

SNAPsolution

Endpoints Module

Admin Guide



CONTENTS

Introduction	v
Document Conventions	v
1. Getting Started	6
Logging in.....	7
About Support.....	7
Model Compatibility	7
2. General Provisioning Process	9
Provisioning Overview	10
Pointing a Phone to the Endpoints Module	10
Cisco SPA/Linksys.....	10
GrandStream	10
Polycom.....	11
UC4 or Later Web Interface	11
Phone Menu.....	11
Yealink.....	11
Adding a Phone	12
Adding a Phone Using the Portal	12
Adding a Phone Using the Endpoints Admin UI	14
Adding an Analog Gateway	15
Defaults and Overrides	16
Setting the Scope of a Parameter	18
Entering a Brand Default.....	18
Entering a Model Default	20
Entering a Domain Default.....	21
Entering a Handset/MAC Default.....	22
3. Polycom	23
Configuration Files.....	24
How the Endpoints Module Decides Which Configuration File to Use.....	24
Bootroms and Firmware.....	25
Bootroms	25
Firmware.....	26
Split or Combined Firmware	26
Uploading Firmware	26
Adding Firmware to the Device Definitions	27

Selecting Firmware	28
Upgrading Soundpoint Phones to UC4.....	29
Downgrading Soundpoint Phones from UC4	29
Which Firmware Version Should I Run?.....	30
4. Yealink.....	31
Configuration Files.....	32
How the Endpoints Module Decides Which Configuration File to Use.....	32
Firmware	33
Selecting the Right Firmware	33
Uploading Firmware.....	33
Upgrading from 6x to 7x Firmware	35
Which Version Firmware Should I Run?.....	36
5. Dealing with New Devices	38
Running a New Device Not in the Device List.....	39
New Device with an Existing Format.....	39
New Device without an Existing Format.....	42
Making the Configuration File.....	42
Creating a New NDP Code Type	43
Loading the Configuration File	44
Managing Pre/Postfix on the Requested Configuration File	44
6. Directories	45
Types of Directories.....	46
Selecting a Directory.....	46
Using the Portal to Select a Directory.....	46
Using the Admin UI to Select a Directory	47
Creating a Custom Directory in the Directory Designer	48
7. Connecting to Cores	51
Validating API Version	52
Geo Clusters.....	52
Adding a New Core Node to the Endpoints Module	53
Preparing the Core.....	53
Adding the Server to the Endpoints Module	54
How Geo Redundancy Works.....	56
8. Security	58
SAFE	59
Reviewing the SAFE Fraud Scores.....	59
Handset Security	59

Contents

Password Protecting Files	60
Updating Deployed Phones	60
Provisioning New Phones	60
Enabling Password Protection	60
Disabling TFTP	61
Secure Admin Login	61
9. Diagnostics and Logs	63
Sync	64
Events	64
Logs	65
10. Configuration Parameters	66
Index	68

INTRODUCTION

Welcome to the SNAPsolution Endpoints Module Admin Guide.

The Endpoints module handles the provisioning of phones and analog telephone adapters (ATAs). It does this by generating configuration files for each make and model of phone based on parameters you set in the SNAPsolution system.

The Endpoints module can also host firmware and bootroms, enabling upgrading or downgrading of phones.

Document Conventions

This guide uses the following conventions to draw your attention to certain information.

Convention	Description
Note	Notes emphasize or supplement important points of the main text.
Bold	Indicates text on a window, other than the window title, including menus, menu options, buttons, fields, and labels.
<i>Italic</i>	Indicates a variable, which is a placeholder for actual text provided by the user or system. Angle brackets (< >) are also used to indicate variables.
screen/code	Indicates text that is displayed on screen or entered by the user.

Please Note:

This SNAPsolution Endpoints Module Administrator's guide attempts to be comprehensive and may include references to sections, tools, or features that do not apply to your implementation..

1. GETTING STARTED

Topics:

- ^ *Logging in (page 7)*
- ^ *About Support (page 7)*
- ^ *Model Compatibility (page 7)*

This chapter describes how to get started with the Endpoints module.

Logging in

To log in to the Endpoints module:

1. Launch a web browser.
2. In the browser address bar, type `https://<endpoints-FQDN>/ndp/adminlogin.php`.
3. At the login page, enter the default user name and password (both are **tac** on a new system). For security, each typed password character is masked by a dot (●).
4. Click **Login**.

The Endpoints module login credentials do not change when you change the Core Module password, as these Modules do not have one-to-one relationships. Therefore, be sure to change these default logins at **System > Admin Accounts**.

About Support

NetSapiens is responsible for supporting the Endpoints module, but not devices such as phones and ATAs. For device specific support, contact the device manufacturer.

Model Compatibility

Every phone manufacturer follows a different style for its configuration file, with some manufacturers even varying styles between models of the same brand. Some configuration files are plain text, for example, while others are XML. Each company's parameters and formatting are different as well. The Endpoints module tries to abstract you from these details by handling formats for a variety of popular phone makes and models.

For example:

- Polycom has the older "SIP" and newer "UC" configuration files.
- Yealink has the M1, M3, and M7 configuration file format.
- Grandstream has an older encrypted file and newer XML format.

The Endpoints module generally supports new models of phones, as long as they follow the configuration format of prior models.

This guide references Polycom and Yealink devices, as they are the most popular in the SNAPsolution user base. However, other brands, such as Cisco, Grandstream, Panasonic, and more, can be provisioned using the Endpoints module.

When a manufacturer introduces a new configuration file format, NetSapiens assesses the popularity of that device and brand in our user base and might include native support for the phone in future releases. The Endpoints module also has a Custom File Format, which allows you to add support for nearly any device.

2. GENERAL PROVISIONING PROCESS

Topics:

- ^ *Provisioning Overview (page 10)*
- ^ *Pointing a Phone to the Endpoints Module (page 10)*
- ^ *Adding a Phone (page 12)*
- ^ *Adding an Analog Gateway (page 15)*
- ^ *Defaults and Overrides (page 16)*
- ^ *Setting the Scope of a Parameter (page 18)*
- ^ *Entering a Brand Default (page 18)*
- ^ *Entering a Model Default (page 20)*
- ^ *Entering a Domain Default (page 21)*
- ^ *Entering a Handset/MAC Default (page 22)*

This chapter describes the general provisioning process.

Provisioning Overview

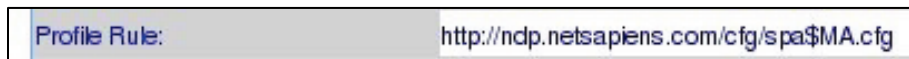
At boot, phones try to pull a configuration file from a provisioning service. The location of the configuration file can be set via Dynamic Host Configuration Protocol (DHCP) options, manual entry on the phone, or redirection services like Polycom's ZTP and Yealink's RPS. If the phone pulls the configuration file(s) successfully, the phone tries to apply the new configuration. It might also try a bootrom or firmware upgrade, depending on the phone.

Pointing a Phone to the Endpoints Module

Note: These directions might vary slightly by phone model and firmware version.

Cisco SPA/Linksys

1. Access the phone's web interface (typically, press the **Setup** button, and then navigate down to **Network**).
2. Go to the **Admin > Advanced** page, and then click the **Provisioning** tab.
3. Change the Profile Rule to match to the following figure using the syntax **http://<endpoint-FQDN>/cfg/spa\$MA.cfg**.



4. Once set, reboot your phone to force it to request the configuration file from the Endpoints module.

GrandStream

1. Access the phone's web interface.
2. Log in using the default login and password (both are **admin**). If the web interface prompts you for a password only, type **admin** or **123**.
3. Go to the Advanced Settings page, and then scroll down to the **Firmware Upgrade and Provisioning** section.
4. For **Upgrade Via**, click **HTTP** and change **Config Server Path** to **<endpoint-FQDN>/cfg**.



5. Once set, reboot your phone to force it to request the configuration file from the Endpoints module.

Polycom

UC4 firmware allows you to set the provisioning URL via web; otherwise, you can set the provisioning URL from the phone menu.

UC4 or Later Web Interface

1. Obtain the phone's IP address by going to **Menu > (Settings) > Status > Network > TCP/IP Parameters**.
2. Launch a web browser (newer UC firmware use SSL), and then go to the IP address you found in step 1.
3. Log in as username **Polycom** using the password **456**.
4. Go to **Settings > Provisioning Server**.
5. Set the **Server Type** to **HTTP** and the **Server Address** to **< endpoint-FQDN >/cfg**.
6. Once set, reboot your phone to force it to request the configuration file from the Endpoints module.

Phone Menu

1. Press the **Menu** button, and then go to **Settings > Advanced**.
2. Enter the password (default is **456**).
3. Go to **Admin Settings > Network Configuration**, and the **Server** menu.
4. Change **Server Type** to **HTTP**.
5. In **Server Address**, type **< endpoint-FQDN >/cfg**.
6. Exit and save. The phone should reboot. If it doesn't, reboot the phone to force it to request the configuration file from the Endpoints module.

Yealink

1. Determine the phone's IP address.
2. Launch a web browser, and then go to the IP address you found in step 1.
3. Log in (the default username and password are both **admin**).
4. Go to **Settings**, and then click the **Auto Provision** subtab.
5. Set the **Server URL** as **http://<endpoint-FQDN>/cfg/**.
6. Confirm the URL, and then click **Autoprovision Now**.

- Once set, reboot your phone to force it to request the configuration file from the Endpoints module.

Adding a Phone

Phones can be added using the Portal or Endpoints Admin UI.

Adding a Phone Using the Portal

After you log in to the Portal, you can add a phone using the Add Phone page.

- Click **Inventory**, and then click the **Phone Hardware** tab.

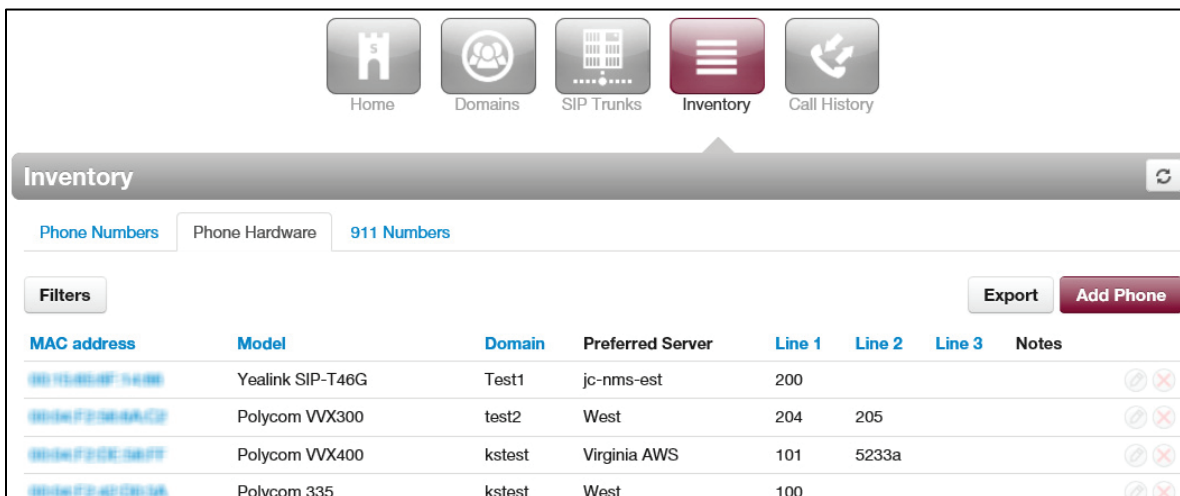


Figure 2-1. Inventory > Phone Hardware Tab

- Click **Add Phone**. The Add Phone page appears, with the **Basic** tab displayed.

The screenshot shows a web interface titled "Add Phone" with a close button (X) in the top right corner. Below the title are two tabs: "Basic" (selected) and "Advanced". The form contains the following fields:

- Model:** A dropdown menu showing "Yealink SIP-T48G".
- MAC Address:** A text input field containing "000000001524".
- Domain:** A text input field containing "kevin.netsapiens.com (Kevin Selkowitz)".
- Line 1:** A text input field containing "100 (Michael Scott)".

Figure 2-2. Add Phone Page with Basic Tab Displayed

3. In the **Basic** tab, complete the fields (see Table 2-1).

Table 2-1. Fields on the Add Phone - Basic Tab

Setting	Description
Model	Select the model of phone you have.
MAC Address	Enter the MAC address for your phone (omit formatting such as colons or dashes).
Domain	Enter the domain to which the phone will be associated. For this lab, type kevin.netsapiens.com.
Line 1	Enter the name of the user to assign to the phone.

4. Click **Save** to add a phone.
5. Repeat steps 2 through 4 to add a second phone whose **Line 1** setting is Line 101

Note: You can assign only one active phone to an extension at a time. For example, if extension 100 is assigned to the handset 0080F0C8C645, this extension cannot be assigned to another handset. If you require more than one handset to be associated with the same extension, the additional handsets will be 100a, 100b, and so on.

Adding a Phone Using the Endpoints Admin UI

The procedure for adding a phone using the Endpoints Admin UI varies a bit, depending on whether your Endpoints Module is associated with one or many Cores and whether geo-redundancy is enabled.

To add a device:

1. Go to **Configurations > Devices**.
2. Click **Add Configuration**.
3. In the first screen:
 - a. Enter the MAC address of the device. Omit formatting such as dashes and colons.
 - b. Select the model of the device, and the SiPbx Server or Domain. **SiPbx server** appears as an option if the Endpoints module configures devices on many Cores; otherwise, **Domain** appears as an option).
 - c. Click the **Select** button to continue.

The screenshot shows a web form titled '>> Phones / ATAs >> Select Server'. It contains the following fields:

- MAC**: A text input field.
- Device Model #**: A dropdown menu with 'Aastra 480i' selected.
- SiPbx Server**: A dropdown menu with 'Core1' selected.
- Domain**: A dropdown menu with 'foo-neworleans' selected.

4. You might have an intermediate step to select the domain. Once selected, click **Select Domain**.

The screenshot shows a web form titled '>> Phones / ATAs >> Select Domain'. It contains the following fields:

- MAC**: A text input field containing '000000000085'.
- Device Model #**: A dropdown menu with 'Aastra 480i' selected.
- SiPbx Server**: A dropdown menu with 'Blastoise @ HQ' selected.
- Redundancy type**: A dropdown menu with 'system default' selected.
- Transport**: A dropdown menu with 'UDP' selected.
- Domain**: A dropdown menu with 'ABC' selected.

5. Finally you are taken to a page to associate lines to the device. After you assign the lines, click **Create** to save the new device.

The screenshot shows a web interface titled '>> Phones / ATAs >> Select Devices'. The form contains the following fields and values:

- MAC : 000000000085
- Device Model # : Astra 480i
- SiPbx Server : Core1
- Domain : foo-neworleans
- Phone Extension 1 : n/a
- Phone Extension 2 : n/a
- Phone Extension 3 : n/a
- Phone Extension 4 : n/a
- Notes : (empty text box)

At the bottom of the form are two buttons: 'Create' and 'Cancel'.

Adding an Analog Gateway

Analog gateways are similar to phones/ATAs, with two major differences:

- Analog gateways support trunks (one trunk's registration can be associated to many lines which the gateway device will hunt)
- Analog gateways support devices up to 24 ports

A few examples of gateways include the Linksys/Cisco SPA8000 and Grandstream GXW-4008.

To add a gateway in Endpoints Admin UI:

1. Go to **Configurations > Gateways > Analog**.

2. After entering the MAC and selecting the server and domain, a screen similar to the following allows you to assign trunks and lines.

>> Analog Gateways >> Select Devices

MAC ⓘ : 000000000085

Device Model # ⓘ : Linksys spa8000

SiPbx Server ⓘ : Corp.netsapiens.com

Domain ⓘ : kevin.netsapiens.com

Trunk 1 ⓘ : sip:800@kevin.netsapiens.com

Trunk 2 ⓘ : n/a

Trunk 3 ⓘ : n/a

Trunk 4 ⓘ : n/a

Line 1 ⓘ : Trunk 1

Line 2 ⓘ : Trunk 1

Line 3 ⓘ : Trunk 1

Line 4 ⓘ : Trunk 1

Line 5 ⓘ : Trunk 1

Line 6 ⓘ : Trunk 1

Line 7 ⓘ : Trunk 1

Line 8 ⓘ : Trunk 1

3. After you set the trunks/lines, click **Create** to add the device.

Defaults and Overrides

Configuration files are generated on-the-fly by combining the brand defaults and overrides into a configuration file format suitable for the phone model. Parameters are defined by the phone manufacturer and usually described in an Administrator's or Provisioning Guide.

To enable multicast paging on a Polycom phone, for example, refer to the Polycom UC Software Admin Guide for the following parameter:

ptt.pageMode.enable	0 or 1	0
If 0, group paging is disabled. If 1, group paging is enabled.		

To do the same for a Yealink phone, refer to the Yealink Administrator's Guide for the following parameters:

General Provisioning Process

Parameters	Permitted Values	Default
multicast.paging_address.X.ip_address	String	Blank
<p>Description: Configures the multicast IP address and port number for a paging list key. X ranges from 1 to 10.</p> <p>Example: multicast.paging_address.1.ip_address = 224.5.6.20:10008</p> <p>Note: The valid multicast IP addresses range from 224.0.0.0 to 239.255.255.255.</p> <p>Web User Interface: Directory->Multicast IP->Paging List->Paging Address</p> <p>Phone User Interface: Menu->Features->Others->Option->Edit->Address</p>		
multicast.paging_address.X.label	String	Blank
<p>Description: Configures the multicast paging group name for a paging list key. X ranges from 1 to 10.</p> <p>Example: multicast.paging_address.1.label = Product</p> <p>Web User Interface: Directory->Multicast IP->Paging List->Label</p> <p>Phone User Interface: Menu->Features->Others->Option->Edit->Label</p>		

Parameters	Permitted Values	Default
linekey.X.type/programablekey.X.type	66	Refer to the following content
<p>Description: Configures a DSS key as a paging list key on the IP phone. The digit 66 stands for the key type Paging List.</p> <p>For line keys: X ranges from 1 to 29 (for SIP-T48G). X ranges from 1 to 27 (for SIP-T46G). X ranges from 1 to 15 (for SIP-T42G/T41P).</p> <p>For programable keys: X=1-10, 12-14 (for SIP-T48G/T46G) X=1-10, 13 (for SIP-T42G/T41P)</p> <p>Example: linekey.1.type = 66</p>		

To enable multicast paging on a Yealink, set:

- linekey.2.type="66"

- multicast.paging_address.1.ip_address="224.5.6.20:10008"
- multicast.paging_address.1.label="Page All"

Each manufacturer's Administrator's or Provisioning Guide contains useful parameters for customizing phones. Best practices dictate that you read these guides for all lines of phones you intend to support.

Setting the Scope of a Parameter

Parameters can be set in different places depending upon to which phones you want the parameters applied.

Level	Description	To Set...
Brand	Applies to all phones in the brand. A good place to set common features and security for the devices.	Go to Configurations > Defaults > Select a Brand.
Model	Applies to the specific model of phone. Used for model specific features.	Go to System > Device Definitions.
<i>Domain</i>	Applies to phones in a specific domain. Useful for customer specific preferences (logos, ringtones), VLANs, and so on.	Go to Configurations > Defaults > Domain Specific, and then select or add the domain.
Handset/MAC	Applies to a specific handset. Useful for testing and user specific settings.	Click the Device Model field next to the MAC for the phone.

Entering a Brand Default

Brand defaults affect all phones for a specific brand. In this example, we'll apply the Polycom paging parameter to all Polycom phones.

1. In Endpoints Admin UI, go to **Configurations > Defaults > Polycom**.
2. Click **Add**.

>> **Polycom Defaults** >> Current Time : 17:25:52 on Sunday, 21st February 2016 GMT

Server ? : default

Parameter ? : ptt.pageMode.enable

Value ? : 1

Description ? : enable paging

Create Cancel

3. Complete the fields (see Table 2-2).
4. Click **Create**.

Table 2-2. Polycom Paging Parameters

Field	Description
Server	One Endpoints module can configure phones for many Core servers. You can select to set a parameter for a single or all (default) Core servers.
Parameter	The parameter to set on the phone (only the parameter, no = or value).
Value	The value to set on the phone (no quotes).
Description	Notes field.

Entering a Model Default

Model defaults affect all phones for a specific model. In this example, we'll apply the Polycom paging to only the VVX 310 phone.

1. In the Endpoints Admin UI, go to **System > Device Definitions**.
2. Click the **Model** field and select the VVX 310 phone.
3. In the **Overrides** field of the edit screen, enter the parameter using the format `parameter="value"`. To enter multiple parameters, place each parameter on a separate line.

Details

Brand : Polycom

Model : VVX 310

Type : Device

Force HTTPS : no

Allow TFTP : no

NDP code Structure : Polycom

of Phone Lines : 6

of FXS Lines : 0

of FXO Lines : 0

Supported # of Trunks : 0

Directory Enabled : yes

Presense Support : yes

SLA Support : yes

Sidecar Support : no

Resync Enabled : yes

Encrypt Support : yes

Firmware Support : yes

Available Firmware : sip5.3.0-vvx310.uc.ld,sip5.4.0-vvx310.uc.ld

Show in portal : yes

Overrides :
`ptt.pageMode.enable="1"`

Description :

Entering a Domain Default

Domain defaults affect phones only in a specific domain. The parameter only applies to the correct brand in that domain. For example, if a domain has both Yealink and Polycom phones, setting `ptt.pageMode.enable="1"` enables paging only on Polycom phones in that domain. Overrides for multiple brands can be mixed in one domain default entry.

In this example, we'll apply the Polycom paging to the testdomain on server "Corp at NYC."

1. In Endpoints Admin UI, go to **Configurations > Defaults > Domain Specific**.
2. Click **Add**.
3. Complete the fields (see Table 2-3).
4. Click **Create**.

The screenshot shows a form with the following fields and values:

- Server**: Corp at NYC
- Domain**: testdomain
- Parameters / Values**: ptt.pageMode.enable="1"
- Description**: (empty)

Buttons: Create, Cancel

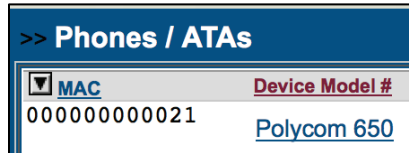
Table 2-3. Polycom Domain Parameters

Field	Description
Server	One Endpoints module can configure phones for many Core servers. You can select to set a parameter for a single or all (default) Core servers.
Domain	Select the domain to which the parameters will be applied.
Parameters / Values	Enter the parameters and values in format parameter="value" and separate multiple parameters on separate lines.
Description	Notes field.

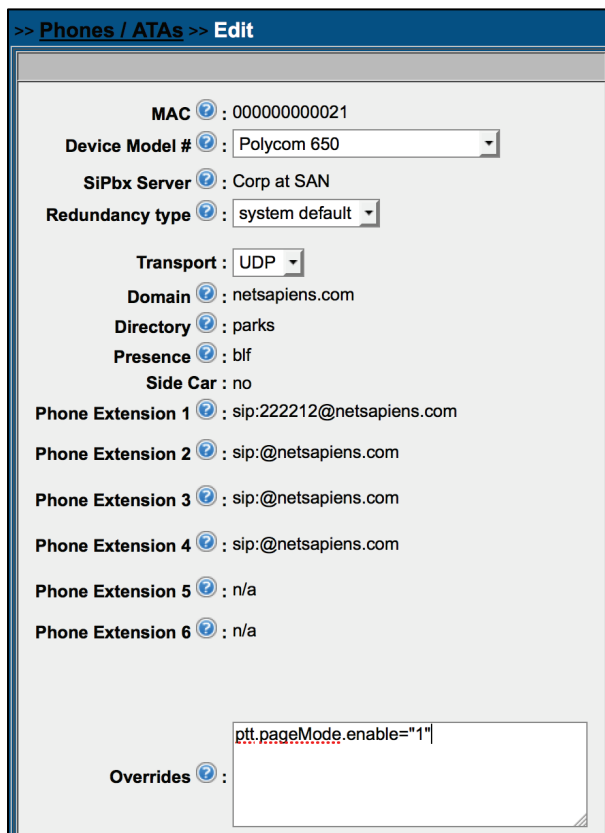
Entering a Handset/MAC Default

Handset defaults affect one specific phone only. In this example, we'll apply the Polycom paging override to the device with Media Access Control (MAC) address 000000000021.

1. In Endpoints Admin UI, go to **Configurations > Devices**.
2. Identify the device you want to edit, and then click the link below the **Device Model #** column.



3. In the **Overrides** field, enter the parameters and values using the format `parameter="value"`. Enter multiple parameters on separate lines.



4. Click **Modify**.

3. POLYCOM

Topics:

- ^ *Configuration Files (page 24)*
- ^ *How the Endpoints Module Decides Which Configuration File to Use (page 24)*
- ^ *Bootroms and Firmware (page 25)*

This chapter describes how to configure Polycom phones.

Configuration Files

Polycom has two configuration file formats:

- SIP
- UC

SIP is the older format used by firmware 3.2 and lower. UC is the newer format used by firmware 3.3 and later.

Table 3-1 shows which phones support which format. Some phones support both UC and SIP, and can load firmware of both generations.

Table 3-1. Matching Phones with the Configuration File Formats They Support

Model	SIP (Firmware 3.2 and Lower)	UC
SoundPoint 301, 430, 501, 601 SoundStation 4000	X	
SoundPoint 320,321, 330,331, 450, 550, 560, 650, 670 SoundStation 5000, 6000, 7000	X	X
VVX 1500	X	X
VVX models other than VVX 1500 RealPresence Trio		X

It is best to upgrade any SoundPoint and SoundStation to UC-compatible firmware. The reason is because they have more features, security fixes, and will be easier to manage, as they share the same parameters as the new VVX line.

How the Endpoints Module Decides Which Configuration File to Use

When the phone requests a configuration file, the Endpoints module responds with either a phone SIP or UC configuration file, depending on the following factors:

- If the phone model contains `vvx`, the UC format is used.
- If the override `UC="1"` is set in the Model Definitions or Handset/MAC overrides, the UC format is used.
- If the firmware assigned to the phone has `uc` in the filename (for example, `sip3_3.uc.ld`), the UC format is used.
- Otherwise, the SIP format is used.

Bootroms and Firmware

The following sections describe bootroms and firmware.

Bootroms

A bootrom is low-level software designed to power on the phone, start the network, and load the firmware. Separate bootroms files apply to phones running 3.3 firmware or lower. In UC4, firmware and bootroms are combined into one file. Depending on the version of firmware you want to load, you must have the proper bootrom loaded on the Endpoints module.

In the following example, we will load bootrom 4.3.1 for a SoundPoint 550, so the phone can use firmware 3.3.5.

1. Launch a browser, go to the Polycom website, and download the bootrom and release notes.
2. After the bootrom file is downloaded, unzip it.
3. Locate the unzipped folder, which will be a file full of bootroms named similarly to 3111-30900-001.bootrom.ld. In the release notes, find a table relating each model to the bootrom filename(s). In our example, we will load 2345-12500-001.bootrom.ld for the SoundPoint 550.
4. In the Endpoints module, go to **System > Files and Firmwares**, and then click **Upload File**.
5. Complete the fields (see Table 3-2).
6. Click **Start File Upload** and wait for the upload to complete. Polycom phones request a new bootrom automatically by exact filename at each boot. Therefore, load the filename without renaming it. All phones on your Endpoints module must run the same bootrom version.

Table 3-2. SoundPoint 550 Bootrom Upload File Settings

Field	Description
Filename	Filename for the firmware once uploaded. For bootroms, do not rename the files. In our example, we type 2345-12500-001.bootrom.ld.
File to upload	Click Browse... and select the file to upload.

Firmware

Loading firmware is a lot like loading bootroms. However, you can rename the firmware file and assign different firmware versions to the same model phone.

Split or Combined Firmware

Polycom offers each firmware in two formats:

- Split
- Combined

The split file breaks out each model's firmware into separate files. The combined file is one file that contains firmware for all compatible phones. While using a combined file sounds easier to use than using a split file, the combined file is large (around 300 MB). A split file, by comparison, is about 45 MB. If you have a large number of phones upgrading at the same time, using split files can save time and resources.

Uploading Firmware

In this example, we will load firmware 5.4.2 rev D for a VVX 310 phone.

1. Launch a browser, go to the Polycom website, and download the split firmware and release notes.
2. After the firmware file is downloaded unzip it.
3. Locate the unzipped folder, which will be full of firmware files, named something like 3111-30900-001.sip.ld.
4. In the release notes, find a table relating each model to the firmware filenames. In our example we must load 3111-46161-001.sip.ld for the VVX 310.
5. In the Endpoints module, go to **System > Files and Firmwares**, and then click **Upload File**.
6. Complete the fields (see Table 3-3).
7. Click **Start File Upload** and wait for the upload to complete.

Table 3-3. SoundPoint 550 Firmware Upload File Settings

Field	Description
Filename	Filename for the firmware once uploaded. For firmware, you can rename the files, so for easier organization we could rename it sip5.4.2d-vvx310.uc.ld
File to upload	Click Browse... and select the file to upload

Adding Firmware to the Device Definitions

After firmware is uploaded, you must add it to the device definitions, so it can be loaded to phones. The Endpoints module can have multiple firmware versions loaded for each phone and you can select which version for each handset/MAC.

1. Go to **System > Device Definitions** and select the phone you want to edit (vvx 310 in our example).
2. In the **Available Firmware** field, enter the filename of the firmware uploaded to make it available to the phone. If you want different versions as options, create a comma-separated list of each filename. The first firmware on the list will be the “model default” that will be the firmware provided to all phones of that model, unless another version is specified.

Brand	:	Polycom
Model	:	VVX 310
Type	:	Device
Force HTTPS	:	no
Allow TFTP	:	no
NDP code Structure	:	Polycom
# of Phone Lines	:	6
# of FXS Lines	:	0
# of FXO Lines	:	0
Supported # of Trunks	:	0
Directory Enabled	:	yes
Presence Support	:	yes
SLA Support	:	yes
Sidecar Support	:	no
Resync Enabled	:	yes
Encrypt Support	:	no
Firmware Support	:	yes
Available Firmware	:	sip.5.4.2d-vvx310.uc.ld,sip.5.4.1-vvx310.uc.
Show in portal	:	yes
Overrides	:	
Description	:	

3. Click **Create**.

Selecting Firmware

By default, the phone gets the first firmware in the **Available Firmware** list. To select a different firmware:

1. In Endpoints Admin UI, go to **Configurations > Devices**.
2. Identify the device you want to edit, and then click the link in the **Used Lines** column.

3. In the device edit page, find the firmware entry where you can select a specific firmware for the device.

Firmware ? :	Model Default
Auth User :	Model Default
Auth Pass :	sip5.3.0-vvx310.uc.ld
	sip5.4.0-vvx310.uc.ld

Upgrading Soundpoint Phones to UC4

Upgrading a Soundpoint phone from version 3 software to UC4 follows the standard directions; however, the bootrom is called the Polycom Upgrader 4.4.0 Utility.

1. Launch a browser, go to the Polycom website, and download the Polycom Upgrader 4.4.0 Utility.
2. Follow the bootrom directions to load the utility to Endpoints module.
3. Download the desired UC4 firmware from the Polycom website.
4. Follow the firmware directions to load the firmware to the Endpoints module. Generally, you set the UC4 firmware as the model default.
5. Reboot the phones and wait for the upgrade to complete.

For more information, refer to the Polycom Engineering Advisory 64731.

Downgrading Soundpoint Phones from UC4

Downgrading a Soundpoint phone from UC4 software to UC4 largely follows the standard firmware directions; however, the firmware is called the “Polycom UC Downgrader 4.5.0b Utility.”

1. Download the Polycom UC Downgrader 4.5.0b Utility and follow the firmware directions to load it to the Endpoints module.
2. After the downgrader firmware is uploaded, select it as the active firmware for any phones you want to downgrade.
3. Reboot the phones, and then wait for the upgrade to complete.
4. When the phone downgrader completes, the phone will be running UC3.3.2 firmware and 4.5.0 bootrom.

For more information, refer to the Polycom Engineering Advisory 64731.

Which Firmware Version Should I Run?

NetSapiens completed Polycom's VIP Test plan using select VVX models running firmware version 5.3 and SoundPoint models running firmware version 4.0.9. These firmware versions are a good place to start. However, new versions of firmware include security improvements, bug fixes, and new features. In addition, new phone models, such as the VVX refresh phones, D60, and RealPresence Trio, require newer firmware.

Before deploying new firmware to customers, we recommend you:

- Keep a lab of your most commonly sold phones before deploying new firmware to customers.
- Test the new firmware with your lab phones against your standard system/network configurations.

4. YEALINK

Topics:

- ^ *Configuration Files (page 32)*
- ^ *How the Endpoints Module Decides Which Configuration File to Use (page 32)*
- ^ *Firmware (page 33)*

This chapter describes how to configure Yealink phones.

Configuration Files

Yealink has three configuration file formats. Yealink and NetSapiens have a different naming method for each format, shown in Table 4-1.

Table 4-1. Yealink Common File Names

Yealink Name	NetSapiens Name
M1	Yealink
M2	Yealink2
M7	Yealink3

Depending on the firmware used and the phone model, different configuration files should be used (see Table 4-2).

Table 4-2. Matching Configuration Files with Yealink Phones

Yealink Phone	6x Firmware	7x and 8x Firmware
T2x Series	Yealink (M1) format	Yealink3 (M7) format
T3x Series	Yealink2 (M2) format	Yealink2 (M2) format
T4x Series	n/a	Yealink3 (M7) format

Upgrading T2x series to 7x firmware is easier because most devices can run the same Yealink3 format.

How the Endpoints Module Decides Which Configuration File to Use

Selecting a configuration file format is set as a parameter of each model definition. To review and change configuration file formats:

1. In the Endpoints module Admin UI, go to **System>Device Definitions**.
2. In the list of device definitions find the **NDP Code Structure** column, which specifies the configuration format that the model will use.
3. Edit the device to change the code structure used for that model.
4. To support two different code structures for the same model, create a second device definition for that model, one for each code structure. For more information, see Chapter 5.

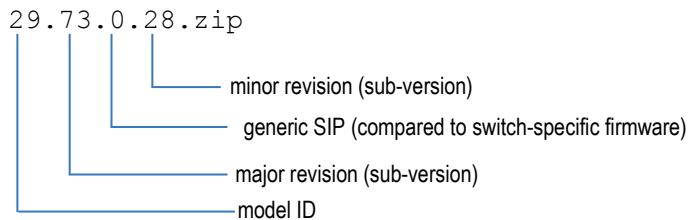
Details	
Brand	Yealink
Model	SIP-T42G
Type	Device
Force HTTPS	no
Allow TFTP	no
NDP code Structure	Yealink3

Firmware

Selecting the Right Firmware

Yealink firmware is available in the support section of the company webpage. Traditionally, firmware file names resemble `29.73.0.28.zip`, but newer ones resemble `T42-29.80.0.95.zip`.

Selecting the right firmware can be tricky. The following figure shows how to decode firmware files for a T42:



Uploading Firmware

In this example, we will load firmware `29.73.0.28.zip` for a T42.

1. Launch a browser, go to the Yealink website, and download the firmware file.
2. Unzip the firmware file. After the file is unzipped, you'll have a file similar to `29.73.0.28.rom`.
3. To load the new file to the Endpoints module, go to **System > Files and Firmwares**, and then click **Upload File**.
4. After you complete the fields, click **Start File Upload** and wait for the upload to complete.

Table 4-3. Yealink Firmware Upload File Settings

Field	Description
Filename	Filename for the firmware once uploaded. For firmware, you can rename the files, so for easier organization we could rename it t42-29.73.0.28.rom.
File to upload	Click Browse... and select the file to upload.

Selecting Firmware

After you upload the firmware, add an override to tell the phone which file to use. We set this as a model default in Device Definitions, although it can also be set as a Handset/MAC override. To do so, the override is `firmware.url="http://<Endpoints-FQDN>/frm/<filename>"`.

Do not set `firmware.url` as a brand or domain default because it could apply firmware to a different phone model.

Details

Brand: Yealink

Model: SIP-T42G

Type: Device

Force HTTPS: no

Allow TFTP: no

NDP code Structure: Yealink3

of Phone Lines: 3

of FXS Lines: 0

of FXO Lines: 0

Supported # of Trunks: 0

Directory Enabled: yes

Presense Support: yes

SLA Support: yes

Sidecar Support: yes

Resync Enabled: yes

Encrypt Support: no

Firmware Support: no

Available Firmware:

Show in portal: yes

Overrides: `firmware.url="http://endpoints.acmetelco.com/firm/t42-29.73.0.28.rom"`

Description: SIP-T42G

Upgrading from 6x to 7x Firmware

To upgrade phones running version 6x firmware to version 7x firmware, send the phone a Yealink/M1 format configuration file with the new firmware information. The following procedure describes the easiest way to perform this step, but there are other ways to do this.

When booting a Yealink phone, the phone looks for a common or “y” file. For a T26, the filename is `y0000000000004.cfg`.

Note: The common file number does not correlate with the firmware model number.

In this file, you can place commands in the Yealink/M1 format to upgrade to new firmware.

Table 4-4. Yealink and NetSapiens Configuration File Naming Methods

Model	Common File Name
T18	y0000000000009.cfg
T20	y0000000000007.cfg

Model	Common File Name
T22	y000000000005.cfg
T26	y000000000004.cfg
T28	y000000000000.cfg

The following is a template of the common file contents for upgrading firmware:

```
[ firmware ]
path = /tmp/download.cfg
server_type = http
server_ip = <Your-Endpoints_IP>
server_port = 80
login_name =
login_pswd =
http_url = http://<Your-Endpoints_IP>/frm/
firmware_name = <filename>.rom
```

1. Copy and paste the above into a plain-text file.
2. Replace <Your-Endpoints_IP> with the IP or FQDN of your Endpoints module.
3. Replace <filename>.rom with the filename of the 7x firmware for the specific phone model.
4. Save the file with the common file name and upload to **Files and Firmware** section in the Endpoints Admin UI.
5. Reboot the phones to have them apply the new firmware.

For more information, refer to the V70 Upgrading Manual, which you can download from the Yealink website.

Which Version Firmware Should I Run?

NetSapiens completed Yealink’s Compatibility Test plan using select models running firmware versions 72 and 73. However, new firmware versions include security improvements, bug fixes, and new features. In addition, new phone models (T49g, and so on) require newer firmware.

Before deploying new firmware to customers, we recommend you:

- Keep a lab of your most commonly sold phones before deploying new firmware to customers.
- Test the new firmware with your lab phones against your standard system/network configurations.

5. DEALING WITH NEW DEVICES

Topics:

- ^ *Running a New Device Not in the Device List (page 39)*
- ^ *New Device with an Existing Format (page 39)*
- ^ *New Device without an Existing Format (page 42)*

Eventually you may want to run a new device that isn't in the device list. This chapter describes how to deal with new devices.

Running a New Device Not in the Device List

There might be situations when you want to run a new device that is not in the device list. There are two cases for this situation:

- The new device uses the same configuration file as other provisionable devices. For example, Polycom releases a VVX 800 that uses the same UC configuration format as other VVX phones.
- The new device uses a different configuration file than other provisionable devices. For example, the Algo door phone does not use the same format or parameters as other devices.

Generally speaking new devices in the same brand use the same configuration file format. But there are exceptions, which can be solved with the Custom File Format.

Phones that are not from the same brand as other provisionable devices likely will need a custom file format.

New Device with an Existing Format

For devices that use the same configuration file format as other phones, adding a new device configuration is fairly simple.

1. In the Endpoints Admin UI, go to **System > Device Definitions**, and then click **Add**.
2. Complete the fields (see Table 5-1).
3. Click **Create**.

After a new configuration is defined, the Endpoints module is ready to configure the new phone model.

Brand :

Model :

Type : Device

Force HTTPS : no

Allow TFTP : no

NDP code Structure : Aastra

of Phone Lines : 0

of FXS Lines : 0

of FXO Lines : 0

Supported # of Trunks : 0

Directory Enabled : no

Presense Support : no

SLA Support : no

Sidecar Support : no

Resync Enabled : no

Encrypt Support : no

Firmware Support : no

Available Firmware :

Show in portal : no

Overrides :

Description :

Create Cancel

Table 5-1. Configuring a New Device with an Existing Format

Field	Description
Brand	Brand of the phone. Be sure to match existing phones of the same brand (for example, Polycom).
Model	Model of the phone (for example, VVX 900).
Type	<ul style="list-style-type: none"> • Device = phones and small ATAs (1-2 ports). • AnalogGW = analog gateways. • DigitalGW = digital gateways.
Force HTTPS	Force phone to provision via HTTPS.
Allow TFTP	Allows phone to provision via TFTP. Recommended to set no for all phones aside from those that only support TFTP.
NDP Code Structure	Compatible configuration file code structure the phone will use (for example, Polycom for Polycom phones and Yealink3 for new Yealink phones).
# Phone Lines	Number of phone lines the device supports. Refer to the manufacturer's device specifications to confirm the value. Maximum is 8.

Dealing with New Devices

Field	Description
# of FXS Lines	If Type is set to AnalogGW, specify the number of FXS lines the device supports. Refer to the manufacturer's device specifications to confirm the value. Maximum: 24 combined FXO and FXS lines.
# of FXO Lines	If Type is set to AnalogGW, specify the number of FXO lines the device supports. Refer to the manufacturer's device specifications to confirm the value. Maximum: 24 combined FXO and FXS lines.
Supported # of Trunks	If Type is set to AnalogGW, specify the number of trunks the device supports.
Directory Enabled	Select yes to enable the Endpoints module to generate directory/BLF for the phone. The Endpoints module must support directory generation for the specified code structure.
Presence Support	Select yes to enable BLF/Presence on the phone, Directory Enabled must also be set yes.
SLA Support	Select yes to enable Shared Line Appearance (SLA) if desired. SLA is only supported on select brands like Polycom and Yealink. (others?)
Sidecar Support	Enable Sidecars (Expansion Modules). This selection is used by Yealink3 only. Other brands support sidecars, but Yealink handles them differently and requires this setting to be enabled if sidecar support is desired.
Resync Enabled	Select yes if the device supports resync. This setting allows the SNAPsolution to force the phone to pull a new configuration. Most new devices support resync.
Encrypt Support	Select yes to enable the brand-specific configuration file encryption tool. Available for select brands like Cisco/Linksys SPA and older Grandstream phones.
Firmware Support	Enables advanced firmware management for Polycom, and Cisco only. See Chapter 3 for implementation details.
Available Firmware	If Firmware Support is enabled, enter a comma-separated list of firmware filenames loaded to Files and Firmwares, which are compatible with the phone.
Show In Portal	<ul style="list-style-type: none"> • Yes = shows the phone in Portal. • No = hides the phone in the Portal.
Overrides	Parameters and values to apply to the phone model.
Description	Notes field.

New Device without an Existing Format

The custom file format allows you to provision nearly any brand of phone by defining your own configuration file formats.

This works by allowing you to take a properly formatted configuration file template for a given device, and then add wildcards that the Endpoints module completes with values such as the proxy and user to make an operational configuration file.

Observe the following guidelines:

- Compatible devices are those that accept a text/XML configuration file. Binary or encrypted configuration files are not supported.
- You must run Endpoints module version 1225 or later.
- The new API must be used for the Core connection (see Chapter 7 if unsure).
- Brand defaults and device/model/MAC overrides do not apply to custom format-provisioned devices.
- Directories are not available to be applied to custom format provisioned devices.
- Custom formats can configure a maximum of eight lines on a device.
- Use a plain-text editor such as Notepad++ to edit and save configuration files. Do not use programs such as Microsoft Word, which add extra formatting.

Making the Configuration File

To make the configuration file:

1. Obtain a configuration file for the device in question. The easiest way to start is to provision the device manually, and then export the configuration. If this is not an option, obtain the provisioning file format from the manufacturer.
2. Edit the file with the default values you want applied to all phones (admin password, registration period, and so on). Fill in the wildcards for fields such as user, password, domain, and outbound proxy. The list of wildcards is shown below:

```
[[outboundproxy_1]] - primary proxy
[[outboundproxy_2]] - backup proxy
[[outboundpostfix_1]] - primary server postfix when using geo (commonly used as
[[domain]].[[outboundpostfix_1]]) [[outboundpostfix_2]] - secondary server postfix when using geo
[[outbound_port_1]] - the SIP port of the proxy
[[outbound_port_2]] - the SIP port of the backup proxy
[[domain]] - customer domain
[[device_n]] - device/auth AOR
[[device_pass_n]] - auth password
[[user_n]] - owner user
[[name_n]] - owner name
[[time_zone_name]] - time zone in format like US/Eastern
[[time_zone_offset]] - time zone in format like -5
[[time_zone_minutes]] - time zone in minutes from GMT like -480
[[time_zone_abbreviation]] - time zone as abbreviation like PST, MST
[[random10]] - random integer with max value 10
[[random60]] - random integer with max value 60
[[random600]] - random integer with max value 600
[[random3600]] - random integer with max value 3600
```

The following excerpt shows a configuration file for an Algo SIP Alerter:

```
admin.devname = doorphone
admin.pwd = g00dpass
sip.obproxy = [[outboundproxy_1]]
sip.proxy = [[domain]]
sip.regexp = 60
sip.u1.auth = [[device_1]]
sip.u1.pwd = [[device_pass_1]]
sip.u1.user = [[user_1]]
```

Some parameters have wildcards, while others do not. The registration interval `sip.regexp`, for example, is the same for all devices. Other parameters, such as `sip.proxy`, have a wildcard because that value varies, depending on the domain assigned.

Creating a New NDP Code Type

After you create a new template:

1. Upload the file with any name into the **NDP Files and Firmware** section.
2. In the Endpoints Admin UI, go to **System > Custom Formats**, and then click **Add**.
3. Specify the name of the format and filename you uploaded previously, and then click **Create**.

>> **Custom Definitions** >> Current Time : 23:38:05 on Thursday, 2nd April 2015 GMT

Format Name :

Template :

Now that the format is set, you can follow the directions under “New Device with an Existing Format” on page 39 to add the device definition.

Loading the Configuration File

Now that the configuration is made, add the device’s MAC like any normal device (see Adding a Phone on page 12). In the device interface, look for the provisioning server configuration (varies by make/model) and point the device to your Endpoints module.

Managing Pre/Postfix on the Requested Configuration File

If the phone doesn’t configure:

1. In the Endpoints module, go to **Diagnostics > Events**.
2. Look for the configuration file that the phone requested. The Endpoints module must be aware of the pre/postfix to strip from the filename to derive the MAC address. Common pre/postfixes that are already stripped include `.cfg`, `.conf`, `.html`, and `poly-`.
3. If the phone has an unusual pre/postfix, such as `foo000000000012.bar`:
 - d. Go to **System > Configuration**.
 - e. Add the unusual values (for instance, `foo` and `bar` in our example) as a comma-separated list to the configuration parameter **PreParseStrip**, as shown below:

>> **Configuration** >> Configuration Add Current Time : 0:11:43 on Friday, 3rd April 2015 GMT

Configuration Add

Parameter ? :

Value ? :

6. DIRECTORIES

Topics:

- ^ *Types of Directories (page 46)*
- ^ *Selecting a Directory (page 46)*
- ^ *Creating a Custom Directory in the Directory Designer (page 48)*

This chapter describes directories. Directories allow BLFs to be sent to select Cisco/Linksys SPA phones, Grandstream GXP, Panasonic UT series, and Polycom phones.

Types of Directories

Table 6-1 lists the types of directories.

Table 6-1. Types of Directories

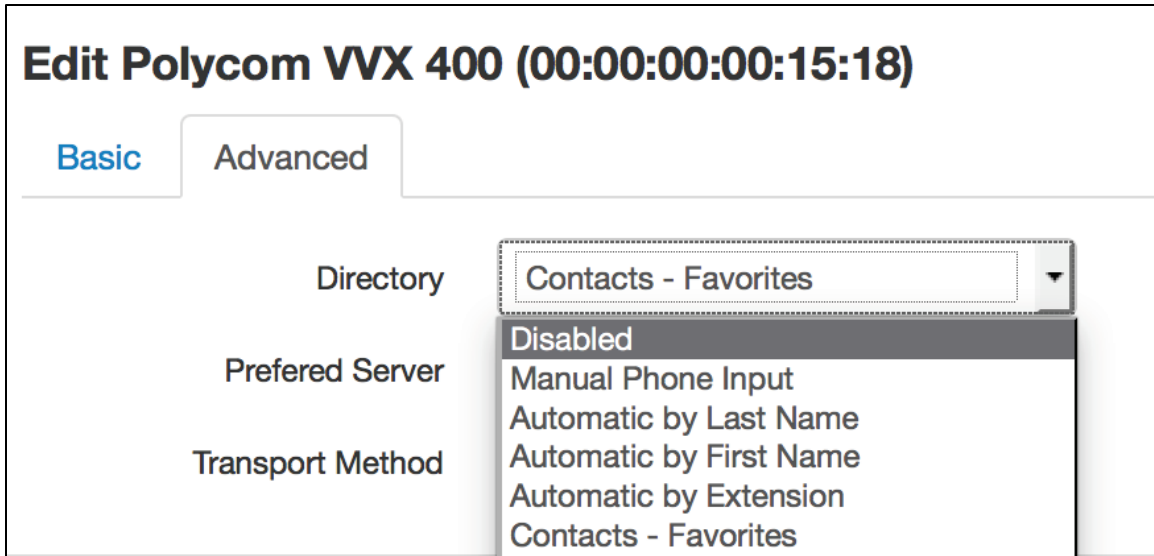
Portal Name	Endpoints Admin UI Name	Description
Disabled	Disabled	No directory will be provided to the phone.
Manual Phone Input	Local only	Allows the directory to be added using a phone instead of the Endpoints module.
Automatic by Last Name	Automatic by lastname	Auto-generated directory sorted by last name in a-to-z order.
Automatic by First Name	Automatic by firstname	Auto-generated directory sorted by first name in a-to z order.
Automatic by Extension	Automatic by extension	Auto-generated directory sorted by extension number in ascending order.
Contacts – Favorites	User's contacts	Directory made of favorited contacts.
Custom - XXXX	XXXX	Directory generated by the directory designer. XXXX is the name of the directory you create. This option does not appear if there are no directories created by directory designer.

Selecting a Directory

Directories can be selected using the Portal or the Endpoints Admin UI.

Using the Portal to Select a Directory

1. In Inventory, edit the phone.
2. Click the **Advanced** tab.
3. In the **Directory** field, click the directory that you want to apply to the phone.
4. Click **Save**.











Using the Admin UI to Select a Directory

1. In the Admin UI, click **Configurations > Devices** for the phone you want to edit.
2. Below the **Directories** column, click a link.

The Admin UI also provides a **Presence** toggle that might show the following options:

- **BLF** – shown for Polycom only. Select this option for UC firmware (defaults to BLF for VVX).
- **Enabled** – configures presence (like BLF) to show on the phone.
- **Disabled** – no presence status appears for directory entries.

MAC  : 000000001518
Device Model #  : Polycom VVX 400
Redundancy type  : force primary ▾
Transport : UDP ▾
Domain  : kevin.netsapiens.com
Directory  : user's contacts ▾
Presence  : disabled
Side Car : automatic by lastname
Phone Extension 1  : automatic by firstname om
Phone Extension 2  : automatic by extension
 : user's contacts
 : local only
 : blank

Creating a Custom Directory in the Directory Designer

Directory Designer allows you to create custom directories with more flexibility than the automatic directories.

To create a custom directory:

1. In the Endpoints Admin UI, go to **Configurations > Directory Designer**.
2. Click **Add**.
3. Complete the fields (see Table 6-2).

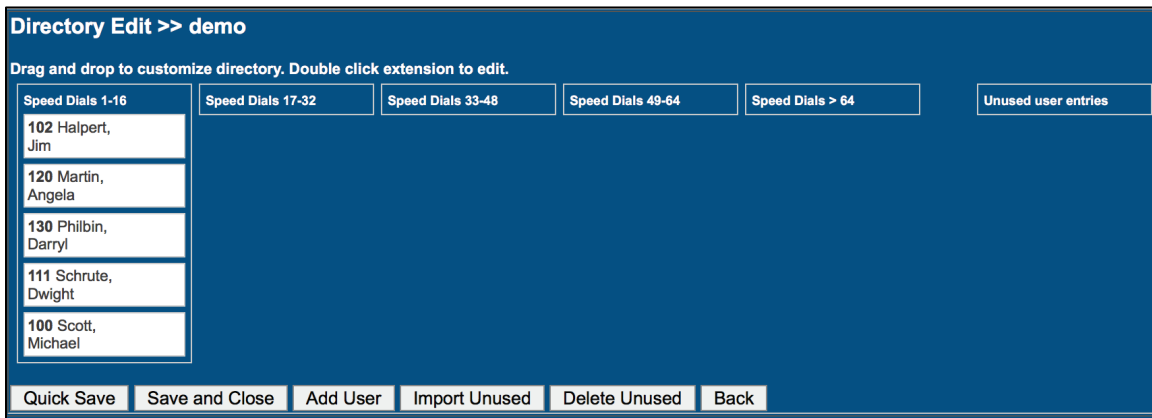
Table 6-2. Fields for Creating a Custom Directory

Field	Description
Directory Name	Name of the directory.
Domain	Server and domain to which the directory will apply.
Description	Notes field.
Creation Assistance	Will help autofill entries from the domain. Choices are: <ul style="list-style-type: none"> • Insert alphabetical = adds entries for domain users as active sorted by last name • Insert by Extension = adds entries for domain users as active sorted by extension • Insert as Unused = adds entries for domain users but makes them inactive • None = blank directory .

4. Click **Create**.

After you create a directory, you return to the directory listing, where you can modify your directory by clicking **Modify Directory**.

When you edit a directory, a screen similar to the following appears.



The directory shows the list of users in the first five columns (these columns show the order, but not necessarily the column placement on the phone). The **Unused user entries** column allows you to place users you want to remove, but not delete, from the directory.

To rearrange users, drag and drop them in order between the **Speed Dials** columns and **Unused user entries** column.

Table 6-3 describes the buttons at the bottom of this page.

Table 6-3. Buttons for Creating a Custom Directory

Button	Description
Quick Save	Saves the directory, but allows you to continue editing.
Save and Close	Saves the directory and redisplay the main directory listing.
Add User	Allows you to add a new directory entry.
Import Unused	Imports new users from the Core user listing.
Delete Unused	Removes entries listed in the Unused user entries column.
Back	Redisplay the directory list without saving.

Note: These directories do not update automatically. If you rename user 100 from Betty to Susan in the Portal or Core Admin UI, for example, the directory does not automatically reflect the change.

7. CONNECTING TO CORES

Topics:

- ^ *Validating API Version (page 52)*
- ^ *Geo Clusters (page 52)*
- ^ *Adding a New Core Node to the Endpoints Module (page 53)*
- ^ *How Geo Redundancy (page 56)*

While your Endpoints module should already be connected to your Core Modules, we'll still review how this feature is configured.

This chapter describes how the Endpoints module acquires information about users and registration credentials, along with defining geo clusters.

Validating API Version

The Endpoints modules and Core(s) can communicate via the old or new API.

To check which is being used:

1. In the Endpoints Admin UI, go to **System>Configuration**.
2. Look for the parameter **useOAuth**:
 - If **useOAuth** is set to yes, the new API is being used.
 - If **useOAuth** is missing or set to no, the old API is being used.

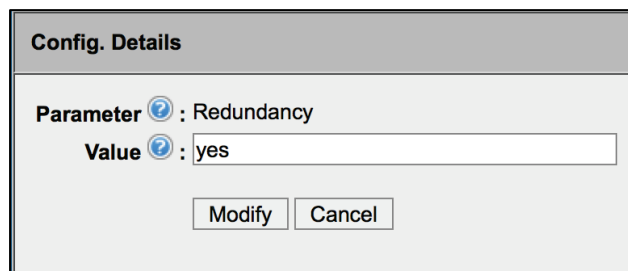
Note: Systems running version 1225 or later of the Endpoints module should use the new API.

Geo Clusters

While phones have a primary Core assigned to them, enabling geo-redundancy allows the phone to be programmed with other Core(s) in the cluster in case its primary Core suffers an outage.

If you have geo-redundant Cores:

1. In the Endpoints Admin UI, go to **System > Configuration**.
2. Ensure that the parameter **Redundancy** is set to **yes**.



The screenshot shows a dialog box titled "Config. Details". Inside the dialog, there is a section for "Parameter" with a question mark icon, showing "Redundancy". Below that, there is a section for "Value" with a question mark icon, showing "yes" in a text input field. At the bottom of the dialog, there are two buttons: "Modify" and "Cancel".

The group itself is defined in the Endpoints Admin UI:

1. Go to **Configuration > SiPbx Servers**.
2. In the column **Redundancy Group**, any Core that shares the same value of the Redundancy Group field is part of the same geo cluster.

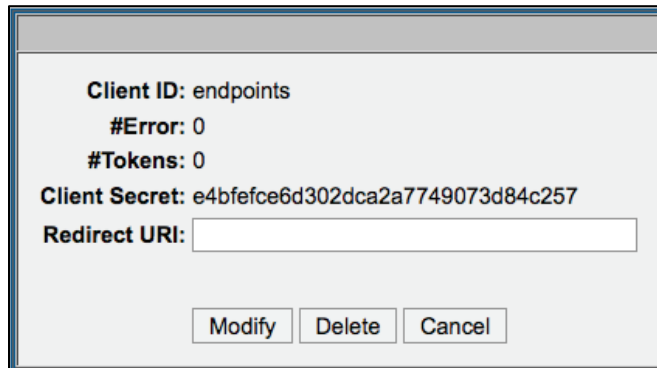
Redundancy Group
alpha
alpha

Adding a New Core Node to the Endpoints Module

To add a new Core node to Endpoints module, collect information from the Core and ensure its configured properly.

Preparing the Core

1. In the Admin UI of the Core Module, go to **System > Settings > Advanced > Oauth Clients**.
2. Identify an existing Oauth credential for the Endpoints module or create a new one.
3. Copy the Client ID and Client Secret.



The screenshot shows a configuration window for an Oauth Client. It contains the following text: Client ID: endpoints, #Error: 0, #Tokens: 0, Client Secret: e4bfefce6d302dca2a7749073d84c257, and a text input field for Redirect URI. At the bottom, there are three buttons: Modify, Delete, and Cancel.

4. Go to **Users > Configuration** and edit or create a User with a Scope of NDP.
5. Copy and retain the Login Name.
6. Copy and retain the PIN.

User Name:	endpointsuser
Domain:	NSTEST
First Name:	
Last Name:	
Login Name:	<User Name>@NSTEST
E-Mail:	
PIN:	272535485
Dept.:	n/a
Site:	n/a
Dir Match By:	Last Name
Dir Ord:	1
Dir Anc:	no
Dir Lst:	Yes
Time Zone:	US/Pacific
NoAns T/O(s):	25
Rej Anonymous:	No
VMail Prov:	Yes
VMail U-Ctrl:	Yes
Data Limit:	10 MB
Call Limit:	Unlimited
Caller ID Name:	[*]
Caller ID Number:	[*]
911 Caller ID:	[*]
Area Code:	
Privacy:	No
Dial Translation:	Cloud PBX Features
Dial Permission:	US and Canada
Scope:	NDP

Adding the Server to the Endpoints Module

The last step is to add the server to the Endpoints module.

1. In Endpoints Admin UI, go to **Configurations > SiPbx Servers**.
2. Click **Add**.
3. Complete the fields (see Table 7-1).
4. Click **Create**.

Table 7-1. Fields in the Add Dialog Box

Field	Description
Server Name	Arbitrary name for the node.
Hostname	Fully qualified domain name or IP address of the node (for example, core1-pdx.mycompany.com).
DNS Postfix	For Geo use only. DNS record set up with a wildcard for this node (typically, the same as the hostname).
Database hostname	Hostname of the database for Core (typically, the same as the hostname).
UDP port	SIP UDP port. Default is 5060.
TCP port	SIP TCP port. Default is 5060.
TLS port	SIP TLS port. Default is 5061.
SiPbx DB	Database name of the Core's database. Default is SiPbxDomain,
User	User for the database. Default is dbSiPbx.

Field	Description
Password	Password for the database. Default is sipbx.
NsApi FQDN/IP	Fully qualified domain name or IP address of the server running the API (typically, the same as the hostname).
NsApi client_id	Client ID entered in the previous step.
NsApi client_secret	Client secret generated in the previous step.
NsApi oauth_username	The user@domain created in the previous step.
NsApi oauth_password	Password for the user created in the previous step.
Redundancy Group	For Geo use only. Label for the cluster for Cores. If this new Core is part of an existing cluster, enter the same label assigned to those nodes. Otherwise, enter an arbitrary string.
Allow Failover to this server	For Geo use only. Choices are: <ul style="list-style-type: none"> • Yes = this can be a secondary Core to a phone in the same redundancy group. • No = this is not assigned as a secondary Core to phones in the same redundancy group, but can still be assigned as a primary Core.
Latitude	No longer supported.
Longitude	No longer supported.
Location	Notes field.
TLS Cert data	When using TLS only, enter TLS certificate content from the certificate loaded on Core.
TLS CA data	When using TLS only, enter TLS CA content from the CA file loaded on Core.

How Geo Redundancy Works

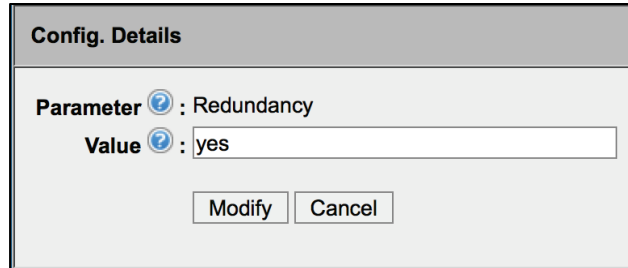
If you have geo-redundant Cores, your phones are automatically provisioned differently to support this feature. Some phones accomplish this via service (SRV) records, while others use a primary and backup proxy.

Phones like Cisco and Grandstream use the SRV record method. The SRV record `core.mycompany.com`, for example, would contain DNS information for each Core in the cluster, along with a priority. These phones register to the highest priority Core available. Each phone manufacturer decides when to consider a Core unavailable and switch to a backup Core, as well as when to switch back if a higher priority Core becomes available again.

Other phones, like Polycom and Yealink (NDP 1225 or later), will dual register, maintaining constant registration to two Cores. This has an advantage of faster recovery in case of failure, but generally limits redundancy to two Cores only.

Yealink phones allow you to force SRV instead of dual registration (see Chapter 10).

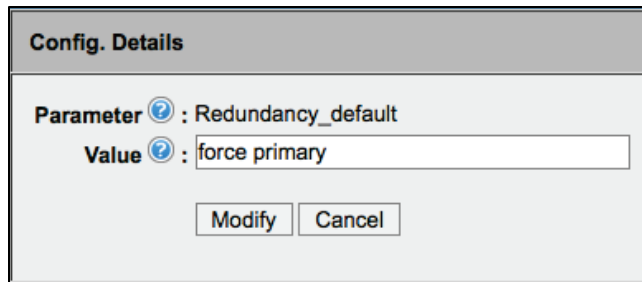
If you have geo-redundant Cores, you can configure redundancy settings in the Endpoints Admin UI by going to **System > Configuration** and setting the value of the parameter **Redundancy** to **yes**.



The screenshot shows a dialog box titled "Config. Details". It contains two fields: "Parameter" with a help icon and the value "Redundancy", and "Value" with a help icon and the value "yes". Below the fields are two buttons: "Modify" and "Cancel".

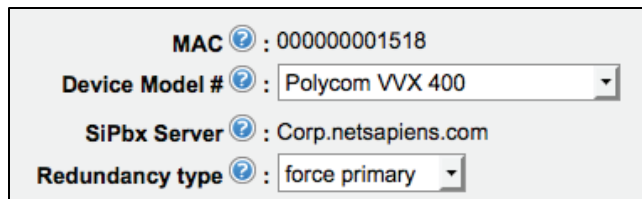
The parameter **Redundancy_default** sets the default redundancy method. Acceptable values are:

- **none** = disables geo.
- **force primary** = enables geo.



The screenshot shows a dialog box titled "Config. Details". It contains two fields: "Parameter" with a help icon and the value "Redundancy_default", and "Value" with a help icon and the value "force primary". Below the fields are two buttons: "Modify" and "Cancel".

When editing a MAC, you can override the default redundancy setting for the specific phone.



The screenshot shows a configuration form with four fields: "MAC" with a help icon and the value "000000001518", "Device Model #" with a help icon and a dropdown menu showing "Polycom VVX 400", "SiPbx Server" with a help icon and the value "Corp.netsapiens.com", and "Redundancy type" with a help icon and a dropdown menu showing "force primary".

8. SECURITY

Topics:

- ^ *SAFE (page 59)*
- ^ *Handset Security (page 59)*
- ^ *Password Protecting Files (page 60)*
- ^ *Disabling TFTP (page 61)*
- ^ *Secure Admin Login (page 61)*

The Endpoints module provides configuration files containing registration credentials. As a result, it is important to secure your system to prevent hacking.

SAFE

SAFE is an intelligent filter that protects configuration files from dictionary attacks. SAFE monitors requests for configuration files, and then adds to the score of the requester IP address if they request a file for a MAC that does not exist. Files such as license files and zero files are ignored.

SAFE was added in version 1224 and is enabled by default. To customize this setting:

1. In the Endpoints Admin UI, go to **System > Configurations**.
2. The following parameters can be set to configure SAFE:
 - **SAFE_whitelist** = comma-separated list of IP addresses that will not be part of this logic. To disable filtering, select *.
 - **SAFE_error_empty** = yes returns an empty 200 ok message instead of a 403 message on error.
 - **SAFE_error_500** = yes returns a 503 message instead of a 403 message on error.
 - **SAFE_MaxFraudScore** = maximum number of fail attempts permitted before a permanent IP block is in place. Default is 50 (version 1225+).

Reviewing the SAFE Fraud Scores

SAFE versions 1225 and later allow you to see the current status of SAFE fraud scores:

1. Go to **Diagnostics>Fraud Scores by IP**.
2. To clear the fraud score for the IP, click **Allow** under the **Action** column.

>> IP List <input type="text" value="Filter:"/> <input type="button" value="Refresh"/> Refreshed: Tue 2016-03-08 18:05:39 GMT -8			
IP	Status	Score	Action
63.224.54.246	no block	2	Allow

Handset Security

Gaining registration credentials through handsets is the most common attack vector on any system. To combat this vulnerability:

- Disable all local interfaces on the phone (web, Telnet, SSH, and so on), as local configuration is generally not necessary with the Endpoints module.

- Change the default passwords on phones and deploy them whenever possible behind a NAT firewall rather than with a public IP.

Password Protecting Files

This option requires the phone to authenticate when requesting a configuration file. While this security measure is powerful, it is more difficult to deploy because each phone must be preconfigured with this information. If you use this feature, prepare your system prior to enabling this feature; otherwise, provisioning will fail.

Updating Deployed Phones

For phones already deployed, you can assign the username and password using overrides and forcing a resync/reboot of the phones. For specific parameters, refer to the manufacturer's admin or provisioning guide.

Be sure to check the valid input range for the provisioning username and password on each phone, then select a username and password for the system that are within the input ranges for all phone brands you use. For example, if Panasonic allows you to enter up to 128 characters as the password, but Yealink allows only 32 characters, set your password to 32 characters or less to support both phones.

Provisioning New Phones

For future deployment of phones, the best way to assign usernames and passwords is to use a pre-provisioning service, such as Polycom ZTP and Yealink RPS. Doing so ensures that phones will automatically fetch this information, even after they are reset to factory default settings.

Enabling Password Protection

After all deployed phones have the username and password set, and new phones receive that information via pre-provisioning, you're ready to enable password protection.

1. In the Endpoints Admin UI, go to **System > Configuration**.
2. Add or edit the following properties:
 - **PasswordProtectFiles** = set to yes to enable password protection.
 - **username**: enter the authentication username you selected.
 - **Password** = enter the authentication password you selected.

- Optional: Set **PerDevicePasswords** to **yes** to allow overriding the default username and password at the MAC level. Then, when you edit a phone in the Endpoints Admin UI, there will be fields to set the username and password just for this device.

Auth User :	<input type="text"/>
Auth Pass :	<input type="password"/>

Disabling TFTP

SAFE and password protection do not protect Trivial FTP (TFTP). Consequently, it is preferred to provision phones using HTTP or HTTPS instead, and then disable TFTP whenever possible.

For each phone model whose TFTP provisioning you want to disable.

Note: Older phones like the Cisco 79xx do not support HTTP/HTTPS. If you use these phones, leave TFTP enabled for those models.

- In the Endpoints Admin UI, go to **System > Device Definitions**.
- Set **Allow TFTP** to **no**.

Brand ?	: Cisco
Model ?	: spa525G
Type ?	: Device
Force HTTPS ?	: no
Allow TFTP ?	: no

Secure Admin Login

To protect your administrative login, ensure good quality passwords. Beyond that, you can configure the web server to allow logins only from specific IP addresses you know.

Perform the following steps at the command line:

Note: The NetSapiens IP address is 66.185.162.140.

- Edit or create the `.htaccess` file using the following command:

```
pico /usr/local/NetSapiens/ndp/.htaccess
```

- Add the following information to the file:

```
Order deny,allow
Deny from all
Allow from 127.0.0.1
Allow from <your IP>
Allow from 66.185.162.140
```

3. Reboot Apache:

```
service apache2 restart
```

9. DIAGNOSTICS AND LOGS

Topics:

- ^ [Sync \(page 64\)](#)
- ^ [Events \(page 64\)](#)
- ^ [Logs \(page 65\)](#)




The Endpoints Module features a variety of diagnostic and logging tools to help you understand what is happening with your devices.

Sync

Sync refers to the endpoint pulling a configuration file from the Endpoints module. When viewing the list of devices in the **Configurations > Phones** page of the Endpoints Admin UI, three sync related columns appear next to each device.

Re-sync sends the message SIP NOTIFY to the phone to instruct it to pull a new configuration file. Some devices reboot when they receive the re-sync message, while others apply the new configuration without rebooting. The phone must be registered to a Core for re-sync to be successful.

The **Last sync of current cfg** column shows the last time and date the endpoint pulled a configuration file from the Endpoints module. The **Cfg last changed** column shows the last time handset-specific changes (device overrides, line changes, directories, and so on) were applied. These two timestamps can help identify whether the phone has a current configuration and is in communication with the Endpoints module.

Re-sync	Last sync of current cfg	 Cfg last changed
	0000-00-00 00:00:00	2016-02-16 18:10:41
	2016-02-12 19:55:13	2016-02-13 03:54:05

Events

Events is a history of specific details about endpoint communication. For example, when a phone requests a configuration file, that request will be detailed along with any other requested files such as licenses, ringtones, firmwares, and so on. Errors generated by bad configuration parameters might also appear here. For example, a Cisco SPA device's configuration file runs through a Cisco "compiler" tool and errors are output to the Events table.

The Endpoints module also functions as a syslog server. Phones can be configured to send syslog to the Endpoints module. These syslog entries can be viewed in the Events table.

Events					Filter:	Refresh	Refreshed: Thu 2016-03-10 16:29:42 GMT -8
Type	device/mac	server	domain	message			time
syslog NDP	0015655b1dfc	alpha1 kevinland		Sent file 0015655b1dfc.cfg			2016-03-09 22:52:43
syslog NDP	0015655b1dfc	alpha1 kevinland		Requested Yealink file using agent Yealink SIP-T41P 36.73.0.50			2016-03-09 22:52:43
syslog NDP	0015655b1dfc	alpha1 kevinland		Built Yealink file for 0015655b1dfc. Included 79 configuration lines w/ 0 defaults used and 0 overrides used			2016-03-09 22:52:43
syslog NDP	-			Setting primary server to alpha1 in Alpha 1 (AWS). Setting secondary server to alpha2 in Alpha 2 (AWS).			2016-03-09 22:52:41
syslog NDP	0015655b1dfc	alpha1 kevinland		ndp_syntax is = Yealink3 for mac 0015655b1dfc			2016-03-09 22:52:41
syslog NDP	0015655b1dfc	alpha1 kevinland		Attempting to build/find file 0015655b1dfc.cfg, device mac= 0015655b1dfc or local Path = /usr/local/NetSapiens/ndp/fm/0015655b1dfc.cfg			2016-03-09 22:52:41
syslog NDP	0015655b1dfc	alpha1 kevinland		Http request received for file 0015655b1dfc.cfg from 63.224.54.246(,)			2016-03-09 22:52:41
syslog NDP	000000000036			Sent file 404 FILE NOT FOUND for y000000000036.cfg			2016-03-09 22:52:41
syslog NDP	000000000036			Attempting to build/find file y000000000036.cfg, device mac= y000000000036 or local Path = /usr/local/NetSapiens/ndp/fm/y000000000036.cfg			2016-03-09 22:52:41
syslog NDP	000000000036			Http request received for file y000000000036.cfg from 63.224.54.246(,)			2016-03-09 22:52:41

Logs

The Endpoints module collects boot and app logs from Polycom devices. These logs can be viewed in the **Diagnostics > Logs**. Although these logs are rather terse, they can be helpful for identifying handset problems (for example, wrong bootrom or firmware). Most commonly, the logs will be sent to Polycom support for analysis when dealing with a phone problem.

10. CONFIGURATION PARAMETERS

Parameter	Version	Default	Notes
AcceptChangesFromDevice	1211	no	Allows local phone config to be saved to the device's overrides.
AllowPassInPath	1222	no	Allows a password in the request for a configuration file.
dontForceBLFonV VX	1224	no	<ul style="list-style-type: none"> no = sets BLF on V VX phones. yes = sets presence/buddy list instead of BLF on V VX phones.
includeDirectoryWithBLF	1224	no	Polycom specific. <ul style="list-style-type: none"> no = if BLF is enabled, do not create directory. yes = creates directory when BLF is enabled.
NoSpeedDialonBlfOff	1225	no	Polycom specific. <ul style="list-style-type: none"> no = if BLF is OFF, include <SD> in the directory. yes = directory entries appear on the phone screen in used line locations.
password	1222	Blank	Sets the password for provisioning authentication. PasswordProtectFiles must be set to yes to apply this parameter. See the username parameter below for setting the username.
PerDevicePasswords		Blank	<ul style="list-style-type: none"> no = disables provisioning passwords to be set at each MAC, and uses the default username and password instead. yes = enables provisioning passwords to be set at each MAC. If not set at the MAC level, the username and password values are used instead. PasswordProtectFiles must be set to yes to apply this parameter.
PolycomLongAddress	1225	no	Changes reg.1.address to the long form, such as sip:user@domain, and sets reg.1.server.1.address and .2.address to outbound proxies.
PreParseStrip	1225	Blank	Comma-separated list of values to strip requests for configuration files and leave only the MAC. See Managing Pre/Postfix on the Requested Configuration File on page 44.
Redundancy	1222	no	<ul style="list-style-type: none"> no = disables geo redundant provisioning of phones. yes = enables geo redundant provisioning of phones.
Redundancy_default	1222	none	<ul style="list-style-type: none"> none = disables redundancy. force primary = enables redundancy.
SAFE_error_500	1224	no	Requesting a non-existent configuration file returns a 503 result instead of a 403 result.
SAFE_error_empty	1224	no	Requesting a non-existent configuration file returns an empty 200OK result instead of a 403 result.
SAFE_MaxFraudScore	1225	50	Maximum fraud score until IP address is blacklisted.
SAFE_whitelist	1224	Blank	Comma-separated list of IP addresses to exclude from SAFE scoring/blacklisting.

Configuration Parameters

Parameter	Version	Default	Notes
SkipTimeStamp		no	<ul style="list-style-type: none"> no = includes the time stamp in many vendor configuration files. yes = skips the time stamp for many vendor configuration files.
TimeZone		no	<ul style="list-style-type: none"> Sets the time zone for the logs.
UseOauth	1225	no	<ul style="list-style-type: none"> no = use for the old API. See Validating API Version on page 52. yes = sets communication between endpoints and Core to use the new API.
username	1222	Blank	<ul style="list-style-type: none"> Sets the user name for provisioning authentication. PasswordProtectFiles must be yes to apply this parameter. See the password parameter above for setting the password.
useTCPandTLS	1225	no	<ul style="list-style-type: none"> no = disables TCP and TLS transport options. yes = enables TCP and TLS transport options for devices to communicate with Core. Core must also be enabled for TCP and TLS.
yealinkT2XnoMemoryKeys	1226	no	<ul style="list-style-type: none"> no = adds BLFs to the memory keys instead of line keys. Applies to T26 and T28 using Yealink3 code structure if "use sidecar" is also set to no. yes = BLFs are applied to line keys instead of memory keys.

INDEX

A

Adding

- core nodes, 53
- phones
 - Endpoints Admin UI, 14
 - Portal, 12

Admin login, 61

API version, validating, 52

B

Bootroms, Polycom, 25

Brand default, 18

C

Cisco SPA/Linksys, 10

Compatibility, 7

Configuration files

- loading, 44
- making, 42
- Polycom, 24
- pre/postfix, 44
- Yealink, 32

Configuration parameters, 66

Conventions in this document, v

Core nodes, adding, 53

Cores, 51

- geo redundant, 56

Custom directory, 48

D

Defaults, 9, 16

- brand, 18
- domain, 21
- handset/MAC, 22

model, 20

Device list, 39

Devices, new, 38

Diagnostics, 63

Directories, 45

- custom, 48
- selecting, 46
- types, 46

Directory Designer, 48

Disabling TFTP, 61

Document conventions, v

Domain default, 21

E

Endpoints module

- logging in, 7
- pointing a phone, 10

Events, 64

Existing format and new device, 39

F

Files

- configuring Polycom phones, 24
- configuring Yealink phones, 32
- password protecting, 60

Firmware

- Polycom, 26
- Yealink, 33

Fraud scores, 59

G

Geo clusters, 52

Geo redundancy, 56

GrandStream, 10

H

- Handset
 - MAC default, 22
 - security, 59
- How the Endpoints module decides which configuration file to use
 - Polycom, 24
 - Yealink, 32

L

- Loading a configuration file, 44
- Log in
 - Endpoints module, 7
 - secure admin, 61
- Logs, 63, 65

M

- Making a configuration file, 42
- Model
 - compatibility, 7
 - default, 20

N

- NDP code type, 43
- New device
 - existing format, 39
 - no existing format, 42
 - not in the device list, 39
- No existing format and new device, 42

O

- Overrides, 16

P

- Parameters, 66
 - scope, 18
- Password protection, 60
 - enabling, 60
- Phone, adding, 12

- Pointing to the Endpoints module
 - Cisco SPA/Linksys, 10
 - GrandStream, 10
 - Polycom, 11
 - Yealink, 11

- Polycom, 11
 - bootroms, 25
 - configuration file to use, 24
 - configuration files, 24
 - firmware, 26
- Pre/postfix, 44

R

- Running a new device not in the device list, 39

S

- SAFE, 59
 - fraud scores, 59
- Secure admin login, 61
- Security, 58, 63
 - handset, 59
- Selecting a directory, 46
- Setting the scope of a parameter, 18
- Support, 7
- Sync, 64

T

- TFTP, 61
- Trivial FTP, 61
- Types of directories, 46

V

- Validating API version, 52
- Versions of API for validating, 52

Y

- Yealink, 11
 - configuration file to use, 32
 - configuration files, 32
 - firmware, 33