

# 425HD, 445HD, and C450HD IP Phones

Version 3.5.4



---

## Table of Contents

---

|  |           |
|--|-----------|
| <b>Notice .....</b>  | <b>ix</b> |
| Security Vulnerabilities .....   | ix        |
| WEEE EU Directive .....  | ix        |
| Customer Support .....   | ix        |
| Stay in the Loop with AudioCodes .....                                 | ix        |
| Abbreviations and Terminology.....                                     | ix        |
| Related Documentation.....   | x         |
| Document Revision Record.....  | x         |
| Documentation Feedback.....  | x         |
| <b>1 Introduction .....</b>  | <b>1</b>  |
| <b>2 Configuration Methods.....</b>                                    | <b>2</b>  |
| 2.1 Phone Screen.....  | 2         |
| 2.1.1 Administration Menu .....  | 2         |
| 2.1.2 Configuring User Login Credentials.....                          | 3         |
| 2.2 Configuration File .....   | 3         |
| 2.2.1 File Syntax.....   | 3         |
| 2.2.2 Linking Multiple Files.....                                      | 4         |
| 2.2.3 Using the Encryption Tool .....                                  | 4         |
| 2.2.3.1 Encrypting Configuration Files.....                            | 4         |
| 2.2.3.2 Encrypting Passwords in the Configuration File.....            | 5         |
| 2.3 Device Manager.....  | 5         |
| 2.4 AudioCodes Device Manager Validation.....                          | 6         |
| 2.4.1 Introduction .....   | 6         |
| 2.4.2 Prerequisites .....  | 6         |
| 2.4.3 Overview.....  | 6         |
| 2.4.4 Existing Root CA Files in IP Phone .....                         | 7         |
| 2.4.5 Certification Details Dialog .....                               | 8         |
| <b>3 Configuring Automatic Provisioning.....</b>                       | <b>9</b>  |
| 3.1 Setting up Network for Auto Provisioning .....                     | 10        |
| 3.1.1 Provisioning Hunt Order .....                                    | 10        |
| 3.1.2 Dynamic URL Provisioning.....                                    | 10        |
| 3.1.2.1 Provisioning using DHCP Option 160 .....                       | 13        |
| 3.1.2.2 Configuring Automatic Provisioning by DHCP Server .....        | 13        |
| 3.1.2.3 Provisioning using the User-Class Option .....                 | 13        |
| 3.1.2.4 Redirect Server .....  | 21        |
| 3.1.3 Static URL Provisioning.....                                     | 22        |
| 3.2 Firmware Header–Based Download Optimization for HTTP Servers ..... | 23        |
| 3.3 Verifying Firmware Signature .....                                 | 23        |

---

|          |  |           |
|----------|--|-----------|
| <b>4</b> | <b>Configuring Networking.....</b>   | <b>24</b> |
| 4.1      | Configuring Date and Time Manually .....   | 24        |
| 4.1.1    | Configuring Daylight Saving Time .....   | 25        |
| 4.1.2    | Configuring the NTP Server .....   | 28        |
| 4.1.3    | Configuring NTP Server via DHCP .....  | 29        |
| 4.2      | Configuring IP Network Settings .....  | 29        |
| 4.2.1    | Configuring Static IP Address.....   | 29        |
| 4.2.1.1  | Configuring Static IP Address on the Phone.....  | 30        |
| 4.2.1.2  | Configuring IP Network Settings.....   | 30        |
| 4.2.2    | Configuring Partial DHCP .....   | 31        |
| 4.3      | Configuring LAN and PC Port Settings.....  | 32        |
| 4.4      | Configuring VLAN Settings .....  | 33        |
| 4.4.1    | Configuring Manual or Automatic VLAN Assignment .....  | 34        |
| 4.4.1.1  | Configuring Manual VLAN Assignment to the Phone.....   | 34        |
| 4.4.1.2  | Configuring Automatic VLAN Assignment to the Phone .....   | 34        |
| 4.4.1.3  | Configuring VLAN via DHCP Provisioning Path .....  | 34        |
| 4.4.2    | Wi-Fi Capability .....   | 34        |
| <b>5</b> | <b>Configuring VoIP Settings .....</b>   | <b>36</b> |
| 5.1      | Configuring SIP Settings.....  | 36        |
| 5.1.1    | Configuring General SIP Settings .....   | 36        |
| 5.1.2    | Configuring Proxy and Registration .....   | 40        |
| 5.1.2.1  | Configuring Proxy Redundancy .....   | 42        |
| 5.1.2.2  | Device Registration Failover/Failback.....   | 44        |
| 5.1.2.3  | Preventing Unregistering after Changing Settings and Reloading .....   | 45        |
| 5.1.2.4  | Prevent SIP UNSUBSCRIBE on VoIP Reload Upon Failover/Failback .....  | 46        |
| 5.1.2.5  | Redundancy Failback when DNS Resolution of the SIP Proxy Server's FQDN<br>returns a Different IP Address ..... | 46        |
| 5.1.3    | Configuring a Line.....  | 47        |
| 5.1.3.1  | Assigning Programmable Keys to Lines (SIP Accounts) .....  | 48        |
| 5.1.4    | Configuring Shared Call Appearance.....  | 49        |
| 5.1.5    | Configuring SIP Timers.....  | 49        |
| 5.1.6    | Configuring SIP QoS.....   | 51        |
| 5.1.7    | Configuring SIP Reject Code .....  | 51        |
| 5.2      | Configuring Dialing .....  | 51        |
| 5.2.1    | Configuring General Dialing Parameters .....   | 52        |
| 5.2.2    | Configuring Dial Tones.....  | 53        |
| 5.2.3    | Configuring DTMF .....   | 54        |
| 5.2.4    | Configuring Digit Maps and Dial Plans .....  | 54        |
| 5.2.5    | Configuring Headset LED to Stay On .....   | 56        |
| 5.2.6    | Configuring Default Audio Device.....  | 57        |
| 5.3      | Configuring Ring Tones.....  | 58        |
| 5.3.1    | Configuring Distinctive Ring Tones .....   | 58        |

|          |   |    |
|----------|---|----|
| 5.3.1.1  | Example of Configuring a Distinctive Ring .....   | 58 |
| 5.3.2    | Configuring CPT Regional Settings .....   | 59 |
| 5.3.3    | Uploading Ring Tones .....  | 61 |
| 5.3.4    | Configuring the Phone to play Fast Busy Tone if Automatically Disconnected on Remote Side ..... | 62 |
| 5.4      | Configuring Media Settings .....  | 63 |
| 5.4.1    | Configuring Media Streaming .....   | 63 |
| 5.4.2    | Configuring RTP Port Range and Payload Type .....   | 64 |
| 5.4.3    | Configuring RTP QoS.....  | 64 |
| 5.4.4    | Configuring Codecs.....   | 65 |
| 5.5      | Configuring Voice Settings.....   | 66 |
| 5.5.1    | Configuring Gain Control .....  | 66 |
| 5.5.2    | Configuring Jitter Buffer .....   | 66 |
| 5.5.3    | Configuring Silence Compression .....   | 66 |
| 5.6      | Configuring Extension Lines.....  | 67 |
| 5.7      | Enabling Phone Lock.....  | 68 |
| 5.8      | Configuring Supplementary Services .....  | 69 |
| 5.8.1    | Selecting the Application Server .....  | 69 |
| 5.8.2    | Configuring Call Waiting .....  | 70 |
| 5.8.3    | Configuring Call Forwarding .....   | 71 |
| 5.8.4    | Configuring a Conference .....  | 73 |
| 5.8.5    | Configuring Automatic Dialing.....  | 73 |
| 5.8.6    | Configuring Automatic Answer.....   | 74 |
| 5.8.7    | Configuring Do Not Disturb (DnD) .....  | 76 |
| 5.8.8    | Configuring Call Pick Up.....   | 77 |
| 5.8.9    | Configuring Message Waiting Indication .....  | 78 |
| 5.8.10   | Configuring Busy Lamp Field.....  | 79 |
| 5.8.11   | Configuring a Tone to Alert to Long Hold.....   | 79 |
| 5.8.12   | Configuring Onhook Disconnect when Held.....  | 80 |
| 5.8.13   | Configuring the Ringer's Default Audio Device .....   | 81 |
| 5.8.14   | Allowing an Incoming Call when the Phone is Locked .....  | 81 |
| 5.8.15   | Configuring Call Transfer .....   | 82 |
| 5.8.15.1 | Configuring the TRANSFER Key to Perform Consultative Transfer .....                             | 82 |
| 5.8.16   | Configuring a Speed Dial.....   | 83 |
| 5.8.17   | Configuring Call Park .....   | 84 |
| 5.9      | Configuring Volume Levels .....   | 85 |
| 5.9.1    | Configuring Gain Control .....  | 85 |
| 5.9.2    | Configuring Tone Volume.....  | 85 |
| 5.9.3    | Configuring Ringer Volume.....  | 85 |
| 5.9.4    | Configuring Speaker Volume .....  | 86 |
| 5.9.5    | Configuring Handset Volume.....   | 88 |
| 5.9.6    | Configuring Headset Volume .....  | 90 |

|          |   |            |
|----------|---|------------|
| 5.10     | Prioritized of Incoming Calls Displayed .....                                 | 91         |
| 5.11     | UI to Return to Idle Screen Timeout .....                                     | 91         |
| 5.12     | Call No Answer Timeout .....  | 92         |
| 5.13     | Emergency Calls.....  | 92         |
| <b>6</b> | <b>Configuring Phone Settings.....</b>  | <b>93</b>  |
| 6.1      | Configuring the Phone Directory .....   | 93         |
| 6.1.1    | Configuring the LDAP-based Corporate Directory .....                          | 93         |
| 6.1.2    | Loading a Text-based Corporate Directory File .....                           | 94         |
| 6.2      | Configuring Keys .....  | 96         |
| 6.2.1    | Configuring Function and Programmable Keys .....                              | 96         |
| 6.2.1.1  | Configuring a Configuration File for Speed Dials Only.....                    | 98         |
| 6.2.2    | Configuring Softkeys.....   | 98         |
| 6.2.2.1  | Disable New Call Softkey in Incoming Call screen .....                        | 99         |
| 6.2.2.2  | Configuring Programmable Softkeys (PSKs).....                                 | 100        |
| 6.2.2.3  | Configuring a PSK to Allow Paging during an Ongoing Call   Call Hold .....    | 102        |
| 6.2.2.4  | Configuring a PSK for a Customized UI Experience .....                        | 103        |
| 6.3      | Configuring Font Size of Functional Keys .....                                | 103        |
| 6.4      | Enhanced Sidecar Management and LED Customization .....                       | 104        |
| 6.5      | Ability to Disable/Enable Features and Keys on IP Phone .....                 | 105        |
| 6.5.1    | Enabling/Disabling Display of DTMF Digits.....                                | 105        |
| 6.6      | Configuring Paging.....   | 107        |
| 6.6.1    | Configuring Barge-in.....   | 108        |
| 6.7      | Configuring Phone Screen Settings.....  | 109        |
| 6.8      | C450HD Screen Saver Configuration .....                                       | 111        |
| 6.9      | Configuring Personal Settings.....  | 112        |
| 6.9.1    | Configuring Language.....   | 112        |
| <b>7</b> | <b>Configuring Security .....</b>   | <b>113</b> |
| 7.1      | Implementing X.509 Authentication.....  | 113        |
| 7.1.1    | Factory-Set Certificates and AudioCodes Trusted Root CA.....                  | 114        |
| 7.1.2    | User-Generated Certificates .....   | 114        |
| 7.1.3    | External Trusted Root CAs .....   | 115        |
| 7.1.3.1  | Supported Trusted Root CAs .....  | 116        |
| 7.2      | Loading a Certificate.....  | 117        |
| 7.2.1    | Loading Trusted Root CA Certificate Using Configuration File .....            | 117        |
| 7.2.2    | Loading the Client Certificate to the Phone .....                             | 117        |
| 7.2.2.1  | Enabling Server-side Authentication (Mutual Authentication).....              | 119        |
| 7.2.3    | Generating a Certificate Signing Request.....                                 | 119        |
| 7.2.4    | CA File Configuration.....  | 120        |
| 7.3      | Simple Certificate Enrollment Protocol (SCEP) .....                           | 120        |
| 7.4      | Configuring SIP TLS .....   | 122        |
| 7.4.1    | Server Certificate Validation for Secured HTTPS Communications over SSL ..... | 122        |

|           |  |            |
|-----------|--|------------|
| 7.5       | Configuring 802.1x.....  | 123        |
| 7.5.1     | Configuring 802.1x in the Phone Screen .....                     | 124        |
| 7.5.1.1   | Configuring EAP-MD5 Mode .....                                   | 124        |
| 7.5.1.2   | Configuring EAP-TLS Mode.....                                    | 124        |
| 7.5.2     | Configuring 802.1x .....   | 125        |
| 7.5.2.1   | Configuring EAP MD5 Mode.....                                    | 125        |
| 7.6       | Configuring SRTP .....   | 126        |
| 7.7       | Configuring HTTP/S Login .....                                   | 128        |
| <b>8</b>  | <b>Maintaining an IP Telephony Network.....</b>                  | <b>129</b> |
| 8.1       | Changing Administrator Login Credentials .....                   | 129        |
| 8.2       | Administration.....  | 129        |
| 8.2.1     | Managing Users .....   | 129        |
| 8.2.2     | Allowing / Disallowing Management via the Web Interface.....     | 130        |
| 8.3       | Restoring Phone Defaults .....                                   | 130        |
| 8.3.1     | Restoring Factory Defaults from the Phone's Screen .....         | 130        |
| 8.4       | Restarting the Phone .....                                       | 130        |
| 8.5       | Enabling Remote Management .....                                 | 132        |
| 8.5.1     | Enabling Telnet Access .....                                     | 132        |
| 8.5.2     | Enabling SSH Access .....  | 132        |
| <b>9</b>  | <b>Monitoring the Network.....</b>                               | <b>133</b> |
| 9.1       | Determining Network Status .....                                 | 133        |
| 9.1.1     | Determining LAN Status .....                                     | 133        |
| 9.1.2     | Determining Port Mode Status .....                               | 133        |
| 9.1.3     | Determining 802.1x Status .....                                  | 134        |
| 9.2       | Determining VoIP Status.....                                     | 134        |
| 9.2.1     | Viewing Line Status .....  | 134        |
| 9.2.2     | Determining Memory Status .....                                  | 135        |
| 9.3       | Viewing Call History .....                                       | 136        |
| 9.3.1     | Exclude 'feature code dialing' from Call Log .....               | 136        |
| 9.3.2     | Disable the presence SUBSCRIBE message (for Call Log lists)..... | 137        |
| 9.4       | Accessing System Information.....                                | 138        |
| 9.5       | Monitoring Quality of Experience.....                            | 139        |
| 9.6       | Configuring Remote Voice Quality Monitoring.....                 | 140        |
| 9.6.1     | Configuring RTCP Extended Report.....                            | 140        |
| 9.6.2     | Configuring Voice Quality Monitoring .....                       | 141        |
| <b>10</b> | <b>Diagnosing Problems &amp; Troubleshooting .....</b>           | <b>142</b> |
| 10.1      | Monitor the Status of Software Modules .....                     | 142        |
| 10.2      | Configuring System Logging (Syslog) .....                        | 142        |
| 10.3      | Viewing Error Messages Displayed in the Phone Screen .....       | 145        |
| 10.4      | Debugging using Packet Recording Parameters .....                | 146        |

|          |  |            |
|----------|--|------------|
| 10.5     | Activating Core Dump.....  | 148        |
| 10.6     | Configuring Port Mirroring .....   | 149        |
| 10.7     | Supporting Transition Recording .....  | 149        |
| <b>A</b> | <b>Accessing Office 365 Exchange Services .....</b>                                | <b>150</b> |
| <b>B</b> | <b>Installing the Expansion Module .....</b>                                       | <b>151</b> |
| B.1      | Installation Procedure .....   | 151        |
| B.1.1    | Step 1: Place Phone and Module on a Table .....                                    | 151        |
| B.1.2    | Step 2: Invert and Unscrew Three Screws.....                                       | 152        |
| B.1.3    | Step 3: Remove Rubber Cover and Connect .....                                      | 153        |
| B.1.4    | Step 4: Attach the Panel .....   | 153        |
| B.1.5    | Step 5: Secure the Side Panel .....  | 154        |
| B.1.6    | Step 6: Secure the Connection of the Two Units.....                                | 154        |
| B.1.7    | Step 7: Mount Phone on Base Stand, Expansion Module on Base Stand .....            | 155        |
| <b>C</b> | <b>Configuring Phones in Server-Specific Deployments .....</b>                     | <b>156</b> |
| C.1      | BroadSoft's BroadWorks.....  | 156        |
| C.1.1    | Configuring BLF .....  | 157        |
| C.1.2    | Configuring Call Forwarding .....  | 158        |
| C.1.2.1  | From the Phone .....   | 158        |
| C.1.2.2  | From BroadSoft's BroadWorks .....  | 158        |
| C.1.3    | Configuring DnD .....  | 159        |
| C.1.4    | Configuring FKS .....  | 160        |
| C.1.5    | Configuring Phones to Connect to Xsi using HTTP/S Authentication .....             | 160        |
| C.1.6    | Configuring Shared Call Appearance.....  | 163        |
| C.1.7    | Setting up a Remote Conference .....   | 167        |
| C.2      | Asterisk.....  | 168        |
| C.2.1    | Configuring BLF .....  | 168        |
| C.3      | OpenSpace SIP Proxy .....  | 168        |
| <b>D</b> | <b>AudioCodes' HTTPS Redirect Server .....</b>                                     | <b>170</b> |
| <b>E</b> | <b>Recovering the Phone.....</b>   | <b>172</b> |
| E.1      | Identifying that the Phone is in Recovery Mode.....                                | 172        |
| E.2      | Verifying that the Phone is in Recovery Mode .....                                 | 173        |
| E.3      | Recovering the Phone.....  | 174        |
| E.4      | Verifying that the Phone is Downloading the Image File .....                       | 176        |
| E.4.1    | Verifying that the Phone is Downloading the Image File Using Wireshark .....       | 176        |
| E.4.2    | Verifying That the Phone Is Downloading the Image File Using TFTP Server App ..... | 178        |
| E.4.3    | Verifying That the Phone Is Downloading the Image File Using the Phone.....        | 179        |
| <b>F</b> | <b>Supported SIP RFCs and Headers .....</b>  | <b>180</b> |
| F.1      | SIP Compliance Tables .....  | 181        |
| F.1.1    | SIP Methods .....  | 181        |
| F.1.2    | SIP Headers .....  | 182        |

|          |   |            |
|----------|---|------------|
| <b>G</b> | <b>RTCP-XR Parameters.....</b>                              | <b>184</b> |
| <b>H</b> | <b>Example SIP - PUBLISH Message .....</b>                  | <b>186</b> |
| <b>I</b> | <b>Intrado ERS Location Information Service (HELD).....</b> | <b>187</b> |



## 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: January-13-2026

## Security Vulnerabilities

All security vulnerabilities should be reported to [vulnerability@audiocodes.com](mailto:vulnerability@audiocodes.com).

## WEEE EU Directive

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

## Customer Support

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

## Stay in the Loop with AudioCodes



## Abbreviations and Terminology

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

## Related Documentation

| Document Name  |
|--|
| 445HD IP Phone User's Manual - Generic SIP               |
| 445HD IP Phone Quick Guide - Generic SIP                 |
| C450HD IP Phone User's Manual - Generic SIP              |
| C450HD IP Phone Quick Guide - Generic SIP                |
| Device Manager Pro Administrator's Manual                |
| One Voice Operations Center IOM Manual                   |
| One Voice Operations Center (OVOC) User's Manual         |
| Live Platform Guide for AudioCodes Professional Services |
| Live Platform Service Providers User's Manual            |
| Live Platform Channel Resellers User's Manual            |
| Live Platform End Customers User's Manual                |

## Document Revision Record

| LTRT  | Description  |
|-------|--|
| 11978 | This is the initial release of the document.   |
| 09965 | 425HD added and IP Phones no longer supported removed.   |
| 09993 | Added configuration parameters to General SIP Settings, SIP Proxy Server Redundancy, and Emergency Calls. Added Call History capabilities and a new feature to monitor the status of software modules. |

## Documentation Feedback

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

# 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' high-end phone models 425HD, 445HD, and C450HD.



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*.

## 2 Configuration Methods

The phones support several 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** – 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.
- **Web interface** – The Web interface is intended for lab and debugging purposes only. See section 8.2.2 [Allowing / Disallowing Management via the Web Interface](#) 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



- 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**.



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 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 1: User Name and Password Parameters**

| Parameter                | Description  |
|--------------------------|--|
| system/web_user_name     | The phone user name. Default: user.<br>Applies only to the Web interface.                            |
| system/web_user_password | The encrypted phone password. Default: 1234.<br>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=445HD
voip/line/0/enabled=1
voip/line/0/id=1234
voip/line/0/description=445HD
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=445HD
include 445HD_<MAC>_voip.cfg
include vlan_conf.cfg
include network_conf.cfg
include provisioning_conf.cfg
```



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 Using the Encryption Tool

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

### 2.2.3.1 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').

### 2.2.3.2 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="}
```



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.



- 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: 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.<br>Default: 60 minutes |
| ems_server/provisioning/url  | Defines the URL of the OVOC server, for example, <a href="http://10.1.8.23:8081">http://10.1.8.23:8081</a>   |
| 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:<br>{"Y6QYmP53BDkoTvuIFjEBuQ=="}   |

## 2.4 AudioCodes Device Manager Validation

### 2.4.1 Introduction

This section describes the configuration requirements of working with AudioCodes IP-Phone device series **Generic SIP** out of the box in secured environment.

The security process (SSL connection) starts with a phone request to the server, followed phone verification if the server can be trusted. During this process the server send his certificate to the phone and the phone verifies this certificate based on its pre burned trusted certificates list. TLS handshake is strict security.

A valid server cert defined if (1) the server's certificate chain is valid against a list of Trusted CAs (see appendix A) pre-installed on the phone, (2) the server's hostname is valid for each certificate in the chain (issuer field of the certificate should match subject field of the upper issuer in the chain certificate) and (3) the expiration date is valid.

### 2.4.2 Prerequisites

AudioCodes IP-Phone device with pre-installed trusted CAs

### 2.4.3 Overview

The device validates the AudioCodes Device Manager identity using known root CA:

The device is shipped with known Root CAs installed. (See Appendix B – AudioCodes Root) CA Certificate)

For the initial connection phase, the AudioCodes Device Manager should access the device using a known CA.

Once a successful secured connection has been established between the device and the Device Manager, the user can replace the root CA on the Device Manager and on the device and re-establish the connection leveraging any private root CA.

#### Backward compatibility is supported:

To implement backward compatibility, the configuration file parameter 'security/SSLCertificateErrorsMode' must be changed from the default to Ignore:

- SSLCertificateErrorsMode = **Disallow** (default)
- SSLCertificateErrorsMode = **Ignore** (allows backward compatibility though vulnerability will increase); the phone will proceed without checking the received certificates and without any notifications
- In case the server isn't signed by one of the root-CAs IP-Phone supports, it is recommended to:
- Download the needed root-CA via HTTP by IPP configuration using **security/ca\_certificate/<0-4>/uri**
- This way the user doesn't need to change security/SSLCertificateErrorsMode to IGNORE.
- Before upgrade to 3.5.4.x version download the root-CA using the secured connection https.



## 2.4.4 Existing Root CA Files in IP Phone

The following list are existing Root CA Files in IP Phone:

- CNNIC\_ROOT.cer
- Comodo\_AAA\_Certificate\_Services.cer
- COMODO\_Root\_CA.cer
- Cybetrust\_Baltimore\_CyberTrust\_Root.cer
- Cybetrust\_GlobalSign\_Root\_CA.cer
- Cybetrust\_GTE\_CyberTrust\_Global\_Root.cer
- DigiCert\_Cloud\_Services\_CA-1.cer
- DigiCertGlobalG2TLSRSASHA2562020CA1.cer
- DigiCertGlobalRootCA.cer
- DigiCertGlobalRootG2.cer
- DigiCertGlobalRootG3.cer
- DigiCert\_High\_Assurance\_EV\_Root\_CA.cer
- DigiCertSHA2SecureServerCA.cer
- DST\_Root\_CA\_X3.cer
- D-Trust\_Root\_Class\_3\_CA\_2\_2009.cer
- D-TRUST\_Root\_Class\_3\_CA\_2\_EV\_2009.cer
- Entrust\_Entrust.net\_Certification\_Authority\_2048.cer
- Entrust\_Root\_Certification\_Authority\_G2.cer
- GeoTrustEVRSA2018.cer
- GeoTrust\_GeoTrust\_Global\_CA.cer
- GlobalSign.cer
- Go\_Daddy\_Go\_Daddy\_Class\_2\_Certification\_Authority.cer
- Go\_Daddy\_Starfield\_Class\_2\_Certification\_Authority.cer
- isrgrootx1.pem.cer
- letsencryptauthorityx3.cer
- StartCom\_Certification\_Authority.cer
- thawte\_Primary\_Root\_CA\_G3.cer
- VeriSign\_Class\_2\_Public\_Primary\_Certification\_Authority.cer
- VeriSign\_Class\_3\_Public\_Primary\_Certification\_Authority.cer
- VeriSign\_Class\_3\_Public\_Primary\_Certification\_Authority\_G1.cer
- VeriSign\_Class\_3\_Public\_Primary\_Certification\_Authority\_G2.cer
- VeriSign\_Class\_3\_Public\_Primary\_Certification\_Authority\_G3.cer
- VeriSign\_Class\_3\_Public\_Primary\_Certification\_Authority\_G5.cer

## 2.4.5 Certification Details Dialog

Certificate Details for File 'New Text Document.cer'

Certificate Hierarchy:

- RootCA

Version: 3

Subject: CN=RootCA,O=ACL

Issuer: CN=RootCA,O=ACL

Serial Number: 0x1

Valid From: 1/1/2000 2:00:00 AM IST

Valid Until: 1/1/2030 2:00:00 AM IST

Public Key: RSA 2048 bits

Signature Algorithm: SHA256WITHRSA

Fingerprint: MD5 AD:F7:94:DE:B3:1D:F0:3F:74:3B:C5:42:34:51:19

Import Extensions PEM ASN.1

OK

```
-----BEGIN CERTIFICATE-----
MIIDMTCCAhmGAWIBAgIBATANBgkqhkiG9w0BAQsFADAfMQwwCgYDVQQKEwNBQ0wx
DzANBgNVBAMTB1Jvb3RDQTAeFw0wMDAxMDEwMDAwMDBaFw0zMDEwMDAwMDAwMDBa
MB8xDDAKBgNVBAoTAFQDTDEPMA0GA1UEAxMGUm9vdENBMIIBIjANBgkqhkiG9w0B
AQEFAAOCAQ8AMIIBCgKCAQEA6GK495KUCXAm/UE17G4/cjnZN4LNaxYEYzbfZL0a
EhgSKYt/LQ+iUcDhojsneusNgrcGkpwKklKsGsvGWmSRNULV01CW+TX2VJN73+hh
V0uzhyOIYAUhbDaoqNM6Kp5b7sJ1ew4Ig9kfd/ma9Cz15koESLlw/inLj/r+rD96
mUcPElWrKspv7Qy4I14fsK/yMARixRopTL1munVVPpSFM9Jh8IY3JHyr5CQJXKKs
EhGAJsnHaRqsR2Su3X/WtslgEF+cvP34pxhlhFL29nMfnaFATSS3rgGaFlSv11ZS
esLMqkWjp9cqGYrvt7K61sYnvMMb+o/KbWqVokXb+Fr7bwIDAQABo3gwdjAMBgNV
HRMEBTADAQH/MB0GA1UdDgQWBBDXySn9hz15lDraZ+iXddZGReB+zBHBgNVHSME
QDA+gBQDXySn9hz15lDraZ+iXddZGReB+6EjpCEwHzEMMAoGA1UEChMDQUNMMQ8w
DQYDVQQDEwZSb290Q0GCAQEwDQYJKoZIhvcNAQELBQADggEBAI0rUywommWWJnH3
JOOfKiS3+VnX5hJITZymvWanMXUz/6FonHccPXEBYTrUYwhiWx3dwELAFXDFKkxMp
0KKWZ4F39cAOLRjqhzya+xUeeJ9HQZCXyAJ6XgvTfN2BtyZk9Ma8WG+H1hNvvTZY
QLbWsjQdu4eFniEufeYDkeljQ6800LwM1Flc59hMQCeJTEnRx4HdJbJV86klgBUE
A7fJT1ePrRnXNDRz6QtADWoX3OmN7Meqen/roTwvLpEP22nYwvB28dq3JetlQKwu
XC4gwI/o8K2wo3pySLU9Y/vanXXCr0/en5l3RDz1YpYWmQwHA8jJIu8rxdhr+VNQ
Zv6R/Ys=
-----END CERTIFICATE-----
```

## 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.



- In the DHCP Discover message, the phone publishes its model name in Option fields 60 and 77 (e.g. 445HD). 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).



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).



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
3. AudioCodes Redirect server (see Section 3.1.2.4)

### 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: DHCP Automatic Provisioning Parameters**

| Parameter           | Description  |
|---------------------|--|
| provisioning/method | Defines the provisioning method: <ul style="list-style-type: none"><li>■ Disable - Automatic update is disabled. The phone does not attempt to upgrade its firmware and configuration</li><li>■ Dynamic - DHCP Options (Dynamic URL) (default) - Using DHCP option 160 as well as option 66/67 for provisioning</li><li>■ Static URL - Using Static URL for provisioning</li></ul> |

| Parameter                     | Description  |
|-------------------------------|--|
| provisioning/url_option_value | <p>Determines the DHCP option number to be used for receiving the URL for provisioning.</p> <p>The default value is 160.</p> <p>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.</p> <p>The following syntax is available for DHCP option 160:</p> <ul style="list-style-type: none"> <li>■ &lt;protocol&gt;://&lt;server IP address or host name&gt;</li> <li>■ &lt;protocol&gt;://&lt;server IP address or host name&gt;/&lt;firmware file name&gt;</li> <li>■ &lt;protocol&gt;://&lt;server IP address or host name&gt;/&lt;firmware file name&gt;;&lt;configuration file name&gt;</li> <li>■ &lt;protocol&gt;://&lt;server IP address or host name&gt;/;&lt;configuration file name&gt;</li> </ul> <p>Where &lt;protocol&gt; can be one of the following: <b>ftp</b>, <b>tftp</b>, <b>http</b> or <b>https</b>.</p> <p>For example:</p> <ul style="list-style-type: none"> <li>■ <b>ftp://192.168.2.1</b> – retrieved firmware file is <i>445HD.img</i> and the configuration file name is &lt;MAC address&gt;.cfg. For example, 001122334455.cfg</li> <li>■ <b>tftp://192.168.2.1/different_firmware_name.img</b> - retrieved firmware file is <i>Different_Firmware_Name.img</i> and the configuration file name is &lt;MAC address&gt;.cfg. For example, 001122334455.cfg</li> <li>■ <b>http://192.168.2.1/different_firmware_name.img;</b> &lt;MODEL&gt;_&lt;MAC&gt;_conf.cfg - retrieved firmware file is <i>different_firmware_name.img</i> and the configuration file name is &lt;Model type&gt;_&lt;MAC address&gt;_conf.cfg. For example, <b>445HD_001122334455_conf.cfg</b></li> <li>■ <b>https://192.168.2.1/;&lt;MODEL&gt;_&lt;MAC&gt;_conf.cfg</b> - if the model is 445HD, the retrieved firmware file is <i>445HD.img</i> and the configuration file name is <i>445HD_&lt;MAC Address&gt;_conf.cfg</i>. For example, <i>445HD_001122334455_conf.cfg</i></li> </ul> <p>The following syntax is available for DHCP Options 66/67:</p> <ul style="list-style-type: none"> <li>■ Option 66 must be a valid IP address or host name of a TFTP server only.</li> <li>■ Option 67 must be the firmware name.</li> </ul> <p>If Option 67 is absent, the phone requests for the 445HD.img image file.</p> <p>For example:</p> <ul style="list-style-type: none"> <li>■ <b>Option 66:</b> 192.168.2.1 or myTFTPServer</li> <li>■ <b>Option 67:</b> 445HD_3.4.4.img</li> </ul> <p><b>Note:</b></p> <ul style="list-style-type: none"> <li>■ This parameter is applicable only when <b>method</b> is configured to <b>Dynamic</b>.</li> <li>■ It is recommended to leave the parameter at its default value to avoid conflict with other DHCP options settings.</li> </ul> |

| Parameter                                 | Description   |
|---|---|
| provisioning/random_provisioning_time     | <p>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 <b>random_provisioning_time</b> and performs the check only after the random time.</p> <p>The valid range is 0-65535. The default value is 120.</p>  |
| provisioning/period/type                  | <p>Defines the period type for automatic provisioning:</p> <ul style="list-style-type: none"> <li>■ <b>every5minutes</b> Minimum definable time. Sets the interval at every five minutes.</li> <li>■ <b>every15minutes</b> Sets the interval at every five minutes.</li> <li>■ <b>hourly</b> - Sets an interval in hours.</li> <li>■ <b>daily</b> (default) - Sets an hour in the day.</li> <li>■ <b>weekly</b> - Sets a day in the week and an hour in the day.</li> <li>■ <b>powerup</b> Irrespective of what value is defined, the phone always checks on powerup, but if <b>powerup</b> is defined, the phone will check <i>only</i> on powerup.</li> </ul> |
| provisioning/period/hourly/hours_interval | <p>The interval in hours for automatically checking for new firmware and configuration files.</p> <p>The valid range is 1 to 168. The default is 24.</p> <p><b>Note:</b> This parameter is applicable only when <b>type</b> is configured to <b>hourly</b>.</p>   |
| provisioning/period/daily/time            | <p>The hour in the day for automatically checking for new firmware and configuration files.</p> <p>The format of this value is <b>hh:mm</b>, where <b>hh</b> is hour and <b>mm</b> is minutes. For example, <b>00:30</b>.</p> <p>The default time is <b>00:00</b>.</p> <p><b>Note:</b> This parameter is applicable only when <b>type</b> is configured to <b>daily</b>.</p>  |
| provisioning/period/weekly/day            | <p>The day in the week for automatically checking for new firmware and configuration files.</p> <ul style="list-style-type: none"> <li>■ Sunday (default)</li> <li>■ Monday</li> <li>■ Tuesday</li> <li>■ Wednesday</li> <li>■ Thursday</li> <li>■ Friday</li> <li>■ Saturday</li> </ul> <p><b>Note:</b> This parameter is applicable only when <b>type</b> is configured to <b>weekly</b>.</p>   |
| provisioning/period/weekly/time           | <p>The hour in the day for automatically checking for new firmware and configuration files.</p> <p>The format of this value is: <b>hh:mm</b>, where <b>hh</b> is hour and <b>mm</b> is minutes. For example: <b>00:30</b></p> <p>The default time is <b>00:00</b>.</p> <p><b>Note:</b> This parameter is applicable only when <b>type</b> is configured to <b>weekly</b>.</p>   |

### 3.1.2.1 Provisioning using DHCP Option 160

Phones can get a provisioning URL from DHCP Option 160 [support pending for 66/67]. Option 160 has the highest priority, followed by Option 66/67.

### 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.



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 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.

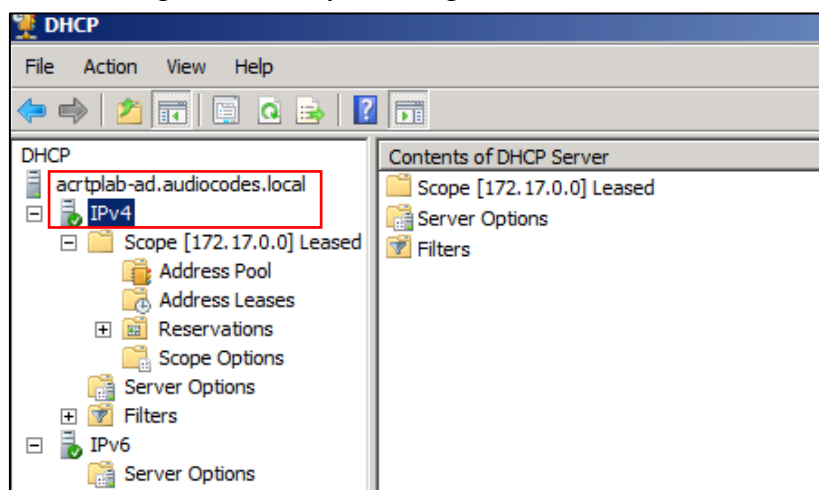
**To configure provisioning of AudioCodes phones using the User-Class Option:**

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



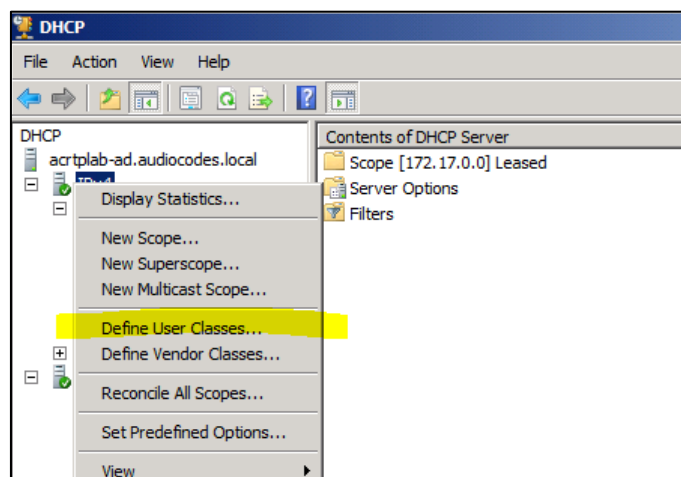
- The examples below show DHCP server **acrtplab-ad.audiocodes.local**
- The examples below show IPv4 addresses

**Figure 1: DHCP Options Assigned to IPv4 Addresses**



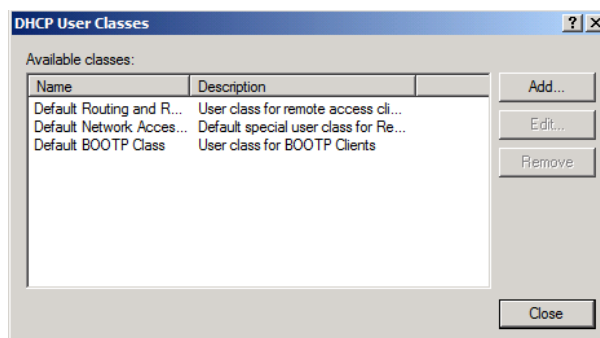
3. Define a separate **User Class** for each phone deployed. Right-click the **IPv4** server icon and from the popup menu, select **Define User Classes...**

Figure 2: Defining User Classes



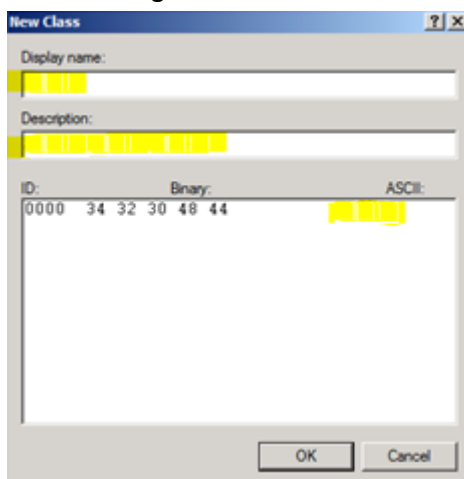
The DHCP User Classes screen opens.

Figure 3: DHCP User Classes



4. Click the **Add...** button.

Figure 4: New Class



5. 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 5: Packet Bytes Window [Illustrative Purposes Only]

| No. | Time                          | Source      | Destination     | DPort | Protocol | Length | Info                                      |
|-----|-------------------------------|-------------|-----------------|-------|----------|--------|---|
| 140 | 2015-06-01 15:58:12.413405000 | 0.0.0.0     | 255.255.255.255 | 67    | DHCP     | 590    | DHCP Discover - Transaction ID 0x42c58f43 |
| 141 | 2015-06-01 15:58:12.436583000 | 10.7.14.252 | 10.7.14.82      | 68    | DHCP     | 363    | DHCP Offer - Transaction ID 0x42c58f43    |
| 142 | 2015-06-01 15:58:12.441290000 | 10.7.14.251 | 10.7.14.82      | 68    | DHCP     | 363    | DHCP Offer - Transaction ID 0x42c58f43    |
| 143 | 2015-06-01 15:58:12.473426000 | 0.0.0.0     | 255.255.255.255 | 67    | DHCP     | 590    | DHCP Request - Transaction ID 0x42c58f43  |
| 144 | 2015-06-01 15:58:12.485196000 | 10.7.14.251 | 10.7.14.82      | 68    | DHCP     | 363    | DHCP ACK - Transaction ID 0x42c58f43      |
| 145 | 2015-06-01 15:58:12.486309000 | 10.7.14.252 | 10.7.14.82      | 68    | DHCP     | 363    | DHCP ACK - Transaction ID 0x42c58f43      |

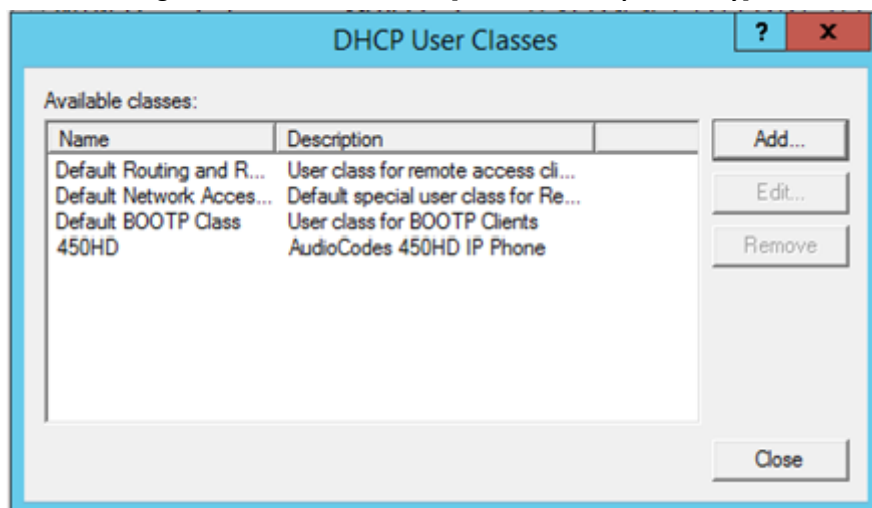
|  |  |
|--|--|
| Host Name: 420HD-00908F3BC566  |  |
| Option: (60) Vendor class identifier                                     |  |
| Length: 11   |  |
| Vendor class identifier: CPE-OCPHONE                                     |  |
| Option: (77) User Class Information                                      |  |
| Length: 5  |  |
| Instance of User Class: [0]  |  |
| User Class Length: 52  |  |
| [Expert Info (Error/Protocol): User Class Information: malformed option] |  |
| [User Class Information: malformed option]                               |  |
| [Severity level: Error]  |  |
| [Group: Protocol]  |  |
| Option: (55) Parameter Request List                                      |  |

|      |   |                  |
|------|---|------------------|
| 0140 | 4f 43 50 48 4f 4e 45 d0 05 34 32 30 48 44 37 0f | OCPHONEM : 420HD |
| 0150 | 01 02 03 04 06 0c 0f 1c 28 29 2a 2b 42 43 a0 ff | (*)fBC           |
| 0160 | 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00    |                  |
| 0170 | 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00    |                  |
| 0180 | 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00    |                  |
| 0190 | 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00    |                  |
| 01a0 | 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00    |                  |

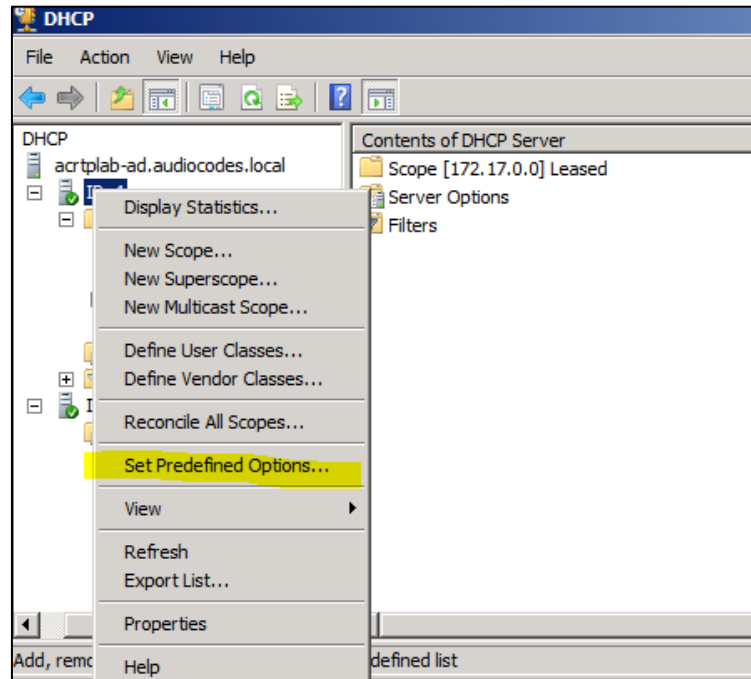
- Make sure one DHCP User Class entry exists for each AudioCodes phone model deployed in the enterprise.

Figure 6: DHCP User Classes [Illustrative Purposes Only]



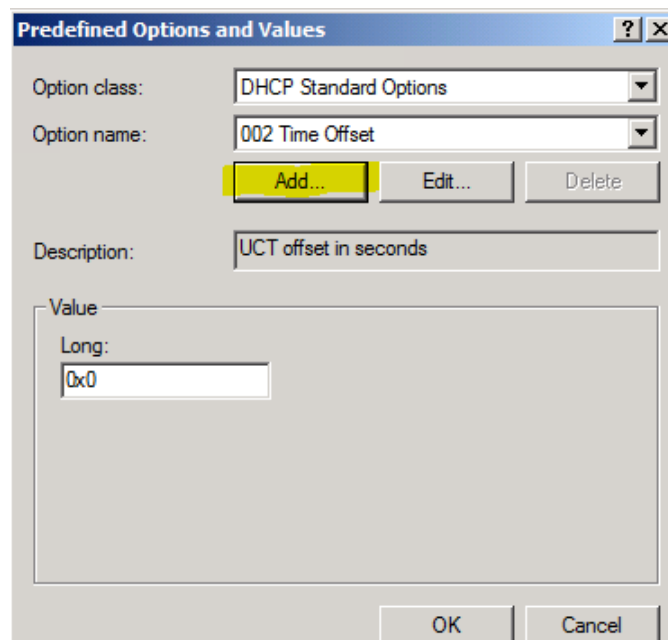
- Configure Scope Option 160. This is not a *standard* Scope Option, so it needs to be created. To create it on the server, select the IP version (**IPv4**) and select **Set Predefined Options...**

Figure 7: Set Predefined Options



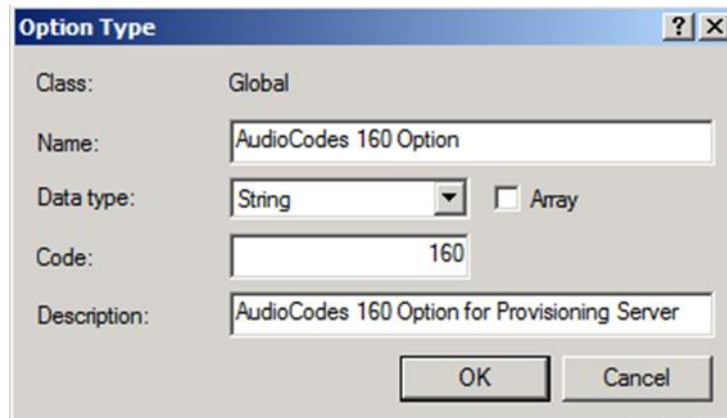
8. From the 'Option class' dropdown, select **DHCP Standard Options**, and then click the **Add...** button.

Figure 8: Predefined Options and Values



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

Figure 9: Option Type – Add AudioCodes 160 Option



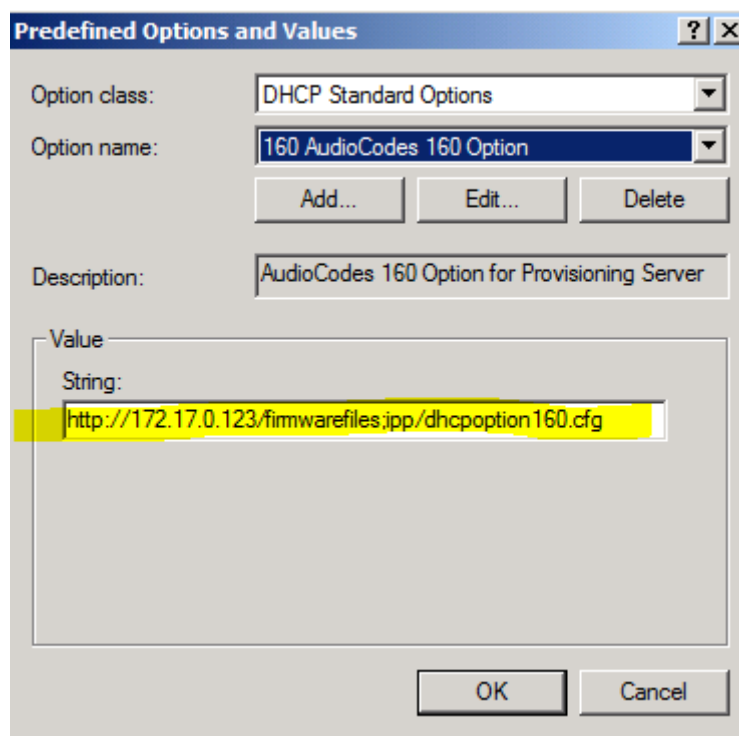
The 'Option Type' dialog box is shown with the following fields:

- Class:** Global
- Name:** AudioCodes 160 Option
- Data type:** String (selected from a dropdown menu, with an unchecked 'Array' checkbox next to it)
- Code:** 160
- Description:** AudioCodes 160 Option for Provisioning Server

Buttons at the bottom: OK, Cancel.

10. 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 10: Predefined Options and Values – Add OVOC Server Location



The 'Predefined Options and Values' dialog box is shown with the following fields and buttons:

- Option class:** DHCP Standard Options (selected from a dropdown menu)
- Option name:** 160 AudioCodes 160 Option (selected from a dropdown menu)
- Buttons:** Add..., Edit..., Delete
- Description:** AudioCodes 160 Option for Provisioning Server
- Value section:**
  - String:** `http://172.17.0.123/firmwarefiles;ipp/dhcpoption160.cfg` (highlighted in yellow)

Buttons at the bottom: OK, Cancel.



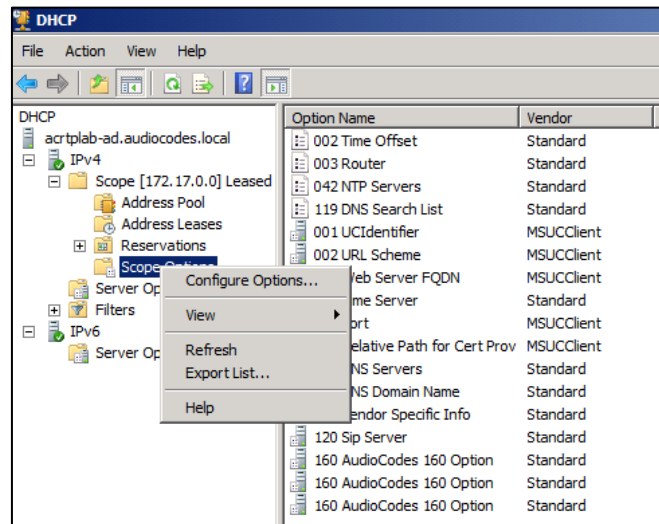
Make sure you defined in the enterprise's DHCP server **`http://<OVOC server IP address>/firmwarefiles;ipp/dhcpoption160.cfg`** for DHCP Option 160.

11. 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

12. 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.

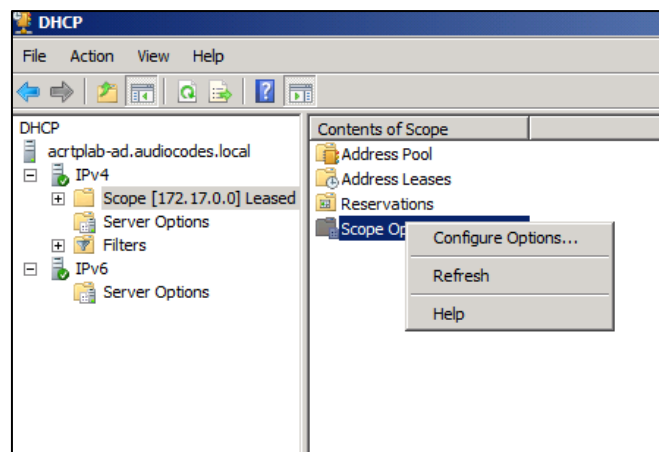
Figure 11: 'Scope Leased' Folder - Configure Options



-OR-

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

Figure 12: Configure Options 1

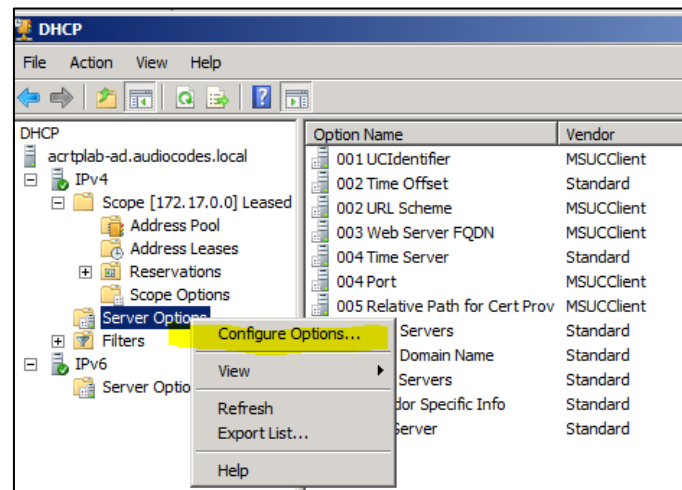


-OR-

Server Option

13. 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...**

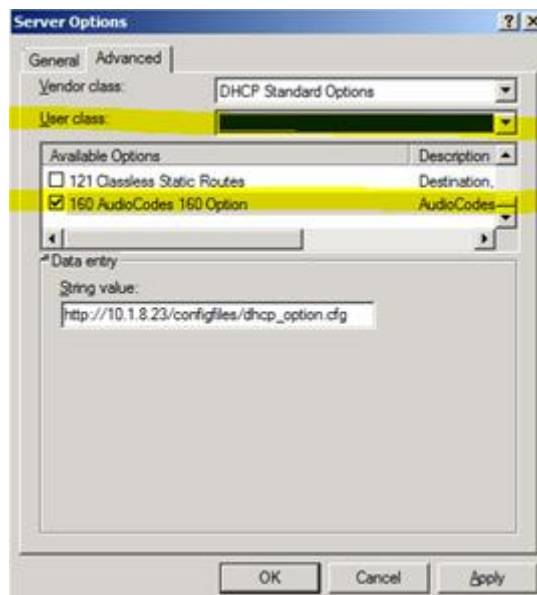
Figure 13: Configure Options 2



14. 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.

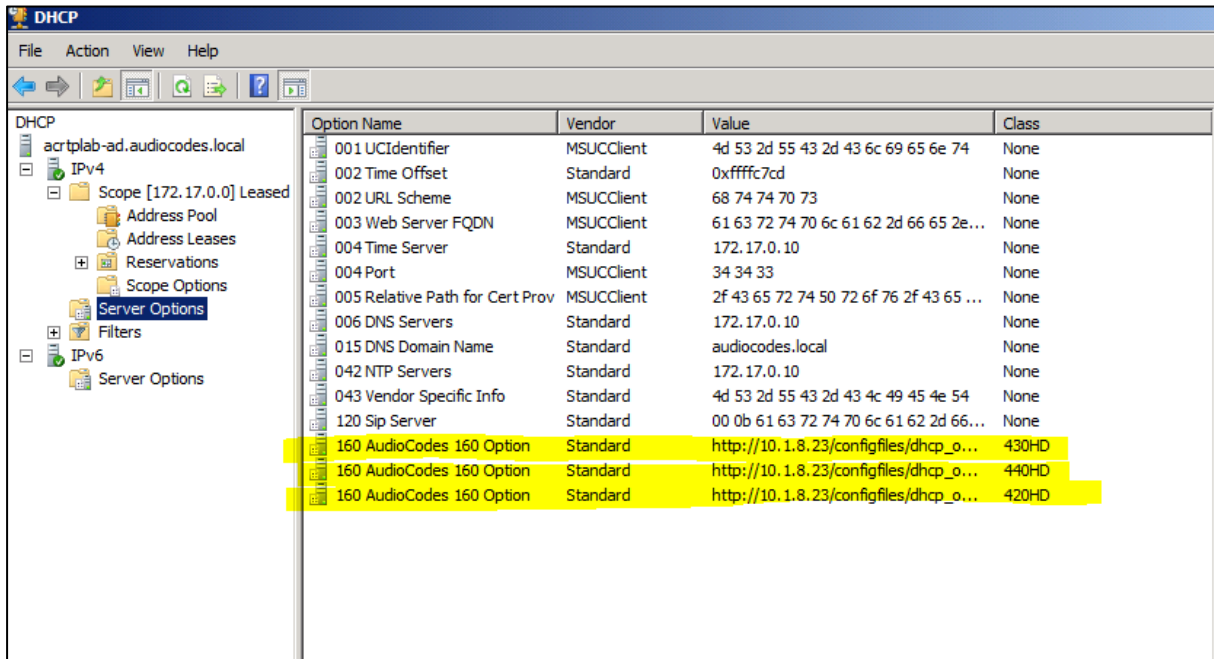
Figure 14: Server Options



15. 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 15: Scope Options Created [Illustrative Purposes Only]**



| Option Name                     | Vendor    | Value                                   | Class |
|---------------------------------|-----------|---|-------|
| 001 UCIIdentifier               | MSUCCient | 4d 53 2d 55 43 2d 43 6c 69 65 6e 74     | None  |
| 002 Time Offset                 | Standard  | 0xffffc7cd                              | None  |
| 002 URL Scheme                  | MSUCCient | 68 74 74 70 73                          | None  |
| 003 Web Server FQDN             | MSUCCient | 61 63 72 74 70 6c 61 62 2d 66 65 2e...  | None  |
| 004 Time Server                 | Standard  | 172.17.0.10                             | None  |
| 004 Port                        | MSUCCient | 34 34 33                                | None  |
| 005 Relative Path for Cert Prov | MSUCCient | 2f 43 65 72 74 50 72 6f 76 2f 43 65 ... | None  |
| 006 DNS Servers                 | Standard  | 172.17.0.10                             | None  |
| 015 DNS Domain Name             | Standard  | audiocodes.local                        | None  |
| 042 NTP Servers                 | Standard  | 172.17.0.10                             | None  |
| 043 Vendor Specific Info        | Standard  | 4d 53 2d 55 43 2d 43 4c 49 45 4e 54     | None  |
| 120 Sip Server                  | Standard  | 00 0b 61 63 72 74 70 6c 61 62 2d 66...  | None  |
| 160 AudioCodes 160 Option       | Standard  | http://10.1.8.23/configfiles/dhcp_o...  | 430HD |
| 160 AudioCodes 160 Option       | Standard  | http://10.1.8.23/configfiles/dhcp_o...  | 440HD |
| 160 AudioCodes 160 Option       | Standard  | http://10.1.8.23/configfiles/dhcp_o...  | 420HD |

### 3.1.2.4 Redirect Server

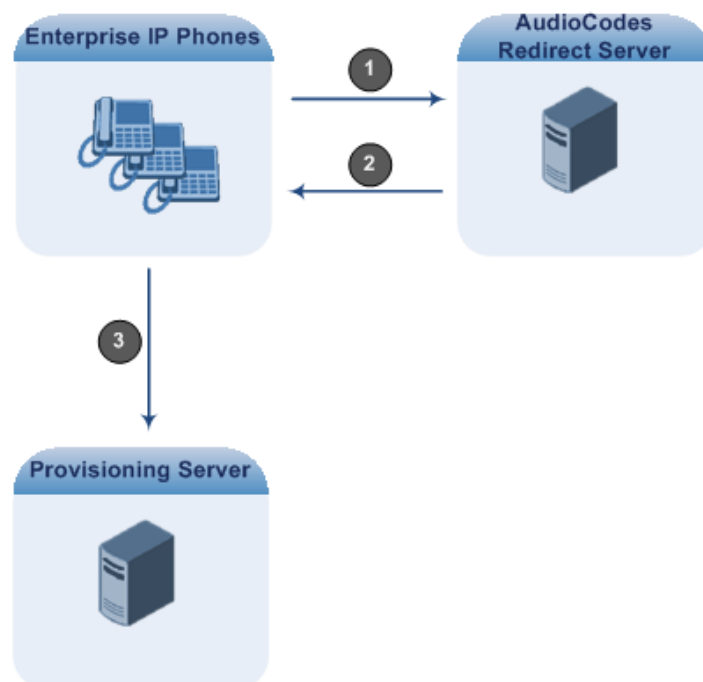
Network administrators can use the AudioCodes Redirect server to direct to the appropriate Provisioning server URL to download the relevant configuration and firmware files.

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.



- 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 16: 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.



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 4: Static URL Automatic Provisioning Parameters**

| Parameter                      | Description   |
|--------------------------------|---|
| provisioning/method            | <p>Defines the provisioning method:</p> <ul style="list-style-type: none"> <li>■ Disable - Automatic update is disabled. The phone attempts to upgrade its firmware and configuration</li> <li>■ Dynamic DHCP Options (Dynamic URL) (default) - Using DHCP Option 160 and Options 66/67 for provisioning</li> <li>■ Static URL - Using Static URL for provisioning</li> </ul>   |
| provisioning/firmware/url      | <p>The static URL for checking the firmware file. The URL must be entered using one of the following syntax options:</p> <ul style="list-style-type: none"> <li>■ &lt;protocol&gt;://&lt;server IP address or host name&gt;</li> <li>■ &lt;protocol&gt;://&lt;server IP address or host name&gt;/&lt;firmware file name&gt;</li> </ul> <p>Where&lt;protocol&gt; can be one of the following protocols: <b>ftp</b>, <b>tftp</b>, <b>http</b> or <b>https</b>. For example:</p> <ul style="list-style-type: none"> <li>■ tftp://192.168.2.1 – retrieved firmware file is 445HD.img</li> <li>■ ftp://192.168.2.1/Different_Firmware_Name.img - retrieved firmware file is Different_Firmware_Name.img</li> </ul> <p><b>Note:</b> This parameter is applicable only when 'method' is configured to <b>Static</b>.</p>                             |
| provisioning/configuration/url | <p>Static URL for checking the configuration file, entered using syntax:</p> <ul style="list-style-type: none"> <li>■ &lt;protocol&gt;://&lt;server IP address or host name&gt;</li> <li>■ &lt;protocol&gt;://&lt;server IP address or host name&gt;/&lt;configuration file name&gt;</li> </ul> <p>Where&lt;protocol&gt; can be one of the following protocols: "ftp", "tftp", "http" or "https". For example:</p> <ul style="list-style-type: none"> <li>■ http://192.168.2.1 - configuration file name is &lt;MAC Address&gt;.cfg, for example, 001122334455.cfg</li> <li>■ https://192.168.2.1/445HD_&lt;MAC&gt;_conf.cfg - retrieved configuration file name is 445HD_&lt;MAC Address&gt;_conf.cfg, for example, 445HD_001122334455_conf.cfg</li> </ul> <p><b>Note:</b> Applicable only when 'method' is configured to <b>Static</b>.</p> |



## 3.2 Firmware Header–Based Download Optimization for HTTP Servers

- Firmware header download method for HTTP server to avoid downloading entire file if device version is the same as on the server

| Parameter               | Description  |
|-------------------------|--|
| system/http/support_206 | Firmware header download method for HTTP server. <ul style="list-style-type: none"><li>■ <b>0</b> = HTTP server that does not support 206 response</li><li>■ <b>1</b> = HTTP server that supports 206 response (Default)</li></ul> |

## 3.3 Verifying Firmware Signature

- Starting from Version 3.5.0, AudioCodes firmware is now signed by AudioCodes CA. AudioCodes Signed firmware is verified during upgrade.

| Parameter                               | Description  |
|---|--|
| system/verify_firmware_signature/enable | 1 = Enable - Verifies the signature during the upgrading firmware.<br>0 = Disable (default).<br>For 425HD IP Phone, default = 1. |

## 4 Configuring Networking

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



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



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 5: Date Display Format**

| Parameter                      | Description  |
|--------------------------------|--|
| system/ntp/date_display_format | Select either: <ul style="list-style-type: none"><li>■ <b>EUROPEAN</b> (default)</li><li>■ <b>AMERICAN</b></li></ul> The European date format is DDMMYYYY.<br>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 6: 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.<br><ul style="list-style-type: none"> <li>■ <b>DISABLE</b> Disable (default)</li> <li>■ <b>ENABLE</b> Enable</li> </ul>   |
| system/daylight_saving/start_date        | This subsection defines the starting day for the daylight saving offset.<br><ul style="list-style-type: none"> <li>■ month - defines specific month in year</li> <li>■ day - defines specific day in month</li> <li>■ hour - defines specific hour in day</li> <li>■ minute - defines specific minute in hour</li> </ul> <p>Example: To configure the phone to start daylight savings with a specific offset on February 22<sup>nd</sup> at 14:30, set the following:</p> <pre>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</pre> |
| system/daylight_saving/start_date/month  | The month in a year.<br>The valid range is 1 to 12.   |
| system/daylight_saving/start_date/day    | The day in a month.<br>The valid range is 1 to 31.  |
| system/daylight_saving/start_date/hour   | The hour in the day.<br>The valid range is 0 to 23.   |
| system/daylight_saving/start_date/minute | The minute in an hour.<br>The valid range is 0 to 59.   |

| Parameter                                     | Description   |
|---|---|
| system/daylight_saving/end_date               | <p>This subsection defines the ending day for the daylight saving offset.</p> <ul style="list-style-type: none"> <li>■ <b>month</b> - defines the specific month in a year</li> <li>■ <b>day</b> - defines the specific day in a month</li> <li>■ <b>hour</b> - defines the specific hour in a day</li> <li>■ <b>minute</b> - defines the specific minute in an hour</li> </ul> <p>For example: To configure the phone to end the daylight savings on July 16<sup>th</sup> at 22:15, set the following:</p> <pre>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</pre> |
| system/daylight_saving/end_date/month         | <p>The month in a year.</p> <p>The valid range is 1 to 12.</p>  |
| system/daylight_saving/end_date/day           | <p>The day in a month.</p> <p>The valid range is 1 to 31.</p>   |
| system/daylight_saving/end_date/hour          | <p>The hour in the day</p> <p>The valid range is 0 to 23.</p>   |
| system/daylight_saving/end_date/minute        | <p>The minute in an hour.</p> <p>The valid range is 0 to 59.</p>  |
| system/daylight_saving/offset                 | <p>The offset value for the daylight saving.</p> <p>The valid range is 0 to 180. The default offset is 60.</p>  |
| system/daylight_saving/mode                   | <p>Configures the daylight saving mode.</p> <p>Valid values are</p> <p><b>FIXED</b>= Date is specified as: Month, Day of month.</p> <p><b>DayOfWeek</b>= Date is specified as: Month, Week of month, Day of week.</p>   |
| system/daylight_saving/start_date/week        | <p>Relevant to 'Day of week' mode:</p> <p>The week of month (values 1-5) for start of daylight saving time.</p>   |
| system/daylight_saving/start_date/day_of_week | <p>Relevant to 'Day of week' mode:</p> <p>The day of week for daylight saving time start</p> <p>Valid values:</p> <p><b>SUNDAY</b></p> <p><b>MONDAY</b></p> <p><b>TUESDAY</b></p> <p><b>WEDNESDAY</b></p> <p><b>THURSDAY</b></p> <p><b>FRIDAY</b></p> <p><b>SATURDAY</b></p>  |

| Parameter                                   | Description   |
|---|---|
| system/daylight_saving/end_date/week        | Relevant to 'Day of week' mode:<br>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:<br>The day of week for daylight saving time start<br>Valid values:<br><b>SUNDAY</b><br><b>MONDAY</b><br><b>TUESDAY</b><br><b>WEDNESDAY</b><br><b>THURSDAY</b><br><b>FRIDAY</b><br><b>SATURDAY</b> |

### 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 7: NTP Server Parameters**

| Parameter                           | Description  |
|-------------------------------------|--|
| system/ntp/enabled                  | Enables the NTP server from which the phone automatically retrieves the date and time. <ul style="list-style-type: none"> <li>■ <b>0</b> = Disable</li> <li>■ <b>1</b> = Enable – obtains the time information automatically from a configured NTP server (default)</li> </ul>   |
| 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. <ul style="list-style-type: none"> <li>■ <b>days</b> = defines the number of days</li> <li>■ <b>hours</b> = defines the number of hours</li> </ul> For example: To configure the phone to perform an update with an NTP server every 1 day and 6 hours, set the following:<br><b>system/ntp/sync_time/days=1</b><br><b>system/ntp/sync_time/hours=6</b> |
| system/ntp/sync_time/days           | The number of days.<br>The valid range is 0 to 7. The default of days is 0.  |
| system/ntp/sync_time/hours          | The number of hours.<br>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. <ul style="list-style-type: none"> <li>■ <b>24Hour</b> (default)</li> <li>■ <b>12Hour</b></li> </ul>   |
| system/ntp/add_special_ntp_server   | Disable/Enable sending NTP query for the well-known (public) NTP servers. <ul style="list-style-type: none"> <li>■ <b>0</b> = Don't send</li> <li>■ <b>1</b> = Send (Default)</li> </ul>   |

### 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).



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.



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 8: NTP Server and GMT Parameters**

| Parameter             | Description   |
|-----------------------|---|
| system/ntp/gmt_offset | <p>The format of this value is <b>hh:mm</b>, where <b>hh</b> is hour and <b>mm</b> is minutes.<br/>Default: 00:00</p> <p>Enables the NTP server from which the phone retrieves the date and time.</p> <ul style="list-style-type: none"> <li>■ <b>0</b> = Disable (default)</li> <li>■ <b>1</b> = Enable – obtains the time information from a configured NTP server</li> </ul> |

## 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 9: Network Settings Parameters**

| Parameter                          | Description   |
|------------------------------------|---|
| network/lan_type                   | Defines the IP addressing method: <ul style="list-style-type: none"> <li>■ <b>STATIC</b> IP (default)- Phone's IP address is defined manually</li> <li>■ <b>DHCP</b> Automatic IP DHCP - Phone's IP address is acquired automatically from a DHCP server</li> </ul> |
| network/lan/fixed_ip               | This subsection defines the relevant parameters if 'lan_type' is configured to <b>STATIC</b> 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.  |
| <b>Domain Name Server (DNS)</b>    |   |
| 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 10: Partial DHCP Parameters**

| Parameter                                | Description   |
|--|---|
| <b>Partial DHCP</b>                      |   |
| network/lan/dhcp                         | If 'lan_type' is configured to <b>DHCP</b> , this parameter and the parameters in this table must be configured.  |
| network/lan/dhcp/domain_name/enabled     | Enables setting the domain name manually.<br><ul style="list-style-type: none"> <li>■ 0 = Disable (default)</li> <li>■ 1 = Enable</li> </ul> <b>Note:</b> If enabled, <b>network/lan/fixed_ip/domain_name</b> must be set.  |
| network/lan/dhcp/ip_address/enabled      | Enables setting the IP address manually.<br><ul style="list-style-type: none"> <li>■ 0 = Disable</li> <li>■ 1 = Enable (default)</li> </ul> <b>Note:</b> If enabled, <b>network/lan/fixed_ip/ip_address</b> must be set.  |
| network/lan/dhcp/netmask/enabled         | Enables setting the network mask manually.<br><ul style="list-style-type: none"> <li>■ 0 = Disable</li> <li>■ 1 = Enable (default)</li> </ul> <b>Note:</b> If enabled, <b>network/lan/fixed_ip/netmask</b> must be set.   |
| network/lan/dhcp/gateway/enabled         | Enables setting the default gateway manually.<br><ul style="list-style-type: none"> <li>■ 0 = Disable</li> <li>■ 1 = Enable (default)</li> </ul> <b>Note:</b> If enabled, <b>network/lan/fixed_ip/gateway</b> must be set.  |
| network/lan/dhcp/primary_dns/enabled     | Enables setting the primary DNS manually.<br><ul style="list-style-type: none"> <li>■ 0 = Disable (default)</li> <li>■ 1 = Enable</li> </ul> <b>Note:</b> If enabled, <b>network/lan/fixed_ip/primary_dns</b> must be set.  |
| network/lan/dhcp/secondary_dns/enabled   | Enables setting the secondary DNS manually.<br><ul style="list-style-type: none"> <li>■ 0 = Disable (default)</li> <li>■ 1 = Enable</li> </ul> <b>Note:</b> If enabled, <b>network/lan/fixed_ip/secondary_dns</b> must be set.  |
| <b>DHCP-Related Parameters</b>           |   |
| 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 ( <b>system/ntp/primary_server_address</b> and <b>system/ntp/secondary_server_address</b> ).<br><ul style="list-style-type: none"> <li>■ 0 = Disable</li> <li>■ 1 = Enable (default)</li> </ul> |

| Parameter                               | Description   |
|---|---|
| network/lan/dhcp/ntp/gmt_offset/enabled | <p>Enables prioritization of the NTP GMT offset information received from the DHCP server (Option field 2), over the static configuration (<b>system/ntp/gmt_offset</b>).</p> <ul style="list-style-type: none"> <li>■ 0 = Disable</li> <li>■ 1 = Enable (default)</li> </ul> |

### 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 11: Port Settings**

| Parameter             | Description   |
|-----------------------|---|
| network/lan/port_mode | <p>Sets the LAN port mode.</p> <p>Valid values are:</p> <ul style="list-style-type: none"> <li>■ AUTOMATIC = Auto negotiation.</li> <li>■ FULL_10 = 10Mbps + full duplex</li> <li>■ FULL_100 = 100Mbps + half duplex</li> <li>■ HALF_10 = 10Mbps + full duplex</li> <li>■ HALF_100 = 100Mbps + half duplex</li> <li>■ FULL_1Gbps = 1 Gbit/s port + full duplex</li> </ul> |
| network/pc/port_mode  | <p>Sets the computer port mode.</p> <p>Valid values are:</p> <ul style="list-style-type: none"> <li>■ AUTOMATIC = Auto negotiation</li> <li>■ FULL_10 = 10Mbps + full duplex</li> <li>■ FULL_100 = 100Mbps + half duplex</li> <li>■ HALF_10 = 10Mbps + full duplex</li> <li>■ HALF_100 = 100Mbps + half duplex</li> <li>■ DISABLE = Disables the PC port mode</li> </ul>  |

## 4.4 Configuring VLAN Settings

Network administrators can configure VLAN settings.

To configure the phone's VLAN settings:

Use the table as reference:

**Table 12: VLAN Settings**

| Parameter                               | Description  |
|---|--|
| network/lan/vlan/mode                   | <p>Determines how VLAN is assigned to your phone, i.e., manually or automatically, and if automatically, according to which protocol.</p> <ul style="list-style-type: none"> <li>■ <b>Disable</b></li> <li>■ <b>Manual Configuration of VLAN Manual</b> - 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.</li> <li>■ <b>Automatic Configuration of VLAN (CDP)</b> CDP - VLAN discovery mechanism based on Cisco Discovery Protocol (CDP). See Section 4.4.1 below for a detailed explanation.</li> <li>■ <b>Automatic Configuration of VLAN (LLDP)</b> LLDP - VLAN discovery mechanism based on LLDP. See Section 4.4.1 below for a detailed explanation.</li> <li>■ <b>Automatic Configuration of VLAN (CDP+LLDP)</b> CDP_LLDP (default) - VLAN discovery mechanism based on LLDP and CDP. LLDP is higher priority. See below for a detailed explanation.</li> </ul> |
| 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 = <b>Disable 0</b> . Change to <b>Enable (1)</b> 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



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.

Wi-Fi can be configured from the configuration file.

| Parameter                                | Description   |
|--|---|
| network/wifi/x/verify_server_certificate | Enable/disable verify server certificate.<br>Default = 0  |
| network/wifi/x/eap_method                | Set eap method (PEAP/ TLS/ TTLS/ PWD).<br>Default = PEAP  |
| network/wifi/x/auto_reconnect            | Enable/disable wifi auto reconnect.<br>Default = 1  |
| network/wifi_enabled                     | Enable/disable wifi feature.<br>Default = 0   |
| network/wifi/x/client_cert               | 1=Enable, bring a client certificate during wifi authentication (eap-tls/ttls).<br>0 = Disable (default)        |
| network/wifi/x/identity                  | Set ipp identity.<br>Default = null   |
| network/wifi/x/password                  | Set ssid password.<br>Default = null  |
| network/wifi/x/phase2_authentication     | Set phase2 authentication method( NONE/PAP/MSCHAP/MSCHAPV2 /CHAP/MD5/GTC).<br>Default = NONE                    |
| network/wifi/x/private_key               | 1=Enable, bring client private key during wifi authentication (eap-tls/ttls).<br>Default = 0                    |
| network/wifi/x/security                  | Set ssid security method (NONE/WPA2PERSONAL/WPA2PERSONAL /WPA2ENTERPRISE/WPA2ENTERPRISE/WEP).<br>Default = NONE |
| network/wifi/x/ssid                      | Set ssid name.<br>Default = null  |
| network/wifi/x/wps_method                | Set wps method (NONE/ALL/PIN/AUTH/PBC).<br>Default = NONE   |

## 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 13: SIP General Parameters**

| Parameter                                | Description   |
|--|---|
| voip/signalling/sip/transport_protocol   | Determines the transport layer for outgoing SIP calls initiated by the phone. <ul style="list-style-type: none"> <li>■ <b>UDP</b> UDP (default)</li> <li>■ <b>TCP</b> TCP</li> <li>■ <b>TLS</b> TLS</li> </ul>  |
| voip/signalling/sip/tls_port             | Defines the local TLS SIP port for SIP messages.<br>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.<br>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.<br><b>Note:</b> <ul style="list-style-type: none"> <li>■ Ensure that the name you choose is the one with which the Proxy is configured to identify the phone.</li> <li>■ If not specified, the phone's IP address is used (default).</li> </ul> |
| voip/signalling/sip/prack/enabled        | Determines whether the phone sends PRACK (Provisional Acknowledgment) messages upon receipt of 1xx SIP reliable responses. <ul style="list-style-type: none"> <li>■ <b>0</b> = Disable</li> <li>■ <b>1</b> = Enable (default)</li> </ul>  |

| Parameter  | Description  |
|--|--|
| voip/signalling/sip/rport/enabled                    | <p>Determines whether the phone adds the 'rport' parameter to the relevant SIP message (in the SIP Via header).</p> <ul style="list-style-type: none"> <li>■ 0 = Disable (default)</li> <li>■ 1 = Enable</li> </ul>  |
| voip/signalling/sip/sdp_include_ptime                | <p>Determines whether the phone adds the PTIME parameter to the SDP message body.</p> <ul style="list-style-type: none"> <li>■ 0 = Disable (default)</li> <li>■ 1 = Enable</li> </ul>  |
| voip/signalling/sip/keepalive_options/enabled        | <p>Determines whether keep-alive is performed using SIP OPTIONS messages sent to the Proxy.</p> <ul style="list-style-type: none"> <li>■ 0 = Disable (default)</li> <li>■ 1 = Enable</li> </ul>  |
| voip/signalling/sip/keepalive_options/timeout        | <p>Defines the Proxy keep-alive time interval (in seconds) between Keep-Alive messages.</p> <ul style="list-style-type: none"> <li>■ The valid range is 0 to 86400. The default value is 300.</li> </ul>   |
| voip/signalling/sip/connect_media_on_180             | <p>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.</p> <ul style="list-style-type: none"> <li>■ 0 = Disable (default)</li> <li>■ 1 = Enable</li> </ul>  |
| voip/signalling/sip/block_callerid_on_outgoing_calls | <p>Can be configured only if the BroadSoft BroadWorks application server is used.</p> <p>When enabled, the outgoing INVITE message is sent with an anonymous From header and P-Asserted-Identityheader.</p> <ul style="list-style-type: none"> <li>■ 0 = Disable (default)</li> <li>■ 1 = Enable</li> </ul> <p>For example:</p> <ul style="list-style-type: none"> <li>■ FROMheader contains anonymous URI:<br/><i>From: "Anonymous"</i><br/><i>sip:anonymous@anonymous.invalid</i></li> <li>■ P-Asserted-Identityheader:<br/><i>P-Asserted-Identity: "1001" 1115551001@proxy.net</i></li> </ul> |
| voip/signalling/sip/anonymous_calls_blocking         | <p>Can be configured only if the BroadSoft BroadWorks application server is used.</p> <p>When enabled, incoming INVITE messages with anonymous From header are rejected.</p> <ul style="list-style-type: none"> <li>■ 0 = Disable (default)</li> <li>■ 1 = Enable</li> </ul> <p>For example:</p> <p><i>From: "Anonymous" &lt;sip:anonymous@anonymous.invalid&gt;</i></p> <p>The phone responds with a SIP 403 "Forbidden" response.</p>  |
| voip/signalling/sip/auth_retries                     | <p>Defines the number of times authenticated register messages are re-sent if 401 or 407 SIP responses with a different "nonce" are received.</p> <p>The valid range is 0 to 100.</p> <p>The default value is 10.</p>  |

| Parameter  | Description  |
|--|--|
| voip/signalling/sip/display_name_in_registration_msg/enabled | <p>Sets the Display Name in the 'To' and 'From' fields of the SIP REGISTER message.</p> <ul style="list-style-type: none"> <li>■ 0 = Disable (default)</li> <li>■ 1 = Enable</li> </ul>  |
| voip/signalling/sip/semi_transfer_with_no_cancel/enabled     | <p>Determines whether semi-attendant transfer is performed without sending the SIP CANCEL message to the remote side.</p> <ul style="list-style-type: none"> <li>■ 0 = Disable (default)</li> <li>■ 1 = Enable</li> </ul> <p><b>Note:</b></p> <ul style="list-style-type: none"> <li>■ 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 <a href="http://tools.ietf.org/html/draft-ietf-sipping-cc-transfer-03">http://tools.ietf.org/html/draft-ietf-sipping-cc-transfer-03</a>.</li> <li>■ Existing / current behavior is retained for backward compatibility (disabled by default)</li> </ul> |
| voip/signalling/sip/PAI_On_Replay/enable                     | <p>Enables the P-Asserted Identity header to be added to "18x" and "200" responses.</p> <ul style="list-style-type: none"> <li>■ 0 (Default) PAI header is not added to "18x" and "200" responses</li> <li>■ 1 PAI header is added to "18x" and "200" responses</li> </ul>   |
| voip/services/display_PAI_enable                             | <p>Display caller ID from <b>P-Asserted identity</b> header instead of <b>From</b> header in incoming call (if exists).</p> <ul style="list-style-type: none"> <li>■ 0 = Disable</li> <li>■ 1 = Enable (Default)</li> </ul>  |
| voip/signalling/sip/add_sip_instance/enable                  | <p>Unique User Agent Identifier for SIP registration, enabling the identification of an agent without relying on its IP address.</p> <ul style="list-style-type: none"> <li>■ 0 = Disable (default)</li> <li>■ 1 = Enable</li> </ul>   |
| voip/signalling/invite/remove_default_port_from_request_line | <p>Removes the default SIP port from the <b>Request-URI</b> in the INVITE message.</p> <ul style="list-style-type: none"> <li>■ 0 = Do not Remove (Default)</li> <li>■ 1 = Remove</li> </ul>   |
| voip/signalling/invite/remove_default_port_from_to_header    | <p>Removes the default SIP port from the <b>To</b> header in the INVITE message.</p> <ul style="list-style-type: none"> <li>■ 0 = Do not Remove (Default)</li> <li>■ 1 = Remove</li> </ul>   |
| voip/signalling/invite/add_port_to_contact_header            | <p>Add the SIP port to <b>CONTACT</b> header in INVITE message</p> <ul style="list-style-type: none"> <li>■ 0 = Do not Add (Default)</li> <li>■ 1 = Add</li> </ul>   |
| voip/services/subs/retry_after_404                           | <p>Determine whether IPP sends SUBSCRIBE retry when 404 response is received. Retry timer (If enabled) is configured in: voip/services/subs/retry/timeout.</p> <ul style="list-style-type: none"> <li>■ 0 = Disable (Default)</li> <li>■ 1 = Enable</li> </ul>   |



| Parameter                                  | Description  |
|--|--|
| voip/services/subs/retry/timeout           | <p>Configure the SUBSCRIBE retry timeout.</p> <p>The value is specified in units of 100 msec (<math>X \times 100</math> msec).</p> <p><b>Range:</b> 10–10000</p> <p>Effective timeout: 1000–1,000,000 msec</p> <p><b>Default:</b> 300 (equivalent to 30,000 msec or 30 seconds).</p> |
| voip/services/speed_dial_subscribe/enabled | <p>Disable the presence SUBSCRIBE message for <b>Speed_Dial</b> functional key type only (personal_settings/functional_key/x/type = Speed_Dial).</p> <ul style="list-style-type: none"><li>■ <b>0</b> = Disable</li><li>■ <b>1</b> = Enable (Default)</li></ul>                      |

## 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 14: Proxy and Registrar Parameters**

| Parameter   | Description  |
|---|--|
| voip/signalling/sip/use_proxy                       | Determines whether to use a SIP Proxy server.<br><ul style="list-style-type: none"> <li>■ 0 = Disable (default)</li> <li>■ 1 = Enable</li> </ul>   |
| 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.<br>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.<br><ul style="list-style-type: none"> <li>■ 0 = Disable (default)</li> <li>■ 1 = Enable</li> </ul> <b>Note:</b> <ul style="list-style-type: none"> <li>■ 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)</li> <li>■ When the phone re-registers, the keep-alive messages are re-sent periodically.</li> </ul> |
| voip/signalling/sip/registrar_ka/timeout            | Defines the registration keep-alive time interval (in seconds) between Keep-Alive messages.<br>Range: 40 to 65536. Default: 60.  |
| voip/signalling/sip/proxy_timeout                   | The SIP proxy server registration timeout (in seconds).<br>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.<br><ul style="list-style-type: none"> <li>■ 0 = Disable</li> <li>■ 1 = Enable (default)</li> </ul>  |
| voip/signalling/sip/sip_registrar/enabled           | Determines whether the phone registers to a separate SIP Registrar server.<br><ul style="list-style-type: none"> <li>■ 0 = Disable (default)</li> <li>■ 1 = Enable</li> </ul>  |
| voip/signalling/sip/sip_registrar/addr              | Only displayed if the 'Use SIP Registrar' parameter is enabled.<br>The IP address or host name of the Registrar server. Default: 0.0.0.0   |

| Parameter   | Description   |
|---|---|
| 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.<br>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.<br>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).<br>■ 0 = Disable (default)<br>■ 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.<br>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.   |



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 15: SIP Proxy Server Redundancy Parameters**

| Parameter   | Description   |
|---|---|
| <code>voip/signalling/sip/redundant_proxy/enabled</code>          | Mandatory for the phone to operate in redundancy. Commands the phone to operate with the other <b><code>voip/signalling/sip/redundant_proxy</code></b> parameters.  |
| <code>voip/signalling/sip/redundant_proxy/mode</code>             | 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. <ul style="list-style-type: none"> <li>■ <b>Disable</b> = (Default) Phone doesn't use redundant proxy.</li> <li>■ <b>Primary-Fallback</b> = Phone registered to redundant proxy if the primary proxy does not respond to SIP signaling messages.</li> <li>■ <b>Simultaneous</b> = Applies only in some environments. If selected, dual registration is performed; the phone registers simultaneously to both servers.</li> </ul> |
| <code>voip/signalling/sip/redundant_proxy/address</code>          | Only displayed if the 'Redundant Proxy Mode' parameter is enabled (Primary-Fallback)<br>Defines the IP address of the backup proxy server. Default: <b>0.0.0.0</b>  |
| <code>voip/signalling/sip/redundant_proxy/keepalive_period</code> | Only displayed if the 'Redundant Proxy Mode' parameter is enabled (Primary-Fallback)<br>Defines how often a keep alive message is sent by the phone to the proxy server.<br>Range: 0 to 300.<br>Default: Every 60 seconds.  |

| Parameter  | Description   |
|--|---|
| voip/signalling/sip/redundant_proxy/port           | <p>Only displayed if the 'Redundant Proxy Mode' parameter is enabled (Primary-Fallback)</p> <p>Defines the UDP or TCP port of the backup redundant proxy server. If occupied by other enterprise devices, you can configure another.</p> <p>Range: 1024 to 65535. Default = 5060.</p>   |
| voip/signalling/sip/redundant_proxy/symmetric_mode | <p>Only displayed if the 'Redundant Proxy Mode' parameter is enabled (Primary-Fallback)</p> <p>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.</p> <p><b>0</b> = 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.</p> <p><b>1</b> = 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.</p> <p>In both modes, the following applies:</p> <p>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.</p> <p>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.</p> |

### 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.



- 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 16: Device Registration Failover Parameters**

| Parameter   | Description   |
|---|---|
| voip/signalling/sip/transport_protocol                      | Either: <ul style="list-style-type: none"> <li>■ UDP (default)</li> <li>■ TCP</li> <li>■ TLS encryption</li> </ul> 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/address              | Configure this parameter as an SRV host name.   |
| voip/signalling/sip/sip_outbound_proxy/port                 | Configure a value of <b>65535</b> for this parameter. Configure the parameter when you're using an Outbound Proxy. Either configure <i>this</i> parameter <i>or</i> 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 <b>65535</b> for this parameter. Configure the parameter when you're using a regular Proxy server. Either configure <i>this</i> parameter <i>or</i> the parameter 'Outbound Proxy Port'.   |
| 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 17: Device Registration Failback Parameter**

| Parameter                                  | Description  |
|--|--|
| voip/signalling/sip/failback_retry_timeout | <p>Only applies to BroadSoft. Applies only if you're operating with the DNS mode of failover, i.e., with a DNS server.</p> <ul style="list-style-type: none"> <li>■ <b>0</b> = Disable (default) – it'll never try to access back to the first one.</li> <li>■ <b>n</b> = Time, in seconds, that must lapse before failback is performed.</li> </ul> |

### 5.1.2.2.3 Failback - Using Register Message to Detect if Primary Server Is Active

#### To configure:

**Table 18: Using Register Message to Detect if Primary Server Is Active**

| Parameter                                       | Value (Default) | Description  |
|---|-----------------|--|
| voip/signalling/sip/detect_primary_proxy/method | OPTIONS         | <p><b>OPTIONS</b> - send SIP OPTIONS message to detect if primary server or primary outbound proxy (server) is active.</p> <p><b>REGISTER</b> - send SIP REGISTER message to detect if primary server or primary outbound proxy (server) is active.</p> <p>(voip/signalling/sip/failback_retry_timeout configuration value must be &gt; 0)</p> |

### 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 19: Preventing Unregistering**

| Parameter                                     | Description  |
|---|--|
| voip/signalling/sip/unregister_on_voip_reload | <p>Either:</p> <ul style="list-style-type: none"> <li>■ <b>0</b> = SIP Registration message with <b>Expires:0</b> (unregister) is <i>not</i> sent.</li> <li>■ <b>1</b> = (Default) SIP Registration message with <b>Expires:0</b> (unregister) is sent.</li> </ul> |

#### 5.1.2.4 Prevent SIP UNSUBSCRIBE on VoIP Reload Upon Failover/Failback

Controls whether a SIP **UNSUBSCRIBE** message (Expires: 0) is sent after a VoIP application reload upon failover/failback.

| Parameter                                      | Description  |
|--|--|
| voip/signalling/sip/unsubscribe_on_voip_reload | <ul style="list-style-type: none"><li>■ <b>0</b> = Don't send an unsubscribe message when the VoIP service reloads.</li><li>■ <b>1</b> (Default) = Sends an unsubscribe message when the VoIP service reloads.</li></ul> |

#### 5.1.2.5 Redundancy Failback when DNS Resolution of the SIP Proxy Server's FQDN returns a Different IP Address

Enable or disable redundancy failback when DNS resolution of the SIP proxy server's FQDN returns a different IP address.

| Parameter name                           | Description                                       |
|--|---|
| voip/signalling/sip/dns_fail_back/enable | <b>0</b> = Disable (Default)<br><b>1</b> = Enable |



### 5.1.3 Configuring a Line

The network administrator can configure a line.

#### To configure line mode:

Use the table as reference:

**Table 20: Line Settings**

| Parameter   | Description   |
|---|---|
| voip/line/n/description<br><b>C450HD/445HD:</b> n = [0-29]<br><b>425HD:</b> n = [0-7]       | 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/n/enabled<br><b>C450HD/445HD:</b> n = [0-29]<br><b>425HD:</b> n = [0-7]           | Activates or deactivates the line.<br><b>0</b> = Disabled (this is the default for the second line and higher in the configuration file)<br><b>1</b> = Enabled (this is the default for the first line <b>voip/line/0/</b> in the configuration file).  |
| voip/line/n/id<br><b>C450HD/445HD:</b> n = [0-29]<br><b>425HD:</b> n = [0-7]                | 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.<br>Default: 0  |
| voip/line/n/auth_name<br><b>C450HD/445HD:</b> n = [0-29]<br><b>425HD:</b> n = [0-7]         | Defines the SIP username credential used in the registration process when attempting to associate with the above Line ID.<br>Default: 0   |
| voip/line/n/auth_password<br><b>C450HD/445HD:</b> n = [0-29]<br><b>425HD:</b> n = [0-7]     | Defines the SIP password associated with the above Line ID identifier during the registration process.<br>Default: 0  |
| voip/line/n/line_mode<br><b>C450HD/445HD:</b> n = [0-29]<br><b>425HD:</b> n = [0-7]         | 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/n/extension_display<br><b>C450HD/445HD:</b> n = [0-29]<br><b>425HD:</b> n = [0-7] | Defines the label displayed in the phone screen.  |

### 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 21: Assigning Programmable Keys to Lines (SIP Accounts)**

| Parameter Name                                   | Description   |
|--|---|
| personal_settings/functional_key/12-17/key_label | These are the labels displayed in the screen next to Programmable Keys <b>1-6</b> .<br>Define the string of characters you want displayed (name, extension, etc.).        |
| personal_settings/functional_key/12-17/type      | Default: <b>SIP_ACCOUNT</b> . Can be set to perform other functions such as Speed Dial or Key Event.<br><br>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 22: Assigning Programmable Keys to Lines (SIP Accounts)**

| Parameter Name                                 | Description   |
|--|---|
| personal_settings/functional_key/0-5/key_label | These are the labels displayed in the screen next to Programmable Keys <b>1-6</b> .<br>Define the string of characters you want displayed (name, extension, etc.).        |
| personal_settings/functional_key/0-5/type      | Default: <b>SIP_ACCOUNT</b> . Can be set to perform other functions such as Speed Dial or Key Event.<br><br>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

Figure 17: 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 23: SIP Timers Parameters

| Parameter  | Description   |
|--|---|
| voip/signalling/sip/sip_t1                               | <p>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).</p> <p>The valid range is 100 to 60000. The default value is 500.</p> <p><b>Note:</b> 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):</p> <ul style="list-style-type: none"> <li>■ The first retransmission is sent after 500 msec.</li> <li>■ The second retransmission is sent after 1000 (2*500) msec.</li> <li>■ The third retransmission is sent after 2000 (2*1000) msec.</li> <li>■ The fourth retransmission and subsequent retransmissions until SIPMaxRtx are sent after 4000 (2*2000) msec.</li> </ul> |
| voip/signalling/sip/redundant_proxy/dual_registration/t1 | <p>Only relevant if dual registration / redundancy server is configured. Allows quicker retransmission of SIP messages. Default: 20 milliseconds. Range: 20-200.</p>  |
| voip/signalling/sip/sip_t2                               | <p>The maximum interval (in msec) between retransmissions of SIP messages (according to RFC 3261).</p> <ul style="list-style-type: none"> <li>■ The valid range is 4000 to 60000.</li> <li>■ The default value is 4000.</li> </ul> <p><b>Note:</b> The time interval between subsequent retransmissions of the same SIP message starts with SipT1Rtx and is multiplied by two until SipT2Rtx.</p>   |

| Parameter                                     | Description   |
|---|---|
| voip/signalling/sip/sip_t4                    | The SIP T4 retransmission timer according to RFC 3261.<br><ul style="list-style-type: none"> <li>■ The valid range is 5000 to 60000.</li> <li>■ The default value is 5000.</li> </ul>   |
| voip/signalling/sip/sip_invite_timer          | The SIP INVITE timer according to RFC 3261.<br>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.<br>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.<br><ul style="list-style-type: none"> <li>■ The valid range is 0 to 65535. The default value is 90.</li> </ul>  |
| 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 <b>Expires:0</b> , which means unregister.<br><br>By setting this parameter to <b>1</b> (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 24: 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.<br><br>The default value is 0x60.<br><br>Values can be set in decimal (e.g. 96) or hexadecimal (e.g. 0x60). |

For information on configuring RTP QoS, see Section 5.4.3.

### 5.1.7 Configuring SIP Reject Code

Reject Code can be configured.

**To configure Reject Code:**

Use the table as reference:

**Table 25: Reject Code Parameters**

| Parameter                       | Description   |
|---------------------------------|---|
| voip/services/dnd_reject_code   | Configures the dnd reject code that the phone sends when the <b>Reject</b> softkey is pressed or while DND is activated.<br>Valid values are between 400 to 699 (default 603)     |
| voip/services/other_reject_code | Configures other reject code that the phone sends when the <b>Reject</b> softkey is pressed or while DND is activated.<br>Valid values are between 400 to 699 (default 486)       |
| voip/services/sk_reject_code    | Configures the softkey reject code that the phone sends when the <b>Reject</b> softkey is pressed or while DND is activated.<br>Valid values are between 400 to 699 (default 603) |

## 5.2 Configuring Dialing

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

## 5.2.1 Configuring General Dialing Parameters

Network administrators can configure general dialing parameters.

**To configure general dialing parameters:**

Use the table as reference:

**Table 26: Dialing Parameters**

| Parameter   | Description  |
|---|--|
| voip/dialing/timeout                              | The duration (in seconds) of allowed inactivity between dialed digits. When you work with a proxy, the number you have dialed 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 <b>0S</b> for the Dial Map. If a user wants to make an international call by dialing <b>00</b> and wants to dial the secretary/operator by dialing <b>0</b> , the user can do both by adding <b>0S</b> to the Dial Map. For example, if the digit map string= *xx 2-9]11 0S 2-9]xxxxxxxx 1xxx2-9]xxxxxx, it has <b>0S</b> in it. When the user dials <b>0</b> , <b>0</b> will match <b>0S</b> and will therefore start the 'Interdigit Short Timeout' timer. After this timeout, <b>0</b> is dialed out. User can dial <b>00</b> or <b>0123</b> 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<br>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 dialed digits even if there is no match in the dial plan or digit map. <ul style="list-style-type: none"> <li>■ <b>0</b> = Disable</li> <li>■ <b>1</b> = Enable (default)</li> <li>■ Note: This parameter is available only if the parameter 'voip/dialing/dial_complete_key/enabled' is set to 1.</li> </ul>  |
| 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.  |
| voip/dialing/allow_calling_self_extension/enabled | If disabled (default), calling the self-number (user ID) will be blocked.<br><br>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).   |

## 5.2.2 Configuring Dial Tones

Dial Tones settings can be configured.

### To configure Dial Tones:

Use the table as reference:

**Table 27: 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.<br>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.<br>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.<br>Range:1 to 300. Default: 120.  |
| voip/dialing/secondary_dial_tone/enabled        | <ul style="list-style-type: none"> <li>■ Enables the secondary dial tone.</li> <li>■ <b>0</b> = Disable (default) - Phone doesn't use secondary dial tone.</li> <li>■ <b>1</b> = Enable - Phone plays secondary dial tone if the secondary dial tone key is pressed (first digit). For example, when pressing <b>9</b> to get an external dial tone, a different dial tone (not configurable) is played as the second dial tone.</li> </ul> |
| voip/dialing/secondary_dial_tone/key_sequence   | <p>Defines the secondary dial tone is played if this is the first key pressed.</p> <ul style="list-style-type: none"> <li>■ Range: 0 to 9. Default: 9.</li> </ul> <p><b>Note:</b> This parameter is available only if the parameter 'voip/dialing/secondary_dial_tone/enabled' is set to <b>1</b>.</p>  |
| voip/services/out_of_service_behavior           | <p>Determines whether a reorder tone is played instead of a dial tone if you configured a Registrar IP address and the registration failed.</p> <ul style="list-style-type: none"> <li>■ <b>NONE</b> No Tone</li> <li>■ <b>REORDER_TONE</b> Reorder Tone (default)</li> </ul>   |
| voip/services/msg_waiting/stutter_tone_duration | <p>Defines the duration for which a stutter tone is played when you have unheard messages.</p> <ul style="list-style-type: none"> <li>■ Range:1000 to 60000.</li> <li>■ Default: 2500.</li> </ul>   |
| voip/dialing/automatic_disconnect               | <p>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.</p> <ul style="list-style-type: none"> <li>■ <b>0</b> = Disable</li> <li>■ <b>1</b> = Enable (default)</li> </ul>   |

### 5.2.3 Configuring DTMF

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

#### To configure DTMF:

Use the table as reference:

**Table 28: DTMF Transport Mode**

| Parameter                                   | Description   |
|---|---|
| voip/media/out_of_band_dtmf                 | DTMF transport mode. <ul style="list-style-type: none"> <li>■ <b>INBAND</b> Inband</li> <li>■ <b>RFC2833</b> RFC 2833 (default)</li> <li>■ <b>VIA_SIP</b> Via SIP</li> </ul>  |
| voip/media/dtmf_via_sip_force_flag          | Must be set to <b>1</b> to enable <b>Via SIP</b> as DTMF transport type.  |
| voip/audio/gain/dtmf_rtp_event_signal_level | Allows the network administrator to control the DTMF tones level. <ul style="list-style-type: none"> <li>■ <b>0 db</b> (Minimum)</li> <li>■ <b>31 db</b> (Maximum)</li> </ul> |



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.

### 5.2.4 Configuring Digit Maps and Dial Plans

Digit maps and Dial plans can be configured.

#### To configure digit map and dial plan:



Invalid Tokens will be ignored by the application.

Use the table as reference:



Table 29: Digit Map and Dial Plan Parameters

| Parameter                        | Description   |
|----------------------------------|---|
| voip/signalling/sip/digit_map    | <p>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.</p> <p>The valid value can be up to 256 characters.</p> <p>There are two main formats for the digit map configuration. The formats are distinguished by the separator ';' or ' '.</p> <p>■ <b>Using ' ' separator:</b> The following constructs can be used in each numbering scheme:</p> <ul style="list-style-type: none"> <li>• <b>Digit:</b> A digit from <b>0</b> to <b>9</b>.</li> <li>• <b>DTMF:</b> A digit, or one of the symbols <b>A, B, C, D, #</b>, or <b>*</b>. Extensions may be defined.</li> <li>• <b>Wildcard:</b> The symbol <b>x</b> which matches any digit (<b>0</b> to <b>9</b>).</li> <li>• <b>* Range:</b> One or more DTMF symbols enclosed between square brackets ([ and ]).</li> <li>• <b>Sub range:</b> 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 ].</li> <li>• <b>Position:</b> A period (.) which matches an arbitrary number, including zero, of occurrences of the preceding construct.</li> </ul> <p><b>For example:</b> [2-9]11 0 100 101 011xxx. 9011xxx. [12-9]xxxxxxxx [92-9]xxxxxxxx [912-9]xxxxxx *xx 8]xxxx 2-7]xxx</p> <p>This example includes the following rules:</p> <ul style="list-style-type: none"> <li>• <b>[2-9]11:</b> 911 rule: 211, 311, 411, 511, 611, 711, 811, 911 are dialed immediately</li> <li>• <b>0:</b> Local operator rule: After dialing <b>0</b> the phone waits T seconds and then completes the call automatically</li> <li>• <b>100:</b> Auto-attendant default extension</li> <li>• <b>101:</b> Voicemail default extension</li> <li>• <b>011xxx:</b> International rule without prefix</li> <li>• <b>9011xxx:</b> International rule with prefix</li> <li>• <b>[12-9]xxxxxxxx:</b> LD rule without prefix</li> <li>• <b>[912-9]xxxxxxxx:</b> LD rule with prefix</li> <li>• <b>[92-9]xxxxxx:</b> Local call with prefix</li> <li>• <b>*xx:</b> 2-digit star codes</li> <li>• <b>[1-7]xx:</b> A regular 3 digit extension that does not start with 9 or 8 is dialed immediately</li> <li>• <b>[2-7]xx:</b> A regular 3 digit extension that does not start with 9 or 8 or 1 is dialed immediately</li> <li>• <b>[2-7]xxx:</b> A regular 4 digit extension that does not start with 9 or 8 or 1 is dialed immediately</li> <li>• <b>[8]xxx:</b> A 3 digit extension prefixed with an 8 (routes calls directly to voicemail of extension xxx)</li> <li>• <b>[8]xxxx:</b> A 4 digit extension prefixed with an 8 (routes calls directly to voicemail of extension xxxx)</li> <li>• <b>T:</b> Refers to the <b>Dialing Timeout</b>.</li> </ul> <p>■ <b>Using ';' separator:</b> An 'x' in the pattern indicates any digit. ';' separates between patterns.</p> <p>For example: '10x;05xxxxxxxx;4xxx'.</p> <p>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.</p> |
| voip/signalling/sip/number_rules | <p>This parameter works in conjunction with the parameter <b>voip/signalling/sip/digit_map</b> and enables translation of specific patterns to specific SIP destination addresses.</p> <p>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 ';'.</p> <p>The valid value can be up to 256 characters.</p> <p>For example: '4xxx=Line_\\@10.1.2.3'</p> <p>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.</p>  |

## 5.2.5 Configuring Headset LED to Stay On



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.



Headset must be configured as the default audio device for the feature to function (see Section 5.2.6).

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

Use the table as reference:

**Table 30: Headset LED Parameter**

| Parameter                   | Description  |
|-----------------------------|--|
| voip/highlight_audio_device | <p>Allows the headset LED to stay on when the phone is on standby <i>and</i> when it is in conversation mode.</p> <p>Functions only when headset is configured as the default audio device.</p> <p>Configure either:</p> <ul style="list-style-type: none"><li>■ <b>NONE</b> (Default) Headset LED illuminates only when the phone is in conversation mode.</li><li>■ <b>HEADSET</b> = Headset LED illuminates when the phone is on standby <i>and</i> when it is in conversation mode</li></ul> |

## 5.2.6 Configuring Default Audio Device

The default audio device can be configured.

**To configure default audio device:**

Use the table as reference:

**Table 31: Audio Device Parameter**

| Parameter                              | Description   |
|--|---|
| audio/stream/voice_call/0/audio_device | <p>Valid values:</p> <ul style="list-style-type: none"><li>■ TYPE_SPEAKER</li><li>■ BUILTIN_SPEAKER (default)</li><li>■ USB_SPEAKER</li><li>■ BLUETOOTH_SPEAKER</li><li>■ TYPE_HEADSET</li><li>■ USB_HEADSET</li><li>■ BLUETOOTH_HEADSET</li><li>■ TYPE_USB</li><li>■ TYPE_BLUETOOTH</li><li>■ ANALOG (applies to the 445HD and C450HD phones only)</li></ul> <p>Sets the default audio device to answer or initiate a new call when no explicit audio device is set.</p> <p>For example:</p> <ul style="list-style-type: none"><li>■ When pressing the <b>Answer</b> softkey.</li><li>■ When initiating a call by speed dial key, call history or phone directory.</li><li>■ Answering talk event or auto-answer.</li><li>■ When starting to dial in 'on hook' mode.</li></ul> |

## 5.3 Configuring Ring Tones

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

### 5.3.1 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 32: 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 5.3.3). 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.  |

#### 5.3.1.1 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 **external\_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 18: Example of the Alert-Info Header**



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

### 5.3.2 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 33: Regional Parameters**

| Parameter   | Description   |
|---|---|
| voip/regional_settings/selected_country   | <p>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:</p> <ul style="list-style-type: none"> <li>■ Israel</li> <li>■ China</li> <li>■ France</li> <li>■ Germany</li> <li>■ Netherlands</li> <li>■ UK</li> <li>■ Brazil</li> <li>■ Italy</li> <li>■ Argentina</li> <li>■ Portugal</li> <li>■ Russia</li> <li>■ Australia</li> <li>■ USA (Default)</li> <li>■ India</li> </ul> |
| voip/regional_settings/use_config_file_values   | <p>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.</p> <ul style="list-style-type: none"> <li>■ <b>0</b> - Disable (default)</li> <li>■ <b>1</b> - Enable</li> </ul>   |
| <b>Call Progress Tones (CPT)</b><br><b>Note:</b> Up to 10 CPTs can be configured ( <b>voip/regional_settings/call_progress_tones/0...9</b> ). |   |
| voip/regional_settings/call_progress_tones/%d/enabled   | <p>Enables the specific CPT.</p> <ul style="list-style-type: none"> <li>■ <b>0</b> - Disable</li> <li>■ <b>1</b> - Enable</li> </ul>  |
| voip/regional_settings/call_progress_tones/%d/name  | <p>Defines the name of the CPT.</p>   |
| voip/regional_settings/call_progress_tones/%d/cadence   | <ul style="list-style-type: none"> <li>■ Defines the cadence type of the tone.</li> <li>■ <b>0</b> - Continuous signal</li> <li>■ <b>1</b> - Cadence signal</li> <li>■ <b>2</b> - Burst signal</li> </ul>   |
| voip/regional_settings/call_progress_tones/%d/frequency_a   | <p>Defines the low frequency (in Hz) of the tone.<br/>           Range:300 - 1980 Hz, in steps of 1 Hz.<br/>           Unused frequencies must be set to zero.</p>  |
| voip/regional_settings/call_progress_tones/%d/frequency_b   | <p>Defines the high frequency (in Hz) of the tone.<br/>           Range:300 - 3000 Hz, in steps of 1 Hz.<br/>           Unused frequencies must be set to zero.</p>   |

| Parameter   | Description  |
|---|--|
| voip/regional_settings/call_progress_tones/<br>%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/<br>%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/<br>2/name               | Default: <b>busy_tone</b> 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/<br>%d/tone_on_0         | tone_on_0 to tone_on_3.<br>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/<br>%d/tone_off_0        | tone_off_0 to tone_on_3.<br>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. |

### 5.3.3 Uploading Ring Tones

New Ring Tones can be uploaded.



- 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 34: Ring Tone Parameters**

| Parameter  | Description  |
|--|--|
| provisioning/ring_tone_uri   | <p>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.</p> <p>For example: <b>provisioning/ring_tone_uri=tones.tgz</b></p> <p><b>Note:</b></p> <ul style="list-style-type: none"> <li>■ The ringtone file is downloaded only after boot up, and not periodically.</li> <li>■ If the tones file is new, the phone updates the information, but does not reboot.</li> <li>■ 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.</li> </ul> |
| personal_settings/lines/0/ring_tone -<br>personal_settings/lines/3/ring_tone | <p>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: <b>Ring01 - Ring11</b>. There is also a silent option.</p>  |

### 5.3.4 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 35: Configuring the Phone to Play a Fast Busy Tone when Automatically Disconnected on Remote Side**

| Parameter                                     | Description   |
|---|---|
| enable_remote_disconnect_warningTone          | <p>Allows you to enable or disable playing a fast busy tone if the phone is automatically disconnected on the remote side.</p> <ul style="list-style-type: none"> <li>■ <b>0</b> (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.</li> <li>■ <b>1</b> 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).</li> </ul> |
| voip/dialing/automatic_disconnect_delay_timer | <p>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.</p>  |



## 5.4 Configuring Media Settings

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

### 5.4.1 Configuring Media Streaming

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

**Table 36: Media Streaming Parameters**

| Parameter                              | Description   |
|--|---|
| voip/media/rtp_mute_on_hold            | Mute sending RTP packets to remote in HOLD state. <ul style="list-style-type: none"> <li>■ <b>0</b> - Disabled. RTP packets are sent to remote end when in HOLD state.</li> <li>■ <b>1</b> - Enabled (default). RTP packets are not sent to remote end when in HOLD state.</li> </ul> |
| voip/media/allow_multiple_rtp          | Defines whether to allow multiple RTP streams from different remote ends to be played toward the phone in a single call. <ul style="list-style-type: none"> <li>■ <b>0</b> = Disable (default)</li> <li>■ <b>1</b> = Enable</li> </ul>  |
| voip/media/ignore_rfc_2833_packets     | Defines whether to ignore playing DTMF when RFC 2833 arrives from the network. <ul style="list-style-type: none"> <li>■ <b>0</b> = Disable</li> <li>■ <b>1</b> = Enable (default)</li> </ul>  |
| voip/media/broken_connection_detection | If enabled an active call will be automatically disconnected if no RTP packet is received within pre-defined time. <ul style="list-style-type: none"> <li>■ <b>0</b> = Disable</li> <li>■ <b>1</b> = Enable (default)</li> </ul>  |
| 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.  |

## 5.4.2 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 37: 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.<br>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.<br>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. |

## 5.4.3 Configuring RTP QoS

RTP QoS can be configured.

**To configure RTP QoS:**

Use the table as reference:

**Table 38: 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 <b>0xb8</b> .<br>Values can be set in decimal (e.g., 184) or hexadecimal (e.g., 0xb8). Default: 184. |

## 5.4.4 Configuring Codecs

### To define the Codecs:

Use the table as reference:

**Table 39: Codec Parameters**

| Parameter                               | Description   |
|---|---|
| voip/codec/codec_info/%d/enabled        | <p>Determines the codecs that you want to implement and their priority. Up to five codecs can be configured, where the first codec (i.e., <b>voip/codec/0/...</b>) 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.</p> <p>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.</p> <p>The <b>%d</b> variable stands for the priority:</p> <ul style="list-style-type: none"> <li>■ <b>0</b> - Disabled</li> <li>■ <b>1</b> (default) - Enabled</li> </ul> |
| voip/codec/codec_info/%d/name           | <p>Name of the codec. The variable <b>%d</b> depicts the index number of the codec entry and its priority, where the first codec (i.e. <b>voip/codec/codec_info/0/name=...</b>) has the highest priority. The valid codec parameters are:</p> <ul style="list-style-type: none"> <li>■ <b>G722</b> G.722 (default)</li> <li>■ PCMA G.711 A-Law</li> <li>■ PCMU G.711 Mu-Law</li> <li>■ G729 G.729</li> <li>■ OPUS</li> </ul> <p>For example, <b>voip/codec/codec_info/0/name=G.722</b></p> <p><b>Note:</b></p> <ul style="list-style-type: none"> <li>■ 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'.</li> </ul>  |
| voip/media/opus_payload                 | <p>Allows the network administrator to configure the OPUS dynamic payload type. Default: 111.</p>   |
| voip/codec/opus/%d /ptime               | <p>Packetization time - length of the digital voice segment that each packet holds. The default is 20 millisecond packets.</p>  |
| voip/codec/opus/jitter_buffer/min_delay | <p>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).</p> <ul style="list-style-type: none"> <li>■ Range: 30-500. Default: 30.</li> </ul>  |

## 5.5 Configuring Voice Settings

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

### 5.5.1 Configuring Gain Control

See Section 5.9.1 for detailed information.

### 5.5.2 Configuring Jitter Buffer

Jitter Buffer can be configured.

**To define Jitter Buffer:**

Use the table as reference:

**Table 40: 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).<br>■ 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.<br>■ Range: 0 to 13. Default: 10.   |

### 5.5.3 Configuring Silence Compression

The Silence Compression feature can be configured.

**To configure Silence Compression:**

Use the table as reference:

**Table 41: Silence Compression Parameters**

| Parameter                              | Description  |
|--|--|
| voip/audio/silence_compression/enabled | Enables silence compression for reducing network bandwidth consumption.<br>■ 0 = Disable (default)<br>■ 1 = Enable |

## 5.6 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:

**Table 42: Line Parameters**

| Parameter                       | Description   |
|---------------------------------|---|
| voip/line/0-5/enabled           | Activates or deactivates the line.<br><b>0</b> = Disabled (this is the default for the second line and higher in the configuration file)<br><b>1</b> = Enabled (this is the default for the first line <b>voip/line/0/</b> 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).<br>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).<br>The authentication password can be up to 35 characters.   |
| voip/line/0-5/extension_display | Defines 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         | 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. |



- You can activate DnD per phone line (see Section [5.8.7](#)).

## 5.7 Enabling Phone Lock

The 425HD, 445HD, and C450HD IP Phones support the capability to automatically lock after a preconfigured period of time. The feature secures the phone against unwanted (mis)use.

When the phone is locked:

- Incoming calls are allowed
- Outgoing calls are not allowed
- Voice Mail, Call Log, and Contacts cannot be accessed

To enable the feature:

**Table 43: PIN Lock Parameter**

| Parameter Name                      | Description  |
|-------------------------------------|--|
| system/pin_lock/enabled             | Determines whether phone lock option is enabled. <ul style="list-style-type: none"> <li>■ <b>[0]</b> Disable</li> <li>■ <b>[1]</b> Enable (default)</li> </ul>   |
| system/pin_lock/server_configurable | Determines whether IP Phone lock pin code is configurable from server.<br>If enabled, then <i>lync/security/lock_pin</i> parameter contains the pin number used.<br>If disabled, IP Phone user will be prompted to enter a pin code. <ul style="list-style-type: none"> <li>■ <b>[0]</b> Disable</li> <li>■ <b>[1]</b> Enable (default)</li> </ul> |
| lync/security/lock_pin              | Phone lock pin code, the default value is "Null" (no lock code).<br>If this parameter is Null and <i>system/pin_lock/server_configurable</i> is set to Enable, then IP Phone user will be prompted to enter a pin code which will be saved with encryption.  |

## 5.8 Configuring Supplementary Services

Network administrators can configure various supplementary services supported by the phone such as Call Waiting, Call Forwarding, 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.



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 44: General Supplementary Services Parameters**

| Parameter                                   | Description  |
|---|--|
| voip/services/application_server_type       | <p>Defines the type of the application server to which the device is registered.</p> <ul style="list-style-type: none"> <li>■ <b>Generic</b> Generic (default)</li> <li>■ <b>Asterisk</b> Asterisk</li> <li>■ <b>FreeSWITCH</b> FreeSWITCH</li> <li>■ <b>BSFT</b> BroadSoft</li> </ul> <p><b>Note:</b></p> <ul style="list-style-type: none"> <li>■ Parameters unique to the selected application server become applicable in addition to this page's parameters.</li> </ul> |
| system/current_user_presence_status/enabled | <p>Only displayed if the application server selected [FreeSWITCH] supports it. Enables the presence feature. The <b>DND</b> softkey on the phone is replaced by <b>Status</b>; the phone shows and publishes the presence status.</p>  |
| system/feature_key_synchronization/enabled  | <p>Applies only to the BroadSoft application server. See section <a href="#">C.1.2</a> for more information.</p>   |

## 5.8.2 Configuring Call Waiting

Call Waiting can be configured.

**To configure call waiting:**

Use the table as reference:

**Table 45: Call Waiting Parameters**

| Parameter  | Description  |
|--|--|
| voip/services/call_waiting/enabled               | Enables the Call Waiting feature. <ul style="list-style-type: none"><li>■ <b>0</b> = Disable</li><li>■ <b>1</b> = Enable (default)</li></ul>   |
| voip/services/call_waiting/sip_reply             | Determines the SIP response that is sent when another call arrives while a call is in progress: <ul style="list-style-type: none"><li>■ <b>RINGING</b> - 180 Ringing</li><li>■ <b>QUEUED</b> (default) - 182 Queued</li></ul>    |
| voip/services/call_waiting/generate_tone/enabled | Determines whether the phone plays a call waiting tone: <ul style="list-style-type: none"><li>■ <b>0</b> The phone doesn't play a call waiting tone.</li><li>■ <b>1</b> The phone plays a call waiting tone (default).</li></ul> |



### 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 B for detailed information).

#### To configure call forwarding:

Use the table as reference:

**Table 46: Call Forward Parameters**

| Parameter   | Description   |
|---|---|
| voip/line/n/call_forward/enabled<br><b>C450HD/445HD:</b> n = [0-29]<br><b>425HD:</b> n= [0-7]               | Enables the Call Forward feature.<br><ul style="list-style-type: none"> <li>■ 0 = Disable</li> <li>■ 1 = Enable (default)</li> </ul>  |
| voip/line/n/call_forward_always/activated   | Activates call forwarding to always, incoming calls are forwarded independently of the status of the line.<br><ul style="list-style-type: none"> <li>■ 0 (default) - Disable</li> <li>■ 1 Enable</li> </ul>   |
| voip/line/n/call_forward_always/destination<br><b>C450HD/445HD:</b> n = [0-29]<br><b>425HD:</b> n= [0-7]    | The destination to which the call is directed when call forward to always is activated.   |
| voip/line/n/call_forward_busy/activated<br><b>C450HD/445HD:</b> n = [0-29]<br><b>425HD:</b> n= [0-7]        | Activates call forwarding to busy, incoming calls are forwarded only if the phone is busy.<br><ul style="list-style-type: none"> <li>■ 0 (default) - Disable</li> <li>■ 1 Enable</li> </ul>   |
| voip/line/n/call_forward_busy/destination<br><b>C450HD/445HD:</b> n = [0-29]<br><b>425HD:</b> n= [0-7]      | The destination to which the call is directed when call forward to busy is activated.   |
| voip/line/n/call_forward_no_answer/activated<br><b>C450HD/445HD:</b> n = [0-29]<br><b>425HD:</b> n= [0-7]   | Activates call forwarding to no answer, incoming calls are forwarded only if the phone does not answer before a user-defined timeout.<br><ul style="list-style-type: none"> <li>■ 0 (default) - Disable</li> <li>■ 1 Enable</li> </ul>  |
| voip/line/n/call_forward_no_answer/destination<br><b>C450HD/445HD:</b> n = [0-29]<br><b>425HD:</b> n= [0-7] | The destination to which the call is directed when call forward to no answer is activated.  |
| voip/line/n/call_forward_no_answer/timeout<br><b>C450HD/445HD:</b> n = [0-29]<br><b>425HD:</b> n= [0-7]     | 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.<br><br>If feature key sync enabled, this parameter defines as 'number of rings'. For example, if the BroadSoft Feature Key is enabled and 'voip/call_forward/timeout_mode' is configured to RINGS_COUNT, the phone will by default ring 2r (2 rings) before the call is forwarded. |

| Parameter                      | Description  |
|--------------------------------|--|
| voip/call_forward/timeout_mode | The 'Forward No Reply' timeout mode. <ul style="list-style-type: none"><li>■ SECONDS (default)</li><li>■ RINGS_COUNT</li></ul> |

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 47: Conference Parameters**

| Parameter                             | Description  |
|---------------------------------------|--|
| voip/services/conference/mode         | Sets the conference mode (when establishing 3-Way Conference).<br><b>LOCAL</b> = phone will establish the conference by itself.<br><b>REMOTE</b> = phone will use remote media server to establish the conference. |
| voip/services/conference/conf_ms_addr | Relevant only if 'Mode'(above) is <b>REMOTE</b> .<br>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 48: 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).<br>■ <b>0</b> = Disable (default)<br>■ <b>1</b> = 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.<br>■ 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.<br>The valid value can be up to 32 characters.  |

## 5.8.6 Configuring Automatic Answer

The Automatic Answer feature is configured.

Use the table as reference:

**Table 49: Automatic Answer Parameters**

| Parameter                         | Description   |
|-----------------------------------|---|
| voip/auto_answer/enabled          | <p>Enables the Automatic Answering feature.</p> <ul style="list-style-type: none"> <li>■ <b>0</b> = Disable (default)</li> <li>■ <b>1</b> = Enable</li> </ul> <p>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:</p> <ul style="list-style-type: none"> <li>■ <b>Phone answers after a timeout:</b> The phone automatically answers the call after a timeout if the INVITE message includes a SIP Call-Info header with a tag value, <b>answer-after=</b> 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.</li> <li>■ <b>Phone answers immediately:</b> The phone answers the call immediately in any of the following cases: <ul style="list-style-type: none"> <li>■ If the SIP Alert-Info header contains the tag value <b>ring answer</b>.</li> <li>■ If the SIP Alert-Info header contains the tag value <b>info=alert-autoanswer</b>.</li> </ul> </li> </ul> <p><b>Note:</b></p> <ul style="list-style-type: none"> <li>■ If the SIP Call-Info header includes all the above answer types or any two different types (i.e., <b>answer-after=</b>, <b>ring answer</b>, and <b>alert-autoanswer</b>), the <b>answer-after=</b> type takes precedence.</li> <li>■ If there is an existing call when an INVITE message for automatic answer is received, the existing call is automatically put on hold.</li> </ul> |
| voip/talk_event/enabled           | <p>Enables the 'talk' event feature.</p> <ul style="list-style-type: none"> <li>■ <b>0</b> = Disable (default)</li> <li>■ <b>1</b> = Enable</li> </ul> <p>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.</p>  |
| voip/advanced_auto_answer/timeout | <p>The timeout before the call is answered (in seconds). Range: 0 – 60 (seconds)</p> <ul style="list-style-type: none"> <li>■ <b>5</b> = 5 seconds (default)</li> <li>■ <b>0</b> = immediately</li> </ul>   |
| voip/advanced_auto_answer/type    | <ul style="list-style-type: none"> <li>■ <b>SIP_Header</b> (default) = identical to the parameter 'voip/auto_answer/enabled' described above</li> <li>■ <b>Manual</b> = the phone automatically answers incoming calls according to the timeout configured in the 'voip/advanced_auto_answer/timeout' parameter</li> </ul>  |

| Parameter                          | Description  |
|------------------------------------|--|
| voip/auto_answer_use_180/enabled=0 | <p>Determines whether or not the phone will ring before auto answer, or if auto answer will occur immediately, before the phone rings.</p> <ul style="list-style-type: none"><li>■ <b>0</b> = Disable (default) = No ringing occurs before auto answer; auto answer occurs immediately</li><li>■ <b>1</b> = Enable – Ringing occurs before auto answer</li></ul> |



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 [C.1.3](#)).

#### To configure DnD:

Use the table as reference:

**Table 50: Do Not Disturb Parameters**

| Parameter  | Description  |
|--|--|
| voip/line/n/do_not_disturb/enabled<br><b>C450HD/445HD:</b> n = [0-29]<br><b>425HD:</b> n = [0-7]   | Enables the DND feature. <ul style="list-style-type: none"><li>■ <b>0</b> = Disable</li><li>■ <b>1</b> = Enable (default)</li></ul>  |
| voip/line/n/do_not_disturb/activated<br><b>C450HD/445HD:</b> n = [0-29]<br><b>425HD:</b> n = [0-7] | Activates the DnD feature per phone line, if the parameter is enabled. <ul style="list-style-type: none"><li>■ <b>0</b> = Disable(default)</li><li>■ <b>1</b> = Enable</li></ul> |

#### To configure DnD on the phone:

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

### 5.8.8 Configuring Call Pick Up

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 51: 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'.<br><ul style="list-style-type: none"><li>■ 0 = Disable</li><li>■ 1 = Enable</li></ul>   |
| 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.<br>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 52: MWI Parameters**

| Parameter  | Description  |
|--|--|
| voip/services/msg_waiting_ind/voice_mail_number        | Defines the extension number for accessing your voice mail messages.<br>■ The valid value is up to 64 characters.  |
| voip/services/msg_waiting_ind/enabled                  | Enables the MWI feature.<br>■ 0 = Disable<br>■ 1 = Enable (default)  |
| voip/services/msg_waiting_ind/subscribe                | Determines whether the phone registers to an MWI server.<br>■ 0 = Disable (default)<br>■ 1 = Enable  |
| voip/services/msg_waiting_ind/subscribe_address        | The IP address or host name of the MWI server.<br>Default: 0.0.0.0   |
| voip/services/msg_waiting_ind/subscribe_port           | The port number of the MWI server.<br>Range: 1024-65535. Default: 5060.  |
| voip/services/msg_waiting_ind/expiration_timeout       | The interval between the MWI Subscribe messages.<br>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.<br>■ 0 = Disable<br>■ 1 = Enable (default)  |
| voip/sub/contact_type/enable                           | To disable sending Subscribe messages, set the following parameter to disable sending Subscribe messages:<br>0=Disable sending Subscribe messages<br>1=Enable sending Subscribe messages (default) |
| voip/services/busy_lamp_field/local_presence_for_lines | To disable local presence, set the following parameter to disable sending Subscribe messages:<br>0=Disable local presence (default)<br>1=Enable local presence                                     |



### 5.8.10 Configuring Busy Lamp Field

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

#### To configure BLF:

Use the table as reference:

**Table 53: BLF Parameters**

| Parameter  | Description   |
|--|---|
| voip/services/busy_lamp_field/enabled                          | Enables the BLF feature: <ul style="list-style-type: none"> <li>■ 0 = Disable</li> <li>■ 1 = Enable (default)</li> </ul>  |
| 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 <b>BSFT</b> . The user resource list. This must be the username (not the domain name). For example, if the URI resource list is <b>mylist@server.com</b> , then only the value <b>mylist</b> 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 <b>BSFT</b> . 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. <ul style="list-style-type: none"> <li>■ 0 = Disable (default)</li> <li>■ 1 = Enable</li> </ul> |
| voip/services/busy_lamp_field/application_server/addr          | Only displayed if 'Type' is set to <b>BSFT</b> and the 'voip/services/busy_lamp_field/application_server/use_registrar' parameter is set to <b>0</b> . Defines the IP address or host name of the application server. The valid value is up to 64 characters. Default: 0.0.0.0  |
| <b>BLF Call Pickup</b>   |   |
| 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 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 54: Reminder Tone after Long Hold**

| Parameter             | Description   |
|-----------------------|---|
| voip/lhcwrr_enabled   | <p>Enables the feature.</p> <p><b>1</b> Enabled. After the length of time configured for configuration file parameter <i>voip/lhcwrr_wait_time</i> lapses (see the parameter below), a reminder tone (beep) is played every 10 seconds until the call is taken off hold.</p> <p><b>0</b> Disabled (Default). No reminder tone (beep) is played, regardless of how long the call is on hold.</p> |
| voip/lhcwrr_wait_time | <p>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.</p>  |

### 5.8.12 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 55: Onhook Disconnect when Held**

| Parameter                                | Description   |
|--|---|
| voip/onhook_disconnect_when_held/enabled | <p>Choose either:</p> <ul style="list-style-type: none"> <li>■ <b>0</b> = 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.</li> <li>■ <b>1</b> = Enable - If the receiver is placed on-hook after a call is put on hold, the call is disconnected.</li> </ul> |

### 5.8.13 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 56: Configuring the Ringer's Default Audio Device**

| Parameter                          | Description  |
|------------------------------------|--|
| audio/stream/ringer/0/audio_device | <p>Determines which device rings when a call comes in. Valid values are:</p> <ul style="list-style-type: none"> <li>■ TYPE_SPEAKER</li> <li>■ BUILTIN_SPEAKER (default)</li> <li>■ USB_SPEAKER</li> <li>■ BLUETOOTH_SPEAKER</li> <li>■ TYPE_HEADSET</li> <li>■ USB_HEADSET</li> <li>■ BLUETOOTH_HEADSET</li> <li>■ TYPE_USB</li> <li>■ TYPE_BLUETOOTH</li> <li>■ ANALOG (applies to the 445HD and C450HD phones only)</li> </ul> |

### 5.8.14 Allowing an Incoming Call when the Phone is Locked

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 57: Allowing an Incoming Call when the Phone is Locked**

| Parameter  | Description   |
|--|---|
| system/lock/n/allow_incoming_calls<br><b>C450HD/445HD:</b> n = [0-29]<br><b>425HD:</b> n = [0-7] | <p>Allows incoming calls when the phone is locked (default). If allowed, the user can answer an incoming call without the unlock password.</p> <ul style="list-style-type: none"> <li>■ If not allowed, the incoming call will be automatically rejected by the phone.</li> </ul> |
| system/lock/n/enabled<br><b>C450HD/445HD:</b> n = [0-29]<br><b>425HD:</b> n = [0-7]              | Enables the phone's lock feature.   |
| system/lock/n/activated<br><b>C450HD/445HD:</b> n = [0-29]<br><b>425HD:</b> n = [0-7]            | To Activate lock feature on a specific line(s).   |

### 5.8.15 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 58: Configuring a Softkey with Attended and Blind Call Transfer Functionality**

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

#### 5.8.15.1 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 59: Changing TRANSFER Key Functionality**

| Parameter                                    | Description  |
|--|--|
| voip/signalling/sip/hk_blind_transfer/enable | Changes the hard TRANSFER key's functionality from performing blind transfer (default) to performing consultative transfer.<br><ul style="list-style-type: none"> <li>■ <b>0</b> TRANSFER hard key performs Consultative Transfer</li> <li>■ <b>1</b> TRANSFER hard key performs Blind Transfer (default)</li> </ul> |

### 5.8.16 Configuring 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
```

### 5.8.17 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.



The feature is not supported on:

C450HD phones without an Expansion Module (the feature *is supported* on these phones when they have an Expansion Module)

#### 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 60: Call Park Parameters**

| Parameter Name                        | Value                                 | Type   | Description  |
|---------------------------------------|---------------------------------------|--------|--|
| personal_settings/parking_lot/enabled | 1                                     | Bool   | Enable/Disable call park feature<br><ul style="list-style-type: none"> <li>■ 0 = Disabled</li> <li>■ 1 = Enable (Default)</li> </ul> |
| voip/services/call_parking/method     | INVITE                                | String | Method used for Call Parking<br><ul style="list-style-type: none"> <li>■ INVITE (Default)</li> <li>■ INFO</li> </ul>                 |
| voip/services/busy_lamp_field/enabled | 1                                     | Bool   | BLF support<br><b>0</b> =Disable<br><b>1</b> =Enable (default)]  |
| voip/services/park_with_refer         | 1                                     | Bool   | Automatic blind transfer for parking<br><b>0</b> =Disable (default)<br><b>1</b> =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 61: 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.



It's strongly advised 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.



It's strongly advised *not* to change the default values.

#### To configure tone volume:

Use the table as reference:

**Table 62: 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.<br>The valid range is:<br><b>445HD/C450HD:</b> Range: [0 to 31 dB], Default: 2 dB<br><b>425HD:</b> Range: [1 to 31 dB], Default: 16 dB |

### 5.9.3 Configuring Ringer Volume

The ringer volume can be configured.



It's strongly advised *not* to change the default values.

#### To configure the ringer volume:

Use the table as reference:

**Table 63: 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.<br>The valid range is -32 to 31 dB, Default: 0 dB |

## 5.9.4 Configuring Speaker Volume

The speaker volume can be configured.



It's strongly advised *not* to change the default values.

To configure speaker volume:

Use the table as reference:

**Table 64: Speaker Parameters**

| Parameter   | Description  |
|---|--|
| <b>Hands-free Gain Parameters</b><br><b>Note:</b> Values are in decibels (dB)<br>Decimal places: Use underscore instead of period (e.g., <b>plus19_5db</b> ). |  |
| voip/audio/gain/NB/handsfree_digital_input_gain   | Digital input gain (in dB) – Narrow Band.<br><b>425HD/445HD:</b> Default = 0.<br><b>C450HD:</b> Default = -6.<br>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.<br><b>425HD:</b> Default = 3<br><b>445HD:</b> Default = -8<br><b>C450HD:</b> Default = -10<br>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.<br><b>425HD/445HD:</b> Default = 0.<br><b>C450HD:</b> Default = -6.<br>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.<br><b>425HD:</b> Default = -12<br><b>445HD:</b> Default = -8<br><b>C450HD:</b> Default = -10<br>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.<br>Valid values: <b>0db</b> (default), <b>minus1_5db</b> , <b>minus3db</b> , <b>minus4_5db</b> , <b>minus6db</b> , <b>minus7_5db</b> , <b>minus9db</b> , <b>minus10_5db</b> , <b>minus12db</b> , <b>minus13_5db</b> , <b>minus15db</b> , <b>minus16_5db</b> , <b>minus18db</b> , <b>minus19_5db</b> , <b>minus21db</b> , <b>minus22_5db</b> , <b>minus24db</b> , <b>minus25_5db</b> , <b>minus27db</b> , <b>minus28_5db</b> , <b>minus30db</b> , <b>minus31_5db</b> , <b>minus33db</b> , <b>minus34_5db</b> , <b>minus36db</b> , <b>minus37_5db</b> , <b>minus39db</b> , <b>minus40_5db</b> , <b>minus42db</b> , <b>minus48db</b> , <b>minus54db</b> , <b>MUTE</b> |



| Parameter                                       | Description   |
|---|---|
| voip/audio/gain/WB/handsfree_analog_output_gain | Analog output gain (in dB) – Wide Band.<br>Valid values:<br><b>0db</b> (default), <b>minus1_5db</b> , <b>minus3db</b> , <b>minus4_5db</b> , <b>minus6db</b> , <b>minus7_5db</b> , <b>minus9db</b> , <b>minus10_5db</b> , <b>minus12db</b> , <b>minus13_5db</b> , <b>minus15db</b> , <b>minus16_5db</b> , <b>minus18db</b> , <b>minus19_5db</b> , <b>minus21db</b> , <b>minus22_5db</b> , <b>minus24db</b> , <b>minus25_5db</b> , <b>minus27db</b> , <b>minus28_5db</b> , <b>minus30db</b> , <b>minus31_5db</b> , <b>minus33db</b> , <b>minus34_5db</b> , <b>minus36db</b> , <b>minus37_5db</b> , <b>minus39db</b> , <b>minus40_5db</b> , <b>minus42db</b> , <b>minus48db</b> , <b>minus54db</b> , <b>MUTE</b> |
| voip/audio/gain/NB/handsfree_analog_input_gain  | Analog input gain (in dB) – Narrow Band<br>Valid values: <b>0db</b> , <b>plus1_5db</b> , <b>plus3db</b> , <b>plus4_5db</b> , <b>plus6db</b> , <b>plus7_5db</b> , <b>plus9db</b> , <b>plus10_5db</b> , <b>plus12db</b> , <b>plus13_5db</b> , <b>plus15db</b> , <b>plus16_5db</b> , <b>plus18db</b> , <b>plus19_5db</b> , <b>plus21db</b> , <b>plus22_5db</b> , <b>plus24db</b> , <b>plus25_5db</b> , <b>plus27db</b> , <b>plus28_5db</b> , <b>plus30db</b> , <b>plus31_5db</b> , <b>plus33db</b> , <b>plus34_5db</b> , <b>plus36db</b> , <b>plus37_5db</b> , <b>plus39db</b> (default), <b>plus40_5db</b> , <b>PLUS42DB</b> , <b>plus48db</b> , <b>plus54db</b> , <b>MUTE</b>                                  |
| voip/audio/gain/WB/handsfree_analog_input_gain  | Analog input gain (in dB) – Wide Band.<br>Valid values: <b>0db</b> , <b>plus1_5db</b> , <b>plus3db</b> , <b>plus4_5db</b> , <b>plus6db</b> , <b>plus7_5db</b> , <b>plus9db</b> , <b>plus10_5db</b> , <b>plus12db</b> , <b>plus13_5db</b> , <b>plus15db</b> , <b>plus16_5db</b> , <b>plus18db</b> , <b>plus19_5db</b> , <b>plus21db</b> , <b>plus22_5db</b> , <b>plus24db</b> , <b>plus25_5db</b> , <b>plus27db</b> , <b>plus28_5db</b> , <b>plus30db</b> , <b>plus31_5db</b> , <b>plus33db</b> , <b>plus34_5db</b> , <b>plus36db</b> , <b>plus37_5db</b> , <b>plus39db</b> (default), <b>plus40_5db</b> , <b>PLUS42DB</b> , <b>plus48db</b> , <b>plus54db</b> , <b>MUTE</b>                                   |
| voip/audio/gain/NB/additional_speaker_gain      | Additional parameter for speaker gain configuration, for Narrow Band.<br>Valid values:<br><ul style="list-style-type: none"> <li>■ <b>0</b> 0dB</li> <li>■ <b>1</b> 1dB</li> <li>■ <b>2</b> 2dB</li> <li>■ <b>3</b> 3Db (default)</li> </ul>  |
| voip/audio/gain/WB/additional_speaker_gain      | Additional parameter for speaker gain configuration, for Wide Band.<br>Valid values:<br><ul style="list-style-type: none"> <li>■ <b>0</b> 0dB</li> <li>■ <b>1</b> 1dB</li> <li>■ <b>2</b> 2dB</li> <li>■ <b>3</b> 3dB (default)</li> </ul>  |

## 5.9.5 Configuring Handset Volume

The handset volume can be configured.



It's strongly advised *not* to change the default values.

### To configure handset volume:

Use the table as reference:

**Table 65: Handset Gain Parameters**

| Parameter                                      | Description   |
|--|---|
| <b>Handset Gain Parameters</b>                 |   |
| <b>Note:</b> Values are in decibels (dB)       |   |
| voip/audio/gain/NB/handset_digital_input_gain  | Digital input gain (in dB) – Narrow Band.<br><b>425HD:</b> Default = 0<br><b>445HD:</b> Default = 2<br><b>C450HD:</b> Default = -2<br>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.<br><b>425HD:</b> Default = 2<br><b>445HD:</b> Default = 0<br><b>C450HD:</b> Default = -2<br>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.<br><b>425HD:</b> Default = -6<br><b>445HD:</b> Default = -5<br><b>C450HD:</b> Default = -8<br>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.<br>Valid values:<br><b>0dB, minus1_5db, minus3db, minus4_5db, minus6db, minus7_5db, minus9db (default), 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, minus40_5db, minus42db, minus48db, minus54db, MUTE</b> |

| Parameter                                     | Description  |
|---|--|
| voip/audio/gain/WB/handset_analog_output_gain | <p>Analog output gain (in dB), for Wide Band.</p> <p>Valid values:</p> <p><b>0dB, minus1_5db, minus3db, minus4_5db, minus6db, minus7_5db, minus9db (default), 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, minus40_5db, minus42db, minus48db, minus54db, MUTE</b></p> |
| voip/audio/gain/NB/handset_analog_input_gain  | <p>Analog input gain (in dB), for Narrow Band.</p> <p>Valid values:</p> <p><b>0dB, plus1_5dB, plus3dB, plus4_5dB, plus6dB, plus7_5dB, plus9dB, plus10_5dB, plus12dB, plus13_5dB, plus15dB, plus16_5dB, plus18dB, plus19_5dB (default), 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</b></p>                              |
| voip/audio/gain/WB/handset_analog_input_gain  | <p>Analog input gain (in dB), for Wide Band.</p> <p>Valid values:</p> <p><b>0dB, plus1_5dB, plus3dB, plus4_5dB, plus6dB, plus7_5dB, plus9dB, plus10_5dB, plus12dB, plus13_5dB, plus15dB, plus16_5dB, plus18dB, plus19_5dB (default), 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</b></p>                                |
| voip/audio/gain/handset_analog_sidetone_gain  | <p>Analog side tone gain (in db).</p> <p>Valid values: <b>minus9db, MINUS12db, minus15db, minus18db, minus21db, minus24db, minus27db, MUTE</b></p> <p>Default value:</p> <p><b>425HD: MINUS12DB</b></p> <p><b>445HD/C450HD: MINUS18DB</b></p>  |

## 5.9.6 Configuring Headset Volume

Headset volume can be configured.



It's strongly advised *not* to change the default values.

**To configure headset volume:**

Use the table as reference:

**Table 66: Headset Gain Parameters**

| Parameter  | Description  |
|--|--|
| <b>Headset Gain Parameters</b><br><b>Note:</b> Values are in decibels (dB)<br>■ Decimal places: Use underscore instead of period (e.g., <b>plus19_5db</b> ). |  |
| voip/audio/gain/NB/headset_digital_input_gain  | Digital input gain (in dB) – Narrow Band.<br>Default value:<br><b>425HD/445HD:</b> Default = 0<br><b>C450HD:</b> Default = -4<br>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.<br>Default value:<br><b>425HD:</b> Default = -4<br><b>445HD:</b> Default = -8<br><b>C450HD:</b> Default = -12<br>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.<br>Default value:<br><b>425HD/445HD:</b> Default = 0<br><b>C450HD:</b> Default = -4<br>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.<br>Valid values: <b>0DB, minus1_5db, minus3db, minus4_5db, minus6db, minus7_5db, minus9db, minus10_5db, minus12db (default), 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, minus40_5, minus42db, minus48db, minus54db, MUTE</b> |
| voip/audio/gain/WB/headset_analog_output_gain  | As above, but for Wide Band.   |

| Parameter                                    | Description  |
|--|--|
| voip/audio/gain/NB/headset_analog_input_gain | Analog input gain (in dB).<br>Valid values: <b>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 (default), plus34_5db, plus36db, plus37_5db, plus39db, plus40_5db, plus42db, plus48db, plus54db, MUTE</b> |
| voip/audio/gain/WB/headset_analog_input_gain | Analog input gain (in dB).<br>Valid values: <b>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 (default), plus34_5db, plus36db, plus37_5db, plus39db, plus40_5db, plus42db, plus48db, plus54db, MUTE</b> |
| voip/audio/gain/headset_analog_sidetone_gain | Analog side tone gain (in db).<br>Valid values: <b>minus9db, MINUS12DB (default), minus15db, minus18db, minus21db, minus24db, minus27db, MUTE</b>  |

## 5.10 Prioritized of Incoming Calls Displayed

The priority of incoming calls can be set so that older calls get displayed higher on the list than newer calls.

**Table 67: Older of incoming calls**

| Parameter  | Description  |
|--|--|
| personal_settings/incoming_call_fairness/enabled | Older incoming calls get prioritized over newer incoming calls.<br>0 = Disable (default)<br>1 = Enable |

## 5.11 UI to Return to Idle Screen Timeout

**Table 68: UI to Return to Idle Screen Timeout**

| Parameter                                    | Description  |
|--|--|
| personal_settings/GetBackToIdleScreenTimeout | Defines the number of sec the IdleScreen will return to idle screen. If this parameter is set to 0 then timeout is disabled. Range 0 to 180<br>Default=0 |

## 5.12 Call No Answer Timeout

- `call_no_answer_timeout` parameter is used to stop unanswered calls from ringing after a specific timeout.

| Parameter name                                    | Description  |
|---|--|
| <code>voip/services/call_no_answer_timeout</code> | <ul style="list-style-type: none"> <li>■ 0 = disabled</li> <li>■ 1-600 = Timeout (in seconds)</li> </ul> |

## 5.13 Emergency Calls

### Define Emergency Phone Call Numbers

This section defines the emergency phone numbers that the device recognizes as emergency calls.

| Parameters                                     | Description  |
|--|--|
| <code>voip/services/emergency_call_list</code> | <p>List of emergency numbers.</p> <p>Maximum String Length = 128 characters</p> <p><b>example:</b> <code>voip/services/emergency_call_list=911 933</code></p> <p>(Use [space] delimiter, without commas)</p> |

### Prevent Caller from Disconnecting

Once an emergency call is placed, only the called emergency service can disconnect the call — the caller cannot terminate it.

| Parameters   | Description   |
|--|---|
| <code>personal_settings/emergency_no_disconnect/enabled</code> | <p>1 = Enable (Prevents caller from ending an emergency call.)</p> <p>0 = Disable (Default)</p> |

## 6 Configuring Phone Settings

### 6.1 Configuring the Phone Directory

#### 6.1.1 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 69: LDAP Parameters**

| Parameter Name             | Description  |
|----------------------------|--|
| system/ldap/enable         | Enables or disables LDAP. Values: <ul style="list-style-type: none"> <li>■ 0 =Disable - (default)</li> <li>■ 1 =Enable</li> </ul>  |
| lync/contact_search_method | Set contact search method: <ul style="list-style-type: none"> <li>■ LDAP</li> <li>■ DISABLE</li> <li>■ LYNC_CONTACT (default)</li> </ul>   |
| system/ldap/TLSMode        | Set LDAP encryption method: <ul style="list-style-type: none"> <li>■ NONE</li> <li>■ OVERTLS</li> <li>■ STARTTLS (default)</li> </ul>  |
| 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 username 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 the search pattern for name lookups: <p><b>Example 1: When you type in the following field:</b></p> <pre>(&amp;(telephoneNumber=*)(sn=%%))</pre> <p>the search result includes all LDAP records, which have the 'telephoneNumber' field set and the '("sn"--&gt;surname)' field starting with the entered prefix.</p> <p><b>Example 2: When you type in the following field:</b></p> <pre>( (cn=%%)(sn=%%))</pre> <p>the search result includes all LDAP records which have the '("cn"--&gt;CommonName)' OR '("sn"--&gt;Surname)' field starting with the entered prefix.</p> <p><b>Example 3: When you type in the following field:</b></p> <pre>(!(cn=%%))</pre> <p>the search result includes all LDAP records which “do not” have the “cn” field starting with the entered prefix.</p> |

| Parameter Name   | Description  |
|--|--|
| system/ldap/number_filter  | Specifies the search pattern for number lookups:<br><b>Example 1: When you type in the following field:</b><br>(   (telephoneNumber=%) (Mobile=%) (ipPhone=%) ),<br>The search result finds LDAP records where 'telephoneNumber,' 'Mobile,' or 'ipPhone' matches the searched number.<br><b>Example 2: When you type in the following field:</b><br>( & (telephoneNumber=%) (sn=*) ) ,<br>The search result finds LDAP records with a set 'sn' (surname) field and a 'telephoneNumber' matching the searched number. |
| system/ldap/max_hits   | Specifies the maximum number of entries expected to be sent by the LDAP server.<br>This parameter is sent to the LDAP server.  |
| system/ldap/send_queries_while_typing  | Sends an LDAP search each time the user presses an alphanumeric key.   |
| system/ldap/DisplayName_attr<br>system/ldap/Title_attr<br>system/ldap/MobileNumber_attr<br>system/ldap/HomePhoneNumber_attr<br>system/ldap/BusinessPhoneNumber_attr<br>system/ldap/Extension_attr<br>system/ldap/SipUri_attr | Specify the data fields to be displayed in search results by assigning the appropriate field names to each parameter (e.g., assign the title field's name to Title_attr). If a specific field does not exist, leave it empty.<br>The attributes specified will be included in the search results for both Name-to-Number and Number-to-Name lookups.   |
| system/ldap/DirectoryDisplayName   | Defines the display name for the 'LDAP Contacts' entry. For example:<br>For a general LDAP server, it can be set to reflect the type of contact information managed by that server (e.g., 'Employee Directory').   |
| system/ldap/network_timeout  | Timeout duration for the connection.   |

### 6.1.2 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 70: Provisioning Parameters**

| Parameter                            | Description   |
|--------------------------------------|---|
| provisioning/corporate_directory_uri | <p>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.</p> <p>For example:<br/> <b>provisioning/corporate_directory_uri=corporate_dir.txt</b></p> <p><b>Note:</b></p> <ul style="list-style-type: none"> <li>■ The corporate directory file is loaded after boot up and after that, periodically.</li> <li>■ If the corporate directory file is new, the phone updates the information and does not reboot.</li> </ul> |
| lync/corporate_directory/enabled     | <p>Enable/Disable <b>corporate directory</b>.</p> <p><b>0</b> = Disable (Default)</p> <p><b>1</b> = Enable</p>  |
| lync/contact_search_method           | <p>Defines contact search method for call extension. Must be set to DISABLE to use local directory. Three values can be set:</p> <ul style="list-style-type: none"> <li>■ DISABLE(Default)</li> <li>■ LDAP</li> <li>■ LYNC_CONTACT</li> </ul>   |
| personal_settings/max_directory_size | <p>Define the max number of contacts for corporate directory.</p> <p>Range: [0-&gt;700]</p> <p>Default: 700</p>   |

## 6.2 Configuring Keys

The network administrator can configure the following keys:

- Function and Programmable Keys (see Section 6.2.1)
- 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 6.2.2.2)

### 6.2.1 Configuring Function and Programmable Keys

On the 445HD phone, 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 6.6). 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 13<sup>th</sup>, the 12<sup>th</sup> Speed Dial shows the page number and the name in the 12<sup>th</sup> moves to the 13<sup>th</sup>.

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 425HD / C450HD, Ability to configure 1-8 Programmable Keys, (configure **n = 0-7** correspondingly).

On the C450HD phone with Expansion Module Ability to support two pages and a total of 40 Functional Keys, (configure **n = 8-27** for the first page and **n = 28-47** for the second page).

**Table 71: 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              | <p>Choose either:</p> <ul style="list-style-type: none"> <li>■ <b>EMPTY</b> = (default) If left as is, the key will be disabled.</li> <li>■ <b>SPEED_DIAL</b> = key to help users quickly dial numbers that are often used or hard to remember.</li> <li>■ <b>PAGING</b> = When the Paging feature is enabled, you can define Paging Groups (see Section 6.6).</li> <li>■ <b>SIP_ACCOUNT</b> = 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).</li> <li>■ <b>Event</b> = Key used to access events like DnD, Missed Call, etc. (See the next parameter for more information).</li> <li>■ <b>Parking_Lot</b> = Gives users the ability to monitor the parking extension (busy, idle) and park/unpark calls by pressing the functional key.</li> <li>■ <b>Speed_Dial_BLF</b> = combined Speed Dial and Busy Lamp Field (BLF) configuration that allows a user to quickly dial a predefined contact while also displaying that contact's line status (such as idle, busy, or ringing) on the device. This enables one-touch calling with real-time visual presence indication.</li> </ul> |
| personal_settings/functional_key/n/key_event         | <ul style="list-style-type: none"> <li>■ Missed_Calls</li> <li>■ Received_Calls</li> <li>■ Dialed_Calls</li> <li>■ Directory</li> <li>■ Dnd_All</li> <li>■ Forward_All</li> </ul>   |
| 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              | <ul style="list-style-type: none"> <li>■ If the functional key 'type' is <b>SIP_ACCOUNT</b>, configure a value corresponding line ID. n = the value you configured as the line index as shown in Section 5.1.3.</li> <li>■ If the functional key 'type' is <b>SPEED_DIAL</b>, configure a value corresponding to the line ID. n = the value you configured as the line index as shown in Section 5.1.3. This allows speed dialing to be initiated by a speed dial calling line of choice. The feature determines through which line the call goes out when speed dialing. The feature only applies to phones configured with multiple lines.</li> </ul>   |

### 6.2.1.1 Configuring a Configuration File for Speed Dials Only

See Section 5.8.16 for more information.

## 6.2.2 Configuring Softkeys

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

**Table 72: 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 73: SoftKey Parameters**

| Parameter Name   | Description  |
|--|--|
| personal_settings/soft_key/n/key_function                | <p>Possible values: <b>n</b> = 0-19. Select one of the following key function types for the idle screen:</p> <ul style="list-style-type: none"> <li>■ NONE</li> <li>■ New_call</li> <li>■ Missed_calls</li> <li>■ Received_calls</li> <li>■ Dialed_calls</li> <li>■ All_calls</li> <li>■ Directory</li> <li>■ Dnd_all</li> <li>■ Forward_all</li> <li>■ PSK</li> </ul> |
| personal_settings/soft_keys/ongoing_call/n/key_function  | <p>Possible values: <b>n</b> = 0-19. Select one of the following key function types for the Ongoing call state:</p> <ul style="list-style-type: none"> <li>■ NONE</li> <li>■ Transfer</li> <li>■ Blind_transfer</li> <li>■ Hold</li> <li>■ Conf</li> <li>■ New_call</li> <li>■ End</li> <li>■ PSK</li> <li>■ Call_Menu</li> <li>■ Rec_call</li> </ul>                  |
| personal_settings/soft_keys/initiate_call/n/key_function | <p>Possible values: <b>n</b> = <b>0-3</b>.</p> <ul style="list-style-type: none"> <li>■ NONE</li> <li>■ Contacts</li> <li>■ Call_Log</li> <li>■ Speed_Dial</li> <li>■ URL</li> </ul>   |

### 6.2.2.1 Disable New Call Softkey in Incoming Call screen

| Parameter                          | Description   |
|------------------------------------|---|
| system/AllowNewCallsDuringIncoming | <p>Disable/Enable <b>New Call</b> Softkey in <b>Incoming Call</b> screen.</p> <ul style="list-style-type: none"> <li>■ <b>0</b> = Disable</li> <li>■ <b>1</b> = Enable (Default)</li> </ul> |

### 6.2.2.2 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
```



You can configure the PSK to perform any action that is supported by your enterprise'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 74: PSK Parameters

| Parameter Name  | Description  |
|---|--|
| personal_settings/soft_keys/n/psk_index<br>personal_settings/soft_keys/ongoing_call/n/psk_index | <p>There are separate index number series for the idle screen and ongoing call screen.</p> <p>For the first parameter (idle screen): <b>n=0-19</b>. Valid values that can be configured: <b>0-11</b>.</p> <p>For the second parameter (ongoing call screen): <b>n=0-19</b>. Valid values that can be configured: <b>0-11</b>.</p> <p>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).</p> |
| personal_settings/soft_keys/psk/n/is_dial_required  | <p>Configure either:</p> <ul style="list-style-type: none"> <li>■ <b>0</b> (disable) (default)</li> <li>■ <b>1</b> (enable)</li> </ul> <p>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.</p> <p>The parameter only applies when 'Programmable SK' is set as the key_function.</p> <p><b>n=0-11</b></p>  |
| personal_settings/soft_keys/psk/n/PSKlabel  | <p>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.</p> <p><b>n=0-11</b></p>   |
| personal_settings/soft_keys/psk/n/prefix  | <p>Defines the prefix which sends a SIP INVITE to the softswitch to activate this feature (event). For example, <b>*70</b>. This parameter only applies when <b>PSK</b> is configured for parameter key_function. Up to 128 characters (any characters).</p>   |

### 6.2.2.3 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.



Paging must be configured as described in Section 6.6 as a prerequisite for the feature to function. Default: Disabled ('voip/services/group\_paging/enabled' = 0).

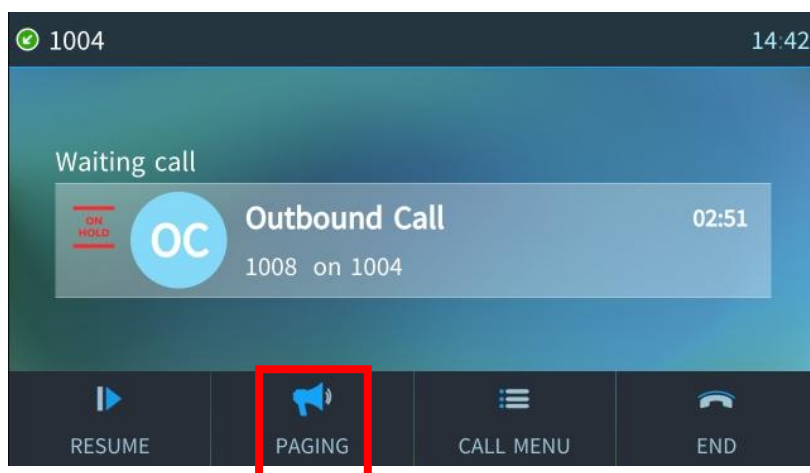
#### To configure a PSK for paging during call hold | ongoing call:

Use the table as reference:

**Table 75: Configuring a PSK for Paging during an Ongoing Call | Call Hold**

| Parameter   | Description                              |
|---|--|
| personal_settings/soft_keys/ongoing_call/n/key_function | Set to <b>PAGING</b> . 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):

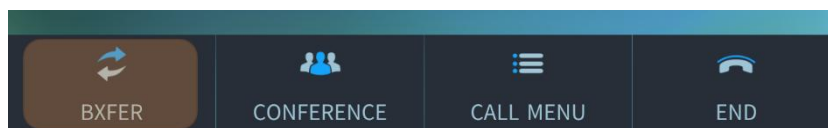




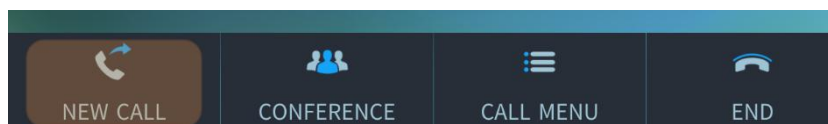
### 6.2.2.4 Configuring a PSK for a Customized UI Experience

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.



## 6.3 Configuring Font Size of Functional Keys

Devices support configurable font sizes for the text displayed on functional keys. This enhancement allows administrators to adjust the font size based on user preferences or specific use case requirements, improving readability and usability.

| Parameter                                      | Description  |
|--|--|
| personal_settings/functional_key_font_size     | Minimum Value = 20<br>Maximum Value = 43<br>Default = 39                             |
| personal_settings/exp_functional_key_font_size | Minimum Value = 10<br>Maximum Value = 30<br>Default = 26                             |
| personal_settings/running_string               | Defines whether the running string feature is enabled<br>1 = Enabled<br>0 = Disabled |

| Parameter                                | Description  |
|--|--|
| personal_settings/running_string/timeout | <p>Sets the value (in ms) for the running string to scroll left one pixel.</p> <p>Value:</p> <p>Default: 150 seconds</p> |

## 6.4 Enhanced Sidecar Management and LED Customization

The following features have been introduced to improve sidecar usability and provide customizable LED options for the 445HD IP Phone:

### Automatic Sidecar Page Switching

When a user selects a new call line on the **New Call** screen, the sidecar automatically switches to the corresponding page.

Similarly, the sidecar view switches automatically when the active call changes.

### Default Sidecar Page

The sidecar can now display a default page based on the first Shared Call Appearance (SCA) index. This default page is determined by a configurable parameter.

### Configurable PK LED Color

Provides the ability to control the Programmable Key (PK) LED color for different call states, enabling better visual distinction.

### Configuration Parameters:

| Parameter name                                 | Description  |
|--|--|
| personal_settings/sidecar_mode                 | <p>Determines whether 445HD IPP's sidecar is automatically switched when user chooses current line (e.g., on pressing Line's PK, on answering the call etc.)</p> <ul style="list-style-type: none"> <li>■ [Dynamic] (Default)</li> <li>■ [STATIC]</li> </ul> |
| personal_settings/sidecar/default_page_line    | <p>Determines what page will be displayed by default on the 445HD sidecar.</p> <ul style="list-style-type: none"> <li>■ [-1] (Default)(Minimum)</li> <li>■ [29] (Maximum)</li> </ul>   |
| personal_settings/led_color_for_incoming_state | <p>Allows control the LED color for incoming state.</p> <ul style="list-style-type: none"> <li>■ OFF</li> <li>■ RED</li> <li>■ GREEN (Default)</li> <li>■ ORANGE</li> </ul>  |

| Parameter name                                  | Description   |
|---|---|
| personal_settings/led_color_for_initiated_state | Allows control the LED color for initiated state. <ul style="list-style-type: none"> <li>■ OFF</li> <li>■ RED</li> <li>■ GREEN (Default)</li> <li>■ ORANGE</li> </ul> |

## 6.5 Ability to Disable/Enable Features and Keys on IP Phone

The network administrator can disable access to specific features. The feature is motivated by the requirement on the part of some enterprises to control the setting remotely to comply with company policy.

| Parameters                      | Description  |
|---------------------------------|--|
| system/feature/contacts/enabled | Ability to disable the user from <b>accessing the Contact list</b> .<br>0 = Disable<br>1 = Enable (Default)        |
| system/feature/vmail/enabled    | Ability to disable the user from <b>accessing the Voice Mail</b> .<br>0 = Disable<br>1 = Enable (Default)          |
| system/feature/menu/enabled     | Ability to disable the user from <b>accessing the Main Menu screen</b> .<br>0 = Disable<br>1 = Enable (Default)    |
| system/feature/speaker/enabled  | Ability to disable the user from <b>accessing the speaker hard key</b> .<br>0 = Disable<br>1 = Enable (Default)    |
| system/feature/headset/enabled  | Ability to disable the user from <b>accessing the headset hard key</b> .<br>0 = Disable<br>1 = Enable (Default)    |
| system/feature/handset/enabled  | Ability to disable the user from <b>accessing the handset</b> .<br>0 = Disable<br>1 = Enable (Default)             |
| system/feature/transfer/enabled | Ability to disable the user from <b>blind/consult transferring a call</b> .<br>0 = Disable<br>1 = Enable (default) |
| system/feature/hold/enabled     | Ability to disable the user from <b>holding a call</b> .<br>0 = Disable<br>1 = Enable (default)                    |

### 6.5.1 Enabling/Disabling Display of DTMF Digits

The network administrator can disable the display of DTMF digits on screen during a call.

| Parameter                         | Description  |
|-----------------------------------|--|
| security/mask_dtmf_digits/enabled | Disable/Enable <b>mask DTMF digits</b> during a call.<br><b>0</b> = Disable (default)<br><b>1</b> = Enable |

## 6.6 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 76: Configuration File Paging Parameters**

| Parameter  | Description  |
|--|--|
| voip/services/group_paging/enabled                   | Enables group paging. <ul style="list-style-type: none"> <li>■ 0 = Disabled (default)</li> <li>■ 1 = Enabled</li> </ul>  |
| voip/services/group_paging/group/0-38/activated      | Defines the group to page to.<br>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.<br>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.<br>Available options are: <ul style="list-style-type: none"> <li>■ PCMU, PCMA</li> <li>■ G729</li> <li>■ G722</li> <li>■ G722_8000</li> </ul> <b>Note:</b> 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.<br>Default: 500 milliseconds. Optionally, you can configure 500~ milliseconds to 100000 milliseconds.  |

### 6.6.1 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.



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 77: 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. <ul style="list-style-type: none"><li>■ <b>0</b> = Disabled (default)</li><li>■ <b>1</b> = Enabled</li></ul> |



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

## 6.7 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 78: Brightness Parameters**

| 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 dial pad, etc. <ul style="list-style-type: none"> <li>■ LOW</li> <li>■ MEDIUM</li> <li>■ HIGH (default)</li> </ul> |
| 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).<br>Either: 15 (default), 30, 45 or 60 minutes.   |
| 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 timeout configured for 'active mode' times out (see the parameter above).<br>Either: <ul style="list-style-type: none"> <li>■ LOW</li> <li>■ MEDIUM (default)</li> <li>■ HIGH</li> </ul>  |
| 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.   |

| Parameter   | Description  |
|---|--|
| 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 it's in 'night mode'. The screen changes to 'night mode' after the timeout configured for 'dimmer mode' times out (see the parameter above). Either: <ul style="list-style-type: none"> <li>■ LOW (default)</li> <li>■ MEDIUM</li> <li>■ HIGH</li> <li>■ There is no timeout for 'night mode'.</li> </ul> |
| 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'.  |
| 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'.  |



## 6.8 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 79: Disabling the C450HD IP Phone Screen Saver**

| Parameter Name                            | Description   |
|---|---|
| personal_settings/ScreenSaverEnabled      | Enables / disables the C450HD phone screen saver. <ul style="list-style-type: none"><li>■ Disable</li><li>■ Enable (default)</li></ul>    |
| 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. |

## 6.9 Configuring Personal Settings

### 6.9.1 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 80: Language Display**

| Parameter                  | Description  |
|----------------------------|--|
| personal_settings/language | <p>Determines the phone screen language.</p> <ul style="list-style-type: none"> <li>■ [English] English (default)</li> <li>■ [Spanish] Spanish</li> <li>■ [Russian] Russian</li> <li>■ [Portuguese] Portuguese</li> <li>■ [German] German</li> <li>■ [Ukraine] Ukrainian</li> <li>■ [French] French</li> <li>■ [Italian] Italian</li> <li>■ [Hebrew] Hebrew</li> <li>■ [Polish] Polish</li> <li>■ [Korean] Korean</li> <li>■ [Finnish] Suom alainen</li> <li>■ [Chinese] Chinese Simplified</li> <li>■ [Chinese] Chinese Traditional</li> <li>■ [Magyar] Hungarian</li> <li>■ [Japanese] Japanese</li> <li>■ Slovak</li> <li>■ Czech</li> <li>■ Dutch</li> </ul> |

## 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 Trusted 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).



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.



- 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 Website. 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.

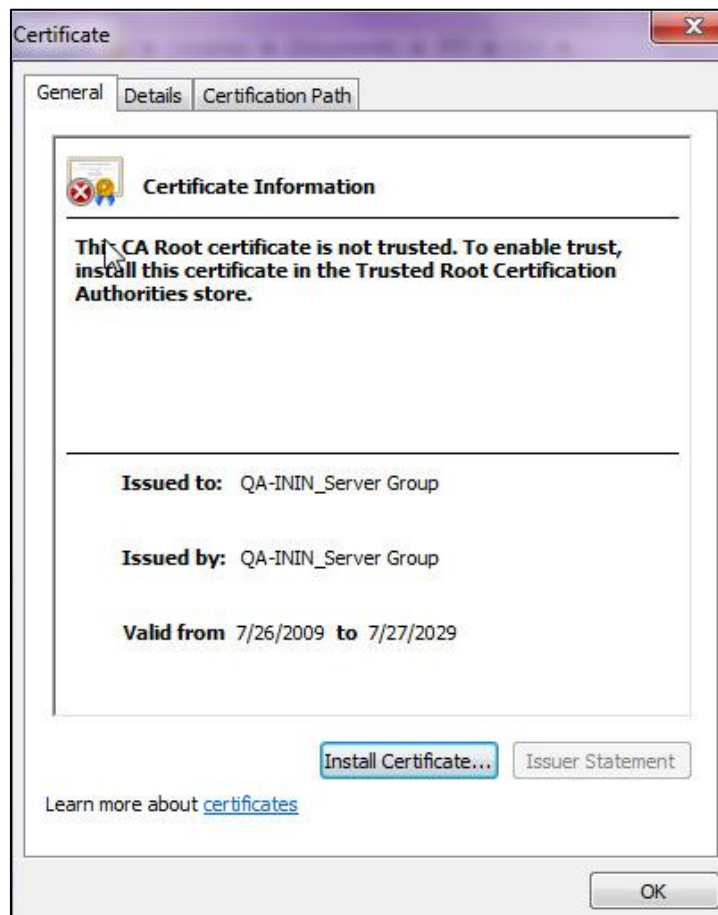


- You can load one certificate for each connection type.
- If you do not load a certificate to support a specific connection type, then the factory-set certificate is used to authenticate the connection. For example if you load user-generated certificates to support Automatic Updates (Provisioning server) 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 19: 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).



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\_AAA\_Certificate\_Services
- 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
- DigiCertGlobalG2TLSRSASHA2562020CA1
- DigiCertGlobalRootG2
- DigiCertGlobalRootG3
- 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
- GeoTrustEVRSA2018
- GlobalSign
- Go\_Daddy\_Go\_Daddy\_Class\_2\_Certification\_Authority
- Go\_Daddy\_Root\_Certificate\_Authority\_G2
- Go\_Daddy\_Starfield\_Class\_2\_Certification\_Authority
- isrgrootx1.pem
- letsencryptauthorityx3
- Microsoft\_ECC\_Root\_Certificate\_Authority\_2017
- Microsoft\_RSA\_Root\_Certificate\_Authority\_2017
- StartCom\_Certification\_Authority
- thawte\_Primary\_Root\_CA\_G3
- USERTrustRSA
- 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

## 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 Trusted Root CA Certificate Using Configuration File

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



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 81: 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.



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 82: 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.                             |

| Parameter                           | Description  |
|-------------------------------------|--|
| 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.           |



### 7.2.2.1 Enabling Server-side Authentication (Mutual Authentication)

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



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

**Table 83: 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 Certificate 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 20: 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 CA File Configuration

This section shows the values of the CA file parameters.



It is **highly recommended** to change the CA file configuration using the methods described in the preceding sections.

Certificate file settings are as follows:

```
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
```

## 7.3 Simple Certificate Enrollment Protocol (SCEP)

The IP Phones support certificate enrollment using Simple Certificate Enrollment Protocol (SCEP) with Microsoft's Network Device Enrollment Service (NDES) server. This feature allows for scalable provisioning of device certificates and CA certificates across multiple devices, streamlining certificate management in larger deployments.

When devices are configured with SCEP-related settings, the process proceeds as follows:

1. **Receive CA Certificate:** Devices retrieve a CA certificate from the NDES server.
2. **Certificate Signing Request (CSR):** Devices issue a CSR to the NDES server.
3. **Device Certificate Issuance:** Devices receive a device certificate signed by the CA certificate provided by the NDES server.

This functionality ensures that devices can efficiently obtain the necessary certificates for secure operation within an enterprise environment.

### SCEP Parameter Descriptions:

| Parameter                              | Description  |
|--|--|
| security/SCEPEnroll/ca_fingerprint     | Define the thumbprint (hash value) for the CA certificate. Default value: NULL.<br>Network admins must set its value to (for example):<br>3EBE50003ABF1DF5E6B5A3230B02B856 |
| security/SCEPEnroll/password_challenge | Define the enrollment challenge password. Default value: NULL.<br>Network admins must set its value to (for example):<br>7A7F9FC4BB7625F0935E67EA6D6322ED                  |

| Parameter   | Description   |
|---|---|
| security/SCEPServerURL                                  | Define the SCEP server URL. Default: NULL.<br>If you use Microsoft NDES server, use:<br>https://<NDES server IP address/Hostname>/certsrv/mscep/mscep.dll/pkiclient.exe   |
| security/SCEPEnroll/renewal/advancethreshold            | Define the renewal advance threshold of the device certificate.<br>Configure between 50 and 100 (in units of percentage)<br>Default: 80<br>This indicates that a renewal of the certificate (device.crt) will be initiated when 80 percent of its validity is reached.                          |
| security/SCEPEnroll/rollover/advancethreshold           | Specify the threshold of the CA Root certificate's validity at which to initiate a renewal.<br>Configure between 50 and 100 (in units of percentage).<br>Default: 90<br>This indicates a renewal of the certificate (CAROOT.crt.) will be initiated when 90 percent of its validity is reached. |
| security/CSR/CommonName                                 | Define a value according to the following 'wildcard' format:<br>{mac} – the device's MAC address<br>{IP} – the device's IP address<br>{model} - the device model  |
| security/CSR/Country                                    | Define the name of the country used to generate the certificate signing request (CSR). Note: The ISO (International Organization for Standardization) code of the country / region in which the organization is located.  |
| security/CSR/Organization                               | Optionally, define the legal name of the organization used to generate the CSR.   |
| security/CSR/State                                      | Optionally, define the name of the state / province used to generate the CSR.   |
| security/CSR_SubjectAltName_DNS/[0-9]/dns_names         | Optionally, define CSR DNS name.  |
| security/CSR_SubjectAltName_Email/[0-4]/email_addresses | Optionally, define CSR email address.   |
| security/CSR_SubjectAltName_IP/[0-4]/ip_addresses       | Optionally, define CSR ip address.  |
| security/CSR_SubjectAltName_URI/[0-4]/uris              | Optionally, define CSR URI.   |
| security/SCEPEnroll/otp_server_url                      | Optionally, set the One-Time Password and Certificate server URL  |
| security/SCEPEnroll/otp_password                        | Optionally, set the One-Time Password and Certificate Thumbprint  |
| security/SCEPEnroll/otp_username                        | Optionally, set the One-Time Password and Certificate server username   |

## 7.4 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.



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 84: SIP-over-TLS Parameters**

| Parameter                              | Description   |
|--|---|
| voip/signalling/sip/transport_protocol | Specifies the SIP Transport protocol. <ul style="list-style-type: none"> <li>■ If using the 'sip' prefix, set to 'TLS'</li> <li>■ If using the 'sips' prefix, set to 'TCP'</li> </ul> |
| voip/signalling/sip/tls_port           | Defines the local TLS SIP port for SIP messages.<br>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:"                           |

### 7.4.1 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 85: Server Certificate Validation for Secured HTTPS Communications over SSL**

| Parameter Name                    | Description   |
|-----------------------------------|---|
| security/SSLCertificateErrorsMode | <ul style="list-style-type: none"> <li>■ <b>Disallow</b> (default) = TLS connection will be rejected and the phone will not communicate with the server.</li> <li>■ <b>Ignore</b> = Allows backward compatibility though vulnerability will increase; the phone will proceed without checking the received certificates and without any notifications.</li> </ul> |

## 7.5 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.



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.

## 7.5.1 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 7.5.1.1
  - EAP-TLS - see Section 7.5.1.2

### 7.5.1.1 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**.

### 7.5.1.2 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 86: EAP TLS Parameters**

| Parameter                        | Description   |
|----------------------------------|---|
| network/lan/_802_1x/eap_type     | Sets 802.1X EAP mode.<br>[Disable] = Disables the use of 802.1X<br>[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  |



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

## 7.5.2 Configuring 802.1x

802.1x can be configured.

### 7.5.2.1 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 87: EAP MD5 Parameters**

| Parameter                        | Description   |
|----------------------------------|---|
| network/lan/_802_1x/eap_type     | Sets 802.1x Extensible Authentication Protocol mode: <ul style="list-style-type: none"><li>■ <b>Disable</b> = Disables the use of 802.1x</li><li>■ <b>EAP_MD5</b> = Authentication is implemented by user name and password (Password is optional).</li><li>■ <b>EAP_TLS</b> = Authentication is implemented by Certificate, Client Certificate and Client Private Key.</li></ul> |
| 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).  |

## 7.6 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 88: SRTP Parameters**

| Parameter                        | Description   |
|----------------------------------|---|
| voip/media/srtp/mode             | <ul style="list-style-type: none"> <li>Three encryption levels are supported:</li> <li><b>DoNotSupportEncryption</b> (Default) SRTP is disabled</li> <li><b>SupportEncryption</b> Negotiation</li> <li><b>RequireEncryption</b> SRTP is enabled; both sides must support encryption</li> <li><b>Note regarding backward compatibility:</b><br/>This configuration file parameter replaced the legacy <b>voip/media/srtp/enabled</b> configuration file parameter.</li> <li>The configuration file parameter <b>voip/media/srtp/enabled=1</b> in previous releases is compatible with the configuration file parameter <b>voip/media/srtp/mode=REQUIRE_ENCRYPTION</b> in this release</li> </ul> |
| voip/media/srtp/negotiation/mode | <ul style="list-style-type: none"> <li>If <b>voip/media/srtp/mode=SUPPORT_ENCRYPTION</b>, two SRTP negotiation modes are supported:</li> <li><b>Basic</b> (default) RTP/SRTP negotiation according to the document <i>IMTC Best Practices for SIP Security</i>. This mode is supported by Broadsoft, Microsoft and many other vendors</li> <li><b>RFC5939</b> RTP/SRTP capability negotiation using the attributes "a=tcap", "a=acap" and "a=pcfg" as described in RFC 5939</li> </ul>  |
| voip/media/srtp/method           | <p>The SRTP encryption method.</p> <ul style="list-style-type: none"> <li>AEAD_AES_ALL_METHODS<br/>(i.e., AEAD_AES_256_GCM and AEAD_AES_128_GCM)</li> <li>AES_CM_128_HMAC_SHA1_80</li> <li>AES_CM_128_HMAC_SHA1_32</li> <li>AES_CM_128_ALL_METHODS</li> <li>AES_ALL_METHODS</li> </ul>  |
| voip/media/srtp/use_MKI          | <p>Defines the usage of the SRTP Master Key Index.</p> <ul style="list-style-type: none"> <li><b>0</b> = MKI is not used (default)</li> <li><b>1</b> = MKI is used</li> </ul>   |
| voip/media/srtp/MKI_length       | <p>Defines the maximum length of the SRTP Master Key Index. Range: 1 - 4. Default: 1.</p>   |



| Parameter                            | Description   |
|--------------------------------------|---|
| voip/media/srtp/use_lifetime         | <p>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:</p> <ul style="list-style-type: none"> <li>■ <b>0</b> = the lifetime is removed</li> <li>■ <b>1</b> = the lifetime is retained (default)</li> </ul> |
| voip/media/srtp/RTCP_encrypt_enabled | <p>Default: <b>1</b>. If set to <b>0</b>, <b>UnencryptedSRTCP</b> will present at the end of the "a=crypto" line in the SDP offer, for example:</p> <pre>a=crypto:1 AES_CM_128_HMAC_SHA1_32 inline:rcO4NFj0PcKk3Pbo7IVhVqpCpQI3MWytScjRL1IS 2^31 UNENCRYPTED_SRTCP</pre>  |
| voip/media/srtp/RTP_encrypt_enabled  | <p>Default: <b>1</b>. If set to <b>0</b>, <b>UnencryptedSRTP</b> will present at the end of the "a=crypto" line in the SDP offer, for example:</p> <pre>a=crypto:1 AES_CM_128_HMAC_SHA1_32 inline:rcO4NFj0PcKk3Pbo7IVhVqpCpQI3MWytScjRL1IS 2^31 UNENCRYPTED_SRTCP</pre>   |
| voip/media/srtp/RTP_auth_enabled     | <p>Default: <b>1</b>. If set to <b>0</b>, <b>UnauthenticatedSRTP</b> will present at the end of the "a=crypto" line in the SDP offer, for example:</p> <pre>a=crypto:1 AES_CM_128_HMAC_SHA1_32 inline:TDejshzv6Y04By7Add2KuZaJ9YrvteWSEncpBMZ4 2^31 UNAUTHENTICATED_SRTCP</pre>   |

## 7.7 Configuring HTTP/S Login

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



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

## 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 89: Username and Password Parameters**

| Parameter        | Description   |
|------------------|---|
| system/user_name | The name of the phone user defined as Administrator.<br>The default value is <b>admin</b> .   |
| system/password  | The password of the phone user defined as Administrator is by default encrypted. The default value is <b>1234</b> .<br>To regenerate an encrypted password, see Section <a href="#">2.2.3.2</a> . |

### 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.



- 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 90: Administrator account - Username and Password**

| Parameter  | Description  |
|--|--|
| <b>Note:</b> To add a value to these parameters, enter <b>system/</b> followed by the parameter name, equal sign and then the value (e.g. <code>system/user_name=admin</code> ). |  |
| 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** (default for 425HD) disallows management via the phone's Web interface
- **1** (default for 445HD, C450HD) allows management via the phone's Web interface

### 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.

Use the table as reference:

**Table 91: Port Parameters**

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

## 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.



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's 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:

- MENU key > **Administration** > **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.



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 92: Telnet Parameters**

| Parameter                 | Description   |
|---------------------------|---|
| management/telnet/enabled | Enables telnet access to the phone. <ul style="list-style-type: none"><li>■ 0 = Disable (default)</li><li>■ 1 = Enable</li></ul> The user name and password for telnet access are according to the parameters: <b>system/user_name</b> and <b>system/password</b> . |

### 8.5.2 Enabling SSH Access

Secure Shell (SSH) protocol can be configured for secure remote login to the IP Phones.

#### To configure SSH:

Use the table as reference:

**Table 93: SSH Parameters**

| Parameter              | Description   |
|------------------------|---|
| management/ssh/enabled | Enables SSH access to the phone. <ul style="list-style-type: none"><li>■ 0 = Disable (default)</li><li>■ 1 = Enable</li></ul> The user name and password for SSH access are according to the parameters: <b>system/user_name</b> and <b>system/password</b> . |

## 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.

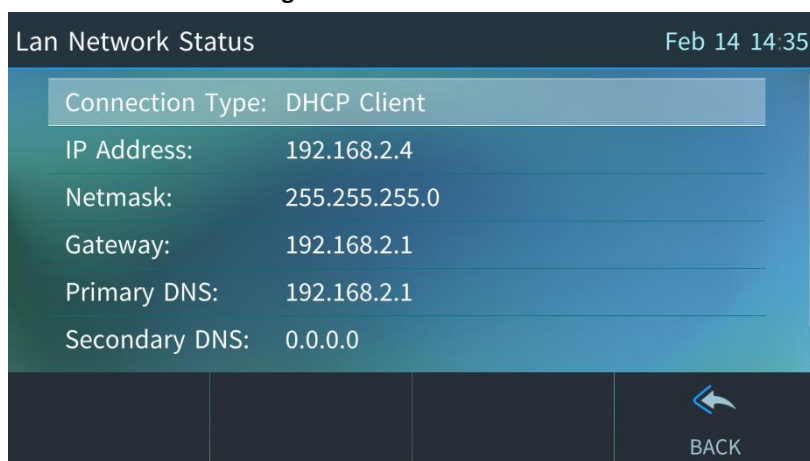
#### 9.1.1 Determining LAN Status

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:**

- From UI Menu, Select **Device Status > Network Status**

**Figure 21: LAN Information**



#### 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 22: 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       |

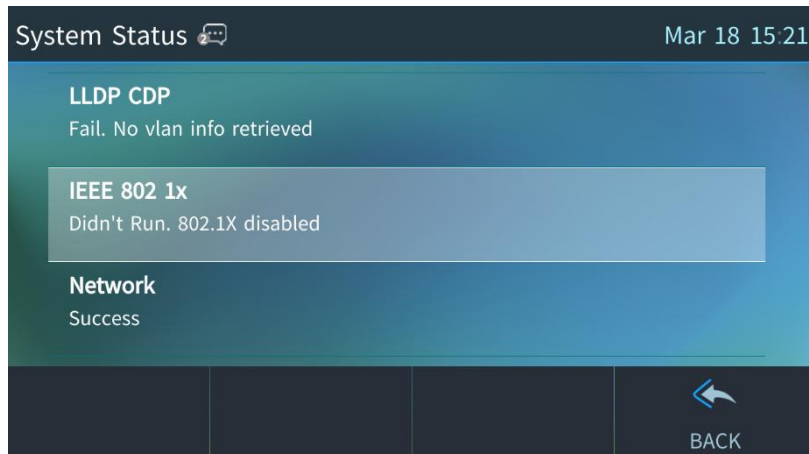
### 9.1.3 Determining 802.1x Status

802.1x status can be viewed.

To determine 802.1x status:

- From UI Menu, Select **Device Status > System Status**.

Figure 23: 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.

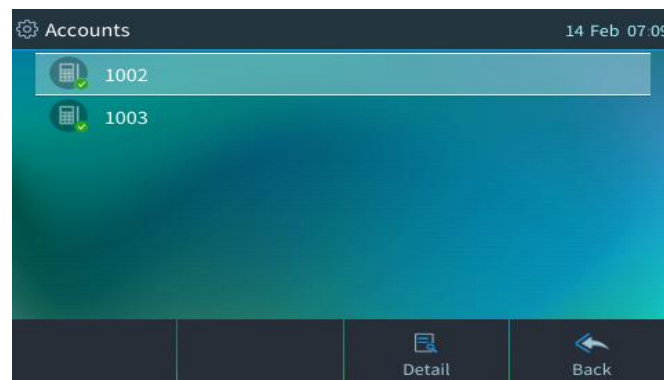
### 9.2.1 Viewing Line Status

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:

- From UI Menu, Select **Settings > Accounts**

Figure 24: Line Status





## 9.2.2 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:**

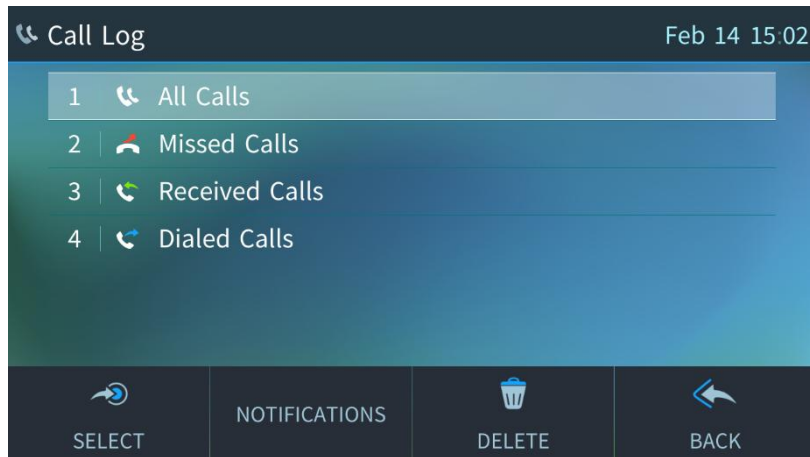
## 9.3 Viewing Call History

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. From UI Menu, Select **Call Log**

Figure 25: Call History



2. Select the type of call history (i.e., missed calls, received calls, or dialed calls) that you want to view.
3. You can delete a logged call history entry, by selecting the **Delete** softkey.

To disable the user from accessing call history:

| Parameter                      | Description  |
|--------------------------------|--|
| system/feature/calllog/enabled | Disable/Enable call log access.<br>0 = Disable<br>1 = Enable (default) |

To disable the user from using the redial option:

| Parameter                     | Description   |
|-------------------------------|---|
| system/feature/redial/enabled | Disable/ Enable redial access.<br>0 = Disable<br>1 = Enable (default) |

### 9.3.1 Exclude 'feature code dialing' from Call Log

Feature code dialing is a PBX mechanism used for special functions (e.g., follow me, Call Forwarding, Do Not Disturb, etc.) rather than for regular call dialing.

Feature codes typically include identifiable prefixes and/or suffixes such as #123#, \*678\*, \*#123456\*#, or other administrator-defined patterns.

| Parameter                                  | Description  |
|--|--|
| personal_settings/call_log/exclude_pattern | <p>Any dialed number matching one of these patterns (set by administrator) is treated as a feature code and is excluded from the call history display.</p> <p>You can define multiple patterns (up to 1024 characters total), separated by the ' ' symbol.</p> <p>Each pattern can use the following building blocks:</p> <ul style="list-style-type: none"> <li>■ <b>DTMF digits:</b> 0–9, *, #</li> <li>■ <b>Wildcard x:</b> Matches any single digit (0–9)</li> <li>■ <b>Range:</b> Square brackets ([ and ]) including an Asterisk (*) and one or more characters</li> <li>■ <b>Repeat:</b> The character followed by a period (.) means the previous element can repeat any number of times (including zero)</li> </ul> <p><b>Example:</b></p> <pre>personal_settings/call_log/exclude_pattern = *x. #x. *#x.*# #*x.*# **#x.**# #[1-7]*#</pre> <p>The following dial strings will be recognized as feature codes and hidden from the call log:</p> <ul style="list-style-type: none"> <li>■ *123 - (*x.)</li> <li>■ #456 - (#x.)</li> <li>■ *#789#* - (*#x.#*)</li> <li>■ #*666888*# - (#*x.*#)</li> <li>■ **#123456**# - (**#x.**#)</li> <li>■ #*56*# - (#*[1-7]*#)</li> </ul> |

### 9.3.2 Disable the presence SUBSCRIBE message (for Call Log lists)

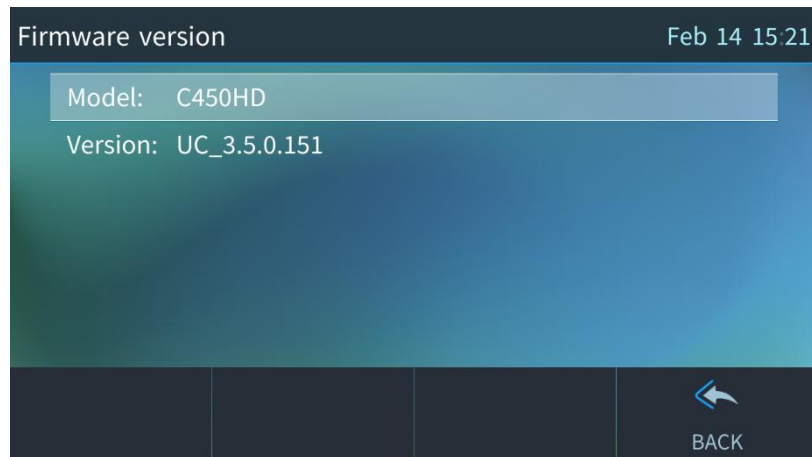
| Parameter Name                            | Description   |
|---|---|
| voip/services/subscribe_call_log_presence | <p>Determine whether IPP sends SUBSCRIBE when opening the <b>Call Log</b> screen.</p> <ul style="list-style-type: none"> <li>■ <b>0</b> = Disable</li> <li>■ <b>1</b> = Enable (Default)</li> </ul> |

## 9.4 Accessing System Information

This section describes the System Information page and Release Information page.

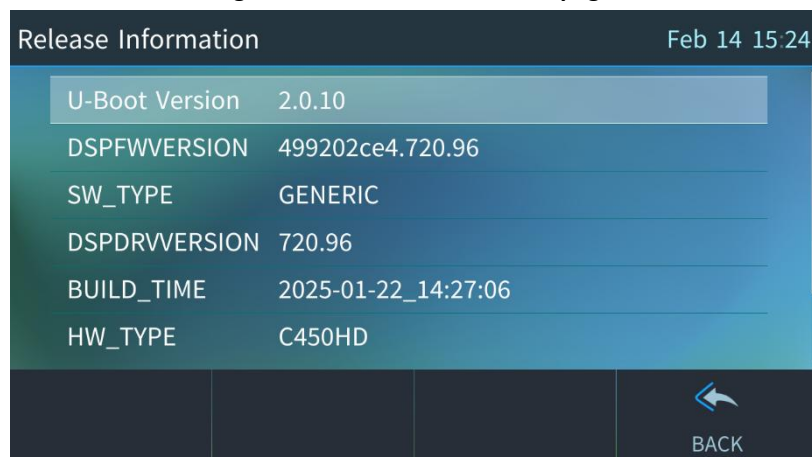
- To view Firmware version, from UI Menu, Select **Device Status > Firmware**

**Figure 26: System Information page**



- To view Release Information, from UI Menu, Select **Device Status > Release Information**

**Figure 27: Release Information page**



## 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 94: RTCP\_XR Parameters**

| Parameter                       | Description   |
|---------------------------------|---|
| voip/rtcp_xr/vq_statistics/mode | <p>Sets RTCP_XR working mode. Select either:</p> <ul style="list-style-type: none"> <li>■ <b>DISABLE</b> (default). 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).</li> <li>■ <b>EVENTS_ONLY</b>. 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 OVOC (or other QoE) server via SIP PUBLISH messages.</li> <li>■ <b>REMOTE_AND_EVENTS</b>. 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 OVOC (or other QoE) server via SIP PUBLISH messages.</li> </ul> |

## 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 95: 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 listing of RTCP XR parameters that may be sent to the QoE server, see Appendix [G](#).

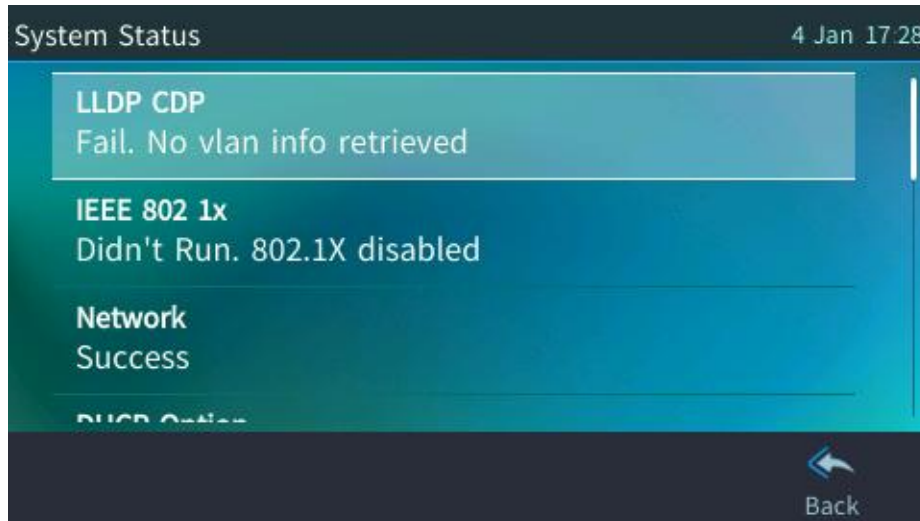
For example SIP PUBLISH messages, see Appendix [H](#).

## 10 Diagnosing Problems & Troubleshooting

### 10.1 Monitor the Status of Software Modules

Administrators can monitor the status of the device's various software modules. For example, if initial provisioning fails, or if a network or Device Manager connectivity issue occurs, the system provides clear indications of the root cause.

Debugging is available directly from the phone screen without relying on external systems. Administrators can verify connectivity independently of external applications by navigating to **Status > System State**.



### 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 96: Syslog Parameters**

| Parameter                    | Description   |
|------------------------------|---|
| system/syslog/mode           | Enables Syslog. Possible values are: <ul style="list-style-type: none"> <li>■ <b>LOCAL</b> (Default)</li> <li>■ <b>NETWORK</b> = Syslog is sent to the Syslog server (recommended)</li> <li>■ <b>SERIAL</b> = 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).</li> <li>■ <b>ALL</b> = Syslog sends to the Syslog server <i>and</i> to the console.</li> </ul> |
| system/syslog/log_level      | Default: DETAILED. Defines the log level.   |
| system/syslog/sip_log_filter | Default: 0. Defines the SIP log filter.   |



| Parameter   | Description  |
|---|--|
| 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. <b>Note:</b> This parameter is applicable when Activate is set to <b>Network</b> or <b>Both</b> . |
| system/syslog/server_port   | Defines the UDP port of the Syslog server.<br>The valid range is 0 to 65,535. The default port is 514.<br><b>Note:</b> This parameter is applicable when Activate is set to <b>Network</b> or <b>Both</b> .  |
| <b>Note:</b> The following Severity level options are applicable for the fields below: <ul style="list-style-type: none"> <li>■ NONE</li> <li>■ EMERGENCY</li> <li>■ ERROR</li> <li>■ WARNING</li> <li>■ NOTICE</li> <li>■ INFO</li> <li>■ DEBUG</li> </ul> |  |
| <b>Note:</b> The following two Severity level options are applicable for the fields below: <ul style="list-style-type: none"> <li>■ NONE</li> <li>■ DEBUG</li> </ul>  |  |
| system/syslog/component/btoe  | Default: NONE.   |
| system/syslog/component/cert  | 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.  |
| system/syslog/component/emsc  | Default: NONE.   |
| system/syslog/component/ice_stack   | Default: NONE.   |
| 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.   |

| Parameter                                | Description   |
|--|---|
| 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.                    |

## 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 97: 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 |



- 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 98: 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).<br>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.<br>The valid range is 1024 to 65535.<br>The default value is 52000 for <b>425HD</b> .<br>The default value is 50000 for <b>445HD/C450HD</b> . |
| voip/packet_recording/enabled                           | Activates the packet recording mechanism.<br>■ 0 = Disable (default)<br>■ 1 = Enable  |
| voip/packet_recording/rtp_recording/enabled             | Only displayed if the parameter 'Enable DSP Recording' is enabled.<br>Activates the DSP RTP recording.<br>■ 0 = Disable (default)<br>■ 1 = Enable   |
| voip/packet_recording/ec_debug_recording/enabled        | Activates the Echo Canceller Debug recording.<br>■ 0 = Disable (default)<br>■ 1 = Enable  |
| voip/packet_recording/noise_reduction_recording/enabled | Traffic on the network stops when the MUTE key is activated.<br>■ 0 = Disable (default)<br>■ 1 = Enable   |
| voip/packet_recording/network_recording/enabled         | Activates the DSP network (TDM Out) recording.<br>■ 0 = Disable (default)<br>■ 1 = Enable   |
| voip/packet_recording/tdm_recording/enabled             | Activates the DSP TDM (TDM In) recording.<br>■ 0 = Disable (default)<br>■ 1 = Enable  |
| voip/packet_recording/cng_debug_recording/enabled       | Applicable for <b>445HD/C450HD only</b> :<br>Activates the Comfort Noise Generator Debug recording.<br>■ 0 = Disable (default)<br>■ 1 = Enable  |

| Parameter   | Description   |
|---|---|
| voip/packet_recording/AFE_tx_input_recording/enabled    | Applicable for <b>425HD only</b> :<br>Activates the AFE Transmit Input Recording (Voice record location 0)<br><ul style="list-style-type: none"> <li>■ 0 = Disable (default)</li> <li>■ 1 = Enable</li> </ul> |
| voip/packet_recording/agc_rx_debug_recording/enabled    | Applicable for <b>425HD only</b> :<br>Activates the AGC Receive Debug recording packets<br><ul style="list-style-type: none"> <li>■ 0 = Disable (default)</li> <li>■ 1 = Enable</li> </ul>                    |
| voip/packet_recording/agc_tx_debug_recording/enabled    | Applicable for <b>425HD only</b> :<br>Activates the AGC Transmit Debug recording packets<br><ul style="list-style-type: none"> <li>■ 0 = Disable (default)</li> <li>■ 1 = Enable</li> </ul>                   |
| voip/packet_recording/eq_rx_debug_recording/enabled     | Applicable for <b>425HD only</b> :<br>Activates the Equalizer Receive Debug recording packets<br><ul style="list-style-type: none"> <li>■ 0 = Disable (default)</li> <li>■ 1 = Enable</li> </ul>              |
| voip/packet_recording/eq_tx_debug_recording/enabled     | Applicable for <b>425HD only</b> :<br>Activates the Equalizer Transmit Debug recording packets<br><ul style="list-style-type: none"> <li>■ 0 = Disable (default)</li> <li>■ 1 = Enable</li> </ul>             |
| voip/packet_recording/force_coder_output_record/enabled | Ac49x support, <b>not for 425HD</b> :<br><ul style="list-style-type: none"> <li>■ 0 = Record location 0 (default)</li> <li>■ 1 = Record location 1</li> </ul>   |
| voip/packet_recording/input_rx_debug_recording/enabled  | Applicable for <b>425HD only</b> :<br>Activates the Input Receive Debug recording packets(DSP to AFE)<br><ul style="list-style-type: none"> <li>■ 0 = Disable (default)</li> <li>■ 1 = Enable</li> </ul>      |
| voip/packet_recording/osns_debug_recording/enabled      | Applicable for <b>425HD only</b> :<br>Activates the Open Space Noise Suppressor Debug packets<br><ul style="list-style-type: none"> <li>■ 0 = Disable (default)</li> <li>■ 1 = Enable</li> </ul>              |
| voip/packet_recording/output_tx_debug_recording/enabled | Applicable for <b>425HD only</b> :<br>Activates the Output Transmit Debug packets (AFE to DSP)<br><ul style="list-style-type: none"> <li>■ 0 = Disable (default)</li> <li>■ 1 = Enable</li> </ul>             |

| Parameter                                       | Description  |
|---|--|
| voip/packet_recording/srtp_audit_events/enabled | <p>Ac49x support, <b>not for 425HD</b>:<br/>Support Protection Audit Event Transfer Mode.</p> <ul style="list-style-type: none"> <li>■ <b>0</b><br/>EVENT_SENT_IN_RESPONSE_TO_REQUEST_COMMAND (default)</li> <li>■ <b>1</b><br/>EVENT_SENT_IN_RESPONSE_TO_REQUEST_COMMAND_AND_ON_ERROR_REPORT_INTERVALS (default)</li> </ul> |

## 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 28: Web Interface – Core Dump

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 99: Core Dump Parameter

| Parameter                   | Description   |
|-----------------------------|---|
| kernel/cfg/enable_core_dump | <p>Enables core dump.</p> <ul style="list-style-type: none"> <li>■ <b>0</b> = Disable</li> <li>■ <b>1</b> = Enable (default)</li> </ul> |

## 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 100: Port Mirroring Parameters**

| Parameter                         | Description  |
|-----------------------------------|--|
| network/pc_port_mirroring/enabled | <p>Enables port mirroring.</p> <ul style="list-style-type: none"> <li>■ <b>0</b> = Disable (default) - LAN/PC network interfaces operate in SWITCH mode.</li> <li>■ <b>1</b> = Enable - LAN/PC network interfaces operate in HUB mode. The network traffic on the LAN port is reflected in the PC port.</li> </ul> |

## 10.7 Supporting Transition Recording

The **Transition Recording** feature enhances the user experience by allowing the IP Phone to capture screenshots of its interface for various purposes, such as troubleshooting, documentation, or training. This feature supports both manual and automatic modes, providing flexibility based on the user's needs. Configuration options enable precise control over the behavior and storage of screenshots, ensuring they are efficiently managed and accessible.

**Transition Recording:**

| Parameter                | Description   |
|--------------------------|---|
| system/screenshots_path  | <p>This new configuration parameter defines a path in the file system of the IP Phone, where screenshots are saved to this specified folder in *.png format. if the folder does not exist it will be created.</p> <p>Default path = "/tmp/screenshots".</p> |
| system/screenshots_mode  | <p>manual or auto mode doing of screenshots, it should be MANUAL or SCREENS_TRANSITION</p> <p>Default=NONE</p>  |
| system/screenshots_timer | <p>delay(in ms) after release keys when a screenshot will be taken in auto mode</p> <p>Default=500</p>  |

## A Accessing Office 365 Exchange Services

IP Phone support Office 365 exchange services in Generic SIP mode. User can:

- Sign in to Office 365 exchange services via cloud login or username and password.
- View the calendar.
- Join Teams or Zoom meeting via calendar.
- Search for contacts from the corporate directory

### Required configuration:

| Parameter                    | Description   |
|------------------------------|---|
| account/office365/permission | Set this parameter to USER.<br>Default = ADMIN                  |
| lync/ews/GetEwsAddressMethod | Set the method to FROM_CONFIGURATION_ONLY.<br>Default = DYNAMIC |



Basic Authentication in Office 365 Exchange services are no longer supported by Microsoft.



## B Installing the Expansion Module

Before installing the Expansion Module for your phone, make sure the following items are included in the shipped box:

- Expansion Module
- Kit containing five screws



Applies to AudioCodes' C450HD phones.

### B.1 Installation Procedure



Before proceeding with the installation:

- Disconnect the phone from the Power Supply / Power over Ethernet (PoE)
- Obtain a Philips screwdriver

**To connect the Expansion Module to the C450HD phone:**

1. Step 1: Prepare the two units – see below
2. Step 2: Remove the phone's side panel – see [below](#)
3. Step 3: Connect the Expansion Module to the phone – see [below](#)
4. Step 4: Attach the panel removed from the phone in Step 3, to the Expansion Module – see [below](#)
5. Step 5: Secure the assembly – see [below](#)
6. Step 6: Install the Expansion Module's base stand and the phone's base stand - see [below](#)
7. Step 7: Mount the assembled unit - see [below](#)

#### B.1.1 Step 1: Place Phone and Module on a Table

Place the phone and the Expansion Module on a table alongside one other.



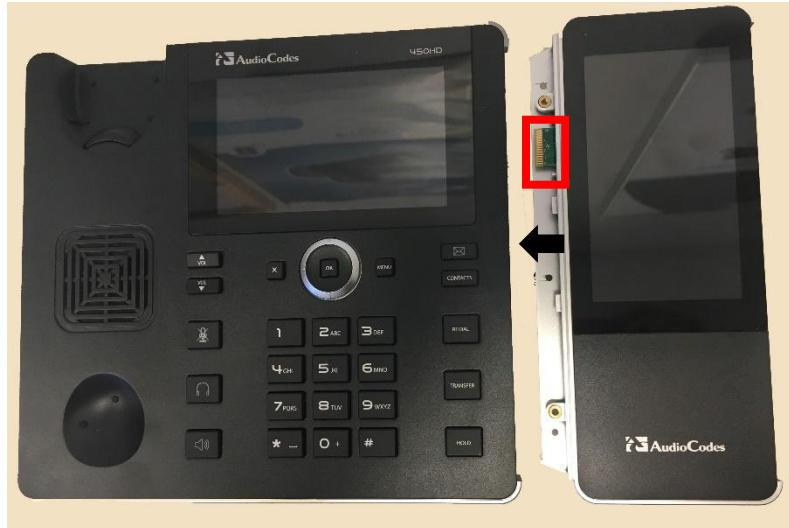
### B.1.2 Step 2: Invert and Unscrew Three Screws

Invert the phone on a surface that won't scratch the screen such as a towel or printer paper. Avoid inverting the phone on the surface of a desk. Then unscrew the three screws shown below in order to remove the phone's side panel:



### B.1.3 Step 3: Remove Rubber Cover and Connect

Return the phone to an upright position. Remove the Expansion Module's connector's rubber cover and then connect the Expansion Module to the phone. Note the connector and PEM direction.



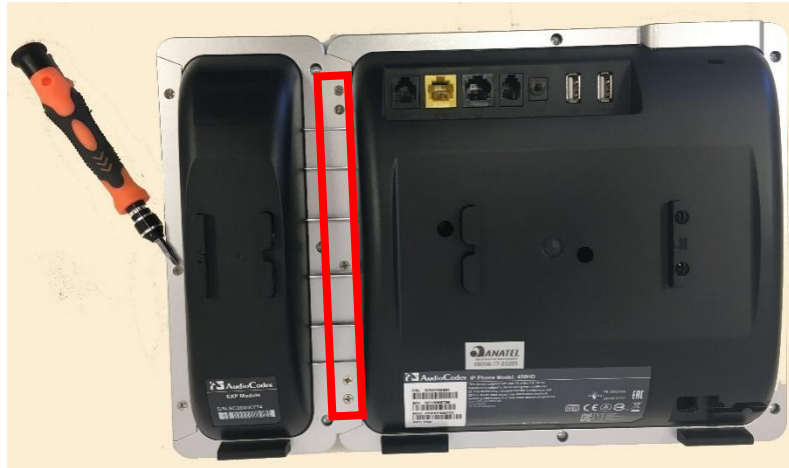
### B.1.4 Step 4: Attach the Panel

Attach the panel that you removed from the phone in Step 3 to the side of the Expansion Module:



### B.1.5 Step 5: Secure the Side Panel

Invert the assembled unit and secure the side panel by screwing in the three screws:



### B.1.6 Step 6: Secure the Connection of the Two Units

[Refer again to the figure above] Secure the connection of the two units by screwing in these five screws.

### B.1.7 Step 7: Mount Phone on Base Stand, Expansion Module on Base Stand

With the assembly inverted, mount the phone on its dedicated base stand and the Expansion Module on its dedicated base stand, like this:



Slots in the stands are slid onto rails on the units. The figure above shows the phone mounted on the short edge of its 'L' shaped base stand, and the Expansion Module mounted on the short edge of its 'L' shaped base stand. The long edge of the 'L' can alternatively be used per user preference, depending on sources of glare in the office.

## C Configuring Phones in Server-Specific Deployments

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

### C.1 BroadSoft's BroadWorks

Features supported in a BroadSoft environment are listed below.

- BSFT DMS for provisioning [Support pending]
- BLF Support
- 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
- Broadworks Phone book support [Support pending]
- Voice Message Support
- DNS SRV Lookup for Redundancy and register failover
- ACD (Automatic Call Distribution) [Support pending]

### C.1.1 Configuring BLF

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

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

Use the table as reference:

**Table 101: 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 <b>1</b> (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.    |

## C.1.2 Configuring Call Forwarding



Before configuring Call Forwarding in the phone's screen, make sure the parameter 'system/feature\_key\_synchronization/enabled=1' (see Section C.1.4).

### C.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:

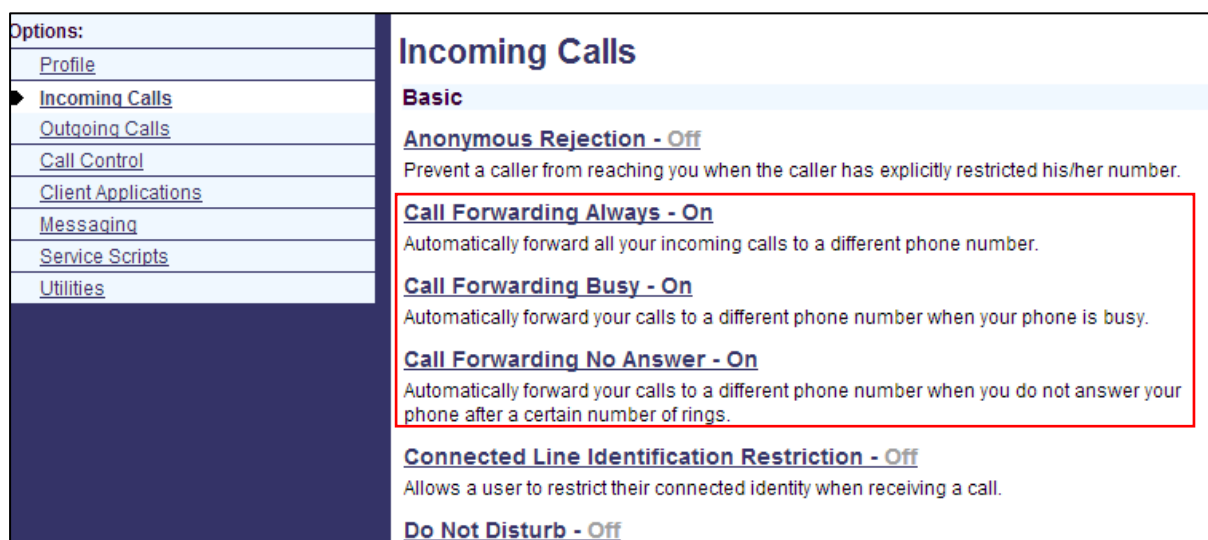
- See the phone's *User's Manual* for detailed information.

### C.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 29: Configuring Call Forwarding using BroadSoft's BroadWorks**



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 documentation.



### C.1.3 Configuring DnD

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



Before configuring DnD, make sure the configuration file parameter 'system/feature\_key\_synchronization/enabled' is set to **1** (see Section C.1.4).

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 30: Configuring DnD in BroadSoft's BroadWorks - Status

Figure 31: Configuring DnD in BroadSoft's BroadWorks

For detailed information, see related BroadSoft documentation.

### C.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.

### C.1.5 Configuring Phones to Connect to Xsi 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:

- **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 or disable this feature using configuration file parameter *xsi/contact/enable* which by default is disabled. 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 or disable this feature using configuration file parameter *xsi/callog/enable* which by default is disabled.

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

Use the table as reference:

**Table 102: Connecting Phones to BroadWorks over HTTP/S – Configuration File Parameters**

| Parameter          | Description   |
|--------------------|---|
| xsi/calllog/enable | <p>Enable or disable the XSI Call Log.</p> <ul style="list-style-type: none"> <li>■ <b>0</b> = (Default) The XSI Call Log is disabled and the IP Phone displays the local call log.</li> <li>■ <b>1</b> = The IP Phone retrieves and displays call history from the configured XSI server.</li> </ul>   |
| xsi/contact/enable | <ul style="list-style-type: none"> <li>■ <b>1</b> Contacts and contact information are saved on the BroadWorks server.</li> <li>■ <b>0</b> Contacts and contact information are saved locally on the phone (default).</li> </ul>  |
| xsi/host           | <p>Defines the phones host, BroadWorks server. The phones receive two web services from the server:</p> <ul style="list-style-type: none"> <li>■ Contacts list</li> <li>■ Call Log (history of calls dialed, received, missed, etc.)</li> </ul>   |
| xsi/http_port      | <p>Defines the BroadSoft BroadWorks Online Server port number. This parameter specifies the port used by the phone to receive web services from the BroadSoft BroadWorks Online Server.</p> <p><b>Range:</b> 0–65535</p> <p><b>Default:</b> 443</p> <p><b>Note:</b> The default port is 443, since the default value of xsi/http_security is <b>HTTPS</b>. When HTTP is used instead, the port must be configured accordingly.</p>  |
| xsi/http_security  | <p>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.</p>  |
| xsi/update_time    | <p>Every 10 minutes (default) phones update their call center status. Programmable keys on the phone indicate call centers' statuses.</p> <ul style="list-style-type: none"> <li>■ Key illuminated red = Phone unavailable</li> <li>■ Key illuminated green = Phone available</li> </ul> <p>Phone users can press a key to change the phone's status <i>in that call center</i>. If a user presses a key illuminated red, the key turns green and the phone's status <i>in that call center</i> changes from unavailable to available. If a key is illuminated green and the user presses it, the phone's status <i>in that call center</i> changes from available to unavailable.</p> <p>The BroadWorks server updates phone status every 20 minutes by default.</p> |
| xsi/user_id        | <p>Defines the user ID required for the phone to access the BroadSoft BroadWorks online server.</p>   |

| Parameter                               | Description   |
|---|---|
| xsi/password                            | Defines the password required for the phone to access the BroadSoft BroadWorks online server.   |
| xsi/calllog/delete/enable               | Controls whether a <b>DELETE</b> softkey is shown on the <i>Call Log</i> and <i>Call Details</i> screens. <ul style="list-style-type: none"> <li>■ <b>0</b> = (Default) The DELETE softkey is not displayed.</li> <li>■ <b>1</b> = A <b>DELETE</b> softkey is displayed (supported only if the XSI server allows call-log deletion).</li> </ul> |
| xsi/contact/directory/0-7/label         | Configure XSI directories   |
| xsi/contact/directory/0-7/type          | XSI directories Type: <ul style="list-style-type: none"> <li>■ GROUP</li> <li>■ ENTERPRISE</li> <li>■ GROUP_COMMON</li> <li>■ ENTERPRISE_COMMON</li> <li>■ PERSONAL</li> <li>■ NONE (Default)</li> </ul>  |
| xsi/contact/user_id/mac_address/enabled | Add MAC address to the user ID <ul style="list-style-type: none"> <li>■ <b>0</b> = Disable (Default)</li> <li>■ <b>1</b> = Enable</li> </ul>  |
| xsi/contact/search_on_empty/enabled     | Define whether search contacts or not when searching string is empty.<br>If set to 1, it will search by "*", means search call contacts. <ul style="list-style-type: none"> <li>■ <b>0</b> = Disable</li> <li>■ <b>1</b> = Enable (Default)</li> </ul>  |

### C.1.6 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.

**Figure 32: 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 33: BroadSoft Server - Assigning Shared Calls Appearance to a User**

**Shared Call Appearance**

Shared Call Appearance allows administrators to allocate additional devices or lines to you. These devices or lines also ring just like your primary phone. Define the line policy on Device Policies page.

OK Apply Add Cancel

☒ Alert all appearances for Click-to-Dial calls  
☒ Alert all appearances for Group Paging calls  
☒ Allow Call Retrieve from another location

Multiple Call Arrangement: ☒ On ☐ Off  
☐ Allow bridging between locations  
☒ Enable Call Park notification

Bridge Warning tone: ☐ None  
☒ Barge-in only  
☐ Barge-in and repeat every 30 seconds

Device Policies: [Configure device policies](#)

| Delete                   | Identity/Device Profile Type | Identity/Device Profile Name | Line/Port             | Edit                 |
|--------------------------|------------------------------|------------------------------|-----------------------|----------------------|
| <input type="checkbox"/> | Generic SIP Phone            | AudioCodesPhone4 (Group)     | 2421114084_2@as.io... | <a href="#">Edit</a> |
| <input type="checkbox"/> | Generic SIP Phone            | AudioCodesPhone4 (Group)     | 2421114098@as.iop1... | <a href="#">Edit</a> |
| <input type="checkbox"/> | Generic SIP Phone            | AudioCodesPhone4 (Group)     | 2421114097@as.iop1... | <a href="#">Edit</a> |
| <input type="checkbox"/> | Generic SIP Phone            | AudioCodesPhone4 (Group)     | 2421114098@as.iop1... | <a href="#">Edit</a> |

[ Page 1 of 1 ]

Identity/Device Profile Type Starts With Find Find All

OK Apply Add Cancel

- 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 103: BroadSoft Server - Shared Call Appearance – Identity/Device Profile Type**

| Parameter                                     | Description   |
|---|---|
| Alert all appearances for Click-to-Dial calls | <p>See BroadSoft's documentation for detailed information.</p> <p>Select this option when you want your Click-To-Dial calls to ring all phones that have your line appearance.</p> <p>Clear the option if you prefer your line to ring your phone only.</p> |
| Alert all appearances for Group Paging calls  | <p>See BroadSoft's documentation for detailed information.</p>  |
| Allow call retrieve from another location     | <p>See BroadSoft's documentation for detailed information.</p> <p>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.</p>                            |

| Parameter                 | Description  |
|---------------------------|--|
| Multiple Call Arrangement | <p>See BroadSoft's documentation for detailed information.</p> <p>Select <b>On</b> to allow multiple calls using your phone number / ID to be dialed or answered simultaneously across all Shared Call Appearances of your number.</p> <p>Select <b>Allow bridging between locations</b> 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.</p> <p>Select <b>Enable Call Park notification</b> for the phone to alert the user visually and audially when a parked call is received.</p> |
| Bridge Warning tone       | <p>See BroadSoft's documentation for detailed information.</p> <p>Select the type of Bridge Warning tone treatment you prefer when you bridge and join a call using a feature access code.</p> <p>Select <b>None</b> to apply no tone alert treatment upon your entry to the call.</p> <p>Select <b>Barge-in only</b> to provide a single tone alert.</p> <p>Select <b>Barge-in and repeat every 30 seconds</b> to provide a tone alert at that interval.</p>  |

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

**Figure 34: BroadSoft Server – Shared Call Appearance Add**

**Options:**

- Profile
- Incoming Calls
- Outgoing Calls
- **Call Control**
- Client Applications
- Messaging
- Service Scripts
- Utilities

### Shared Call Appearance Add

Allows administrators to allocate additional devices or lines to you.

OK Cancel

Identity/Device Profile Name: AudioCodesPhone4 (Group) ▼

\* Line/Port: 2421114099 @

as.iop1.broadworks.net ▼

☒ Enable this location

☒ Allow Origination from this location

☒ Allow Termination to this location

OK Cancel

**Table 104: BroadSoft Server - Shared Call Appearance Add**

| Parameter                            | Description  |
|--------------------------------------|--|
| Identity/Device Profile Name         | See BroadSoft's documentation for detailed information.<br>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):<br><b>2421114099@as.iop1.broadworks.net</b>          |
| 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 105: Shared Line Parameter**

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



### C.1.7 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 106: Remote Conference Parameters**

| Parameter                             | Description  |
|---------------------------------------|--|
| voip/services/application_server_type | Set to <b>BSFT</b> .   |
| voip/services/conference/conf_ms_addr | Set the address of the server hosting the remote conference. Example:<br>conference@as.iop1.broadworks.net |
| voip/services/conference/mode         | Set the mode to <b>REMOTE</b> .  |

## C.2 Asterisk

### C.2.1 Configuring BLF

Configuration of the BLF feature is unique when the selected application server is Asterisk.

**To configure BLF for application server type:**

1. Configure voip/services/application\_server\_type=ASTERISK
2. Configure voip/services/busy\_lamp\_field/enabled=1
3. (Optional) Configure voip/services/busy\_lamp\_field/subscription\_period parameter.

Enter the interval between BLF and SIP SUBSCRIBE messages:

Range: [0->86400]

Default: 3600



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. Define speed dial keys with the BLF feature (see Section 6.2).

## C.3 OpenSpace SIP Proxy

Configuring feature key synchronization for DND and call forward using the following parameters:

| Parameter                                  | Description  |
|--|--|
| system/feature_key_synchronization/enabled | 1 = Enable<br>0 = Disable<br>Default = 0   |
| system/feature_key_synchronization/method  | Configure this parameter to NOTIFY.<br>Default = SUBSCRIBE.                          |
| voip/call_forward/support_multiple_type    | Supports only one forward type. Set this parameter to 0.<br>Default = 1              |
| voip/call_forward/support_timeout          | Set the parameter to 0, disable call forward timeout setting feature.<br>Default = 1 |

Configuring group call pickup. When one member receives an incoming call, other members are notified and can pick up the call using the following parameters:

| Parameter  | Description   |
|--|---|
| personal_settings/functional_key/x/type              | Set the function key type to GROUP_CALL_PICKUP.<br>Default= EMPTY |
| voip/services/group_call_pickup/access_code          | Set the parameter to empty (null).<br>Default *98.                |
| personal_settings/functional_key/x/speed_dial_number | Configure the pickup group number (e.g., *60).                    |

Configuring current status monitoring via BLF LEDs to monitor the state of other extensions using the following parameters:

| Parameter  | Description  |
|--|--|
| voip/services/busy_lamp_field/enabled                  | 1 = Enable<br>0 = Disable<br>Default = 1                               |
| voip/services/busy_lamp_field/subscription_period      | The interval between BLF and SIP SUBSCRIBE messages.<br>Default = 3600 |
| voip/services/busy_lamp_field/local_presence_for_lines | Set to 1 to use local presence.<br>Default = 0                         |

Configuring remote conference call with four or more participants using the following parameters:

| Parameter                             | Description  |
|---------------------------------------|--|
| voip/services/application_server_type | Set the server type to GENERIC.<br>Default = GENERIC   |
| voip/services/conference/conf_ms_addr | Set the address of the server hosting the remote conference.<br>Example: <a href="tel:*66@sbc.teleswyz.ru">*66@sbc.teleswyz.ru</a> |
| voip/services/conference/mode         | Set the mode to REMOTE.<br>Default = LOCAL   |

## D 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.

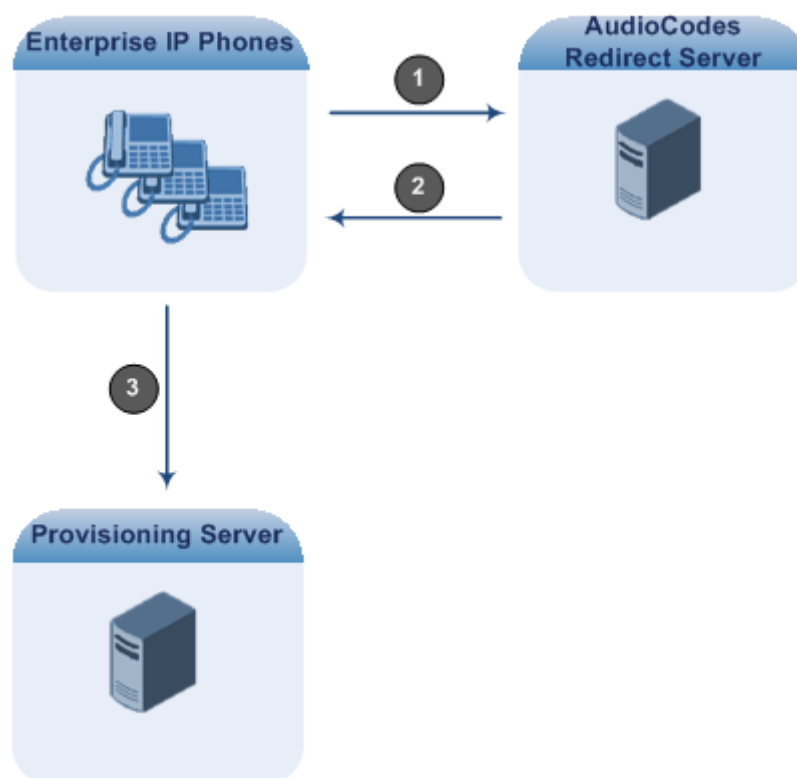
After the phone is powered up and network connectivity is established, the phone automatically requests provisioning information. If it doesn't get it according to the regular provisioning methods, it sends an HTTPS request to AudioCodes' HTTPS redirect server. The server responds to the phone with an 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.



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 URL is: <https://redirect.audiocodes.com>.

**Figure 35: HTTPS Redirect Server Directing Phones to Provisioning Server**



### Redirection Process

Here's how redirection is performed (refer to [Figure 35](#)):

- 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.



The phone repeats the redirect process whenever reset to factory defaults.

## E 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 applicable for C450 & 445HD. 425HD has two image banks/slots for recovery and therefore does not require the recovery procedure.

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](#))

### E.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 36: 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.

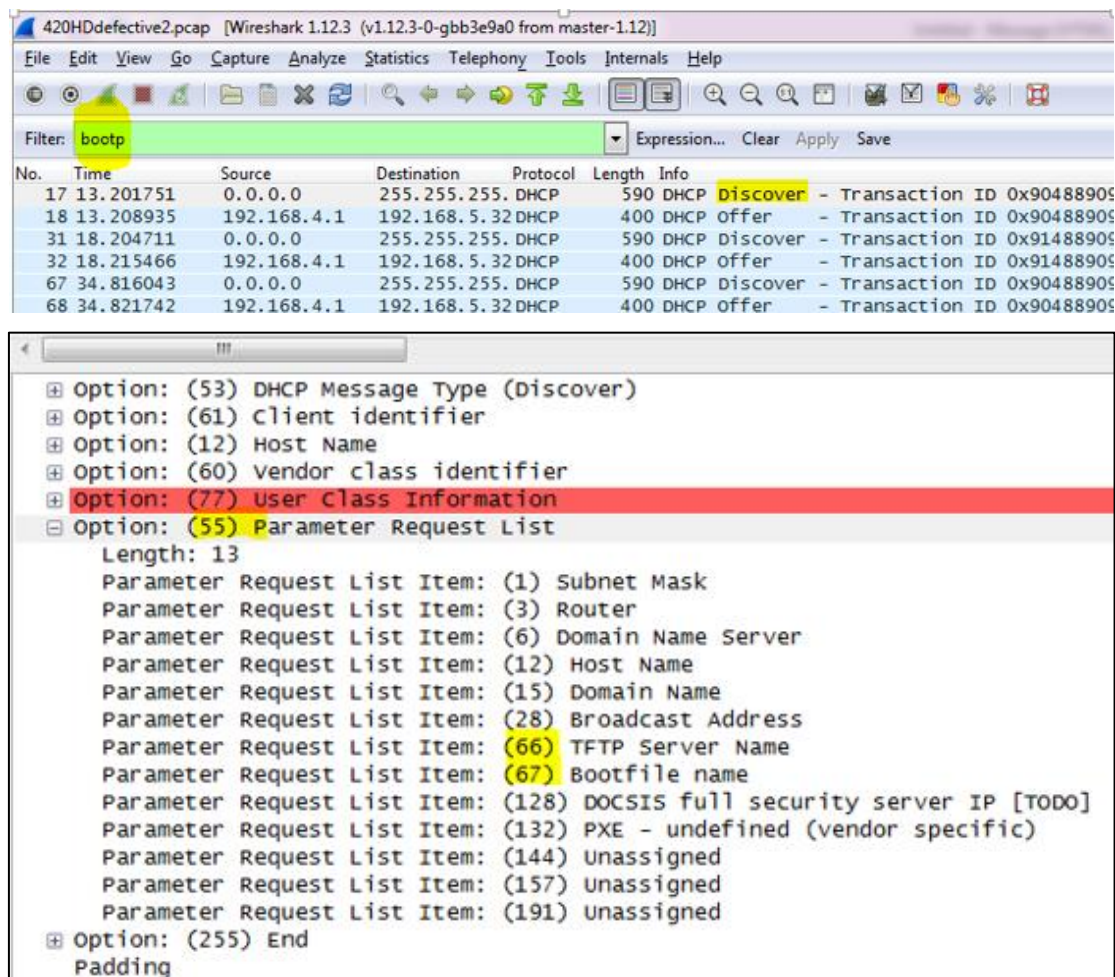
## E.2 Verifying that the Phone is in Recovery Mode

Network administrators can verify that the phone is in recovery mode.

To verify that the phone is in recovery mode:

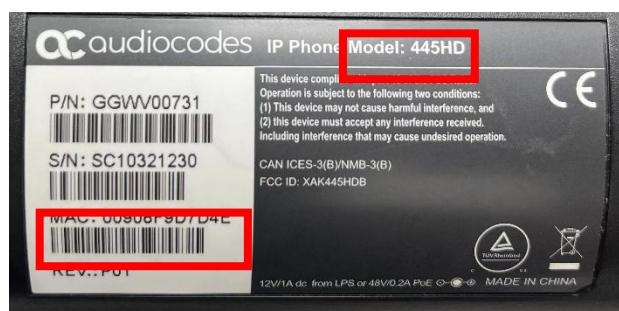
1. Connect the phone to the PC and run WireShark.
2. In WireShark, filter by **bootp** and then check if the phone is requesting Option 66 (TFTP Server) & Option 67 (Boot file) under Option 55 in the 'DHCP Discover' message, as shown in the figures below.

Figure 37: 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 38: Source Ethernet MAC Address in Wireshark Identical to Phone Base's



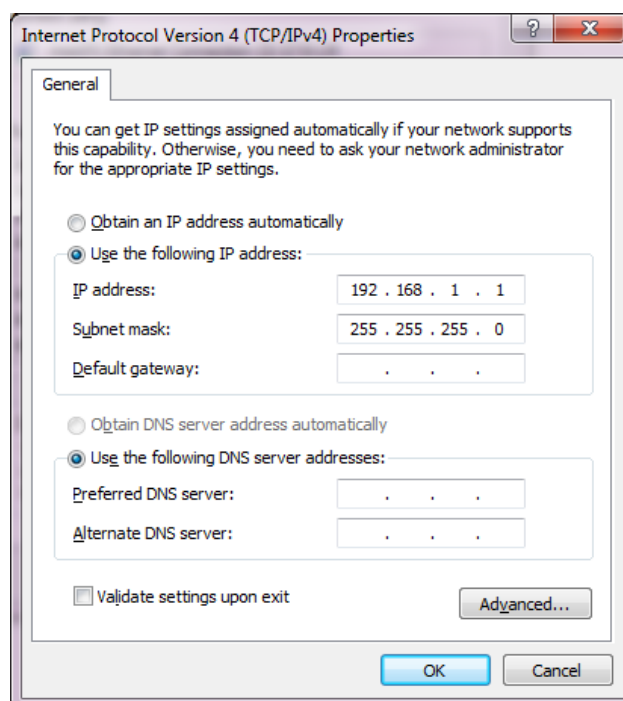
## E.3 Recovering the Phone

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 39](#) 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 39: Recovering the Phone - Configure the PC NIC to which the Phone is Connected**



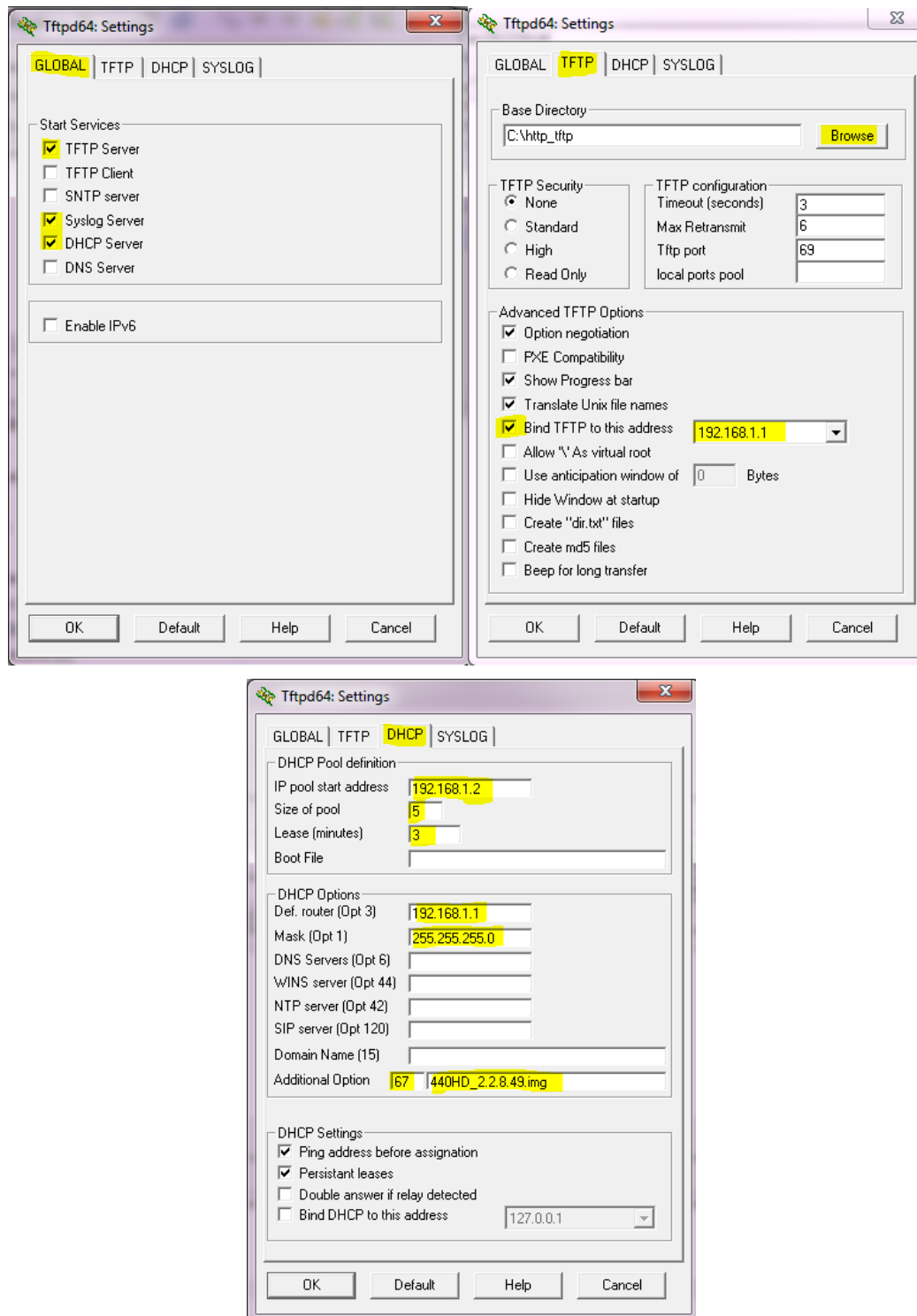
4. Download the following **tftpd64** freeware tool:  
[http://tftpd32.jounin.net/tftpd32\\_download.html](http://tftpd32.jounin.net/tftpd32_download.html)
5. Run the tftpd64.exe executable.
6. Click Settings and configure the following settings:

**Table 107: 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 <b>192.168.1.1</b>                                | 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.

## E.4 Verifying that the Phone is Downloading the Image File

The network administrator can verify that the phone is downloading the firmware image file.

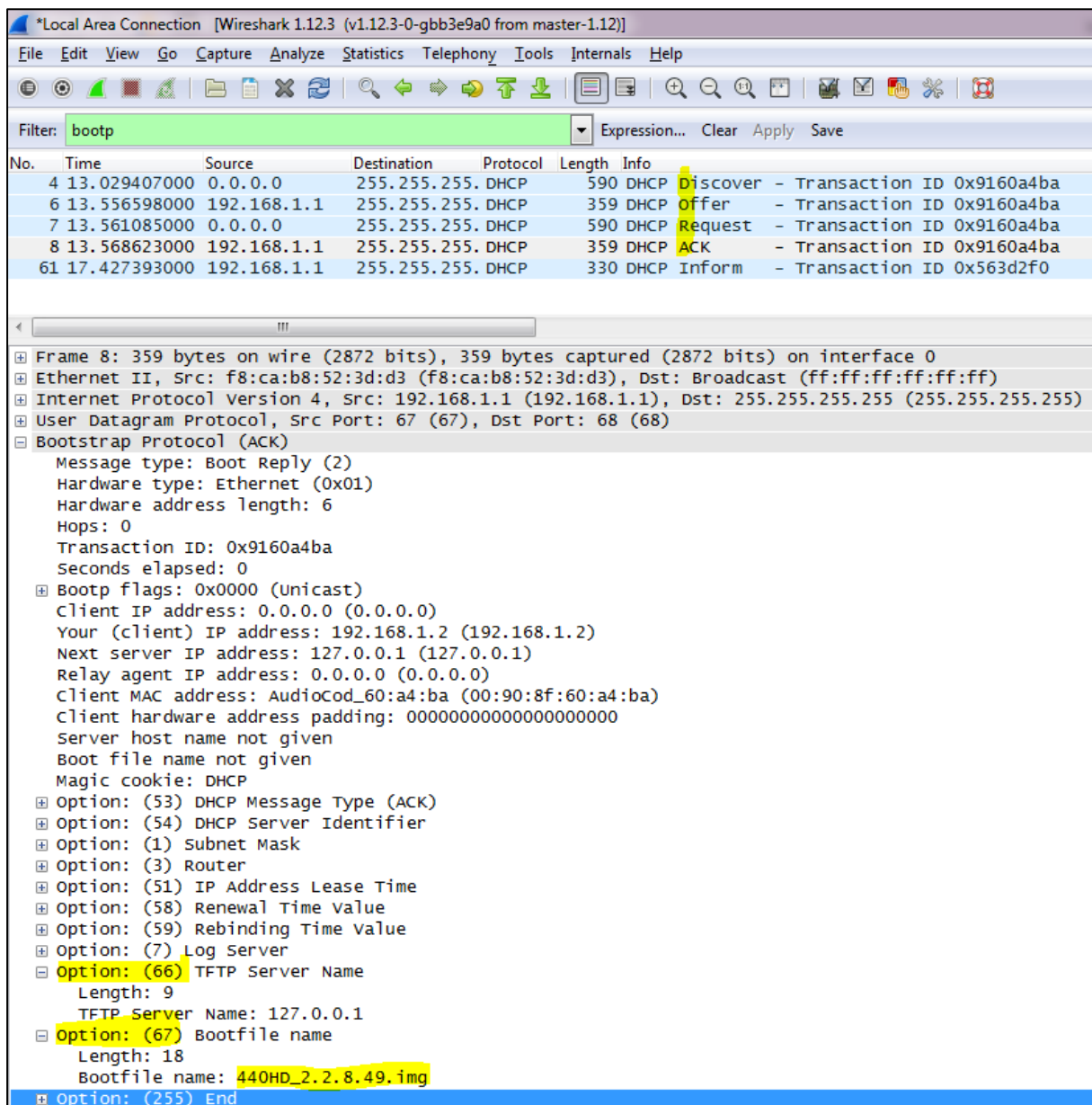
To verify that the phone is downloading the image file, use:

- Wireshark -or-
- tftpd64 -or-
- the phone screen

### E.4.1 Verifying that the Phone is Downloading the Image File Using Wireshark

1. In Wireshark, verify that the four DHCP 'DORA' (Discover; Offer; Request; ACK) steps are accomplished, as shown in the figure below.

Figure 40: Verifying with Wireshark that the Phone is Downloading Phone .img File



- Filter by **TFTP**, as shown in the figure below.

**Figure 41: Verifying .img File Download with Wireshark – Filtering by TFTP**

Wireshark interface showing the filter bar set to **tftp**. The packet list displays the following data:

| No.   | Time         | Source      | Destination | Protocol | Length | Info                             |
|-------|--------------|-------------|-------------|----------|--------|----------------------------------|
| 40012 | 23.860735000 | 192.168.1.1 | 192.168.1.2 | TFTP     | 558    | Data Packet, Block: 19947        |
| 40013 | 23.860735000 | 192.168.1.2 | 192.168.1.1 | TFTP     | 60     | Acknowledgement, Block: 19947    |
| 40014 | 23.860874000 | 192.168.1.1 | 192.168.1.2 | TFTP     | 558    | Data Packet, Block: 19948        |
| 40015 | 23.861483000 | 192.168.1.2 | 192.168.1.1 | TFTP     | 60     | Acknowledgement, Block: 19948    |
| 40016 | 23.861640000 | 192.168.1.1 | 192.168.1.2 | TFTP     | 558    | Data Packet, Block: 19949        |
| 40017 | 23.862268000 | 192.168.1.2 | 192.168.1.1 | TFTP     | 60     | Acknowledgement, Block: 19949    |
| 40018 | 23.862411000 | 192.168.1.1 | 192.168.1.2 | TFTP     | 558    | Data Packet, Block: 19950        |
| 40019 | 23.863113000 | 192.168.1.2 | 192.168.1.1 | TFTP     | 60     | Acknowledgement, Block: 19950    |
| 40020 | 23.863236000 | 192.168.1.1 | 192.168.1.2 | TFTP     | 558    | Data Packet, Block: 19951        |
| 40021 | 23.863909000 | 192.168.1.2 | 192.168.1.1 | TFTP     | 60     | Acknowledgement, Block: 19951    |
| 40022 | 23.864020000 | 192.168.1.1 | 192.168.1.2 | TFTP     | 558    | Data Packet, Block: 19952        |
| 40023 | 23.864948000 | 192.168.1.2 | 192.168.1.1 | TFTP     | 60     | Acknowledgement, Block: 19952    |
| 40024 | 23.865084000 | 192.168.1.1 | 192.168.1.2 | TFTP     | 558    | Data Packet, Block: 19953        |
| 40025 | 23.867477000 | 192.168.1.2 | 192.168.1.1 | TFTP     | 60     | Acknowledgement, Block: 19953    |
| 40026 | 23.867640000 | 192.168.1.1 | 192.168.1.2 | TFTP     | 558    | Data Packet, Block: 19954        |
| 40027 | 23.868322000 | 192.168.1.2 | 192.168.1.1 | TFTP     | 60     | Acknowledgement, Block: 19954    |
| 40028 | 23.868463000 | 192.168.1.1 | 192.168.1.2 | TFTP     | 558    | Data Packet, Block: 19955        |
| 40029 | 23.869159000 | 192.168.1.2 | 192.168.1.1 | TFTP     | 60     | Acknowledgement, Block: 19955    |
| 40030 | 23.869308000 | 192.168.1.1 | 192.168.1.2 | TFTP     | 558    | Data Packet, Block: 19956        |
| 40031 | 23.870009000 | 192.168.1.2 | 192.168.1.1 | TFTP     | 60     | Acknowledgement, Block: 19956    |
| 40032 | 23.870235000 | 192.168.1.1 | 192.168.1.2 | TFTP     | 558    | Data Packet, Block: 19957        |
| 40033 | 23.870898000 | 192.168.1.2 | 192.168.1.1 | TFTP     | 60     | Acknowledgement, Block: 19957    |
| 40034 | 23.871040000 | 192.168.1.1 | 192.168.1.2 | TFTP     | 246    | Data Packet, Block: 19958 (last) |
| 40035 | 23.871442000 | 192.168.1.2 | 192.168.1.1 | TFTP     | 60     | Acknowledgement, Block: 19958    |

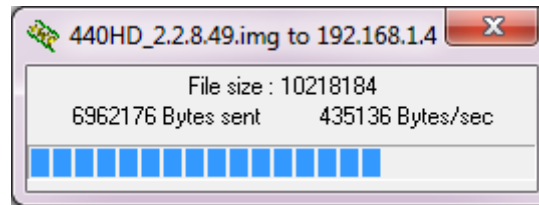
Details of selected packet 40026:

- Frame 40026: 558 bytes on wire (4464 bits), 558 bytes captured (4464 bits) on interface 0
- Ethernet II, Src: f8:ca:b8:52:3d:d3 (f8:ca:b8:52:3d:d3), Dst: AudioCod\_60:a4:ba (00:90:8f:60:a4:ba)
- Internet Protocol Version 4, Src: 192.168.1.1 (192.168.1.1), Dst: 192.168.1.2 (192.168.1.2)
- User Datagram Protocol, Src Port: 53520 (53520), Dst Port: 2000 (2000)
- Trivial File Transfer Protocol
  - [Source File: 440HD\_2.2.8.49.img]
  - Opcode: Data Packet (3)
  - Block: 19954
  - Data (512 bytes)

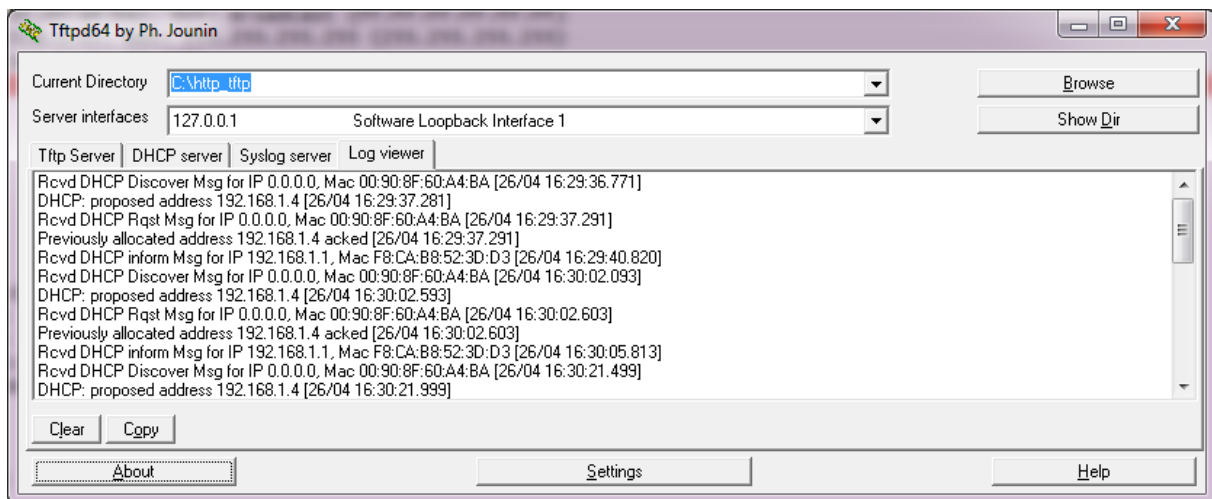
## E.4.2 Verifying That the Phone Is Downloading the Image File Using TFTP Server App

In **TFTP Server**, view the indications shown in the figures below.

**Figure 42: Verifying .img File Download using TFTP Server**



**Figure 43: Verifying .img File Download using TFTP Server**



### E.4.3 Verifying That the Phone Is Downloading the Image File Using the Phone

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.



**Important:** Do not unplug / power-off the phone while the screen displays the message shown below.

## F Supported SIP RFCs and Headers

The following is a list of supported SIP RFCs and methods you can use for the phone.

**Table 108: Supported IETF RFCs**

| RFC Number  | RFC Title   |
|---|---|
| <b>RFC 2327</b>   | SDP   |
| <b>RFC 2617</b>   | HTTP Authentication: Basic and Digest Access Authentication   |
| <b>RFC 2782</b>   | A DNS RR for specifying the location of services  |
| <b>RFC 2833</b>   | Telephone event   |
| <b>RFC 3261</b>   | SIP   |
| <b>RFC 3262</b>   | Reliability of Provisional Responses in SIP   |
| <b>RFC 3263</b>   | Locating SIP Servers  |
| <b>RFC 3264</b>   | Offer/Answer Model  |
| <b>RFC 3265</b>   | (SIP)-Specific Event Notification   |
| <b>RFC 3310</b>   | Hypertext Transfer Protocol (HTTP) Digest Authentication Using Authentication and Key Agreement (AKA) |
| <b>RFC 3326 (Partially Supported)</b>                         | Reason header   |
| <b>RFC 3389</b>   | RTP Payload for Comfort Noise   |
| <b>RFC 3515</b>   | Refer Method  |
| <b>RFC 3605</b>   | RTCP attribute in SDP   |
| <b>RFC 3611</b>   | RTP Control Protocol Extended Reports (RTCP XR)   |
| <b>RFC 3665</b>   | SIP Basic Call Flow Examples  |
| <b>RFC 3711</b>   | The Secure Real-time Transport Protocol (SRTP)  |
| <b>RFC 3725</b>   | Third Party Call Control  |
| <b>RFC 3842</b>   | MWI   |
| <b>RFC 3891</b>   | "Replaces" Header   |
| <b>RFC 3892</b> (Sections 2.1-2.3 and 3 are supported)        | The SIP Referred-By Mechanism   |
| <b>RFC 3960</b> (Partially Supported)                         | Early Media and Ringing Tone Generation in SIP (partial compliance)                                   |
| <b>RFC 3966</b>   | The tel URI for Telephone Numbers   |
| <b>RFC 4028</b> (Partially Supported)                         | Session Timers in the Session Initiation Protocol   |
| <b>RFC 4240</b>   | Basic Network Media Services with SIP - NetAnn  |
| <b>RFC 6035</b>   | RTCP XR information publishing for Quality of Experience server monitoring.                           |
| <b>draft-ietf-sip-privacy-04.txt</b><br>(Partially Supported) | SIP Extensions for Network-Asserted Caller Identity using Remote-Party-ID header                      |
| <b>draft-ietf-sipping-cc-transfer-05</b>                      | Call Transfer   |

| RFC Number                                   | RFC Title  |
|--|--|
| <b>draft-ietf-sipping-realtimefax-01</b>     | SIP Support for Real-time Fax: Call Flow Examples            |
| <b>draft-choudhuri-sip-info-digit-00</b>     | SIP INFO method for DTMF digit transport and collection      |
| <b>draft-mahy-sipping-signaled-digits-01</b> | Signaled Telephony Events in the Session Initiation Protocol |



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 109: 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 110: 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       |

## G RTCP-XR Parameters

The following table lists the RTCP-XR parameters that may be reported to the QoE server.

**Table 111: RTCP-XR Parameters**

| Group                      | Metric Name                      |
|----------------------------|----------------------------------|
| <b>General</b>             | Start Timestamp                  |
|                            | Stop Timestamp                   |
|                            | Call-ID                          |
|                            | Local Address (IP, Port & SSRC)  |
|                            | Remote Address (IP, Port & SSRC) |
| <b>Session Description</b> | Payload Type                     |
|                            | Payload Description              |
|                            | Sample Rate                      |
|                            | Frame Duration                   |
|                            | Frame Octets                     |
|                            | Frames per Packets               |
|                            | Packet Loss Concealment          |
|                            | Silence Suppression State        |
| <b>Jitter Buffer</b>       | Jitter Buffer Adaptive           |
|                            | Jitter Buffer Rate               |
|                            | Jitter Buffer Nominal            |
|                            | Jitter Buffer Max                |
|                            | Jitter Buffer Abs Max            |
| <b>Packet Loss</b>         | Network Packet Loss Rate         |
|                            | Jitter Buffer Discard Rate       |
| <b>Burst Gap Loss</b>      | Burst Loss Density               |
|                            | Burst Duration                   |
|                            | Gap Loss Density                 |
|                            | Gap Duration                     |
|                            | Minimum Gap Threshold            |
| <b>Delay</b>               | Round Trip Delay                 |
|                            | End System Delay                 |
|                            | One Way Delay                    |
|                            | Interarrival Jitter              |
|                            | Min Absolute Jitter              |
|                            | Signal                           |
|                            | Signal Level                     |
|                            | Noise Level                      |
| <b>Quality Estimates</b>   | Listening Quality R              |
|                            | RLQ Est. Algorithm               |
|                            | Conversational Quality R         |

| Group | Metric Name           |
|-------|-----------------------|
|       | RCQ Est. Algorithm    |
|       | 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
```



Remote Metrics are not supported in this version.

# I Intrado ERS Location Information Service (HELD)

Support Intrado ERS Location Information Service (HELD)

HELD (HTTP-Enabled Location Delivery) is a protocol that allows devices to request location information from a Location Information Service (LIS). Devices supporting the HELD protocol can seamlessly integrate with ERS via the HELD service. This service is available for ERS Enterprise SIP accounts and requires special activation and configuration.

HELD-compliant hard phones and softphones send network information to the ERS in an XML request. ERS then determines the phone's location based on a pre-provisioned network map and sends the location back to the phone as a locationURI or civic address. During a call, the phone includes the locationURI in the SIP invite, enabling ERS to route the call to the appropriate PSAP (Public Safety Answering Point).

**Table 112: HELD Configuration**

| Parameter                           | Description  |
|-------------------------------------|--|
| location/HELD/server_url            | Specify the HELD Server URL.   |
| location/HELD/request_location_type | Either LocationURI, Civic, LocationURI_and_Civic.  |
| location/HELD/nai.enable            | Network Access Identifier (NAI).<br>Default = 1 (Boolean)  |
| location/HELD/Identity              | Set the vendor-specific element to include in a location request message.<br>Default = CompanyID |
| location/HELD/Identity_value        | Set the value for the vendor-specific element to include in a location request message.          |
| security/HELD_certificate_url       | Certificate URL to use for server secure connection.   |
| security/HELD_private_key_url       | Private key URL to use for server secure connection.   |

**Table 113: HELD Status**

| Parameter                                     | Description   |
|---|---|
| status/diagnostics/lldp/chassis/chassisId     | Chassis ID of the switch that the device is connected to.<br>MAC address: 12-digit hexadecimal number represented by colon- hexadecimal notation. Interface Name: String format.<br>Example: <ChassisID>AgcEiFqSa oqA</ChassisID> |
| status/diagnostics/lldp/chassis/portId        | ID of the switch port that the device is connected to.<br>MAC address: 12-digit hexadecimal number represented by colon- hexadecimal notation. Interface Name: String format.<br>Example: <PortID>BAkFR2kyLzA vMTc=</PortID>      |
| status/diagnostics/lldp/chassis/chassisIdType | ERS supports the following Chassis ID subtypes: <ul style="list-style-type: none"> <li>■ "Switch Hostname" / (6)</li> <li>■ "Switch IP" /(5)</li> <li>■ "Switch MAC Address"/(4)</li> </ul>                                       |

|   |  |
|---|--|
| status/diagnostics/ldp/chassis/portIdType | ERS supports the following Port ID subtypes: <ul style="list-style-type: none"><li>■ "Port Name" (5)</li><li>■ "Port MAC Address" /(3)</li></ul> |
|---|--|

**International Headquarters**

Naimi Park  
6 Ofra Haza Street  
Or Yehuda, 6032303, Israel  
Tel: +972-3-976-4000  
Fax: +972-3-976-4040

**AudioCodes Inc.**

80 Kingsbridge Rd  
Piscataway, NJ 08854, USA  
Tel: +1-732-469-0880  
Fax: +1-732-469-2298

Contact us: <https://www.audiocodes.com/corporate/offices-worldwide>

Website: <https://www.audiocodes.com>

©2026 AudioCodes Ltd. All rights reserved. AudioCodes, AC, HD VoIP, HD VoIP Sounds Better, IPmedia, Mediant, MediaPack, What's Inside Matters, OSN, SmartTAP, User Management Pack, VMAS, VoIPerfect, VoIPerfectHD, Your Gateway To VoIP, 3GX, AudioCodes One Voice, AudioCodes Meeting Insights, and AudioCodes Room Experience are trademarks or registered trademarks of AudioCodes Limited. All other products or trademarks are property of their respective owners. Product specifications are subject to change without notice.

Document #: LTRT-09993

