Administrator's Manual

AudioCodes High Definition IP Phones Series

405HD, 430HD, 440HD, 445HD, 450HD and C450HD IP Phones
RX50 Conference Phone
HRS Conference Device

Version 3.4.1

audiocodes

Table of Contents

List of Figures

List of Tables

This page is intentionally left blank.

Notice

Information contained in this document is believed to be accurate and reliable at the time of printing. However, due to ongoing product improvements and revisions, AudioCodes cannot guarantee accuracy of printed material after the Date Published nor can it accept responsibility for errors or omissions. Updates to this document can be downloaded from https://www.audiocodes.com/library/technical-documents.

This document is subject to change without notice.

Date Published: June-23-2020

WEEE EU Directive

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

Customer Support

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

Stay in the Loop with AudioCodes

Abbreviations and Conventions

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

Related Documentation

Document Name
405HD IP Phone User's Manual
405HD IP Phone Quick Guide
430HD IP Phone User's Manual
430HD IP Phone Quick Guide
440HD IP Phone User's Manual
440HD IP Phone Quick Guide
445HD Generic SIP IP Phone User's Manual
445HD Generic SIP IP Phone Quick Guide
450HD Generic SIP IP Phone User's Manual
450HD Generic SIP IP Phone Quick Guide
C450HD Generic SIP IP Phone User's Manual
C450HD Generic SIP IP Phone Quick Guide
HRS Conference Device User's Manual
HRS Conference Device Quick Guide
RX50 Conference Phone User's Manual
RX50 Conference Phone Release Notes
400HD Series IP Phone Administrator's Manual
Device Manager Pro Administrator's Manual
One Voice Operations Center (OVOC) IOM Manual
OVOC User's Manual

Document Revision Record

LTRT	Description
11973	This is the initial release of the unified product documentation.

Documentation Feedback

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

1 Introduction

This *Administrator's Manual* is intended for network administrators responsible for configuring AudioCodes' IP phones in their enterprise telephony networks.

The manual covers AudioCodes' low-end and high-end phone models:

- Low-end phone models: 405HD, 430HD and 440HD
- High-end phone models: 445HD, 450HD, C450HD, RX50 conference phone and the HRS conference device

Note:

- *Release Notes version 3.4.3* documents support only the following high-end phone models:
  - √ 445HD
  - √ 450HD
  - √ C450HD
  - √ RX50 conference phone
  - √ HRS conference device
- This *Administrator's Manual* documents support both these *and* the following low-end phone models:
  - √ 405HD
  - √ 430HD
  - √ 440HD
- When a feature is documented but support is still pending, a note will indicate this.

AudioCodes' IP phones are based on AudioCodes' proprietary High Definition (HD) voice technology, providing clarity and a rich audio experience in Voice-over-IP (VoIP) calls. The phones are fully-featured telephones that provide voice communication over an IP network, allowing you to place and receive phone calls, put calls on hold, transfer calls, make conference calls, and so on.

For a detailed description on hardware installation and for operating the phone's call features, see the phone's *User's Manual*.

This page is intentionally left blank.

2 Configuration Methods

The phones feature four optional configuration methods:

- Configuration file. Text-based file, created using a text editor such as Microsoft's Notepad. Contains configuration parameters. Loaded to the phone using provisioning methods TFTP, FTP, HTTP/HTTPS. See Section 2.2 for more information.
- Device Manager Pro/Express. See Section 2.3 for more information.
- Phone screen. Easy-to-use, menu-driven screen providing basic phone configuration and status capabilities. See the next section for more information.

2.1 Phone Screen

The Liquid Crystal Display (LCD) phone screen allows configuring phone Settings, Keys and Administration menus.

2.1.1 Administration Menu

Note:

- The phone is password protected. The default password is 1234. To change the login password, use the phone's configuration file.
- After entering the password, the access session is applied to all the submenus.
- To change the Administration screen's login password, use the configuration file.

➢ **To access the Administration screen:**

1. Press the MENU key on the phone and navigate down to **Administration**.

Note: Alternatively, after pressing the MENU key you can press an item's number to navigate to the item, for example, in the 445HD, press **5** to navigate to **Administration**.

2. Press **Select**; you're prompted for a password.
3. Enter the administration password (Default: **1234**) and then press the **OK** softkey.

2.1.2 Configuring the Web Interface's Port

If the network administrator requires the Web interface for a configuration purpose, they need to assign it a port number.

➢ **To configure the Web interface port:**

- Use the table as reference.

Table 2-1: Port Parameters

Parameter	Description
system/http_server_port	Assigns a port number to the Web interface. The HTTP server by default uses port number 80. Range: 0-65535.
system/https_server_port	Assigns a port number to the Web interface. The HTTPS server by default uses port number 443. Range: 0-65535.

2.1.3 Configuring User Login Credentials

The network administrator can configure the phone user's name and password.

➢ **To configure user's name and password:**

- Use the table as reference.

Table 2-2: User Name and Password Parameters

Parameter	Description
system/web_user_name	The phone user name. Default: admin. Applies only to the Web interface.
system/web_user_password	The encrypted phone password. Default: 1234. Applies only to the Web interface, and phone screen.

2.2 Configuration File

This section describes the configuration file and the parameters you can configure in it. The configuration file can be loaded to the phone using automatic provisioning or from the Device Manager. The subsections below describe configuration file syntax and linking additional configuration files to a configuration file.

2.2.1 File Syntax

The configuration file can be created using a standard ASCII, text-based program such as Notepad. The configuration file is a *.cfg* file with the file name being the phone's MAC address: **<phone's MAC address>.cfg**.

The syntax of the configuration file is as follows:

```
<parameter name>=<value>
```

Make sure the configuration file conforms to these guidelines:

- No spaces on either side of the equals (=) sign.
- Each parameter must be on a new line.

Below is an example of part of a configuration file:

```
system/type=440HD
voip/line/0/enabled=1
voip/line/0/id=1234
voip/line/0/description=440HD
voip/line/0/auth_name=1234
voip/line/0/auth_password=4321
```

2.2.2 Linking Multiple Files

The Configuration file allows you to include links (URL and/or file name) to other Configuration files that provide additional parameter settings. This is especially useful in deployments with multiple phones, where the phones share common configuration but where each phone has some unique settings. In such a scenario, a phone's Configuration file can include unique parameter settings as well as links to additional Configuration files with settings common to all phones.

Linking additional files is achieved by using the **include** function in the phone's Configuration file. For example, the below Configuration file provides links to additional Configuration files (shown in bolded font):

```
system/type=440HD
```

```
include 440HD_<MAC>_voip.cfg
include vlan_conf.cfg
include network_conf.cfg
include provisioning_conf.cfg
```

In addition, the Configuration file can provide URL paths (FTP, TFTP, HTTP, or HTTPS) to where the additional files are located, as shown in the example below (shown in bolded font):

```
system/type=440HD
include http://10.10.10.10/440HD_<MAC>_voip.cfg
include https://remote-pc/vlan_conf.cfg
include tftp://10.10.10.10/440HD_<MAC>_network.cfg
include ftp://remote-pc/provisining_conf.cfg
```

Note: If no URL is provided in the Configuration file, the files are retrieved according to the provisioning information (e.g. DHCP Option 160 as well as Option 66/67).

2.2.3 Creating Configuration Files using VoIProvision Utility

When installing AudioCodes' phones, the network administrator typically configures each installed phone automatically. Using DHCP options or other methods, the phone can be instructed to download a configuration file. This file is typically unique to each phone, based on the MAC address. This MAC-specific configuration file is generated with phone specific configuration parameters; such as, the extension ID, name and authentication password.

Not all of the iPBX and SoftSwitch vendors (and especially the full solution vendors) include provisioning in their interoperability programs. As an IP phone vendor, AudioCodes is required to provide a standalone provisioning tool that will enable the provisioning of its phones in such environments.

AudioCodes provides a tool that assists in the automatic generation of configuration files. These files can be generated for the initial configuration of the phones and then later regenerated for subsequent configuration updates as required.

2.2.3.1 Configuration File Format

The detailed format of the phones' configuration files are described in the appendix. The following is an output example of an automatically generated MAC-specific file:

```
system/type=440HD
voip/line/0/enabled=1
voip/line/0/id=56832432
voip/line/0/auth_name=3423fdwer2tre
voip/line/0/auth_password=123456
include global.cfg
```

2.2.3.2 Global Configuration File

In addition to the MAC-specific files, it is recommended to maintain a single global configuration file, which contains parameters that are common to all phones in the specific site. The MAC-specific files can call the global file (using the 'include' method) as illustrated in the above example. For more information, see 'Linking Additional Files using “Include”' in the Administrator's Manual.

2.2.3.3 VoIProvision Utility Overview

The VoIProvision utility is a generic tool that automatically generates multiple MAC-specific configuration files (*.cfg*). The utility generates a separate *.cfg* file for each phone.

To execute the utility, the user needs to prepare a *csv* file and a *template* file. The *csv* file contains the tagged records for each phone and the template file maps these tagged records to a configuration file format, which can be read by the phone.

2.2.3.4 CSV File

The *csv* file contains a list of tags and a list of the tag's values. The first line in the file contains the list of tags (comma-separated) and each of the other lines contains a list of values, where each line record represents an individual phone.

The *csv* file is usually exported from the customer's IP-PBX or some other database and typically contains the list of phones (e.g. MAC, extension ID, user name and password of each phone).

Table 2-3: Example of CSV File

[mac]	[name]	[id]	[password]
00908F123456	Jonathan	4071	12345
00908F123457	David	4418	12345

When opened as a text file, the *csv* file appears similar to the example below:

```
[mac],[name],[id],[password]
00908F123456,Jonathan,4071,12345
00908F123457,David,4418,12345
```

2.2.3.5 Template File

The template file defines the format of the generated configuration files, but contains tags instead of actual values. The **VoIProvision** utility reads the template file and replaces each tag with actual values from the *csv* file.

Example of a template file:

```
system/type=440HD
voip/line/0/enabled=1
voip/line/0/id=id
voip/line/0/auth_name=name
voip/line/0/auth_password=password
include global.cfg
```

2.2.3.6 Generated Configuration Files

The generated configuration (*.cfg*) files use a similar format to the template file; however the tags are replaced with the actual values that are read by the VoIProvision utility from the *csv* file. One of the tags defined in the *csv* file, should be used as the *.cfg* file name (in order for the VoIProvision utility to generate a separate *.cfg* file for each line record in the csv file). Typically the tag which defines the MAC address is used as the *.cfg* file name.

2.2.3.7 Starting the VoIProvision Utility

The VoIProvision utility can run on both the Linux and Windows platforms. The VoIProvision utility initially parses the *csv* file to generate the list of tags. The VoIProvision then reads each line record of values in the *csv* file and for each line record, does the following:

- Parses the line record to create a list of values
- Opens the template file
- Generates the *.cfg* file name and create a new *.cfg* file
- Reads the template file, associates the mapped tags with actual values from the *csv*

file and writes the result to the *.cfg* file

- Closes the *.cfg* file and template file

2.2.3.8 Usage

```
USAGE: VoIProvision<csv file><template file><.cfg file>
```

Note the following:

- The first line of the *csv* file contains the list of tags (e.g., mac,name,id).
- The remainder of the *csv* file contains a line record per .cfg file (e.g. 00908f112233,4071,Ethan).
- There is no restriction on the format of the tags (e.g., tag or @tag@).
- The template file defines the *.cfg* file format. During VoIProvision run-time, the mapped tags in the template file are associated to actual values that are read from the *csv* file.
- Currently only a single tag can be defined per line record in the template file.
- The *.cfg* file name should represent the string of one of the predefined tags in order to generate a separate *.cfg* file per *csv* line record (e.g., mac.cfg).

2.2.4 Using the Encryption Tool

AudioCodes' phones use the Triple Data Encryption Standard (3DES) algorithm for encryption.

Note: Support pending.

2.2.4.1 Encrypting Configuration Files

The configuration file can be encrypted. For example, you may wish to encrypt the configuration file when it is sent over an insecure network.

➢ **To encrypt the configuration file:**

- At the command line prompt, specify the following:

```
encryption_tool.exe -f <filename>.cfg
```

where <*file name*>.cfg specifies the name of the Configuration file that you wish to encrypt.

Once the Configuration file is encrypted, it receives the suffix '.cfx' (e.g. Conf.cfx). This is the file that you should specify in the 'Configuration URL' and the 'Dynamic Configuration URL' fields when performing automatic provisioning (see Part II 'Automatic Provisioning').

2.2.4.2 Encrypting Passwords in the Configuration File

Phone passwords used in the configuration process can be encrypted, for example, the 'System' password and the 'SIP Authentication' password.

➢ **To encrypt passwords:**

1. At the command line prompt, specify the following:

```
encryption_tool.exe -s <password_string>
```

where *<password_string>* specifies the string of the password that you wish to encrypt.

Once the password is encrypted, a string is generated with the following syntax:

```
{"<encrypted_string>"}
```

For example:

```
{"0qrNRpSJ6aE="}
```

2. Copy the generated string (including the {“ “}) with the syntax specified above to the relevant parameter in the Configuration file.

For example, if you encrypted the SIP authentication password, the following is displayed in the relevant line in the configuration file:

```
voip/line/0/auth_password={"0qrNRpSJ6aE="}
```

Note: It's recommended to encrypt the 'System' password using this procedure. If you choose not to, the 'System' password is by default encrypted using MD5.

2.3 Device Manager

Network administrators can provision an enterprise's phones from the server of the One Voice Operations Center (OVOC) module, Device Manager.

Note:

- Device Manager and OVOC share the same server location.
- For more information on using Device Manager to provision phones, see the *Device Manager Administrator's Manual*.

➢ **To configure provisioning phones from the OVOC server:**

■ Use the table as reference.

Table 2-4: OVOC Server Parameters

Parameter	Description
ems_server/keep_alive_period	The OVOC server sends a keep alive message at a configured interval to verify that its link with the network is operating. If no reply is received, the link is determined to be down or not working. Default: 60 minutes
ems_server/provisioning/url	Defines the URL of the OVOC server, for example, http://10.1.8.23:8081
ems_server/user_name	Defines the username of the administrator who'll use the OVOC server for provisioning, for example, John Smith.
ems_server/user_password	Defines the password (encrypted) of the network administrator who'll provision the phones from the OVOC server, for example: {"Y6QYmP53BDkoTvuIFjEBuQ=="}

This page is intentionally left blank.

3 Configuring Automatic Provisioning

By default, the phone is ready for out-of-the-box deployment using its automatic provisioning capabilities.

The phone offers a built-in mechanism for automatically upgrading its software image and updating its configuration. This method is used to upgrade the phone firmware and update its configuration, by remotely downloading an updated software image and configuration file.

The automatic update mechanism helps you keep your software image and configuration up-to-date, by performing routine checks for newer software versions and configuration files, as well as allowing you to perform manual checks.

The automatic update mechanism is as follows:

- Before connecting the phone, verify that the provisioning server is running and that the firmware and configuration files are located in the correct location.
- Connect your phone to the IP network, and then connect the phone to the power outlet.
- During DHCP negotiation, the phone requests for DHCP options 66/67/160 to receive provisioning information. The DHCP server should respond with Option 160 providing the provisioning URL or Options 66 and 67 providing the TFTP IP address and firmware file name respectively.
- The phone then checks whether new firmware is available by checking the firmware file header. If the version is different from the one currently running on the phone, the phone downloads the complete image and burns it to its flash memory.
- If a new firmware is unavailable, the phone then checks whether a new configuration is available. If a configuration file is available on the server, the phone downloads it and updates the phone's configuration after verifying that the configuration file is related to the phone model. When a configuration update is needed, the phone might reboot.

Note:

- In the DHCP Discover message, the phone publishes its model name in Option fields 60 and 77 (e.g. 440HD). If the administrator wants to provide different provisioning information to different phone models, the administrator can set up a policy in the DHCP server according to the phone model name.
- If the phone is powered off for some reason during the firmware upgrade process, the phone will be unusable and the recovery process must be performed.
- You can only use firmware files with an *.img* extension and configuration files with a *.cfg* extension.
- An additional auto-provisioning mechanism is supported if the provisioning environment does not provide all the required information (e.g. DHCP options).

Note: Automatic mass provisioning of phones using DHCP can alternatively be performed from the OVOC's Device Manager module. For more information, see the *Device Manager Pro Administrator's Manual*.

3.1 Setting up Network for Auto Provisioning

The phone supports dynamic VLAN discovery, dynamic IP addressing (DHCP), and NTP (as client).

Note: For manual configuration of Network Settings, see Section 4.2.

3.1.1 Provisioning Hunt Order

The phone always attempts to use the *first* provisioning method listed below (DHCP Option 160). If it cannot use this method, it attempts to use the second method listed below, and so on, until it reaches a successful provisioning method. This is called the provisioning 'hunt order'. The 'hunt order' is:

1. DHCP Option 160 (see Section 3.1.2.1)
2. DHCP Options 66-67 (see Section 3.1.2.2)
3. DHCP Options 43 (see Section 3.1.2.5)
4. SIP SUBSCRIBE and NOTIFY Messages (see Section 3.1.2.7)
5. Static and Globally Accessible Domain (see Section 3.1.2.8)
6. Cached Addresses of the Last Provisioning Server Used on Reboots (see Section 3.1.2.9)
7. AudioCodes Redirect server (see Section 3.1.2.10)

3.1.2 Dynamic URL Provisioning

Dynamic Host Configuration Protocol (DHCP) can be used to automatically provision the phone.

➢ **To configure DHCP:**

- Use the table as reference.

Table 3-1: DHCP Automatic Provisioning Parameters

Parameter	Description
provisioning/method	Defines the provisioning method: ▪ Disable - Automatic update is disabled. The phone attempts to upgrade its firmware and configuration ▪ Dynamic - DHCP Options (Dynamic URL) (default) - Using DHCP option 160 as well as option 66/67 for provisioning ▪ Static URL - Using Static URL for provisioning
provisioning/url_option_value	Determines the DHCP option number to be used for receiving the URL for provisioning. The default value is 160. The phone supports DHCP Option 160 for complete URL as well as Options 66/67 for TFTP usage. Option 160 has the highest priority and if absent, Options 66/67 are used. The following syntax is available for DHCP option 160: ▪ <protocol>://<server IP address or host name>

Parameter	Description
	▪ <protocol>://<server IP address or host name>/<firmware file name> ▪ <protocol>://<server IP address or host name>/<firmware file name>;<configuration file name> ▪ <protocol>://<server IP address or host name>/;<configuration file name> Where <protocol> can be one of the following: **ftp**, **tftp**, **http** or **https**. For example: ▪ **ftp://192.168.2.1** – retrieved firmware file is*440HD.img* and the configuration file name is <MAC address>.cfg. For example, 001122334455.cfg ▪ **tftp://192.168.2.1/different_firmware_name.img** - retrieved firmware file is Different_Firmware_Name.img and the configuration file name is <MAC address>.cfg. For example, 001122334455.cfg ▪ **http://192.168.2.1/different_firmware_name.img; <MODEL>_<MAC>_conf.cfg** - retrieved firmware file is different_firmware_name.img and the configuration file name is <Model type>_<MAC address>_conf.cfg. For example, **440HD_001122334455_conf.cfg** • **https://192.168.2.1/;<MODEL>_<MAC>_conf.cfg** - if the model is 440HD, the retrieved firmware file is 440HD.img and the configuration file name is 440HD_<MAC Address>_conf.cfg. For example, 440HD_001122334455_conf.cfg The following syntax is available for DHCP Options 66/67: ▪ Option 66 must be a valid IP address or host name of a TFTP server only. ▪ Option 67 must be the firmware name. If Option 67 is absent, the phone requests for the 440HD.img image file. For example: ▪ **Option 66:** 192.168.2.1 or myTFTPServer ▪ **Option 67:** 440HD_2.2.2.img **Note:** ▪ This parameter is applicable only when **method** is configured to **Dynamic**. ▪ It is recommended to leave the parameter at its default value to avoid conflict with other DHCP options settings.
provisioning/random_provisioning_time	Defines the maximum random number to start the provisioning process. This is used for periodic checking of firmware and configuration files to avoid multiple devices from starting the upgrade process at the same time. When the device is meant to start the upgrade, the device randomly selects a number between 1 and the value set for

Parameter	Description
	random_provisioning_time and performs the check only after the random time. The valid range is 0-65535. The default value is 120.
provisioning/period/type	Defines the period type for automatic provisioning: ▪ **every5minutes** Minimum definable time. Sets the interval at every five minutes. ▪ **every15minutes** Sets the interval at every five minutes. ▪ **hourly -** Sets an interval in hours. ▪ **daily** (default) - Sets an hour in the day. ▪ **weekly** - Sets a day in the week and an hour in the day. ▪ **powerup** Irrespective of what value is defined, the phone always checks on powerup, but if **powerup** is defined, the phone will check *only* on powerup.
provisioning/period/hourly/hours_interval	The interval in hours for automatically checking for new firmware and configuration files. The valid range is 1 to 168. The default is 24. **Note:** This parameter is applicable only when **`type`** is configured to **hourly**.
provisioning/period/daily/time	The hour in the day for automatically checking for new firmware and configuration files. The format of this value is **hh:mm**, where **hh** is hour and **mm** is minutes. For example, **`00:30.`** The default time is **00:00**. **Note:** This parameter is applicable only when **type** is configured to **daily**.
provisioning/period/weekly/day	The day in the week for automatically checking for new firmware and configuration files. ▪ Sunday (default) ▪ Monday ▪ Tuesday ▪ Wednesday ▪ Thursday ▪ Friday ▪ Saturday **Note:** This parameter is applicable only when **type** is configured to **weekly**.
provisioning/period/weekly/time	The hour in the day for automatically checking for new firmware and configuration files. The format of this value is: **hh:mm**, where **hh** is hour and **mm** is minutes. For example: **`00:30`** The default time is **00:00**. **Note:** This parameter is applicable only when **type** is configured to **weekly**.

3.1.2.1 Provisioning using DHCP Option 160

Phones can get a provisioning URL from DHCP Option 160, 66/67 or 43 [support pending]. Option 160 has the highest priority, following by Option 66/67, and then Option 43.

3.1.2.2 Configuring Automatic Provisioning by DHCP Server

Phones are *automatically provisioned* by the enterprise's DHCP server when initially connected to the IP network and to the power supply.

Network administrators can then configure *periodic* automatic provisioning by DHCP server. For more information, see Configuring Automatic Provisioning under Section 3.

Note: To implement secure provisioning using HTTP/S, the HTTP/S server on the far end (from where you are loading the files) must also support HTTP/S.

3.1.2.3 Technician's Digit Key Code

Note: Support pending.

Technicians installing phones at customer sites do not need to connect laptops to phones to provision them. After connecting phones to the network, technicians can enter a specific digit key code which changes the phones' provisioning URL to the server's URL. If the code that the technician enters matches, the phones are automatically provisioned from that server.

Note: The feature requires software customization.

3.1.2.4 Provisioning using DHCP Option 66/67

Phones can get a provisioning URL from DHCP Option 66/67. Option 160 has the highest priority, followed by Option 66/67, and then Option 43 [support pending]. The table below shows the behaviors for Option 66/67.

Table 3-2: Auto Provisioning via DHCP Option 66/67

	Option 66	Option 67	Result	Comment
1	Doesn't exist or empty	Any	No URL from Option 66/67	When Option 66 doesn't exist, or it's empty, the phone cannot get a URL from Option 66/67.
2	Server address exists but there is no protocol header such as TFTP, FTP, HTTP, HTTPS. File names do not exist. Example: **Audiocodes.com** **192.168.0.11**	Non-existent	**Firmware URL:** Tftp://audiocodes.com/<hardware type>.img **Configuration file url:** Tftp://audiocodes.com/.<mac>cfg	When protocol is not specified, tftp is added as the default protocol.
		Contains names. Example: **abc.img;efg.cfg**	**Firmware URL:** Tftp://audiocodes.com/abc.img **Configuration file URL:** Tftp://audiocodes.com/efg.cfg	
3	Server address exists File names do not exist. Example: http://Audiocodes.com http://192.168.0.11	Non-existent	**Firmware URL:** http://audiocodes.com/<hardware type>.img **Configuration file URL:** http://audiocodes.com/.<mac>cfg	Support pending
		Contains names. Example: **abc.img;efg.cfg**	**Firmware URL:** http://audiocodes.com/abc.img **Configuration file URL:** http://audiocodes.com/efg.cfg	
4	Server address exists. File names exist. Example: http://Audiocodes.com/abc.image;efg.cfg	Any	**Firmware URL:** http://audiocodes.com/abc.img **Configuration file URL:** http://audiocodes.com/efg.cfg	[Support pending] If any file name exists in Option 66, the names in Option 67 are ignored.

➢ **To operate with DHCP Options 66 and 67:**

- Configure DHCP Options 66 and 67 in the DHCP server, instead of configuring Option 160. See the DHCP server related documentation for detailed information.

3.1.2.5 Provisioning using DHCP Option 43

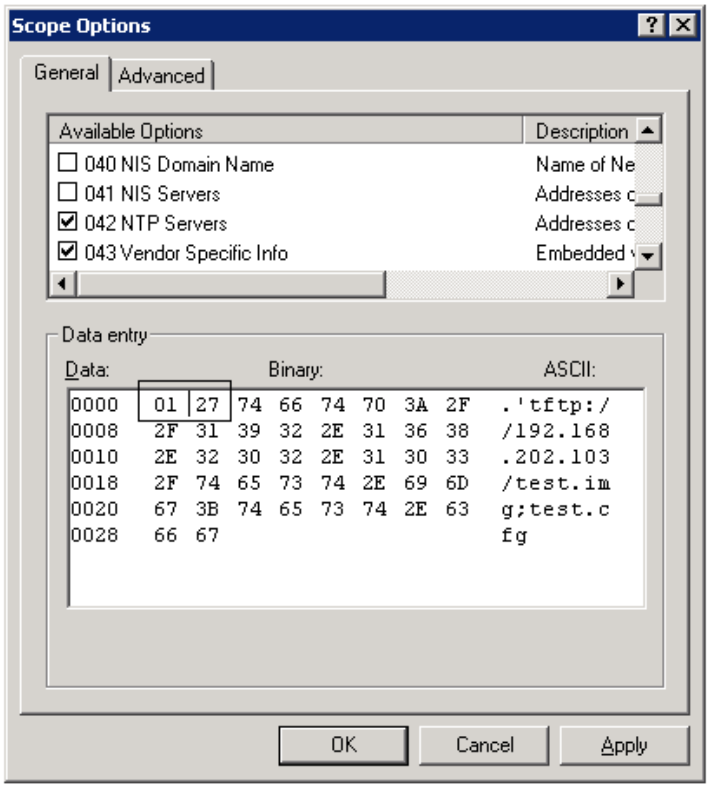
Note: Support pending.

Phones can get a provisioning URL from DHCP Option 43. Option 160 has the highest priority, following by Option 66/67, and then Option 43.

➢ **To operate with DHCP Options 43:**

- Configure DHCP Options 43 in the DHCP server. Use the example in the figure below as reference.

Figure 3-1: Provisioning using DHCP Option 43 in the DHCP Server



Note:

- **01** is the sub option
- **27** is the length (in HEX) of the provisioning path string that you configured
- The remainder is the provisioning path, in ASCII code.
  Example: **tftp://192.168.202.103/test.img;test.cfg**

3.1.2.6 Provisioning using the User-Class Option

Provision using the User-Class Option if vendor phones other than those of AudioCodes are deployed in the same enterprise as AudioCodes' phones and a DHCP Option cohabitation issue consequently occurs.

The network administrator can configure provisioning of AudioCodes phones using the User-Class Option when other vendor phones in the enterprise point to the same DHCP server and use one of the standard DHCP Options described in the previous sections.

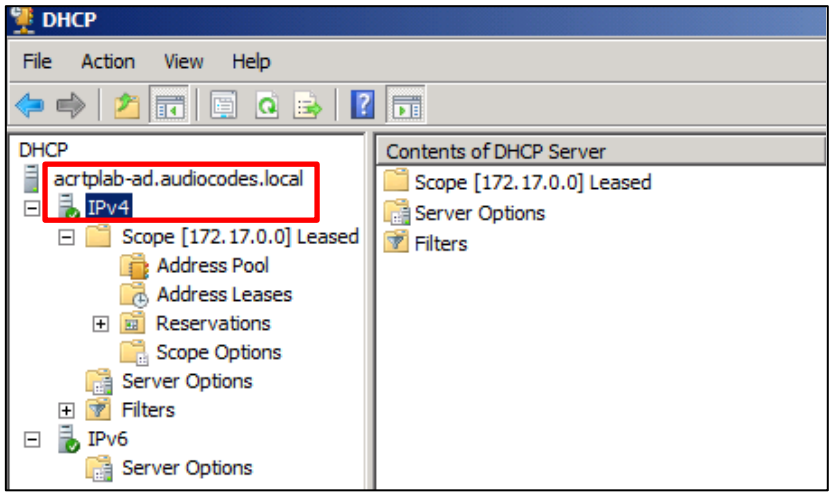
➢ **To configure provisioning of AudioCodes phones using the User-Class Option:**

1. Determine the DHCP server hosting the phones.
1. Determine if DHCP Options are assigned to IPv4 or IPv6 addresses.

Note:

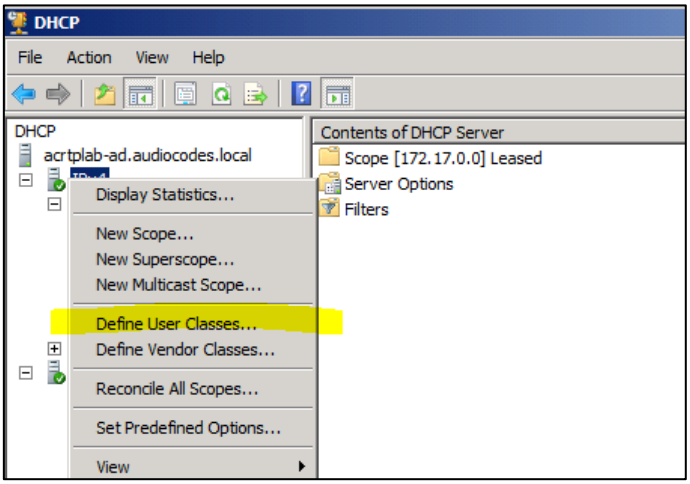
- The examples below show DHCP server **acrtplab-ad.audiocodes.local**
- The examples below show IPv4 addresses

Figure 3-2: DHCP Options Assigned to IPv4 Addresses



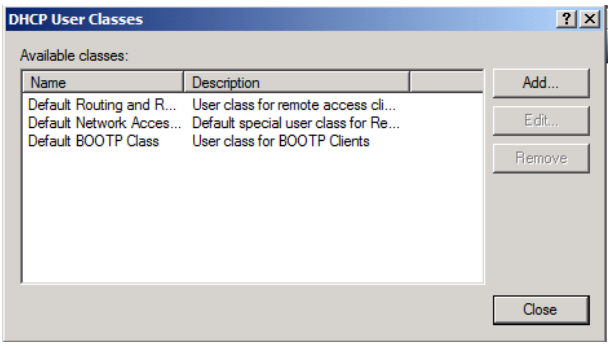
2. Define a separate **User Class** for each phone deployed. Right-click the **IPv4** server icon and from the popup menu, select **Define User Classes…**

Figure 3-3: Defining User Classes



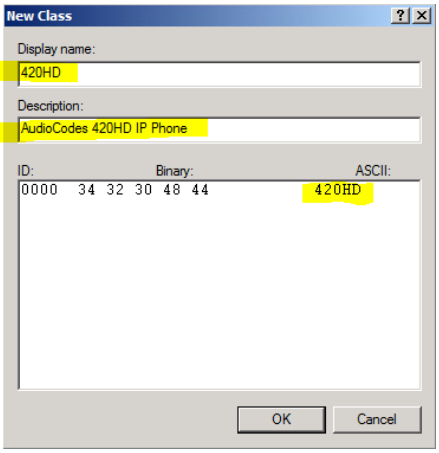
The DHCP User Classes screen opens.

Figure 3-4: DHCP User Classes



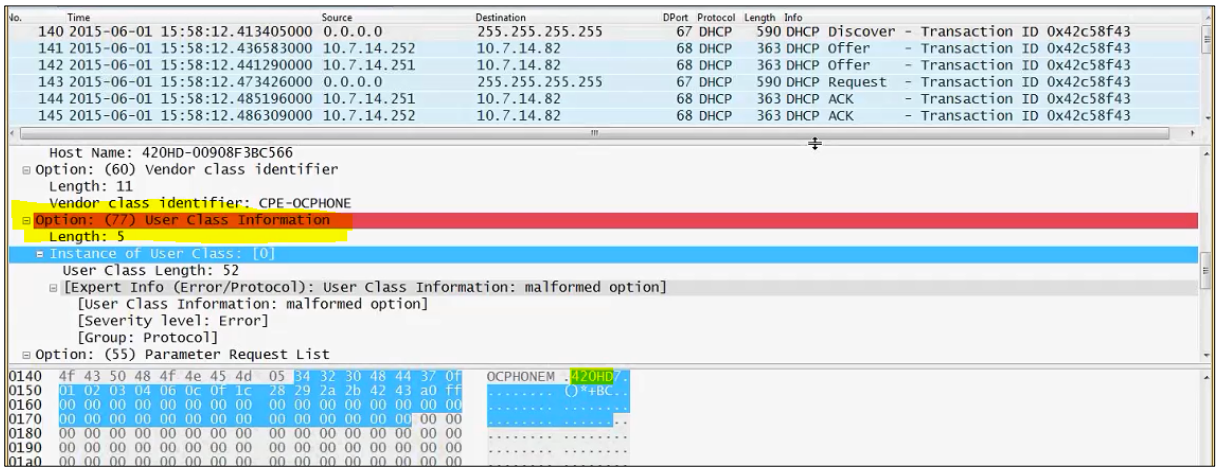
3. Click the **Add…** button.

Figure 3-5: New Class



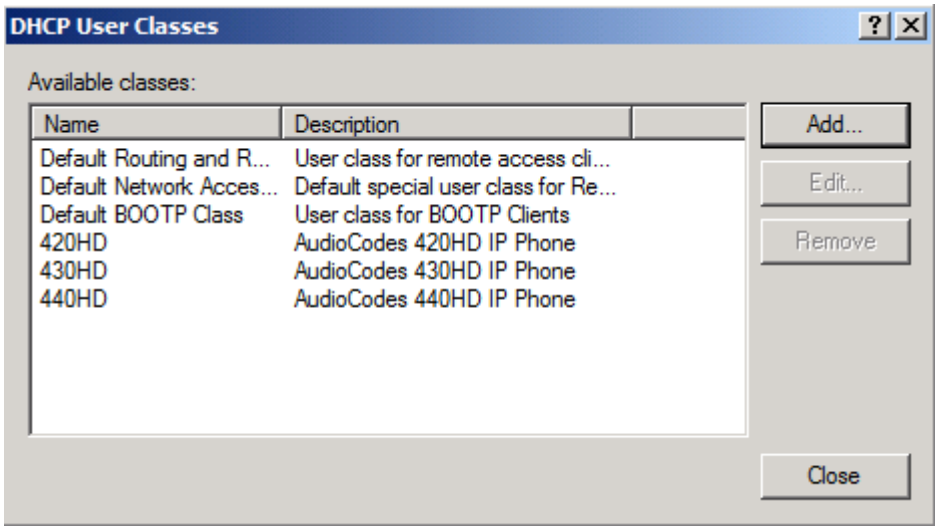
4. In the New Class screen, enter **Display name** and **Description** as shown in the figure above, and then in the **ASCII** field, enter the **User Class Phone Type** (see the Packet Bytes window in Wireshark below, and see the table below for the other AudioCodes phone models) to be sent from the phone during DHCP Discover via Option 77 (supported by DHCP Server 2008). Do this for each AudioCodes phone model so that a User Class entry for each model deployed will exist when completed.

Figure 3-6: Packet Bytes Window



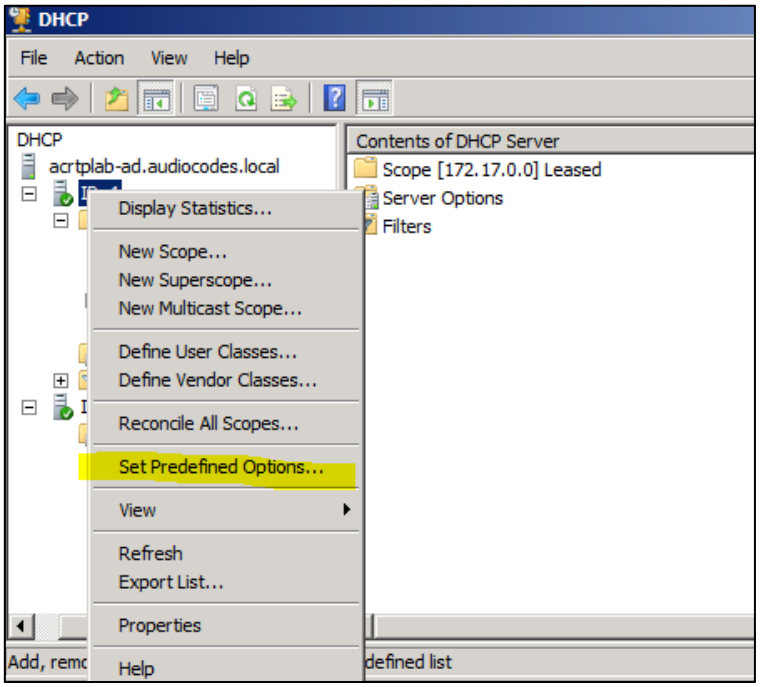
5. Make sure one DHCP User Class entry exists for each AudioCodes phone model deployed in the enterprise.

Figure 3-7: DHCP User Classes [Illustration only]



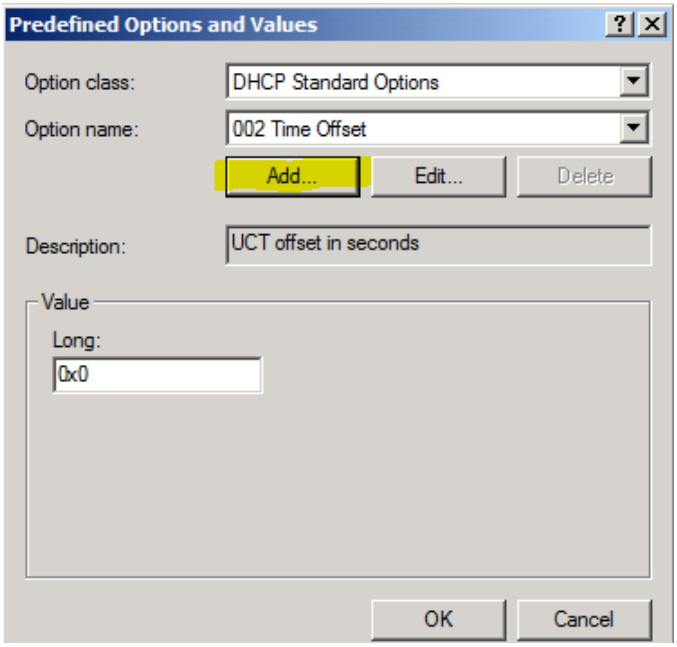
6. Configure Scope Option 160. This is not a *standard* Scope Option, so it needs to be created. To create it on the server, select the IP version (**IPv4**) and select **Set Predefined Options…**

Figure 3-8: Set Predefined Options



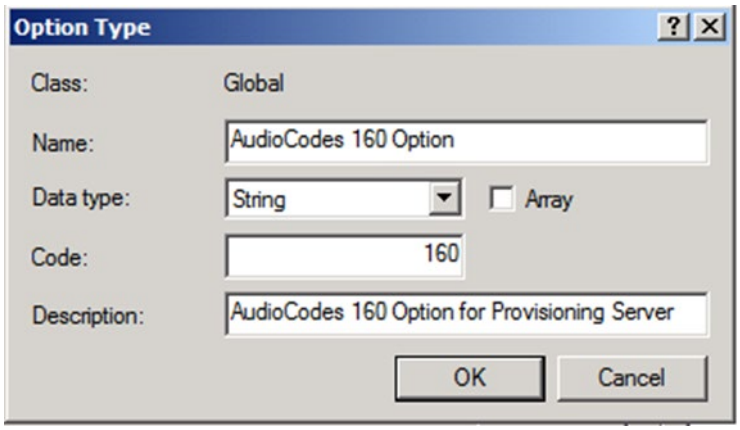
7. From the 'Option class' dropdown, select **DHCP Standard Options**, and then click the **Add…** button.

Figure 3-9: Predefined Options and Values



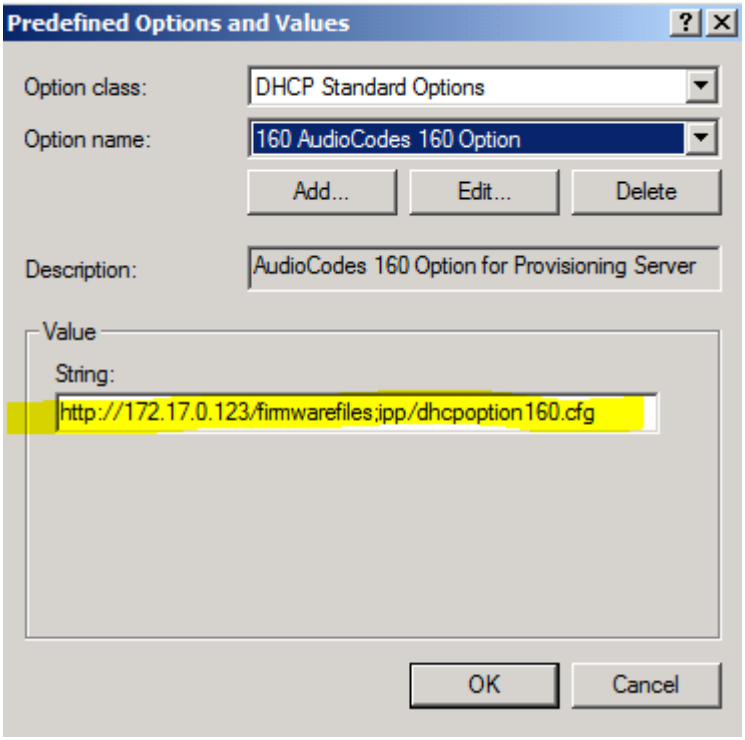
8. Add the **AudioCodes 160 Option** as shown below, and then click **OK**.

Figure 3-10: Option Type – Add AudioCodes 160 Option



9. Add the OVOC server location using HTTP. In the figure below, it's **http://<OVOC server IP address>/firmwarefiles;ipp/dhcpoption160.cfg**. See the *Device Manager Pro Administrator's Manual* for more information.

Figure 3-11: Predefined Options and Values – Add OVOC Server Location



Note: Make sure you defined in the enterprise's DHCP server **http://<OVOC server IP address>/firmwarefiles;ipp/dhcpoption160.cfg** for DHCP Option 160.

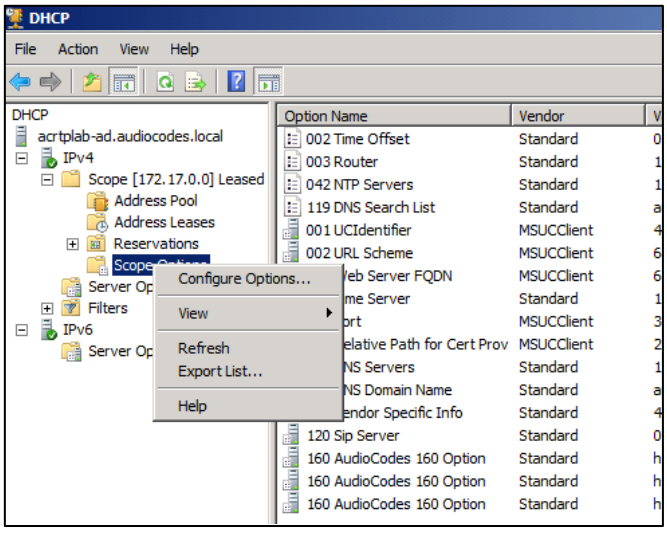
10. Decide if the DHCP Scope Option needs to be assigned to phones in a *specific VLAN (Scope)*, or to the *entire server* (acrtplab-ad.audiocodes.local) for IPv4 addresses.

    VLAN Scope

11. Assign to a specific VLAN (Scope of IP addresses such as the Scope below 172.17.0.0, or to multiple Scopes, to be performed separately on each Scope).

    a. If selecting a VLAN, expand the 'Scope Leased' folder, select 'Scope Options', and then select **Configure Options** from the popup menu.

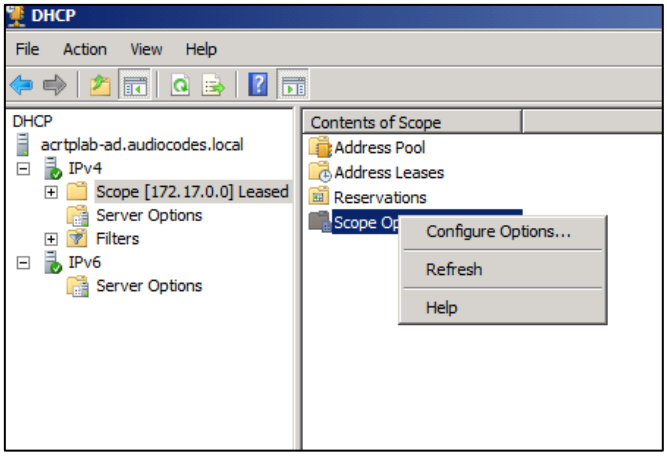
Figure 3-12: 'Scope Leased' Folder - Configure Options



-OR-

b. Select the collapsed folder 'Scope Leased' and in the main screen, right-click 'Scope Options' and select **Configure Options…**

Figure 3-13: Configure Options 1

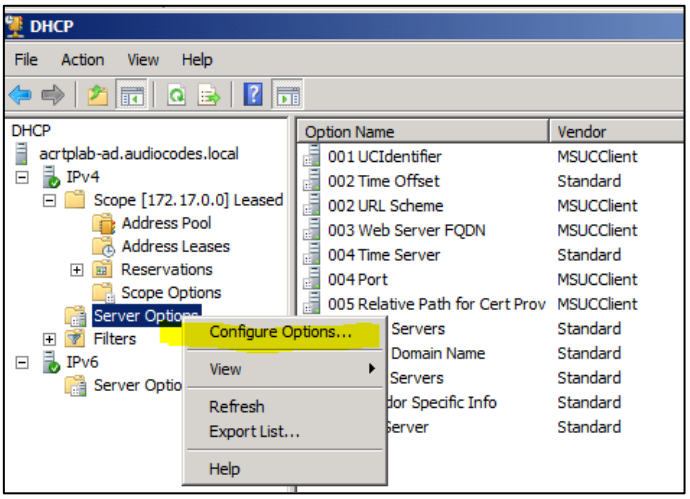


-OR-

Server Option

12. If assigning to the entire server (acrtplab-ad.audiocodes.local), select the 'Server Options' folder under server **IPv4**, right-click 'Server Options' and select **Configure Options...**

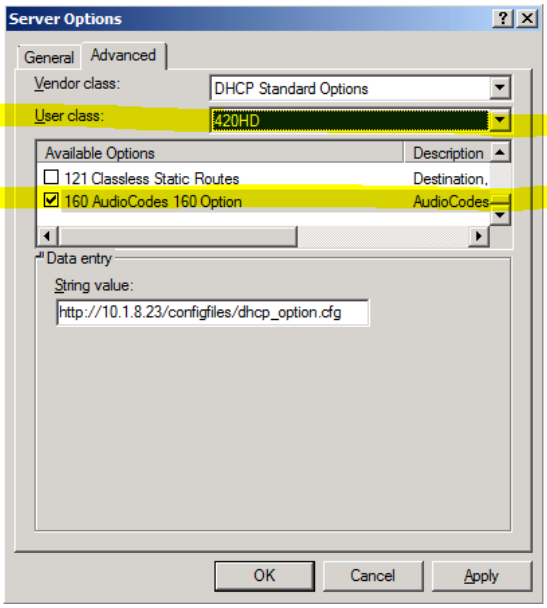
Figure 3-14: Configure Options 2



13. In the Server Options page (or Scope Options page) that opens, select the **Advanced** tab, make sure **DHCP Standard Options** remains selected, and select the first phone model to be defined. Scroll through the Available Options (all are cleared) and select only **160 AudioCodes 160 Option**.

The figure below shows the Server Options page. The Scope Options page is identical. Note that the String value you defined for Scope Option 160 is automatically populated so it's unnecessary to change it. Note also that if additional DHCP Options are required (such as DNS or time server) that are different from the Servers Options for the rest of the Scopes on the server, they can also be selected, but this is typically not needed.

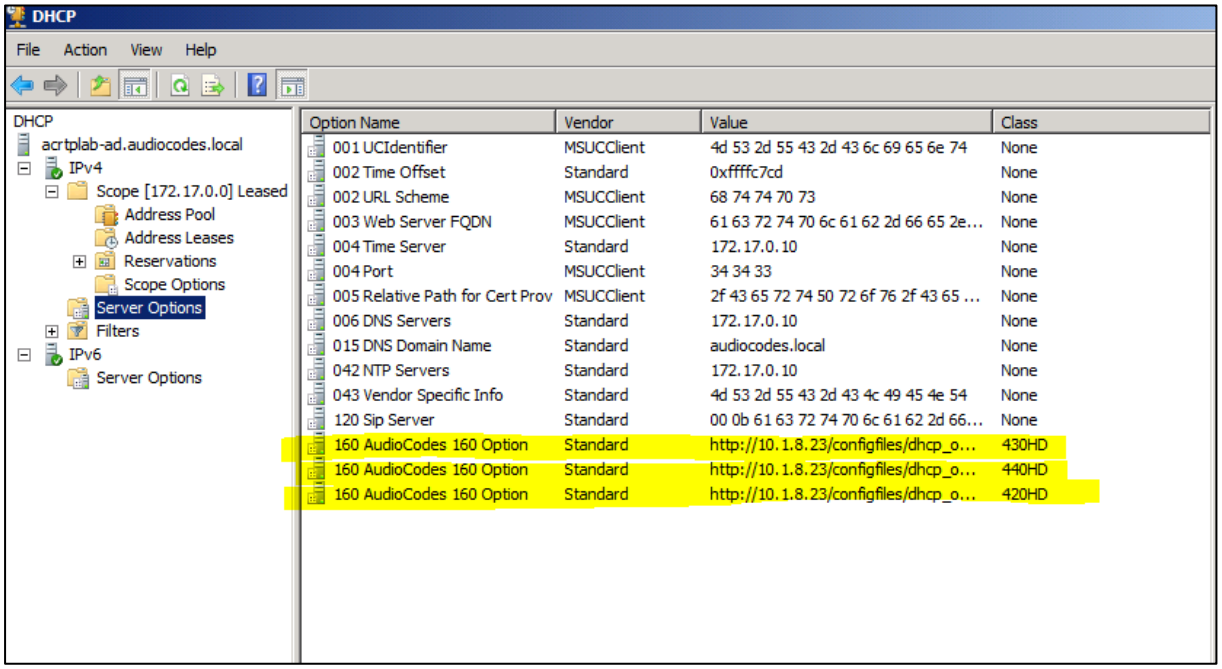
Figure 3-15: Server Options



14. Click **Apply** and then follow the same procedure to add the other user classes. After adding them, click the **OK** button.

You've successfully created Scope Options that will only allow AudioCodes phones to connect to the Device Manager when they boot up and will prevent other vendor phones from receiving the Device Manager as their provisioning server.

Figure 3-16: Scope Options Created



3.1.2.7 SIP SUBSCRIBE and NOTIFY Messages

If the provisioning information (e.g. Option fields 66/67/160) is not provided by the DHCP server, the phone sends a SIP SUBSCRIBE message to the multicast address **224.0.1.75:5060** as shown below.

Note: If the provisioning server supports using SIP SUBSCRIBE and NOTIFY messages and the device receives the provisioning URL in the NOTIFY message, the automatic provisioning mechanism then periodically tries to retrieve a new firmware/configuration according to the information provided.

```
SUBSCRIBE sip:224.0.1.75:5060 SIP/2.0
From: <sip:00000001@10.13.2.37:5060>;tag=87a5a8-25020d0a-13c4-
50029-386d4398-66dc40c-386d4398
To: <sip:224.0.1.75:5060>
Call-ID: 8884c8-25020d0a-13c4-50029-386d4398-3e2bcb8e-386d4398
CSeq: 1 SUBSCRIBE
Via: SIP/2.0/UDP 10.13.2.37:5060;rport;branch=z9hG4bK-386d4398-
6ad00ca2-7ca3606e
Expires: 0
Event: ua-profile;profile-
type="application";model="440HD";version="2.2.2"
Max-Forwards: 70
Supported: replaces,100rel
Accept:  application/url
Contact: <sip:00000001@10.13.2.37:5060>
User-Agent: AUDC-IPPhone/2.2.2
Content-Length: 0
```

The provisioning server or any other entity replies with a 200 OK message to the SUBSCRIBE message (see below) and sends a NOTIFY SIP message with the provisioning URL in the message body as shown below. (The provisioning URL can be in any format as described in the Administrator's Manual).

If no response is received by the provisioning server, the phone resends SUBSCRIBE messages for five seconds.

With the above method, the phone uses its built-in auto-provisioning mechanism while the provisioning information is retrieved through the NOTIFY message.

The following code describes **SIP 200 OK Response on the SUBSCRIBE Message**:

```
SIP/2.0 200 OK
Via: SIP/2.0/UDP 10.13.2.37:5060;rport;branch=z9hG4bK-386d4398-
6ad00ca2-7ca3606e
Contact: <sip:10.13.2.37:5060>
To: <sip:224.0.1.75:5060>
From: <sip:00000001@10.13.2.37:5060>;tag=87a5a8-25020d0a-13c4-
50029-386d4398-66dc40c-386d4398
Call-ID: 8884c8-25020d0a-13c4-50029-386d4398-3e2bcb8e-386d4398
CSeq: 1 SUBSCRIBE
Expires: 0
Content-Length: 0
```

The following code describes **SIP NOTIFY Message with Provisioning Information**.

```
NOTIFY sip:10.13.2.37:5060 SIP/2.0
Via: SIP/2.0/UDP 10.13.2.37:5060;rport;branch=z9hG4bK-386d4398-
6ad00ca2-7ca3606e
Max-Forwards: 20
Contact: <sip:10.13.4.121:5060>
To: <sip:224.0.1.75:5060>
```

```
From: <sip:00000001@10.13.2.37:5060>;tag=87a5a8-25020d0a-13c4-
50029-386d4398-66dc40c-386d4398
Call-ID: 8884c8-25020d0a-13c4-50029-386d4398-3e2bcb8e-386d4398
CSeq: 1 NOTIFY
Content-Type: application/url
Subscription-State: terminated;reason=timeout
Event: ua-profile;profile-
type="application";model="440HD";version="2.2.2"
Content-Length: 18
tftp://10.13.4.121
```

The following code describes **SIP SUBSCRIBE Message to Obtain Provisioning Information.**

```
SUBSCRIBE sip:224.0.1.75:5060 SIP/2.0
From: <sip:00000001@10.13.2.37:5060>;tag=87a5a8-25020d0a-13c4-
50029-386d4398-66dc40c-386d4398
To: <sip:224.0.1.75:5060>
Call-ID: 8884c8-25020d0a-13c4-50029-386d4398-3e2bcb8e-386d4398
CSeq: 1 SUBSCRIBE
Via: SIP/2.0/UDP 10.13.2.37:5060;rport;branch=z9hG4bK-386d4398-
6ad00ca2-7ca3606e
Expires: 0
Event: ua-profile;profile-
type="application";model="440HD";version="2.2.2"
Max-Forwards: 70
Supported: replaces,100rel
Accept:  application/url
Contact: <sip:00000001@10.13.2.37:5060>
User-Agent: AUDC-IPPhone/2.2.2
Content-Length: 0
```

With the above method, the phone uses its built-in auto-provisioning mechanism while the provisioning information is retrieved through the NOTIFY message.

3.1.2.8 Hardcoded Domain Name for Provisioning Server

If no higher-priority provisioning method applied, the phone automatically searches in the DNS server for the domain named "ProvisioningServer". After the DNS server gives the domain IP address, the phone contacts the provisioning server. The phone tries to retrieve firmware and configuration files using URL **tftp://ProvisioningServer/<Phone Model Name>/**

For example:

- The phone tries to obtain the following firmware file:
  tftp://ProvisioningServer/440HD.img

  where **440** is optional; if omitted, the phone will try to retrieve the firmware file according to its model name.
- The phone tries to obtain the following configuration file:
  tftp://ProvisioningServer/<MAC address>.cfg

  where **MAC address** is optional; if omitted, the phone will try to retrieve the configuration file according to its MAC address.

  (e.g. tftp://ProvisioningServer/440HD/001122334455.cfg)

The network administrator must configure a DNS entry called "ProvisioningServer" on the DNS server and set it to the TFTP server IP address.

Note: If Generic Domain Name is used, the automatic provisioning feature periodically tries to retrieve new firmware/configuration from Provisioning Server domain name.

3.1.2.9 Cached Address of Last Provisioning Server Used

These are the addresses of the last provisioning servers used, stored in cache memory.

When the device starts up and connects to the provisioning server, it can pull firmware, configuration and private label files from the provisioning server using the cached address of the last provisioning server used.

After the phone creates a successful connection with a provisioning server, this server's address is cached by the phone. The next time the phone is rebooted, if it doesn't receive provisioning details, the device performs provisioning using the cached IP address.

3.1.2.10 Redirect Server

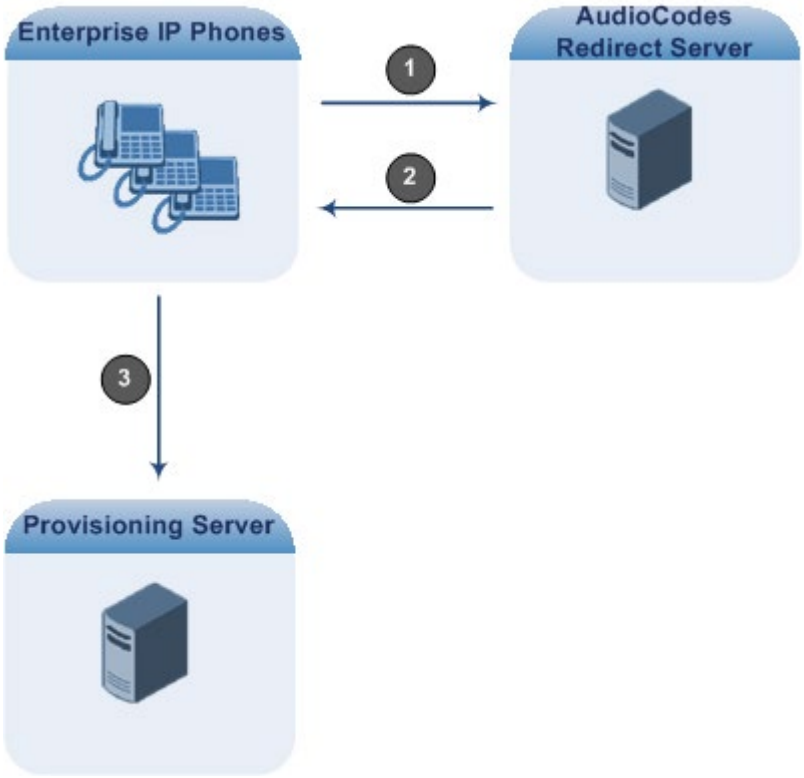
Network administrators can use the AudioCodes Redirect server to direct to the appropriate Provisioning server URL to download the relevant configuration and firmware files.

After the phone is powered up and network connectivity is established, it automatically requests provisioning information. If it doesn't get these files according to the regular provisioning hunt order methods, it sends an HTTPS request to the AudioCodes HTTPS Redirect server. The server responds to the phone with an HTTPS Redirect response containing the URL of the provisioning server where the firmware and configuration files are located. After the phone successfully connects to the provisioning server URL, the Automatic Update mechanism commences.

Note:

- The MAC addresses of the phones and the provisioning server's URL are pre-configured on the HTTPS Redirect server. For more information, contact AudioCodes support.
- The default URL of the Redirect server is:
  provisioning/redirect_server_url=https://redirect.audiocodes.com
  This address can be reconfigured if required.

Figure 3-17: Redirect Server Configuration Process



1. Device sends HTTPS request to AudioCodes HTTPS Redirect server.
2. Redirect server sends HTTPS response with redirect URL of the provisioning server.
3. Phone sends request to redirected URL (i.e., provisioning server).

For security, communication between the phone and the HTTPS Redirect server is encrypted (HTTPS) and uses the pre-installed AudioCodes factory-set certificate to authenticate itself with the HTTPS Redirect server and to verify authenticity of the latter. If the redirect URL (where the configuration file is stored) also uses the HTTPS protocol, the phone can use a regular certificate or the AudioCodes factory-set certificate to authenticate itself and to validate the server's certificate if a trusted root certificate (regular) is configured.

Note: The phone repeats the redirect process whenever it undergoes a reset to factory defaults.

3.1.3 Static URL Provisioning

The network administrator can configure the phone using the Static URL method.

➢ **To configure static provisioning information:**

- Use the table as reference.

Table 3-3: Static URL Automatic Provisioning Parameters

Parameter	Description
provisioning/method	Defines the provisioning method: ▪ Disable - Automatic update is disabled. The phone attempts to upgrade its firmware and configuration ▪ Dynamic DHCP Options (Dynamic URL) (default) - Using DHCP Option 160 and Options 66/67 for provisioning ▪ Static URL - Using Static URL for provisioning
provisioning/firmware/url	The static URL for checking the firmware file. The URL must be entered using one of the following syntax options: ▪ <protocol>://<server IP address or host name> ▪ <protocol>://<server IP address or host name>/<firmware file name> Where<protocol> can be one of the following protocols: **ftp**, **tftp**, **http** or **https**. For example: ▪ tftp://192.168.2.1 – retrieved firmware file is440HD.img ▪ ftp://192.168.2.1/Different_Firmware_Name.img - retrieved firmware file is Different_Firmware_Name.img **Note:** This parameter is applicable only when 'method' is configured to **Static**.
provisioning/configuration/url	Static URL for checking the configuration file, entered using syntax: ▪ <protocol>://<server IP address or host name> ▪ <protocol>://<server IP address or host name>/<configuration file name> Where<protocol> can be one of the following protocols: "ftp", "tftp", "http" or "https". For example: ▪ http://192.168.2.1 - configuration file name is <MAC Address>.cfg, for example, 001122334455.cfg ▪ https://192.168.2.1/440HD_<MAC>_conf.cfg - retrieved configuration file name is 440HD_<MAC Address>_conf.cfg, for example, 440HD_001122334455_conf.cfg **Note:** Applicable only when 'method' is configured to **Static**.

3.1.4 Forcing a Reboot on Provisioning

This feature lets the call center's network administrator configure a forced reboot on phones after provisioning.

Note: Support pending.

➢ **To force a reboot on provisioning using configuration file:**

- Use the table as reference.

Table A-4: Forcing a Reboot on Provisioning

Parameter	Description
voip/services/notify/check_sync/force_reboot_enabled	Determines whether or not to force a reboot on provisioning. ▪ **0** Disable (default) ▪ **1** Enable

4 Configuring Networking

Network settings can be configured *manually*, if required.

Note: By default, the network settings are set for *automatic provisioning*. However, if you need to change them, you can do so *manually*, as described in this section.

4.1 Configuring Date and Time Manually

Note: By default, date and time settings are *automatically provisioned* via the enterprise DHCP server when the phone is connected to the Internet and to the power supply, but you can *manually* change them if required. This section shows how.

The phone automatically retrieves date and time from a Network Time Protocol (NTP) server when connected to the internet. To configure the NTP server for automatic provisioning of date and time, see Section 4.1.2. NTP is a protocol for distributing Coordinated Universal Time (UTC) by synchronizing the clocks of computer systems over packet-switched, variable-latency data networks.

➢ **To configure date and time:**

- Use the table as reference.

Table 4-1: Date Display Format

Parameter	Description
system/ntp/date_display_format	Select either: ▪ **EUROPEAN** (default) ▪ **AMERICAN** The European date format is DDMMYYYY. The American format is MMDDYYYY.

4.1.1 Configuring Daylight Saving Time

Network administrators can configure Daylight Saving Time.

➢ **To configure Daylight Saving Time:**

- Use the table as reference.

Table 4-2: Daylight Saving Time Parameters

Parameter	Description
system/daylight_saving/activate	Determines whether the phone automatically detects the Daylight Saving Time for the selected Time Zone. ▪ **DISABLE** Disable (default) ▪ **ENABLE** Enable
system/daylight_saving/start_date	This subsection defines the starting day for the daylight saving offset. ▪ month - defines specific month in year ▪ day - defines specific day in month ▪ hour - defines specific hour in day ▪ minute - defines specific minute in hour Example: To configure the phone to start daylight savings with a specific offset on February 22nd at 14:30, set the following: system/daylight_saving/start_date/month=2 system/daylight_saving/start_date/day=22 system/daylight_saving/start_date/hour=14 system/daylight_saving/start_date/minute=30
system/daylight_saving/start_date/month	The month in a year. The valid range is 1 to 12.
system/daylight_saving/start_date/day	The day in a month. The valid range is 1 to 31.
system/daylight_saving/start_date/hour	The hour in the day. The valid range is 0 to 23.
system/daylight_saving/start_date/minute	The minute in an hour. The valid range is 0 to 59.

Parameter	Description
system/daylight_saving/end_date	This subsection defines the ending day for the daylight saving offset. ▪ **month** - defines the specific month in a year ▪ **day** - defines the specific day in a month ▪ **hour** - defines the specific hour in a day ▪ **minute** - defines the specific minute in an hour For example: To configure the phone to end the daylight savings on July 16th at 22:15, set the following: system/ntp/daylight_saving/end_date/month=7 system/ntp/daylight_saving/end_date/day=16 system/ntp/daylight_saving/end_date/hour=22 system/ntp/daylight_saving/end_date/minute=15
system/daylight_saving/end_date/month	The month in a year. The valid range is 1 to 12.
system/daylight_saving/end_date/day	The day in a month. The valid range is 1 to 31.
system/daylight_saving/end_date/hour	The hour in the day The valid range is 0 to 23.
system/daylight_saving/end_date/minute	The minute in an hour. The valid range is 0 to 59.
system/daylight_saving/offset	The offset value for the daylight saving. The valid range is 0 to 180. The default offset is 60.
system/daylight_saving/mode	Configures the daylight saving mode. Valid values are **FIXED=** Date is specified as: Month, Day of month. **DayOfWeek=** Date is specified as: Month, Week of month, Day of week.
system/daylight_saving/start_date/week	Relevant to 'Day of week' mode: The week of month (values 1-5) for start of daylight saving time.
system/daylight_saving/start_date/day_of_week	Relevant to 'Day of week' mode: The day of week for daylight saving time start Valid values : **SUNDAY** **MONDAY** **TUESDAY** **WEDNESDAY** **THURSDAY** **FRIDAY** **SATURDAY**

Parameter	Description
system/daylight_saving/end_date/week	Relevant to 'Day of week' mode: The week of month (values 1-5) for end of daylight saving time.
system/daylight_saving/end_date/day_of_week	Relevant to 'Day of week' mode: The day of week for daylight saving time start Valid values : **SUNDAY** **MONDAY** **TUESDAY** **WEDNESDAY** **THURSDAY** **FRIDAY** **SATURDAY**

4.1.2 Configuring the NTP Server

The Network Time Protocol (NTP) server can be configured. When activated, date and time are automatically obtained from the NTP server.

➢ **To configure the NTP server:**

- Use the table as reference.

Table 4-3: NTP Server Parameters

Parameter	Description
system/ntp/enabled	Enables the NTP server from which the phone automatically retrieves the date and time. ▪ **0** Disable ▪ **1** Enable – obtains the time information automatically from a configured NTP server (default)
system/ntp/primary_server_address	Defines the address of the main NTP server (this can be a domain name, for example, tick.nap.com.ar).
system/ntp/secondary_server_address	Defines the address of the secondary NTP server.
system/ntp/sync_time	This sub-section defines how often the phone must perform an update with the NTP server. ▪ **days** -defines the number of days ▪ **hours** - defines the number of hours For example: To configure the phone to perform an update with an NTP server every 1 day and 6 hours, set the following: **system/ntp/sync_time/days=1** **system/ntp/sync_time/hours=6**
system/ntp/sync_time/days	The number of days. The valid range is 0 to 7. The default of days is 0.

Parameter	Description
system/ntp/sync_time/hours	The number of hours. The valid range is 0 to 24. The default is 12.
system/ntp/time_display_format	The format of the time displayed on the phone screen. ▪ **24Hour** (default) ▪ **12Hour**

4.1.3 Configuring NTP Server via DHCP

If the phone is set to obtain GMT offsets and NTP servers via DHCP (default), it receives the following fields in the DHCP options:

- Primary Server and Secondary Server – (Option 4 or 42).

Note: If both options (4 and 42) are received, priority is given to Option 42.

- Time Zone – (Option 2)

The phone sends an NTP request to the Primary NTP server. If there is no response, the NTP request is sent to the Secondary NTP server.

After obtaining the time from the server, it adds the GMT offset in Option 2. This is the updated system time.

Note: These values will have no effect if TimeZone is set to be obtained from DHCP. If Time Zone and NTP server are manually set, the phone acts as described above but the values are obtained from the configuration file and not from DHCP.

Table 4-4: NTP Server and GMT Parameters

Parameter	Description
system/ntp/gmt_offset	Default: 00:00 Enables the NTP server from which the phone retrieves the date and time. ▪ **0** Disable (default) ▪ **1** Enable – obtains the time information from a configured NTP server

4.2 Configuring IP Network Settings

The following section shows how to configure IP Network Settings including:

- Static IP Address
- Partial DHCP

4.2.1 Configuring Static IP Address

The static IP address can be configured using the following:

- Phone screen
- Configuration file

4.2.1.1 Configuring Static IP Address on the Phone

The network administrator can configure Static IP Address on the phone. The LAN connection interface can be manually defined (static IP address) or automatically provisioned using a DHCP server from where the LAN IP address is obtained.

➢ **To configure the phone's LAN connection type:**

1. Access and select the **LAN Connection Type** option (MENU key > **Administration** > **Network Settings**).
2. Navigate to and select **LAN Connection Type**.
3. In the LAN Connection Type screen, select **Static IP**.
4. Define a static IP addressing scheme:
   a. Press the **Edit** softkey; the Static IP screen is displayed.
   b. Configure each required network parameter: **IP Address**, **Netmask**, **Gateway**, **Primary DNS** and **Secondary DNS**.
   c. Enter the new address in dotted-decimal notation, using the **Clear** softkey to delete the digit to the left of the cursor. Press the * key to enter a dot.
5. Press the **Save** softkey that becomes activated.

4.2.1.2 Configuring IP Network Settings

IP Network settings can be configured. The phone's LAN configuration includes defining the method for obtaining an IP address. The phone's IP address can be *static* whereby the IP address is manually entered, or *automatic* whereby the IP address is acquired from a DHCP server. For Automatic IP, you can manually define some of the main parameters.

➢ **To define the phone's LAN settings:**

- Use the table as reference.

Table 4-5: Network Settings Parameters

Parameter	Description
network/lan_type	Defines the IP addressing method: ▪ **STATIC** IP (default)- Phone's IP address is defined manually ▪ **DHCP** Automatic IP DHCP - Phone's IP address is acquired automatically from a DHCP server
network/lan/fixed_ip	This subsection defines the relevant parameters if 'lan_type' is configured to **STATIC** or the corresponding 'network/lan/dhcp' parameter is set to 1.
network/lan/fixed_ip/ip_address	The LAN IP address.
network/lan/fixed_ip/netmask	The subnet mask address.
network/lan/fixed_ip/gateway	The IP address of the default gateway.
network/lan/fixed_ip/domain_name	The domain name.
Domain Name Server (DNS)	
network/lan/fixed_ip/primary_dns	The primary DNS server address.
network/lan/fixed_ip/secondary_dns	The secondary DNS server address. The phone connects to this server if the primary DNS server is unavailable.

4.2.2 Configuring Partial DHCP

Partial DHCP can be configured with the following parameters:

Table 4-6: Partial DHCP Parameters

Parameter	Description
Partial DHCP	
network/lan/dhcp	If 'lan_type' is configured to **DHCP**, this parameter and the parameters in this table must be configured.
network/lan/dhcp/domain_name/enabled	Enables setting the domain name manually. ▪ **0** Disable (default) ▪ **1** Enable **Note:** If enabled, **network/lan/fixed_ip/domain_name** must be set.
network/lan/dhcp/ip_address/enabled	Enables setting the IP address manually. ▪ **0** Disable ▪ **1** Enable (default) **Note:** If enabled, **network/lan/fixed_ip/ip_address** must be set.
network/lan/dhcp/netmask/enabled	Enables setting the network mask manually. ▪ **0** Disable ▪ **1** Enable (default) **Note:** If enabled, **network/lan/fixed_ip/netmask** must be set.
network/lan/dhcp/gateway/enabled	Enables setting the default gateway manually. ▪ **0** Disable ▪ **1** Enable (default) **Note:** If enabled, **network/lan/fixed_ip/gateway** must be set.
network/lan/dhcp/primary_dns/enabled	Enables setting the primary DNS manually. ▪ **0** Disable (default) ▪ **1** Enable **Note:** If enabled, **network/lan/fixed_ip/primary_dns** must be set.
network/lan/dhcp/secondary_dns/enabled	Enables setting the secondary DNS manually. ▪ **0** Disable (default) ▪ **1** Enable **Note:** If enabled, **network/lan/fixed_ip/secondary_dns** must be set.

Parameter	Description
DHCP-Related Parameters	
network/lan/dhcp/ntp/server_list/enabled	Enables prioritization of the NTP server's information received from the DHCP server (Option fields 42 or 4), over the static configuration (**system/ntp/primary_server_address** and **system/ntp/secondary_server_address**). ▪ **0** Disable ▪ **1** Enable (default)
network/lan/dhcp/ntp/gmt_offset/enabled	Enables prioritization of the NTP GMT offset information received from the DHCP server (Option field 2), over the static configuration (**system/ntp/gmt_offset**). ▪ **0** Disable ▪ **1** Enable (default)

4.3 Configuring LAN and PC Port Settings

Port settings can be configured.

➢ **To define the phone's port settings:**

- Use the table as reference.

Table 4-7: Port Settings

Parameter	Description
network/lan/port_mode	Sets the LAN port mode. Valid values are: AUTOMATIC = Auto negotiation. FULL_10 = 10Mbps + full duplex FULL_100 = 100Mbps + half duplex HALF_10 = 10Mbps + full duplex HALF_100 = 100Mbps + half duplex FULL _ 1Gbps = 1 Gbit/s port + full duplex
network/pc/port_mode	Sets the computer port mode. Valid values are: AUTOMATIC = Auto negotiation FULL_10 = 10Mbps + full duplex FULL_100 = 100Mbps + half duplex HALF_10 = 10Mbps + full duplex HALF_100 = 100Mbps + half duplex DISABLE = Disables the PC port mode

4.4 Configuring VLAN Settings

Network administrators can configure VLAN settings.

➢ **To configure the phone's VLAN settings:**

- Use the table as reference.

Table 4-8: VLAN Settings

Parameter	Description
network/lan/vlan/mode	Determines how VLAN is assigned to your phone, i.e., manually or automatically, and if automatically, according to which protocol. ▪ Disable **Disable** ▪ Manual Configuration of VLAN **Manual** - If selected, the screen extends to also display 'VLAN ID' and 'VLAN Priority' (see these settings below) for static configuration of VLAN ID and priority. See Section 4.4.1 below for a detailed explanation. ▪ Automatic Configuration of VLAN (CDP) **CDP** - VLAN discovery mechanism based on Cisco Discovery Protocol (CDP). See Section 4.4.1 below for a detailed explanation. ▪ Automatic Configuration of VLAN (LLDP) **LLDP** - VLAN discovery mechanism based on LLDP. See Section 4.4.1 below for a detailed explanation. ▪ Automatic Configuration of VLAN (CDP+LLDP) **CDP_LLDP** (default) - VLAN discovery mechanism based on LLDP and CDP. LLDP is higher priority. See below for a detailed explanation.
network/lan/vlan/period	The time period, in seconds, between discovery messages when configured to CDP, LLDP or CDP+LLDP. The default value is 30.
network/lan/vlan/id	The VLAN ID. The valid range is 0 to 4094. The default is 0.
network/lan/vlan/priority	The priority of traffic pertaining to this VLAN. The valid range is 0 to 7 (where 7 is the highest priority). The default is 0.
network/lan/vlan/pc_port_tagging/enable	Default = **Disable 0**. Change to **Enable (1)** for the traffic from the PC to the network to be VLAN-tagged.

4.4.1 Configuring Manual or Automatic VLAN Assignment

Network administrators can configure the VLAN to be assigned manually or automatically to the phone. This section shows when to configure what, and why.

4.4.1.1 Configuring Manual VLAN Assignment to the Phone

Configure manual assignment of the VLAN in order to set up two separate VLANs in your enterprise, one for voice (your phone) and the other for data (your pc). Security considerations may require this. If you configure manual assignment, the switch in your enterprise will assign the VLAN to your phone. See Sections 4.2.1.1 and 4.2.1.2 for details.

4.4.1.2 Configuring Automatic VLAN Assignment to the Phone

Configure automatic assignment of VLAN if you do not need to separate voice from data, i.e., if there are no security considerations requiring it. In this case, configure either:

- Automatic Configuration of VLAN (CDP) **CDP**

  Automatic Configuration of VLAN (LLDP) **LLDP** -OR-
- Automatic Configuration of VLAN (CDP+LLDP) **CDP_LLDP**

What you select depends on whether the switch deployed in your enterprise supports Cisco-proprietary Cisco Discovery Protocol (CDP), or LLDP (Link Layer Discovery Protocol) which is a vendor-neutral protocol used by devices in an IEEE 802 LAN to advertise their identity, capabilities, and neighbors. Not all switches support CDP. If You're unsure, select **CDP+LLDP**. LLDP includes enhanced LLDP for Media Endpoint Devices, i.e., LLDP-MED, to specifically address voice applications.

4.4.1.3 Configuring VLAN via DHCP Provisioning Path

VLAN can be configured using (1) Link Layer Discovery Protocol (LLDP) (2) Cisco Discovery Protocol (CDP) (3) manually (4) no method.

If (1) is unsuccessful, (2) is attempted.

If (2) is unsuccessful, (3) is attempted.

If (3) is unsuccessful, (4) is attempted.

The capability provides an alternative VLAN configuration option.

4.4.2 Wi-Fi Capability

Note: Only applies to the 445HD and C450HD phone. See the *Release Notes* for supported models.

The phone can connect to an Access Point via Wi-Fi. The Wi-Fi interface can be used when the phone is installed in an environment free of LAN/cables, to perform VoIP calls over Wi-Fi. The phone can be connected by pressing the **Networks** icon in the phone's main menu -or- navigating in the 'Settings' menu and then selecting the **Wi-Fi** option.

This page is intentionally left blank.

5 Configuring VoIP Settings

5.1 Configuring SIP Settings

Network administrators can configure the following SIP settings:

- General
- Proxy and Registration
- SIP Timers
- SIP QoS

5.1.1 Configuring General SIP Settings

The phone's General SIP settings can be configured.

➢ **To configure General SIP parameters:**

- Use the table as reference.

Table 5-1: SIP General Parameters

Parameter	Description
voip/signalling/sip/transport_protocol	Determines the transport layer for outgoing SIP calls initiated by the phone. ▪ **UDP** UDP (default) ▪ **TCP** TCP ▪ **TLS** TLS
voip/signalling/sip/tls_port	Defines the local TLS SIP port for SIP messages. The valid range is 1024 to 65535. The default value is 5061.
voip/signalling/sip/enable_sips	Relevant for TLS only, if enabled, the request URI prefix will be “sips:” otherwise, the prefix will be “sip:”
voip/signalling/sip/subs_no_notify_timer	Indicates the maximum time (in milliseconds) that a subscription waits from receiving 2xx response for a SUBSCRIBE request, until receiving the first NOTIFY request. If the timer expires, the subscription will be terminated.
voip/signalling/sip/port	Defines the local SIP port (UDP or TCP) for SIP messages. The valid range is 1024 to 65535. The default value is 5060.
voip/signalling/sip/proxy_gateway	Assigns a name to the phone. The name is used as the host part of the SIP URI in the From header. **Note:** ▪ Ensure that the name you choose is the one with which the Proxy is configured to identify the phone. ▪ If not specified, the phone's IP address is used (default).

Parameter	Description
voip/signalling/sip/prack/enabled	Determines whether the phone sends PRACK (Provisional Acknowledgment) messages upon receipt of 1xx SIP reliable responses. ▪ **0** Disable ▪ **1** Enable (default)
voip/signalling/sip/rport/enabled	Determines whether the phone adds the 'rport' parameter to the relevant SIP message (in the SIP Via header). ▪ **0** Disable (default) ▪ **1** Enable
voip/signalling/sip/sdp_include_ptime	Determines whether the phone adds the PTIME parameter to the SDP message body. ▪ **0** Disable (default) ▪ **1** Enable
voip/signalling/sip/keepalive_options/enabled	Determines whether keep-alive is performed using SIP OPTIONS messages sent to the Proxy. ▪ **0** Disable (default) ▪ **1** Enable
voip/signalling/sip/keepalive_options/timeout	Defines the Proxy keep-alive time interval (in seconds) between Keep-Alive messages. ▪ The valid range is 0 to 86400. The default value is 300.
voip/signalling/sip/connect_media_on_180	Determines whether the media is connected upon receipt of SIP 180, 183, or 200 messages. When the parameter is disabled, media is connected upon receipt of 183 and 200 messages only. ▪ **0** Disable (default) ▪ **1** Enable
voip/signalling/sip/block_callerid_on_outgoing_calls	Can be configured only if the BroadSoft BroadWorks application server is used. When enabled, the outgoing INVITE message is sent with an anonymous From header and P-Asserted-Identityheader. ▪ **0** Disable (default) ▪ **1** Enable For example: ▪ FROMheader contains anonymous URI: *From: "Anonymous" sip:anonymous@anonymous.invalid* ▪ P-Asserted-Identityheader: *P-Asserted-Identity:* "1001" 1115551001@proxy.net

Parameter	Description
voip/signalling/sip/anonymous_calls_blocking	Can be configured only if the BroadSoft BroadWorks application server is used. When enabled, incoming INVITE messages with anonymous From header are rejected. ▪ **0** Disable (default) ▪ **1** Enable For example: *From:"Anonymous"<sip:anonymous@anonymous.invalid>* The phone responds with a SIP 403 "Forbidden" response.
voip/signalling/sip/auth_retries	Defines the number of times authenticated register messages are re-sent if 401 or 407 SIP responses with a different "nonce" are received. The valid range is 0 to 100. The default value is 10.
voip/signalling/sip/display_name_in_registration_msg/enabled	Sets the Display Name in the 'To' and 'From' fields of the SIP REGISTER message. ▪ **0** Disable (default) ▪ **1** Enable
voip/signalling/sip/semi_transfer_with_no_cancel/enabled	Determines whether semi-attendant transfer is performed without sending the SIP CANCEL message to the remote side. ▪ **0** Disable (default) ▪ **1** Enable **Note:** ▪ In this flow ("with_no_cancel"), the Transferor's User Agent continues the transfer as an attended transfer even after the Transferor hangs up. This is the recommended flow defined by http://tools.ietf.org/html/draft-ietf-sipping-cc-transfer-03. ▪ Existing / current behavior is retained for backward compatibility (disabled by default)
voip/signalling/sip/PAI_On_Replay/enable	Enables the P-Asserted Identity header to be added to “18x” and “200” responses. ▪ **0** (Default) PAI header is not added to “18x” and “200” responses ▪ **1** PAI header is added to “18x” and “200” responses

5.1.2 Configuring Proxy and Registration

Proxy and Registration settings can be configured.

➢ **To configure Proxy and Registration:**

- Use the table as reference.

Table 5-2: Proxy and Registrar Parameters

Parameter	Description
voip/signalling/sip/use_proxy	Determines whether to use a SIP Proxy server. ▪ **0** Disable (default) ▪ **1** Enable
voip/signalling/sip/proxy_address	The IP address or host name of the SIP proxy server. Default: 0.0.0.0
voip/signalling/sip/proxy_port	The UDP or TCP port of the SIP proxy server. Range: 1024 to 65535. Default: 5060.
voip/signalling/sip/registrar_ka/enabled	Determines whether to use the registration keep-alive mechanism based on SIP OPTION messages. ▪ **0** Disable (default) ▪ **1** Enable **Note:** ▪ If there is no response from the server, the timeout for re-registering is automatically reduced to a user-defined value (voip/signalling/sip/registration_failed_timeout) ▪ When the phone re-registers, the keep-alive messages are re-sent periodically.
voip/signalling/sip/registrar_ka/timeout	Defines the registration keep-alive time interval (in seconds) between Keep-Alive messages. Range: 40 to 65536. Default: 60.
voip/signalling/sip/proxy_timeout	The SIP proxy server registration timeout (in seconds). Range: 0 to 86400. Default: 3600.
voip/signalling/sip/use_proxy_ip_port_for_registrar	Determines whether to use the SIP proxy's IP address and port for registration. When enabled, there is no need to configure the address of the registrar separately. ▪ **0** Disable ▪ **1** Enable (default)
voip/signalling/sip/sip_registrar/enabled	Determines whether the phone registers to a separate SIP Registrar server. ▪ **0** Disable (default) ▪ **1** Enable

Parameter	Description
voip/signalling/sip/sip_registrar/addr	Only displayed if the 'Use SIP Registrar' parameter is enabled. The IP address or host name of the Registrar server. Default: 0.0.0.0
voip/signalling/sip/sip_registrar/port	Only displayed if the 'Use SIP Registrar' parameter is enabled. The UDP or TCP port of the Registrar server. Range: 1024 to 65535. Default: 5060.
voip/signalling/sip/registration_failed_timeout	If registration fails, this parameter determines the interval between the register messages periodically sent until successful registration. Range: 1 to 86400. Default: 60.
voip/signalling/sip/sip_outbound_proxy/enabled	Determines whether an outbound SIP proxy server is used (all SIP messages are sent to this server as the first hop). ▪ **0** Disable (default) ▪ **1** Enable
voip/signalling/sip/sip_outbound_proxy/addr	Only displayed if the 'Use SIP Outbound Proxy' parameter is enabled. The IP address of the outbound proxy. If this parameter is set, all outgoing messages (including Registration messages) are sent to this Proxy according to the Stack behavior. Default: Blank.
voip/signalling/sip/sip_outbound_proxy/port	Only displayed if the 'Use SIP Outbound Proxy' parameter is enabled. The port on which the outbound proxy listens. Range: 1024 to 65535. Default: 5060.
voip/signalling/sip/register_before_expires_percent	Allows administrators to configure the registration expired time. The registration expired time is that time that lapses before the refresh registration message is sent. Default: 15%. Non-percentage values are 5-85. These represent the time that must lapse before the new registration message is sent, for example, 15% means that if the expiration time is 100 seconds, the registration refresh message will be sent after 85% of the registration expiring timeout. In releases before version 2.2.12, it was 33%.
voip/signalling/sip/redundant_proxy/mode	See the next section.

Note: It's recommended to use DNS queries to complete FQDN for a redundant outbound proxy.

5.1.2.1 Configuring Proxy Redundancy

The Redundant Proxy feature allows the configuration of a backup SIP proxy server to increase QoS stability. After the feature is enabled, the phone identifies cases where the primary proxy does not respond to SIP signaling messages. In these scenarios, the phone registers to the redundant proxy and the phone seamlessly continues normal functionality, without the user noticing any connectivity failure or malfunction with the primary proxy.

The Redundant Proxy feature can operate in one of the following modes:

- **Asymmetric mode**: The primary proxy is assigned a higher priority for registration than the redundant proxy. Once the phone is registered to the primary proxy, it sends keep-alive messages (using SIP OPTIONS messages) to the primary proxy. If the primary proxy does not respond, the phone registers to the redundant proxy, but continues sending keep-alive messages to the primary proxy**. If the primary proxy responds to these keep-alive messages, the phone re-registers to the primary proxy.**
- **Symmetric mode:** Both proxies are assigned the same priority for registration. Once the phone is registered to a proxy, it sends keep-alive messages to this proxy. The phone switches proxies only once the proxy to which it has registered, does not respond.

For more information see the voip/signalling/sip/redundant_proxy/symmetric_mode description in the SIP Proxy Server Redundancy Parameters table below.

➢ **To configure Proxy Redundancy:**

- Use the table as reference.

Table 5-3: SIP Proxy Server Redundancy Parameters

Parameter	Description
voip/signaling/sip/redundant_proxy/enabled	Mandatory for the phone to operate in redundancy. Commands the phone to operate with the other **voip/signalling/sip/redundant_proxy** parameters.
voip/signalling/sip/redundant_proxy/mode	Mandatory for the phone to operate in redundancy. Defines the two proxies' mode of operation: Primary-Fallback or Simultaneous. Defines a backup SIP proxy server to increase QoS stability. Enable the parameter if you want to operate with a proxy server that will serve as a backup if the first goes down. ▪ **Disable** = (Default) Phone doesn't use redundant proxy. ▪ **Primary-Fallback** = Phone registered to redundant proxy if the primary proxy does not respond to SIP signaling messages. ▪ **Simultaneous** = Applies only in some environments. If selected, dual registration is performed; the phone registers simultaneously to both servers. .
voip/signalling/sip/redundant_proxy/address	Only displayed if the 'Redundant Proxy Mode' parameter is enabled (Primary-Fallback) Defines the IP address of the backup proxy server. Default: **0.0.0.0**
voip/signalling/sip/redundant_proxy/keepalive_period	Only displayed if the 'Redundant Proxy Mode' parameter is enabled (Primary-Fallback) Defines how often a keep alive message is sent by the phone to the proxy server. Range: 0 to 300. Default: Every 60 seconds.

Parameter	Description
voip/signalling/sip/redundant_proxy/port	Only displayed if the 'Redundant Proxy Mode' parameter is enabled (Primary-Fallback) Defines the UDP or TCP port of the backup redundant proxy server. If occupied by other enterprise devices, you can configure another. Range: 1024 to 65535. Default = 5060.
voip/signalling/sip/redundant_proxy/symmetric_mode	Only displayed if the 'Redundant Proxy Mode' parameter is enabled (Primary-Fallback) The phone identifies cases where the primary proxy does not respond to SIP signaling messages. In these scenarios, the phone registers to the redundant proxy and the phone seamlessly continues normal functionality, without the user noticing any connectivity failure or malfunction with the primary proxy. **0** = Asymmetric (default). In this mode, the primary proxy is assigned a higher priority for registration than the redundant proxy. Once the phone is registered to the primary proxy, it sends keep-alive messages (using SIP OPTIONS messages) to the primary proxy. If the primary proxy does not respond, the phone registers to the redundant proxy, but continues sending keep-alive messages to the primary proxy. If the primary proxy responds to these keep-alive messages, the phone re-registers to the primary proxy. Therefore, the phone assigns the primary proxy a higher priority for registration. If asymmetric mode is configured and the primary server goes down, an attempt will be made to revert to the primary server. **1** = Symmetric. In this mode, both proxies are assigned the same priority for registration. Once the phone is registered to a proxy, it sends keep-alive messages to this proxy. The phone switches proxies only once the proxy to whom it has registered does not respond. Therefore, the phone assigns both proxies the same priority for registration. If symmetric mode is configured and the primary server goes down, you'll operate with the redundant proxy without ever reverting to the primary unless the redundant proxy also goes down. In both modes, the following applies: If the phone is not registered (i.e., if the proxy server – redundant or primary – to which the phone currently tries to register does not respond), the phone attempts to register to an alternative proxy. These attempts continue until the phone successfully registers. If this feature is enabled and the user reboots the phone, the phone registers to the last proxy to which it was trying to register, and not necessarily to the primary proxy.

5.1.2.2 Device Registration Failover/Failback

5.1.2.2.1 Failover

This feature enables a secondary server to take over the functions of the primary server on the enterprise network, if SIP communication between the SIP access device and the primary proxy server is blocked or delayed or the primary server isn't available.

No phone functionality is lost when the secondary server takes over.

Note:

- For failover to function, the Proxy DNS server must be configured with a list of the names of the proxies, in order and priority, i.e, SRV record. Before the phone tries to register, it performs an NAPTR / SRV query (see the table below for an explanation of these). The DNS server send a prioritized list. The phone sends a Registration request to the first SIP server; if it isn't responsive in *n* time retries (i.e., 'outgoing_request_no_response_timeout' parameter), it goes to the second, etc., until it gets a response.
- SIP Proxy/Outbound Proxy must be configured as the host name.

➢ **To configure failover:**

- Use the table as reference.

Table 5-4: Device Registration Failover Parameters

Parameter	Description
voip/signalling/sip/transport_protocol	Either: ▪ UDP (default) ▪ TCP ▪ TLS encryption In the SIP protocol, Name Authority Pointers (NAPTRs) are used to map servers and user addresses. Combined with Service Records (SRVs), they enable determining the service types available for a name, the name to use for an SRV lookup, and the port and 'A' DNS records to use to find the IP for the service.
voip/signalling/sip/outgoing_request_no_response_timeout_ms	This is the timeout, in milliseconds, that lapses until the phone failovers to the secondary proxy. Default: 32000
voip/signalling/sip/sip_outbound_proxy/addr	Configure this parameter as an SRV host name.
voip/signalling/sip/sip_outbound_proxy/port	Configure a value of **65535** for this parameter. Configure the parameter when you're using an Outbound Proxy. Either configure *this* parameter *or* the parameter 'Proxy Port'.
voip/signalling/sip/proxy_address	Configure this parameter as an SRV host name.
voip/signalling/sip/proxy_port	Configure a value of **65535** for this parameter. Configure the parameter when you're using a regular Proxy server. Either configure *this* parameter *or* the parameter 'Outbound Proxy Port'.

Parameter	Description
voip/signalling/sip/sip_registrar/port	Configure this parameter when you're using a regular Proxy server.

5.1.2.2.2 Failback

➢ **To configure failback:**

- Use the table as reference.

Table 5-5: Device Registration Failback Parameter

Parameter	Description
voip/signalling/sip/failback_retry_timeout	Only applies to BroadSoft. Applies only if you're operating with the DNS mode of failover, i.e., with a DNS server. ▪ **0** Disable (default) – it'll never try to access back to the first one. ▪ **n** Time, in seconds, that must lapse before failback is performed.

5.1.2.3 Preventing Unregistering after Changing Settings and Reloading

An unregistration message is *by default* sent after making a change to the VoIP application configuration and reloading.

The VoIP application *by default* sends a SIP Registration message with **Expires:0** (unregister).

The network administrator can change the default and prevent unregistering.

➢ **To prevent unregistering:**

- Use the table as reference.

Table 5-6: Preventing Unregistering

Parameter	Description
voip/signalling/sip/unregister_on_voip_reload	Either: ▪ **0** SIP Registration message with **Expires:0** (unregister) is sent. ▪ **1** (Default) SIP Registration message with **Expires:0** (unregister) is *not* sent.

5.1.3 Configuring a Line

The network administrator can configure a line.

➢ **To configure line mode:**

- Use the table as reference.

Table 5-7: Line Settings

Parameter	Description
voip/line/0-5/description	Defines the SIP User ID which is sent in "INVITE" packets to the called party in the "From" field, and should appear to the called party as "Caller ID". Default: 400HD
voip/line/0-5/enabled	Activates or deactivates the line. **0** = Disabled (this is the default for the second line and higher in the configuration file) **1** = Enabled (this is the default for the first line **voip/line/0/** in the configuration file).
voip/line/0-5/id	Defines the SIP User ID provided by the SIP server which the phone attempts to associate itself with during the registration process. This is also the default ID sent in the "INVITE" if the Line Display Name above is left blank. Default: 0
voip/line/0-5/auth_name	Defines the SIP username credential used in the registration process when attempting to associate with the above Line ID. Default: 0
voip/line/0-5/auth_password	Defines the SIP password associated with the above Line ID identifier during the registration process. Default: 0
voip/line/0-5/line_mode	Applies to models except RX50 and 405HD. Determines the line mode: PRIVATE (default) or SHARED. PRIVATE line - only presented with private call appearances. SHARED line – lets users share an extension number and manage a call as a group. When an employee places a call on a SHARED line on hold, the call can be resumed from any other employee sharing the line. A SHARED line is a line that is only presented with shared call appearances. Icons displayed in the phone's screen indicate if lines are configured in a Shared Call Appearance group, or as private lines.
voip/line/0-5/extension_display	Supported only on the 430HD/440HD phones. Defines the label displayed in the phone screen. To meet requirements for users with the 405HD phone, use the parameter 'voip/line/0/description' (see Table 5-7 for more information).

5.1.3.1 Assigning Programmable Keys to Lines (SIP Accounts)

The administrator can assign programmable keys to lines (SIP accounts).

➢ **To assign programmable keys to lines (SIP accounts):**

- Use the table as reference.

Table 25-4: Assigning Programmable Keys to Lines (SIP Accounts) [430HD, 440HD and 445HD]

Parameter Name	Description
personal_settings/functional_key/12-17/key_label	These are the labels displayed in the screen next to Programmable Keys **1**-**6**. Define the string of characters you want displayed (name, extension, etc.).
personal_settings/functional_key/12-17/type	Default: **SIP_ACCOUNT**. Can be set to perform other functions such as Speed Dial or Key Event. Do not change these for keys you want to assign to SIP lines.
personal_settings/functional_key/12-17/line	Configure 0-5 corresponding to the lines configured in the preceeding table.

Table 25-4: Assigning Programmable Keys to Lines (SIP Accounts) [450HD, C450HD, RX50 and HRS]

Parameter Name	Description
personal_settings/functional_key/0-5/key_label	These are the labels displayed in the screen next to Programmable Keys **1**-**6**. Define the string of characters you want displayed (name, extension, etc.).
personal_settings/functional_key/0-5/type	Default: **SIP_ACCOUNT**. Can be set to perform other functions such as Speed Dial or Key Event. Do not change these for keys you want to assign to SIP lines.
personal_settings/functional_key/0-5/line	Configure 0-5 corresponding to the lines configured in the preceeding table.

5.1.4 Configuring Shared Call Appearance

Note: Support pending.

Figure 5-1: Shared Call Appearance

Parameter	Description
voip/line/0/shared_call_appearance/call_info_expiration_timeout	Default: 3600
voip/line/0/shared_call_appearance/call_info_subscription_failed_timeout	Default: 60
voip/line/0/shared_call_appearance/line_seize_expiration_timeout	Default: 15
voip/line/0/shared_call_appearance/speed_dial_delay	Default: 2
voip/line/0/shared_call_appearance/waiting_to_line_seize_tone	Default: SILENCE

5.1.5 Configuring SIP Timers

SIP Timers can be configured.

➢ **To configure SIP timer settings:**

- Use the table as reference.

Table 5-8: SIP Timers Parameters

Parameter	Description
voip/signalling/sip/sip_t1	The time interval (in msec) between the first transmission of a SIP message and the first retransmission of the same message (according to RFC 3261). The valid range is 100 to 60000. The default value is 500. **Note:** The time interval between subsequent retransmissions of the same SIP message starts with SipT1Rtx and is multiplied by two until SipT2Rtx. For example (assuming that SipT1Rtx = 500 and SipT2Rtx = 4000): ▪ The first retransmission is sent after 500 msec. ▪ The second retransmission is sent after 1000 (2*500) msec. ▪ The third retransmission is sent after 2000 (2*1000) msec. ▪ The fourth retransmission and subsequent retransmissions until SIPMaxRtx are sent after 4000 (2*2000) msec. **Note also:** If dual registration / redundant Genesys server is configured and the configuration file parameter 'voip/signalling/sip/redundant_proxy/dual_reg/t1' is then configured, its value will override 'Retransmission Timer T1'. See also Section A.3.12 and Section A.3.12.1.
voip/signalling/sip/redundant_proxy/dual_reg/t1	Only relevant if dual registration / redundancy server is configured. Allows quicker retransmission of SIP messages. Default: 20 milliseconds. Range: 20-200.
voip/signalling/sip/sip_t2	The maximum interval (in msec) between retransmissions of SIP messages (according to RFC 3261). ▪ The valid range is 4000 to 60000. ▪ The default value is 4000. **Note:** The time interval between subsequent retransmissions of the same SIP message starts with SipT1Rtx and is multiplied by two until SipT2Rtx.
voip/signalling/sip/sip_t4	The SIP T4 retransmission timer according to RFC 3261. ▪ The valid range is 5000 to 60000. ▪ The default value is 5000.

Parameter	Description
voip/signalling/sip/sip_invite_timer	The SIP INVITE timer according to RFC 3261. The valid range is 0 to 65535. The default value is 32000.
voip/signalling/sip/session_timer	The time (in seconds) at which an element considers the call timed out if no successful INVITE transaction occurs beforehand. This value is inserted into every INVITE in the Session-Expires header unless it is configured to 0. If the timer option tag is not part of the supported list, the sessionExpires value is ignored. The valid range is 0 to 65535. The default value is 1800.
voip/signalling/sip/min_session_interval	The minimum value for the session interval that the application is willing to accept. ▪ The valid range is 0 to 65535. The default value is 90.
voip/signalling/sip/unregister_on_voip_reload	If the VoIP application needs to be reloaded, the application by default sends a SIP Registration message with **Expires:0**, which means unregister. By setting this parameter to **1** (default), the application will not send the unregistration message when its reloaded.

5.1.6 Configuring SIP QoS

SIP Quality of Service (QoS) can be configured.

➢ **To configure SIP QoS:**

- Use the table as reference.

Table 5-9: SIP QoS Parameters

Parameter	Description
voip/signalling/sip/tos	QoS in hexadecimal format. This is a part of the IP header that defines the type of routing service to tag outgoing signalling packets originated from the phone. It informs routers that this packet must receive a specific QoS. The default value is 0x60. Values can be set in decimal (e.g. 96) or hexadecimal (e.g. 0x60).

For information on configuring RTP QoS, see Section 5.5.3.

5.1.7 Configuring SIP Reject Code

Reject Code can be configured.

➢ **To configure Reject Code:**

- Use the table as reference.

Table 5-10: Reject Code Parameter

Parameter	Description
voip/services/reject_code	Configures the reject code that the phone sends when the **Reject** softkey is pressed or while DND is activated. Valid values are: **CODE_603** **CODE_486**

5.2 Configuring Dialing

Network administrators can configure dialing parameters to enable different ways users can dial other parties.

5.3 Configuring Voice Dialing through VocaNOM

Users can use the AudioCodes VocaNOM voice dialing service to *directly* voice dial other parties by vocalizing their name. Additionally, the phone numbers of parties who are voice-dialed are displayed in the the Call Log from where users can redial. The feature powers up efficiency in organizations, increases productivity and improves users' telephony experience. Users can configure a key which they can press and then vocalize the name of the party to whose number the VocaNOM service will directly dial.

➢ **To enable the service:**

- Use the table as reference.

Table 5-11: Voice-Dialing Parameter Descriptions

Parameter	Description
voip/services/vocanom/number	Defines the number that the phone dials to access the VocaNOM server, either directly, or indirectly, via the Skype for Business server. Example: 7777
voip/services/vocanom/label	Defines the name that will be displayed in phone screens after users press their configured VocaNOM key to voice-dial another party using the VocaNOM service. Default: VocaNOM
voip/services/vocanom_server/enabled	Can be enabled or disabled. The user's experience remains the same whether enabled (direct voice dialing) or disabled (indirect voice dialing). Direct or indirect voice dialing occurs in the background, so user experience is unaffected. When enabled (direct voice dialing), the call is forwarded directly to the server. When disabled (indirect voice dialing), the call is forwarded via the Skype for Business server. The VocaNOM server can be on premises or in the cloud. ▪ **0** Access to the VocaNOM server is indirect via the Skype for Business server default ▪ **1** Access to the VocaNOM server is direct
voip/services/vocanom_server/ip_address	Defines the VocaNOM server's IP address. The server can be either in the AWS cloud (Amazon Web Services) or on premises. Default: 0.0.0.0
voip/services/vocanom_server/port	Defines the port number on the VocaNOM server. Its value must match Transport Mode. ▪ **5060** for UDP, TCP ▪ **5061** default for TLS
voip/services/vocanom/transport_mode	Defines the Transport Mode for sending SIP messages. ▪ TLS Default ▪ UDP ▪ TCP

Note: All parameters must be configured for the user's VocaNOM key to be activated.

5.3.1 Configuring General Dialing Parameters

Network administrators can configure general dialing parameters.

➢ **To configure general dialing parameters:**

- Use the table as reference.

Table 5-12: Dialing Parameters

Parameter	Description
voip/dialing/timeout	The duration (in seconds) of allowed inactivity between dialled digits. When you work with a proxy, the number you have dialled before the dialing process has timed out is sent to the proxy as the user ID to be called. This is useful for calling a remote party without creating a speed dial entry (assuming the remote party is registered with the proxy). Range is 0 to 10. Default = 5.
voip/dialing/interdigit_short_timeout	Shorter than 'Dialing Timeout' (see above). Default: 3 seconds. Implemented as **0S** for the Dial Map. If a user wants to make an international call by dialing **00** and wants to dial the secretary/operator by dialing **0**, the user can do both by adding **0S** to the Dial Map. For example, if the digit map string= *xx|2-9]11|0S|2-9]xxxxxxxxx|1xxx2-9]xxxxxx, it has **0S** in it. When the user dials **0**, **0** will match **0S** and will therefore start the 'Interdigit Short Timeout' timer. After this timeout, **0** is dialed out. User can dial **00** or **0123** within the 'Interdigit Short Timeout'. After the 'Dialing Timeout', the string is dialed out.
voip/dialing/phone_number_max_size	The maximum length of shortcut numbers that you can enter and the maximum number of digits that you can dial Range is 3 to 32. Default = 32.
voip/dialing/dial_complete_key/enabled	Enables the feature for defining a key to indicate that dialing has completed. Pressing the Dialing Complete key (defined below) forces the phone to make a call to the dialled digits even if there is no match in the dial plan or digit map. ▪ **0** Disable ▪ **1** Enable (default) ▪ **Note:** This parameter is available only if the parameter 'voip/dialing/dial_complete_key/enabled' is set to **1**.
voip/dialing/dial_complete_key/key	Defines the Dialing Complete key. The valid value is a single character. The default value is the pound (#) key.
voip/dialing/unanswered_call_timeout	Timeout before the phone automatically sends a Cancel message. When the phone makes a call and the other side doesn't answer, the phone sends a Cancel after this timeout. Range: 1 to 300. Default = 60.

Parameter	Description
voip/dialing/allow_calling_self_extension/ enabled	If disabled (default), calling the self-number (user ID) will be blocked. If enabled, the phone will send the invite although it is for its own extension. (In some proxies this is how you access voice mail).

5.3.2 Configuring Auto Redial

Note: Support pending.

The administrator is responsible for enabling/disabling the auto-redial feature. If enabled and a called party is unavailable because they're busy (for example), the caller's phone's SCREEN prompts **Extension Busy. Activate auto redial on busy?**

If the caller then activates auto-redial by pressing **Yes**, the busy extension is automatically redialed every *n* seconds.

The administrator is also responsible for configuring this frequency.

➢ **To configure dialing:**

- Use the table as reference.

Table 5-13: Automatic Redial On Busy Parameters

Parameter	Description
voip/dialing/automatic_redial_on_busy/ enabled	Allows the administrator disable/enable the feature. **0**=Disabled **1**=Enabled Default: **0**
voip/dialing/automatic_redial_on_busy/ retry_timer	Visible only if the feature is enabled. Range: 3-120. Default: **30**. If the feature is activated and the timer lapses, an outgoing call to the busy destination is established. If the feature is activated, a countdown screen is displayed: **Dialing <ext> within <x>s (Line <n>)** The screen shows the timer, the remote extension and the line number.

5.3.3 Configuring Dial Tones

Dial Tones settings can be configured.

➢ **To configure Dial Tones:**

- Use the table as reference.

Table 5-14: Dial Tones Parameters

Parameter	Description
voip/dialing/dialtone_timeout	Defines the maximum duration of the dial tone (in seconds) after which the dial tone stops and a reorder tone is played. Range:1 to 300. Default: 30.
voip/dialing/warning_tone_timeout	Defines the maximum duration of the reorder tone (in seconds) after which the reorder tone stops and a howler tone is played. Range:1 to 300. Default: 40.
voip/dialing/offhook_tone_timeout	Defines the duration (in seconds) of the howler tone. If the limit is exceeded, the howler tone stops. The howler tone indicates that the phone has been left in an off-hook state. Range:1 to 300. Default: 120.
voip/dialing/secondary_dial_tone/enabled	▪ Enables the secondary dial tone. ▪ **0** Disable (default) - Phone doesn't use secondary dial tone. ▪ **1** Enable - Phone plays secondary dial tone if the secondary dial tone key is pressed (first digit). For example, when pressing **9** to get an external dial tone, a different dial tone (not configurable) is played as the second dial tone.
voip/dialing/secondary_dial_tone/key_sequence	Defines the secondary dial tone is played if this is the first key pressed. ▪ Range: 0 to 9. Default: 9. **Note:** This parameter is available only if the parameter 'voip/dialing/secondary_dial_tone/enabled' is set to **1**.
voip/services/out_of_service_behavior	Determines whether a reorder tone is played instead of a dial tone if you configured a Registrar IP address and the registration failed. ▪ **NONE** No Tone ▪ **REORDER_TONE** Reorder Tone (default)
voip/services/msg_waiting/stutter_tone_duration	Defines the duration for which a stutter tone is played when you have unheard messages. ▪ Range:1000 to 60000. ▪ Default: 2500.

Parameter	Description
voip/dialing/automatic_disconnect	Determines whether the phone automatically goes idle (i.e. on-hook) when the last remaining call is disconnected. This is only relevant when the speaker or headset is used. ▪ **0** Disable ▪ **1** Enable (default)

5.3.4 Configuring DTMF

Dual-Tone Multi-Frequency (DTMF) signaling can be configured.

➢ **To configure DTMF:**

- Use the table as reference.

Table 5-15: DTMF Transport Mode

Parameter	Description
voip/media/out_of_band_dtmf	DTMF transport mode. ▪ **INBAND** Inband ▪ **RFC2833** RFC 2833 (default) ▪ **VIA_SIP** Via SIP
voip/media/dtmf_via_sip_force_flag	Must be set to **1** to enable **Via SIP** as DTMF transport type.
voip/audio/gain/dtmf_rtp_event_signal_level	Allows the network administrator to control the DTMF tones level. ▪ **0** db (Minimum) ▪ **31** db (Maximum)

Note: If the cfg file parameter 'voip/media/dtmf_via_sip_force_flag' is enabled, a SIP message is sent in addition to the RTP message. If it is disabled, only one message is sent, according to the selected DTMF transport type.

5.3.5 Configuring Digit Maps and Dial Plans

Digit maps and Dial plans can be configured.

➢ **To configure digit map and dial plan:**

- Use the table as reference.

Note: Invalid Tokens will be ignored by the application.

Table 5-16: Digit Map and Dial Plan Parameters

Parameter	Description
voip/signalling/sip/digit_map	Enables the administrator to predefine possible formats (or patterns) for the dialed number. A match to one of the defined patterns terminates the dialed number. The valid value can be up to 256 characters. There are two main formats for the digit map configuration. The formats are distinguished by the separator ';' or '|'. ▪ **Using '|' separator:** The following constructs can be used in each numbering scheme: ✓ **Digit:** A digit from **0** to **9**. ✓ **DTMF:** A digit, or one of the symbols **A**, **B**, **C**, **D**, **#**, or *. Extensions may be defined. ✓ **Wildcard:** The symbol **x** which matches any digit (**0** to **9**). ✓ * **Range:** One or more DTMF symbols enclosed between square brackets ([and]). ✓ **Sub range:** Two digits separated by hyphen (**-**) which matches any digit between and including the two. The subrange construct can only be used inside a range construct, i.e., between [and]. ✓ **Position:** A period (.) which matches an arbitrary number, including zero, of occurrences of the preceding construct. **For example: [**2-9]11|0|100|101|011xxx.|9011xxx.|[12-9]xxxxxxxxx|[92-9]xxxxxxxxx|[912-9]xxxxxx|*xx|8]xxxx|2-7]xxx This example includes the following rules: ✓ **[2-9]11:** 911 rule: 211, 311, 411, 511, 611, 711, 811, 911 are dialed immediately ✓ **0:** Local operator rule: After dialing **0** the phone waits T seconds and then completes the call automatically ✓ **100:** Auto-attendant default extension ✓ **101:** Voicemail default extension ✓ **011xxx.:** International rule without prefix ✓ **9011xxx.:** International rule with prefix ✓ **[12-9]xxxxxxxxx:** LD rule without prefix ✓ **[912-9]xxxxxxxxx:** LD rule with prefix ✓ **[92-9]xxxxxx:** Local call with prefix ✓ ***xx:** 2-digit star codes ✓ **[1-7]xx:** A regular 3 digit extension that does not start with 9 or 8 is dialed immediately ✓ **[2-7]xx:** A regular 3 digit extension that does not start with 9 or 8 or 1 is dialed immediately

Parameter	Description
	✓ **[2-7]xxx:** A regular 4 digit extension that does not start with 9 or 8 or 1 is dialed immediately ✓ **[8]xxx:** A 3 digit extension prefixed with an 8 (routes calls directly to voicemail of extension xxx) ✓ **[8]xxxx:** A 4 digit extension prefixed with an 8 (routes calls directly to voicemail of extension xxxx) ✓ **T**: Refers to the **Dialing Timeout.** ▪ **Using ';' separator:** An 'x' in the pattern indicates any digit. ';' separates between patterns. For example: '10x;05xxxxxxxx;4xxx'. In this example, three patterns are defined. A number that starts with 10 is terminated after the third digit, and so on. If the user dials a number that does not match any pattern, the number is terminated using the timeout or when the user presses the pound ('#') key.
voip/signalling/sip/number_rules	This parameter works in conjunction with the parameter **voip/signalling/sip/digit_map** and enables translation of specific patterns to specific SIP destination addresses. An 'x' represents any dialed digit. Each backslash at the right side of the '=' represents one of the dialed digits. Rules are separated by the character ';'. The valid value can be up to 256 characters. For example: '4xxx=Line_\\\@10.1.2.3' This rule issues a call to 10.1.2.3 with the SIP ID of Line_ followed by the last three digits of the dialed number.

5.3.6 Configuring Headset LED to Stay On

Note: Support pending for all models.

IT administrators can configure the headset LED to stay on when the phone is on standby *and* when it is in conversation mode.

Note: Headset must be configured as the default audio device for the feature to function (see Section 5.3.7).

➢ **To configure the headset LED to stay on:**

- Use the table as reference.

Table 5-17: Headset LED Parameter

Parameter	Description
voip/highlight_audio_device	Allows the headset LED to stay on when the phone is on standby *and* when it is in conversation mode. Functions only when headset is configured as the default audio device. Configure either: ▪ **NONE** (Default) Headset LED illuminates only when the phone is in conversation mode. ▪ **HEADSET** = Headset LED illuminates when the phone is on standby *and* when it is in conversation mode

5.3.7 Configuring Default Audio Device

The default audio device can be configured.

Note: On the RX50 conference phone, only the phone speaker is available.

➢ **To configure default audio device:**

- Use the table as reference.

Table 5-18: Audio Device Parameter

Parameter	Description
audio/stream/voice_call/0/audio_device	Valid values: ▪ TYPE_SPEAKER ▪ BUILTIN_SPEAKER (default) ▪ USB_SPEAKER ▪ BLUETOOTH_SPEAKER (applies to the 445HD and C450HD phones only) ▪ TYPE_HEADSET ▪ USB_HEADSET ▪ BLUETOOTH_HEADSET ▪ TYPE_USB ▪ TYPE_BLUETOOTH ▪ ANALOG Sets the default audio device to answer or initiate a new call when no explicit audio device is set. For example: ▪ When pressing the **Answer** softkey. ▪ When initiating a call by speed dial key, call history or phone directory. ▪ Answering talk event or auto-answer. ▪ When starting to dial in 'on hook' mode.

5.4 Configuring Ring Tones

Network administrators can configure and upload ring tones to the phone.

5.4.1 Configuring Distinctive Ring Tones

Network administrators can configure a phone to ring in a distinct tone per caller, thus facilitating caller recognition and saving others from unnecessary disruptions to their activities if the phone is shared.

➢ **To configure a distinctive ring:**

- Use the table as a reference.

Table 5-19: Distinctive Ringing Parameters

Parameter	Description
voip/distinctive_ringing/0-4/ringtone	A name to assign to a distinctive ring tone. The default ring tone names are Ring01 – Ring11. (Optionally, select and manually upload a customized tone – see Section 5.4.3). If you don't enter a name, the phone assigns the tone's filename (without the .wav file extension) as the tone name.
voip/distinctive_ringing/0-4/type	The 'Alert-Info' header's content in the INVITE message. It should be configured in the SIP proxy or application server. Used to distinguish between different calls.

5.4.1.1 Example of Configuring a Distinctive Ring

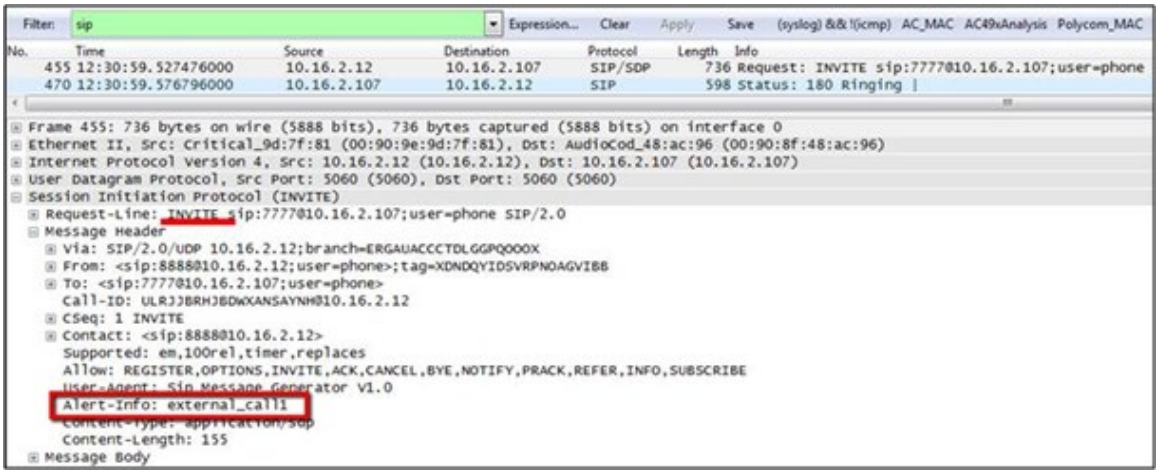
A ring tone whose name is **Ring05** is configured to ring when the Alert-Info Header received in the INVITE message contains **external_call1**.

➢ **Example:**

- Configure parameter 'voip/distinctive_ringing/4/ringtone' to **Ring05**
- Configure parameter 'voip/distinctive_ringing/4/type' to **externall_call1**

The Alert-Info header must contain **external_call1**, as shown below. This is the INVITE the phone receives from the proxy / application server.

Figure 5-2: Example of the Alert-Info Header



The phone will play **ring tone 5** irrespective of the selected line ring tone.

5.4.2 Configuring CPT Regional Settings

It's important to match your phone's Call Progress Tones (CPT) to the country in which your phone is located.

➢ **To configure regional location:**

- Use the table as reference.

Table 5-20: Regional Parameters

Parameter	Description
voip/regional_settings/selected_country	Defines the country in which your phone is located. The behavior and parameters of analog telephones lines vary between countries. CPTs are country-specific. The phone automatically selects the correct regional settings according to this parameter. Supported countries are: ▪ Israel ▪ China ▪ France ▪ Germany ▪ Netherlands ▪ UK ▪ Brazil ▪ Italy ▪ Argentina ▪ Portugal ▪ Russia ▪ Australia ▪ USA (Default) ▪ India
voip/regional_settings/use_config_file_values	Enables the user-defined CPT. When this parameter is enabled, the 'selected_country' parameter is not relevant and the CPT values below can be determined by the user. ▪ **0** - Disable (default) ▪ **1** - Enable
Call Progress Tones (CPT) **Note:** Up to 10 CPTs can be configured (**voip/regional_settings/call_progress_tones/0…9**).	
voip/regional_settings/call_progress_tones/%d/enabled	Enables the specific CPT. ▪ **0** - Disable ▪ **1** - Enable
voip/regional_settings/call_progress_tones/%d/name	Defines the name of the CPT.
voip/regional_settings/call_progress_tones/%d/cadence	▪ Defines the cadence type of the tone. ▪ **0** - Continuous signal ▪ **1** - Cadence signal ▪ **2** - Burst signal

Parameter	Description
voip/regional_settings/call_progress_tones/%d/frequency_a	Defines the low frequency (in Hz) of the tone. Range:300 - 1980 Hz, in steps of 1 Hz. Unused frequencies must be set to zero.
voip/regional_settings/call_progress_tones/%d/frequency_b	Defines the high frequency (in Hz) of the tone. Range:300 - 3000 Hz, in steps of 1 Hz. Unused frequencies must be set to zero.
voip/regional_settings/call_progress_tones/%d/frequency_a_level	Output level of the low frequency tone (in -dBm) in Call Progress generation. Range: 0 - 63, where 63 is mute.
voip/regional_settings/call_progress_tones/%d/frequency_b_level	Output level of the low frequency tone (in -dBm) in Call Progress generation.Range:0 - 63, where 63 is mute.
voip/regional_settings/call_progress_tones/2/name	Default: **busy_tone** The calling party hears a busy tone if the called party's line is busy. The busy tone complies with international telcom standards in traditional non-VOIP telephony systems.
voip/regional_settings/call_progress_tones/%d/tone_on_0	tone_on_0 to tone_on_3. If the signal is Cadence or Burst, then this value represents the on duration. If a Continuous tone, then this value represents the minimum detection time. In units of 10 msec.Range:0 - 10000.
voip/regional_settings/call_progress_tones/%d/tone_off_0	tone_off_0 to tone_on_3. If the signal is Cadence, then this value represents the off duration, in units of 10 msec. If not used, then set it to zero. If the signal is Burst, only tone_off 0 is relevant. It represents the off time that is required from the end of the signal to the detection time.Range:0 - 10000.

5.4.3 Uploading Ring Tones

New Ring Tones can be uploaded.

Note:

- The ring tone file must be in WAV file format (A/Mu-Law, 8-kHz audio sample rate and 8-bit audio sample size or PCM 16-kHz audio sample rate and 16-bit audio sample size, Intel PCM encoding).
- For the phone to use an uploaded ring tone, select it on the phone (see the phone's *User's Manual*).

➢ **To upload Ring Tones:**

- Use this table as reference.

Table 5-21: Ring Tone Parameters

Parameter	Description
provisioning/ring_tone_uri	The URI for retrieving the ring tones file. The ring tones can be compressed to zip or tgz files and provided to the phone during provisioning. For example:**provisioning/ring_tone_uri=tones.tgz** **Note:** ▪ The ringtone file is downloaded only after boot up, and not periodically. ▪ If the tones file is new, the phone updates the information, but does not reboot. ▪ For the feature to function, the file must first be compressed to zip / tgz format. The phone won't accept a simple .wav file format.
personal_settings/lines/0/ring_tone - personal_settings/lines/3/ring_tone	Lets administrators set a ring tone for each line extension (up to four line extensions). Administrators can choose any one of the eleven ring tones available: **Ring01** - **Ring11**. There is also a silent option.

5.4.4 Configuring Beeps to Headsets when a Call Comes in to a Call Center

Note: Support pending.

Network administrators can configure a beep instead of ringing to be played to agents' headsets when a call comes in to a Call Center. The beep is heard even if 'Auto answer' is configured to **0**.

➢ **To play beeps to headsets instead of ringing:**

- Use the table as reference.

Table 5-22: Configuring Beeps to be Played to Headsets when Calls Come in

Parameter	Description
voip/beep_to_ringing_device/enabled	Enables/disables beeping the device. ▪ **0** Disable (default) ▪ **1** Enable
voip/beep_to_ringing_device/number_of_beeps	If the feature is enabled, the number of beeps must be configured. Default: 3.
voip/hands_free_mode/enabled	Enables/disables hands-free mode. ▪ **0** Disable (default) ▪ **1** Enable
voip/handset_mode/enabled	Enables/disables handset mode. ▪ **0** Disable (default) ▪ **1** Enable
voip/headset_only/enabled	Enables/disables 'only headset'. ▪ **0** Disable (default) ▪ **1** Enable

5.4.5 Configuring the Phone to play Fast Busy Tone if Automatically Disconnected on Remote Side

Network administrators can configure the phone to play a fast busy tone if it is automatically disconnected on the remote side. Network administrators can also configure for how long this fast busy tone is played. When the phone plays the tone, it also displays a 'Disconnected' message for the same length of time.

➢ **To configure this feature:**

- Use the table as reference.

Table 5-23: Configuring the Phone to Play a Fast Busy Tone when Automatically Disconnected on Remote Side

Parameter	Description
enable_remote_disconnect_warningTone	Allows you to enable or disable playing a fast busy tone if the phone is automatically disconnected on the remote side. ▪ **0** (default) If the phone accepts an incoming call and the remote side automatically ends it (disconnects), the phone does not play any tone and no message is displayed. ▪ **1** If the phone accepts an incoming call and the remote side automatically ends (disconnects) it, the phone plays a fast busy tone and displays a Disconnected message (see the parameter description below).
voip/dialing/automatic_disconnect_delay_timer	Defines for how long the fast busy tone is played and for how long the 'Disconnected' message is displayed if the warningTone parameter above is enabled and the phone is automatically disconnected on the remote side. Default: 600 ms.

5.5 Configuring Media Settings

Network administrators can configure media settings such as media streaming, RTP Port Range and Payload Type, shown in the following sections.

5.5.1 Configuring Media Streaming

The network administrator can configure the Media Streaming feature. Configure the parameters using the table below as reference.

Table 5-24: Media Streaming Parameters

Parameter	Description
voip/media/rtp_mute_on_hold	Mute sending RTP packets to remote in HOLD state. ▪ **0** - Disabled. RTP packets are sent to remote end when in HOLD state. ▪ **1** - Enabled (default). RTP packets are not sent to remote end when in HOLD state.
voip/media/allow_multiple_rtp	Defines whether to allow multiple RTP streamsfrom different remote ends to be played toward the phone in a single call. ▪ **0** Disable (default) ▪ **1** Enable
voip/media/ignore_rfc_2833_packets	Defines whether to ignore playing DTMF when RFC 2833 arrives from the network. ▪ **0** Disable ▪ **1** Enable (default)
voip/media/broken_connection_detection	If enabled an active call will be automatically disconnected if no RTP packet is received within pre-defined time. ▪ **0** Disable ▪ **1** Enable (default)
voip/media/broken_connection_timeout	If no RTP packet arrives for an active call within this timeout (in seconds), the connection will be considered broken and the call will be disconnected. Default: 30.

5.5.2 Configuring RTP Port Range and Payload Type

RTP Port Range and Payload Type can be configured.

➢ **To configure RTP Port Range and Payload Type:**

- Use the table as reference.

Table 5-25: RTP Port Range and Payload Type Parameters

Parameter	Description
voip/media/dtmf_payload	Defines the RTP payload type used for RFC 2833 DTMF relay packets. Range: 96 - 127. Default: 101.
voip/media/media_port	Defines the base port for the range of Real Time Protocol (RTP) voice transport ports which the enterprise IT administrator must open on the network's firewall. Default: 4000. Valid possible ports (if the default is selected as base port): 4000-4126. If, for example, 5000 is selected as the base port, the valid possible ports will be 5000-5126.

5.5.3 Configuring RTP QoS

RTP QoS can be configured.

➢ **To configure RTP QoS:**

- Use the table as reference.

Table 5-26: RTP QoS Parameter

Parameter	Description
voip/media/media_tos	QoS in hexadecimal format. This is a part of the IP header that defines the type of routing service to tag outgoing voice packets originated from the phone. It informs routers that this packet must receive a specific QoS. The default value is **0xb8**. Values can be set in decimal (e.g., 184) or hexadecimal (e.g., 0xb8). Default: 184.

5.5.4 Configuring Codecs

Note: OPUS currently applies to the 405HD, 430HD and 440HD low-end phones, the 450HD high-end phone, HRS conference device and RX50 conference phone. Support pending on the other models.

➢ **To define the Codecs:**

- Use the table as reference.

Table 5-27: Codec Parameters

Parameter	Description
voip/codec/codec_info/%d/enabled	Determines the codecs that you want to implement and their priority. Up to five codecs can be configured, where the first codec (i.e., **voip/codec/0/…**) has the highest priority. To make a call, at least one codec must be configured. For best performance it's recommended to select as many codecs as possible. When you start a call to a remote party, your available codecs are compared with the remote party's to determine the codec to use. If there is no codec that both parties have made available, the call attempt fails. Note that if more than one codec is common to both parties, you cannot force which of the common codecs are used by the remote party's client. To force the use of a specific codec, configure the list with only that specific codec. The *%d* variable stands for the priority: ▪ **0** - Disabled ▪ **1** (default) - Enabled
voip/codec/codec_info /%d/name	Name of the codec. The variable *%d* depicts the index number of the codec entry and its priority, where the first codec (i.e. **voip/codec/codec_info/0/name=…**) has the highest priority. The valid codec parameters are: ▪ **G722** G.722 (default) ▪ **PCMA** G.711 A-Law ▪ **PCMU** G.711 Mu-Law ▪ **G729** G.729 ▪ **OPUS** For example, **voip/codec/codec_info/0/name=G.722** **Note**: ▪ If OPUS is selected from the list of codecs on a phone that doesn't support the OPUS codec, a warning pops up: 'The hardware doesn't support the OPUS codec'. ▪ To enable OPUS management for enhanced voice quality, see Section 5.5.5.
voip/media/opus_payload	Allows the network administrator to configure the OPUS dynamic payload type. Default: 111.
voip/codec/opus/%d /ptime	Packetization time - length of the digital voice segment that each packet holds. The default is 20 millisecond packets.

Parameter	Description
voip/codec/opus/jitter_buffer/min_delay	The initial and minimum delay of the OPUS adaptive Jitter Buffer mechanism, which compensates for network impairments. The value should be set according to the expected average jitter in the network (in milliseconds). ▪ Range: 30-500. Default: 30.

5.5.5 Configuring OPUS Management

Note: Currently applies to the 405HD, 430HD and 440HD low-end phones, the 450HD high-end phone, HRS conference device and RX50 conference phone. Support pending on the other models.

OPUS management for enhanced voice quality allows the OPUS audio codec's configuration to be changed on the fly when impairments are detected in the network. The OPUS functions at a lower channel bit rate and consumes less bandwidth, delivering better voice quality despite the poor network conditions. OPUS management can be configured using configuration file.

➢ **To configure OPUS management:**

- Use the table as reference.

Table 5-28: OPUS Management Parameters

Parameter	Description
voip/voice_quality/mode	Enables OPUS management and extended OPUS management for enhanced voice quality. ▪ **DISABLE** (default) ▪ **ENABLE_RTCP** ▪ **ENABLE_RTCP_FEEDBACK**

5.6 Configuring Voice Settings

Voice settings such as gain control and jitter buffer can be configured by network administrators.

5.6.1 Configuring Gain Control

See Section 5.9.1 for detailed information.

5.6.2 Configuring Jitter Buffer

Jitter Buffer can be configured.

➢ **To define Jitter Buffer:**

- Use the table as reference.

Table 5-29: Jitter Buffer Parameters

Parameter	Description
voip/audio/jitter_buffer/min_delay	The initial and minimal delay of the adaptive jitter buffer mechanism, which compensates for network problems. The value should be set according to the expected average jitter in the network (in milliseconds). ▪ Range:10 to 150. Default: 10.
voip/audio/jitter_buffer/optimization_factor	The adaptation rate of the jitter buffer mechanism. Higher values cause the jitter buffer to respond faster to increased network jitter. ▪ Range: 0 to 13. Default: 10.

5.6.3 Configuring Silence Compression

The Silence Compression feature can be configured.

➢ **To configure Silence Compression:**

- Use the table as reference.

Table 5-30: Silence Compression Parameters

Parameter	Description
voip/audio/silence_compression/enabled	Enables silence compression for reducing network bandwidth consumption. ▪ **0** Disable (default) ▪ **1** Enable

5.6.4 Configuring Noise Reduction

Network administrators can configure noise reduction.

Note: It's strongly advisable *not* to change the noise reduction default values without consulting AudioCodes. Consult your AudioCodes representative in the event you wish to modify the defaults.

5.6.5 Configuring Echo Cancellation

Note:

- It is strongly advisable to leave the echo cancellation parameters at their defaults and *not* to configure different values.
- Contact your AudioCodes representative if you encounter an echo cancellation related issue.

Network administrators can view the following echo cancellation related parameters in the configuration file.

- voip/audio/echo_cancellation/enabled
- voip/audio/echo_cancellation/extended_nlp/enabled
- voip/audio/echo_cancellation/handset/HPF_mode
- voip/audio/echo_cancellation/handsfree/HPF_mode
- voip/audio/echo_cancellation/headset/HPF_mode
- voip/audio/echo_cancellation/nlp/max_delay
- voip/audio/echo_cancellation/nlp/mode

5.7 Configuring Extension Lines

Before you can make a call, you must configure an extension line (SIP account) on the phone.

➢ **To configure an extension line (SIP account):**

- Use the table as reference. **%d** refers to the line number.

Table 5-31: Line Parameters

Parameter	Description
voip/line/0-5/enabled	Activates or deactivates the line. **0** = Disabled (this is the default for the second line and higher in the configuration file) **1** = Enabled (this is the default for the first line **voip/line/0/** in the configuration file).
voip/line/0-5/id	Lines VoIP user's ID for identification to initiate and accept calls. The user's ID can be up to 30 characters.
voip/line/0-5/description	Arbitrary name to intuitively identify the line and that is displayed to remote parties as your caller ID.
voip/line/0-5/auth_name	User name provided to you from the VoIP service provider. This is used when sending a response to Unauthorized or Proxy Authentication Requested (401/407). The authentication name can be up to 35 characters.
voip/line/0-5/auth_password	Password provided to you from the VoIP Service Provider. This is used when sending a response to Unauthorized or Proxy Authentication Requested (401/407). The authentication password can be up to 35 characters.
voip/line/0-5/extension_display	Applies to all phone models but on the 405HD phone the parameter is voip/line/**0-1**/extension_display. Set the string that will be displayed in the phone screen for local extension. If not set, the local extension displayed will be the user ID (self-number).
voip/line/0-5/line_mode	Applies to all phone models. Determines the line mode: PRIVATE (default) or SHARED. SHARED allows enterprise employees to share an extension number and manage a call as a group. When an employee places a call on a SHARED line on hold, the call can be resumed from any other employee sharing the line.

Note:

- You can activate DnD per phone line (see Section 5.8.7).
- The RX50 conference phone does not support DnD.

5.8 Configuring Supplementary Services

Network administrators can configure various supplementary services supported by the phone such as Call Waiting, Call Forwarding (inapplicable to the RX50 conference phone), Three-way Conferencing, and Message Waiting Indication (MWI).

5.8.1 Selecting the Application Server

By default, the phone is set for a generic application server. However, you can select a specific third-party application server as described below.

Note: Configuration of specific supplementary services depends on the third-party application server used in your organization.

➢ **To select the application server:**

- Use the table as reference.

Table 5-32: General Supplementary Services Parameters

Parameter	Description
voip/services/application_server_type	Defines the type of the application server to which the device is registered. ▪ **Generic** Generic (default) ▪ **Asterisk** Asterisk ▪ **FreeSWITCH** FreeSWITCH ▪ **GENBAND** Kandy Business Solutions softswitch solution ▪ **BSFT** BroadSoft (support pending) ▪ **Coral** Coral (support pending) ▪ **Metaswitch** Metaswitch (support pending) **Note:** ▪ Parameters unique to the selected application server become applicable in addition to this page's parameters. ▪ For more information about Genband KBS environment, see the *Kandy Business Solutions Feature Description Guide*.
system/current_user_presence_status/enabled	Only displayed if the application server selected [FreeSWITCH] supports it. Enables the presence feature. The **DND** softkey on the phone is replaced by **Status**; the phone shows and publishes the presence status.
system/feature_key_synchronization/enabled	Applies only to the BroadSoft application server. See Section 6.5 for more information.

5.8.2 Configuring Call Waiting

Call Waiting can be configured.

➢ **To configure call waiting:**

- Use the table as reference.

Table 5-33: Call Waiting Parameters

Parameter	Description
voip/services/call_waiting/enabled	Enables the Call Waiting feature. ▪ **0** Disable ▪ **1** Enable (default)
voip/services/call_waiting/sip_reply	Determines the SIP response that is sent when another call arrives while a call is in progress: ▪ **RINGING** - 180 Ringing ▪ **QUEUED** (default) - 182 Queued
voip/services/call_waiting/generate_tone/enabled	Determines whether the phone plays a call waiting tone: ▪ **0** The phone doesn't play a call waiting tone. ▪ **1** The phone plays a call waiting tone (default).

5.8.3 Configuring Call Forwarding

Call Forwarding can be configured using the configuration file or phone screen. In a BroadSoft environment, Call Forwarding can be configured in the BroadSoft BroadWorks application server (see under Appendix A for detailed information).

➢ **To configure call forwarding:**

- Use the table as reference.

Table 5-34: Call Forward Parameters

Parameter	Description
voip/line/0-5/call_forward/enabled	Enables the Call Forward feature. ▪ **0** Disable ▪ **1** Enable (default)
voip/line/0-5/call_forward/active	Activates call forwarding, if it was enabled with the parameter above. ▪ **0** (default) - Disable ▪ **1** Enable **Note:** Call Forwarding is typically activated on the phone screen (see the *User's Manual*).

Parameter	Description
voip/line/0-5/call_forward/type	Determines the condition on which incoming calls are forwarded to another destination: ▪ **Unconditional** - incoming calls are forwarded independently of the status of the line. ▪ **Busy** - incoming calls are forwarded only if the phone is busy. ▪ **No_Reply** (default) - incoming calls are forwarded only if the phone does not answer before a user-defined timeout.
voip/line/0-5/call_forward/timeout	If calls are forwarded when the condition is No-Reply, then this parameter defines the time (in seconds) after which incoming calls are forwarded when this is no reply. Range:0 - 7200. Default: 6.
voip/line/0-5/call_forward/destination	The destination to which the call is directed when call forward is activated.

➢ **To configure call forwarding using the phone's screen:**

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

5.8.4 Configuring a Conference

Three-way conferencing can be configured.

➢ **To configure three-way conferencing:**

- Use the table as reference.

Table 5-35: Conference Parameters

Parameter	Description
voip/services/conference/mode	Sets the conference mode (when establishing 3-Way Conference). **LOCAL** = phone will establish the conference by itself. **REMOTE** = phone will use remote media server to establish the conference. Note that the default mode of the RX50 conference phone is **REMOTE** as the RX50 does not support local conference.
voip/services/conference/conf_ms_addr	Relevant only if 'Mode'(above) is **REMOTE**. Defines the media server for establishing remote conference.

For more information on this feature, see RFC 4579, Session Initiation Protocol (SIP) - Call Control - Conferencing for User Agents.

5.8.5 Configuring Automatic Dialing

Automatic Dialing can be configured.

➢ **To define Automatic Dialing:**

- Use the table as reference.

Table 5-36: Automatic Dialing Parameters

Parameter	Description
voip/dialing/auto_dialing/enabled	Determines whether automatic dialing is enabled (i.e., phone number is automatically dialed when you off-hook the phone). ▪ **0** Disable (default) ▪ **1** Enable
voip/dialing/auto_dialing/timeout	Timeout (in seconds) before automatic dialing occurs after the phone is off-hooked. When set to 0, automatic dialing is performed immediately. The valid range is 0 to 120. The default value is 15.
voip/dialing/auto_dialing/destination	The number that is automatically dialed when the phone is off-hooked. The valid value can be up to 32 characters.

5.8.6 Configuring Automatic Answer

Note: Support pending.

The Automatic Answer feature is configured. Use the table as reference.

Table 5-37: Automatic Answer Parameters

Parameter	Description

voip/auto_answer/enabled	Enables the Automatic Answering feature.
	▪ **0** Disable (default)
	▪ **1** Enable
	When this parameter is enabled and an incoming SIP INVITE message is received containing information that informs the phone to automatically answer the call, the phone answers the call immediately or after a timeout, depending on the auto-answer type specified in the INVITE message:
	▪ **Phone answers after a timeout:** The phone automatically answers the call after a timeout if the INVITE message includes a SIP Call-Info header with a tag value, **answer-after=** set to a number representing the timeout. During the timeout interval, the phone rings normally. If the call is answered or rejected during this interval, then the automatic answering mechanism is not used. However, if the phone is left to ring throughout the timeout interval, it automatically answers the call once this timeout expires.
	▪ **Phone answers immediately:** The phone answers the call immediately in any of the following cases:
	  ▪ If the SIP Alert-Info header contains the tag value **ring answer**.
	  ▪ If the SIP Alert-Info header contains the tag value **info=alert-autoanswer**.
	Note:
	▪ If the SIP Call-Info header includes all the above answer types or any two different types (i.e., **answer-after=**, **ring answer**, and **alert-autoanswer**), the answer-after= type takes precedence.
	▪ If there is an existing call when an INVITE message for automatic answer is received, the existing call is automatically put on hold.

voip/talk_event/enabled	Enables the 'talk' event feature. ▪ **0** Disable (default) ▪ **1** Enable The phone automatically answers an incoming call if it receives a SIP NOTIFY message with the 'talk' event. If a call is already in progress, the call is put on hold and the incoming call is answered.

Parameter	Description
voip/advanced_auto_answer/timeout	The timeout before the call is answered (in seconds). Range: 0 – 60 (seconds) ▪ **5** = 5 seconds (default) ▪ **0** = immediately
voip/advanced_auto_answer/type	▪ **SIP_Header** (default) = identical to the parameter 'voip/auto_answer/enabled' described above ▪ **Manual** = the phone automatically answers incoming calls according to the timeout configured in the 'voip/advanced_auto_answer/timeout' parameter
voip/auto_answer_use_180/enabled=0	Determines whether or not the phone will ring before auto answer, or if auto answer will occur immediately, before the phone rings. ▪ **0** Disable (default) = No ringing occurs before auto answer; auto answer occurs immediately ▪ **1** Enable – Ringing occurs before auto answer

Note:

- The configuration file parameter 'voip/auto_answer/enabled' must be set to **1** to support the following:
  - √ voip/advanced_auto_answer/timeout
  - √ voip/advanced_auto_answer/type
  - √ voip/auto_answer_use_180/enabled

5.8.7 Configuring Do Not Disturb (DnD)

The Do not Disturb (DnD) feature can be configured. It can also be configured in BroadSoft's BroadWorks (see under Appendix A.1.3).

➢ **To configure DnD:**

- Use the table as reference.

Table 5-38: Do Not Disturb Parameters

Parameter	Description
voip/services/do_not_disturb/enabled	Enables the DnD feature. ▪ **0** Disable ▪ **1** Enable (default)

Parameter	Description
voip/line/0-5/do_not_disturb/activated	Activates the DnD feature per phone line, if the parameter 'voip/services/do_not_disturb/enabled' is enabled. ▪ **0** – Deactivate (default) ▪ **1** - Activate Three DnD configurations are possible in phones' idle screens: (1) If DnD is disabled, no notification will be displayed (2) If DnD is enabled for one line extension, one notification is displayed (3) If DnD is configured for two line extensions, two notifications are displayed. **Note:** DnD can also be activated in the phone's screen (more common).

➢ **To configure DnD on the phone:**

■ See the phone's *User's Manual* for detailed information.

5.8.8 Configuring Call Pick Up

Note: Applies to all devices except the 405HD phone.

Since the Call Pick Up feature is relevant only when Busy Lamp Field (BLF) is activated, the call pickup parameters appear as BLF related parameters.

➢ **To configure Call Pick Up:**

■ Use the table as reference.

Table 5-39: Call Pick Up Parameters

Parameter	Description
voip/services/call_pickup/enabled	Allows call pickup by pressing on the relevant BLF key when the remote phone's state is 'ringing'. ▪ **0 Disable** ▪ **1 Enable**
voip/services/call_pickup/access_code	Allows a user to answer another's call by pressing a user-defined sequence of phone keys. The default sequence is **. The user dials the sequence + the other user's phone number; the incoming call from the other phone is forwarded to the user's phone. For example, to pick up a call for extension 5000, dial ****5000**.

5.8.9 Configuring Message Waiting Indication

The Message Waiting Indication (MWI) feature can be configured.

➢ **To configure MWI:**

- Use the table as reference.

Table 5-40: MWI Parameters

Parameter	Description
voip/services/msg_waiting_ind/voice_mail_number	Defines the extension number for accessing your voice mail messages. ▪ The valid value is up to 64 characters.
voip/services/msg_waiting_ind/enabled	Enables the MWI feature. ▪ **0** Disable ▪ **1** Enable (default)
voip/services/msg_waiting_ind/subscribe	Determines whether the phone registers to an MWI server. ▪ **0** Disable (default) ▪ **1** Enable
voip/services/msg_waiting_ind/subscribe_address	The IP address or host name of the MWI server. Default: 0.0.0.0
voip/services/msg_waiting_ind/subscribe_port	The port number of the MWI server. Range: 1024-65535. Default: 5060.
voip/services/msg_waiting_ind/expiraition_timeout	The interval between the MWI Subscribe messages. Range:0-86400. Default: 3600
voip/services/msg_waiting_ind/always_send_port	If the SIP port is the default port (i.e. 5060), then remove it from the Request-URI of the MWI SUBSCRIBE. ▪ **0** Disable ▪ **1** Enable (default)

5.8.10 Configuring Busy Lamp Field

The Busy Lamp Field (BLF) feature can be configured.

Note: Applies to all devices except the 405HD phone.

➢ **To configure BLF:**

- Use the table as reference.

Table 5-41: BLF Parameters

Parameter	Description
voip/services/busy_lamp_field/enabled	Enables the BLF feature: ▪ **0** Disable ▪ **1** Enable (default)
voip/services/busy_lamp_field/subscription_period	The interval between BLF and SIP SUBSCRIBE messages. Range: 0 to 86400. Default: 3600.
voip/services/busy_lamp_field/uri	Only displayed if 'Type' is set to **BSFT**. The user resource list. This must be the username (not the domain name). For example, if the URI resource list is **mylist@server.com**, then only the value **mylist** must be entered. The valid value is up to 64 characters.
voip/services/busy_lamp_field/application_server/use_registrar	Only displayed if 'Type' is set to **BSFT**. Determines whether to use the registrar as the application server address. When enabled, there is no need to configure the application server address or domain name separately. ▪ **0** Disable (default) ▪ **1** Enable
voip/services/busy_lamp_field/application_server/addr	Only displayed if 'Type' is set to **BSFT** and the 'voip/services/busy_lamp_field/application_server/use_registrar' parameter is set to **0**.. Defines the IP address or host name of the application server. The valid value is up to 64 characters. Default: 0.0.0.0
BLF Call Pickup	
voip/services/call_pickup/access_code	See Section 5.8.8.
voip/services/call_pickup/enabled	See Section 5.8.8.

5.8.11 Configuring Advice of Charge

Note: Support pending.

The Advice of Charge (AOC) feature can be configured. The feature permits an accurate estimate of the size of the bill which will eventually be charged to be displayed.

➢ **To configure AOC:**

- Use the table as reference.

Table 5-42: AOC Parameters

Parameter	Description
system/aoc/enabled	Enables the 'advice of charge' feature. **0 Disable** **1 Enable**
system/aoc/currency	Sets the required currency for AOC display. The string represents the currency name (e.g., USD, EUR, NIS, etc.)
system/aoc/ratio	Sets the conversion ratio from the local currency. The string represents the ratio between the base currency to the set currency with a decimal point, e.g., : 3.8, 4.95, 1.

5.8.12 Configuring a Tone to Alert to Long Hold

Network administrators can configure an audible indication to be played after a call has been on hold for a long time. After a call has been on hold for a long time (the time is configurable), a reminder tone will be played every 10 seconds until the call is taken off hold.

➢ **To configure the feature**

- Use the table as reference.

Table 5-43: Reminder Tone after Long Hold

Parameter	Description
voip/lhcwrr_enabled	Enables the feature. **1** Enabled. After the length of time configured for configuration file parameter *voip/lhcwrr_wait_time* lapses (see the parameter below), a reminder tone (beep) is played every 10 seconds until the call is taken off hold. **0** Disabled (Default). No reminder tone (beep) is played, regardless of how long the call is on hold.
voip/lhcwrr_wait_time	Defines the length of time that must lapse before a reminder tone (beep) is played. The tone will then be played every 10 seconds until the call is taken off hold. Default: 120 seconds.

5.8.13 Disabling the HOLD Key

Note: Support pending.

The network administrator can disable hard keys and softkeys on phones. The feature is motivated by the requirement on the part of some enterprises to control settings remotely to comply with company policy.

➢ **To disable the HOLD key**:

- Use the table as reference.

Table 5-44: Disabling the HOLD Key

Parameter	Description
system/disable_hold_button	Disables the HOLD key on the phone's keypad. The HOLD key is used to place a call on hold, or to resume a held call.

Besides the HOLD key, other hard keys that can be disabled include speaker, headset, voicemail, REDIAL, CONTACTS, MENU, TRANSFER, VOL and mute.

For more information, see Section 6.3.

5.8.14 Configuring Onhook Disconnect when Held

Network administrators can configure whether the device automatically goes idle (i.e., on-hook) when the last remaining call is disconnected, or not.

➢ **To configure onhook disconnect when held:**

- Use the table as reference.

Table 5-45: Onhook Disconnect when Held

Parameter	Description
voip/onhook_disconnect_when_held/enabled	Choose either: ▪ **0** Disable (default) - If the receiver is placed on-hook after a call is put on hold, the call is put on speaker rather; it isn't disconnected. ▪ **1** Enable - If the receiver is placed on-hook after a call is put on hold, the call is disconnected.

5.8.15 Configuring the Ringer's Default Audio Device

The network administrator can configure the ringer's default audio device.

➢ **To configure the ringer's default audio device:**

- Use the table as reference.

Table 5-46: Configuring the Ringer's Default Audio Device

Parameter	Description
audio/stream/ringer/0/audio_device	Determines which device rings when a call comes in. Valid values are: ▪ **TYPE_SPEAKER** ▪ **BUILTIN_SPEAKER** (default) ▪ **USB_SPEAKER** ▪ **BLUETOOTH_SPEAKER (**applies to the 445HD and C450HD phones only) ▪ **TYPE_HEADSET** ▪ **USB_HEADSET** ▪ **BLUETOOTH_HEADSET** ▪ **TYPE_USB** ▪ **TYPE_BLUETOOTH** ▪ **ANALOG**

5.8.16 Enabling Hands Free Mode

Note: Support pending.

This feature maximizes flexibility for call center administrators, who can - for example - disable ringing on the speaker yet enable hands-free mode (talking and listening using the speaker).

➢ **To configure hands free mode:**

- Use the table as reference.

Table 5-47: Configuring Hands Free Mode

Parameter	Description
voip/hands_free_mode/enabled	Configure either: ▪ **1** = Enabled (default) ▪ **0** = Disabled When disabled **0**: ▪ hands-free mode becomes unavailable ▪ pressing the speaker key does not have any effect ▪ when answering a call, the headset is the default audio

5.8.17 Enabling Supervisors to Listen in

Note: Support pending.

This feature allows the call center supervisor to pick up an agent's handset and listen in on the conversation that the agent is conducting on headphones with the customer, without the customer at the other end sensing that the supervisor is listening in (because the supervisor is in effect muted).

➢ **To enable supervisors to listen in:**

- Use the table as reference.

Table 5-48: Enabling Supervisors to Listen in

Parameter	Description
voip/services/supervisor_listen_in/enabled	Configure either: ▪ **1** = Enabled ▪ **0** = Disabled (default) If enabled, a call center supervisor can pick up an agent's handset and listen in on the conversation that the agent is conducting on headphones with the customer, without the customer at the other end sensing that the supervisor is listening in (because the supervisor is in effect muted).

5.8.18 Allowing an Incoming Call when the Phone is Locked

Note: Support pending.

The network administrator can configure the phone to allow or not allow an incoming call when the phone is locked.

➢ **To allow an incoming call when the phone is locked:**

- Use the table as reference.

Table 5-49: Allowing an Incoming Call when the Phone is Locked

Parameter	Description
system/lock/2-5/allow_incoming_calls	Allows incoming calls when the phone is locked (default). ▪ If allowed, the user will need to enter an unlock password to answer an incoming call. ▪ If not allowed, the incoming call will be automatically rejected by the phone.
system/lock/2-5/enabled	Enables the phone's lock feature. Relevant for supporting servers only.

5.8.19 Allowing Call Center Agents to Record Welcome Greetings

Note: Support pending.

The network administrator can configure whether to allow or not allow call center agents to record welcome greetings.

➢ **To let Call Center agents record welcome greetings:**

- Use the table as reference.

Table 5-50: Letting Call Center Agents Record Welcome Greetings

Parameter	Description
voip/services/greeting/beep/enabled	Enables a beep to be heard by the agent when the recorded welcome greeting finishes playing. ▪ **1** = Enabled (default) ▪ **0** = Disabled
voip/services/greeting/enabled	Lets agents in a call center record directly on their phones personal voice greetings which play automatically when callers call in, to welcome callers to the service they're seeking. Configure: ▪ **1** = Enabled ▪ **0** = Disabled (default)

5.8.20 Enabling the Electronic Hook Switch

The phone supports the Electronic Hook Switch (EHS) DHSG feature. Calls can be answered and volume level can be changed with EHS-capable headsets. The feature is supported on the following headsets:

- Jabra® PRO 920
- Jabra® PRO 9450

The headset's base unit connects to the phone's headphone port. The Audio connector connects to the headphone's port. The management connector connects to the Auxiliary port using a DHSG cable which can be ordered from AudioCodes.

The feature can be enabled. The feature allows users to handle calls, i.e., answer calls and change volume level, with EHS-capable wireless headsets at a distance from the phone.

➢ **To enable EHS:**

- Configure the EHS parameter using the table below as reference, and then click **Submit**.

Table 5-51: EHS Parameter

Parameter	Description
voip/services/electronic_hook_switch/enabled	Enables the EHS DHSG-standard feature. ▪ **0** Disable (default) ▪ **1** Enable DHSG (Drahtlose Hör-Sprechgarnitur) is the protocol used to convert a wireless headset's internal control signals to a commonly supported standard, and which uses the special AUX port. Supported wireless headsets can be connected to the AUX port (in addition to the regular headset port). This allows the user to connect and disconnect calls by pressing the button on the headset.

The base unit of the headset connects to the phone's headset port, i.e., to the same port that all headsets' base units connect to. The Audio connector must be connected to the headphones port. The management connector must be connected to the Auxiliary port using a DHSG-standard cable which can be ordered from AudioCodes.

5.8.21 Disabling the Hard Mute Key on the Phone

Note: Support pending.

The network administrator can disable the mute hard key on phones. The feature is motivated by the requirement on the part of some enterprises to control the key remotely to comply with company policy.

➢ **To disable the hard mute key on the phone:**

- Use the table as reference.

Table 5-52: Disabling the Hard Mute Key on the Phone

Parameter	Description
voip/block_mute_key	Allows network administrators to configure enabling or disabling the hard mute key on the phone. ▪ **0** (default) Allows the hard mute key on the phone to function regularly. ▪ **1** Disables the hard mute key on the phone.

In addition to the mute key, hard keys that can be disabled include speaker, headset, voicemail, REDIAL, CONTACTS, MENU, TRANSFER, HOLD, and VOL. See also Section 6.3 for information about disabling these keys.

5.8.22 Configuring Call Transfer

The network administrator can configure a softkey with attended and blind call transfer functionality.

➢ **To configure a softkey with attended / blind call transfer functionality:**

Use the table as reference:

Table 5-53: Configuring a Softkey with Attended and Blind Call Transfer Functionality

Parameter	Description
personal_settings/soft_keys/ongoing_call/0/key_function	Default: **BLIND_TRANSFER**. A softkey with blind transfer functionality will be displayed in the phone screen: Change the default to **TRANSFER** to configure the softkey with attended transfer functionality.

5.8.22.1 Configuring the TRANSFER Key to Perform Consultative Transfer

The phone's hard TRANSFER key *by default* performs *blind transfer* but you can change the default for the key to perform *consultative transfer*.

You need to reconfigure the parameter 'voip/signalling/sip/hk_blind_transfer/enable' as shown in this section.

➢ **To change the TRANSFER key functionality:**

- Use the table below as reference, and then click **Submit**.

Table 5-54: Changing TRANSFER Key Functionality

Parameter	Description
voip/signalling/sip/hk_blind_transfer/enable	[Not applicable to 405HD] Changes the hard TRANSFER key's functionality from performing blind transfer (default) to performing consultative transfer. ▪ **0** TRANSFER hard key performs Consultative Transfer ▪ **1** TRANSFER hard key performs Blind Transfer (default)

5.8.23 Creating a Speed Dial

The configuration file parameter 'provisioning/speed_dial_uri' can be configured to point to a user-defined Speed Dial file so that when the cfg file is uploaded to the phone, the speed dial settings are also uploaded.

The file can include a list of speed dial configurations. The file must be a simple text file that can be created using an Excel document and saved as a CSV file.

The syntax is:

```
<memory key>,<speed dial phone number>,<type>
```

where:

- <memory key> denotes the speed dial memory key on the phone.
- <speed dial phone number> denotes the phone number that is automatically dialed when the user presses the speed dial key.
- <type> denotes the Speed Dial feature and must be set to **0**.

Below is an example of a Speed Dial file:

```
1,4418,0
2,4403,0
3,039764432,0
4,4391,0
12,1234,0
```

5.8.24 Configuring Call Park

This service allows a user to 'park' a call in a 'parking lot'. The 'parked' user is placed on hold until a user in the enterprise retrieves the parked call. The feature improves user experience (UX) by providing users with an indication of calls currently parked.

Note: The feature is not supported on:

- 450HD/C450HD phones without an Expansion Module (the feature *is supported* on these phones when they have an Expansion Module)
- HRS conference device
- RX50 conference phone

➢ **To configure a key for Call Park:**

- Open the Configuration File page (**Management** > **Manual Update** > **Configuration File**) and locate the Call Park and Function Key parameters.

Table 5-55: Call Park Parameters

Parameter Name	Value	Type	Description
voip/services/busy_lamp_field/enabled	1	Bool	BLF support **0**=Disable **1**=Enable (default)]
voip/services/park_with_refer	1	Bool	Automatic blind transfer for parking **0**=Disable (default) **1**=Enable
voip/services/retrieve_prefix	According to the server configuration	String	Adds a prefix to the speed dial before retrieving the parked call. Default = *26
voip/services/park_prefix	According to the server configuration	String	Adds a prefix to the speed dial before parking the call. Default = *32

Table 5-56: Functional Key Parameters

Parameter Name	Description
personal_settings/functional_key/0-n/key_label	Defines a label for a Parking Lot.
personal_settings/functional_key/0-n/speed_dial_number	The telephone extension which the speed dial dials. The speed-dial feature helps users quickly dial extensions that are frequently used or that are hard to remember, or which include letters.
personal_settings/functional_key/0-n/type= PARKING_LOT	Gives users the ability to monitor the parking extension (busy, idle) and park/unpark calls by pressing the functional key.

5.9 Configuring Volume Levels

The network administrator can configure volume levels such as gain control and tone volume.

5.9.1 Configuring Gain Control

Automatic Gain Control can be configured.

Note: It's strongly advisable not to change the Automatic Gain Control parameter values. Consult with your AudioCodes representative if you require any modification.

5.9.2 Configuring Tone Volume

Tone volume can be configured.

Note: It's strongly advisable *not* to change the default values.

➢ **To configure tone volume:**

- Use the table as reference.

Table 5-57: Tone Volume Parameter

Parameter	Description
voip/audio/gain/tone_signal_level	Call Progress Tone volume. This volume can be modified on-the-fly by pressing the phone's VOLUME key in certain scenarios. The valid range is 1 to 31 (-dB). The default value is 2.

5.9.3 Configuring Ringer Volume

The ringer volume can be configured.

Note: It's strongly advisable *not* to change the default values.

➢ **To configure the ringer volume:**

- Use the table as reference.

Table 5-58: Ringer Volume Parameters

Parameter	Description
voip/audio/gain/ringer_signal_level	Ringing tone volume. This volume can be modified on-the-fly by pressing the phone's VOLUME key when the phone is in idle state. The valid range is -31 to 31 dB

5.9.4 Configuring Speaker Volume

The speaker volume can be configured.

Note: It's strongly advisable *not* to change the default values.

➢ **To configure speaker volume:**

- Use the table as reference.

Table 5-59: Speaker Parameters

Parameter	Description
Hands-free Gain Parameters **Note:** Values are in decibels (dB) ▪ Decimal places: Use underscore instead of period (e.g.,**plus19_5db**).	
voip/audio/gain/NB/handsfree_digital_input_gain	Digital input gain (in dB) – Narrow Band. Default = -6. The valid range is (-32) to 31 (dB), where -32 is mute.
voip/audio/gain/NB/handsfree_digital_output_gain	Digital output gain (in dB) – Narrow Band. Default = -10. The valid range is (-32) to 31 (dB), where -32 is mute.
voip/audio/gain/WB/handsfree_digital_input_gain	Digital input gain (in dB) – Wide Band. Default = -6. The valid range is (-32) to 31 (dB), where -32 is mute.
voip/audio/gain/WB/handsfree_digital_output_gain	Digital output gain (in dB) – Narrow Band. Default = -10. The valid range is (-32) to 31 (dB), where -32 is mute.
voip/audio/gain/NB/handsfree_analog_output_gain	Analog output gain (in dB) – Narrow Band. Valid values: **0db** (default), **minus1_5db**, **minus3db**, **minus4_5db**, **minus6db**, **minus7_5db**, **minus9db**, **minus10_5db**, **minus12db**, **minus13_5db**, **minus15db**, **minus16_5db**, **minus18db**, **minus19_5db**, **minus21db**, **minus22_5db**, **minus24db**, **minus25_5db**, **minus27db**, **minus28_5db**, **minus30db**, **minus31_5db**, **minus33db**, **minus34_5db**, **minus36db**, **minus37_5db**, **minus39db**, **minus39db**, **minus42db**, **minus48db**, **minus54db, MUTE**

Parameter	Description
voip/audio/gain/WB/handsfree_analog_output_gain	Analog output gain (in dB) – Wide Band. Valid values: **0db** (default), **minus1_5db**, **minus3db**, **minus4_5db**, **minus6db**, **minus7_5db**, **minus9db**, **minus10_5db**, **minus12db**, **minus13_5db**, **minus15db**, **minus16_5db**, **minus18db**, **minus19_5db**, **minus21db**, **minus22_5db**, **minus24db**, **minus25_5db**, **minus27db**, **minus28_5db**, **minus30db**, **minus31_5db**, **minus33db**, **minus34_5db**, **minus36db**, **minus37_5db**, **minus39db**, **minus39db**, **minus42db**, **minus48db**, **minus54db, MUTE**
voip/audio/gain/NB/handsfree_analog_input_gain	Analog input gain (in dB) – Narrow Band Valid values: **0db**, **plus1_5db**, **plus3db**, **plus4_5db**, **plus6db**, **plus7_5db**, **plus9db**, **plus10_5db**, **plus12db**, **plus13_5db**, **plus15db**, **plus16_5db**, **plus18db**, **plus19_5db**, **plus21db**, **plus22_5db**, **plus24db**, **plus25_5db**, **plus27db**, **plus28_5db**, **plus30db** (default), **plus31_5db**, **plus33db**, **plus34_5db**, **plus36db**, **plus37_5db**, **plus39db**, **plus40_5db**, **PLUS42DB**, **plus48db**, **plus54db**, **MUTE**
voip/audio/gain/WB/handsfree_analog_input_gain	Analog input gain (in dB) – Wide Band. Valid values: **0db**, **plus1_5db**, **plus3db**, **plus4_5db**, **plus6db**, **plus7_5db**, **plus9db**, **plus10_5db**, **plus12db**, **plus13_5db**, **plus15db**, **plus16_5db**, **plus18db**, **plus19_5db**, **plus21db**, **plus22_5db**, **plus24db**, **plus25_5db**, **plus27db**, **plus28_5db**, **plus30db** (default), **plus31_5db**, **plus33db**, **plus34_5db**, **plus36db**, **plus37_5db**, **plus39db**, **plus40_5db**, **PLUS42DB**, **plus48db**, **plus54db**, **MUTE**
voip/audio/gain/NB/additional_speaker_gain	Additional parameter for speaker gain configuration, for Narrow Band. Valid values: ▪ **0** 0dB ▪ **1** 1dB ▪ **2** 2dB ▪ **3** 3Db (default)
voip/audio/gain/WB/additional_speaker_gain	Additional parameter for speaker gain configuration, for Wide Band. Valid values: ▪ **0** 0dB ▪ **1** 1dB ▪ **2** 2dB ▪ **3** 3dB (default)

5.9.5 Configuring Handset Volume

The handset volume can be configured.

Note: It's strongly advisable *not* to change the default values. The feature does not apply to the RX50 conference phone.

➢ **To configure handset volume:**

- Use the table as reference.

Table 5-60: Handset Gain Parameters

Parameter	Description
Handset Gain Parameters **Note:** Values are in decibels (dB)	
voip/audio/gain/NB/handset_digital_input_gain	Digital input gain (in dB) – Narrow Band. Default = -2. The valid range is (-32) to 31 (dB), where -32 is mute.
voip/audio/gain/WB/handset_digital_input_gain	Digital input gain (in dB) – Wide Band. Default = -2. The valid range is (-32) to 31 (dB), where -32 is mute.
voip/audio/gain/WB/handset_digital_output_gain	Digital output gain (in dB) – Wide Band. Default = -8. The valid range is (-32) to 31 (dB), where -32 is mute.
voip/audio/gain/NB/handset_analog_output_gain	Analog output gain (in dB), for Narrow Band. Valid values: **0DB** (default), **minus1_5db**, **minus3db**, **minus4_5db**, **minus6db**, **minus7_5db**, **minus9db**, **minus10_5db**, **minus12db**, **minus13_5db**, **minus15db**, **minus16_5db**, **minus18db**, **minus19_5db**, **minus21db**, **minus22_5db**, **minus24db**, **minus25_5db**, **minus27db**, **minus28_5db**, **minus30db**, **minus31_5db**, **minus33db**, **minus34_5db**, **minus36db**, **minus37_5db**, **minus39db**, **minus39db**, **minus42db**, **minus48db**, **minus54db**, **MUTE**

Parameter	Description
voip/audio/gain/WB/handset_analog_output_gain	Analog output gain (in dB), for Wide Band. Valid values: **0DB** (default), **minus1_5db**, **minus3db**, **minus4_5db**, **minus6db**, **minus7_5db**, **minus9db**, **minus10_5db**, **minus12db**, **minus13_5db**, **minus15db**, **minus16_5db**, **minus18db**, **minus19_5db**, **minus21db**, **minus22_5db**, **minus24db**, **minus25_5db**, **minus27db**, **minus28_5db**, **minus30db**, **minus31_5db**, **minus33db**, **minus34_5db**, **minus36db**, **minus37_5db**, **minus39db**, **minus39db**, **minus42db**, **minus48db**, **minus54db**, **MUTE**
voip/audio/gain/NB/handset_analog_input_gain	Analog input gain (in dB), for Narrow Band. Default: **PLUS42DB** Valid values: **0dB, plus1_5dB, plus3dB, plus4_5dB, plus6dB, plus7_5dB, plus9dB, plus10_5dB, plus12dB, plus13_5dB, plus15dB, plus16_5dB, plus18dB, plus19_5dB, plus21dB, plus22_5dB, plus24dB, plus25_5dB, plus27dB, plus28_5dB, plus30dB, plus31_5dB, plus33dB, plus34_5dB, plus36dB, plus37_5dB, plus39dB, plus40_5dB, plus42dB, plus48dB, plus54dB, MUTE**
voip/audio/gain/WB/handset_analog_input_gain	Analog input gain (in dB), for Wide Band. Default: **PLUS42DB** Valid values: **0dB, plus1_5dB, plus3dB, plus4_5dB, plus6dB, plus7_5dB, plus9dB, plus10_5dB, plus12dB, plus13_5dB, plus15dB, plus16_5dB, plus18dB, plus19_5dB, plus21dB, plus22_5dB, plus24dB, plus25_5dB, plus27dB, plus28_5dB, plus30dB, plus31_5dB, plus33dB, plus34_5dB, plus36dB, plus37_5dB, plus39dB, plus40_5dB, plus42dB, plus48dB, plus54dB, MUTE**
voip/audio/gain/handset_analog_sidetone_gain	Analog side tone gain (in db). Valid values: **minus9db**, **MINUS21DB** (default), **minus15db**, **minus18db**, **minus21db**, **minus24db**, **minus27db**, **MUTE**

5.9.6 Configuring Headset Volume

Headset volume can be configured.

Note: It's strongly advisable *not* to change the default values. The feature does not apply to the RX50 conference phone.

➢ **To configure headset volume**:

- Use the table as reference.

Table 5-61: Headset Gain Parameters

Parameter	Description
Headset Gain Parameters **Note:** Values are in decibels (dB) ▪ Decimal places: Use underscore instead of period (e.g.,**plus19_5db**).	
voip/audio/gain/NB/headset_digital_input_gain	Digital input gain (in dB) – Narrow Band. Default = -4. The valid range is (-32) to 31 (dB), where -32 is mute.
voip/audio/gain/WB/headset_digital_output_gain	Digital output gain (in dB) – Wide Band. Default = -12. The valid range is (-32) to 31 (dB), where -32 is mute.
voip/audio/gain/WB/headset_digital_input_gain	Digital input gain (in dB) – Wide Band. Default = -4. The valid range is (-32) to 31 (dB), where -32 is mute.
voip/audio/gain/NB/headset_analog_output_gain	Analog output gain (in dB), for Narrow Band. Valid values: **0DB** (default), **minus1_5db**, **minus3db**, **minus4_5db**, **minus6db**, **minus7_5db**, **minus9db**, **minus10_5db**, **minus12db**, **minus13_5db**, **minus15db**, **minus16_5db**, **minus18db**, **minus19_5db**, **minus21db**, **minus22_5db**, **minus24db**, **minus25_5db**, **minus27db**, **minus28_5db**, **minus30db**, **minus31_5db**, **minus33db**, **minus34_5db**, **minus36db**, **minus37_5db**, **minus39db**, **minus39db**, **minus42db**, **minus48db**, **minus54db**, **MUTE**
voip/audio/gain/WB/headset_analog_output_gain	As above, but for Wide Band.
voip/audio/gain/NB/headset_analog_input_gain	Analog input gain (in dB). Valid values: **PLUS31_5DB**, **plus1_5db**, **plus3db**, **plus4_5db**, **plus6db**, **plus7_5db**, **plus9db**, **plus10_5db**, **plus12db**, **plus13_5db**, **plus15db**, **plus16_5db**, **plus18db**, **plus19_5db**, **plus21db**, **plus22_5db**, **plus24db**, **plus25_5db**, **plus27db**, **plus28_5db**, **plus30db**, **plus31_5db**, **plus33db**, **plus34_5db** (default), **plus36db**, **plus37_5db**, **plus39db**, **plus40_5db**, **plus42db**, **plus48db**, **plus54db**, **MUTE**

Parameter	Description
voip/audio/gain/WB/headset_analog_input_gain	Analog input gain (in dB). Valid values: **0db**, **plus1_5db**, **plus3db**, **plus4_5db**, **plus6db**, **plus7_5db, plus9db, plus10_5db, plus12db, plus13_5db, plus15db, plus16_5db, plus18db, PLUS31_5DB, plus21db, plus22_5db, plus24db**, **plus25_5db**, **plus27db**, **plus28_5db**, **plus30db**, **plus31_5db**, **plus33db**, **plus34_5db** (default), **plus36db**, **plus37_5db**, **plus39db**, **plus40_5db**, **plus42db**, **plus48db**, **plus54db**, **MUTE**
voip/audio/gain/headset_analog_sidetone_gain	Analog side tone gain (in db). Valid values: **minus9db**, **MINUS12DB**(default), **minus15db**, **minus18db**, **minus21db**, **minus24db**, **minus27db**, **MUTE**

6 Configuring Phone Settings

6.1 Configuring the Phone Directory

Note: Support pending.

6.1.1 Configuring the Corporate Directory

The Corporate Directory can be configured.

6.1.1.1 Configuring the LDAP-based Corporate Directory

The network administrator can configure Lightweight Directory Access Protocol (LDAP), which is an application protocol for accessing and maintaining distributed directory information services over an IP network. It is fully described under RFC 4510.

➢ **To configure LDAP:**

- Use the table as reference.

Table 6-1: LDAP Parameters

Parameter Name	Description
system/ldap/enabled	Enables or disable LDAP.
system/ldap/server_address	Defines the IP address or URL of the LDAP server.
system/ldap/port	Defines the LDAP service port.
system/ldap/user_name	Defines the user name used for the LDAP search request.
system/ldap/password	Defines the password of the search requester.
system/ldap/base	Defines the access point on the LDAP tree.
system/ldap/name_filter	Specifies your search pattern for name look ups. For example: When you type in the following field: *(&(telephoneNumber=*)(sn=%))*, 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 following field: *(|(cn=%)(sn=%))*, the search result includes all LDAP records which have the '("cn"-->CommonName)' OR '("sn"-->Surname)' field starting with the entered prefix. When you type in the following field: *(!(cn=%))*, the search result includes all LDAP records which "do not" have the "cn" field starting with the entered prefix.

Parameter Name	Description
system/ldap/name_attrs	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.
system/ldap/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 following field: *(&(telephoneNumber=%)(sn=*))*, the search result is all LDAP records which have the “sn” field set and the “telephoneNumber” match the number being searched.
system/ldap/number_attrs	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.
system/ldap/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, forexample:**%sn, %givenName,** the displayed result returned should be “Black, Mike”.
system/ldap/max_hits	Specifies the maximum number of entries expected to be sent by the LDAP server (this parameter is sent to the LDAP server).
system/ldap/sorting_result	Sorts the search result by display name on the client side.
system/ldap/predict_text	This parameter appears in the configuration file; however, it is currently not supported.
system/ldap/search_timeout	The time out value for LDAP search (this parameter is sent to the LDAP server).
system/ldap/ui/use_right_arrow_active_search	This parameter appears in the configuration file; however, it is currently not supported.
system/ldap/lookup_incoming_call	This parameter appears in the configuration file; however, it is currently not supported.

Parameter Name	Description
system/ldap/call_lookup	Performs an LDAP search during call (search the display name for a number).
system/ldap/country_code	Defines the country code prefix added for number search.
system/ldap/area_code	Defines the area code prefix added for number search.
system/ldap/minimal_name_search_length	Starts to perform an LDAP search after x characters are input.
system/ldap/send_queries_while_typing	Sends an LDAP search each time the user presses a key (all keys with both number and letters).

6.1.1.2 Loading a Text-based Corporate Directory File

The Configuration file can include a link to a user-defined Corporate Directory file, using the 'provisioning/corporate_directory_uri' parameter. This allows you to upload a corporate directory to the phone.

Three types of corporate directory files are supported: txt, cfg, and xml

The corporate directory file includes a list of contacts and their phone numbers.

The syntax of the corporate directory file must be as follows:

```
<full name>,<office>,<home>,<mobile>
```

For example:

```
John Smith,1234,98765432,574685746
```

If not all phone numbers are required, the relevant field must be left empty. For example, in the directory entry below, the home and user-defined numbers are absent:

```
John Smith,1234,,574685746
```

➢ **To configure the Corporate Directory:**

- Use the table as reference.

Table 6-2: Provisioning Parameters

Parameter	Description
provisioning/corporate_directory_uri	The URI for retrieving the corporate directory. The corporate directory must be included in a separate file to be loaded to the phone during provisioning. For example: **provisioning/corporate_directory_uri=corporate_dir.txt** **Note:** ▪ The corporate directory file is loaded after boot up and after that, periodically. ▪ If the corporate directory file is new, the phone updates the information and does not reboot.

6.2 Configuring Keys

The network administrator can configure the following keys:

- Function and Programmable Keys (see Section 6.2.1) – applies to all phones except 405HD
- Speed Dials (with a dedicated configuration file) (see Section 6.2.1.1)
- Softkeys (see Section 6.2.2) – applies to all phones
- Programmable Softkeys (see under Section 6.2.2.1)
- Navigation Keys (see Section 6.2.3) – applies to all phones

6.2.1 Configuring Function and Programmable Keys

On the **430HD** phone, up to 12 Function Keys can be configured for Speed Dials and for Multicast Paging (for configuring Multicast Paging, see Section 6.4). The 12 Function Keys are located on the sidecar. The panes next to the LED keys are covered.

On the 440HD and 445HD phones, up to 33 Function Keys can be configured. Of these, you can configure up to 12 as Speed Dials. When more than 12 are configured, these keys can only be assigned as regular Speed Dials or for Multicast Paging (see Section 6.4). The 33 Speed Dials are configured on pages 1, 2 and 3 of the phone's sidecar. Users define 12 Speed Dials and then when defining the 13th, the 12th Speed Dial shows the page number and the name in the 12th moves to the 13th.

On all three phones, six programmable keys are located adjacent to the screen. There are three on each side.

To configure 1-6 Programmable Keys, configure **n** = **12-17** correspondingly.

To configure 1-12 Functional Keys, configure **n** = **0-11** correspondingly.

To configure 13-33 Functional Keys, configure **n** = **18-38** correspondingly.

On the 450HD / C450HD / HRS:

To configure 1-8 Programmable Keys, configure **n** = **0-7** correspondingly.

On the 450HD / C450HD phone with Expansion Module:

To configure 1-22 Functional Keys, configure **n** = **8-29** correspondingly.

On the 405HD phone:

To configure 1-9 Programmable Keys, configure **n** = **0-8** correspondingly.

On the RX50 conference device configure:

functional_key/0-5

Speed_dial/0-5

Table 6-3: Function / Programmable Keys Parameters

Parameter Name	Description
personal_settings/functional_key/n/key_label	Used to define a free string label allowing users to identify the key.
personal_settings/functional_key/n/type	Choose either: ▪ **EMPTY** = (default) If left as is, the key will be disabled. [N/A to 405HD] ▪ **SPEED_DIAL** = key to help users quickly dial numbers that are often used or hard to remember.

Parameter Name	Description
	▪ **PAGING =** When the Paging feature is enabled, you can define Paging Groups (see Section 6.4). ▪ **SIP_ACCOUNT =** Key dedicated to a specific line. Available for a private and a shared line. The line ID is configured with the 'functional_key/n/line' parameter (see below). [N/A to 405HD] ▪ **Event** = Key used to access events like DnD, Missed Call, etc. (See the next parameter for more information). [N/A to 405HD] ▪ **VocaNOM** = Enable the key if the feature is enabled. See Section 5.3 for more information. ▪ **Parking_Lot** = Gives users the ability to monitor the parking extension (busy, idle) and park/unpark calls by pressing the functional key. [N/A to 405HD]
personal_settings/functional_key/n/key_event	▪ Missed_Calls ▪ Received_Calls ▪ Dialed_Calls ▪ Directory ▪ Dnd_All ▪ Forward_All
personal_settings/functional_key/n/speed_dial_number	Allows the user to quickly call someone whose number is often used or is hard to remember. Default: 4403.
personal_settings/functional_key/n/line	Corresponding to the line ID. **n** = the value you configured as the line index as shown in Section 5.1.3.

6.2.1.1 Configuring a Configuration File for Speed Dials Only

See Section 5.8.23 for more information.

6.2.2 Configuring Softkeys

Note:

- The section applies to all phone models.
- When Genesys' ACD is enabled (support pending), the **Soft Keys** item in the Keys Configuration menu is not displayed.

This section describes how to configure softkeys. Four softkeys, located below the phone's screen, can be configured. Their functionality is context sensitive according to the phone's state. The network administrator can configure softkeys that are activated when the phone is in idle state and when it is in call state. Following are the four default (preconfigured) softkeys (0-3), when the phone is in idle state and when it is in call state.

Table 6-4: Default Softkeys

Key	Idle State	Call State
0	CONTACTS	BXfer
1	Missed	Conf
2	Forward	Call Menu
3	Do Not Disturb (Status)	End

When more than four softkeys are configured, users can scroll to additional softkeys.

- Up to 20 (0-19) softkey functions can be configured for when the phone is in idle call state.
- Up to 20 (0-19) softkey functions can be configured for when the phone is in call state.
- Up to 12 (0-11) programmable softkey (PSKs) functions can be configured to either a call state softkey or an idle state softkey.

➢ **To configure softkeys:**

- Use the table as reference. Note that **n** in the table defines the softkey location number out of several existing options.

Table 6-5: SoftKey Parameters

Parameter Name	Description
personal_settings/soft_key/n/key_function	Possible values: **n** = 0-19. Select one of the following key function types for the idle screen: ▪ **NONE** ▪ **New_call** ▪ **Missed_calls** ▪ **Received_calls** ▪ **Dialed_calls** ▪ **All_calls** ▪ **Directory** ▪ **Dnd_all** ▪ **Forward_all** ▪ **PSK**

Parameter Name	Description
personal_settings/soft_keys/ongoing_call/n/key_function	Possible values: **n** = 0-19. Select one of the following key function types for the Ongoing call state: ▪ **NONE** ▪ **Transfer** ▪ **Blind_transfer** ▪ **Hold** ▪ **Conf** ▪ **New_call** • **End** ▪ **PSK** ▪ **Call_Menu** ▪ **Rec_call**
personal_settings/soft_keys/initiate_call/n/key_function	Possible values: **n** = **0-3**. ▪ **NONE** ▪ **Contacts** ▪ **Call_Log** ▪ **Speed_Dial** ▪ **URL**

6.2.2.1 Configuring Programmable Softkeys (PSKs)

Network administrators can configure a programmable key function and assign it to a softkey (Programmable Softkey-PSK) for either idle state or call state. The PSK can be used for performing actions such as connecting to a Voicemail (Ongoing Call state) server, returning the details of the last call (Idle state), connecting to the Conference server (Idle state) and activate an intercom (Idle state). When these softkeys are configured with such functionality, and the user presses these softkeys, the Enterprise's server (softswitch or application server) is instructed to perform these actions. The instructions to the softswitch or application server are applied using a prefix in the SIP INVITE message. An additional feature enables the user to enter a personal code before the softkey functionality can be activated.

For example, the user wishes to activate their Voice Mail to hear messages whenever the softkey configured for this feature is pressed. In this case, the user dials a prefix, for example *70, and then is prompted to enter a personal code to access their voice mail i.e not configured on the phone, only entered e.g. '1234'. Once this code is entered, the user is connected to the Enterprise's Voice Mail server and can listen to their messages.

The following example shows the configuration of softkey 0 for connecting to a Voicemail server. Note that in this example, psk index-1 is assigned to function key-0.

```
personal_settings/soft_key/0/key_function=PSK
personal_settings/soft_key/0/psk_index=1
personal_settings/soft_keys/psk/1/is_dial_required=1
personal_settings/soft_keys/psk/1/label=Voicemail
personal_settings/soft_keys/psk/1/prefix=*70
```

Note: You can configure the PSK to perform any action that is supported by your enterprises's softswitch or application server. AudioCodes provides the ability to configure a calling prefix and a dialing code and to include these in the SIP INVITE. The PSK can be configured using the configuration file.

Table 6-6: PSK Parameters

Parameter Name	Description
personal_settings/soft_keys/n/psk_index personal_settings/soft_keys/ongoing_call/n/psk_index	There are separate index number series for the idle screen and ongoing call screen. For the first parameter (idle screen): **n=0-19**. Valid values that can be configured: **0-11**. For the second parameter (ongoing call screen): **n=0-19**. Valid values that can be configured: **0-11**. These parameters associate softkeys with the PSK index. However, each index number represents unique functionality. For example, if you configure psk_index 1 to activate an intercom (an idle screen functionality), you cannot use the same index (psk_index 1) to connect to a Voicemail server (ongoing call screen functionality).
personal_settings/soft_keys/psk/n/is_dial_required	Configure either: ▪ **0** (disable) (default) ▪ **1** (enable) Determines whether a personal dialing code is required for the PSK. When enabled, the user is prompted on the phone to enter a personal code to activate this event. For example, to connect to a Voicemail server. The parameter only applies when 'Programmable SK' is set as the key_function. **n=0-11**
personal_settings/soft_keys/psk/n/PSKlabel	Defines the PSK label which is displayed on the phone's screen for the configured PSK.The parameter only applies when 'PSK' is set as the key_function. **n=0-11**
personal_settings/soft_keys/psk/n/prefix	Defines the prefix which sends a SIP INVITE to the softswitch to activate this feature (event). For example, ***70**. This parameter only applies when **PSK** is configured for parameter key_function. Up to 128 characters (any characters).

6.2.2.2 Configuring a PSK to Allow Paging during an Ongoing Call | Call Hold

Network administrators can allow users to perform paging during an ongoing call and during call hold. To enable the feature, administrators must program a softkey for users to use the functionality. The softkey is displayed in the ongoing call screen.

Note: Paging must be configured as described in Section 6.4 as a prerequisite for the feature to function. Default: Disabled ('voip/services/group_paging/enabled' = 0). The RX50 conference phone does not support this feature.

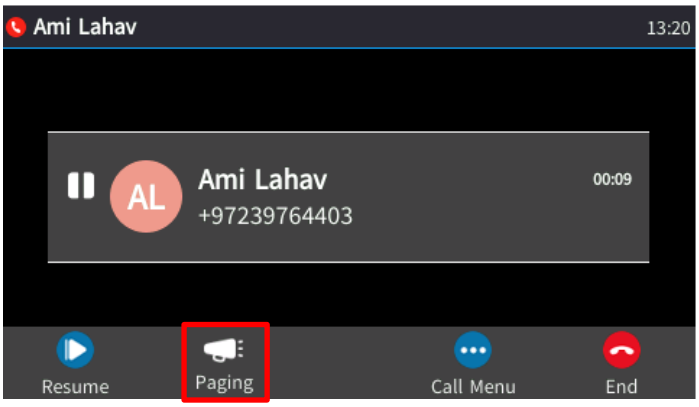
➢ **To configure a PSK for paging during call hold | ongoing call:**

- Use the table as reference:

Table 6-7: Configuring a PSK for Paging during an Ongoing Call | Call Hold

Parameter	Description
personal_settings/soft_keys/ongoing_call/n/key_function	Set to **PAGING**. Note that n=0-19.

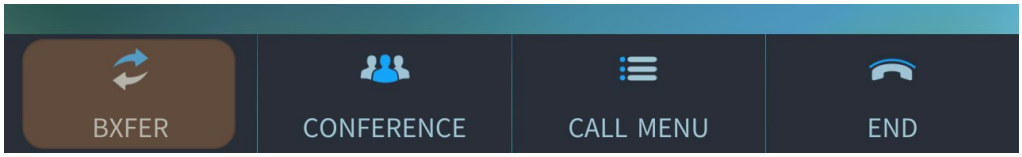
Users will view a 'Paging' softkey in the phone's Hold screen (i.e., in the screen displayed when the user holds a call):



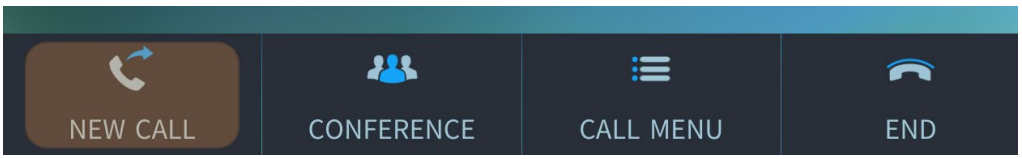
6.2.2.3 Configuring a PSK for a Customized UI Experience

Network administrators can configure Programmable Softkeys for New Call state, Ongoing call state and Idle screen state as part of the phone's capability of allowing a customized user interface experience.

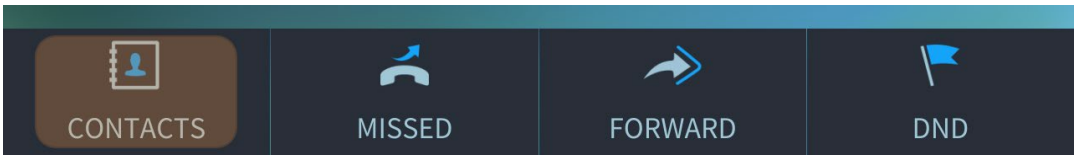
Administrators can customize the ongoing call screen (shown in the figure below) in line with the preferences / requirements of enterprise management and / or the employees.



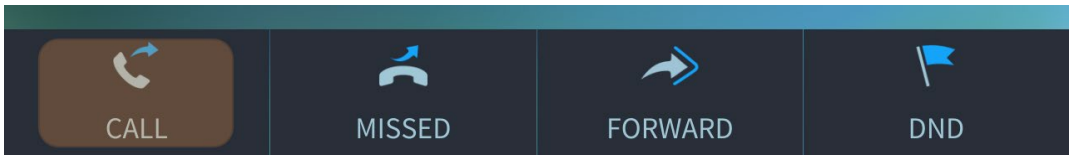
For example, the **BXfer** softkey in the ongoing call screen shown in the preceding figure can be replaced with the **New Call** softkey shown in the figure below on the phones of enterprise users who infrequently transfer calls.



Administrators can customize the idle screen (shown in the figure below) in line with the preferences / requirements of enterprise management and / or the employees.



For example, the **Contacts** softkey in the idle screen shown in the preceding figure can be replaced with the **Call** softkey shown in the figure below.



6.2.3 Configuring Navigation Control Button Positions

Note: Support pending.

Each of the four positions of the navigation control button on the phone, i.e., Up, Down, Left, and Right, as well as its **OK** button, can be configured to perform a one of five functions:

- None (default)
- Missed Calls
- Received Calls
- Dialed Calls
- All Calls
- Directory

The **OK** button can also be configured to perform one of these five functions.

➢ **To configure navigation control button positions:**

- Use the table as reference:

Table 6-8: Navigation Control Button Positions

Parameter Name	Description
personal_settings/navigation_control/0/key_operation	[Up] Allows pressing the upper rim of the navigation control button to perform an operation such as displaying **Missed Calls**.
personal_settings/navigation_control/1/key_operation	[Down] Allows pressing the lower rim of the navigation control button to perform an operation such as displaying **Missed Calls**.
personal_settings/navigation_control/2/key_operation	[Left] Allows pressing the left rim of the navigation control button to perform an operation such as displaying **Missed Calls**.
personal_settings/navigation_control/3/key_operation	[Right] Allows pressing the right rim of the navigation control button to perform an operation such as displaying **Missed Calls**.
personal_settings/navigation_control/4/key_operation	[OK] Allows pressing **OK** in the navigation control button to perform an operation such as displaying **Missed Calls**.

6.3 Disabling Hard Keys and Softkeys

Note: Support pending.

The network administrator can disable hard keys and softkeys on phones. The feature is motivated by the requirement on the part of some enterprises to control the setting remotely to comply with company policy.

Hard keys that can be disabled include speaker, headset, voicemail, REDIAL, CONTACTS, MENU, TRANSFER, HOLD, VOL and mute.

Example 1: To disable the phone's REDIAL hard key, the configuration file parameter *personal_settings/key/redial/enabled* can be set to **0**.

Example 2: To disable the option to restart the phone, the configuration file parameter *personal_settings/menu/restart/enabled* can be set to **0**.

Configuration file parameters that can be configured to disable hard keys and softkeys also include these in the table below.

Table 6-9: Parameters that can be Configured to Disable Hard Keys / Softkeys

Configuration File Parameters
personal_settings/soft_keys/display_idle_screen_keys_when_dialing/enabled
personal_settings/key/speaker_device/enabled
personal_settings/key/headset_device/enabled
personal_settings/key/voice_mail/enabled
personal_settings/key/redial/enabled
personal_settings/key/contacts/enabled
personal_settings/key/menu/enabled
personal_settings/key/hold/enabled
personal_settings/key/volume/enabled
personal_settings/key/mute/enabled
personal_settings/menu/call_log/enabled
personal_settings/menu/directory/enabled
personal_settings/menu/keys_configuration/enabled
personal_settings/menu/keys_configuration/speed_dial_keys/enabled
personal_settings/menu/keys_configuration/soft_keys/enabled
personal_settings/menu/keys_configuration/navigation_keys/enabled
personal_settings/menu/settings/enabled
personal_settings/menu/language/enabled
personal_settings/menu/ring_tone/enabled
personal_settings/menu/callwaiting/enabled
personal_settings/menu/date_and_time/enabled
personal_settings/menu/lcd_contrast/enabled

Configuration File Parameters
personal_settings/menu/backlight_timeout/enabled
personal_settings/menu/answer_device/enabled
personal_settings/menu/restart/enabled
personal_settings/menu/status/enabled
personal_settings/menu/administration/enabled
personal_settings/menu/languages/english/enabled
personal_settings/menu/languages/spanish/enabled
personal_settings/menu/languages/russian/enabled
personal_settings/menu/languages/portuguese/enabled
personal_settings/menu/languages/portuguesebrazilian/enabled
personal_settings/menu/languages/german/enabled
personal_settings/menu/languages/ukrainian/enabled
personal_settings/menu/languages/french/enabled
personal_settings/menu/languages/frenchcanadian/enabled
personal_settings/menu/languages/italian/enabled
personal_settings/menu/languages/hebrew/enabled
personal_settings/menu/languages/polish/enabled
personal_settings/menu/languages/korean/enabled
personal_settings/menu/languages/finnish/enabled
personal_settings/menu/languages/chinese/enabled
personal_settings/menu/languages/chinesetraditional/enabled
personal_settings/menu/languages/turkish/enabled
personal_settings/menu/languages/japanese/enabled
personal_settings/menu/languages/slovak/enabled
personal_settings/menu/languages/czech/enabled
personal_settings/speed_dial_programming/enabled
personal_settings/new_call_screen/call_log_soft_key/enabled
personal_settings/new_call_screen/directory_soft_key/enabled
personal_settings/soft_keys/incoming_call/sk_reject/enable
personal_settings/key/transfer/enabled
personal_settings/key/reject/enabled

6.4 Configuring Paging

Live announcements can be made (paged) from a phone to a group of phones to notify a team (for example) that a meeting is about to commence. The paged announcement is multicast via a designated group IP address, in real time, on all idle phones in the group, without requiring listeners to pick up their receivers. The name of the group is displayed on phone screens when the paging call comes in. A key for paging a group can be configured using the configuration file or on the phone itself (see the *User's Manual*).

➢ **To configure paging:**

- Use the table as reference.

Table 6-10: Configuration File Paging Parameters

Parameter	Description
voip/services/group_paging/enabled	Enables group paging. ▪ **0** Disabled (default) ▪ **1** Enabled
voip/services/group_paging/group/0-38/activated	Defines the group to page to. Default: Group 0
voip/services/group_paging/group/0-38/multicast_addr	Defines the multicast address for group 0-11 to page to. Default: 224.0.1.0
voip/services/group_paging/group/0-38/name	Defines the paging group name to display in the screen.
voip/services/group_paging/group/0-38/port	Defines the multicast port for group 0 to page to. Default: 8888
voip/services/group_paging/codec	The codec of the paging RTP. Since the phones have many DSP versions and different DSPs support different codecs, the codec of the paging call can be configured. Available options are: ▪ PCMU, PCMA ▪ G729 ▪ G722 ▪ G722_8000 **Note**: Phones that are in the same paging group must use the same codec.
voip/services/group_paging/end_income_paging_timeout	Defines the timeout that begins after the phone detects that it is not receiving RTP. The phone ends the incoming paging call when the timeout expires. Default: 500 milliseconds. Optionally, you can configure 500~ milliseconds to 100000 milliseconds.

6.4.1 Configuring Barge-in

When barge-in is disabled (default), users who're in regular calls when a paging call comes in are prompted in their phone screens to accept or reject the paging call. If they *accept*, the regular call is put on hold and the paging call is heard. If they *reject*, the regular call is continued and the paging call goes unheard.

Note: The prompt to accept or reject a paged call is only relevant to users who're in regular calls. If they're *not* in regular calls, the prompt is displayed irrespective of whether barge-in is disabled or enabled.

When barge-in is enabled, paging calls interrupt (barge in on) regular calls in progress, *without* prompting users with an option to accept or reject the paging call.

➢ **To enable barge-in:**

- Use the table as reference.

Table 6-11: Barge-in Parameters

Parameter	Description
voip/services/group_paging/allow_barge_in/enabled	Enables paging to interrupt (i.e., barge into) regular calls currently in progress. ▪ **0** Disabled (default) ▪ **1** Enabled

Note: See the phone's *User's Manual* for examples.

6.5 Configuring Feature Key Synchronization

Note: Support pending.

➢ **To configure Feature Key synchronization:**

- Use the table as reference.

Table 6-12: Feature Key Synchronization Parameters

Parameter	Description
system/feature_key_synchronization/enabled	Disables/enables Feature Key synchronization.
system/feature_key_synchronization/forward/0-3/destination	Forward destination. The number of the telephone to which the call is made.
system/feature_key_synchronization/status/0-3/fks_status	The status of the Feature Key synchronization. Select: ▪ FKS_NONE (Default) ▪ FKS_DND ▪ FKS_CFA ▪ FKS_CFB -or- ▪ FKS_CFNA

6.6 Configuring Phone Screen Settings

This section shows how to configure phone screen settings.

➢ **To configure phone screen settings:**

- Use the tables below as reference.

Table 6-13: Contrast Parameters – 405HD / 430HD / 440HD

personal_settings/lcd_contrast	Determines the phone screen contrast. 405HD / 430HD / 440HD: Range: 55-90. Default: 27.
personal_settings/enhanced_lcd_contrast	[430HD / 440HD] Determines the phone screen contrast. Range: 285-325. Default: 305.
personal_settings/blf_lcd_contrast	[430HD / 440HD) Determines BLF screen contrast. Configure to a level that is comfortable for the user. Range: 100-200. Default: 140.

Table 6-14: Brightness Parameters - 445HD / 450HD / C450HD

Parameter	Description
personal_settings/lcd_active_mode_brightness	Configures the brightness of the screen when its in 'active mode', which is - for example - after a calendar reminder pops up, or when a call comes in, or after you press a key on the dialpad, etc. • LOW • MEDIUM • HIGH (default)
personal_settings/lcd_active_mode_brightness_high	Configures the HIGH level of brightness when the screen is in 'active mode'. Minimum: 0. Maximum: 31 (default).
personal_settings/lcd_active_mode_brightness_low	Configures the LOW level of brightness when the screen is in 'active mode'. Minimum: 0. Maximum: 31. Default: 3.
personal_settings/lcd_active_mode_brightness_medium	Configures the MEDIUM level of brightness when the screen is in 'active mode'. Minimum: 0. Maximum: 31. Default: 20.
personal_settings/lcd_active_mode_timeout	Defines the timeout of 'active mode', in minutes. If the timeout expires, the screen changes to 'dimmer mode' (see the next parameter). Either: 15 (default), 30, 45 or 60 minutes.

Parameter	Description
personal_settings/lcd_dimmer_mode_brightness	Configures the brightness of the screen when its in 'dimmer mode'. The screen changes to 'dimmer mode' after the timout configured for 'active mode' times out (see the parameter above). Either: • LOW • MEDIUM (default) • HIGH
personal_settings/lcd_dimmer_mode_brightness_high	Configures the HIGH level of brightness when the screen is in 'dimmer mode'. Minimum: 0. Maximum: 31 (default).
personal_settings/lcd_dimmer_mode_brightness_low	Configures the LOW level of brightness when the screen is in 'dimmer mode'. Minimum: 0. Maximum: 31. Default: 3.
personal_settings/lcd_dimmer_mode_brightness_medium	Configures the MEDIUM level of brightness when the screen is in 'dimmer mode'. Minimum: 0. Maximum: 31. Default: 20.
personal_settings/lcd_dimmer_mode_timeout	Defines the timeout of 'dimmer mode', in minutes. If it expires, the screen changes to 'night mode' (see the next parameter). Either: 30, 60 (default), 90 or 120 minutes.
personal_settings/lcd_night_mode_brightness	Configures the brightness of the screen when its in 'night mode'. The screen changes to 'night mode' after the timout configured for 'dimmer mode' times out (see the parameter above). Either: • LOW (default) • MEDIUM • HIGH • There is no timeout for 'night mode'.
personal_settings/lcd_night_mode_brightness_high	Configures the HIGH level of brightness when the screen is in 'night mode'. Minimum: 0. Maximum: 31. Default: 26. There is no timeout for 'night mode'.
personal_settings/lcd_night_mode_brightness_low	Configures the LOW level of brightness when the screen is in 'night mode'. Minimum: 0. Maximum: 31. Default: 2. There is no timeout for 'night mode'.

Parameter	Description
personal_settings/lcd_night_mode_brightness_medium	Configures the MEDIUM level of brightness when the screen is in 'night mode'. Minimum: 0. Maximum: 31. Default: 10. There is no timeout for 'night mode'.

6.7 C450HD Screen Saver Configuration

The C450HD phone features a screen saver displaying a digital clock. The feature allows future customization of the phone. By default, the feature is enabled, but the network administrator can disable it on request or change its timeout.

- Use the table below as reference.

Table 6-15: Disabling the C450HD IP Phone Screen Saver

Parameter Name	Description
personal_settings/ScreenSaverEnabled	Enables / disables the C450HD phone screen saver. ▪ Disable ▪ Enable (default)
personal_settings/ScreenSaverAwakeTimeout	The timeout of the screen saver is triggered after 300 seconds by default but it can be configured to 0-600 seconds using this parameter.

6.8 Configuring Personal Settings

6.8.1 Configuring Language

The language displayed in the phone screen can be configured using the configuration file.

➢ **To choose a language using the configuration file:**

- Use the table below as reference.

Table 6-16: Language Display

Parameter	Description
personal_settings/language	Determines the phone screen language. ▪ [English] English (default) ▪ [Spanish] Spanish ▪ [Russian] Russian ▪ [Portuguese] Portuguese ▪ [German] German ▪ [Ukraine] Ukrainian ▪ [French] French ▪ [Italian] Italian ▪ [Hebrew] Hebrew ▪ [Polish] Polish ▪ [Korean] Korean ▪ [Finnish] Suom alainen ▪ [Chinese] Chinese Simplified ▪ [Chinese] Chinese Traditional ▪ [Magyar] Hungarian ▪ [Japanese] Japanese ▪ Slovak ▪ Czech ▪ Dutch

This page is intentionally left blank.

7 Configuring Security

7.1 Implementing X.509 Authentication

X.509 certificates can be used to authenticate a connection with a remote server or HTTP/S client browser. The certificates may be implemented in one of or a combination of the following SSL handshake negotiation scenarios:

- The phone is a client who needs to authenticate the remote server e.g. provisioning server to which it is attempting to connect.

  In this case, the phone needs to load the certificate and Trusted CA used by the remote server.
- The remote server needs to authenticate the incoming connection request from the phone client.

  In this case, the remote server needs to load the certificate and Trusted CA used by the phone.
- The phone is a server who needs to authenticate an incoming connection request from a remote HTTP client browser.

  In this case, the phone needs to load the certificate and Trusted CA used by the remote HTTP client browser.
- The remote HTTP client browser needs to authenticate the phone to which it is attempting to connect.

  In this case, the remote HTTP client browser needs to load the certificate and Trusted CA used by the phone.

The following types of certificates can be used to authenticate the connections described in the above scenarios:

- **Factory-set Certificates** (see Section 7.1.1):

  Certificates that are loaded to the AudioCodes IP Phone using an AudioCodes certificate and AudioCodes Trusted Root CA.
- **User-Generated Certificates** (see Section 7.1.2):

  Certificates that are generated by the user that may use the AudioCodes Tusted Root CA or an external CA.

7.1.1 Factory-Set Certificates and AudioCodes Trusted Root CA

AudioCodes IP phones are loaded with factory-set preinstalled certificate files: private key file, certificate file and a Trusted Root CA file that is signed by AudioCodes (including DIGICert).

Note:

- The phone's screen visually indicates that factory certificates are installed.
  - √ The Release Information menu (**MENU** button > **Status**) displays the 'Device Certificate' parameter.
  - √ The values of the 'Device Certificate' parameter can be **Installed**, **Self-Signed**, or **Not Installed**.

Whenever the phone authenticates with a remote server, it can be authenticated using these certificate files. Each phone receives a uniquely generated private key certificate file based on its MAC address.

Note:

- If the remote server is configured to authenticate the client and AudioCodes factory-set certificates are used for authentication, then the AudioCodes Certificate and AudioCodes Trusted Root CA must be downloaded to the remote server. These files can be downloaded from the AudioCodes Web site. For more information, contact your local AudioCodes sales representative.
- If you use the AudioCodes Redirect server to obtain firmware and configuration files, then the factory-set certificates are used to authenticate the connection with this server.

7.1.2 User-Generated Certificates

If an organizational certificate Infrastructure (PKI) is used, you may wish to instead use certificates provided by your security administrator. You can define up to five additional user-generated certificates, which can be configured to secure different types of connections and paired with external Trusted Root CAs. The following remote server connection types can be configured with user-generated certificates:

- 802.1x RADIUS server
- SIP TLS server
- HTTP/S Provisioning server

When user-generated certificates are loaded to the device to authenticate a specific connection type, then this certificate is used to secure the connection with the assigned connection type. For example, if you load Certificate A for connecting to an HTTPS Provisioning server, then whenever there is an attempt by the phone to connect to a Provisioning server, then the connection is authenticated using Certificate A.

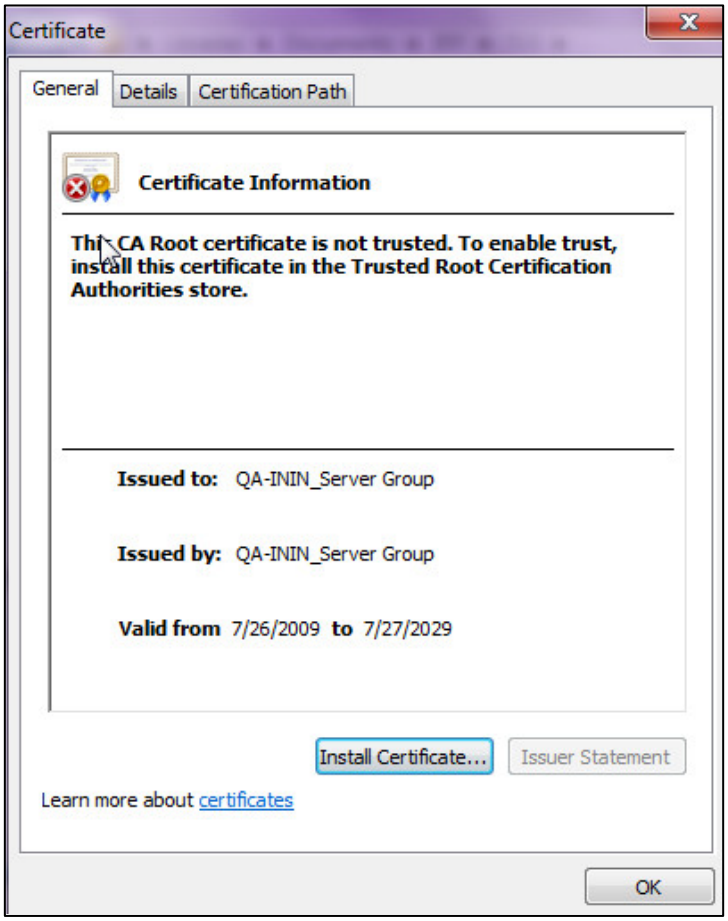
Note:

- You can load one certificate for each connection type.
- If you do not load a certificate to support a specific connection type, then the factory-set certificate is used to authenticate the connection. For example if you load user-generated certificates to support Automatic Updates (Provisioning server) and SIP TLS server connections, and there is an attempt by the phone to connect to a RADIUS server, then this connection is authenticated using the AudioCodes factory-set installed certificate.
- You can use the AudioCodes Trusted Root CA with a user-generated certificate.
- You can use the same certificate for different server connection types.

7.1.3 External Trusted Root CAs

The Certificate Authority is a body that certifies ownership of a certificate by the name subject of the certificate.

Figure 7-1: Certificate



You can define up to five external Trusted Root CAs, which may be configured to secure different types of connections and paired with the loaded user-generated certificates (see Section 7.1.2).

Note: If you do not load any Trusted Root CAs to the phone, then when there is an attempt to connect to a remote server or an attempt by a browser to open the Web interface using HTTPS, the AudioCodes Trusted Root CA is used to authenticate the connection.

7.1.3.1 Supported Trusted Root CAs

Following are the Trusted Root CAs supported by AudioCodes phones:

- CNNIC_ROOT.cer
- COMODO Root CA
- Comodo_AAA_Certificate_Services
- Comodo_AddTrust_External_CA_Root
- COMODO_Root_CA

- Cybetrust_Baltimore_CyberTrust_Root
- Cybetrust_GlobalSign_Root_CA
- Cybetrust_GTE_CyberTrust_Global_Root
- DigiCert_Cloud_Services_CA-1
- DigiCert_High_Assurance_EV_Root_CA
- DigiCertGlobalRootCA
- DigiCertSHA2SecureServerCA
- DST_Root_CA_X3
- D-Trust_Root_Class_3_CA_2_2009
- D-TRUST_Root_Class_3_CA_2_EV_2009
- Entrust_Entrust.net_Certification_Authority_2048
- Entrust_Root_Certification_Authority_G2
- GeoTrust_GeoTrust_Global_CA
- GeoTrustEVRSACA2018
- GlobalSign
- Go_Daddy_Go_Daddy_Class_2_Certification_Authority
- Go_Daddy_Starfield_Class_2_Certification_Authority
- isrgrootx1.pem
- letsencryptauthorityx3
- StartCom_Certification_Authority
- thawte_Primary_Root_CA_G3
- VeriSign_Class_2_Public_Primary_Certification_Authority
- VeriSign_Class_3_Public_Primary_Certification_Authority
- VeriSign_Class_3_Public_Primary_Certification_Authority_G1
- VeriSign_Class_3_Public_Primary_Certification_Authority_G2
- VeriSign_Class_3_Public_Primary_Certification_Authority_G3
- VeriSign_Class_3_Public_Primary_Certification_Authority_G5
- VeriSign_Thawte_Premium_Server_CA
- VeriSign_Thawte_Server_CA

7.2 Loading a Certificate

The network administrator can:

- Load the Trusted Root CA Certificate to the Phone (see below).
- Load the Client Certificate to the Phone (see Section 7.2.2).
- Generate a Certificate Signing Request (CSR) (see Section 7.2.3).

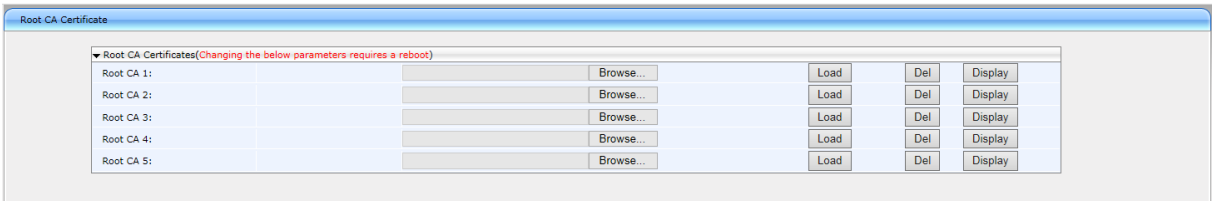
7.2.1 Loading the Trusted Root CA Certificate to the Phone

The network administrator can load the Trusted Root CA certificate to the phone.

➢ **To load the trusted root CA certificate to the phone:**

1. Open the Root CA Certificate page (**Configuration** > **Security** > **Root CA Certificate**).

Figure 7-2: Root CA Certificate



2. Click **Browse** to navigate to the certificate file, and then click the **Load** button to upload it to the phone.

   You can load a maximum of five certificates to the phone. Click the **Del** button to delete a load if necessary. Click the **Display** button to display the certificate if you wish to view it.

7.2.1.1 Loading Trusted Root CA Certificate Using Configuration File

The network administrator can load a Trusted Root CA certificate.

Note: Using this method, Trusted Root CA certificates files are loaded to the phone when it is powered up.

➢ **To load a Trusted Root CA certificate file:**

- Use the table as reference.

Table 7-1: Root CA Certificate Parameters

Parameter	Description
security/ca_certificate/0/uri	The first root CA certificate loaded to the phone.
security/ca_certificate/1/uri	The second root CA certificate loaded to the phone.
security/ca_certificate/2/uri	The third root CA certificate loaded to the phone.
security/ca_certificate/3/uri	The fourth root CA certificate loaded to the phone.
security/ca_certificate/4/uri	The fifth root CA certificate loaded to the phone.

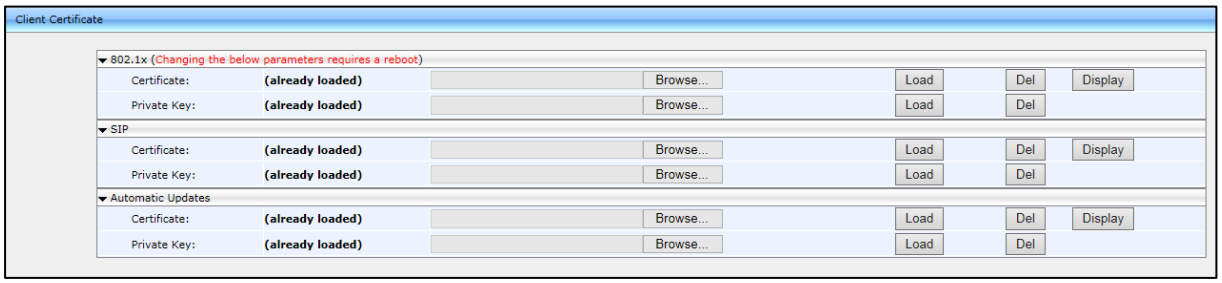
7.2.2 Loading the Client Certificate to the Phone

The section shows how to load the Client Certificate to the phone.

➢ **To load the Client Certificate to the phone:**

1. Open the Client Certificate page (**Configuration** > **Security** > **Client Certificate**).

Figure 7-3: Client Certificate



7.2.2.1 Loading the Client Certificate to a Phone

The Client Certificate file can be loaded to the phone.

Note: Using this method, client certificates files are loaded to the phone when it is powered up.

➢ **To load a client certificate file:**

- Use the table as reference.

Table 7-2: Client Certificate Parameters

Parameter	Description
security/sip_certificate_uri	Downloads from this URI to the phone a Client Certificate for SIP TLS (SIP calls with Transport Layer Security).
security/sip_private_key_uri	Downloads from this URI to the phone a Client Private Key for SIP TLS (SIP calls with Transport Layer Security).
security/ieee802_1x_certificate_uri	Downloads from this URI to the phone a Client Certificate for 802.1X Authentication.
security/ieee802_1x_private_key_uri	Downloads from this URI to the phone a Client Private Key for 802.1X authentication.
security/autoupdate_certificate_uri	Downloads from this URI to the phone an external certificate that is used to secure the connection with the automatic provisioning server.
security/autoupdate_private_key_uri	Downloads from this URI to the phone a private key that is used to secure the connection with the automatic provisioning server.

7.2.2.2 Enabling Server-side Authentication (Mutual Authentication)

You can enable server-side authentication of a connection with the RADIUS and Provisioning server.

Note: OpenSSL 1.0.2p is supported. This open source version supports SHA2 algorithms.

Table 7-3: Server-side Authentication

Parameter	Description
security/ieee802_1x/verify_server_certificate	Configures the phone to verify received server certificates over a secure EAP-TLS connection.
security/provisioning/verify_server_certificate	Configures the phone to verify received server certificates over a secure HTTPS connection with a provisioning server.

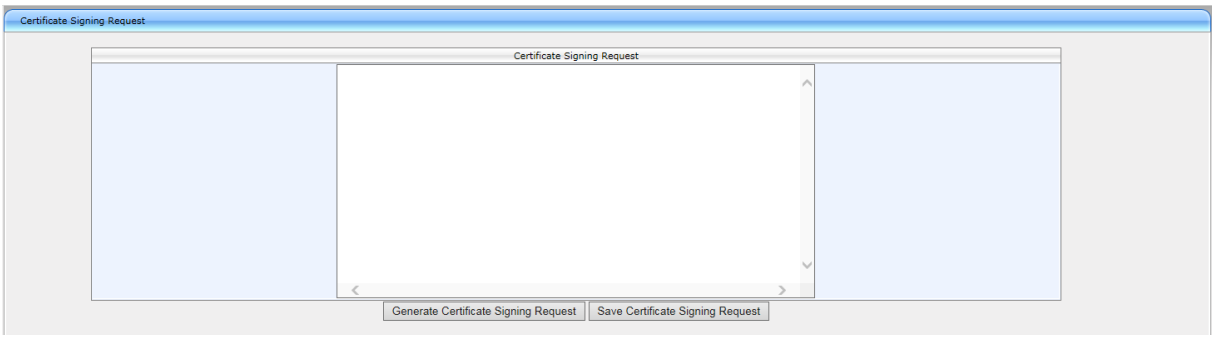
7.2.3 Generating a Certificate Signing Request

The section shows how to generate a certificate signing request (CSR) to send to the Certifcate Authority (CA) for the CA to sign the Client Certificate.

➢ **To generate a CSR:**

1. Open the Certificate Signing Request page (**Configuration** > **Security** > **Certificate Signing Request**).

Figure 7-4: Certificate Signing Request



2. Press the **Generate Certificate Signing Request** button; the phone creates a CSR file.
3. Press the **Save Certificate Signing Request** button and download the CSR file to your PC.
4. Send the CSR file to the Certificate Authority to sign the Client Certificate.
5. You can load the Client Certificate to the phone for 802.1X Authentication or SIP TLS.

7.2.4 Using Previously Loaded Certificates

If you have upgraded to this version and your phones have pre-installed certificates, then the CA configuration parameter values from previous versions are translated to version 2.2.2 parameter values as described below.

Note: It is **highly recommended** to change the CA configuration by using the methods described in the above sections.

- Certificate file settings for versions prior to version 2.2.2:

```
security/ca_certificate_uri= xxx
security/certificate_uri=zzz
security/private_key_uri=yyy
```

where:

xxx is the uri of the root CA

zzz is the uri of the certificate file

yyy is the uri of the private key file

- Certificate file settings translated to version 2.2.2:

```
security/autoupdate_certificate_uri=zzz
security/autoupdate_private_key_uri= yyy
security/ca_certificate/0/uri=xxx
security/ca_certificate/1/uri=
security/ca_certificate/2/uri=
security/ca_certificate/3/uri=
security/ca_certificate/4/uri=
security/ieee802_1x_certificate_uri=zzz
security/ieee802_1x_private_key_uri= yyy
security/sip_certificate_uri= zzz
security/sip_private_key_uri= yyy
```

Note: The CA configuration parameters prior to version 2.2.2 are no longer used on the phone.

7.3 Configuring SIP TLS

This section shows how to manage Transport Layer Security (TLS) and certificates. TLS is a cryptographic protocol which provides communication security over the transport layer (TCP). TLS is used to secure the phone's SIP signaling connections. Typically, TLS protocol uses Private and Public keys for authentication. A Certification Authority (CA) performs authentication. Full protocol specification is updated in RFC 5246.

Note: Before you can connect to a TLS server, you need to make sure the same certificate and Trusted Root CA are loaded to the phone *and* to the TLS server.

➢ **To configure TLS for the phone-server SIP connection:**

- Use the table as reference.

Table 7-4: SIP-over-TLS Parameters

Parameter	Description
voip/signalling/sip/transport_protocol	Specifies the SIP Transport protocol. • If using the 'sip' prefix, set to 'TLS' • If using the 'sips' prefix, set to 'TCP'
voip/signalling/sip/tls_port	Defines the local TLS SIP port for SIP messages. Range:1024 - 65535. Default:5061.
voip/signalling/sip/enable_sips	If signaling protocol is set to TCP and we want to activate TLS, this parameter should be enabled. In this case we will use 'sips' prefix instead of “sip:”

7.3.1 Server Certificate Validation for Secured HTTPS Communications over SSL

This feature decreases vulnerability to breaches of security. If validation fails after installing phone firmware, the SIP TLS application impacted.

The certificate is verified in two steps:

- The Root CA is installed using provisioning.
- The server’s hostname is validated; for each certificate in the chain, the ‘issuer’ field in the certificate must match the ‘subject’ field of the issuer (uppermost in the chain) certificate.

➢ **To configure the feature using the Configuration File:**

- Use the table as reference.

Table 7-5: Server Certificate Validation for Secured HTTPS Communications over SSL

Parameter Name	Description
[security/SSLCertificateErrorsMode]	• **Disallow** (default) = TLS connection will be rejected and the phone will not communicate with the server. • **Ignore** = Allows backward compatibility though vulnerability will increase; the phone will proceed without checking the received certificates and without any notifications.

7.4 Configuring 802.1x

802.1X is an IEEE Standard for Port-based Network Access Control (PNAC). It's part of the IEEE 802.1 group of networking protocols. It provides an authentication mechanism for devices wishing to connect to a LAN or WLAN.

The employee's PC negotiates 802.1X. Messages are sent transparent to the enterprise switch. The phone is uninvolved in the negotiation; however, if an employee's PC is disconnected, their phone notifies the switch. If an employee's PC is disconnected from the phone, a PROXY-EAP-LOGOFF mechanism lets the phone immediately log off the port from the authentication server to prevent anyone else from connecting to it.

The phone performs like this:

- Phone and PC connected to phone's PC port successfully perform 802.1X authentication. The authentication server records the phone and PC as authorized.
- If the PC is disconnected from the phone's PC port, the phone sends an EAPoL-Logoff message for the PC. The authentication server then records the PC as unauthorized.
- If the PC reconnects to the phone's PC port, the authentication server requests the PC to perform 802.1X authentication again.

Note: Before you can connect to a 802.1x server, you need to make sure the same certificate and Trusted Root CA are loaded to the phone *and* to the 802.1x.

7.4.1 Configuring 802.1x in the Phone Screen

The network administrator can configure 802.1x in the phone screen.

➢ **To configure 802.1x in the phone screen:**

1. On the phone, open the 802.1x Settings screen (MENU key > **Administration** > **Network Settings** > **802.1xSettings**).
2. Navigate to and select either:
   - Disabled – disables the 802.1x feature
   - EAP-MD5 – see Section 7.4.1.1
   - EAP-TLS - see Section 7.4.1.2

7.4.1.1 Configuring EAP-MD5 Mode

EAP-MD5 mode can be configured for 802.1x using the phone's screen.

➢ **To configure EAP-MD5 mode for 802.1x using the phone's screen:**

1. Navigate to the **EAP-MD5** option and then press **Select** and **Edit**:
2. Enter the following information:
   - **Identity:** User ID
   - **Password:** MD5 password (optional)
3. Press the **Save** softkey; a message appears notifying you that the phone will restart.
4. Press **Apply**.

7.4.1.2 Configuring EAP-TLS Mode

EAP-TLS mode can be configured for 802.1x using the phone's screen.

➢ **To configure EAP-TLS mode for 802.1x using the phone's screen:**

1. Navigate to the **EAP-TLS** option and press **Select**
2. Press the **Save** softkey; a message appears notifying you that the phone will restart.
3. Press **Apply**.

➢ **To configure EAP TLS using the Configuration File:**

- Open the Configuration File page (**Management** tab > **Manual Update** > **Configuration File**) and configure the parameters using the table below as reference.

Table 7-6: EAP TLS Parameters

Parameter	Description
EAP Type **[/network/lan/_802_1x/eap_type]**	Sets 802.1X EAP mode. [Disable] = Disables the use of 802.1X [EAP_TLS]= Authentication is implemented by Certificate, Client Certificate, and Client Private Key.
network/lan/_802_1x/eap_identity	User ID for EAP-TLS mode

Note: Make sure the Root CA certificate and the Private Key certificate are installed on the RADIUS server as well.

7.4.2 Configuring 802.1x

802.1x can be configured.

7.4.2.1 Configuring EAP MD5 Mode

802.1x settings can be configured for EAP-MD5.

➢ **To configure 802.1x settings for EAP-MD5:**

- Use the table as reference.

Table 7-7: EAP MD5 Parameters

Parameter	Description
network/lan/_802_1x/eap_type	Sets 802.1x Extensible Authentication Protocol mode: ▪ **Disable** = Disables the use of 802.1x ▪ **EAP_MD5** = Authentication is implemented by user name and password (Password is optional). ▪ **EAP_TLS** = Authentication is implemented by Certificate, Client Certificate and Client Private Key.
network/lan/_802_1x/md5_identity	User ID for md5 mode.
network/lan/_802_1x/md5_password	Password for md5 mode. (Leave blank if no password).

7.5 Configuring SRTP

Secure Real-time Transport Protocol (SRTP) is a protocol that allows encryption for RTP data. Since the RTP encryption key is delivered via SIP, this feature is relevant only when SIP transport is secured, so when using this feature you also need to use SIP over TLS.

SRTP can be configured.

➢ **To configure SRTP:**

- Use the table as reference.

Table 7-8: SRTP Parameters

Parameter	Description
voip/media/srtp/mode	▪ Three encryption levels are supported: ▪ **DoNotSupportEncryption** (Default) SRTP is disabled ▪ **SupportEncryption** Negotiation ▪ **RequireEncryption** SRTP is enabled; both sides must support encryption ▪ **Note regarding backward compatibility:** This configuration file parameter replaced the legacy **voip/media/srtp/enabled** configuration file parameter. ▪ The configuration file parameter **voip/media/srtp/enabled=1** in previous releases is compatible with the configuration file parameter **voip/media/srtp/mode=REQUIRE_ENCRYPTION** in this release

Parameter	Description
voip/media/srtp/negotiation/mode	▪ If **voip/media/srtp/mode**=**SUPPORT_ENCRYPTION**, two SRTP negotiation modes are supported: ▪ **Basic** (default) RTP/SRTP negotiation according to the document *IMTC Best Practices for SIP Security*. This mode is supported by Broadsoft, Microsoft and many other vendors ▪ **RFC5939** RTP/SRTP capability negotiation using the attributes "a=tcap", "a=acap" and "a=pcfg" as described in RFC 5939
voip/media/srtp/method	The SRTP encryption method. ▪ **AES_CM_128_HMAC_SHA1_32** (default) ▪ **AES_CM_128_HMAC_SHA1_80** ▪ **AES_CM_128_ALL_METHODS**
voip/media/srtp/use_MKI	Defines the usage of the SRTP Master Key Index. ▪ **0** = MKI is not used (default) ▪ **1** = MKI is used
voip/media/srtp/MKI_length	Defines the maximum length of the SRTP Master Key Index. Range: 1 - 4. Default: 1.
voip/media/srtp/use_lifetime	Allows the removal of the 'lifetime' parameter from the SRTP Crypto line in SDP. According to RFC 4568, an optional 'lifetime' parameter such as "2^31" must be added to the a=crypto line. This parameter allows the removal of the lifetime in all phone crypto lines in SDP. Configurable parameter values are: ▪ **0** = the lifetime is removed ▪ **1** = the lifetime is retained (default)
voip/media/srtp/RTCP_encrypt_enabled	Default: **1**. If set to **0**, **UnencryptedSRTCP** will present at the end of the "a=crypto" line in the SDP offer, for example: a=crypto:1 AES_CM_128_HMAC_SHA1_32 inline:rcO4NFj0PcKk3Pbo7IVhVqpCpQI3MWytScjRL1IS|2^31 UNENCRYPTED_SRTCP
voip/media/srtp/RTP_encrypt_enabled	Default: **1**. If set to **0**, **UnencryptedSRTP** will present at the end of the "a=crypto" line in the SDP offer, for example: a=crypto:1 AES_CM_128_HMAC_SHA1_32 inline:rcO4NFj0PcKk3Pbo7IVhVqpCpQI3MWytScjRL1IS|2^31 UNENCRYPTED_SRTP
voip/media/srtp/RTP_auth_enabled	Default: **1**. If set to **0**, **UnauthenticatedSRTP** will present at the end of the "a=crypto" line in the SDP offer, for example: a=crypto:1 AES_CM_128_HMAC_SHA1_32 inline:TDejshzv6Y04By7Add2KuZaJ9YrvteWSENcpBMZ4|2^31 UNAUTHENTICATED_SRTP

7.6 Configuring HTTP/S Login

Note: Support pending.

HTTP/S login authentication can be configured to secure the connection between the phones and a provisioning server, such as the BroadWorks Device Management Provisioning server. Once the connection is secure, software and/or configuration files can be downloaded to the phone.

HTTP/S authentication is supporting using the following methods (configured on the remote server):

- **Basic** – (RFC 2617) username and password are sent in plain text over plain HTTP over the network.
- **Digest** – a hash function is applied to the password before sending it over the network, therefore it is more secure as usernames and passwords are encrypted

Note:

- The enterprise requires an HTTP/S server to support this feature.
- The authentication method is configured on the remote side e.g. Provisioning server.

7.7 Logging into a Remote HTTP/S Server from the Phone

Note: Support pending.

During automatic provisioning, the phone can optionally prompt the user to enter the login credentials (username and password) of the provisioning server.

The prompt occurs during the server's authentication process, when it is recognized that an HTTP username and/or password has not been specified, or that these credentials are incorrect.

If so, and if the prompt feature is enabled, the 'Prov. Credentials' screen pops up, prompting the user to enter or reenter these login credentials.

➢ **To configure HTTP/S login authentication in the configuration file:**

- Use the table as reference:

Table 7-9: HTTP/S Login Authentication

Parameter	Description
provisioning/configuration/http_auth/ ui_interaction_enabled	Enables the user to be prompted to enter the HTTP username and password on the phone during the automatic provisioning process whenever the login credentials to the provisioning server have not been entered or are incorrect. **0** = (default) The phone's Settings menu's **Prov. Credentials** option is not available on the phone and therefore the user cannot interactively enter the HTTP password and username. In this case, you must enter values for the HTTP username and password in the configuration file, as specified below. **1** = The user can be prompted to enter the HTTP username and password interactively. Whenever this value is configured and the phone attempts to connect to a remote server, then the user is prompted to enter or reenter these credentials. In addition, the user can manually go the Settings menu option **Prov. Credentials** to enter their username and password. When this value is enabled, then it is *highly recommended* to remove the HTTP password and username entries from the configuration file: ▪ provisioning/configuration/http_auth/password ▪ provisioning/configuration/http_auth/user_name
provisioning/configuration/http_auth/ user_name	Defines a username required by the HTTP/S server for logging in with authentication.
provisioning/configuration/http_auth/ password	Defines a password required by the HTTP/S server for logging in with authentication.

7.8 MAC-Based Authentication

Note: Support pending.

The network administrator can configure MAC-based authentication.

➢ **To configure MAC-based authentication:**

- Use the table as reference:

Table 7-10: Authentication

Parameter	Description
provisioning/configuration/mac_address_in_header	Enables MAC-based authentication. **0** = (default) Don't insert the phone's MAC address in the header. **1** = Insert the phone's MAC address in the header.

This page is intentionally left blank.

8 Maintaining an IP Telephony Network

This section shows how to upgrade the phone firmware, perform administration tasks, and enable remote management.

8.1 Changing Administrator Login Credentials

Network administrators can change the administrator phone's login user name and password. This is the login required to access the Administration menu on the phone. The default administrator user name and password is **admin** and **1234** respectively. Administrator Login Credentials can be changed.

➢ **To change the login username and password:**

- Use the table as reference.

Table 8-1: Username and Password Parameters

Parameter	Description
system/user_name	The name of the phone user defined as Administrator. The default value is **admin**.
system/password	The password of the phone user defined as Administrator is by default encrypted. The default value is **1234**. To regenerate an encrypted password, see Section 2.2.4.2.

8.2 Administration

8.2.1 Managing Users

Network administrators can change the phone's login user name and password. This is the login required to access the **Administration** menu in the phone's screen.

Note:

- For the Administrator account, the default 'Username' and 'Password' is **admin** and **1234** respectively. It's advisable for the network administrator to change it to prevent unauthorized access.
- For the User account, the default 'Username' and 'Password' is **user** and **1234** respectively.

➢ **To change the login username and password:**

- Use the tables below as reference.

Table 8-2: Administrator account - Username and Password

Parameter	Description
Note: To add a value to these parameters, enter **system/** followed by the parameter name, equal sign and then the value (e.g. `system/user_name=admin`).	
system/user_name	The phone user name. The default value is admin.
system/password	The encrypted phone password. The default value is 1234.

8.2.2 Allowing / Disallowing Management via the Web Interface

Network administrators can allow / disallow management via the phone's Web interface without requiring a phone reboot. The configuration file parameter 'system/web/enabled' supports the feature.

- **0** disallows management via the phone's Web interface
- **1** (default) allows management via the phone's Web interface

8.3 Restoring Phone Defaults

Phone default settings can be restored from the phone's screen.

8.3.1 Restoring Factory Defaults from the Phone's Screen

Factory defaults can be restored from the phone's screen.

➢ **To restore the phone to default settings:**

1. On the phone, open the Restore Defaults screen (MENU key > **Administration** > **Restore Defaults**).
2. Press the **Select** softkey; a warning message appears requesting you to confirm:
3. Press the **Yes** softkey to confirm reset to defaults or **No** to cancel.

Note: You can restore the phone's settings to their defaults without needing access to the 'Administration' menu.

To restore the phone's settings to their defaults if necessary:

1. Long-press the **OK** and MENU keys simultaneously and while pressed, unplug the power cable.
2. Plug the power cable back into the phone and continue to press the OK + MENU keys for +-5 seconds as the boot process starts after connecting the power supply.
3. Release the **OK** + MENU keys; the phone' settings are restored to their defaults.

8.4 Restarting the Phone

The phone can be restarted from the phone screen.

➢ **To restart the phone from the phone:**

1. On the phone, select the **Restart** option. Either:
   a. MENU key > **Administration** > **Restart**)
   -or-
   b. MENU key > **Settings** > **Restart**

   Here's the Administration screen's **Restart** option:

   A warning message appears requesting you to confirm: **Restart phone?**
2. Press the **Yes** softkey to confirm the restart or **No** to cancel.

8.5 Enabling Remote Management

8.5.1 Enabling Telnet Access

Telnet access can be enabled using the configuration file.

Note: Opening a Telnet connection in an external network is strongly inadvisable due to the widely recognized vulnerability of the protocol.

➢ **To configure Telnet:**

- Use the table as reference.

Table 8-3: Telnet Parameters

Parameter	Description
Note: To add a value to these parameters, enter **management/** followed by the parameter name, equal sign and then the value (e.g. `management/telnet/enabled`=0).	
management/telnet/enabled	Enables telnet access to the phone. ▪ **0** Disable (default) ▪ **1** Enable The user name and password for telnet access are according to the parameters: **system/user_name** and **system/password**.

8.5.2 Enabling SSH Access

Secure Shell (SSH) protocol can be configured for secure remote login to the 450HD, C450HD and 445HD phones and the HRS. Network administrators can use configuration file parameter 'management/ssh/enabled' to enable the feature (by default, it is set to **0**, i.e., disabled).

9 Monitoring the Network

9.1 Determining Network Status

Network statuses such as LAN status, port mode status, 802.1X status, VoIP status, etc., can be determined using the Web interface, for debugging purposes.

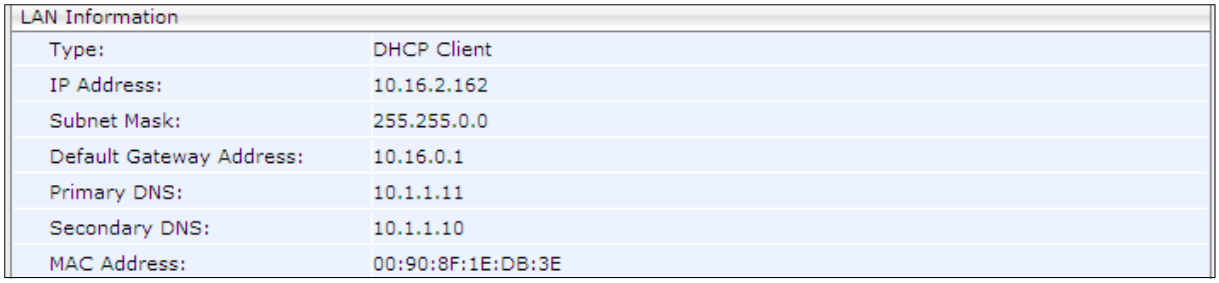
9.1.1 Determining LAN Status

Monitoring the status of the Local Area Network (LAN) provides network administrators with visibility into the telephony devices in the LAN and alerts them to issues.

➢ **To determine LAN status information:**

- Open the Network Status page (**Status & Diagnostics** > **System Status** > **Network Status**).

Figure 9-1: LAN Information



LAN Information	
Type:	DHCP Client
IP Address:	10.16.2.162
Subnet Mask:	255.255.0.0
Default Gateway Address:	10.16.0.1
Primary DNS:	10.1.1.11
Secondary DNS:	10.1.1.10
MAC Address:	00:90:8F:1E:DB:3E

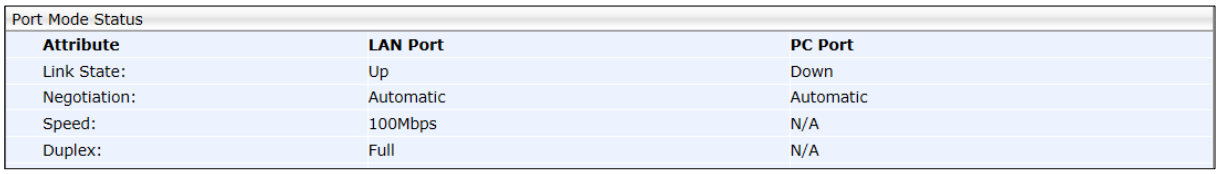
9.1.2 Determining Port Mode Status

The status of the Port Mode and connectivity can be checked using the Web interface.

➢ **To determine Port Mode status:**

- Open the Network Status page (**Status & Diagnostics** > **System Status** > **Network Status**).

Figure 9-2: Port Mode Status



Port Mode Status		
Attribute	**LAN Port**	**PC Port**
Link State:	Up	Down
Negotiation:	Automatic	Automatic
Speed:	100Mbps	N/A
Duplex:	Full	N/A

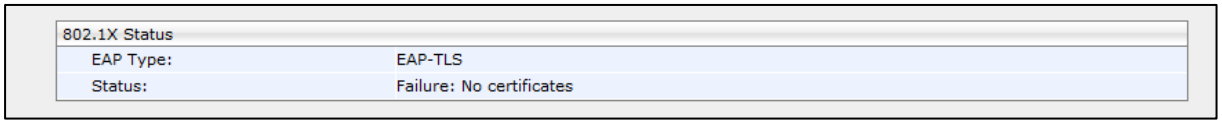
9.1.3 Determining 802.1x Status

802.1x status can be monitored using the Web interface to validate successful 802.1X authentication.

➢ **To determine 802.1x status:**

- Open the Network Status page (**Status & Diagnostics** > **System Status** > **Network Status**).

Figure 9-3: 802.1X Status



9.2 Determining VoIP Status

Network administrators can view VoIP status using the Web interface to determine connection quality in the network.

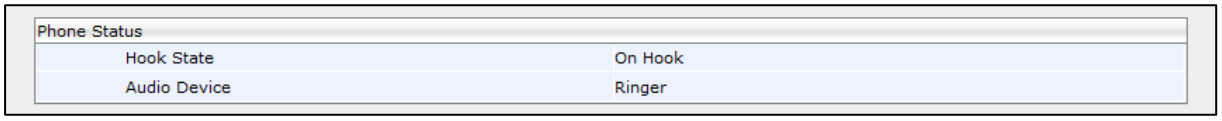
9.2.1 Determining Phone Status

Administrators can view for example if the state of the phone is on-hooked or off-hooked.

➢ **To determine phone status:**

- Open the VoIP Status page (**Status & Diagnostics** > **System Status** > **VoIP Status**).

Figure 9-4: VoIP Status - Phone Status



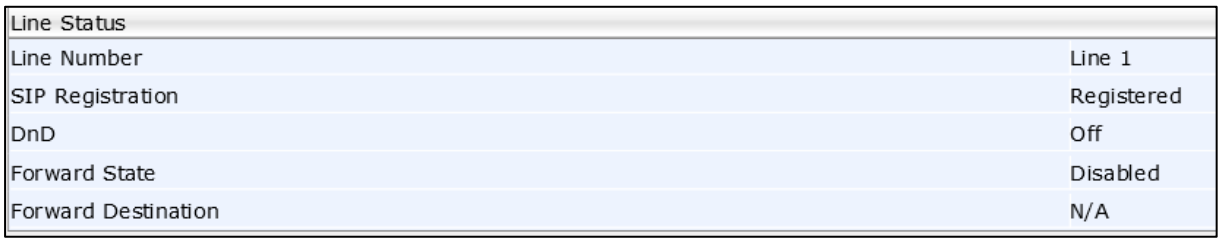
9.2.2 Viewing Line Status

Network administrators can view the line status, i.e., the line number, whether the line is SIP-registered, the IP address of the SIP Registration Server, whether DnD is on, whether mute is on, and whether forwarding is enabled.

➢ **To determine line status:**

- Open the Network Status page (**Status & Diagnostics** > **System Status** > **VoIP Status**).

Figure 9-5: Line Status



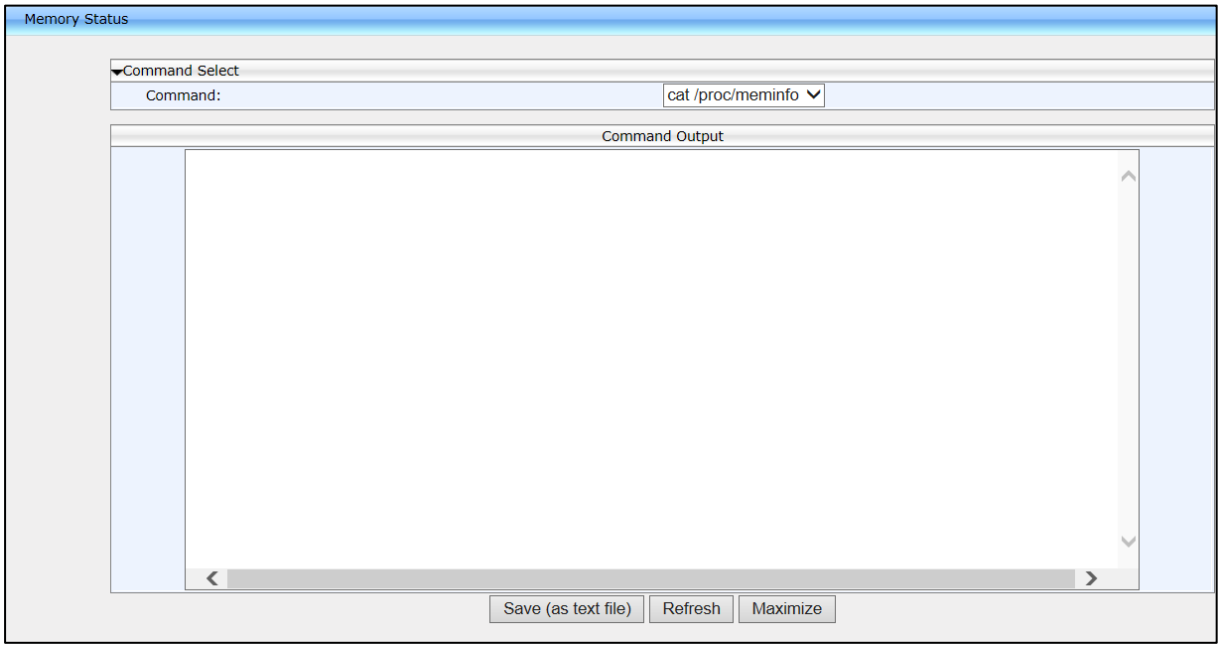
9.2.3 Determining Memory Status

The network administrator can determine the device's memory status in real time, using the three Linux commands that are most frequently used to obtain data related to a device's memory state.

➢ **To determine memory status:**

1. Open the Memory Status page (**Status & Diagnostics** > **System Status** > **Memory Status**).

Figure 9-6: Memory Status



2. From the dropdown list select a Linux command from the three available:
   - **meminfo**
   - **ps**
   - **top**

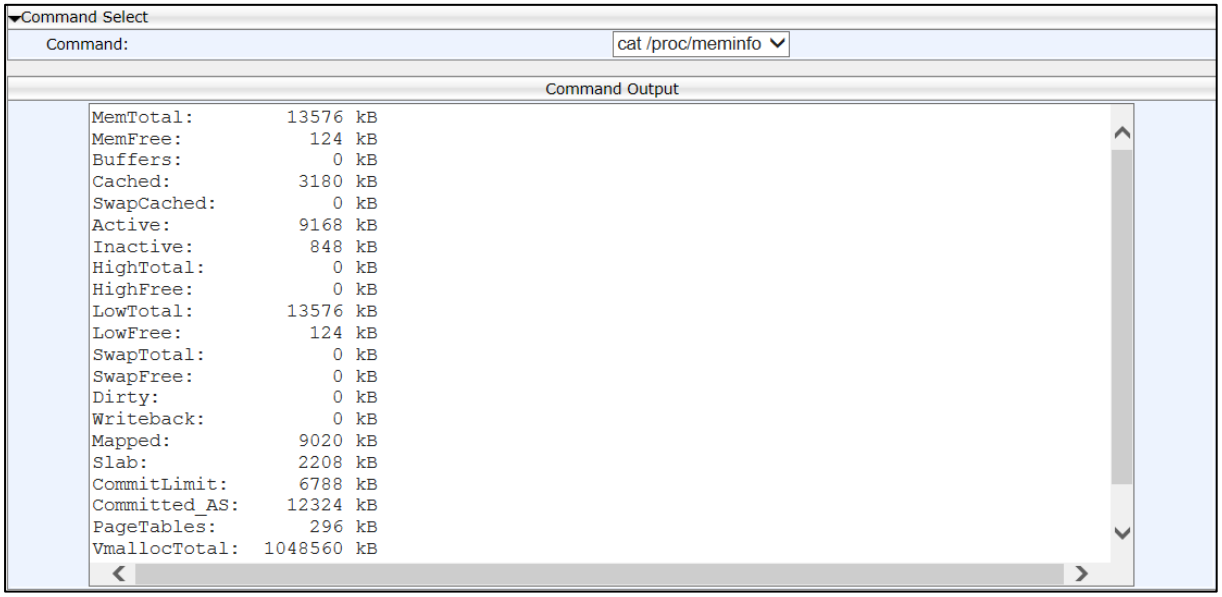
   Use the table as reference.

Table 9-1: Memory Status – Linux Commands

Linux Command	Description
Meminfo	Provides you a snapshot of memory usage on the device.
ps	Provides you a snapshot of the current processes running on the device's CPU.
top	Provides you an ongoing look at processor activity in real time. Displays a listing of the most CPU-intensive tasks on the system.

3. Click **Refresh**; the information requested is displayed.

Figure 9-7: Memory Status – Linux meminfo Command – Displayed Information



4. Click **Save (as text file)** (optional); the information provided by the Linux command is saved to a txt file. You can use the file to make sure all data is stored correctly in memory and to diagnose possible issues such as voice quality, jitter, or memory leakage.
5. Click **Maximize** (optional); the information pane is maximized for an optimal viewing experience.

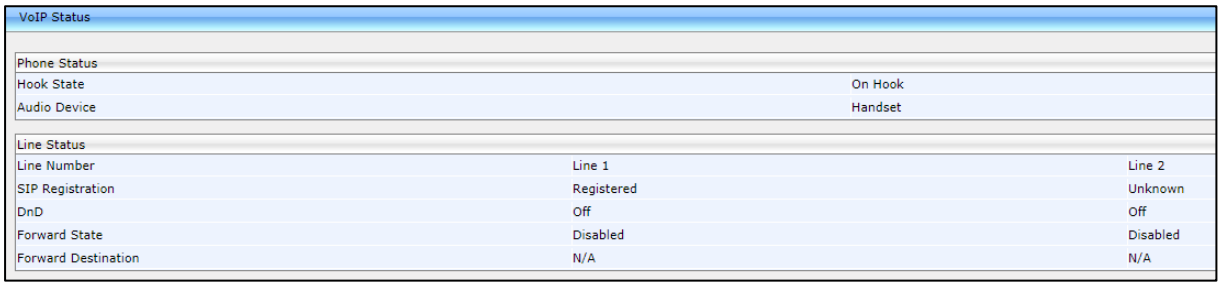
9.2.4 Viewing Information about a Currently Established Call

The Web interface displays information about a *currently established call*.

➢ **To view current call information:**

- Open the Network Status page (**Status & Diagnostics** > **System Status** > **VoIP Status**):

Figure 9-8: Web Interface –Line 1 Call Information



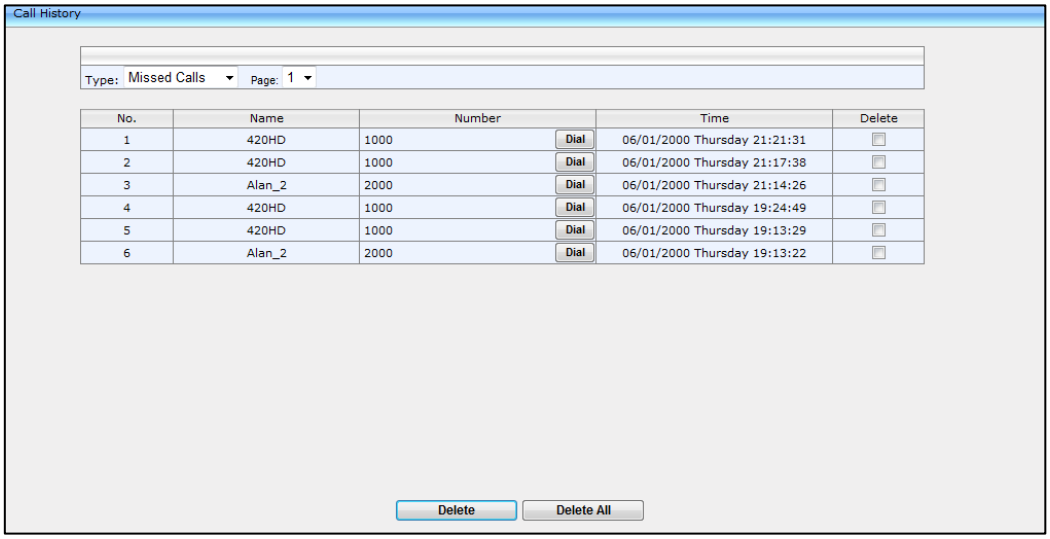
9.3 Viewing Call History

The network administrator can view a list of received calls and a list of missed calls, dialed numbers and call duration.

➢ **To view call history:**

1. Open the Call History page (**Status & Diagnostics** > **History** > **Call History**).

Figure 9-9: Call History



2. From the 'Type' drop-down list, select the type of call history (i.e., missed calls, received calls, and dialed numbers) that you want to view; the table lists the call history according to the chosen call history type.
3. You can delete a logged call history entry, by selecting the 'Delete' check box corresponding to the entry that you want to delete, and then clicking the **Delete** button.

9.4 Accessing System Information

9.5 Monitoring Quality of Experience

Network administrators can configure the phone to send Quality of Experience reports to a QoE collecting server, such as the AudioCodes SEM server. This mechanism is implemented using RTCP-XR (RTCP Extended Reports). These extended reports include voice quality data events, such as Jitter Buffer, Packet Loss, Delay and Burst, which are collected by the phone during the VoIP session.

When the SIP PUBLISH feature is enabled, upon the termination of the VoIP session e.g. call disconnect or Hold states, values are calculated for each voice quality data event and sent to the QoE server in a SIP PUBLISH message.

RTCP XR information publishing is implemented on the phone according to RFC 6035.

RTP Control Protocol Extended Reports (RTCP XR) is a VoIP management control that defines a set of metrics containing information for assessing VoIP call quality and for diagnosing problems. RTCP XR (RFC 3611) extends the RTCP reports defined in RFC 3550 by providing additional VoIP metrics for Quality of Experience.

9.6 Configuring Remote Voice Quality Monitoring

To report voice quality events from the phone to a Quality of Experience Server (QoE):

- Configure the phone to retrieve RTCP XP events on voice quality data (see Section 9.6.1) -and-
- Configure the phone to send SIP PUBLISH messages to the QoE server, including the RTCP XP events described above and the SIP call messages (see Section 9.6.2).

9.6.1 Configuring RTCP Extended Report

The network administrator can configure RTCP-XR (Extended Report for RTP Control Protocol) working mode. The phone You must be enabled to retrieve RTCP-XR events using one of the methods described in the table below (this feature is by default disabled).

➢ **To configure RTCP_XR working mode:**

- Use the table as reference.

Table 9-2: RTCP_XR Parameters

Parameter	Description
voip/rtcp_xr/vq_statistics/mode	Sets RTCP_XR working mode. Select either: ▪ **DISABLE**. In this state, no RTCP events are retrieved from the phone and the SIP PUBLISH is not sent, regardless of the state of parameter 'qoe_publish_enabled' (see below). ▪ **EVENTS_ONLY** (default). In this state, RTCP-XR events with voice quality parameter calculations are sent internally on the phone every five seconds. Each calculation is made on the basis of these RFC 3611 parameters: BT=7, block length = 8SSRC of source, loss rate, discard rate, burst density, gap density, burst duration, gap duration, round trip delay, end system delay, signal level, noise level, Gmin, R factor, ext. R factor, MOS-LQ, MOS-CQ, RX config, JB nominal, JB maximum and JB abs max. The phone sends the summarized RTCP-XR events to the Skype for Business server / OVOC server via SIP SERVICE messages (in Genesis-SIP, SIP PUBLISH messages are used). ▪ **REMOTE_AND_EVENTS**. In this state, the phone sends RTCP-XR events to the remote calling party (i.e. party A sends these events to party B) every five seconds during the VoIP session. The phone sends the summarized RTCP-XR events to the Skype for Business server / OVOC server via SIP SERVICE messages (in Genesis-SIP, SIP PUBLISH messages are used).

9.6.2 Configuring Voice Quality Monitoring

Network administrators can set up the phone to report SIP PUBLISH messages to a remote QoE server.

➢ **To configure voice quality monitoring:**

- Use the table as reference.

Table 9-3: Voice Quality Monitoring Parameters

Name	Role
voip/qoe/qoe_publish_enabled	Determines whether or not to send PUBLISH messages (Default-0).
voip/qoe/qoe_server_address	Sets the QoE server address/hostname to which PUBLISH messages will be sent (Default-0.0.0.0).
voip/qoe/qoe_server_port	Sets the port to which the PUBLISH messages will be sent (Default-5060).

For a full lising of RTCP XR parameters that may be sent to the QoE server, see Appendix G.

For example SIP PUBLISH messages, see Appendix H.

10 Diagnosing Problems & Troubleshooting

10.1 Recovering Phone Firmware

If the phone is powered off for some reason during the firmware upgrade process, the phone becomes unusable. See Appendix D for detailed information. The phone firmware recovery process is also available when the phone is connected to a VLAN.

➢ **To recover the phone firmware:**

1. Make sure your DHCP server supports Options 66 (TFTP server address) and 67 (firmware file), and that these are configurable.
2. Before connecting the phone, verify that the TFTP server is running and the firmware file for recovery is located in the correct location.
3. Connect your phone to the IP network, and then connect the phone to the power outlet;
   a. The phone sends a TFTP request to the IP address indicated in the DHCP Option 66 field to retrieve the firmware file indicated in the DHCP Option 67 field.
   b. The phone, in the DHCP Discover message sends its model name in the DHCP Option 77 field. The DHCP server, according to the phone model, sets the appropriate firmware file name in the DHCP Option 67 field sent to the phone (e.g., 440HD_2.2.2.img).
   c. The phone then upgrades to the recovery firmware.
   d. After the firmware upgrade process completes, the phone boots up successfully.

10.2 Configuring System Logging (Syslog)

The System Logging (Syslog) feature is used for traffic analysis and debugging.

➢ **To configure system logging:**

- Use the table as reference.

Table 10-1: Syslog Parameters

Parameter	Description
system/syslog/mode	Enables Syslog. Possible values are: • **LOCAL** (Default) • **NETWORK** = Syslog is sent to the Syslog server (recommended) • **SERIAL** = Syslog is sent to the phone console (You need to connect a serial cable to view the logs; this causes delays in the phone operation). • **ALL** = Syslog sends to the Syslog server *and* to the console.
system/syslog/log_level	Default: DETAILED. Defines the log level.
system/syslog/sip_log_filter	Default: 0. Defines the SIP log filter.
system/syslog/server_address	The IP address (in dotted-decimal notation) of the computer you are using to run the Syslog server (e.g., Wireshark). The Syslog server is an application designed to collect the logs and error messages generated by the phone. The default IP address is 0.0.0.0. **Note:** This parameter is applicable when Activate is set to **Network** or **Both**.

Parameter	Description
system/syslog/server_port	Defines the UDP port of the Syslog server. The valid range is 0 to 65,535. The default port is 514. **Note:** This parameter is applicable when Activate is set to **Network** or **Both**.
Note: The following Severity level options are applicable for the fields below: • NONE • EMERGENCY • ERROR • WARNING • NOTICE • INFO • DEBUG	
Note: The following two Severity level options are applicable for the fields below: • NONE • DEBUG	
system/syslog/component/btoe	Default: NONE.
system/syslog/component/cert	Default: NONE.
system/syslog/component/cgi	Default: NONE.
system/syslog/component/control_center	Default: NONE. Responsible for Networking and running other processes.
system/syslog/component/dsp	Default: NONE. Defines the voice engine of the phone (430HD and 440HD only).
system/syslog/component/emsc	Default: NONE.
system/syslog/component/ice_stack	Default: NONE.
system/syslog/component/ieee802_1x	Default: NONE. Defines the security protocol.
system/syslog/component/infra	Default: NONE. Defines logging for code infrastructure.
system/syslog/component/kernel	Default: NONE.
system/syslog/component/lcd_display	Default: NONE. Defines the phone screen display.
system/syslog/component/lib	Default: NONE.
system/syslog/component/media	Default: NONE.
system/syslog/component/sip_call_control	Default: NONE. Defines MTR layer Radvision.
system/syslog/component/sip_stack	Default: NONE. Defines SIP Stack Radvision.
system/syslog/component/sipe	Default: NONE.
system/syslog/component/voip_application	Default: NONE. Defines multi-layer VoIP application.
system/syslog/component/watchdog	Default: NONE. Responsible for keeping other processes running.
system/syslog/component/web_server	Default: NONE. Defines the phone Web server.
system/syslog/component/xsi	Default: NONE. Defines logging for the xsi feature.

10.3 Viewing Error Messages Displayed in the Phone Screen

The table below shows the error messages that may be viewed on the phone.

Table 10-2: Error Messages Displayed in the Phone Screen

Message	Description
LAN Link failure	The LAN link is disconnected.
Registration failure	Received error or no response from the SIP proxy

Note:

- With both errors, the 'ringer' LED remains red until the error is fixed.
- While the error message is displayed, the user can`t dial or initiate a call.

10.4 Debugging using Packet Recording Parameters

Packet recording parameters allow you to debug voice activity on the phone.

➢ **To debug:**

- Use the table as reference.

Table 10-3: Recording Parameters

Parameter	Description
voip/packet_recording/remote_ip	The IP address (in dotted-decimal notation) of the remote computer to which the recorded packets are sent. The recorded packets should be captured by a network sniffer (such as Wireshark). The default value is 0.0.0.0.
voip/packet_recording/remote_port	Defines the UDP port of the remote computer to which the recorded packets are sent. The valid range is 1024 to 65535. The default value is 50000.
voip/packet_recording/enabled	Activates the packet recording mechanism. ▪ **0** Disable (default) ▪ **1** Enable
voip/packet_recording/rtp_recording/enabled	Only displayed if the parameter 'Enable DSP Recording' is enabled. Activates the DSP RTP recording. ▪ **0** Disable (default) ▪ **1** Enable
voip/packet_recording/ec_debug_recording/enabled	Activates the Echo Canceller Debug recording. ▪ **0** Disable (default) ▪ **1** Enable
voip/packet_recording/noise_reduction_recording/enabled	Traffic on the network stops when the MUTE key is activated. ▪ **0** Disable (default) ▪ **1** Enable
voip/packet_recording/network_recording/enabled	Activates the DSP network (TDM Out) recording. ▪ **0** Disable (default) ▪ **1** Enable
voip/packet_recording/tdm_recording/enabled	Activates the DSP TDM (TDM In) recording. ▪ **0** Disable (default) ▪ **1** Enable
voip/packet_recording/cng_debug_recording/enabled	Default=0

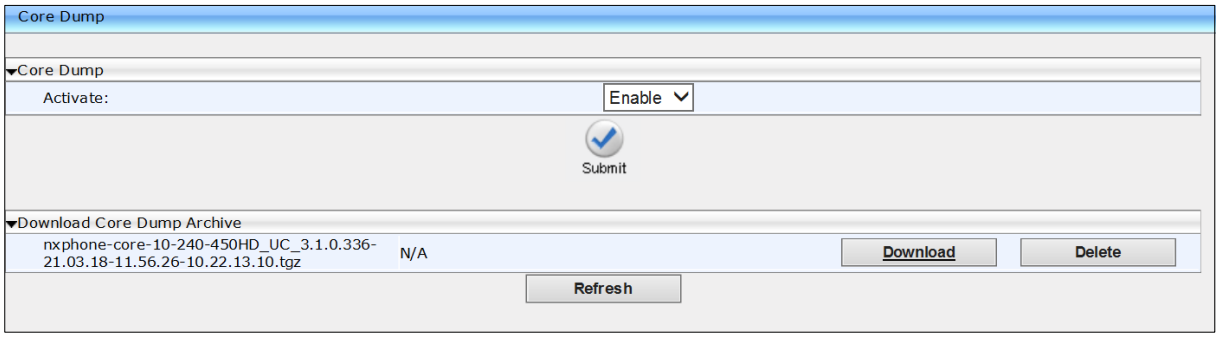
10.5 Activating Core Dump

The phone can perform a core dump providing detailed information related to a firmware exception on the phone. The core dump facilitates problem diagnosis and debugging. The recorded contents of the phone's main memory are stored at a specific time, usually after the phone crashes or is terminated abnormally, and made available for further examination.

➢ **To activate core dump using the Web interface:**

1. Open the Core Dump page (**Status & Diagnostics** > **Diagnostics** > **Core Dump**).

Figure 10-1: Web Interface – Core Dump



Note: The Core Dump feature is by default enabled on the 445HD, 450HD and C450HD phones. On all other phones, it is by default disabled.

2. Under the Core Dump section of the screen, select **Enable** from the 'Activate' dropdown (if it isn't already) and then click **Submit**.
3. If a phone issue is encountered, for example, if the phone crashes or is terminated abnormally, you can download the core dump to examine the issue and resolve it. Click **Download** to download the core dump archive to your pc; IP developers can then examine dumps of all exceptions encountered.

➢ **To enable core dump using the configuration file:**

- Use the table below as reference.

Table 10-4: Core Dump Parameter

Parameter	Description
kernel/cfg/enable_core_dump	Enables core dump. ▪ **0** Disable ▪ **1** Enable (default)

10.6 Configuring Port Mirroring

Traffic on the phone's LAN port can be duplicated on its PC port in order to record calls, analyze traffic, and troubleshoot issues.

➢ **To configure port mirroring:**

- Use the table as reference.

Table 10-5: Port Mirroring Parameters

Parameter	Description
network/pc_port_mirroring/enabled	Enables port mirroring. ▪ **0** Disable (default) - LAN/PC network interfaces operate in SWITCH mode. ▪ **1** Enable - LAN/PC network interfaces operate in HUB mode. The network traffic on the LAN port is reflected in the PC port.

A Configuring Phones in Server-Specific Deployments

This appendix shows how to configure phones in server-specific deployments.

A.1 BroadSoft's BroadWorks

Note: Support pending.

Features supported in a BroadSoft environment are:

Table A-1: Features Supported in a BroadSoft Environment

Feature	405HD	430HD	440HD
BSFT DMS for provisioning	√	√	√
BLF Support	X	√	√
Call FWD	√	√	√
Call Transfer	√	√	√
Call Park	√	√	√
Call hold	√	√	√
Dial Plan	√	√	√
Caller ID	√	√	√
Message Waiting Indication	√	√	√
Local 3-Way Conference	√	√	√
DND	√	√	√
Feature key Sync	√	√	√
Network Conference	√	√	√
Shared Call Appearance	X	√	√
Broadworks Phone book support	√	√	√
Voice Message Support	√	√	√
DNS SRV Lookup for Redundancy and register failover	√	√	√
ACD (Automatic Call Distribution)	√	√	√

A.1.1 Configuring BLF

Configuration of the BLF feature is unique when the selected application server is BroadSoft's BroadWorks application platform.

Note: This section only applies to 430HD and 440HD phones.

➢ **To configure BLF in a BroadSoft environment:**

- Use the table as reference.

Table 10-2: BLF in a BroadSoft Environment

Parameter	Description
voip/services/application_server_type	Change the default GENERIC to BSFT.
voip/services/busy_lamp_field/enabled	Configure **1** (enabled).
voip/services/busy_lamp_field/Uri	Enter the resource list URI to which the phone can subscribe to in order to get the BLF information from the application server.
voip/services/busy_lamp_field/subscription_period	Enter the interval between BLF and SIP SUBSCRIBE messages. Default: 3600 seconds. Up to 86400 seconds can be configured.
voip/services/busy_lamp_field/application_server/use_registrar	Enable this parameter for the Registrar's address to be used as the Application Server's address (see Section 5.1.2).
voip/services/busy_lamp_field/application_server/addr	Disable the previous parameter and then for this parameter configure the IP address or domain name of the application server.

A.1.2 Configuring Call Forwarding

Note: Before configuring Call Forwarding in the phone's screen, make sure the parameter 'system/feature_key_synchronization/enabled=**1**' (see Section A.1.4). The feature does not apply to the RX50 conference phone.

A.1.2.1 From the Phone

Call Forwarding can be configured in a BroadSoft environment using the phone's screen.

➢ **To configure call forwarding on the phone:**

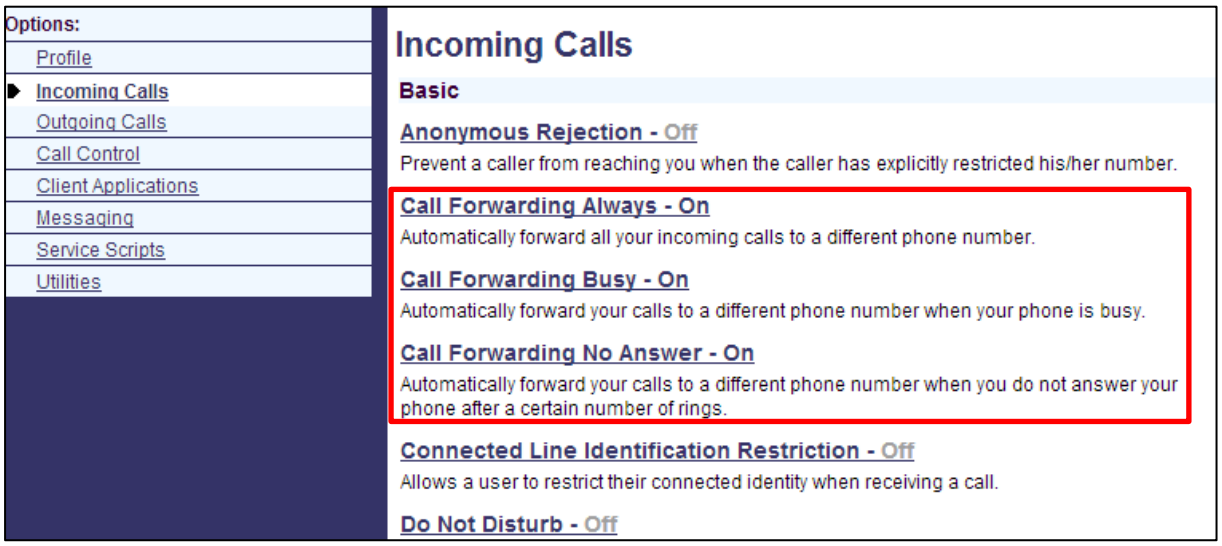
- See the phone's *User's Manual* for detailed information.

A.1.2.2 From BroadSoft's BroadWorks

Call Forwarding can also be configured from the BroadSoft BroadWorks application platform. Call Forwarding status can also be retrieved from it.

The figure below shows Call Forwarding configuration and status in BroadSoft's BroadWorks.

Figure A-2: Configuring Call Forwarding using BroadSoft's BroadWorks



Note: The 'Forward No Reply' timeout can be configured as 'number of rings' rather than as 'seconds' if the BroadSoft Feature Key is enabled (by configuring the cfg file parameter 'voip/line/0/call_forward/timeout_mode' to **RINGS_COUNT** instead of to the default **SECONDS**). For example, if the BroadSoft Feature Key is enabled and 'voip/line/0/call_forward/timeout_mode' is configured to **RINGS_COUNT**, the phone will by default ring 2r (2 rings) before the call is forwarded. The setting can be changed according to user preference to 4r (4 rings), for example. The feature allows compliance with BroadSoft's Feature Key Synchronization method.

For detailed information, see related BroadSoft documention.

A.1.3 Configuring DnD

The DnD feature can be configured in the phone's screen.

Note: Before configuring DnD, make sure the configuration file parameter 'system/feature_key_synchronization/enabled' is set to **1** (see Section A.1.4). The feature does not apply to the RX50 conference phone.

The DnD feature can also be configured using the BroadSoft BroadWorks application server. The figures below show the DnD configuration and status screens in BroadWorks.

Figure A-3: Configuring DnD in BroadSoft's BroadWorks - Status

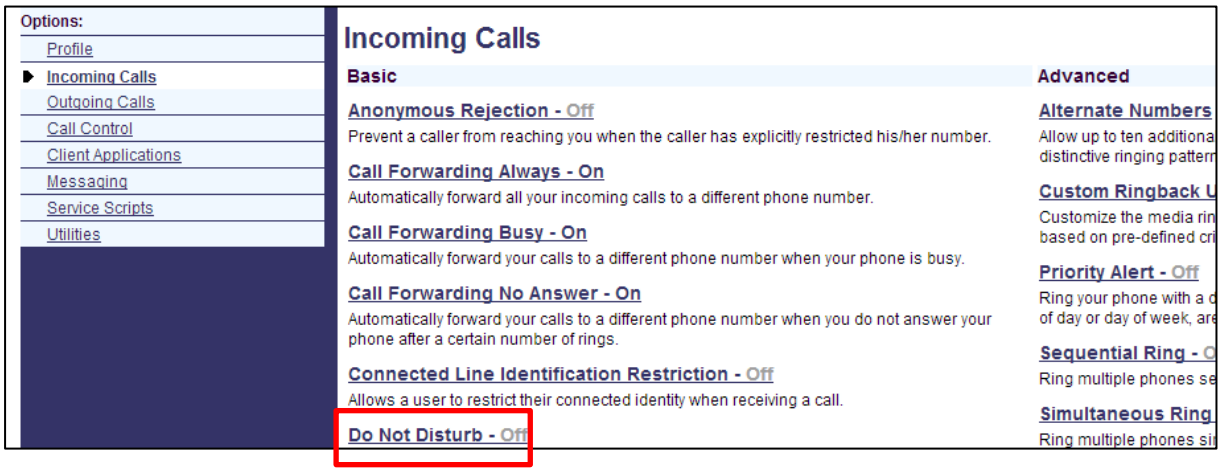


Figure A-4: Configuring DnD in BroadSoft's BroadWorks

For detailed information, see related BroadSoft documention.

A.1.4 Configuring FKS

Enabling Feature Key Synchronization synchronizes the DnD and Call Forward functionalities with the BroadSoft BroadWorks server. After activating the feature, the DnD and Call Forward functionalities are performed by BroadWorks rather than the phone. For more information on DnD functionality, see Section 5.8.7.

➢ **To enable Feature Key Synchronization using the configuration file:**

- Configure parameter 'system/feature_key_synchronization/enabled' to **1**.

A.1.5 Using SIP Authentication for Xsi Access

BroadSoft environment users can enter their BroadWorks user credentials for Xtended Services Interface (Xsi) access. The phones use SIP authentication data to authenticate Xsi access. The phones send the BroadWorks user ID to the Xtended Services Platform (Xsp) to identify the user, along with the SIP authentication user name and password to authenticate access to the Xsi.

A.1.6 Configuring Phones to Connect to Xsi I/F using HTTP/S Authentication

BroadSoft environment users can enter their BroadWorks user credentials for Xsi access using HTTP/S authentication. The phone supports three Xsi services:

- **Call Center list**

  Users can be assigned up to three call centers that will be displayed on the right side of the user's phone screen.

  Configured on programmable keys 4-6, three call centers Dept. B, Dept. C and Dept. A are displayed on the screen above. The network administrator can enable | disable the feature using configuration file parameter *xsi/callcenter/update* which by default is enabled.

  The feature allows enterprise front desk personnel to indicate their availability status (available or unavailable), in each call center, to the BroadWorks server. The server then efficiently distributes incoming calls to front desk personnel, saving callers from the inconvenience of unanswered referrals or disconnections.

- **Contact Synchronization**

  Contact directories are pulled directly from the BroadWorks server. Case-insensitive Abc name search is performed instantly. Supported directories are Group Directory, Enterprise Directory, Group Common, Enterprise Common and Personal Directory. The network administrator can enable | disable the feature using configuration file parameter *xsi/contact/enable* which by default is enabled. The feature cannot coexist with contacts saved locally on the phone.

- **Call Log Synchronization**

  Call Logs are pulled directly from the BroadWorks server. The phone displays the following Call Logs: All Calls, Missed Calls, Received Calls and Dialed Calls. The network administrator can enable | disable the feature using configuration file parameter *xsi/calllog/enable* which by default is enabled.

➢ **To connect phones to BroadWorks over HTTP/S:**

- Use the table as reference.

Table A-3: Connecting Phones to BroadWorks over HTTP/S – Configuration File Parameters

Parameter	Description
xsi/callcenter/update	▪ **1** The phone gets the call center service from the BroadWorks server ▪ **0** The phone does not get the call center service from the BroadWorks server (default).
xsi/contact/enable	▪ **1** Contacts and contact information are saved on the BroadWorks server ▪ **0** Contacts and contact information are saved locally on the phone (default)
xsi/host	Defines the phones host, BroadWorks server. The phones receive three web services from the server. **1** Contacts list **2** Call Log (history of calls dialed, received, missed, etc.) **3** Call Center
xsi/http_port	Defines the BroadSoft BroadWorks online server port number. Default: 80. Must be configured for the phones to receive web services from the BroadSoft BroadWorks online server over HTTP.
xsi/http_security	Defines the authentication method phones will use opposite the BroadSoft BroadWorks online server. Can be HTTP or HTTPS. Must be configured for the phones to receive web services over HTTP/S from the BroadSoft BroadWorks online server.
xsi/update_time	Every 20 minutes (default) phones update their call center status. Programmable keys on the phone indicate call centers' statuses. ▪ Key illuminated red = Phone unavailable ▪ Key illuminated green = Phone available Phone users can press a key to change the phone's status *in that call center*. If a user presses a key illuminated red, the key turns green and the phone's status *in that call center* changes from unavailable to available. If a key is illuminated green and the user presses it, the phone's status *in that call center* changes from available to unavailable. The BroadWorks server updates phone status every 20 minutes by default.
xsi/user_id	Defines the user ID required for the phone to access the BroadSoft BroadWorks online server.
xsi/password	Defines the password required for the phone to access the BroadSoft BroadWorks online server.

A.1.7 Configuring Shared Call Appearance

The SCA feature enables multiple phones to be associated in an SCA group so that calls can be made or received on any phone in the group.

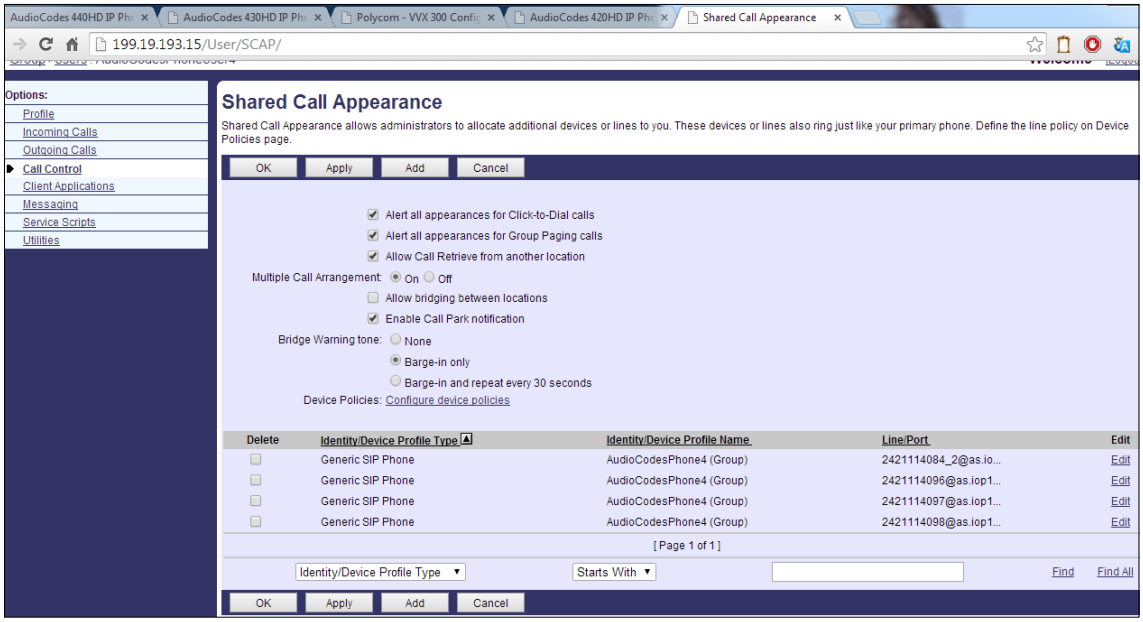
Note: Support pending.

Figure A-5: Shared Call Appearance with Multiple Call Appearance

➢ To configure Shared Calls Appearance:

1. In the BroadSoft server, assign Shared Call Appearance to the user: Under the 'User' level, select the **Call Control** option, and then click the **Shared Call Appearance** tab.

Figure A-6: BroadSoft Server - Assigning Shared Calls Appearance to a User



2. On the Shared Call Appearance page shown in the figure above, click **Add** to configure an 'Identity/Device Profile Type', and then Use the table as reference to configure the parameters.

Table A-4: BroadSoft Server - Shared Call Appearance – Identity/Device Profile Type

Parameter	Description
Alert all appearances for Click-to-Dial calls	See BroadSoft's documentation for detailed information. Select this option when you want your Click-To-Dial calls to ring all phones that have your line appearance. Clear the option if you prefer your line to ring your phone only.
Alert all appearances for Group Paging calls	See BroadSoft's documentation for detailed information.
Allow call retrieve from another location	See BroadSoft's documentation for detailed information. Select this option when you use a feature access code to automatically retrieve a call that was answered at another Shared Call Appearance of your number.
Multiple Call Arrangement	See BroadSoft's documentation for detailed information. Select **On** to allow multiple calls using your phone number / ID to be dialed or answered simultaneously across all Shared Call Appearances of your number. Select **Allow bridging between locations** when you want to use a feature access code to bridge a 3-way conference call automatically for any call that has been answered at another Shared Call Appearance of your number. Select **Enable Call Park notification** for the phone to alert the user visually and audially when a parked call is received.
Bridge Warning tone	See BroadSoft's documentation for detailed information. Select the type of Bridge Warning tone treatment you prefer when you bridge and join a call using a feature access code. Select **None** to apply no tone alert treatment upon your entry to the call. Select **Barge-in only** to provide a single tone alert. Select **Barge-in and repeat every 30 seconds** to provide a tone alert at that interval.

3. Click the **Edit** link adjacent to the selected Line/Port to modify a specific phone that has a Shared Call Appearance of your line.
4. Click **OK**.

Figure A-7: BroadSoft Server – Shared Call Appearance Add

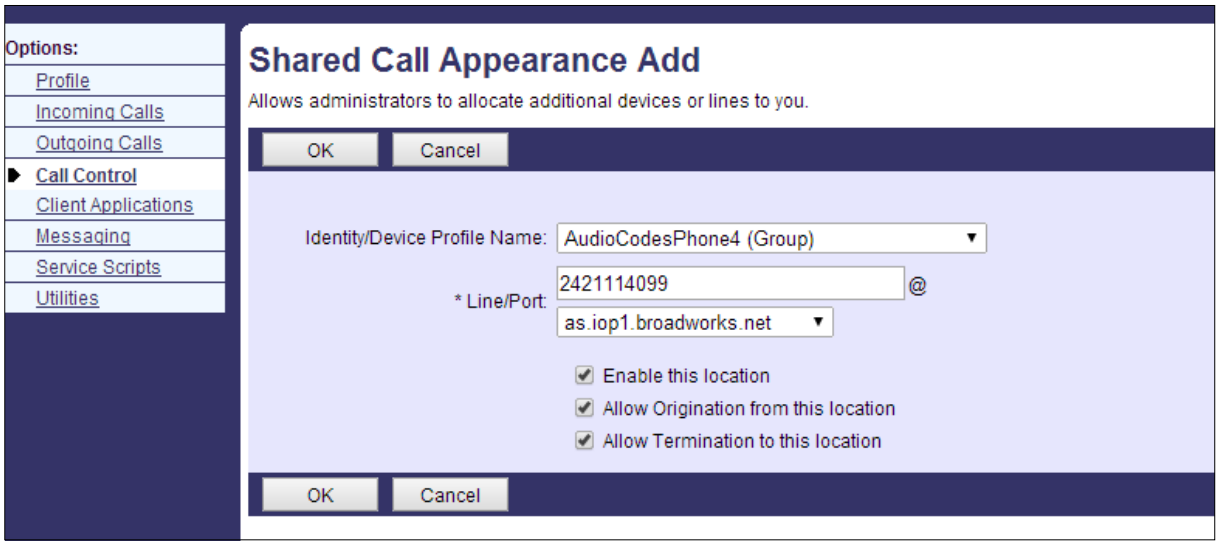


Table A-5: BroadSoft Server - Shared Call Appearance Add

Parameter	Description
Identity/Device Profile Name	See BroadSoft's documentation for detailed information. From the dropdown, select the Identity/Device Profile Type you configured previously.
Line/Port	Enter the required SIP register address-of-record, for example (shown in the figure above): **2421114099@as.iop1.broadworks.net**
Enable this location	Select this option to enable this user station.
Allow Origination from this location	Select this option to allow calls to be made from this user station.
Allow Termination to this location	Select this option to allow calls to be received at this user station.

➢ **To configure shared line using the configuration file:**

- Use the table as reference.

Table 10-6: Shared Line Parameter

Parameter	Description
voip/line/0-5/line_mode	Change the default from PRIVATE to SHARED.

A.1.8 Setting up a Remote Conference

The network administrator can set up BroadSoft's remote conference feature. More than three participants can be added to a remote conference call. A 'local' conference only supports a maximum of three. The feature must be enabled on BroadSoft's BroadWorks server for it to function.

➢ **To set up the remote conference feature:**

- Use the table as reference.

Table 10-7: Remote Conference Parameters

Parameter	Description
voip/services/application_server_type	Set to **BSFT**.
voip/services/conference/conf_ms_addr	Set the address of the server hosting the remote conference. Example: mailto:conference@as.iop1.broadworks.net
voip/services/conference/mode	Set the mode to **REMOTE**.

A.1.9 Loading the Corporate Directory to the Phone

The network administrator can load the Corporate Directory to the phone. The Corporate Directory can be loaded either

- manually, by loading a (configurable) txt, cfg, or xml file listing all employees and their details, to the phone, via 'provisioning/corporate_directory_uri' configuration file parameter. This is the URI used to retrieve the corporate directory. The corporate directory must be included in a separate file to be loaded to the phone during provisioning.
  For example:
  provisioning/corporate_directory_uri=http://10.2.3.4/corporate_dir.txt
  Note: The corporate directory file is loaded after boot up and after that, periodically. If the corporate directory file is new, the phone updates the information and does not reboot.
- automatically, by placing the (configurable) txt, cfg, or xml file on the BroadSoft BroadWorks server, and then when the phone is connected to the network, the phone pulls and automatically uploads the file from the server.

➢ **To load the Corporate Directory automatically, via the BroadSoft server:**

- Place the txt, cfg, or xml file file on the BroadSoft BroadWorks server; when the phone is connected to the network, it pulls and automatically loads the file to the phone.

A.1.10 Adding a Contact to the Corporate Directory

Phone contacts can be added to the Corporate Directory.

➢ **To add a contact to the Corporate Directory:**

- In the Directory page shown in the figure above, enter the contact's Name, Office, Home and Mobile number fields, and then click **Submit**.

A.1.11 Disabling Handset Mode

Administrators can disable handset mode parameter 'voip/handset_mode/enabled' whose default is enabled. Some call centers don't want agents to work with any device other than headsets. In this case, their administrators can change the parameter default to disabled.

Note: Some call centers don't even connnect the handsets to the phones. In this case, even though the handsets are not physically connected to the phones, admininstrators should disable the new parameter.

➢ **To disable handset mode:**

- Use the table as reference.

Table A-8: BroadSoft Server - Shared Call Appearance Add

Parameter	Description
voip/handset_mode/enabled	When disabled **0**, the handset becomes unavailable. Configure either: ▪ **1** = Enabled (default) ▪ **0** = Disabled

A.1.12 Displaying a Message in Agents' Phone Screens

Call center administrators can use a configuration file parameter to define a message that will be displayed in agents' phone screens, for example: 'Reminder: Your calls might be recorded'. Agents will then see this message, together with the date (in month/day format), displayed in their screens when their phones are in idle state.

➢ **To display a message in Agents' phone screens:**

- Use the table as reference.

Table 10-9: Displaying a Message in Agents' Phone Screens

Parameter	Description
system/display/message_on_screen	Defines a message that will be displayed in agents' phone screens together with the date (in month/day format)

A.1.13 Changing Phone Screen Backlight Timeout

Call center administrators can use a configuration file parameter to change phone screens' backlight timeout. A phone screen's backlight timeout can also be changed on the phone by the user, unless the call center administrator has disabled the possibility with the configuration file parameter personal_settings/menu/backlight_timeout/enabled (see Section 6.3 for more information about disabling phone hard keys and softkeys).

➢ **To change the backlight timeout:**

- Use the table as reference.

Table 10-10: Backlight Timeout

Parameter	Description
system/lcd/backlight/timeout	Range: 0-6 0 = Always On 1 = 10 seconds (default) 2 = 20 seconds 3 = 30 seconds 4 = 40 seconds 5 = 50 seconds 6 = 60 seconds

A.2 Asterisk, Coral and Metaswitch

A.2.1 Configuring BLF

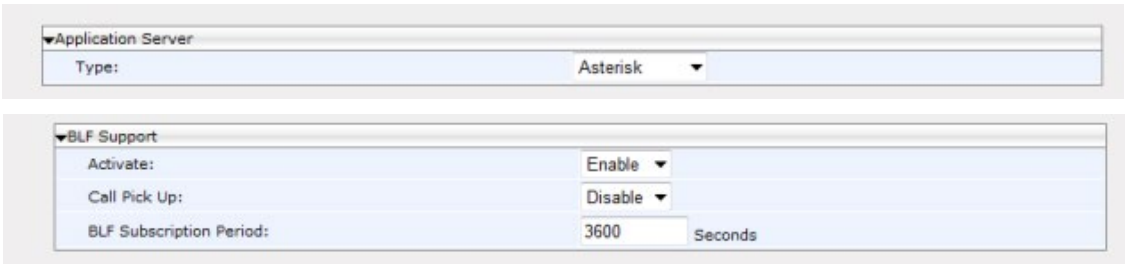
Configuration of the BLF feature is unique when the selected application server is Asterisk, Coral, or Metaswitch.

Note: This section only applies to the 430HD and 440HD phones.

➢ **To configure BLF for Asterisk application server:**

1. Open the Services page (**Configuration** > **Voice Over IP** > **Services**).

Figure A-8: BLF Configuration for Application Server Type - Asterisk



2. From the 'Application Server Type' drop-down list, select either:
   - Asterisk
   - Coral -or-
   - Metaswitch
3. In the BLF Support group, configure the following:
   - From the 'Activate' drop-down list (**voip/services/busy_lamp_field/enabled** parameter), select **Enable**.
   - (Optional) In the 'BLF Subscription Period' field (**voip/services/busy_lamp_field/subscription_period** parameter), enter the interval between BLF and SIP SUBSCRIBE messages.

Note: The application server's address is the same as the SIP Registrar address defined by parameter **voip/signalling/sip/sip_registrar/addr** (see Section 5.1.2).

4. Click **Submit**.
5. Define speed dial keys with the BLF feature (see Section 6.2).

A.3 Genesys SIP Server for Contact Centers

Note: Support pending.

This section shows system administrators how to quickly set up AudioCodes' IP phones to operate with a Genesys SIP Server in a Genesys contact center.

A.3.1 Configuring Dual Registration to Ensure SIP Business Continuity for Agents

The network administrator can configure dual registration for Genesys SIP Business Continuity.

The phone supports dual registration for integrating into Genesys' SIP Business Continuity architecture.

SIP Business Continuity provides the ability for a group of agents to continue offering critical business functions to customers in the event of a loss of all Genesys components running at a particular site.

The SIP Business Continuity architecture uses a synchronized, two-site deployment, where Genesys switch and server components are mirrored at each site in an active-active configuration, so that any agent can log in to either switch, at any time.

In a standalone SIP Server configuration with Business Continuity mode activated, The phone will register on two sites simultaneously (i.e., register on both peer SIP Servers at the same time).

Note: If you choose to use the BroadSoft-based Automatic Call Distributor (ACD) method in a SIP Business Continuity deployment, the 'voip/signalling/sip/redundant_proxy/mode' cfg file parameter cannot be set to **Simultaneous**.

➢ **To configure using configuration file:**

- Use the table as reference.

Table A-11: SIP Proxy and Registrar Parameters

Parameter	Description
voip/signalling/sip/use_proxy	Determines whether to use a SIP Proxy server. Configure **1 Enable**. ▪ **0** Disable (default) ▪ **1** Enable
voip/signalling/sip/proxy_address	Enter the IP address or host name (for example, **audiocodes.com**) of the SIP proxy server. Default: 0.0.0.0
voip/signalling/sip/proxy_port	The UDP or TCP port of the SIP proxy server. Range: 1024 to 65535. Default: 5060.

Parameter	Description
voip/signalling/sip/registrar_ka/enabled	Determines whether to use the registration keep-alive mechanism based on SIP OPTION messages. ▪ **0** Disable (default) ▪ **1** Enable **Note:** ▪ If there is no response from the server, the timeout for re-registering is automatically reduced to a user-defined value (voip/signalling/sip/registration_failed_timeout) ▪ When the phone re-registers, the keep-alive messages are re-sent periodically.
voip/signalling/sip/registrar_ka/timeout	Defines the registration keep-alive time interval (in seconds) between Keep-Alive messages. Range: 40 to 65536. Default: 60.
voip/signalling/sip/proxy_timeout	The SIP proxy server registration timeout (in seconds). Range: 0 to 86400. Default: 300.
voip/signalling/sip/registration_failed_timeout	If registration fails, this parameter determines the interval between the register messages periodically sent until successful registration. Range: 1 to 86400. Default: 60.
voip/signalling/sip/sip_registrar/enabled	Determines whether the phone registers to a separate SIP Registrar server. ▪ **0** Disable (default) ▪ **1** Enable
voip/signalling/sip/use_proxy_ip_port_for_registrar	Determines whether to use the SIP proxy's IP address and port for registration. When enabled, there is no need to configure the address of the registrar separately. ▪ **0** Disable ▪ **1** Enable (default)
voip/signalling/sip/sip_registrar/addr	The IP address or host name of the Registrar server. Default: 0.0.0.0.
voip/signalling/sip/sip_registrar/port	The UDP or TCP port of the Registrar server. Range: 1024 to 65535. Default: 5060.
voip/signalling/sip/sip_outbound_proxy/enabled	Determines whether an outbound SIP proxy server is used (all SIP messages are sent to this server as the first hop). ▪ **0** Disable (default) ▪ **1** Enable

Parameter	Description
voip/signalling/sip/sip_outbound_proxy/addr	The IP address of the outbound proxy (for example, **audiocodes.com**; i.e., the same as that configured for the 'Proxy IP Address or Host Name' parameter above). If this parameter is set, all outgoing messages (including Registration messages) are sent to this Proxy according to the Stack behavior. Default: 0.0.0.0
voip/signalling/sip/sip_outbound_proxy/port	The port on which the outbound proxy listens. Range: 1024 to 65535. Default: 5060.
voip/signalling/sip/redundant_proxy/mode	The call center's network administrator can select either ▪ **Disable** -OR- ▪ **Primary Fallback** -OR- ▪ **Simultaneous** For the dual-registration feature, select **Simultaneous**; two proxies are registered simultaneously so that at least one should be up and running at any time, preventing the call center from going down. Note that when using the BroadSoft ACD in a SIP Business Continuity deployment, this parameter cannot be set to **Simultaneous**.
voip/signalling/sip/secondary_proxy/address	Displayed only when **Simultaneous** is selected for 'Redundant Proxy Mode' (see previous parameter). Define the IP address of the secondary proxy that will be up simultaneously with the primary.
voip/signalling/sip/secondary_proxy/port	Displayed only when **Simultaneous** is selected for 'Redundant Proxy Mode' (see the parameter before the previous). Define the port of the secondary proxy that will be up simultaneously with the primary.

A.3.2 Enabling Agents to Sign in with Phone Numbers

This feature lets the call center administrator power up all phones without setting a valid SIP account. When an agent then wants to use their phone, they register to the network with their phone number.

➢ **To enable the feature using configuration file:**

■ Use the table as reference.

Table A-12: Enabling Agents to Sign in with Phone Numbers

Parameter	Description
system/login_sk_before_signed_in	Determines whether or not to enable agents sign in with phone numbers. ▪ **0** Disable (default) ▪ **1** Enable

A.3.3 Locking Agents' Phones' Alphabetical Keys

Note: Only applies to the 405HD model.

This feature lets call center network administrators lock agents' phones' alphabetical (non-numerical) keys so that only numerical keys are available to them. This feature provides call centers the option to limit agents to work-specific tasks. The feature reduces private activity on the part of agents. Agents cannot, for example, add contacts to a personal directory.

When this feature is enabled, agents can only use numbers. Only two menus are available in agents' phone screens:

- Status
- Administration

➢ **To lock alphabetical keys using configuration file:**

- Use the table as reference.

Table A-13: Locking Agents Phones Alphabetical Keys

Parameter	Description
voip/block_non_numeric_key	Determines whether or not to lock Agents' phones' alphabetical keys and only allow Agents to use numerical keys. ▪ **0** Disable (default) ▪ **1** Enable

A.3.4 Playing a Beep on an Incoming Call

This feature lets call center network administrators configure a beep to be played when a call comes in if auto-answer is configured. The beep is played on both speaker and headset. Agents will know from the beep that they have an incoming call in which to attend.

Note: To configure the auto-answer feature, see Section 5.8.6.

➢ **To configure playing a beep using configuration file:**

- Use the table as reference.

Table A-14: Playing a Beep on an Incoming Call

Parameter	Description
voip/auto_answer/headset_beep/enabled	Determines whether or not to play a beep on an incoming call, on the headset. ▪ **0** Disable (default) ▪ **1** Enable
voip/auto_answer/speakerphone_beep/enabled	Determines whether or not to play a beep on an incoming call, on the speaker. ▪ **0** Disable (default) ▪ **1** Enable

A.3.5 Enabling Proactive Mute

This feature lets call center network administrators enable a proactive mute when calls come in so that when they come in, callers cannot hear the agents until the agents unmute by pressing the **Mute** button. The feature can protect call centers from agent conduct that might be offensive to callers. Agents may for example pass an offensive remark to one another about a caller whose call is coming in, without realizing the caller can hear.

➢ **To enable proactive mute using configuration file:**

- Use the table as reference.

Table A-15: Enabling Proactive Mute

Parameter	Description
voip/proactive_mute/enabled	Determines whether or not to enable proactive mute. ▪ **0** Disable (default) ▪ **1** Enable

A.3.6 Configuring Automatic Answer

Network administrators can configure a supplementary service on the phones called Automatic Answer. Use the table as reference.

Table 10-16: Automatic Answer

Parameter	Description
voip/talk_event/enabled	Enables the 'talk' event feature. ▪ **0** Disable (default) ▪ **1** Enable The phone automatically answers an incoming call if it receives a SIP NOTIFY message with the 'talk' event. If a call is already in progress, the call is put on hold and the incoming call is answered.

A.3.7 Regulating the 'Logged out' Message

This feature lets call center network administrators enable/limit the length of time the 'Logged out' message is displayed in the phone's idle screen after agents log out.

When agents log out, the 'Logged out' message will only be displayed in the phone's idle screen for the length of time, in seconds, configured by the call center network administrator. After the configured time lapses, the message disappears from the screen.

Administrators can also disable the feature.

➢ **To regulate the feature:**

- Use the table as reference.

Table A-17: Regulating the 'Logged out' Message

Parameter	Description
voip/services/ACD/logged_out_message_timer	**-1** Disabled (default) **0** No 'Logged out' message is displayed. **>1** The time, in seconds, that lapses before the 'Logged out' message, displayed in the phone's idle screen after an agent logs out, disappears. This value also enables the feature.

A.3.8 3PCC (Third Party Call Control)

The 3PCC feature lets an agent control their phone remotely from a computer application. 3PCC always supports the following functions:

- MakeCall (call initiation/setup)
- Release
- Hold
- Retrieve
- Transfer
- Consult
- Conference
- DTMF

➢ **To configure 3PCC using configuration file:**

✓ Use the table as reference.

Table A-18: 3PCC Parameters

Parameter	Description
voip/talk_event/enabled	▪ **0** Disable (default) ▪ **1** Enable

Note: voip/talk_event must be enabled for 3PCC to function.

A.3.8.1 Enabling 3PCC Calls

This feature complies with the RFC 3725 standard for 3PCC in SIP for 'Black Holed' and 'Non SDP'. See the RFC for detailed information.

➢ **To enable 3PCC calls:**

- Use the table as reference.

Table A-19: Enabling 3PCC Calls

Parameter	Description
3PCC/make_call/enabled	**0** = Disable (default) **1** = Enable

A.3.9 Disabling Handset Mode

Administrators can disable handset mode parameter 'voip/handset_mode/enabled' whose default is enabled.

Some call centers don't want agents to work with any device other than headsets. In this case, their administrators can change the parameter default to disabled.

Note: Some call centers don't even connnect the handsets to the phones. In this case, even though the handsets are not physically connected to the phones, admininstrators should disable the new parameter.

➢ **To disable handset mode:**

- Use the table as reference.

Table A-20: BroadSoft Server - Shared Call Appearance Add

Parameter	Description
voip/handset_mode/enabled	When disabled **0**, the handset becomes unavailable. Configure either: ▪ **1** = Enabled (default) ▪ **0** = Disabled

A.3.10 Changing Phone Screen Backlight Timeout

Call center administrators can use a configuration file parameter to change phone screens' backlight timeout. A phone screen's backlight timeout can also be changed on the phone by the user, unless the call center administrator has disabled the possibility with the configuration file parameter personal_settings/menu/backlight_timeout/enabled (see Section 6.3 for more information about disabling phone hard keys and softkeys).

➢ **To change the backlight timeout:**

- Use the table as reference.

Table 10-21: Backlight Timeout

Parameter	Description
system/lcd/backlight/timeout	Range: 0-6 0 = Always On 1 = 10 seconds (default) 2 = 20 seconds 3 = 30 seconds 4 = 40 seconds 5 = 50 seconds 6 = 60 seconds

A.3.11 Displaying a Message on Agents' Phones

Call center administrators can use a configuration file parameter to define a message that will be displayed on agents' phones, for example: 'Reminder: Your calls might be recorded'. Agents will then see this message, together with the date (in month/day format), displayed in their screens when their phones are in idle state.

➢ **To display a message on Agents' phones:**

- Use the table as reference.

Table 10-22: Displaying a Message on Agents' Phones

Parameter	Description
system/display/message_on_screen	Defines a message that will be displayed in agents' phone screens together with the date (in month/day format)

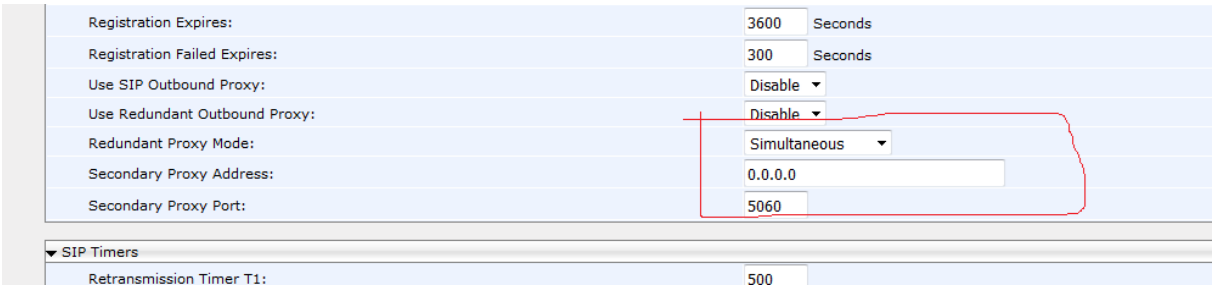
A.3.12 Configuring a Redundant (Backup) Genesys Server

A phone can be registered on two Genesys servers simultaneously, to provide immediate backup. The feature enables quick transition to the redundant backup server; redundant proxy usage is available all the time. The phone is registered on the redundant server in the same way as it is registered on the primary server.

➢ **To register a phone on the redundant server:**

1. Open the Signaling Protocol page (**Configuration** > **Voice Over IP** > **Signaling Protocols**).

Figure A-9: Registering a Phone on the Redundant Genesys Server



2. Scroll down to the 'Redundant Proxy Mode' and 'Secondary Proxy Address' parameters. Configure them using the table below as reference, and then click **Submit**.

Table 10-23: Redundant Genesys Server - Parameters

Parameter	Description
Redundant Proxy Mode	From the dropdown, select **Simultaneously**; you're now in Dual Registration mode; when in this mode, the value of the parameter 'Retransmission Timer T1' is taken from the configuration file parameter 'voip/signalling/sip/redundant_proxy/dual_reg/t1' rather than from the 'Retransmission Timer T1' parameter (see Table 5-8 for more information about this parameter).
Secondary Proxy Address	Provide the IP address of the redundant proxy; the phone then registers on both servers from the outset, instead of transitioning from one to another.

A.3.12.1 Configuring Retransmission Timer T1

Configuration of the T1 retransmission timer is only relevant when in dual registration mode, i.e., after configuring a redundant Genesys server, as shown in the previous section.

➢ **Configuring Retransmission Timer T1:**

1. Use the table as reference.

Table A-24: Retransmission Timer T1 - Parameter

Parameter	Description
voip/signalling/sip/redundant_proxy/dual_reg/t1	Only relevant if dual registration / redundancy server is configured. Default: 20 milliseconds. Range: 20-200.

A.4 Genband: KBS Softswitch Solution

Note: Applies to both the low-end phones and the high-end phones.

Network administrators can configure the following Kandy Business Solutions (KBS) softswitch solution features in the KBS Portal:

- Shared Line Appearance (SLA)
- Call pickup
- Busy Lamp Fields (BLFs)
- Remote conference

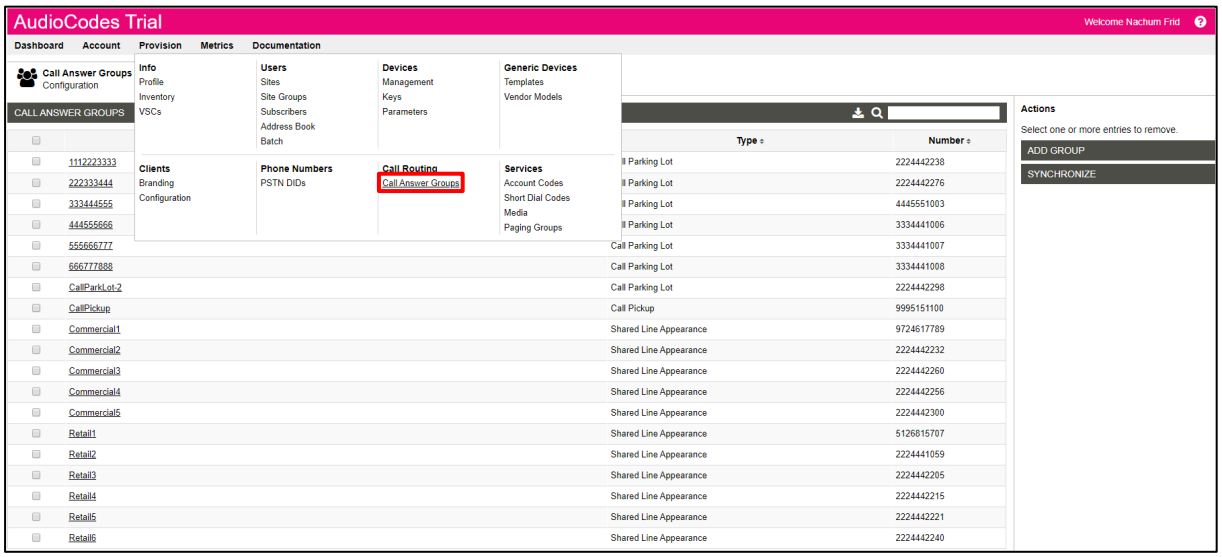
A.4.1 Configuring Shared Line Appearance

When a call comes in on a shared line, all phones ring in the SLA group. When answered by someone in the group, all other users in the group can see there's an active call on the line. When there's an active call on the line, no other phone can initiate a call on the line. When a call is put on hold, the caller hears music; other users in the group can see the call is on hold (color indication or flashing). When a call is on hold, the same phone or another phone can retrieve the call.

➢ To configure an SLA group:

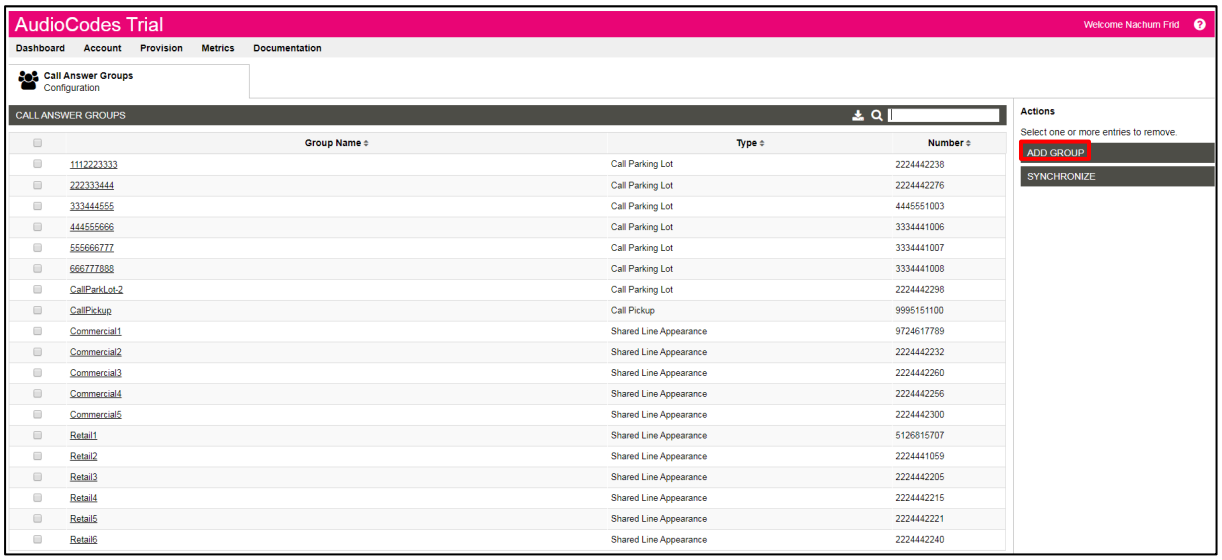
1. Open the Genband portal in your web browser and from the 'Provision' menu, select **Call Answer Groups**.

Figure A-10: Call Answer Groups



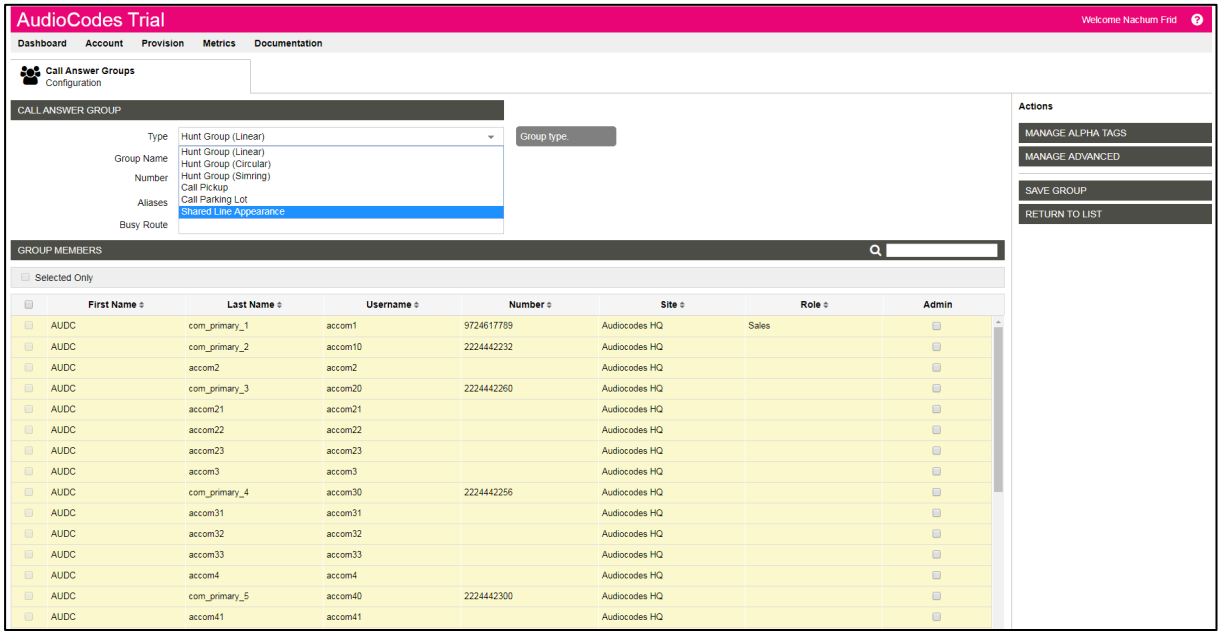
2. In the Call Answer Groups screen that opens, click **Add Group**.

Figure A-11: Call Answer Groups - Add Group



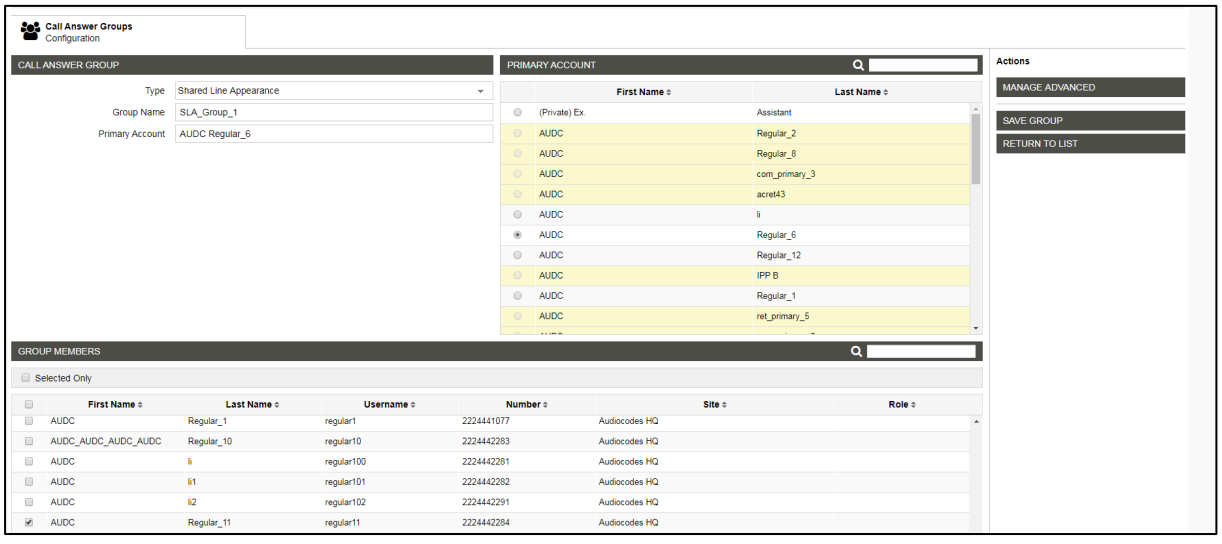
3. From the 'Type' dropdown, select the option **Shared Line Appearance**.

Figure A-12: Call Answer Group - Type



4. In the ‘Group Name’ field, enter the name of a group, for example, **SLA_Group_1**, as shown in the figure below.
5. Under the Group Members section of the screen, select the members of the group. You cannot select members highlighted yellow; they’ve already been assigned to groups. Select from members that aren’t highlighted yellow. In the example shown in the figure below, **Regular_11**, **Regular_12** and **Regular_13** are selected.
6. Click in the field ‘Primary Account’ and in the Primary Account section of the screen that opens, select the primary account. In the example shown in the figure below, AUDC (first name) Regular_6 (last name) is selected; the ‘Primary Account’ field is immediately populated with the selection.

Figure A-13: Call Answer Group – Group Name



7. Click 'MANAGED ADVANCED': 'Bridging', 'Bridging warning tone' or 'Private hold'. The 'Private hold' setting is inactive; the server only supports ‘Public hold’.
8. Click **Save Group**; the SLA group is created.

➢ **To configure Genband configuration file parameters:**

- Use the table as reference.

Table 10-25: Genband Configuration File Parameters

Parameter	Description
voip/media/allow_multiple_rtp	Configure to **1** in order to make calls with PSTN. If it isn't configured, only one-way voice will be heard.
voip/services/SLA/type	Configure to to **GENBAND_SCA**.
voip/services/sla/barging/enable	Configure to **1**. Default: 0.
voip/sla/group/0/description	[440HD only] Configure to **Group1**.
voip/sla/group/0/enabled	[440HD only] Configure to **1**. Default: 0.
voip/sla/group/1/description	[440HD only] Configure to **Group2**.
voip/sla/group/1/enabled	[440HD only] Configure to **1**. Default: **0**.

A.4.2 Configuring Call Pickup

When configuring a call pickup group, basic configuration options determine:

- the numbers that route into a call pickup group
- whether or not vertical service code (VSC) dialing can be used by group members
- group members

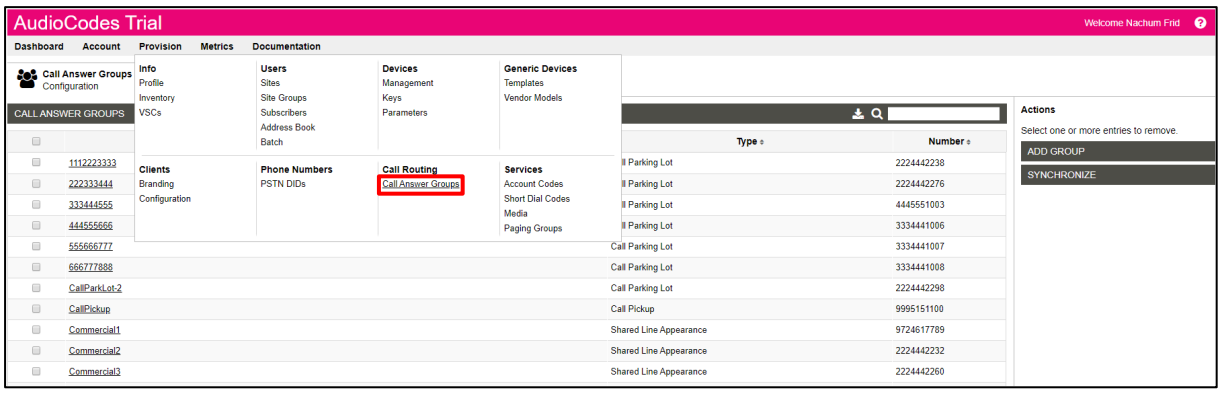
Advanced configuration options allow you to specify:

- the maximum number of group members
- the maximum number of call queues
- whether or not SIP dialog event package subscriptions are enabled

➢ **To configure a Call Pickup group:**

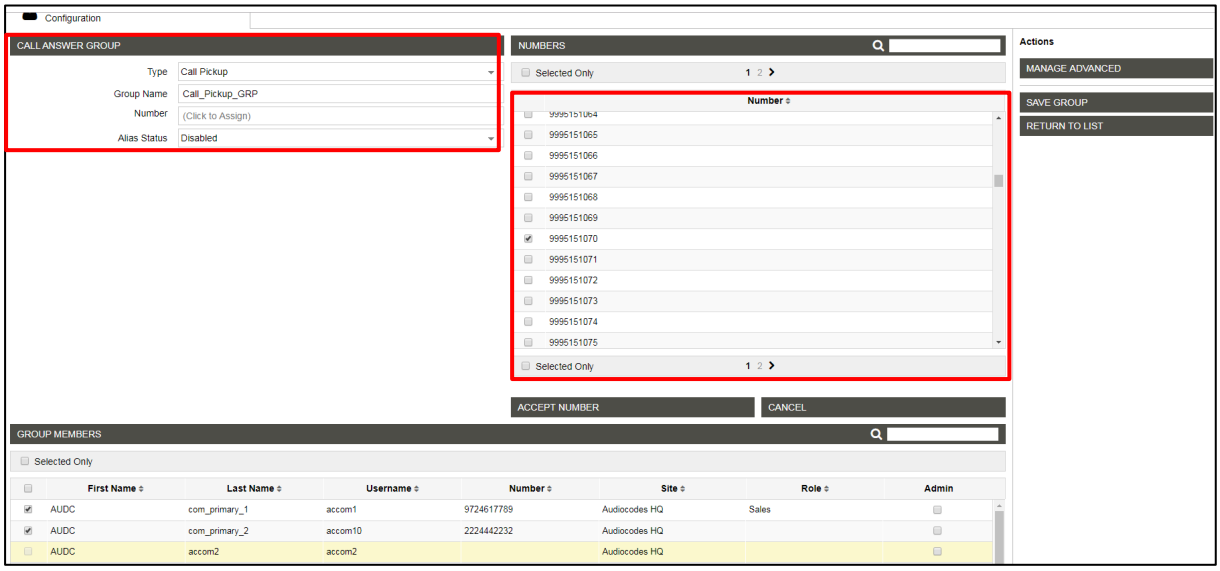
1. Open the Genband portal in your web browser and from the 'Provision' menu, select **Call Answer Groups**.

Figure A-14: Call Answer Groups



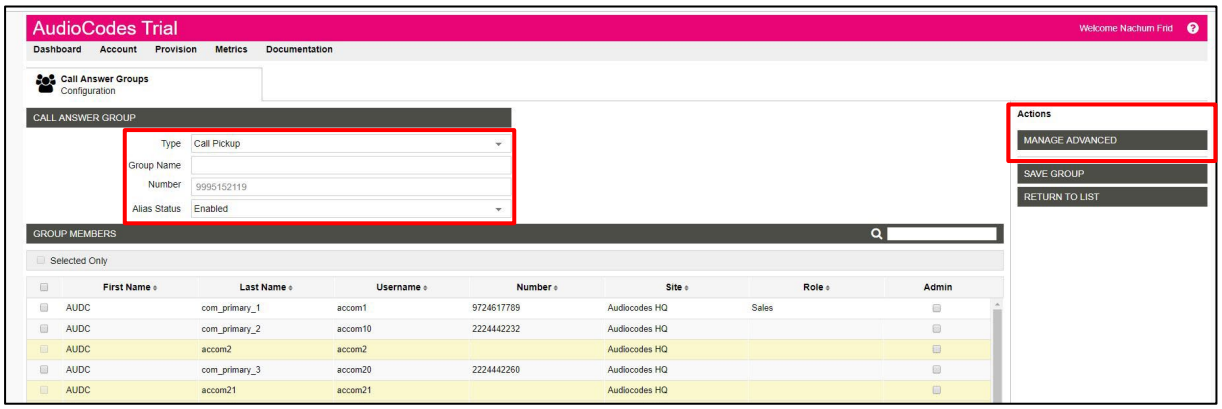
2. Click **Add Group**.

Figure A-15: Call Answer Group



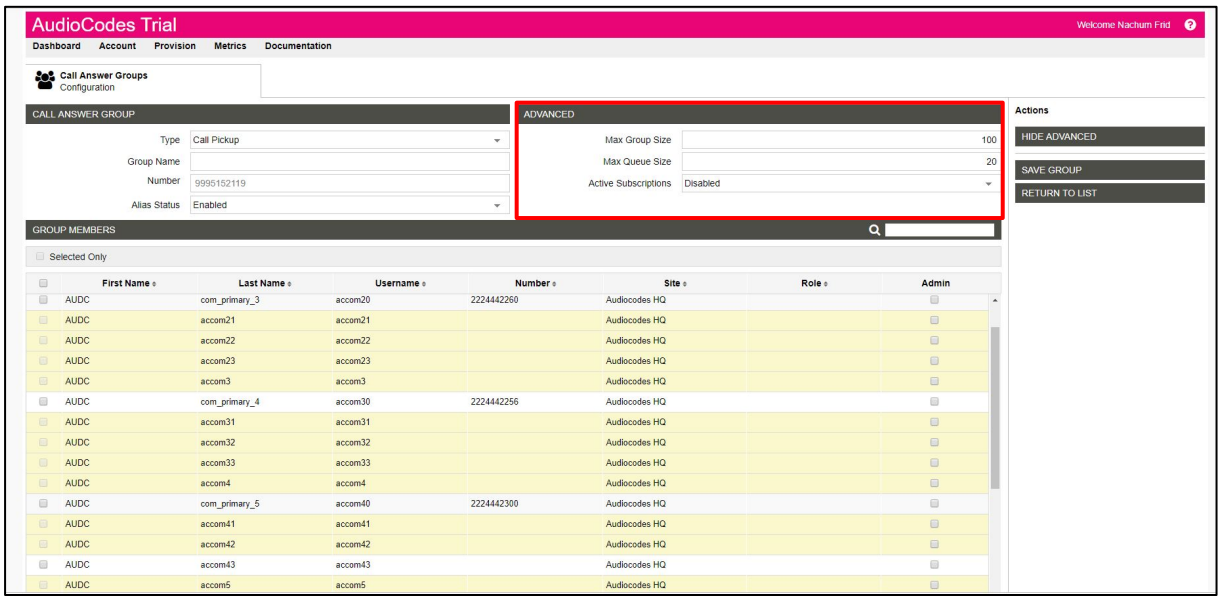
3. From the 'Type' dropdown, select **Call Pickup**.
4. Enter a Group Name, for example, Call_Pickup_GRP, as shown in the preceding figure.
5. Click the 'Number' field; all available numbers are displayed under 'Numbers', as shown in the preceding figure.
6. Select the phone number to route into the group, and then click **Accept Number**; the number is displayed in the 'Number' field, as shown in the figure below.

Figure A-16: Number



7. From the 'Alias Status' dropdown, select **Enabled** to enable VSC dialing, as shown in the preceding figure.
8. Click **Manage Advanced** to configure advanced options.

Figure A-17: Advanced



9. Enter a number in the 'Max Group Size' field to specify the maximum number of members allowed in the group.
10. Enter a number in the 'Max Queue Size' field to specify the maximum number of calls allowed in the queue for the group.
11. From the 'Active Subscriptions' dropdown, select **Enabled** to enable SIP dialog event package subscriptions.
12. To add members to the group, select the checkbox beside the name of each person to be included in the GROUP MEMBERS list.
13. Click **Save Group**.

A.4.3 Setting up a Remote Conference

More than three participants can be added to a remote conference call. By contrast, a 'local' conference only supports a maximum of three. The feature must be enabled on Genband's server. For detailed information about the feature's capabilities, see RFC 4579, Session Initiation Protocol (SIP) - Call Control - Conferencing for User Agents.

➢ **To set up the remote conference feature:**

- Use the table as reference.

Table 10-26: Remote Conference Parameters

Parameter	Description
voip/services/application_server_type	Set to **GENBAND**.
voip/services/conference/conf_ms_addr	Set the address of the server hosting the remote conference: **conference@SIP proxy address of Genband's server**
voip/services/conference/mode	Set the mode to **REMOTE**.

B Alternative Automatic Provisioning Methods

B.1 Static DNS Record Method

The Static DNS (Generic Domain Name) Record method is used for automatic provisioning when you are unable to manage your DHCP server. If the provisioning server does not support using SIP SUBSCRIBE and NOTIFY messages mechanism as described above and no response for the SIP SUBSCRIBE message has been received, the phone tries to retrieve firmware and configuration files using the following URL:
tftp://ProvisioningServer/<*Phone Model Name*>/

For example:

- The phone tries to obtain the following firmware file:
  tftp://ProvisioningServer/445HD.img
- The phone tries to obtain the following configuration file:
  tftp://ProvisioningServer/445HD/<MAC address>.cfg

  (e.g. tftp://ProvisioningServer/445HD/001122334455.cfg)

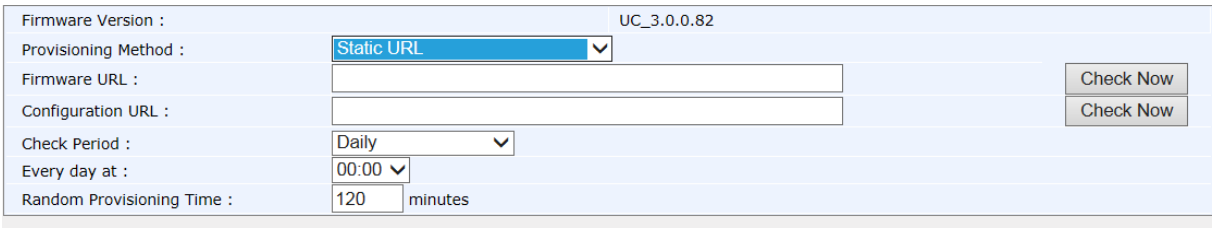
It is the Administrator's responsibility to configure a DNS entry called **ProvisioningServer** on the DNS server and set it to the TFTP server IP address.

Note: If Generic Domain Name is used, the automatic provisioning mechanism periodically tries to retrieve new firmware/configuration from Provisioning Server domain name.

➢ **To configure Static DNS Record using the Web interface:**

1. Open the Automatic Update page (**Management** tab > **Automatic Update** menu > **Automatic Provisioning**).

Figure B-1: Web Interface - Static DNS Record



2. Configure using the table below as reference and click **Submit**.

➢ **To configure Static DNS Record using the Configuration File:**

- Open the Configuration File page (**Management** tab > **Manual Update** > **Configuration File**) and configure the parameters using the table below as reference.

Table B-27: Static DNS Record Parameters

Parameter	Description
provisioning/firmware/url	The static URL for checking the firmware file. The URL must be entered using one of the following syntax options: ▪ <protocol>://<server IP address or host name> ▪ <protocol>://<server IP address or host name>/<firmware file name> Where <protocol> can be one of the following protocols: "ftp", "tftp", "http" or "https". For example: ▪ tftp://192.168.2.1 – retrieved firmware file is 445HD.img ▪ ftp://192.168.2.1/Different_Firmware_Name.img - retrieved firmware file is Different_Firmware_Name.img **Note:** This parameter is applicable only when **method** is configured to "Static".
provisioning/configuration/url	The static URL for checking the configuration file. The URL must be entered using one of the following syntax options: ▪ <protocol>://<server IP address or host name> ▪ <protocol>://<server IP address or host name>/<configuration file name> Where <protocol> can be "ftp", "tftp", "http" or "https" and where <configuration file name> can be either: ▪ A unique configuration file, per phone, for example: <MAC>.cfg -or- ▪ A global configuration file, per deployment, for example, 445HD.cfg Unique Configuration Example **http://192.168.2.1/different.img;<MAC>.cfg** The retrieved firmware file is *different.img* and the configuration file name is *<MAC>.cfg* such as *001122334455.cfg* Global Configuration Example **http://192.168.2.1/<445HD>.cfg** The configuration file name is *445HD.cfg* **Note:** This parameter is applicable only when 'Method' is configured to **Static**.

B.2 AudioCodes' HTTPS Redirect Server

AudioCodes' HTTPS redirect server can be used to direct phones to the provisioning server's URL, for downloading configuration and firmware files.

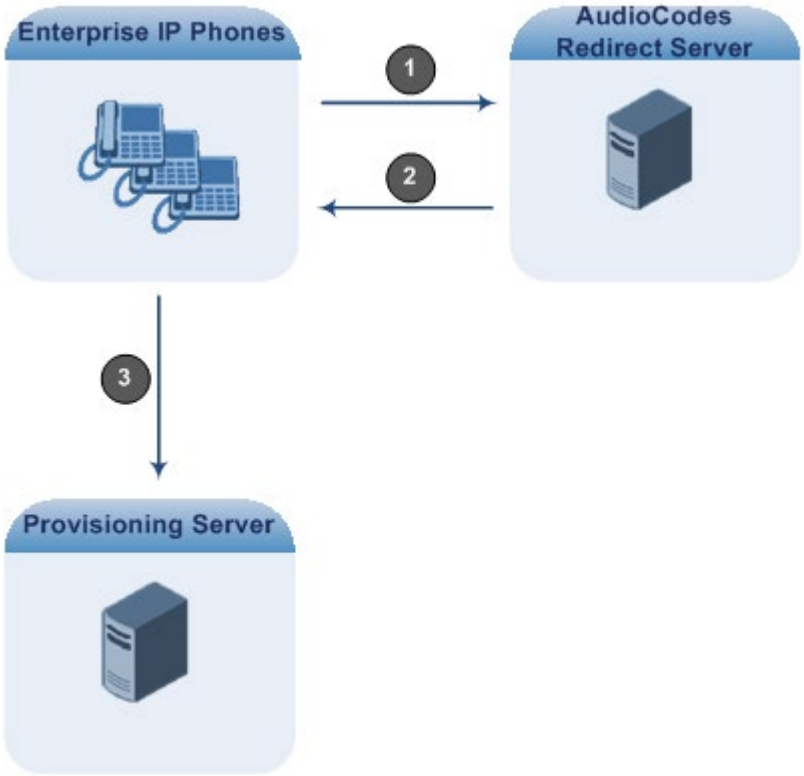
After the phone is powered up and network connectivity is established, the phone automatically requests provisioning information. If it doesn't get it according to the regular provisioning methods, it sends an HTTPS request to AudioCodes' HTTPS redirect server. The server responds to the phone with an HTTPS Redirect response containing the URL of the provisioning server where the firmware and configuration files are located. When the phone successfully connects to the provisioning server's URL, an Automatic Update mechanism begins.

Note: Phones' MAC addresses and the provisioning server's URL are preconfigured on the HTTPS redirect server. For more information, contact AudioCodes support.

AudioCodes' HTTPS redirect server's default URL is:
provisioning/redirect_server_url=https://redirect.audiocodes.com

This address can be reconfigured if required.

Figure B-2: HTTPS Redirect Server Directing Phones to Provisioning Server



B.2.1.1 Redirection Process

Here's how redirection is performed (refer to Figure B-2):

1. The phone sends an HTTPS request to the redirect server.
2. The redirect server sends an HTTPS response with the provisioning server's URL.
3. The phone sends a request for cfg and img files to the provisioning server.

Communications between the phone and the redirect server are encrypted (HTTPS) for security reasons. The phone uses the pre-installed AudioCodes factory-set certificate to authenticate itself with the redirect server and to verify the latter's authenticity. If the redirect URL (where the cfg file is located) also uses HTTPS protocol, the phone can use a regular certificate - or the AudioCodes factory-set certificate - to authenticate itself and to validate the server's certificate if a trusted root certificate (regular) is configured.

Note: The phone repeats the redirect process whenever reset to factory defaults.

C Configuring Automatic Call Distribution (ACD)

Note:

- Support pending.
- The phones seamlessly interwork with Genesys SIP Server to support ACD functionality. The phones support two different ACD methods: Two ACD server types are supported with parameter 'voip/services/ACD/server_type':
  - √ GENESYS
  - √ BROADSOFT
- For optimal ACD functionality with Genesys SIP Server, the BroadSoft-based ACD method must be configured.

This appendix shows how to enable the ACD (Automatic Call Distribution) feature on the phone. The feature automatically distributes incoming calls to agents' phones on the basis of agent availability and unavailability.

In contact centers, ACD is a key feature of CTI (Computer Telephony Integration). The feature automatically distributes incoming calls to a specific group of terminals that contact center agents use. Most ACD functionality is the SIP server's responsibility; however, users must inform the Call Center SIP server on the following events:

- Whenever the call center representitive logs in or out on the phone. This information is included in a SIP SUBSCRIBE message.
- Whenever the call center representitive indicates whether they are ready or not to take a call. When the BroadSoft server is configured, the user can also specify the reason for their unavailability e.g. Lunch break. All this information is included in a SIP NOTIFY message.
- Whenever the user is busy with After Call Work (ACW) (only relevant when a BroadSoft SIP server is configured). This information is included in a SIP NOTIFY message.

All the above actions can be performed on the phone (see the phone's *User's Manual*). The Call Center SIP server then uses the above presence information to automatically distribute calls between agents based on their availability.

ACD systems allow companies that handle a large number of incoming phone calls to direct the callers to a company employee who is able to talk at the earliest opportunity.

The feature is typically implemented in contact centers encountering large numbers of incoming customer calls that must be distributed to available agents to provide immediate support to callers. The feature automatically directs incoming calls to agents working in the contact center whose presence status is 'Ready' rather than not ready. The feature's main benefit is to reduce the time customers are kept waiting and thereby improve service.

AudioCodes' IP phones seamlessly interwork with Genesys' SIP server to support the ACD feature. Once an agent signs in on their phone to ACD, their status is set to 'Ready' and synchronized with Genesys' Server. Incoming calls are directed to an agent whenever their status becomes 'Ready'.

➢ **To configure the ACD server:**

- Define a path and configure the parameters using the table below as reference.

Table C-1: ACD Parameters

Parameter	Description
voip/services/ACD/enabled	Enables / disables the status of the ACD feature for combined ACD/Hoteling, i.e., backwards compatibility. Select either: ▪ **0** Disable (default) ▪ **1** Enable
voip/services/ACD/server_type	From the 'Server Type' drop-down list, select **GENESYS** or **BROADSOFT**. Select the **BROADSOFT** option for optimal ACD functionality with Genesys. When you select **BROADSOFT**, after logging into the ACD server, the **ACW** (After Call Work) softkey will be displayed on the phone and the **Missed** softkey displayed in the command menu along with the FORWARD and DND options. Note that administrators can optionally hide the **ACW** softkey (see the next parameter).
voip/services/ACD/show_acw_softkey/enabled	Allows administrators to hide the **ACW** softkey. After logging into the call center's Automatic Call Distributor (ACD) server, the **ACW** softkey is by default displayed on the phone **1**. Administrators can change this default and hide the softkey **0**. ▪ **0** Disable ▪ **1** Enable (default) The default softkey layout is **ACW**, **READY**/**Not Ready** (when the user is logged on), **Login**/**Logout** and Command menu items including **Missed** and **DND**. When the **ACW** softkey is disabled, the display stays the same but *without* the **ACW** softkey.
system/dnd/show_softkey	Removes the **DND** item from the Call Menu where it's displayed by default when ACD is enabled. ▪ **0** Removes **DND** from the Call Menu ▪ **1** Displays **DND** in the Call Menu (default)
system/forward/show_softkey	Removes the **Forward** item from the Call Menu where it's displayed by default when ACD is enabled. ▪ **0** Removes **Forward** from the Call Menu ▪ **1** Displays **Forward** in the Call Menu (default)
voip/services/ACD/server_use_sip_server	From the drop-down, choose **Enable**. ▪ **0** Disable ▪ **1** Enable
voip/services/ACD/expire_time	The server registration timeout, in seconds. Range: 0 to 86400. Default: 3600.
voip/services/ACD/server_address	Displayed only when 'Use SIP Server As ACD Server' is set to **Disable** (see previous). Defines the IP address of the ACD server. Default: 0.0.0.0

Parameter	Description
voip/services/ACD/server_port	Displayed only when 'Use SIP Server As ACD Server' is set to **Disable** (see previous). Defines the port of the ACD server. Default: 80
system/user_name	Enter the agent's User Name. The agent will use this name when logging in to ACD in order to define or change availability status.
system/password	Enter a password if necessary.
voip/services/ACD/state_after_login [1]	The call center's network administrator can select: ▪ **Ready** ▪ **Not Ready** (default) ▪ **Not Set** If set to **Ready**, each phone in the call center will automatically be set to a state of readiness to take incoming calls immediately after the call center's agents log in. If set to **Not Ready**, agents can log in and then manually configure their readiness status on the phone's screen, giving them time to perform personal tasks before beginning work. If set to **Not Set**, the status of the phone after login will be controlled by the server. For example, if the server is set to be in 'Ready' status following login, the phone will be in 'Ready' status when the user logs in.
voip/services/ACD/first_notify_close/enabled	▪ **0** When an agent logs in, the ACD server is notified that the agent is Ready (available) to take calls. ▪ **1** (Default) When an agent logs in, the ACD server is notified that the agent is Not Ready (unavailable) to take calls. This gives agents time to get organized.
voip/services/ACD/logged_out_message_timer	For detailed information, see Appendix A.3.7.
voip/services/ACD/unavailable_reason/0-9/code Up to 10 reasons can be defined (0-9).	Specifies the code that is sent in the SIP NOTIFY message to the Call Center SIP server to indicate the specific reason for the Call Center representitive's unavailability. This parameter is relevant when the 'Server Type' parameter (see above) is **BroadSoft**.
voip/services/ACD/unavailable_reason/0-9/name	Describes the unavailability reason code (configured above). For example, 'Lunch'. This parameter is relevant when the 'Server Type' parameter (see above) is **BroadSoft**.
voip/services/enhanced_ACD/enabled	Enables / disables the status of the ACD feature (ACD only). ▪ **0** Disabled ▪ **1** Enabled

[1] This parameter is only relevant to Genesys Call Centers.

C.1 Softkey Display and Command Menu Options

The following tables show the different softkey display states and command menu options that are available according to the user's login state and the configured SIP server.

Table C-2: BroadSoft-Softkey Display States and Command Menu Options

State		Softkey #0	Softkey #1	Softkey #2	Softkey #3
Idle	ACD Disabled	Directory	Missed	Forward	DnD
	ACD Enabled (logged out)	Missed	-	Login	Command Menu: ▪ Forward ▪ DnD
	ACD Enabled (logged in)	ACW	Not Ready or Ready	Logout	Command Menu: ▪ Missed ▪ Forward ▪ DnD
Ongoing Call State	ACD Disabled	Hold	Conf	New Call	End
	ACD Enabled (logged out)				
	ACD Enabled (logged in)				
State		**Softkey #0**	**Softkey #1**	**Softkey #2**	**Softkey #3**
Idle	ACD Disabled	Directory	Missed	Forward	DnD
	ACD Enabled (logged out)	Missed	-	Login	Command Menu: ▪ Forward ▪ DnD
	ACD Enabled (logged in)	Missed	Not Ready or Ready	Logout	Command Menu: ▪ Forward ▪ DnD
Ongoing Call State	ACD Disabled	Hold	Conf	New Call	End
	ACD Enabled (logged out)				
	ACD Enabled (logged in				

D Recovering the Phone

If the phone is powered off for some reason during the firmware upgrade process, the phone becomes unusable. This appendix shows how to recover the phone.

The recovery process is also available when the phone is connected to a VLAN.

➢ **To recover the phone, follow this procedure:**

1. Identify that the phone is in recovery mode (see below)
2. Recover the phone (see below)
3. Verify that the phone downloaded the image file (see below)

D.1 Identifying that the Phone is in Recovery Mode

Network administrators can identify when the phone is in recovery mode.

➢ **To identify when the phone is in recovery mode:**

- Observe the following displayed on the phone's screen:

Figure D-1: Identifying Recovery Mode

-OR-

- Observe that the phone reboots every +-5 seconds.

-OR-

- You'll receive a notification notifying you (users *and* network administrators) that the phone has entered recovery mode. All phone models support this notification.

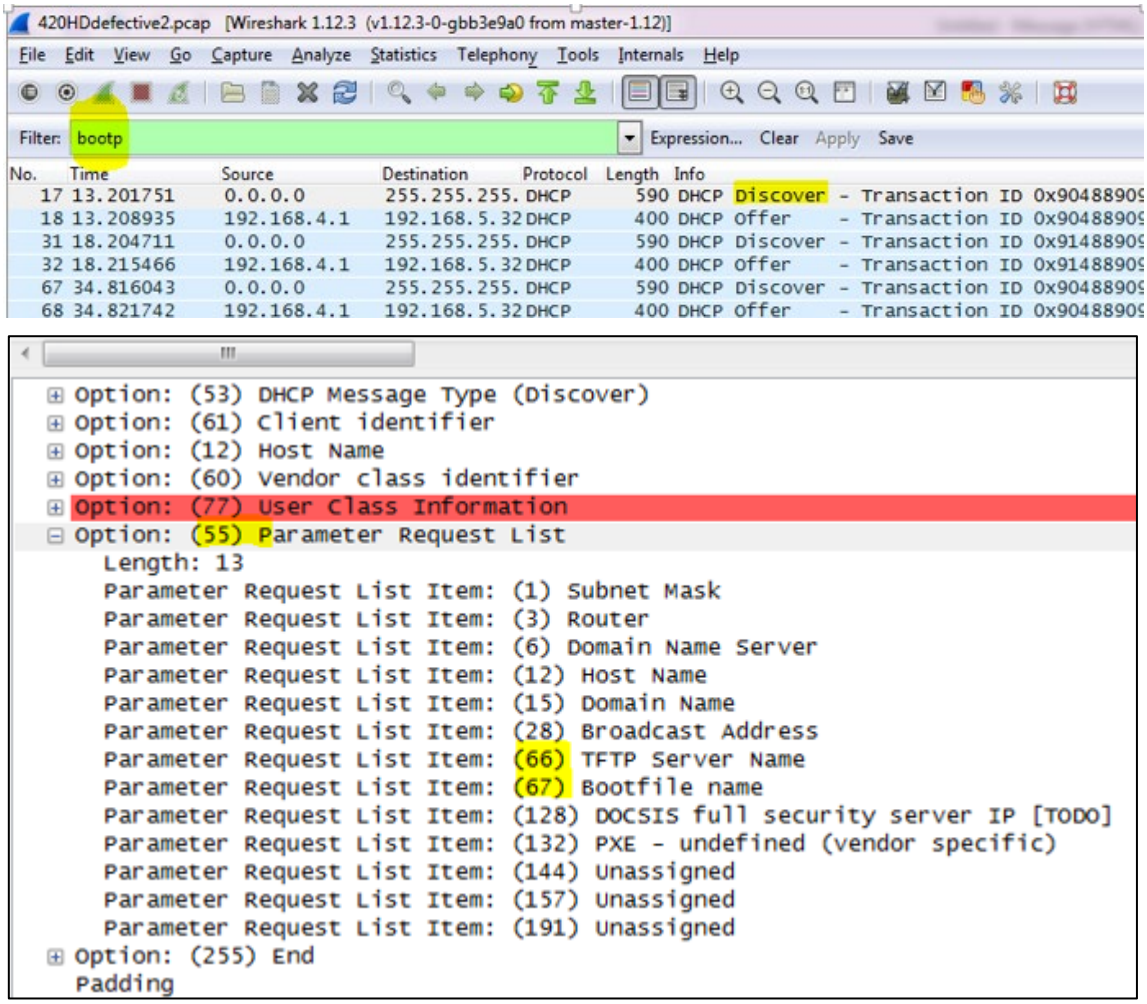
D.2 Verifying that the Phone is in Recovery Mode

Network administrators can verify that the phone is in recovery mode.

➢ **To verify that the phone is in recovery mode:**

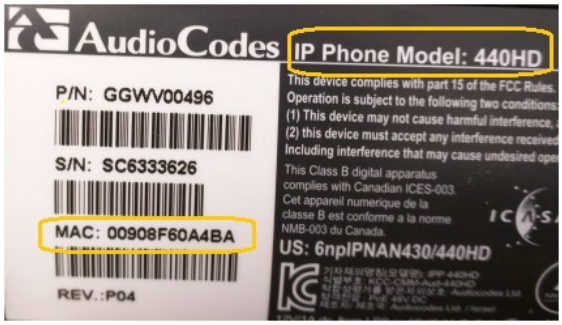
1. Connect the phone to the PC and run WireShark.
2. In WireShark, filter by **bootp** and then check if the phone is requesting Option 66 (TFTP Server) & Option 67 (Bootfile) under Option 55 in the 'DHCP Discover' message, as shown in the figures below.

Figure D-2: Verifying Recovery Mode in Wireshark



3. Make sure that the source Ethernet MAC address is the same as that labeled on the base of the phone. For example:

Figure D-3: Source Ethernet MAC Address in Wireshark Identical to Phone Base's



D.3 Recovering the Phone

The network administrator can recover the phone.

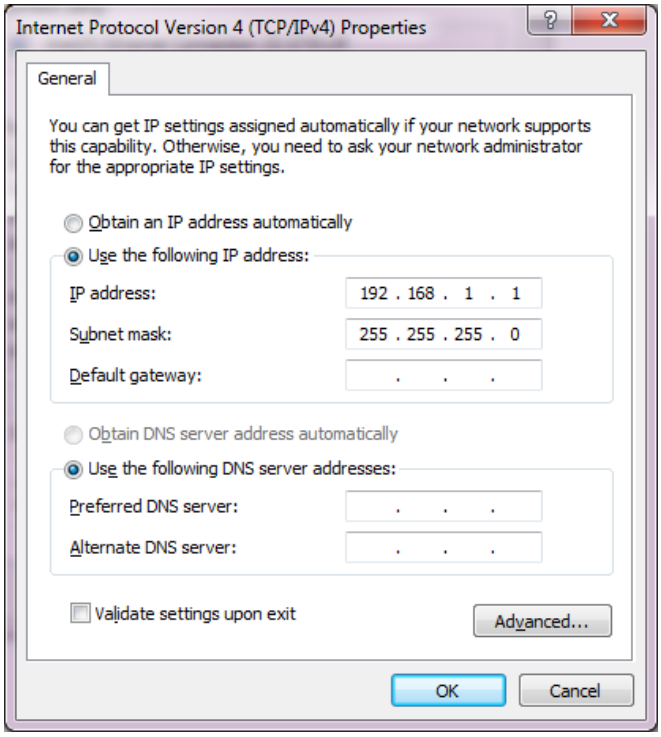
➢ **To recover the phone:**

1. Configure the PC NIC to which the phone is connected as follows:
   - IP address: **192.168.1.1**
   - Subnet mask: **255.255.255.0**

Figure D-4 below shows the configured settings.

2. Make sure the phone is directly connected (or via a network hub) to the PC LAN NIC.
3. Disable all other PC NICs (also wireless NICs).

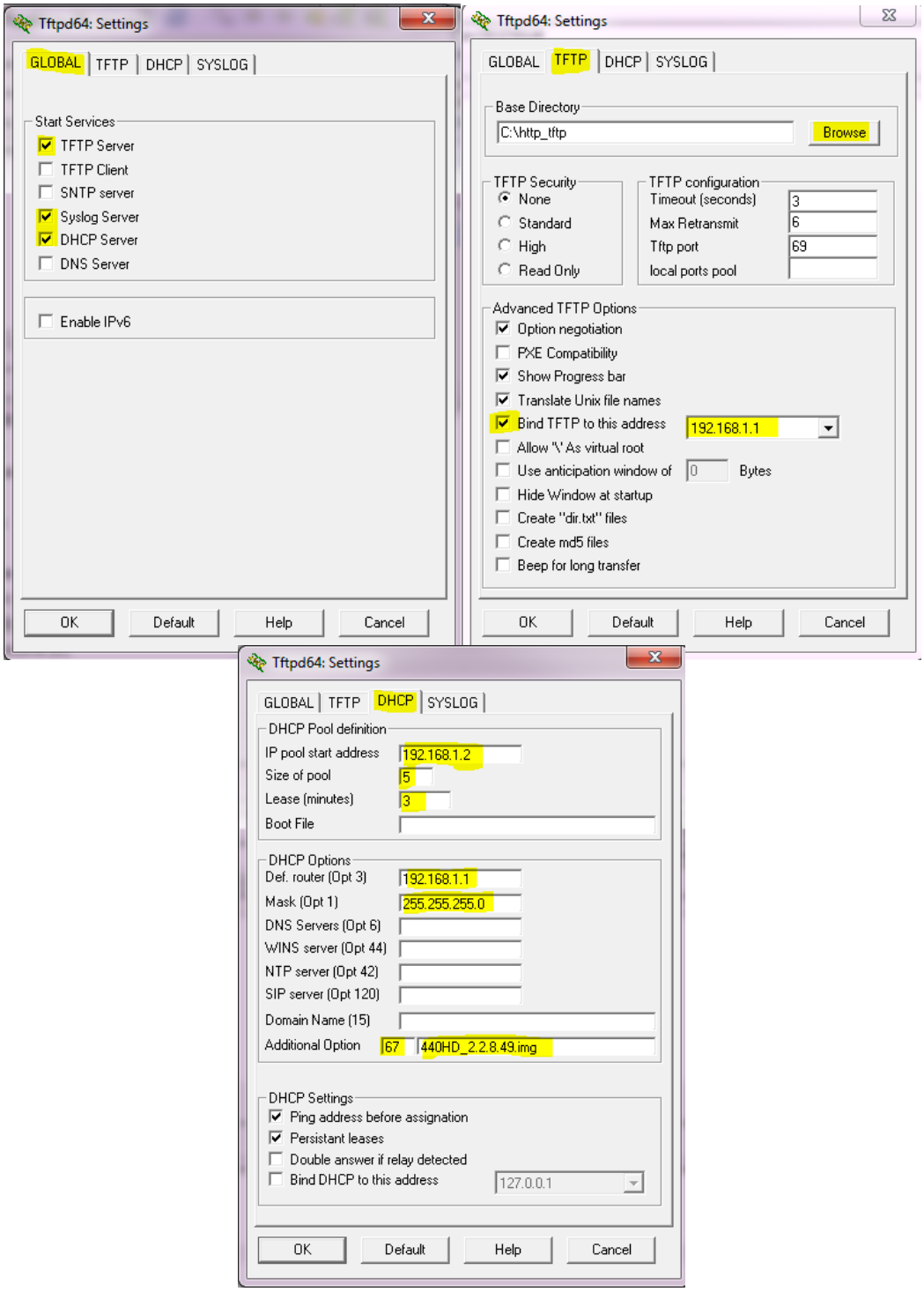
Figure D-4: Recovering the Phone - Configure the PC NIC to which the Phone is Connected



4. Download the following **tftpd64** freeware tool: http://tftpd32.jounin.net/tftpd32_download.html
5. Run the **tftpd64.exe** executable.
6. Click **Settings** and configure the following settings:

Table 10-3: Configuring tftpd64 Settings

Global	TFTP	DHCP
TFTP Server =option66	Browse to the directory in which the AudioCodes IP phone firmware is located.	IP pool start address: 192.168.1.2
Syslog Server	Bind the TFTP to IP address **192.168.1.1**	Size of pool: 5
DHCP Server	Leave all other options at their default.	Lease: 3
		Default.router: 192.168.1.1
		Mask: 255.255.255.0
		Additional Option: 67, FW_file_name.img



7. For **tftps64** to accept the new settings, close and open **tftpd64**.

After (1) **tftpd64** is restarted, (2) the phone is directly connected to the PC, and (3) the network settings referred to above are applied, the phone immediately gets the required options **66** and **67** and begins downloading the firmware. Verify that the phone is downloading the image file as shown in the next section.

D.4 Verifying that the Phone is Downloading the Image File

The network administrator can verify that the phone is downloading the firmware image file.

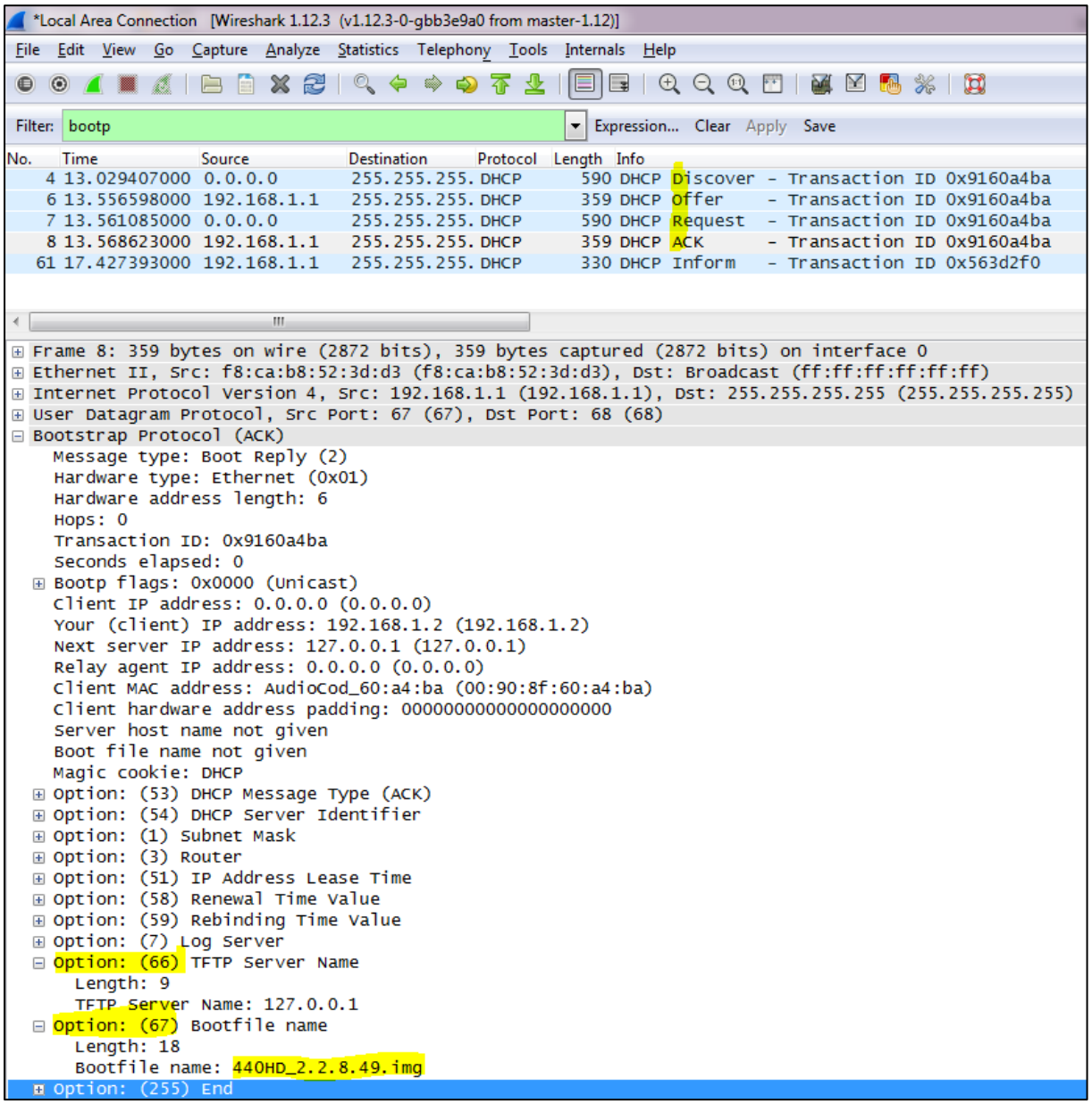
➢ **To verify that the phone is downloading the image file, use:**

- Wireshark -or-
- tftpd64 -or-
- the phone screen

D.4.1 Verifying Using Wireshark

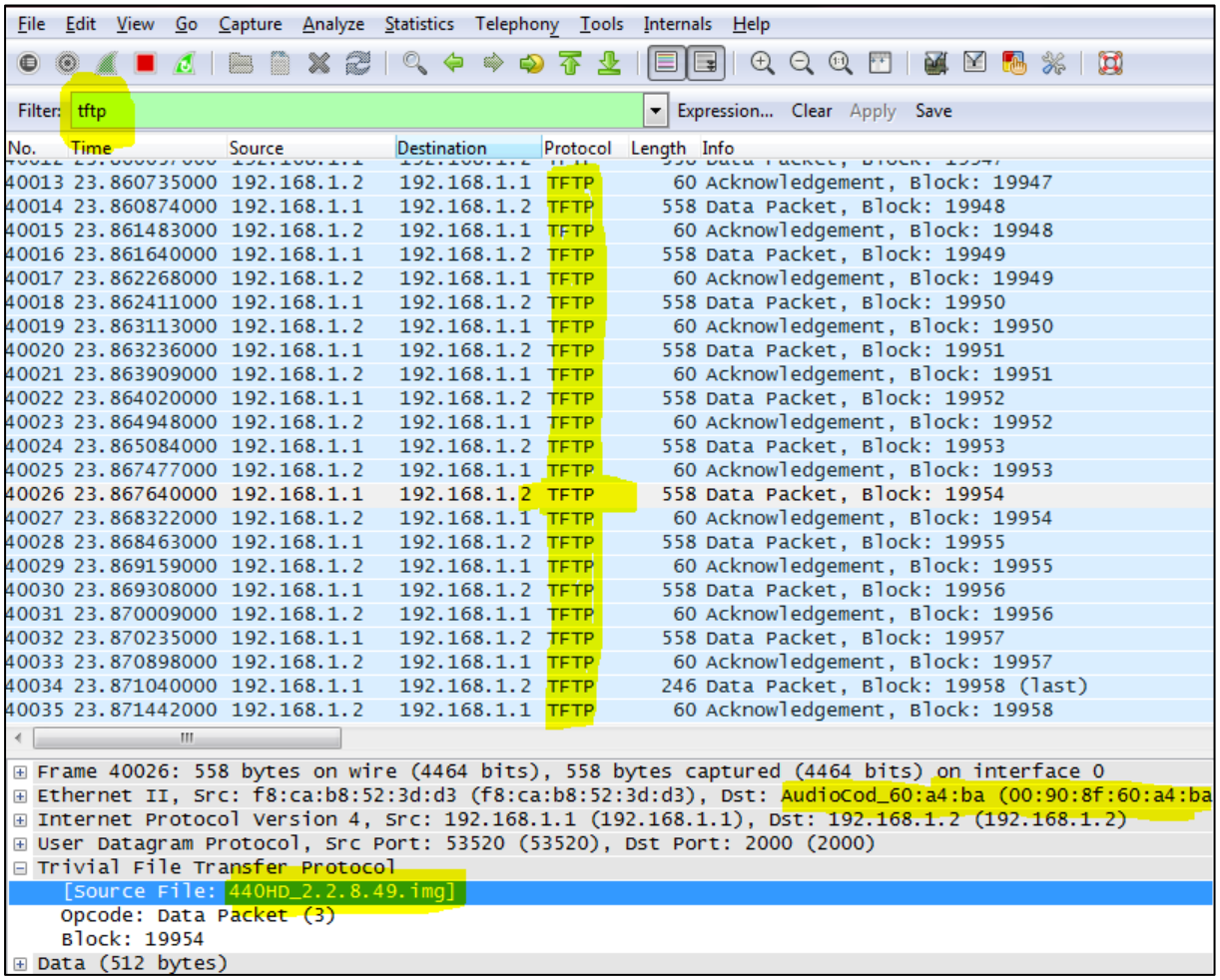
1. In Wireshark, verify that the four DHCP 'DORA' (**D**iscover; **O**ffer; **R**equest; **A**CK) steps are accomplished, as shown in the figure below.

Figure D-5: Verifying with Wireshark that the Phone is Downloading Phone .img File



2. Filter by **TFTP**, as shown in the figure below.

Figure D-6: Verifying .img File Download with Wireshark – Filtering by TFTP



D.4.2 Verifying Using tftpd64

In **tftpd64**, view the indications shown in the figures below.

Figure D-7: Verifying .img File Download using tftpd64

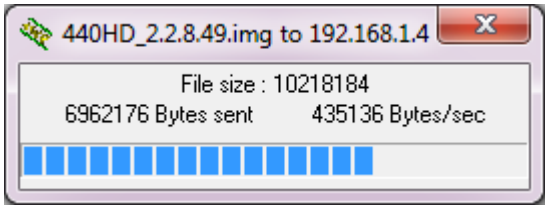
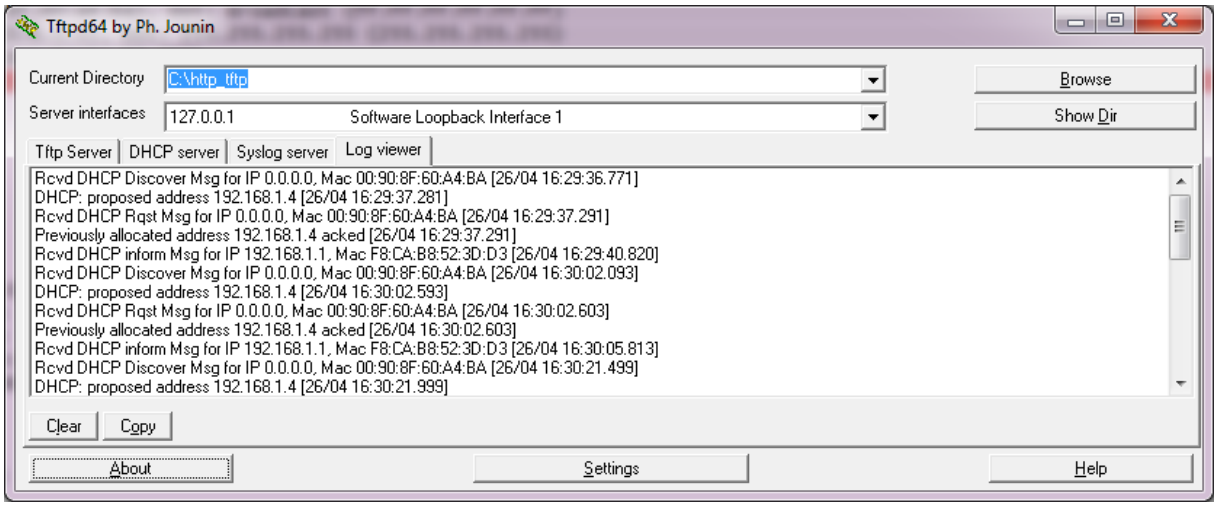


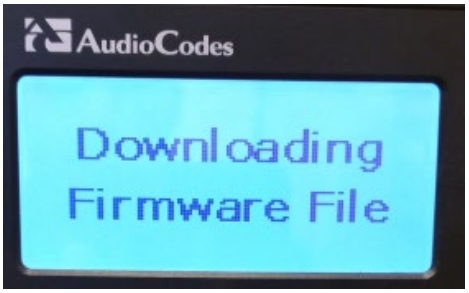
Figure D-8: Verifying .img File Download using tftpd64



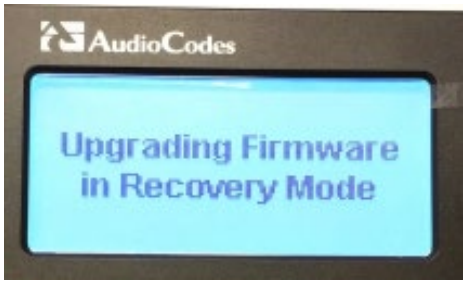
D.4.3 Verifying on the Phone

In tftpd64, view the indications shown in the figures below.

Figure D-9: Verifying .img File Download on the Phone



Important: Do not unplug / power-off the phone while the screen displays the message shown below.



You can disconnect the phone from the PC and connect to the network LAN *only after the firmware upgrade finishes*, that is, after the phone's screen displays the following:

Discovering CDP…Discovering LLDP…Acquiring IP…

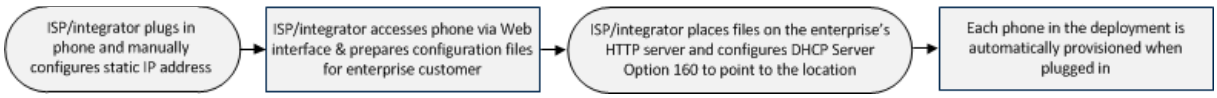
The phone is now up, functioning, and ready to be provisioned.

This page is intentionally left blank.

E Deploying AudioCodes IP Phones - Use Case

In a typical scenario, the ISP/integrator:

1. Connects an out-of-the-box phone to the LAN and power supply and manually configures **Static IP** address on the phone.
2. Prepares configuration files for the enterprise customer.
3. Places the configuration files on the enterprise customer's HTTP server and configures DHCP Server Option 160 to point to the location.



E.1 Preparing Configuration (cfg) Files for the Enterprise Customer

The network administrator can prepare configuration files for the enterprise.

➢ **To prepare configuration files for the enterprise customer:**

1. Save the phone's default configuration to file (see the next section E.2 below)
2. Prepare a global.cfg configuration file (see Section E.1.2)
3. Generate private.cfg configuration files (see Section E.1.3)

E.1.1 Saving the Phone's Default Configuration to File

An out-of-the box phone's default (factory) configuration can be saved to file. This will be the baseline on which to prepare a global.cfg configuration file afterwards.

➢ **To save a phone's default configuration to a file:**

1. Open a Web browser and connect to the phone's Web interface using **http://<phone's IP address>**
2. In the Web interface home page (System Information), make sure the phone is running the latest firmware version. If not, obtain a new firmware file from AudioCodes and load it to the phone using the Web interface's Firmware Upgrade page (**Management** tab > **Manual Update** > **Firmware Upgrade**).
3. In the Web interface's Restore Defaults page, restore the default configuration (**Management** > **Administration** > **Restore Defaults**) in case the default configuration was modified.
4. In the Web interface's Configuration File page, save the default configuration to a file (**Management** > **Manual Update** > **Configuration File**).

E.1.2 Preparing a global.cfg Configuration File

The network administrator can prepare a configuration file containing *parameter settings common to all users* in the enterprise. The file can be named *global.cfg*.

➢ **To prepare a global.cfg configuration file:**

1. Change the default settings of *parameters unique to your enterprise customers* (e.g., Language).
2. Make sure the phone functions as expected.
3. Save the modified configuration parameter settings to a file. Name the file global.cfg.

E.1.3 Generating MAC-specific <private>.cfg Configuration Files

MAC-specific <private>.cfg configuration files that will contain *parameter settings that are unique to each user* in the enterprise can be generated.

➢ **To generate MAC-specific <private>.cfg configuration files:**

1. Prepare a csv file (see the next section below)
2. Prepare a template file (see Section E.1.3.2)
3. Automatically generate MAC-specific <private>.cfg configuration files using VoIProvision tool (see Section E.1.3.3)

E.1.3.1 Preparing a csv File

Export a csv file from your enterprise customer's IP-PBX or another database. The csv file must list the phones in the enterprise, including MAC address, user name, extension ID, and password of each phone. The csv file contains the tagged records for each phone. When opened as a text file, the csv file looks like this:

```
mac,name,id,password
00908F123456,Jonathan,4071,12345
00908F123457,David,4418,12345
```

Table E-1: CSV File Description

mac	name	id	password
00908F123456	Jonathan	4071	12345
00908F123457	David	4418	12345

Note:

- The first line of the csv file contains the list of tags (e.g., mac,name,id).
- The remainder of the csv file contains a line record per cfg file (e.g., 00908f112233,4071,Eitan).
- There is no restriction on the format of the tags (e.g., tag or @tag@).

E.1.3.2 Preparing a Template File

This section shows ISPs/integrators how to prepare a template file.

Example of a template file:

```
system/type=445HD
voip/line/0/enabled=1
voip/line/0/id=id
voip/line/0/auth_name=name
voip/line/0/auth_password=password
include global.cfg
```

Define in the template file parameter settings *unique to each user*. Parameter settings unique to each user are typically:

- Line Settings
- Personal Settings
- Phone Directory

Note that the template file contains tags [ ]. The csv file that you prepared previously contains the values for these tags. You'll later use AudioCodes' VoIProvision tool to read the template file, replace the tags with values pulled from the csv file, and automatically generate MAC-specific <private>.cfg configuration files.

Note also that the template file contains **include** functions to link to other files. In the example above, the function **include global.cfg** pulls all parameter settings common to all users from the global.cfg file you prepared previously.

You can include links to specific configuration files, for example:

```
system/type=445HD
include 445HD_<MAC>_voip.cfg
include vlan_conf.cfg
include network_conf.cfg
include provisioning_conf.cfg
```

You can also include URL paths to files in other locations (FTP, TFTP, HTTP, or HTTPS), for example:

```
system/type=445HD
include http://10.10.10.10/445HD_<MAC>_voip.cfg
include https://remote-pc/vlan_conf.cfg
include tftp://10.10.10.10/445HD_<MAC>_network.cfg
include ftp://remote-pc/provisioning_conf.cfg
```

Note: If no URL is provided in the template file, the files are retrieved according to the provisioning information (e.g., DHCP Option 160 or 66/67).

E.1.3.3 Using AudioCodes' VoIProvision Tool

Multiple MAC-specific <private>.cfg files can be automatically generated using AudioCodes' VoIProvision tool. The tool generates a separate cfg file for each phone in the enterprise.

➢ **To automatically generate MAC-specific <private>.cfg files:**

1. Place AudioCodes' VoIProvision tool (VoIProvision.exe) in a folder on your pc.
2. Place the global.cfg configuration file that you prepared, together with the csv file and the template file, in the same folder.
3. Run the VoIProvision exe; the tool automatically generates the <private>.cfg files.

```
USAGE: VoIProvision <csv file><template file><.cfg file>
```

Note: AudioCodes' VoIProvision tool can run on both Linux and Windows platforms. The tool initially parses the csv file to generate the list of tags. The tool then reads each line record of values in the csv file and for each line record, does this:

- Parses the line record to create a list of values
- Opens the template file
- Generates the cfg file name and creates a new cfg file
- Reads the template file, associates the mapped tags with actual values from the csv file, and writes the result to the cfg file
- Closes the cfg file and template file

Example of an automatically generated MAC-specific file:

```
system/type=445HD
voip/line/0/enabled=1
voip/line/0/id=56832432
voip/line/0/auth_name=3423fdwer2tre
voip/line/0/auth_password=123456
include global.cfg
```

The generated configuration (cfg) files use a similar format to the template file only the tags are replaced with the values read by the VoIProvision tool from the csv file. The tag in the csv file which defines the MAC address is used as the cfg file name.

E.1.3.3.1 Creating Manually a <private>.cfg Configuration File

Network administrators can manually create a <private>.cfg configuration file using a standard ASCII, text-based program such as Notepad. The file name must be the phone's MAC address: **<phone's MAC address>.cfg**. The syntax of the configuration file is as follows:

```
<parameter name>=<value>
```

Ensure that:

- No spaces are on either side of the equals (=) sign
- Each parameter is on a new line

Below is an example of part of a configuration file:

```
system/type=440HD
voip/line/0/enabled=1
voip/line/0/id=1234
voip/line/0/description=440HD
voip/line/0/auth_name=1234
voip/line/0/auth_password=4321
```

E.2 Preparing the DHCP Server to Automatically Provision Phones

➢ **To prepare the DHCP server:**

- Configure DHCP OPTION 160 on the DHCP server. Point the DHCP server to the URL of the configuration files on the HTTP server.
  Use the string <MAC>
  For example: **http://192.168.2.1/;440HD_<MAC>_conf.cfg**

E.3 Making Sure Phones are Correctly Provisioned

➢ **To make sure the phones are correctly provisioned:**

1. Connect one of the phones to the IP network and power supply.
2. Follow the status displayed on the screen. Make sure the phone received an IP address and is upgrading the configuration.
3. The phone reboots with the new configuration.
4. Make sure that all functionalities are functioning flawlessly, e.g., that the phone can make VoIP calls.

This page is intentionally left blank.

F Supported SIP RFCs and Headers

The following is a list of supported SIP RFCs and methods you can use for the phone.

Table F-1: Supported IETF RFCs

RFC Number	RFC Title
RFC 2327	SDP
RFC 2617	HTTP Authentication: Basic and Digest Access Authentication
RFC 2782	A DNS RR for specifying the location of services
RFC 2833	Telephone event
RFC 3261	SIP
RFC 3262	Reliability of Provisional Responses in SIP
RFC 3263	Locating SIP Servers
RFC 3264	Offer/Answer Model
RFC 3265	(SIP)-Specific Event Notification
RFC 3310	Hypertext Transfer Protocol (HTTP) Digest Authentication Using Authentication and Key Agreement (AKA)
RFC 3326 (Partially Supported)	Reason header
RFC 3389	RTP Payload for Comfort Noise
RFC 3515	Refer Method
RFC 3605	RTCP attribute in SDP
RFC 3611	RTP Control Protocol Extended Reports (RTCP XR)
RFC 3665	SIP Basic Call Flow Examples
RFC 3711	The Secure Real-time Transport Protocol (SRTP)
RFC 3725	Third Party Call Control
RFC 3842	MWI
RFC 3891	"Replaces" Header
RFC 3892(Sections 2.1-2.3 and 3 are supported)	The SIP Referred-By Mechanism
RFC 3960(Partially Supported)	Early Media and Ringing Tone Generation in SIP (partial compliance)
RFC 3966	The tel URI for Telephone Numbers
RFC 4028(Partially Supported)	Session Timers in the Session Initiation Protocol
RFC 4240	Basic Network Media Services with SIP - NetAnn
RFC 6035	RTCP XR information publishing for Quality of Experience server monitoring.
draft-ietf-sip-privacy-04.txt (Partially Supported)	SIP Extensions for Network-Asserted Caller Identity using Remote-Party-ID header
draft-ietf-sipping-cc-transfer-05	Call Transfer

RFC Number	RFC Title
draft-ietf-sipping-realtimefax-01	SIP Support for Real-time Fax: Call Flow Examples
draft-choudhuri-sip-info-digit-00	SIP INFO method for DTMF digit transport and collection
draft-mahy-sipping-signaled-digits-01	Signaled Telephony Events in the Session Initiation Protocol

Note: The following SIP features are not supported:

- Preconditions (RFC 3312)
- SDP - Simple Capability Declaration (RFC 3407)
- S/MIME
- Outbound, Managing Client-Initiated Connections (RFC 5626)
- SNMP SIP MIB (RFC 4780)
- SIP Compression – RFC 5049 (SigComp)
- ICE (RFC 5245)
- Connected Identity (RFC 4474)

F.1 SIP Compliance Tables

The SIP device complies with RFC 3261, as shown in the following subsections.

F.1.1 SIP Methods

The device supports the following SIP Methods:

Table F-2: Supported SIP Methods

Method	Supported	Comments
INVITE	Yes	
ACK	Yes	
BYE	Yes	
CANCEL	Yes	
REGISTER	Yes	Send only
REFER	Yes	Inside and outside of a dialog
NOTIFY	Yes	
INFO	Yes	
OPTIONS	Yes	
PRACK	Yes	
PUBLISH	Yes	Send only
SUBSCRIBE	Yes	

F.1.2 SIP Headers

The device supports the following SIP Headers:

Table F-3: Supported SIP Headers

Header Field	Supported
Accept	Yes
Alert-Info	Yes
Allow	Yes
Authorization	Yes
Call-ID	Yes
Call-Info	Yes
Contact	Yes
Content-Length	Yes
Content-Type	Yes
Cseq	Yes
Date	Yes
Diversion	Yes
Encryption	No
Expires	Yes
Fax	Yes
From	Yes
History-Info	Yes
Join	Yes
Max-Forwards	Yes
MIN-SE	Yes
P-Asserted-Identity	Yes
P-Preferred-Identity	Yes
Proxy- Authenticate	Yes
Proxy- Authorization	Yes
Prack	Yes
Record- Route	Yes
Refer-To	Yes
Referred-By	Yes
Replaces	Yes
Remote-Party-ID	Yes
Retry-After	Yes
Route	Yes

Header Field	Supported
Session-Expires	Yes
Supported	Yes
Timestamp	Yes
To	Yes
Unsupported	Yes
User- Agent	Yes
Via	Yes
Voicemail	Yes
Warning	Yes
WWW- Authenticate	Yes

This page is intentionally left blank.

G RTCP-XR Parameters

The following table lists the RTCP-XR parameters that may be reported to the QoE server.

Table G-1: RTCP-XR Parameters

Group	Metric Name
General	Start Timestamp
	Stop Timestamp
	Call-ID
	Local Address (IP, Port & SSRC)
	Remote Address (IP, Port & SSRC)
Session Description	Payload Type
	Payload Description
	Sample Rate
	Frame Duration
	Frame Octets
	Frames per Packets
	Packet Loss Concealment
	Silence Suppression State
Jitter Buffer	Jitter Buffer Adaptive
	Jitter Buffer Rate
	Jitter Buffer Nominal
	Jitter Buffer Max
	Jitter Buffer Abs Max
Packet Loss	Network Packet Loss Rate
	Jitter Buffer Discard Rate
Burst Gap Loss	Burst Loss Density
	Burst Duration
	Gap Loss Density
	Gap Duration
	Minimum Gap Threshold
Delay	Round Trip Delay
	End System Delay
	One Way Delay
	Interarrival Jitter
	Min Absolute Jitter
	Signal
	Signal Level
	Noise Level
Quality Estimates	Listening Quality R
	RLQ Est. Algorithm
	Conversational Quality R
	RCQ Est. Algorithm

Group	Metric Name
	MOS-LQ
	MOS-LQ Est. Algorithm
	MOS-CQ
	MOS-CQ Est. Algorithm
	QoE Est. Algorithm

H Example SIP - PUBLISH Message

This appendix displays an example SIP PUBLISH message extracted from RFC 6035. RTCP-XR values are found under the message body.

```
PUBLISH sip:collector@example.org SIP/2.0
       Via: SIP/2.0/UDP pc22.example.org;branch=z9hG4bK3343d7
       Max-Forwards: 70
       To: <sip:proxy@example.org>
       From: Alice <sip:alice@example.org>;tag=a3343df32
       Call-ID: 1890463548
       CSeq: 4331 PUBLISH
       Allow: INVITE, ACK, CANCEL, OPTIONS, BYE, REFER,
        SUBSCRIBE, NOTIFY
       Event: vq-rtcpxr
       Accept: application/sdp, message/sipfrag
       Content-Type: application/vq-rtcpxr
       Content-Length: ...

       VQSessionReport: CallTerm
       CallID: 6dg37f1890463
       LocalID: Alice <sip:alice@example.org>
       RemoteID: Bill <sip:bill@example.net>
       OrigID: Alice <sip:alice@example.org>
       LocalGroup: example-phone-55671
       RemoteGroup: example-gateway-09871
       LocalAddr: IP=10.10.1.100 PORT=5000 SSRC=1a3b5c7d
       LocalMAC: 00:1f:5b:cc:21:0f
       RemoteAddr:IP=11.1.1.150 PORT=5002 SSRC=0x2468abcd
       LocalMetrics:
       Timestamps:START=2004-10-10T18:23:43Z STOP=2004-10-
01T18:26:02Z
       SessionDesc:PT=18 PD=G729 SR=8000 FD=20 FO=20 FPP=2 PPS=50
                   PLC=3 SSUP=on
       JitterBuffer:JBA=3 JBR=2 JBN=40 JBM=80 JBX=120
       PacketLoss:NLR=5.0 JDR=2.0
       Delay:RTD=200 IAJ=2
       QualityEst:RLQ=90 RCQ=85 MOSLQ=4.2 MOSCQ=4.3
         QoEEstAlg=P.564
       RemoteMetrics:
       Timestamps:START=2004-10-10T18:23:43Z STOP=2004-10-
01T18:26:02Z
       SessionDesc:PT=18 PD=G729 SR=8000 FD=20 FO=20 FPP=2 PPS=50
                   PLC=3 SSUP=on
       JitterBuffer:JBA=3 JBR=2 JBN=40 JBM=80 JBX=120
       PacketLoss:NLR=5.0 JDR=2.0
       Delay:RTD=200 IAJ=2
       QualityEst:RLQ=90 RCQ=85 MOSLQ=4.3 MOSCQ=4.2 QoEEstAlg=P.564
       DialogID:1890463548@alice.example.org;to-tag=8472761;
       from-tag=9123dh311
```

Note: Remote Metrics are not supported in this version.

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: https://www.audiocodes.com/corporate/offices-worldwide
Website: https://www.audiocodes.com/

Document #: LTRT-11975