ab	+4467777778	27.12.2015 22:02:57	00908f5ffe11	10.21.2.16	430HD	UC_2.0.13.121	Lod	28.12.2015 15:03:06		255.255.0.0	
☑	Actions		✓	Yacov Alster	+97239764725	27.12.2015 10:07:49	00908f55fc8a	10.38.2.3	440HD	UC_2.0.13.121	NewYork	28.12.2015 15:08:07		255.255.0.0	
☑	Actions		✗	EMS_05	+97239766605	27.12.2015 10:05:54	00908f48794e	172.17.188.63	420HD	UC_2.0.13.121	NewYork	27.12.2015 10:05:54		255.255.255.0	
☑	Actions		✗	Shay Harel	+97239764720	27.12.2015 09:45:31	00908f484688	10.38.2.8	440HD	UC_2.0.13.121	NewYork	27.12.2015 09:45:31		255.255.0.0	

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

Figure B-3: Approve Device



Approve Device

User Name: Asaf

Password: ••••••••••

Display Name: Asaf

MAC Address: 00098f757595

IP Phone Type: 420Region1

Region: IPP phone

VLAN Discovery mode: NONE

☑ Update IP phone configuaration file and restart the phone

4. In the prompt, select the region and then click **Approve**; all selected users are approved; all phones restart; the cfg file is automatically uploaded to the phones from the EMS 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].

B.2 Non-Lync Environments

After plugging phones in, they report to the Management Server, which does not display user names in the UI.

Note:

- Before plugging in the phones, it's recommended to import a CSV file with users and devices. Best practice is to create one or more users with devices, export them to a CSV file, add users and devices to the CSV file in the same format, and then import the file (see Appendix A).
- 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.

➢ **To approve users in non-Lync environments:**

1. In the IP Phone Management Server UI, open the Devices Status page (**Dashboard** > **Devices Status**), as shown in Figure 8-4; the non Lync screen is identical to the Lync screen.
2. Click the **Approve** button adjacent to the user; the Approve Device dialog opens – the non Lync screen is identical to the Lync screen.
3. Enter the User Name and the Display Name, and then click **OK**.; the user name is displayed in the Management Server UI and the user is approved.

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

Note:

- 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 EMS provisioning server, which the DHCP server points them to.
- In some non-Lync environments, for example, in Genesys contact centers, Password is not specified.

This page is intentionally left blank.

C Managing Templates

This appendix shows how to manage templates.

C.1 Selecting a Template

Templates are available

- per region
- per phone model
- per model for Microsoft Lync server phones
- per model for regular (non-Lync) third-party server phones

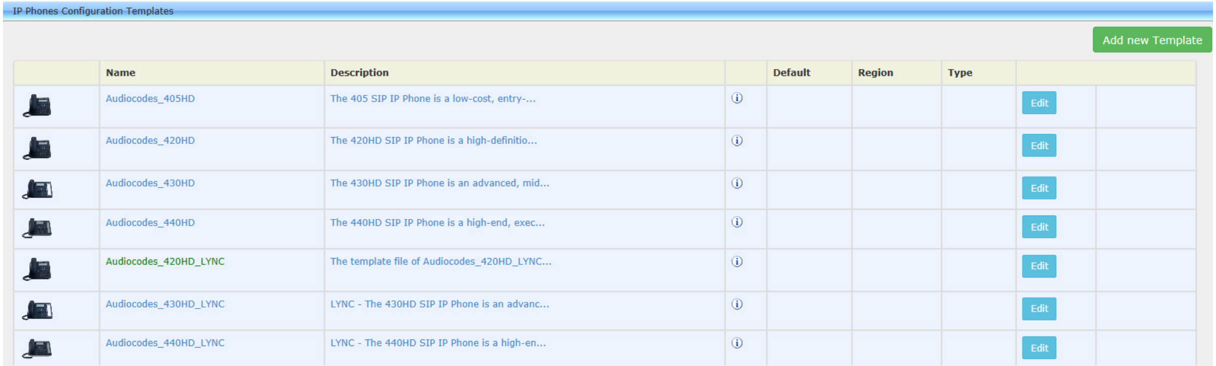
Depending on the region, model and the server in the enterprise, select a template for:

- AudioCodes 405
- AudioCodes 420HD
- AudioCodes 430HD
- AudioCodes 440HD
- AudioCodes 450HD
- AudioCodes 420HD Lync
- AudioCodes 430HD Lync
- AudioCodes 440HD Lync
- AudioCodes 450HD Lync

➢ To select a template:

- In the navigation tree, access the IP Phones Configuration Templates page (**Phones Configuration** > **Templates**):

Figure C-1: IP Phone Models Configuration Templates



IP Phones Configuration Templates

Add new Template

	Name	Description		Default	Region	Type		
☎	Audiocodes_405HD	The 405 SIP IP Phone is a low-cost, entry-...	ⓘ				Edit	
☎	Audiocodes_420HD	The 420HD SIP IP Phone is a high-definitio...	ⓘ				Edit	
☎	Audiocodes_430HD	The 430HD SIP IP Phone is an advanced, mid...	ⓘ				Edit	
☎	Audiocodes_440HD	The 440HD SIP IP Phone is a high-end, exec...	ⓘ				Edit	
☎	Audiocodes_420HD_LYNC	The template file of Audiocodes_420HD_LYNC...	ⓘ				Edit	
☎	Audiocodes_430HD_LYNC	LYNC - The 430HD SIP IP Phone is an advanc...	ⓘ				Edit	
☎	Audiocodes_440HD_LYNC	LYNC - The 440HD SIP IP Phone is a high-en...	ⓘ				Edit	

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

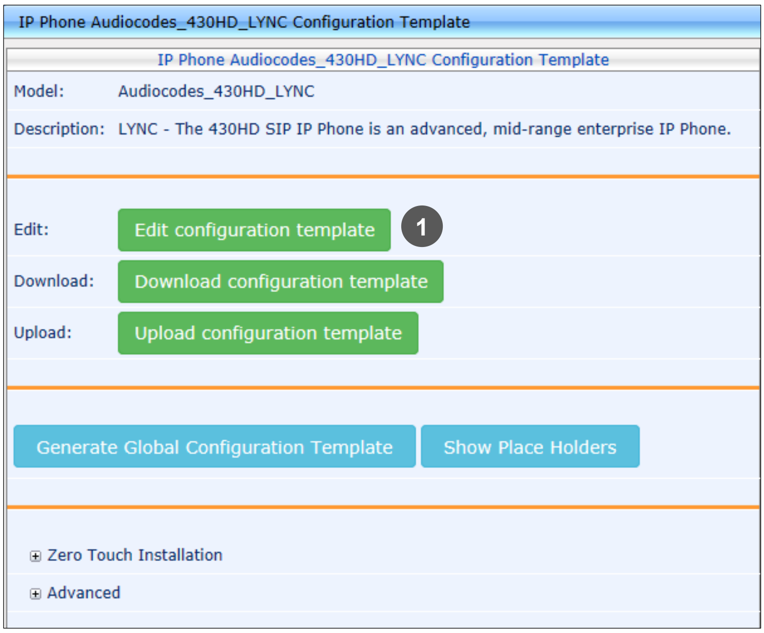
C.2 Editing a Configuration Template

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; this dialog is displayed:

Figure C-2: IP Phone Configuration Template



IP Phone Audiocodes_430HD_LYNC Configuration Template

IP Phone Audiocodes_430HD_LYNC Configuration Template

Model: Audiocodes_430HD_LYNC

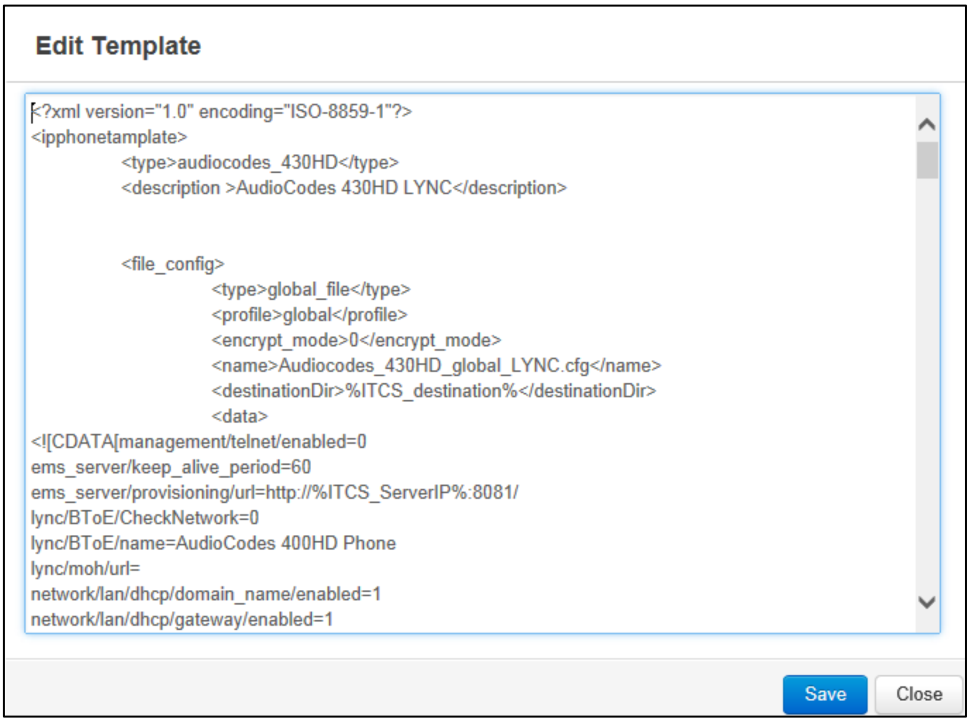
Description: LYNC - The 430HD SIP IP Phone is an advanced, mid-range enterprise IP Phone.

Edit: Edit configuration template
1
Download: Download configuration template
Upload: Upload configuration template
Generate Global Configuration Template
Show Place Holders
⊞ Zero Touch Installation
⊞ Advanced

1 = generic templates can be edited and generated per phone model

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

Figure C-3: Edit Template



Edit Template

```
<?xml version="1.0" encoding="ISO-8859-1"?>
<ipphonetamplate>
            <type>audiocodes_430HD</type>
            <description >AudioCodes 430HD LYNC</description>


            <file_config>
                        <type>global_file</type>
                        <profile>global</profile>
                        <encrypt_mode>0</encrypt_mode>
                        <name>Audiocodes_430HD_global_LYNC.cfg</name>
                        <destinationDir>%ITCS_destination%</destinationDir>
                        <data>
<![CDATA[management/telnet/enabled=0
ems_server/keep_alive_period=60
ems_server/provisioning/url=http://%ITCS_ServerIP%:8081/
lync/BToE/CheckNetwork=0
lync/BToE/name=AudioCodes 400HD Phone
lync/moh/url=
network/lan/dhcp/domain_name/enabled=1
network/lan/dhcp/gateway/enabled=1
```

Edit the template and then click **Save**; the modified template is saved in its URL location on the server, for example, **http://10.59.0.200/ipp/admin/AudioCodes.php**. 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. See also Section C.3.7.

C.3 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

C.3.1 Global Parameters

Global parameters apply to *all* phones in the enterprise network. The **ems_server/provisioning/url** parameter, for example, is a global parameter because all phones in the enterprise network point to the same provisioning server.

Only one file is generated for each template, so every change in the global file will automatically impact all the phones from this template.

C.3.2 User-Specific Parameters

Private user parameters apply to specific phones. They can pull global parameters using the template's ‘include’ function. The **network/lan/vlan/mode=%ITCS_VLANMode%** parameter, for example, is a user parameter because each user in an enterprise is defined in a user-specific VLAN. These parameters are stored in each device's MAC.cfg file.

C.3.3 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 phone model and its description are displayed.

C.3.4 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.

C.3.5 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.

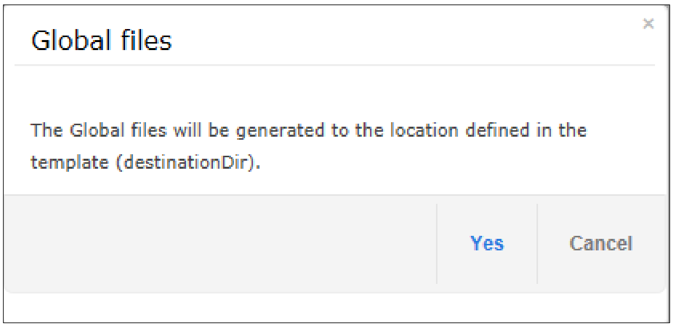
C.3.6 Generating an Edited Template

After editing a template, you must generate the edited template.

➢ To generate an edited template:

1. In the IP Phone Configuration Template page, click the edited template or click its **Edit** button, and then in the Configuration Template screen, click the **Generate Global Configuration Template** button; this prompt is displayed:

Figure C-4: Generate Global Configuration Template – 'Global files' Prompt



Global files

The Global files will be generated to the location defined in the template (destinationDir).

2. Click **Yes**; the generated template reflecting the edit/s is available in the IP Phone Models Configuration Templates page.

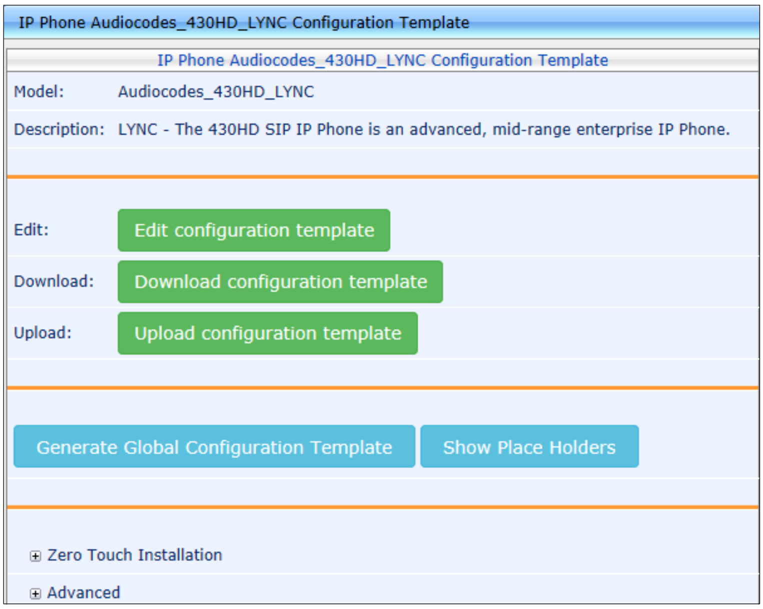
C.3.7 Defining Template Placeholders

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 region, 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 Templates page (**Phones Configuration** > **Templates**), click the **Edit** button adjacent to the phone model; this screen opens:

Figure C-5: Configuration Template



IP Phone Audiocodes_430HD_LYNC Configuration Template

IP Phone Audiocodes_430HD_LYNC Configuration Template

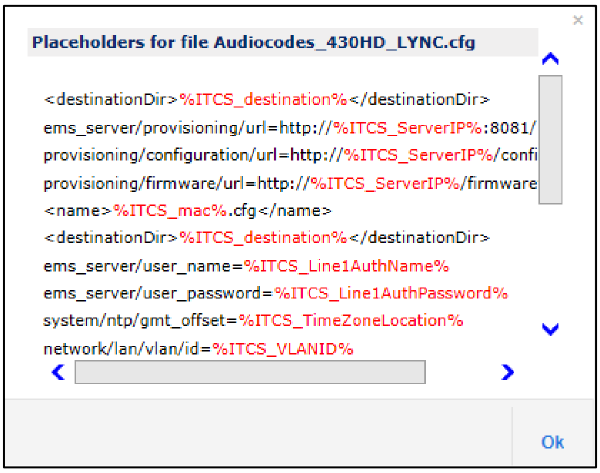
Model: Audiocodes_430HD_LYNC

Description: LYNC - The 430HD SIP IP Phone is an advanced, mid-range enterprise IP Phone.

Edit:
Edit configuration template
Download:
Download configuration template
Upload:
Upload configuration template
Generate Global Configuration Template
Show Place Holders
⊞ Zero Touch Installation
⊞ Advanced

2. Click **Advanced**, and then click the **Show Placeholders** button.

Figure C-6: Show Placeholders



```
<destinationDir>%ITCS_destination%</destinationDir>
ems_server/provisioning/url=http://%ITCS_ServerIP%:8081/
provisioning/configuration/url=http://%ITCS_ServerIP%/confi
provisioning/firmware/url=http://%ITCS_ServerIP%/firmware
<name>%ITCS_mac%.cfg</name>
<destinationDir>%ITCS_destination%</destinationDir>
ems_server/user_name=%ITCS_Line1AuthName%
ems_server/user_password=%ITCS_Line1AuthPassword%
system/ntp/gmt_offset=%ITCS_TimeZoneLocation%
network/lan/vlan/id=%ITCS_VLANID%
```

The figure above shows placeholders currently defined in the xml Configuration Template file for the 430HD Lync phone model.

There are four kinds of placeholders: (1) System (2) Phone Model (3) Region (4) Devices.

- To manage an available placeholder, see Section C.3.7.1
- To add/edit/delete a phone model placeholder, see Section C.3.7.2
- To add/edit/delete a region placeholder, see Section C.3.7.3
- To add/edit/delete a device placeholder, see Section C.3.7.4

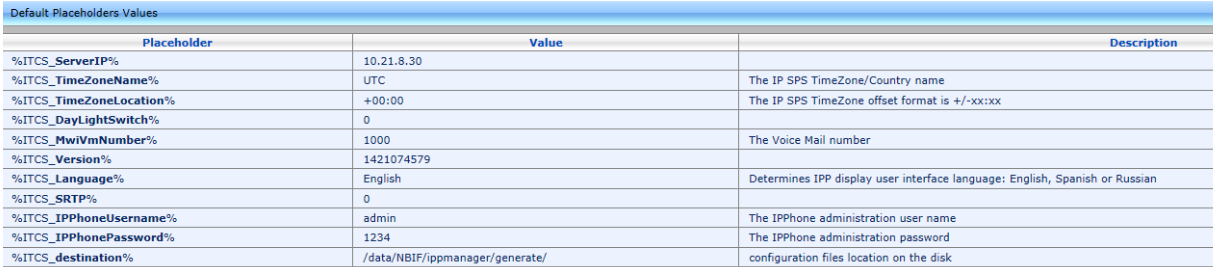
C.3.7.1 Default Placeholders Values

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

➢ To view default placeholders values defined:

- Access the Default Placeholders Values page (**Phones Configuration** > **Default Placeholders Values**):

Figure C-7: Default Placeholders Values



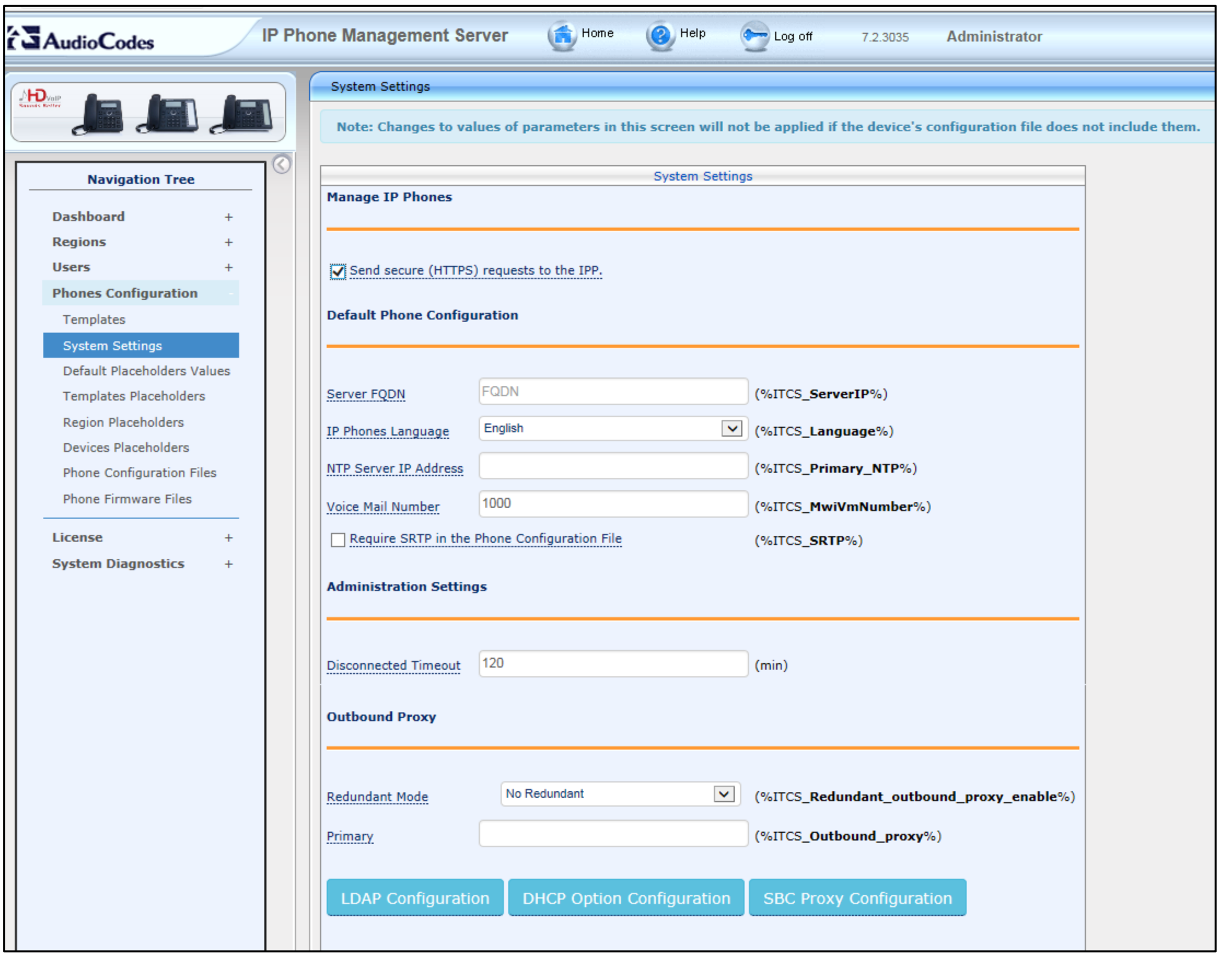
Default Placeholders Values

Placeholder	Value	Description
%ITCS_**ServerIP**%	10.21.8.30	
%ITCS_**TimeZoneName**%	UTC	The IP SPS TimeZone/Country name
%ITCS_**TimeZoneLocation**%	+00:00	The IP SPS TimeZone offset format is +/-xx:xx
%ITCS_**DayLightSwitch**%	0	
%ITCS_**MwiVmNumber**%	1000	The Voice Mail number
%ITCS_**Version**%	1421074579	
%ITCS_**Language**%	English	Determines IPP display user interface language: English, Spanish or Russian
%ITCS_**SRTP**%	0	
%ITCS_**IPPhoneUsername**%	admin	The IPPhone administration user name
%ITCS_**IPPhonePassword**%	1234	The IPPhone administration password
%ITCS_**destination**%	/data/NBIF/ippmanager/generate/	configuration files location on the disk

To define a placeholder value:

1. Access the System Settings page (**Phones Configuration** > **System Settings**).

Figure C-8: System Settings



AudioCodes IP Phone Management Server Home Help Log off 7.2.3035 Administrator

System Settings

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

Navigation Tree
- Dashboard +
- Regions +
- Users +
- Phones Configuration
  - Templates
  - System Settings
  - Default Placeholders Values
  - Templates Placeholders
  - Region Placeholders
  - Devices Placeholders
  - Phone Configuration Files
  - Phone Firmware Files
- License +
- System Diagnostics +

System Settings

Manage IP Phones

☑ Send secure (HTTPS) requests to the IPP.

Default Phone Configuration

Server FQDN	FQDN	(%ITCS_ServerIP%)
IP Phones Language	English	(%ITCS_Language%)
NTP Server IP Address		(%ITCS_Primary_NTP%)
Voice Mail Number	1000	(%ITCS_MwiVmNumber%)
☐ Require SRTP in the Phone Configuration File		(%ITCS_SRTP%)

Administration Settings

Disconnected Timeout	120	(min)

Outbound Proxy

Redundant Mode	No Redundant	(%ITCS_Redundant_outbound_proxy_enable%)
Primary		(%ITCS_Outbound_proxy%)

Note: With the exception of the parameters 'IP Phones Language' and the 'Server FQDN', the screen above only applies to enterprises whose environments are *non Lync*.

2. Define values for available placeholders according to your enterprise IP phone configuration requirements, and then click the **Submit** button. Use the table below as reference. Except for the 'IP Phones Language' parameter, all parameters are only applicable to enterprises whose environments are *non Lync*.

Table C-1: System Settings

Parameter	Description
Send secured (HTTPS) requests to the IP phone	If the option is selected, communications and REST updates such as alarms, alerts and statuses between server and phone will be carried out over HTTPS. Used when there is an SBC proxy. See also Section 1.4).
Server FQDN	[Recommended] Points phones to the EMS server using the server's *name* rather than its IP address. If phones are pointed to the EMS 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.

Parameter	Description
IP Phones Language	From the dropdown select the language you want displayed in the phones' LCD screens: **English** (default), **French**, **German**, **Hebrew**, **Italian**, **Polish**, **Portuguese**, **Russian**, **Spanish** or **Ukraine**.
NTP Server IP Address	Enter the IP address of the Network Time Protocol (NTP) server from which the phones can get the time.
Voice Mail Number	Enter the number of the enterprise's exchange. Configuration depends on the enterprise environment, specifically, on which exchange the enterprise has. If the enterprise has a Lync environment, ignore this parameter. Default=1000.
Require SRTP in the Phone Configuration File	Select this option for *Secure* RTP. Real-time Transport Protocol (**RTP**) is the standard packet format for delivering voice over IP.
Disconnected Timeout	Default: 120 minutes. The IP phone reports its status to the server every hour. If it does not report its status before the 'Disconnect Timeout' lapses, i.e., if the parameter is left at its default and two hours pass without a status report, the status will change from **Registered** to **Disconnected** and the phone's 'Status' column in the Devices Status screen will be red-coded.
Redundant Mode	From the dropdown select **No Redundant** (default) or **Primary/Backup**. Allows the administrator to set the primary PBX / Lync 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/Lync server. If the primary falls, the other backs it up.
Primary	Enter the primary PBX/Lync server's IP address, i.e., the outbound proxy's.
Backup	Displayed only if you select the **Primary/Backup** option for the 'Redundant Mode' parameter (see above).
LDAP Configuration	Lightweight Directory Access Protocol lets you provide distributed directory information services to users in the enterprise. Not applicable in a Microsoft Lync environment. See Section C below.
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. See Section 6.1.1.
HTTP Proxy Configuration	Click this button if your phones are operating with an SBC HTTP proxy. This is mandatory for when the phones are behind a NAT. See Section 6.1.1.

3. View newly defined placeholder values in the IP Phone Placeholders page (**Phones Configuration** > **System Placeholders**).

C.3.7.2 Phone Model Placeholders

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

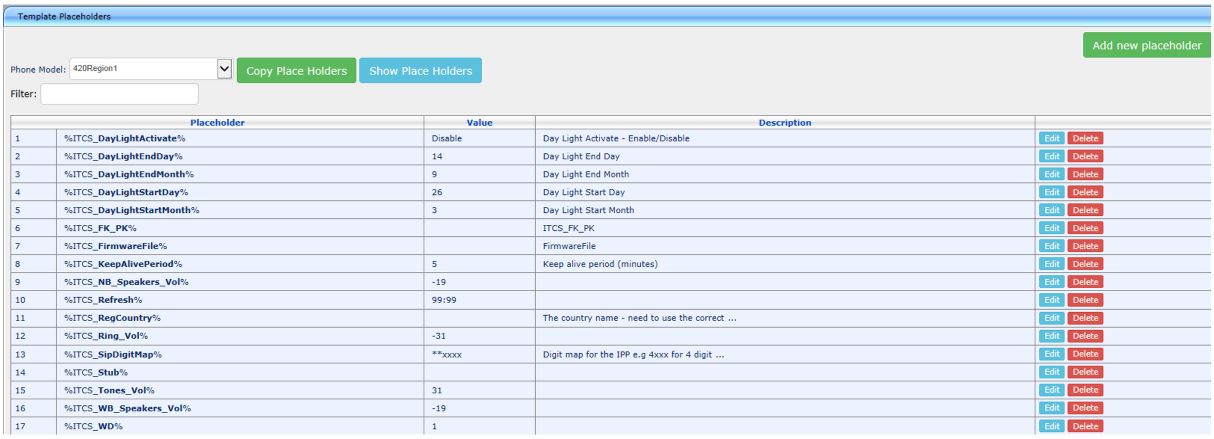
C.3.7.2.1 Editing Phone Model Placeholders

You can edit the values for existing phone model placeholders.

➢ **To edit values for existing phone model placeholders:**

- Open the Phone Model Placeholders page (Phones Configuration > Phone Model Placeholders):

Figure C-9: Phone Model Placeholders



Phone Model: 420Region1

Filter:

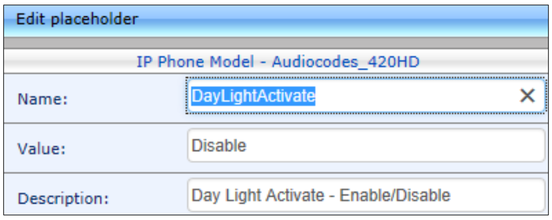
	Placeholder	Value	Description	
1	%ITCS_DayLightActivate%	Disable	Day Light Activate - Enable/Disable	Edit Delete
2	%ITCS_DayLightEndDay%	14	Day Light End Day	Edit Delete
3	%ITCS_DayLightEndMonth%	9	Day Light End Month	Edit Delete
4	%ITCS_DayLightStartDay%	26	Day Light Start Day	Edit Delete
5	%ITCS_DayLightStartMonth%	3	Day Light Start Month	Edit Delete
6	%ITCS_FK_PK%		ITCS_FK_PK	Edit Delete
7	%ITCS_FirmwareFile%		FirmwareFile	Edit Delete
8	%ITCS_KeepAlivePeriod%	5	Keep alive period (minutes)	Edit Delete
9	%ITCS_NB_Speakers_Vol%	-19		Edit Delete
10	%ITCS_Refresh%	99:99		Edit Delete
11	%ITCS_RegCountry%		The country name - need to use the correct ...	Edit Delete
12	%ITCS_Ring_Vol%	-31		Edit Delete
13	%ITCS_SipDigitMap%	**xxxx	Digit map for the IPP e.g 4xxx for 4 digit ...	Edit Delete
14	%ITCS_Stub%			Edit Delete
15	%ITCS_Tones_Vol%	31		Edit Delete
16	%ITCS_WB_Speakers_Vol%	-19		Edit Delete
17	%ITCS_WD%	1		Edit Delete

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

➢ **To edit a value of an existing phone model placeholder:**

1. Click the **Edit** button; the 'Edit placeholder' screen is displayed:

Figure C-10: Edit Phone Model Placeholder



IP Phone Model - Audiocodes_420HD

Name: DayLightActivate

Value: Disable

Description: Day Light Activate - Enable/Disable

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

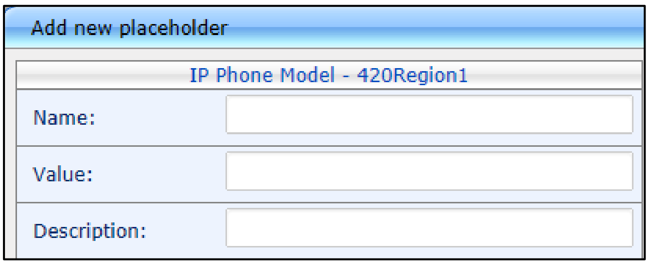
C.3.7.2.2 Adding a New Phone Model Placeholder

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

➢ **To add a new phone model placeholder:**

1. Open the Phone Model Placeholders page (**Phones Configuration** > **Phone Model Placeholders**):
2. From the **IP Phone Model** dropdown in the Phone Model Placeholders page, select the model, e.g., IP Phone Model – Audiocodes_420HD.
3. Click the **Add new placeholder** button.

Figure C-11: Add New Phone Model Placeholder



Add new placeholder

IP Phone Model - 420Region1

Name:	
Value:	
Description:	

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 **Submit**; the new placeholder is added to the table.

C.3.7.3 Region Placeholders

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

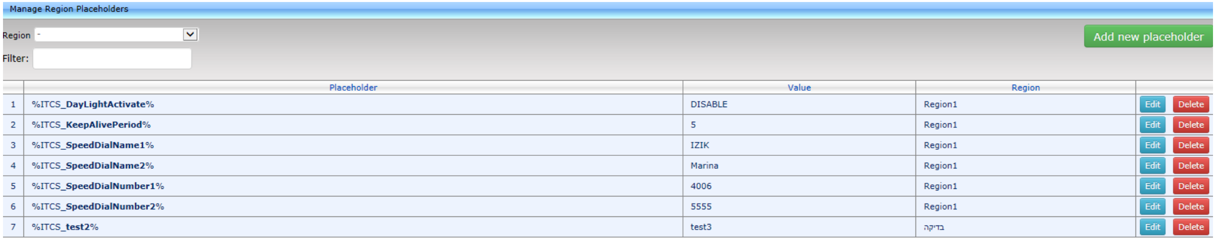
C.3.7.3.1 Editing Region Placeholders

You can edit the values for existing region placeholders.

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

1. Access the Manage Region Placeholders page (**Phones Configuration** > **Region Placeholders**):

Figure C-12: Manage Region Placeholders



Manage Region Placeholders

Region: -

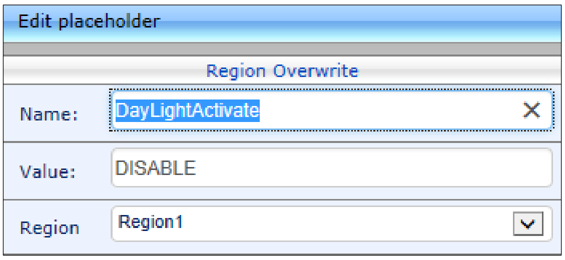
Filter:

	Placeholder	Value	Region	
1	%ITCS_**DayLightActivate**%	DISABLE	Region1	Edit Delete
2	%ITCS_**KeepAlivePeriod**%	5	Region1	Edit Delete
3	%ITCS_**SpeedDialName1**%	IZIK	Region1	Edit Delete
4	%ITCS_**SpeedDialName2**%	Marina	Region1	Edit Delete
5	%ITCS_**SpeedDialNumber1**%	4006	Region1	Edit Delete
6	%ITCS_**SpeedDialNumber2**%	5555	Region1	Edit Delete
7	%ITCS_**test2**%	test3	בדיקה	Edit Delete

➢ **To edit a value of an existing region placeholder:**

1. Click the **Edit** button; the 'Edit placeholder' screen is displayed:

Figure C-13: Edit Region Placeholder



Edit placeholder

Region Overwrite

Name:	DayLightActivate
Value:	DISABLE
Region	Region1

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 'Region' dropdown, you can select another region.
5. Click **Submit**; the edited placeholder is added to the table.

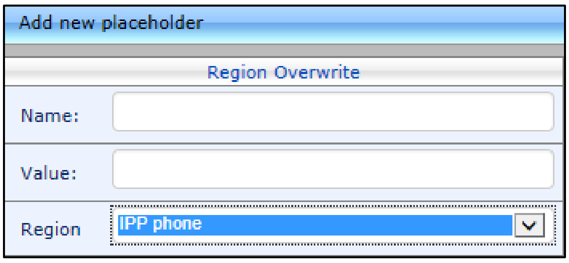
C.3.7.3.2 Adding a New Region Placeholder

You can add a new region placeholder.

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

1. Access the Manage Region Placeholders page (**Phones Configuration** > **Region Placeholders**):
2. From the **Region** dropdown, select a region, and then click the **Add new placeholder** button.

Figure C-14: Add New Region Placeholder



Add new placeholder

Region Overwrite

Name:	
Value:	
Region	IPP phone

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 'Region' dropdown, select a new region.
6. Click **Submit**; the new placeholder is added to the table.

C.3.7.4 Devices Placeholders

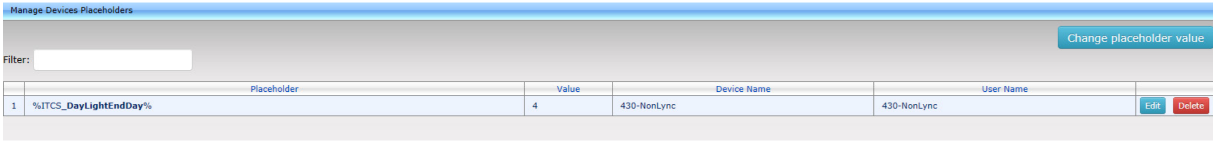
You can change placeholders values for specific phones, for example, you can change placeholders values for the CEO's phone. You can also edit a phone's placeholders values.

C.3.7.4.1 Changing a Device Placeholder Value

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

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

Figure C-15: Manage Devices Placeholders



Manage Devices Placeholders

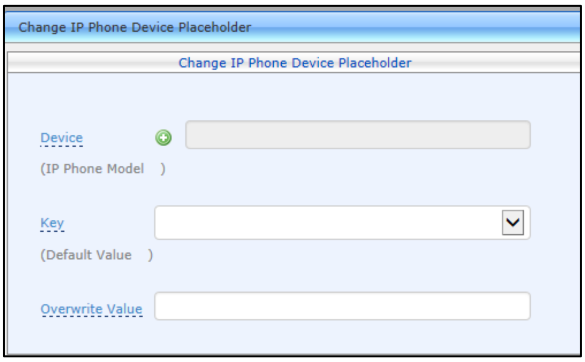
Filter:

	Placeholder	Value	Device Name	User Name	
1	%ITCS_**DayLightEndDay**%	4	430-NonLync	430-NonLync	Edit Delete

Tip: 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 the **Change placeholder value** button; the Change IP Phone Device Placeholder screen opens.

Figure C-16: Change IP Phone Device Placeholder



Change IP Phone Device Placeholder

Change IP Phone Device Placeholder

Device

(IP Phone Model)

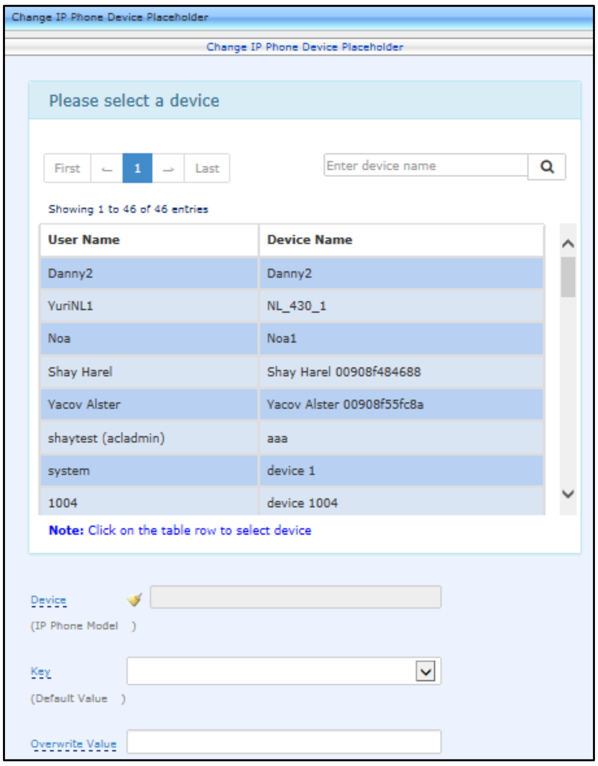
Key

(Default Value)

Overwrite Value

3. From the **Device** dropdown, click the **+**; the screen shown below opens.

Figure C-17: Change IP Phone Device Placeholder – Selecting the Device



Change IP Phone Device Placeholder

Change IP Phone Device Placeholder

Please select a device

Showing 1 to 46 of 46 entries

User Name	Device Name
Danny2	Danny2
YuriNL1	NL_430_1
Noa	Noa1
Shay Harel	Shay Harel 00908f484688
Yacov Alster	Yacov Alster 00908f55fc8a
shaytest (acladmin)	aaa
system	device 1
1004	device 1004

Note: Click on the table row to select device

Device

(IP Phone Model)

Key

(Default Value)

Overwrite Value

4. Select the device; the read-only 'Device' field is filled.
5. From the **Key** dropdown, choose the phone configuration key.
6. Enter the device's overwrite value in the 'Overwrite Value' field, and then click the **Submit** button.

C.3.7.4.2 Editing a Device Placeholder Value

You can edit a device placeholder value.

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

1. Access the Manage Devices Placeholders page (**Phones Configuration** > **Devices Placeholders**).
2. Click the **Edit** button; the 'Edit placeholder' screen is displayed, as shown above.
3. In the 'Overwrite Value' field, enter a new value if necessary.
4. Click **Submit**; the edited device placeholder is added to the table.

Note: The new overwrite value is not automatically generated in the device IP phone configuration file. To generate the new device in the IP phone configuration template file, click the **Generate Configuration Template** button in the Templates page (**Phones Configuration** > **Templates**).

D Configuring the LDAP Directory

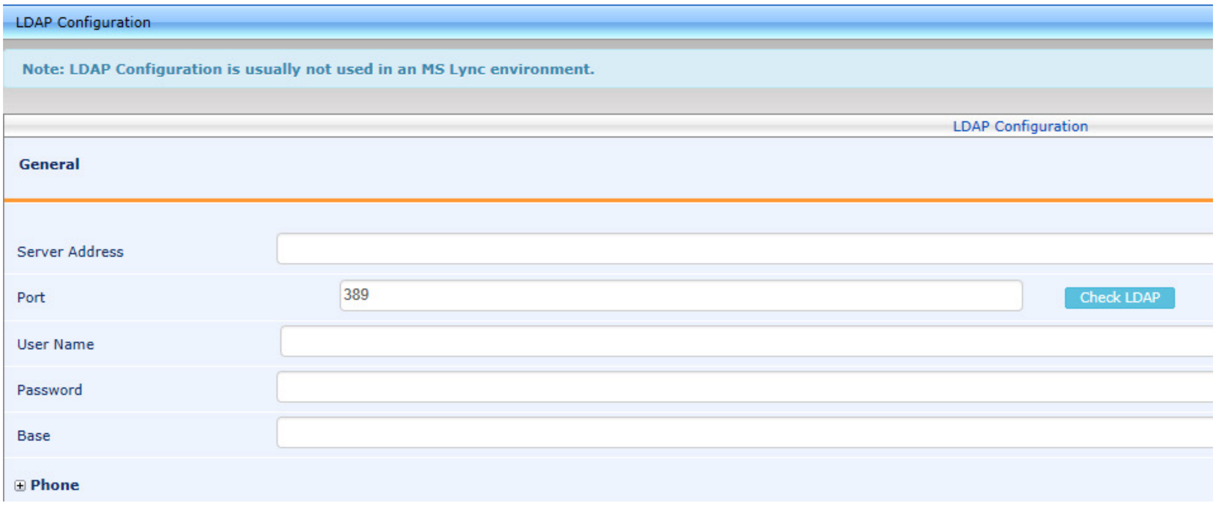
Note: This section is inapplicable when in a Microsoft Lync environment because Lync uses its own Active Directory server.

The IP Phone Management Server lets you configure an enterprise's LDAP directory.

➢ To access the LDAP directory:

1. Access the System Settings page (**Phones Configuration** > **System Settings**).
2. Click the **LDAP Configuration** button; the LDAP Configuration page opens.

Figure D-1: LDAP Configuration



LDAP Configuration

Note: LDAP Configuration is usually not used in an MS Lync environment.

LDAP Configuration

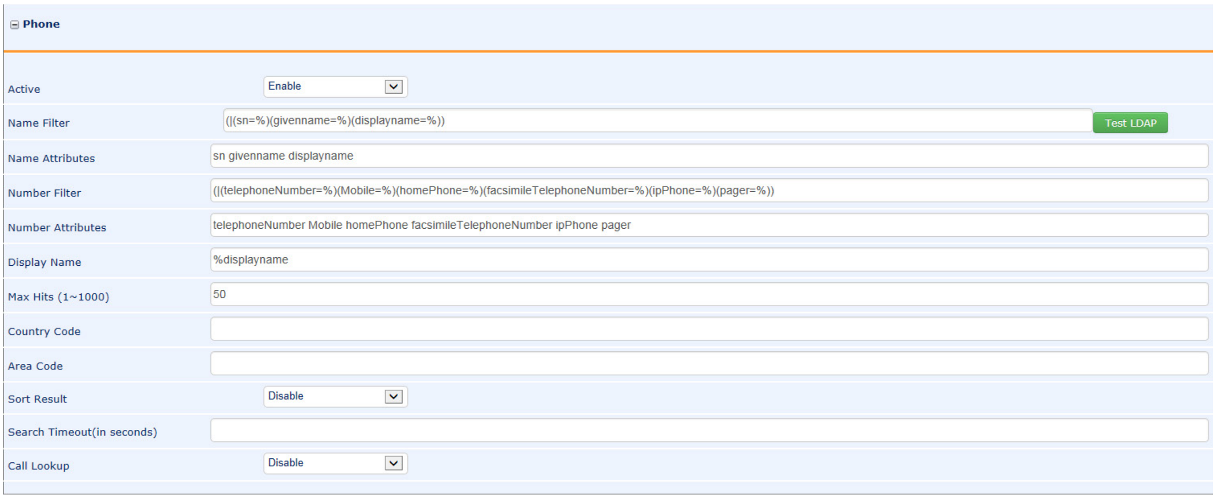
General

Server Address	
Port	389
User Name	
Password	
Base	

⊞ Phone

3. Click **+Phone**; the screen expands to display the 'Active' parameter.
4. From the 'Active' parameter dropdown, select **Enable**; the figure shown below is displayed.

Figure D-2: LDAP Configuration - Phone



⊟ Phone

Active	Enable
Name Filter	(|(sn=%)(givenname=%)(displayname=%))
Name Attributes	sn givenname displayname
Number Filter	(|(telephoneNumber=%)(Mobile=%)(homePhone=%)(facsimileTelephoneNumber=%)(ipPhone=%)(pager=%))
Number Attributes	telephoneNumber Mobile homePhone facsimileTelephoneNumber ipPhone pager
Display Name	%displayname
Max Hits (1~1000)	50
Country Code	
Area Code	
Sort Result	Disable
Search Timeout(in seconds)	
Call Lookup	Disable

5. Configure the parameters using the table below as reference.

Table D-1: LDAP Configuration

Parameter	Description
Server address	Enter the IP address, or URL, of the LDAP server.
Port	Enter the LDAP service port.
User Name	Enter the user name used for the LDAP search request.
Password	Enter the password of the search requester.
Base	Enter the access point on the LDAP tree.
Active	From the dropdown, select **Disable** LDAP (default) or **Enable** LDAP. If **Enable** is selected, the parameters below are displayed.
Name Filter	Specify your search pattern for name look ups. For example, when you type in the *(&(telephoneNumber=*)(sn=%))* field*,* the search result includes all LDAP records which have the 'telephoneNumber' field set, and the '("sn"-->surname)' field starting with the entered prefix. When you type in the *(|(cn=%)(sn=%))* field, the search result includes all LDAP records which have the '("cn"-->CommonName)' OR the '("sn"-->Surname)' field starting with the entered prefix. When you type in the *(!(cn=%))* field*,* the search result includes all LDAP records which "do not" have the 'cn' field starting with the entered prefix.
Name Attributes	Specifies the LDAP name attributes setting, which can be used to specify the "name" attributes of each record which is returned in the LDAP search results. When you type in the following field, for example, *cn sn displayName*", this requires you to specify 'cn-->commonName'. This is the Full name of the user, sn-->Surname, last name or family name and "displayName" fields for each LDAP record.
Number Filter	Specifies your search pattern for number look ups. When you type in the following field, for example, *(|(telephoneNumber=%)(Mobile=%)(ipPhone=%))*, the search result is all LDAP records which have the "telephoneNumber" OR "Mobile" OR "ipPhone"field match the number being searched. When you type in the *(&(telephoneNumber=%)(sn=*))* field, the search result is all LDAP records which have the 'sn' field set and the "telephoneNumber" match the number being searched.
Number Attributes	Specifies the LDAP number attributes setting, which can be used to specify the "number" attributes of each record which is returned in the LDAP search results. When you type in the following field, for example, *Mobile telephoneNumber ipPhone*, you must specify 'Mobile', 'telephoneNumber' and 'ipPhone' fields for each LDAP record.
Display Name	Specifies the format in which the "name, e.g. "Mike Black" of each returned search result is displayed on the IPPHONE. When you type in the following field, for example, %sn, %givenName, the displayed result returned should be "Black, Mike".
Max Hits (1~1000)	Specifies the maximum number of entries expected to be sent by the LDAP server (this parameter is sent to the LDAP server).
Country Code	Defines the country code prefix added for number search.
Area Code	Defines the area code prefix added for number search.
Sort Result	Sorts the search result by display name on the client side.
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.

6. Click **Submit**.

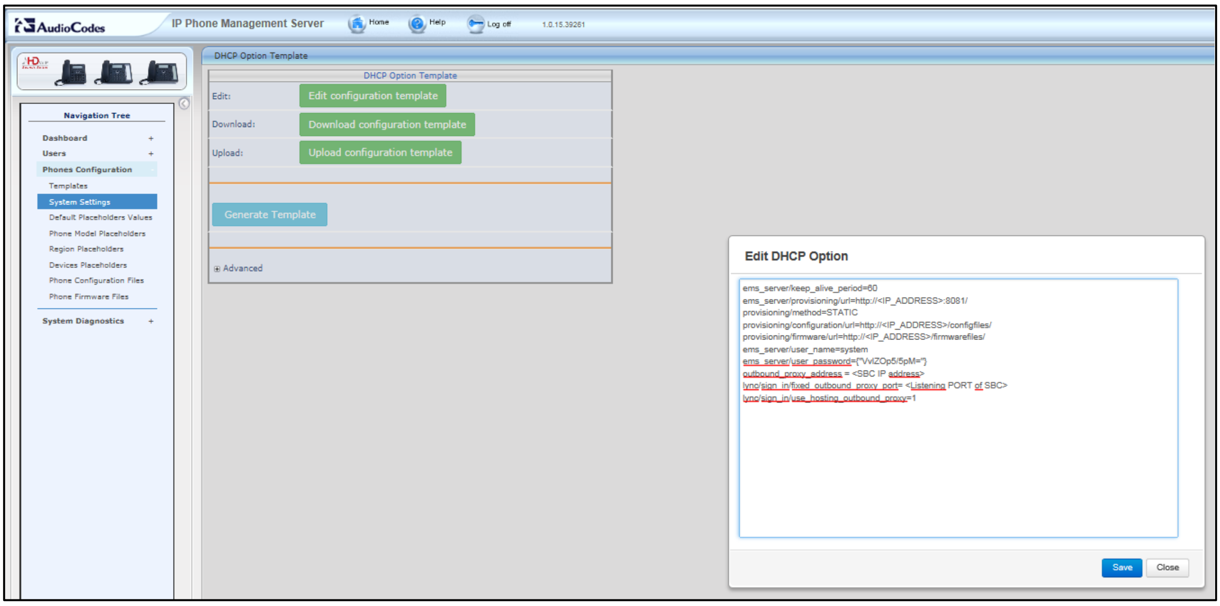
E Configuring Phones to Operate in an OVR Deployment

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. Access the System Settings page (**Phones Configuration** > **System Settings**) and then click the **DHCP Option Configuration** button.
2. Click the **Edit configuration template** button; the Edit DHCP Option pane opens.

Figure E-1: Edit DHCP Option



```
ems_server/keep_alive_period=60
ems_server/provisioning/url=http://<IP_ADDRESS>:8081/
provisioning/method=STATIC
provisioning/configuration/url=http://<IP_ADDRESS>/configfiles/
provisioning/firmware/url=http://<IP_ADDRESS>/firmwarefiles/
ems_server/user_name=system
ems_server/user_password={"VvIZOp5/5pM="}
outbound_proxy_address = <SBC IP address>
lync/sign_in/fixed_outbound_proxy_port= <Listening PORT of SBC>
lync/sign_in/use_hosting_outbound_proxy=1
```

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.

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

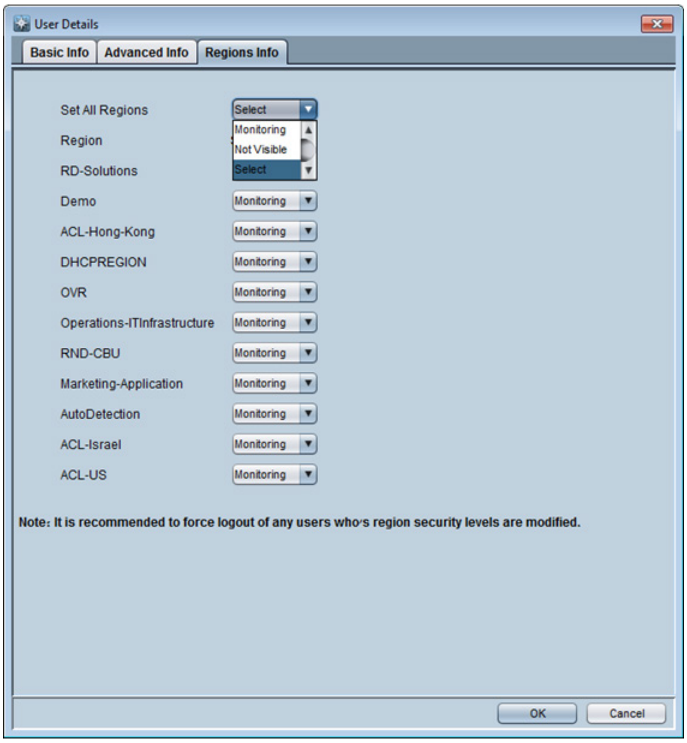
This page is intentionally left blank.

F Configuring Security Level in the EMS

F.1 Per Region

In the EMS's User Details screen under the **Regions Info** tab, you can configure each region with an administrator security level. Only administrators configured with that level will be permitted to manage that region. Optionally, all regions can be set with the same level ('Set All Regions'); all administrators will then be permitted to manage every region.

Figure F-1: Region-Specific Security Level



Set All Regions	Select
Region	
RD-Solutions	
Demo	Monitoring
ACL-Hong-Kong	Monitoring
DHCPREGION	Monitoring
OVR	Monitoring
Operations-ITInfrastructure	Monitoring
RND-CBU	Monitoring
Marketing-Application	Monitoring
AutoDetection	Monitoring
ACL-Israel	Monitoring
ACL-US	Monitoring

Note: It is recommended to force logout of any users who's region security levels are modified.

Each region can be configured with one of the following levels:

- **Operator**. The administrator can perform any action (read-write) and/or provisioning changes on all users, devices and region placeholders.
- **Monitoring**. The administrator can view all data (read-only) but cannot perform any modification.
- **Not Visible**. The administrator can't see this region displayed in the IP Phone Management Server.

See the *EMS User's Manual* for detailed information.

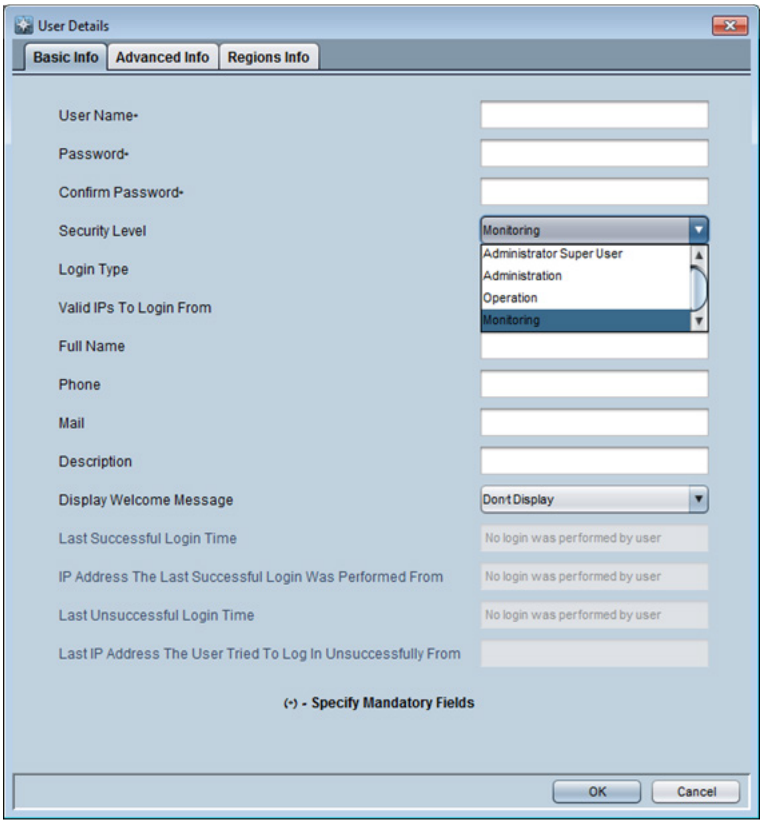
Note:

- An administrator can manage more than one region.
- Administrators who haven't been allocated a region are managed only by the Super Administrator.
- An administrator cannot be assigned a higher security level for a different region. For example, if the administrator is assigned **Monitoring** for Region A, they cannot be assigned **Operator** for Region B.
- A summary of the administrator security level for each region is shown in the Regions screen (see Section 0).

F.2 Per Administrator

Administrator security levels are configured in the EMS's User Details screen, under the **Basic Info** tab, shown below.

Figure F-2: Security Level



User Name*	
Password*	
Confirm Password*	
Security Level	Monitoring Administrator Super User Administration Operation Monitoring
Login Type	
Valid IPs To Login From	
Full Name	
Phone	
Mail	
Description	
Display Welcome Message	Dont Display
Last Successful Login Time	No login was performed by user
IP Address The Last Successful Login Was Performed From	No login was performed by user
Last Unsuccessful Login Time	No login was performed by user
Last IP Address The User Tried To Log In Unsuccessfully From	

(*) - Specify Mandatory Fields

- Administrators with 'Super Administrator' or 'Administrator' permissions can perform all actions and view all users/devices. They can also edit system settings, templates and template placeholders.
- There's no difference between 'Super Administrator' and 'Administrator'.
- See the *EMS User's Manual* for detailed information.

G 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.

Note: Applies only if the Zero Touch provisioning method was used.

This page is intentionally left blank.

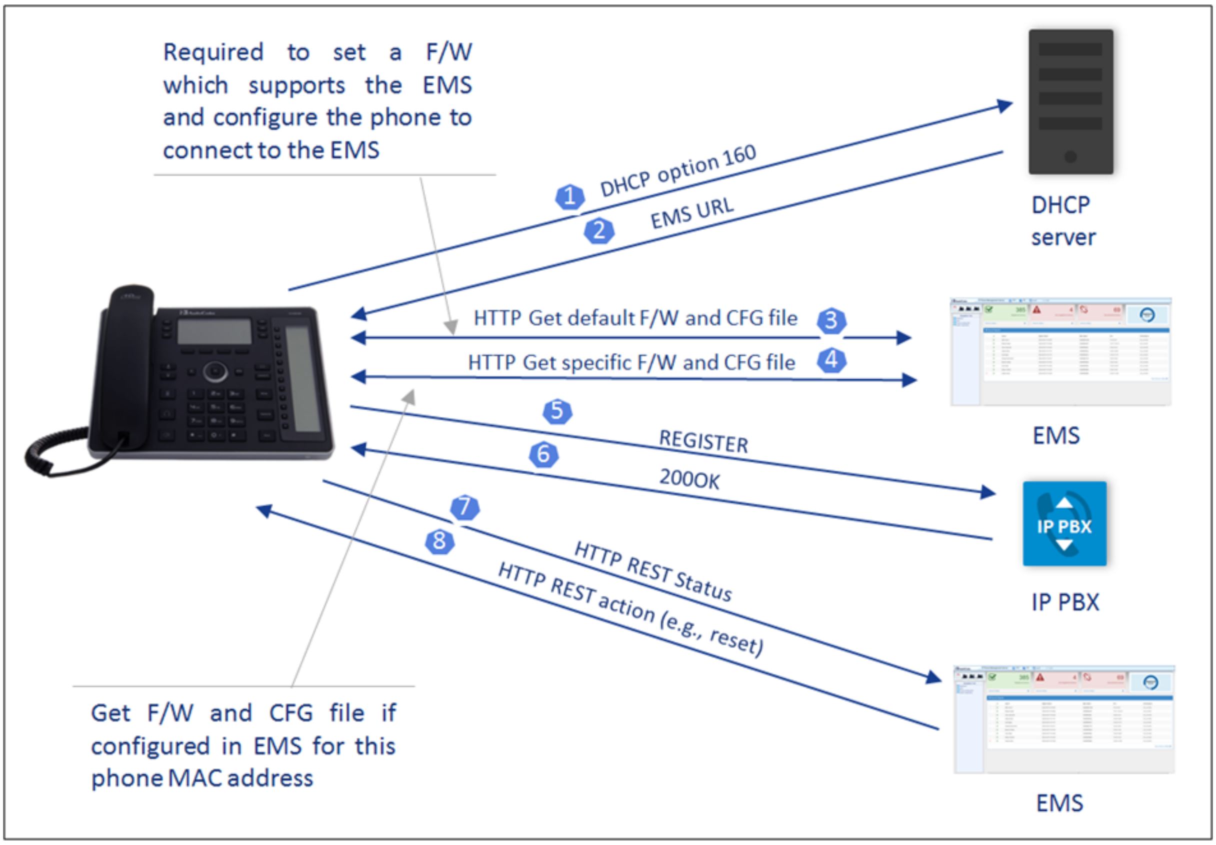
H Provisioning Flows

This appendix illustrates the provisioning flows.

H.1 Generic Phones

The figure below shows the provisioning flow between a generic (non-Lync) phone and the EMS when the MAC address is known.

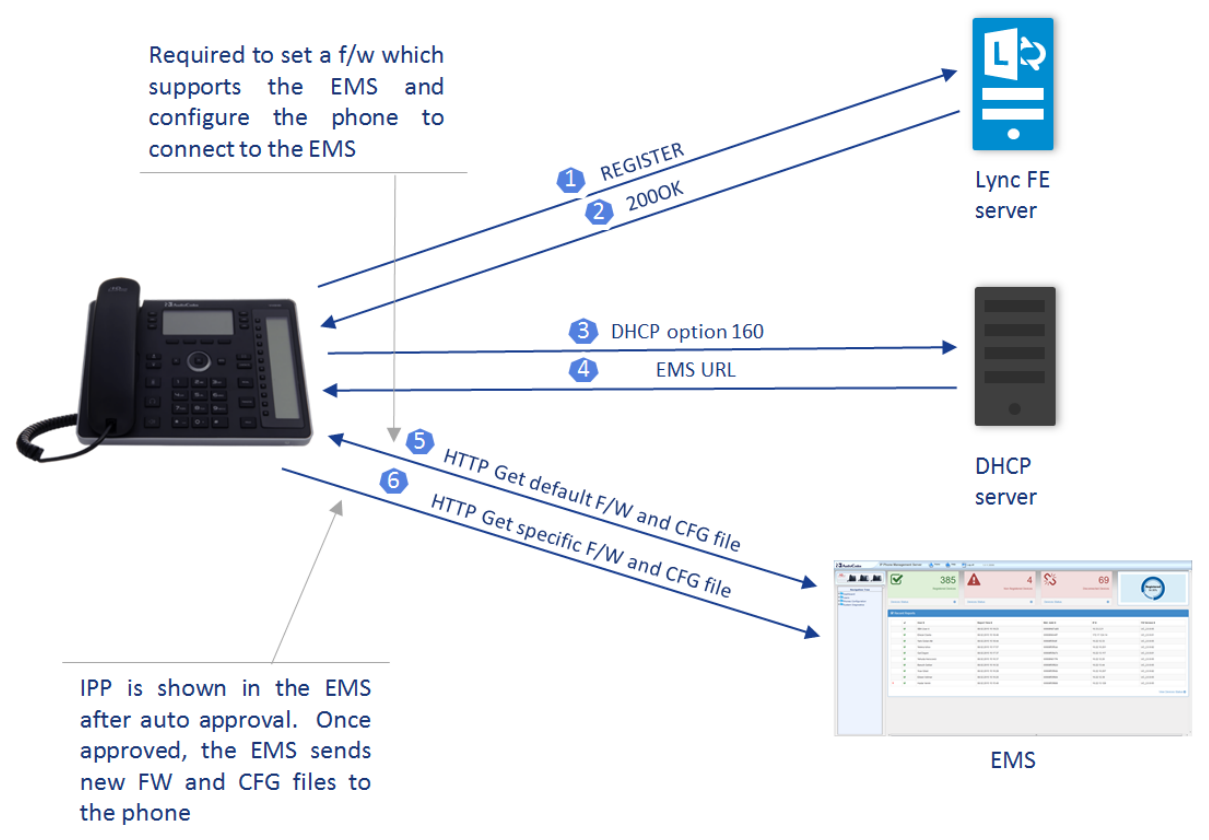
Figure H-1: Generic phone > EMS when MAC is Known


Required to set a F/W which supports the EMS and configure the phone to connect to the EMS
1 DHCP option 160
2 EMS URL
DHCP server
HTTP Get default F/W and CFG file 3
HTTP Get specific F/W and CFG file 4
EMS
5 REGISTER
6 200OK
IP PBX
IP PBX
7 HTTP REST Status
8 HTTP REST action (e.g., reset)
EMS
Get F/W and CFG file if configured in EMS for this phone MAC address

H.2 Lync Phones

The figure below shows the provisioning flow between a Lync phone and the EMS when the MAC address is known.

Figure H-2: Lync Phone > Zero Touch


Required to set a f/w which supports the EMS and configure the phone to connect to the EMS
1 REGISTER
2 200OK
Lync FE server
3 DHCP option 160
4 EMS URL
DHCP server
5 HTTP Get default F/W and CFG file
6 HTTP Get specific F/W and CFG file
EMS
IPP is shown in the EMS after auto approval. Once approved, the EMS sends new FW and CFG files to the phone

This page is intentionally left blank.

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

AudioCodes Inc.
27 World's Fair Drive,
Somerset, NJ 08873
Tel: +1-732-469-0880
Fax: +1-732-469-2298

Contact us: www.audiocodes.com/contact
Website: www.audiocodes.com